Assessing the threat landscape of sectors as they adopt cloud-based email services

Prevalence of cloud service providers in crucial sectors

F. Z. Ghuman

Technische Universiteit Delft

TU Delft

Assessing the threat landscape of sectors as they adopt cloud-based email services

Prevalence of cloud service providers in crucial sectors

by

F. Z. Ghuman

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Tuesday March 29, 2022 at 12:30 PM.

Student number:	4364554	
Project duration:	November 30, 2021 – March 2, 2022	
Thesis committee:	Dr. -ing. T. Fiebig,	TU Delft, supervisor
	Dr. F. S. Gürses,	TU Delft, supervisor
	Dr. Ir. C. Hernandez Ganan,	TU Delft, chair

This thesis is confidential and cannot be made public until March 29, 2022.

TU Delft

Preface

Before you lies my master thesis. A project I knew would not be a piece of cake since the start of my studies. Yet, I had never expected that I would learn this much from this. The process of completing this research was far from straightforward. Still, I can happily say that I have gained a lot of knowledge from the continuous process of iterations.

I would like to thank my first supervisor, Dr. -Ing. T. Fiebig for his patience and support. You provided me with very valuable feedback that steered my direction. I would also like to thank my second supervisor, Dr. F. S. Gürses for her critical feedback. Your comments allowed me to reflect on the concept of privacy. Finally, I would also like to thank my chair, Dr. Ir. C. Hernandez Ganan for his valuable comments.

I am very grateful to this Graduation Committee.

F. Z. Ghuman
The Hague, March

Abstract

Email communication is a crucial part of the daily processes of enterprises. Organizations can opt for traditional infrastructure on-premise or use cloud-based email services provided by (foreign) cloud service providers. In Europe in particular, organizations from crucial sectors have been adopting cloud-based email services. The level of cloud adoption can vary strongly within these sectors. Nevertheless, this trend towards the use of cloud-based email services brings societal implications for the sovereignty of European data. Email services hosted with foreign cloud service providers can be susceptible to surveillance by foreign governments and intelligence agencies, which violates privacy of European individuals. The attack space further includes invasion with political and monetary incentives that may also impact security, as data is hosted with cloud service providers who might have weak security protocols. We measured the level of cloud adoption for seven crucial sectors in Europe: executive governments, healthcare, SME's, higher educational institutes, NGO's and financial services. We have conducted a DNS analysis on MX records from a Farsight (SIE) dataset to measure the prevalence of cloud service providers. The results revealed the prevalence of extremely dominant cloud service providers, Microsoft and Google in Europe. The dominant position obtained by these providers means that two aspects in governance of this socio-technical system in Europe must be attended to if Europe wants to regain control over their data and infrastructures: (1) European regulation focus needs to shift and (2) awareness must be raised at managerial level in enterprises.

Contents

1 Introduction

This chapter will introduce the research problem. We will provide background context to the problem and identify the research gap. The research gap will lead to the research objects, that we aim to explore with this research. Finally, we will set out the research outline.

1.1. Introduction to email

In this section, we introduce the importance of email in the modern world and its shift towards cloud-based email services. We also introduce the impact of the Corona pandemic on the adoption of cloud-based email services.

1.1.1. The notion of email in today's world

Email is a traditional yet popular means of communication in diverse application domains. These electronic mails had initially begun to relay information over the internet rapidly, and soon became acknowledged as legitimate documents. The electronic mail system attained acceptance not just for communication purposes, but also became an effective channel for transmission of sizeable files and documents (Dey, Roy, Bose and Sarddar, 2021). The increase in daily exchanged messages, the sum of user accounts and the count of devices that are being accessed for email have been growing continuously (Cecchinato, Sellen, Shokouhi and Smyth, 2016). Email service provides many advantages for various organizations in these times such as ease of use, speed and less time zone barriers (Acevedo, 2016). In addition, email provides the convenience to maintain history and records of file exchanges, which led the email system to take up a significant position for many businesses. Until a few years ago, many firms were dependent on on-premise email hosting. However, with the progression of cloud computing technology, a spectrum of new opportunities transpired with the hosting of email infrastructure in the cloud (Dey et al., 2021).

1.1.2. Covid-19 and the cloud adoption phenomena

Thus, so far a notable phenomena in the horizon of email is the rise in cloud adoption and the use of Software-as-a-service (SaaS), normalizing the delegation of email services to third party providers with novel technology. Besides the motion of organizations to work remotely during the the covid-19 pandemic (Help Net Security, 2020; Mandal and Khan, 2020), an unforeseen elevation in the use of cloud services to maintain technical infrastructure and adapt computation needs has been introduced. This passive effect of the coronavirus (Zhong et al., 2020; Mandal and Khan, 2020) ensures that organizations spread across healthcare, education or e-commerce, can keep working seamlessly from home by having the facility to access critical infrastructure. Moreover, decisions by companies to prepare for corona related shutdowns include a move to host more applications in the cloud by 51% in 2021 (Help Net Security, 2020). Despite the continuation of business operations through remote login, this trend adds to existing implications with cyber security in cloud-based environments. It is also expected that the cyber attack surface will grow in the future (Mandal and Khan, 2020).

1.2. Problem introduction

A cyber security attack on email systems can reveal sensitive information and have a severe impact on involved individuals. In 2016, the personal emails of John Podesta, the chair of Clinton's 2016 presidential campaign had been compromised in a spear phishing attack (CBS News, 2016). The breach in which his Gmail account had been hacked, disclosed some of his work-related emails. The emails were released by WikiLeaks and clearly explained the insides of the Clinton campaign to the point of upcoming hall meetings and speeches by Clinton (Aisch, Huang and Kang, 2016). Security incidents that impact users' privacy in this manner need to minimized. In the case of political figures, this may even damage the victims reputation. Similar pressing concerns were emphasized by Edward Snowden, who provided insights in the inner workings of the NSA with its intelligence partners across the world. These revelations unveiled the mass surveillance programs which were executed by NSA, and turned out to be active without public awareness (Courage Snowden, 2014).

1.2.1. Cloud-based email services in sectors

Similar to any novel technology, cloud services pose major challenges and opportunities for different sectors. For example, higher educational institutions may shift to cloud services due to low costs, low maintenance or the use of the current technology (Srinivasan, 2011). On the other side, certain businesses can be seen willing to take up the risks for the overpowering benefits since 2012 in the research of Alge. He further states that correct security levels could bring huge benefit to the migration of emails and services to the cloud for both large and small businesses. However, certain uncertainties can arise if particular sectors with a lot of sensitive data at stake decide to deploy cloud based email services. For example, healthcare professionals, which deal with highly personal data on daily basis and are often targeted by attackers. Governments also deal with civilians' personal data. If such susceptible groups use cloud based email services, like Gmail, this may introduce complex challenges in the aim to protect their personal data. We closely follow the move towards cloud adoption in the following sectors:

Executive government: Cloud computing technology has the potential to offer multiple advantages to public administrations. This has been indicated by practitioners and academics, however, cloud adoption in public administration has still been observed to be slow as a result of different influencing factors. Regardless, cloud computing services are expected to be a foundation for the upcoming e-government strategy (Nanos, Manthou and Androutsou, 2019).

Non-governmental organizations (NGO's): Particularly after the breakout of the covid-19 pandemic, the way in which NGO's have been functioning has changed significantly. This has led to a rise in the adoption of cloud services. Previous initiatives with NGO's and international firms in Switzerland have illustrated that the shift towards cloud based services can be labeled unavoidable on the long term (Deloitte Switzerland, 2021).

Healthcare: Application of cloud computing technologies has been investigated for several use cases and suggested to offer opportunities including provision of better access to patient records (Idoga et al., 2019) and increased accessibility to stored information on servers (Sharma and Sehrawat, 2020). In 2014, healthcare providers found a Software-as-a-Service based cloud usage of 66.9% globally among IT executives, which implies the growing acceptance towards cloud technology in this sector (Columbus, 2014; Sharma and Sehrawat, 2020).

Higher educational institutes: In higher educational institutes, a move towards Software-as-a-service applications has been observed in different countries in Europe. For several countries, a constant shift of core functionalities to the cloud can be recognized depending on certain socio-economic determinants (Fiebig et al., 2021).

Large companies: Currently, there is a lack of empirical research to the cloud adoption at business level, but benefits of cloud computing technology in various organizations have shown to be highly favourable for large firms also. While it is commonly believed that large firms are frontrunners in adoption of the newest technology, research by (Karunagaran, Mathew and Lehner, 2019) illustrates that large companies find characteristics of cloud technology complicated to implement.

Financial services: The trend to shift services to cloud platforms in the financial services sectors to solve issues relating to customer availability and data storage has become prevalent. Employment of cloud services enable financial services organizations to provide more opportune and exact services to their customers. Also, dynamics of cloud computing services allow for great scalability, flexibility and low costs, making cloud adoption attractive for this business sector (Hariharan, 2021).

Small and Medium Enterprises (SME's): In the SME's sector, cloud computing has become valuable due to its unique characteristic of providing on-demand service. As SME's have a fairly limited IT budget compared to large companies, development of their internal IT infrastructure is usually infeasible (Khayer, Talukder, Bao and Hossain, 2020). Therefore, SME's possess insufficient IT experts and poor technological competence, thus have to rely on external IT providers to obtain the required outputs. Hence, cloud computing can create opportunities for SME's to deploy novel technologies, which were previously inaccessible (Marston et al., 2011; Khayer et al. (2020)).

1.2.2. Cloud and Security complications

The expansion of network technology and the massive volume of data has introduced pressing concerns with regards to information security (Zaki et al., 2017; Xu, 2018). Email accounts of users and mail servers have always been an ideal target by invaders. They involve collections of valuable private information from years back, but still are easy to jeopardize (Koh, Bellovin and Nieh, 2019). Apart from the phishing attack on John Podesta (CBS News, 2016), many prominent examples exist. The email compromise of Putin's top aides in 2016, or the email disclosure of Sarah Palin (former Vice President candidate)(The Washington Times, 2008) and John Brennan (Director of CIA) (Franceschi-Bicchierai, 2015) show that often high profile figures and firms are targeted with the aim of damaging their reputations. John Podesta's login credentials had been obtained in the spear-phishing attack to access his Gmail account. Sarah Palin's Yahoo account had been accessed by a straightforward password recovery and reset attack. Finally, John Brennan's AOL email account had been probed by social engineering techniques. Aggressors can even capture entire mail servers or endanger them, such as the Sony Pictures case (WikiLeaks-Sony Archives, 2018). The conventional narrative shows that the compromise reveals the complete past record of the targeted user's emails (Koh, Bellovin and Nieh, 2019).

Security is a fundamental principle in the field of information and communication and achieves Confidentiality, Integrity and Availability (CIA) objectives for protection of privacy of individuals (Metheny, 2017). Alge (2012) noted that organizations have kept a reluctant stance on moving email hosting to the cloud in the past with security being the main reason for that. Emails contain sensitive data, which makes it risky for these organizations to entrust the safety of these communications to third parties. Email is vulnerable to several threats, for example, eavesdropping: as email messages move through large networks, it is quite easy for intruders to track and capture the email message (Adeyinka, 2008). Therefore, protection of information is of crucial significance for individuals as it holds sensitive data ranging from shopping behavior, travelling, online banking to social networking for instance (Zaki et al., 2017).

1.2.3. Privacy complications due to dominance of cloud players

The wide adoption of cloud-based service in the modern-day drives multiple fundamental privacy concerns (Henze, Hiller, Hohlfeld, and Wehrle, 2016; Hiller, Kimmerlin, Plauth and Heikkila, 2018). This is indicated by the disclosure of the global surveillance programs by Snowden (Courage Snowden, 2014). The centralized nature of cloud computing can be considered as the root source of this, as the cloud computing services market is dominated by only a certain number of cloud service providers. As a consequence, privacy issues such as a lack of trust, data ownership and legal hindrances on data location, prompt users and businesses to look for a substitute cloud service provider, specifically in the case of a USA based provider (Pearson and Benameur, 2010; Ion et al., 2011; Henze et al., 2016). These factors hinder further growth of cloud computing technology, because users are left with limited control over their personal offloaded data. At the moment, transparency is not always maintained with

regards to where the actual data is being stored and processed by the cloud service providers (Hiller et al., 2018). In addition, lacking transparency on the purpose of data usage augments the perception of having less control over data by users. These facets influence the view users have about cloud services in a negative manner (Henze et al., 2013; Henze et al., 2014). Despite these privacy concerns, cloud services offer attractive functions that often cannot be overlooked by competitive and innovative firms (Henze et al., 2016).

1.3. Research gap

This section identifies the research gap derived from preceding research in this field which we aim to investigate.

1.3.1. Literature review

Email has been facing a shift from a considerably decentralized infrastructure to a centralized infrastructure (Marston et al., 2011). Henze, Sanford and Hohlfeld (2017) investigated the prevalence of cloud computing in the email landscape among internet domains in a measurement study. They analyze this by detecting SMTP servers in the cloud-based environment, and then assess the cloud usage among .com/.net/.org domains. They investigated this transition towards a centralized cloud-based infrastructure and its implications. Relevant observations include the fact that between 13% and 25% of users' emails have been processed by cloud service providers in 2016. Their findings regarding the email infrastructure illustrate that any email sent to a .com/.net/.org domain has a chance of higher than 50% to appear in the cloud.

Fiebig et al. (2021) examined the migration of universities in US and Europe to public clouds by performing a measurement study. They also looked into implications that may arise due to this shift. A frequent pattern of has been identified in the US, UK, the Netherlands and the TOP100 that frequently outsources the universities' main functions to the cloud. However, the research raised concerns about compromised privacy of individuals involved. For example, a lack of transparency in sensitive data collection and processing thereof by cloud service providers has been highlighted (Jones et al., 2020; Lindh and Nolin, 2016; Marek and Skrabut, 2017). A prior research to get insight into readiness of South African higher educational institutes to adopt cloud-based email service by Willet in 2014, also highlighted several concerns regarding privacy and compliance to laws and regulations.

In the financial services sector, the use of cloud computing services including cloud-based email services in general has been investigated (Hon and Millard, 2018). Banks have been using cloud-based email for correspondence with customers and email filtering services. The surveys pointed towards a development in the banking industry: the use of cloud services might begin as a 'shadow cloud' which entails that individual personnel may sign up for cloud-based services without formal approval and compliance checks. A quantitative study by Lundin (2020) looked into factors inducing adoption of cloud services such as email service, among different industrial organizations. The improvement of the followed cloud strategy is a main factor that organizations and cloud service providers should focus on for effective cloud adoption.

Identified knowledge gap

The current cloud adoption trend by organizations has spread to different extents among various sectors, e.g. education, healthcare (Mandal and Khan., 2020), financial services (Hon and Millard, 2018), governments (Anwar, Umair, Sikander and Ubedin, 2019), large companies, SME's (Karunagaran, Mathew and Lehner, 2019) and NGO's (Deloitte Switzerland, 2021). Henze, Sanford and Hohlfeld (2017) and Fiebig et al. (2021) found a prevalence of cloud-based email services on the internet domains and in the particular higher education section. However, the current level of cloud-based email services among these crucial sectors may differ in various sectors depending on internal and external factors. In a risk assessment for cloud adoption, apart from a lack of control over company assets, new security issues have been introduced as a consequence of the rapid expansion in cloud technology (Gritzalis, Stergiopoulos, Vasilellis and Anagnostopoulou, 2020). In addition, traditional risk management methodologies do not seem to suffice the current requirements of firms if they outsource their

operations to the external cloud service providers. Privacy and security related threats such as these combined, constitute to the articulation of a yet undefined threat landscape for these sectors individually. Thus, depending on the extent to which email services have been outsourced in these sectors, the vulnerability may also vary per sector. Therefore, we see the necessity to assess the threat landscape for these sectors in order to define a future prospects.

1.3.2. Scope of the research

Sharing data has never been a matter without implications (Hilden, 2021). Especially, since the exposal of the US surveillance offences and its linked legal and regulatory framework complicate digitisation in Europe, especially in the governmental sector (European Commission, 2010). The use of cloud services transfers control of data and infrastructures to the cloud service provider (Irion, 2012; Hilden, 2021). In situations where transfer of data across borders is needed, the chance of jurisdictional problems exists. Notably, these trans-border floods of private information provoke clashes between abilities of authoritative surveillance instances from countries like the US or China and fundamental rights. Seeing that most popular cloud-based email service providers are based in the US, e.g. Google and Microsoft, it is challenging to come to terms with the European data security requirements and the regulatory framework of the US (Hilden, 2021). Further implications arise when the US CLOUD Act allows law enforcers to impel US-based cloud service providers to publish data stored on their servers if they possess a valid warrant (LII/Legal Information Institute, 2018). Therefore, it has become crucial to evaluate the susceptibility of sensitive European data carried by indispensable sectors in Europe as it is endangered by various external and socio-economic factors.

1.4. Research Objectives

The research objectives revolve around setting out the main objective and questions which we strive to answer in this research.

1.4.1. Main objective and research question

Reflecting back on the previous literature review, we briefly situate the research objective:

Analyze the prevalence of dominant cloud service providers and investigate which implications this may bring for sensitive European data hosted with cloud service providers.

Based on this, we can lay out a threat scenario analysis, which will form the foundation of the requirements we find for each sector. Summarizing, current research is rather limited about the question whether certain sectors move from email infrastructure to cloud based services. Several challenges and threats can arise, which possibly may be hindering potential benefits for various organizations on educational, business or governmental level. We formulate the research question as:

How does the future threat landscape look like for different sectors in Europe as they adopt cloud-based email services?

Therefore, deducing from this research aim, we strive to bring more insight about current factors influencing these sectors to opt for different cloud service providers and patterns that might have appeared over time in the previous five years.

1.4.2. Sub questions

The research objective has been divided into five sub questions:

1. To what extent are emerging privacy and security threats shaping the cloud-based mail ecosystem?

In the first sub question we will gain more insight about the complex cloud based mail ecosystem in which the research problem is situated. We will evaluate the current background setting from different perspectives: Technical domain, Institutional domain and Process domain. In the technical domain, we will have a closer look at the existing email infrastructures and its mechanisms. Also, we will look at how privacy and security has been implemented in this and how it may effect the technical infrastructure environment. In the institutional background, we will shed light on various regulations and institutions as

they influence the system. The involvement of many stakeholders, such as the cloud service providers, private companies, governmental organizations or educational institutes in the process system makes this ecosystem more complex as they each have their own motivations. This research questions aims to analyze this complexity by performing an in-depth literature study of the various facets of the problem. The final product will be the formulation of a theoretical framework on the basis of this insight. A deep understanding of the cloud based email infrastructure and how the infrastructure has evolved over the years is required to form the basis of this framework. This insight will allow us to understand the emerging threat scenario as organizations may move to cloud-based email services.

2. What is the level of cloud-based email adoption per sector?

In the second question we will measure the extent of email cloud adoption per sector. For each sector, we will measure the extent of cloud based email services that can be observed on the SMTP servers. This will provide us an overall view of the ongoing cloud adoption move in the different sectors. We will use lists of companies to identify certain sectors in the bailiwick field of the dataset. The result of this question will be mostly quantitative.

3. Which are the most prevalent cloud service providers among crucial sectors?

We will look at the most prevalent cloud service providers in terms of (1) email hosting and (2) security services among the domains collected for the sectors. We will perform a frequency analysis for gaining more insight regarding this. For this, we will first differentiate between large cloud service providers and smaller ones. Then we will look at the occurrence of each of these providers in the rdata per bailiwick and per cluster of sector. The subdomain in the rdata will indicate the use of a large email service provider. For example, if one organization uses Google, the subdomains in the rdata will contain 'google.com' or 'googlemail.com'. This information will be aggregated into visualizations, and therefore the used data will be quantitative.

4. To what extent does the dominance of cloud service providers impact the sovereignty of European data held by crucial sectors?

In this question we will try to find relations between the identified clusters of sectors and their preference for certain cloud service providers, if any. We will investigate the result of the previous question, thereby analyzing which providers have been dominant in the past, and which providers have become prevalent over the years. Then we will analyze the effect of this phenomena as it influences the privacy and security of European data held by sectors. We will use our background literature, input variables from question (2) and (3) to define our assessment framework and use it to assess the impact of the prevalence of cloud service providers.

5. What are the requirements of the organizations with regard to opting for cloud based email services in order to mitigate emerging cloud threats?

In this question we will interpret the gained results and assess what the current and future threat scenario may be by performing a threat scenario analysis per sector. Based on this, we will try to formulate requirements that may drive the identified groups to move cloud based email services. This is a relevant aspect of the problem, as the data in the cloud often belongs to these individuals and their privacy might be compromised due to being vulnerable to legal extraction by governments. We will look at the impact of the cloud usage on vulnerable sectors and assess their susceptibility in the future with regards to the safeguarding of their private email data. The data used for this question will be qualitative.

1.5. Link to Complex Systems Engineering and Management

This thesis will be conducted in the completion of the Master Complex Systems Engineering and Management. We analyze a complex systems engineering situation withing a multi-actor setting. In order to do this, we designed three subsystems: technical design, institutional design and process design. These subsystems will evaluate the cloud-based mail ecosystem from different perspectives, eventually leading to a threat landscape which constitutes a multi-faceted framework model. The technical design and institutional design more or less identify what needs to be changed in the overall system (Steenhuisen, 2019). On the other hand, the process design shows insights into how it should be changed (Steenhuisen, 2019). Thus, the process subsystem is a combined product of the technical and institutional subsystem, which lead to an integrated all encompassing framework.

1.6. Research outline

We outline the Methodology for the literature study in section 2. The technical threat landscape is explored in Chapter 3, which is followed by the institutional threat landscape in Chapter 4. Chapter 5 explores variables in the process threat landscape. In Chapter 6, we perform data analysis and present visualizations. Chapter 7 interprets and discusses the threat landscape as a consequence of this. Finally, in Chapter 8 we formulate concrete conclusions on the basis of the results.

2

Methodology

In this Chapter, we will discuss the flow of the research. First, we will explain the research design, which contains a general flow of the followed research methodology. After this, we will step wise explain the main aspects of the research process, which are the literature review, the data analysis and threat assessment.

2.1. Research design

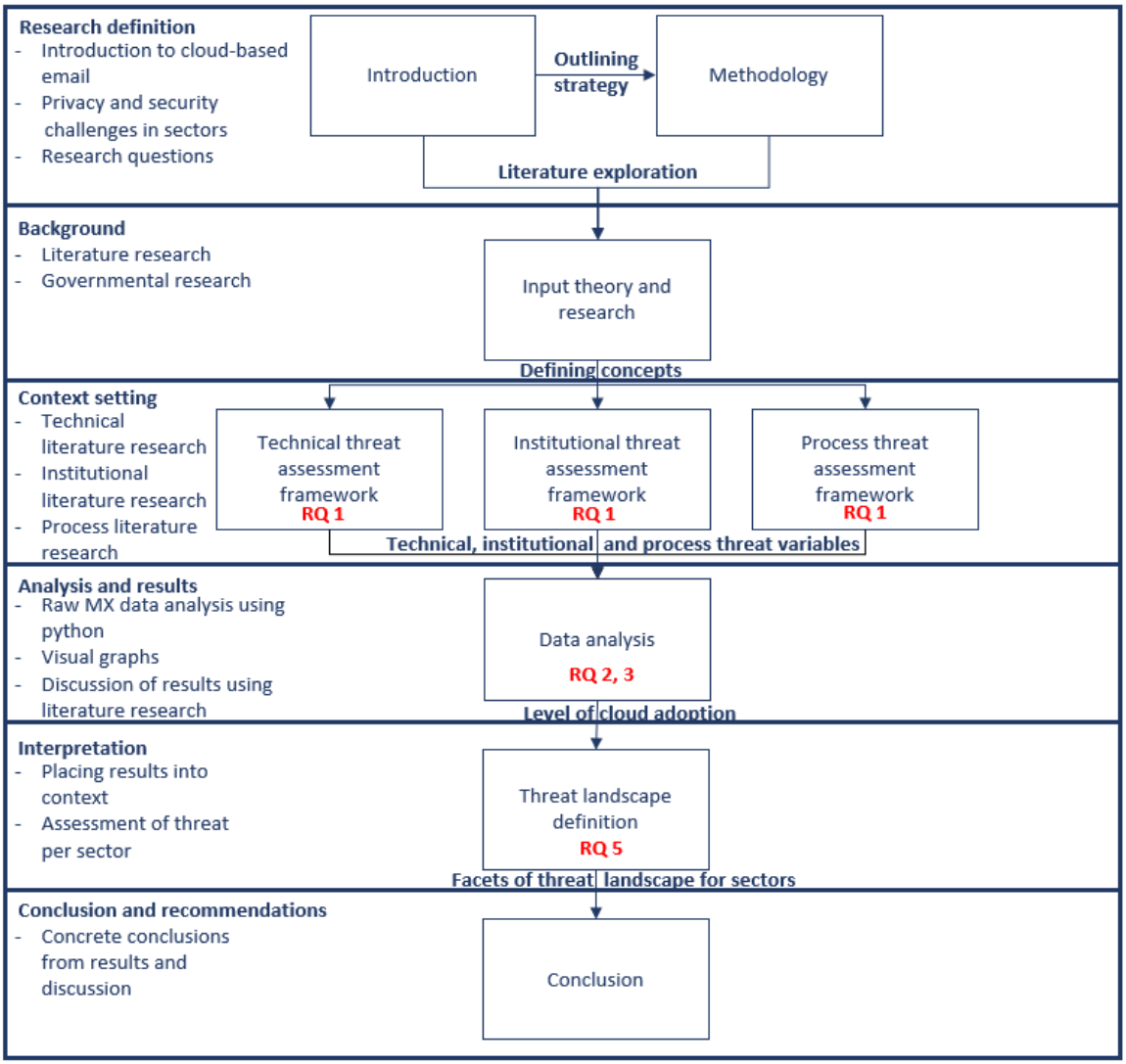
To understand the current level of adoption of cloud-based email services and what this occurrence may entail for the future of crucial sectors, we aim to perform a mixed method research containing a quantitative measurement study and qualitative aspects. A quantitative research generally involves a start with theory which leads to review of prior research, after which theoretical frameworks and hypotheses are developed that will be tested by performing data analysis (Newman, Benz and Ridenour, 1998). The interpretation of data analysis along with the theoretical frameworks results into the definition of the threat landscape. This methodology enables us to find causal relationships between variables in order to verify the pre-defined theory or hypothesis (Creswell, 2022; Teddlie and Tashakkori, 2012; Feilzer, 2010; Haq, 2015). For example, we will try to find relationships between technical, institutional and process factors and threat variables. The research flow has been depicted in Figure 2.1. The quantitative nature of the study allows us to define a highly generalizable threat landscape on the basis of numerical data (Haq, 2015). The qualitative aspects of this study allow us to interpret quantitative results using pre-defined literature and formulate a concrete perspective on the threat environment for different sectors in Europe.

2.2. Literature review for theoretical framework

In Chapter 1, we delineated prior research in the field of cloud-based adoption of email services. This initiated knowledge gaps: (1) the level of adoption of cloud-based email services among crucial sectors is unknown, (2) the use of cloud-based email services provided by cloud service providers may introduce privacy and security related threats and (3) the threat landscape as a consequence of 1 and 2 is yet undefined. We will use a literature review method in order to develop a theoretical framework (Baumeister and Leary, 1997; Torraco, 2005) which will be used to map threats that have impact on sensitive email data hosted in the cloud for seven sectors. To develop the threat framework, we divide the contextual perspectives into three subsystems to investigate: technical, institutional and process subsystem. We perform an integrative review (Torraco, 2005) of each subsystem, so that we can synthesize existing literature on the sub domain to design a novel theoretical threat framework and perspectives.

We used the Google Scholar and Scopus database for retrieving literature concerning the literature background setting. For the literature background of the technical subsystem, we focused our search on general uses of email and metadata, personal information, the technical (cloud-based) email infrastructure, email security mechanisms, different notions of privacy and specifically looking at security and

Figure 2.1: The research design process



privacy related threats. In the institutional subsystem, we narrowed the search space down to institutional aspects to privacy, such as frameworks, regulations and regulatory stance. Finally, we analyzed implications arising due to cross border data transfers with special attention to the US interference. In the process domain, we concentrated the literature search on the side effects that occur as a consequence of the dominance of cloud service providers. We also looked at cloud movements in the crucial sectors and filtered on attack types and motivations.

2.3. Data analysis

The methodology followed for data analysis has been specified in this section. The limitations of data analysis are also described.

2.3.1. Data analysis by measurements

We conducted a measurement study of DNS logs. For this, we used the Farsight Security Information Exchange (SIE) dataset (Farsight Security) to measure (1) the level to which organizations deploy cloud-based email services and (2) which cloud service providers have become prominent over time. The collection of DNS logs occurred through DNS servers within the Domain Name System (DNS). The DNS service permits to resolve IP addresses to names (Zdrnja, Brownlee and Wessels, 2007). The name space has been partitioned into numerous zones, which is 'a variable depth tree' (Mockapetris

and Dunlap, 1998). Therefore, a certain DNS server is only authoritative for its specific zone, in which each zone has been assigned to an organization in the hierarchy of DNS (Zdrnja, Brownlee and Wessels, 2007). Thus, the dataset has been gathered through recursive DNS resolvers of Internet Service Providers (ISP's). This means that associated ISP's can put a sensor in place that can send DNS cache misses (Kumari, Lawrence and Sood, 2020; Mockapetris, 1987) belonging to their customers to Farsight. Farsight also filters any extra information in the aim to restrict the collection of PII data (Farsight Security).

We will use the historic dataset that contains MX records from January 1, 2015 to November 30, 2020 in per month slices. The records have the following fields: count, time_first, time_last, rrname, rrtype, bailiwick and rdata. After confining the search space to rrtype = 'MX', in particular, we look at the bailiwick and rdata fields. Bailiwick fields or second level domains (SLDs) can be used to identify different organizations, after which we use the rdata field to observe the use of a known cloud service provider. The measurements will be performed using Python. The concrete taken steps for the analysis are as follows:

1. **Collection of organizations for sectors:** For each sector, we collect domains of 352 relevant organizations. These lists of domains are comprised manually in order to ensure input data quality; we checked each company's domain for its existence and its eligibility to our research objective. We describe this process in more detail in Chapter 6.1.
2. **Composition of relevant cloud service providers:** We create a predefined list containing 25 accepted cloud email hosters and 25 accepted email security providers. We will use the MX domains of these cloud service providers to observe the usage of a cloud service in the rdata field. We elaborate more on this in Chapter 6.1.
3. **Filtering of dataset:** We base the analysis approach on the methodology followed by Henze et al. (2016) and Fiebig et al. (2021). We filter the dataset on the rrtype MX record, after which we collect all records corresponding to the domains of the predefined organizations in 1.
4. **Observation of cloud usage:** For the second level domains of the organizations, we check whether the rdata points towards a MX domain linked with a cloud service provider. If we observe cloud usage, we increase the counters. However, if we do not observe cloud usage, we look further down the sub-domains of the organization. We repeat this sequence for every sub-domain until we find a link to the use of a cloud service. If we do not find an association to a cloud service provider, we move on to the next organization.
5. **Visualization of results:** We keep track of observed frequencies of cloud usage per sector and report the results in a graph.

2.3.2. Limitations

The research will not focus on identifying hidden use of email cloud services, but will solely center around identifying direct observational cloud usage from its domain name in the rdata field of the Farsight dataset. Therefore, in this research we only focus on detecting cloud hosting which is directly connected with its MX record. One crucial point to note is that certain email security solutions can also be employed without having to make changes to MX records, and therefore will not be detectable.

Furthermore, the research will not take into consideration to what extent email cloud services are being used but rather measure which organizations seem to be utilizing cloud based email services. Also, the research will limit itself around measuring cloud usage for the identified sectors.

This research observes several security threats that can endanger emails in cloud-based environments. However, we do not consider ransomware attacks with special attention, as they occur through phishing. Therefore, we only focus on the issue of phishing.

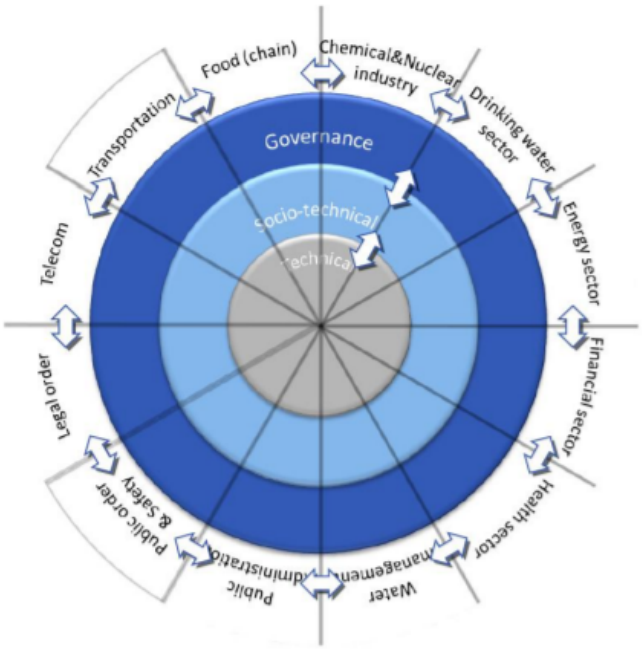
2.4. Threat assessment

We will investigate the threats surrounding a complex mail ecosystem in which connectivity between actors and processes can be observed. In the context of cybersecurity, a NCSC (2019) cybersecurity

report found that an increased complexity and connectivity is responsible for a larger attack surface which results into more opportunities being available for adverse behaviour. In order to determine the cloud-based email services threat landscape for crucial sectors, we will dive further into existing models for defining cyber threat scenario's.

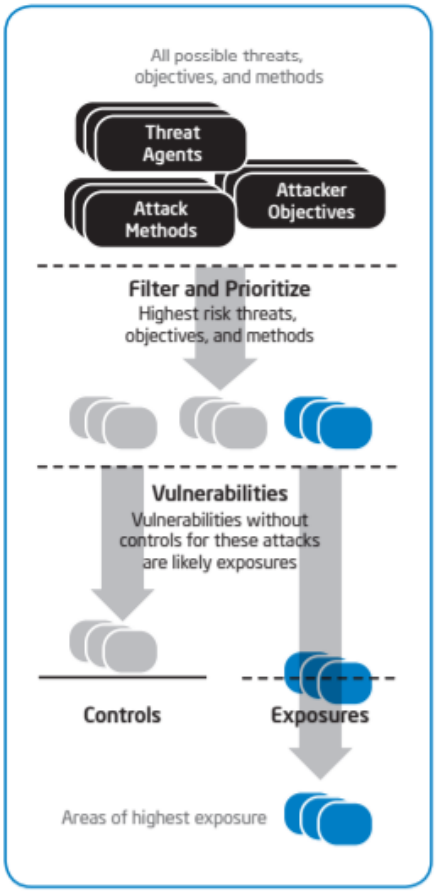
Cyberspace can be understood as the complex environment that results from interactions between humans, their employed software and services through the internet which is backed by globally distributed ICT machines and connected networks (ISO 27032, 2012). The ISO 27032 (2012) guidelines describe cybersecurity as 'the preservation of confidentiality, integrity and availability of information in the cyberspace'. Van den Berg et al. (2014) proposed a framework to classify cyber activities within the cyberspace as shown in Figure 2.2. The innermost technical layer revolves around CIA principles of information security. The socio-technical layer on top of the technical layer allows for modern cyber activities such as information exchange or information retrieval. This layer specifically focuses on characterizing the complex interactions between all humans in the cyberspace and the ample availability of data processing and storage systems. The topmost layer governs the technical and socio-technical layer in complex manners and by an immense range of human stakeholders and institutes. This layer provides rules and regulations in order to minimize cyber risk and ensure ethics and compliance (van Gelder, 2020).

Figure 2.2: Layered cyberspace model with its cyber subdomains by van den Berg et al. (2014)



We will examine threats to European email data hosted in the cloud on these levels. A prior threat agent risk assessment (TARA) model for the conceptualization of a threat assessment has been introduced by Rosenquist (2009). This risk assessment framework allows to gain awareness about the most exposed fields so that risks can be mapped. Whereas many risk models concentrate on identification of vulnerabilities and weakest links, this framework instead on threat actors, their goals, their motivations and their methods and how these can be used to set out available controls. This model presents threat agents, who are the adversaries; these adversaries can be characterized by skills, motives, access, capabilities or resources as they may have malicious motivations. The framework describes threat agents to be the root cause of the threat and these then form input to attack methods. When these attack methods do not meet controls, they can produce exposures which are the foundation for the threat surface. This has been depicted in Figure 2.3.

Figure 2.3: TARA model by Rosenquist (2009).



In this research, we will aim to develop a threat framework by assessing threat perspectives from technical, institutional and process subsystems. In the technical subsystem, we will analyze the technical background and complexities that eventually lead to threat variables. In the institutional background, we will delve into complications arising from existing rules and regulations as they impact the technical system and how these produce institutional threat variables. In the process background, we will have a closer look at stakeholder interactions as they result into process threat variables. We will use these threat variables to determine the threat scenario's for the crucial sectors.

3

Towards a threat landscape for the technical mail ecosystem

The cloud-based email ecosystem will be discussed from a technical perspective in this section. The analysis of this system will result into a threat landscape observed from gathered knowledge. In this section, we first present the process that enabled us to gain the literature review we performed on the technical domain. After this, we present the literature research.

3.1. Literature selection

We used Google Scholar for the retrieval of literature relating to technical aspects of the cloud-based email ecosystem. Literature was retrieved by using input literature, scholar search, forward and backward snowballing. We first investigated the email system and its components. Dabbish, Kraut, Fussell and Kiesler (2005) tried to identify purposes of email messages being sent in enterprises. We further delved into the content of email messages, which was explained by Henze (2018). This allowed us to look deeper into the definition of personal information in the context of email, which was previously analyzed by Pearson (2009), Ghorbel, Ghorbel and Jmaiel (2017) and Sweeney (2000). These papers have been found by using forward snowballing. Email metadata was defined by Grewal (2013), however we used Sanchez (2017), Conly (2015) and Angel and Setty (2016) to understand the difference between metadata and personal information and how it may be threatened.

After this, we tried to understand the overall email infrastructure on-premise and cloud-based infrastructure. Chhabra and Bajwa (2015), Limoncelli, Chalup and Hogan (2016) and NIST (2019) enabled us to gain knowledge about the technical infrastructure on-premise and risks connected to this infrastructure. Also, the Mell and Grance (2011) enabled us to understand cloud computing technology. In this context, Joint, Baker and Eccles (2009) had been found by forward snowballing. In order to identify different type of cloud service providers, we read papers by Hentschel, Leyh and Patznick (2018), Dey, Roy, Bose and Sarddar (2021) and Henze, Sanford and Hohlfeld (2017). Velte, Velte and Elsenpeter (2010), Voorsluys, Broberg and Buyya (2011) allowed insight into standard cloud service provider procedures and have been found by forward snowballing. Srinivan (2011) and Shitole and Divekar (2019) added on to this by highlighting general privacy and security risks of cloud-based email services.

We looked at email security properties by investigating information security properties in Wood (2007), Shimba (2010), Metheny (2017). We found Camp (1999) and Fitzgerald (1995) by forward snowballing to find relations between security properties and privacy properties. In this context, Samonas and Coss (2014) was found by database search and Dinev et al. (2013) was found by forward snowballing. Henze (2018) and Salove (2006) described prevalent privacy principles and processes in digital platforms. Westin (1967), Shen and Pearson (2011) also explained their notion of privacy and have been found by using backward snowballing. We contrasted their vision of privacy with the privacy perspective provided by Diaz, Tene and Gürses (2013) which follows the PETs privacy ideology, also highlighted by Nissenbaum (2013).

For email security protocols, we looked at researches by Durumeric et al. (2015) and Poddebniak et al. (2021) for email in transit which were found by database search. For authentication of email, we found Kitterman (2014), Crocker, Hansen and Kucherawy (2011), Kucherawy and Zwicky (2015), Lee et al. (2020) and NIST (2019). End-to-end security of email was elaborated by Muller et al. (2019). We searched for privacy and security related threats; Mohammed et al. (2013), Cidon et al. (2019), Nurse et al. (2015), M^3AAWG, Bezemer and Zaidman (2010) introduced threats regarding confidentiality. Suryateja (2018), Kumar and Vajpayee (2016), Mandal and Khan (2020), Aaron and Rasmussen (2010), Hong (2012), APWG (2014), FBI (2020) discussed threats regarding integrity. This led us to look into the privacy threat of surveillance by metadata in Beato, Kohlweiss and Wouters (2011) and Diffie and Landau (2010).

3.2. The email message

In this section, we give an account of the context in which email can be used by organizations and we define two major components of email, namely email content and metadata.

3.2.1. Email purposes

Email can be used in various contexts with different purposes by organizations. Dabbish, Kraut, Fussell and Kiesler (2005) defined a framework for identifying purposes of email being used in an organizational setting. They classify the following purposes:

1. **Task and project management:** email is a common means to manage work-related action requests, updates of task status and reminders for deadlines and meetings.
2. **Formal exchange, storage and retrieval of information:** email is used for requesting information and responding to a request. This information can consist of documents, web-links or discussions. When a message is considered relevant, recipients can store the email for retrieval on a later moment.
3. **Planning and Schedule:** email is used for scheduling (informal) meetings and events.
4. **Informal discourse:** even though communication through email is asynchronous, many employees keep track of their email and respond to it regularly on social basis throughout the day. The use can be compared to text messages.

3.2.2. Email content and metadata

The four purposes of emails encapsulate sensitive personal data. In the light of personal information, we distinguish two types of information: (1) PII data and (2) sensitive information. Email content usually contains personally identifiable information (PII), which entails any information of an individual that can be used to identify the person (Pearson, 2009; Henze, 2018). Key attributes of PII data can be for example, names, email addresses, phone numbers or passport numbers (Pearson, 2009; Ghorbel, Ghorbel and Jmaiel, 2017; Henze, 2018). On top of this, quasi-identifiers are the set of fields that can be combined to identify a person uniquely (Sweeney, 2000). For instance, a combination of date of birth and address can be used to identify someone uniquely (Ghorbel, Ghorbel and Jmaiel, 2017; Henze, 2018). On the other side, sensitive information points at a field of more general information that has any connection with a person. For example, this categorization includes information relating to an individuals' membership in association with religion or community. Demographic information regarding a person can range from one's nationality and gender to educational level, profession and criminal records. Thus, summarizing, sensitive data envelops any information that should continue to be private. Private data at organizational level, includes data about the organization itself, its employees and customers also (Ghorbel, Ghorbel and Jmaiel, 2017; Henze, 2018).

Personal Information						
Sensitive Information					PII	
Membership	**Demography**	**Finance**	**Healthcare**	**Intellect**	**Key attributes**	**Quasi identifiers**
Political	Gender	Balance	Medical records	Ideas	Name	Date of birth
Religiosity	Nationality	Account number	Medical outcomes	Inventions	Phone number	Address
Community	Age	Transaction	Diseases		Email	
Sports	Ethnicity	Statements	Medical images		Passport number	
Hobby	Income level		Prescriptions			

Table 3.1: Personal Information adapted from (Ghorbel, Ghorbel and Jmaiel, 2017; Henze, 2018)

Another critical element of an email message is the metadata - which basically is ”any other data other than the contents of a communication” (Grewal, 2013). However, the line between metadata and content is not sharp, and seems more like intertwined spectrum (Sanchez, 2017). We consider the body of the email containing its PII data and sensitive data as content, but the data in the range of To and From lines as metadata (Conly, 2015). Apart from the senders, receivers and subjects, metadata of an email also includes the timestamps of the email message and the number of emails sent in one conversation (Angel and Setty, 2016). Metadata can reveal valuable information for adversaries. We review this risk in Section 3.5.

3.3. Email infrastructure

Email infrastructure consists of several software components that accommodate the process of producing, sending and transferring email. These components act as clients, servers or both. On top of this, organizations may use additional special purpose components to enhance security features (NIST, 2019). The email infrastructure is a quite simple system, consisting of five major components (Chhabra and Bajwa, 2015; Limoncelli, Chalup and Hogan, 2016; NIST, 2019):

- **Mail transport:** the Mail Transport Agent (MTA) ensures email travels from server A (sender) to server B (receiver). MTA’s are responsible for actual transfer of email. Thus, the system must have a MTA client for sending emails and a MTA server for receiving emails. Handling of client/server MTA occurs through the Simple Mail Transfer Protocol (SMTP), which is used in two phases: (1) between sender and his/her mailserver and (2) between server A and B.
- **Mail delivery:** the Mail Delivery Agents (MDA) accept emails from an organization’s inbound MTA and save them at the addressed server. A Mail Submission Agent (MSA) accepts email from MUA’s after authentication of the sender and transmits it to the MTA for further handling.
- **Mail access:** mail access protocols POP3 and IMAP4 are laid out by access servers. These protocols enable Mail User Agents (MUA) on individual computers to access, compose and send personal emails. The MUA allows the transmission of new emails to a server for processing. POP3 and IMAP4 operate between mailserver B and the receiver. The POP3 protocol downloads all mail from the server and removes the copy on the server. Additionally, the possibility exists to keep the copy on the server. IMAP offers more built-in functions for companies. For example, clients can download emails, but the message will be kept on the server. This allows for synchronized email over multiple machines.
- **List processing:** list processing involves delivery of one email to a group of recipients on a list.
- **Filtering:** which filters for spam and viruses.

A crucial element of the email transmission process is the Domain Name System (DNS) which can be considered as a universal, decentralized database that is mostly used to map a domain name to an

IP address. MUA's use the DNS to find the correct MSA's and MTA's use DNS to learn the next hop IP address of the mail server for delivery. The MTA accomplishes this by requesting the MX resource record of the addressee's domain from the DNS which points to the final receiving MTA (NIST, 2019).

There exist several ways for organizations to arrange their email system. In this study, we will consider the deployment of a traditional on-premise email system in comparison to the emerging and novel cloud-based email infrastructure.

3.3.1. Traditional email infrastructure on-premise

Small sites usually arrange a sole system providing all of these functions in order to reduce complexity. Larger sites on the other hand, typically divide the functionality of mail transport, mail delivery or list processing over multiple systems. Mail relays play a relevant role as they deliver mail to list processing or delivery machines (Limoncelli, Chalup and Hogan, 2016). Keeping the email infrastructure on-premise enables firms to set standards for the desired level of privacy or security. However, certain aspects of the email system still make the system vulnerable in various ways.

Characteristics and risks of email infrastructure on-premises (Limoncelli, Chalup and Hogan, 2016)

- Spam and virus blocking has become quite an exhaustive task, for which organizations can make use of outsourcing. However, this induces multiple privacy concerns, as it requires the need to share data with external parties.
- Mail relay hosts that have communication with outer networks are susceptible to attacks, as they travel over extranets or the internet.
- Encryption keys can be weak or can be outsourced to vendors.
- The security model should be pondered in the initial design phase; and is hard to add on later e.g. protection of firewalls, mail relay vulnerability to unauthorized access, customer accessibility to email on other locations which involves transfer of confidential information over unsecured networks.

3.3.2. Cloud-based email infrastructure

Email infrastructure can be implemented utilizing (partially) cloud-based computing services by not employing any machines at all, and instead, leasing capacity from an organization (Limoncelli, Chalup and Hogan, 2016). We closely follow the definition of cloud computing provided by The National Institute of Standards and Technology (NIST): *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell and Grance, 2011). The cloud computing framework can be deployed as Software as a Service (SaaS) model, in which the customer has access to the provider's cloud infrastructure through a client interface, like a web browser. An example of such a service is email (Mell and Grance, 2011; Joint, Baker, Eccles, 2009).

Cloud Service Providers

Cloud service providers can be defined as the providers of software applications, platforms or infrastructure for their consumers (Hentschel, Leyh and Petznick, 2018). In terms of cloud based email infrastructure, we will refer to cloud service providers as the suppliers of email software over the internet, which are not hosted on the customer's machine or on the company's servers but rather within the facilities provided by the SaaS provider (Dey, Roy, Bose and Sarddar, 2021; Joint, Baker and Eccles, 2009). Within cloud service providers, we can differentiate between (Henze, Sanford and Hohlfeld, 2017):

1. Cloud email providers: offer the basic email services wherein the email address will be bound to the domain of the providers, e.g. Google, Microsoft.

2. Cloud email hosters: they provide email services and consumers can have their own domain e.g. Google, GoDaddy, Strato.

3. Email security providers: services that aim to maintain security of mail servers e.g. Proofpoint, Cisco, McAfee and Mimecast.

This research will restrict itself to measure the prevalence of cloud service providers in the scope of 2 and 3, as the adoption of these cloud service providers can be inferred directly from the email servers' domain. For 1, this is not the case.

The cloud computing quality of SaaS architecture permits the flow of a large amount of data transfer through these vendors. Accordingly, cloud service providers are undertaking far-reaching efforts to protect customer data, yet, the likelihood of information being intercepted and modified exists (Velte, Velte and Elsenpeter, 2010). Procedures among which data encryption, data aggregation, information deletion at the end of the service agreement and data aggregation are essential for ensuring security (Voorsluys, Boberg and Buyya, 2011). Most cloud service providers offer access to services through the main protocols IMAP, SMTP and POP3. Standard mail protocols implemented by cloud service providers can come with certain risks in terms of security and privacy:

- SMPT is set up by cloud service providers with several control mechanisms, which restrict SPAM (Srinivasan, 2010). This implies some extent of control over which email is to reach the customer is handed to cloud service provider. This point will be handled in the institutional environment discussed in chapter 3.

- In contrast to on-premise architecture, access protocol IMAP leaves email messages on the cloud service providers IMAP/SMTP server until it is deleted by the user specifically. POP3 on the other hand, allows the user to connect to the server, retrieve the emails and delete it from the server (Shitole and Divekar, 2019).

- In addition, organizations that use cloud based outsourcing of email service may not have immediate access to MTA's or Authoritative DNS servers, but might have configuration control over MUA's (NIST, 2019).

- Emails can possibly pass through a multitude of MTA's before they reach the final addressee. These intermediate MTA's can each have their own security policies. At the moment, there is no means for a sending party to invoke a certain level of security for the sent email. This is a general point of concern for any kind of email infrastructure (NIST, 2019).

3.4. Email Security

We define email security properties that are deemed relevant in information security. We further delve into privacy principles as they intersect with security and set out contrasting views on privacy. Then we elaborate on security protocols which can be implemented in email systems.

3.4.1. Security Properties and its intersection with Privacy

In this section, we will further highlight security properties, email security standards and threats as a consequence of outsourcing to cloud based email services. With regards to security in a cloud computing context, we follow the aforementioned CIA properties (Wood, 2007; Shimba, 2010; Metheny, 2017), in which:

- *Confidentiality* entails what information may be disclosed and to whom. It questions whether the cloud based software will not compromise confidentiality of customer's data and is linked to the fear of losing control over data.

- *Integrity* ensures protection of information (systems) against inappropriate modification. It is related to the clients being convinced that the cloud service provider is performing the correct operation on their data.

- *Availability* guarantees timely access to information (systems) by authorized individuals. This property revolves around what will happen if the cloud service provider is attacked, disaster recovery and business continuity.

This CIA triad can be interpreted in different ways. For example, Camp (1999) views confidentiality as the notion to protect data in a manner that it is only available to authorized individuals with authorized purposes. We observe an intersection with *availability*, as data should only be available to those who are granted rights to access. It was noted by Fitzgerald in 1995, that elements relating to privacy of confidentiality would become more integral in the time to come. Especially in the sectors in which a great focus is placed on management and protection of sensitive data, such as healthcare and finance.

Privacy as a control
Privacy of information according to Westin (1967) revolves around users and their informational autonomy. In the narrative of the cloud computing paradigm, Henze, (2018) describes privacy as: ”Privacy in cloud computing guarantees individual users awareness and control over the collection, processing and dissemination of their personal information”. This perception is inspired by a comprehensive privacy taxonomy by Solove (2006) in Table 3.2, primarily fixating on privacy issues:

Process	Elaboration	Risks
Information collection	End users can be unaware of the harms of data gathering practices. Surveillance has been one of the major issues as it violates fundamental rights to privacy (Salove, 2006; Shen and Pearson, 2011)	Surveillance and Interrogation
Information processing	Information processing includes the use, storage and modification of collected data. Practices relating to how collected data will be handled raise several privacy concerns. Especially, since data can be aggregated and connected in different ways from multiple sources to link it back to individuals (Shen and Pearson, 2011).	Aggregation, Identification, Insecurity, Secondary Use and Exclusion
Information dissemination	The risk of spreading personal information, for example, personalisation (Salove, 2006; Shen and Pearson, 2011).	Confidentiality Breach, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation and Distortion
Invasion	Impingement of an individuals' 'right to privacy' (Salove, 2006; Shen and Pearson, 2011).	Intrusion and Decisional Interference

Table 3.2: The privacy taxonomy (Salove, 2006)

Information can be collected intentionally or unintentionally after which it will be sent to the cloud service provider (Henze, 2018). We speak of intentional data collection when if the user uses a cloud-based service by free will and grants the cloud service provider access to his/her personal data with regards to the purpose of use. Conversely, unintentional data collection occurs when data is gathered unknowingly and has been triggered by the user initially. As per the exposing of NSA and its partner intelligence organizations and other privacy breaches as described in Section 1.2, we cannot depart from a viewpoint in which a cloud service provider, who mainly has the role of a *trusted controller*, should be trusted. Privacy enhancing technologies (PETs) are described by Diaz, Tene and Gürses (2013) to be enabling individuals to take part in digital activities ”free from surveillance and interference”. We

closely follow their perspective on privacy: ”PETs allow individuals to determine what information they disclose and to whom, so that only information they *explicitly* share is available to *intended* recipients”. We observe a stark difference with prevalent privacy ideologies: whereas these theories face privacy issues relating to disclosure of personal information to trusted third parties or identity building (Diaz and Gürses, 2013), instead we concentrate on a minimized collection of information on untrusted platforms. In the American Department of Defense, a ’trusted system or component’ can be defined by ’one which can break the security policy’, so far highlighting the extent of danger users may encounter whilst continuing on this ’trust the cloud service provider’ road.

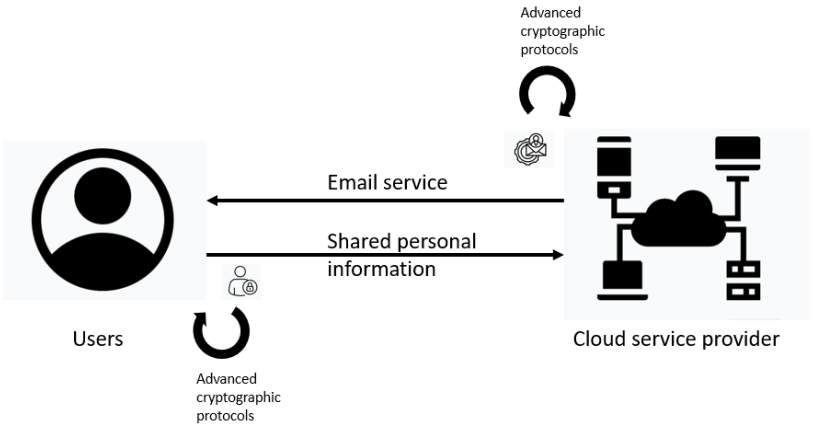
More specifically, they underline three main fundamentals (Diaz, Tene and Gürses, 2013):

Privacy principle	Elaboration
The elimination of the single point of failure that comes with a ’ centralized trusted party	The avoidance of a single point of failure that is underlying to a central trusted cloud service provider, entails that trust should be divided over multiple other system components such as software implementations, protocols and user devices.
Minimization of data disclosure	Only information that a user consciously shares should be available to intended parties by implementation of advanced cryptographic protocols. This principle aims to minimize the collection of information and subsequently leads to a mitigation of the risk of data exploitation for the purpose of surveillance.
Community driven public scrutiny of protocols and software	It should be verifiable by the public that the assumptions about trust have not been mislaid. Thus, software implementations and design protocols have to be openly available to anyone.

Table 3.3: The privacy principles (Diaz, Tene and Gürses, 2013)

These principles can be categorised into multiple application models. We primarily look at two application types (Diaz, Tene and Gürses, 2013), which are relevant for division of responsibilities among involved parties in cloud-based mail ecosystems. The first application type requires the implementation of advanced cryptographic protocols on both sides: users and the cloud service providers. Thus, the performance of this type is dependent on the active partaking of cloud service providers. This application aims to facilitate an email service that feeds in personal information without it becoming open to the cloud service provider. The conceptualization has been depicted in Figure 3.1.

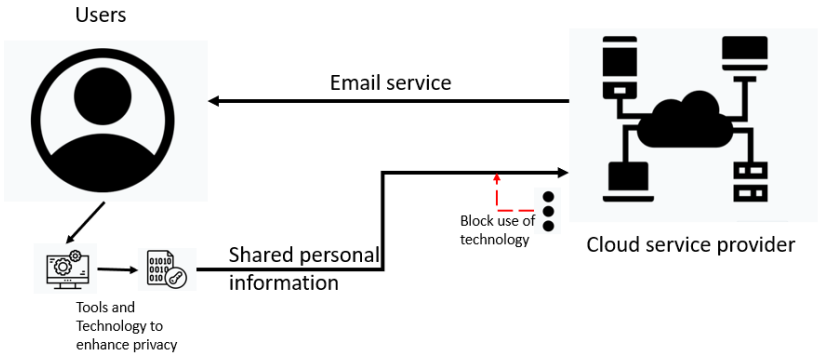
Figure 3.1: The PET application I inspired by (Diaz, Tene and Gürses, 2013)



The second application type consists of the set of tools and technology that the user can deploy in order to protect their privacy when they are making use of email service. This application does

not require active participation by the cloud service provider Nissenbaum (2013). Accordingly, the provided service does not have to be modified by the cloud service provider. However, as the cloud service provider is still the one in control, they possess the power to block the usage of this application service (Diaz, Tene and Gürses, 2013). In Figure 3.2 the concept has been shown.

Figure 3.2: The PET application II inspired by (Diaz, Tene and Gürses, 2013)



This perspective on privacy finds its basis in the *information collection level*. We will dive deeper into privacy implications from an institutional point of view in Chapter 3.

The prevention of such unauthorized access by any entity guarantees *confidentiality*, which in turn enables users to behold a greater *level of control over their personal data* (Dinev et al., 2013; Samonas and Coss, 2014). Thus, privacy is considered to be strongly connected with the foundation of the security CIA triad, and *controls for the management of identity* are considered very important, as it regulates processes around access to data (Samonas and Coss, 2014). Access control is then again directly an element of *availability*.

3.4.2. Security protocols

Cloud service providers and organizations can adopt various security standards to ensure confidentiality, integrity and availability of email in the cloud-based ecosystem.

STARTTLS for email in transit

STARTTLS is an extension to the SMTP protocol, which uses the Transport Layer Security (TLS) for transmission between SMTP servers and clients. The STARTTLS session proceeds as follows: an SMTP connection is first negotiated with the server by the client, after which the STARTTLS command is sent by the client. This initiates a typical TLS handshake, after which the mail content and metadata is transmitted through this protected channel. STARTTLS is functional in email relaying, which occurs from SMTP server to SMTP server. Due to weak TLS validation, email relaying is considered to be opportunistic as SMTP servers retreat to plaintext if the TLS negotiation is not successful (Durumeric et al., 2015; Poddebniak et al., 2021).

Authentication of email

Sender Policy Framework (SPF) is a protocol that permits the cloud service providers to produce a list containing hosts that are authorized to send mail on its behalf. The cloud service provider publishes a SPF record of a TXT type RR in the authoritative DNS zone of the cloud service provider. Therefore, integrity of DNS is vital as SPF leans on it. Only one SPF record is allowed per domain, however, it can hold numerous servers. SPF is effective in blocking remittance of unsolicited bulk mail from unauthorised sources (Kitterman, 2014).

DomainKeys Identified Mail (DKIM) is a standard that enables the MTA on the receivers' side to authenticate the sender and email content. The standard uses digital signatures which bind the message and its origin with the private key. If the cloud service provider supports DKIM, they hold one or more private keys and report their corresponding public keys as a DNS TXT RR, which can then be verified by requesting the DNS record and verifying the signature. Thus, DKIM also depends on the integrity of DNS. This standard is deemed useful in improving authencity and integrity (Crocker, Hansen and Kucherawy, 2011; Durumeric et al., 2015).

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a scalable procedure that enables the outbound cloud service provider to specify whether the messages are secured with SPF or/and DKIM. Also, policies are published to inform the receiver about the proceeding steps if these mentioned authentication mechanisms fail. These DMARC policies are published in DNS TXT RRs, but should also be protected with DNSSEC. DMARC has in combination with SPF/DKIM proven to be effective in combatting fraudlent mail (Kucherawy and Zwicky, 2015).

Domain Name System Security Extensions (DNSSEC) is an extension to DNS to lay out authenticity and integrity of existing DNS records. This extension was introduced because of significant security problems with the original DNS protocol, for example, there are no authentication mechanisms for DNS records (Lee et al., 2020).

DNS-based Authentication of Named Entities (DANE) We have seen that previously discussed security standards are coupled with a Public Key Infrastructure (PKI) and TLS is dependent on certificates which bind a message to its public key. However, problems arise due to vulnerability of certificates provided by Certificate Authorities (CA's), as CA's can produce certificates for each domain possible. So far, validation of certificates builds on third party CA's. Hence, DANE was introduced to support TLS without having to depend on third party CA's. Also, a TLSA record allows for verification of certificate information by retrieving TLSA records, validating it by using DNSSEC signatures and confirming consistency of these records with a TLS server certificate. The Dane addition improves vulnerability of a TLS connection by reducing risk to downgrade and Man-in-the-Middle (MITM) attacks (Lee et al., 2020)
.

SMTP Mail Transfer Agent Strict Transport Security (MTA-STS) was introduced as an alternative to DANE to authenticate mail servers and protect SMTP servers against downgrade attacks (Lee et al., 2020). This was due to the requirement of DANE that has to be secured with DNSSEC, which was considered to be a barrier to deployment. MTA-STS relies on DNS records but employ authentication based on distributed information through HTTPS (NIST, 2019).

End-to-End Security
While technologies such as SPF, DKIM and DMARC aim to authenticate the domain of the sender, they do not extend to authenticate the actual sending person. Therefore, OpenPGP and S/MIME were proposed to provide end-to-end authenticity of email messages by using digital signatures which are also supported by most email clients (Muller et al., 2019). Messages are typically signed by the S/MIME/OpenPGP protocol directly after the message has been composed, usually by sending MUA. Whereas, the DKIM is attached after the email passes through the MSA or MTA of the sender (NIST, 2019).

3.5. Security and privacy threats as organizations move to cloud

We identify various security related threats that correspond to information security principles as mentioned in section 3.4.1. We further find surveillance as the most prominent threat to privacy of individuals in Europe.

1. **Security threats relating to confidentiality**

   Eavesdropping
   In a typical eavesdropping attack, an attacker listens to a communication which is supposed to be private. Encryption, such as TLS and/or S/MIME/OpenPGP, can be used to prevent such attacks (Mohammed et al., 2013; NIST, 2019).

   Public API's
   A research by (Cidon et al., 2019) revealed that popular cloud based providers, such as Gmail and Microsoft offer public API's, which allow third party applications to access historical emails.

   Email headers
   Whereas email content is mostly highly protected with OpenPGP or S/MIME encryption, message headers and other observable aspects associated with the email message may still be vulnerable to traffic analysis attacks. Email headers are the set of metadata included in every email. They contain details regarding the sender, receiver and the traversed path from sender to receiver which can be susceptible to attacks. For example, user information such as usernames, ISPs and the used devices can be disclosed. Also, information regarding the organizations they work for can be found, such as the used email software of server details (Nurse et al., 2015; M^3AAWG, 2016; NIST, 2019). Relationship unobservability entails that an adversary cannot infer information from the act of observing (or by active interference) the network traffic, given that the sender and receiver have not been compromised. If one of the parties has been compromised, it is easy to disclose the identity of the sender or receiver (Angel and Setty, 2016).

   Multi-tenancy
   In a multi-tenant architecture, multiple organizations use shared resources or applications. As data of various tenants is stored in a sole database, there exists a risk of data leakage between these tenants (Bezemer and Zaidman, 2010).

2. **Security Threats relating to Integrity**

   Malicious Insider
   A malicious insider can pose a significant threat, because its impact can be disastrous. The threat can be of different types, such as a former employee, the system administrator or authorized third party. These insiders have access to sensitive information and to critical systems (Suryateja, 2018).

   Monkey-in-the-Middle (MITM) attack
   In a MITM attack, an adversary intrudes in a ongoing message exchange between the sender and the client with the aim of injecting false information and to disclose the information transferred between them (Kumar and Vajpayee, 2016). Due to content tampering and information disclosure, this attack can be seen affecting both integrity and confidentiality of email systems.

   Spoofing
   Email security is fundamentally tangled with the security of DNS. An attacker can spoof DNS records of a target mail server to reallocate the SMPT settings to an mail server controlled by the attacker (Durumeric et al., 2015). DMARC, SPF and DKIM protocols ensure email domain security against spoofing (Mandal and Khan, 2020).

   Phishing and Spear Phishing
   Phishing is the vicious activity in which emails are sent with links/attachments that lead to hidden malware. These emails appear to originate from reliable sources. Also, this is one of the most common method adopted by hacker to try to persuade users to perform certain actions such as requesting access to their computer or revealing personal information (Aaron and Rasmussen, 2010; Hong, 2012; APWG, 2014). A more malevolent variant is spear phishing, which in comparison to phishing, tend to be specifically designed for a particular individual or groups of individuals.

Phishing on the other hand is sent to a large group of individuals and is more generic (APWG, 2014).

Business Email Compromise (BEC)
BEC has become one of the most costly cyber attacks. In 2018, US organizations have lost about 2.7 billion dollars due to this. Several notable organizations, such as Google or Facebook, have become a victim to these attacks. Also, critical governmental infrastructure has been affected by BEC attacks (Cidon et al., 2019). BEC attacks can have different forms: some emails request the victim to send money to the attackers' account and some use a phishing link to obtain credentials (FBI, 2020).

3. **Security Threats relating to Availability**

Denial-of-Service (DoS)
The multi-tenant nature of cloud based services allows multiple users to save their data on a single server using the applications offered by the cloud service provider. DoS attacks (Botnets) are a hostile effort to make the system or resources unavailable to its users. As such infrastructures are shared by millions of customers, it has become challenging to resolve such attacks since the impact is quite profound, compared to single tenanted architectures (Kumar and Vajpayee, 2016).

Spam
In a spam attack, unsolicited emails are sent in mass quantities, such as commercials and advertisements. Spam is not specifically directed towards a certain email domain. In the case that the volume of spam sent to a certain domain surpasses a particular threshold, it can have implications for the availability. This is mostly due to the rise in email traffic on the network and storage space limitations (NIST, 2019).

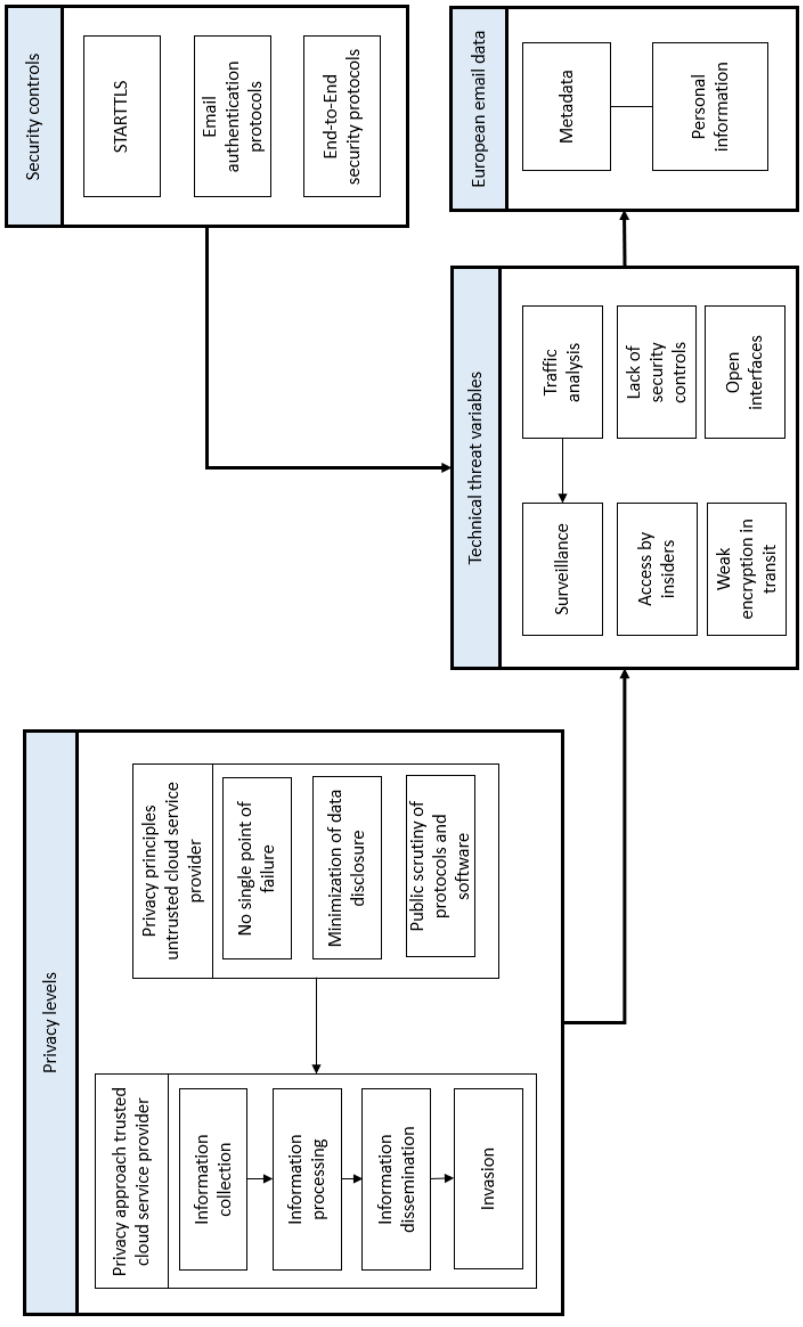
3.5.1. Surveillance as a threat to privacy

Encryption of contention and protocols as meant in Figure 3.1 and Figure 3.2 do not protect users against traffic analysis of email data, which can be performed by cloud service providers by order of governments or intelligence agencies (Diaz, Tene and Gürses, 2013). As already highlighted in Section 2.5, cloud service providers have the ability to follow patterns revealing with whom users engage in their email messages, when this happens and how frequently this occurs (Beato, Kohlweiss and Wouters (2011)). Using these insights, they can derive communication graphs among other things. This interception of communications and processing thereof to find relationships can often be performed when email messages are present in encrypted format (Diffie and Landau (2010)). Traffic analysis is crucial to surveillance activities as it can be considered ”the backbone of communications intelligence” (Diffie and Landau (2010)). Diaz, Tene and Gürses, (2013) describe the manner in which data is openly available to be the reason for this, and namely the information is easy to drill down. Furthermore, an important point to note is: observed patterns through surveillance offer more extensive insight regarding behaviour than content analysis, which then allows surveillance performers to select specific individuals to expose them to advanced intelligence.

3.6. Technical threat landscape

The technical literature has revealed relevant insights about the technical system in which the email ecosystem is located. We identify security controls and privacy levels that determinate the level of certain technical threat variables, which in turn impact European email data. These relations are presented in Figure 3.3.

Figure 3.3: The technical threat system



4

Towards a threat landscape for the institutional mail ecosystem

Protection of privacy is an essential element for organizations, which should not be undermined. A research by Casalini and Gonzalez (2019) illustrated that a majority of firms, about 99%, pinpointed privacy protection as a driving force for ensuring customer trust. At the same time, 78% of the responding firms manifested concerns about the upcoming data and privacy regulations. Also, these firms were also reported to have a high reliance on personal information. Therefore, we will have closer look at complexities arising from laws and regulations and their role in the cloud-based mail ecosystem. In this section, we first present the process that enabled us to gain the literature review we performed on the institutional domain. After this, we present the literature review.

4.1. Literature selection

In order to define the privacy setting in Europe, we analyzed Diaz, Tene and Gürses (2013) and the Charter of Fundamental Rights (2000). These documents illustrated prevailing privacy perspectives in Europe such as the informational perspective. Cavoukian (2009) added to this perspective by providing a privacy by default framework, which has been included by backward snowballing. We analyzed the influence of these frameworks on European regulation, therefore we investigated official government documents by database search, such as Kurtz et al. (2019) and the GDPR by the European Commission (2018). We also looked at several risks of the GDPR which we found in Padden and Öjehag-Pettersson (2021). McDonald and Cranor (2008), Koops (2004), Zuboff (2019) and Srnicek (2017) have been found by forward snowballing and explain privacy complications on digital platforms without physical restrictions.

The revelations from previous resulted into us looking deeper into the regulatory stance of governing bodies. For this, we looked at documents of the European Commission and Rossi (2018). We also noticed issues with the current legislation in Mann and Matzner (2019), Daly (2016) and Bergemann (2018), which have been found by forward snowballing. We examined constitutional privacy perspectives and its implementations in law, which for which we analyzed the GDPR, Diaz, Tene and Gürses (2013) and Lynskey (2015). These researches introduced new challenges in the form of interference from US which are still allowed according to the GDPR. Therefore, we analyzed Hoofnagle, van der Sloot and Zuiderveen (2019) via database search. This led us to find Rodata (2009) by forward snowballing. The different perspective on privacy in the US has been highlighted by Christen, Gordijn, Loi (2020) and Whitman, out of which the latter has been found by forward snowballing.

Within the context of threats from third countries, we investigated a paper by Suresha and Vijayakarthick (2020) and Kaur, Agrawal and Dhiman (2012) about data location issues due to a lack of transparency by forward snowballing. For the problem with cross border data transfer we read some additional papers by Zafar et al. (2014) and Paquette, Jaegr and Wilson (2010).

4.2. The need for transformation from informational privacy to constitutional privacy

In a complex systems environment such as a cloud-sourced email service, a large amount of unrefined (personal) data is collected, transferred, and saved by third party providers such as cloud service providers. When email content is collected in this manner and processed on another organization's servers, this will typically pose privacy challenges (Metheny, 2017). Extensive privacy frameworks up till date exist to encapsulate privacy principles that aim to fulfill the demands of users with regard to the preservation of their privacy and security.

In Chapter 3.4, we highlighted two levels of privacy, namely (1) privacy as a control and (2) the PETs perspective that allows for engaging in digital communication while being free from surveillance. The first mainly centers around on several layers of informational privacy while presuming the cloud service provider to be responsible. The latter perspective however, opposes this as it is a firm believer of data minimization in which the cloud service provider should not be trusted.

4.2.1. Complexities due to the current focus of regulation on informational privacy perspective

The current information privacy legal framework (Diaz, Tene and Gürses, 2013) established in the Charter of Fundamental Rights (European Commission, 2000) incorporates the right of freedom with regard to protection of personal data in Article 8. They mainly focus on ”consent”, ”right of access to data which has been collected” and ”compliance”. This privacy framework places responsibility on the controllers of data (Diaz, Tene and Gürses, 2013). In this perspective, these controllers act as the stewards of this data. This legal framework has been defined, based on the fairly well accepted Fair Information Practice Principles (FIPPs). FIPPs mainly apply to the data controllers; who are the cloud service providers in this case and third party processors such as corporate or governmental firms that collect data, process, store or use the data in another way (Diaz, Tene and Gürses, 2013). Following the FIPPs, cloud service providers can be viewed as a 'trusted data controller' with respect to human rights using concepts such as ”the principles of choice”, ”purpose limitation”, ”security” and ”accountability”. However, on the other hand the FIPPs contain certain aspects that makes us question trusting the cloud service provider, for example ”data minimization” and ”collection limitation”.

In preceding research in 2009, Cavoukian established a universal framework to guarantee the protection of privacy in networked data systems and technology, by default. This Privacy by Design Framework consists of seven fundamental principles which also reflect the ideology of the FIPPs.

1. ***Proactive** not Reactive; **Preventative** not Remedial:* Events that can have an invasive effect on privacy should be anticipated and prevented by the proactive adoption of solid privacy practices.

2. *Privacy as the Default Setting:* a maximum degree of privacy is strived for by ensuring that personal data in any given IT system is automatically protected. The user does not have to take any action. The key foundations of this principle are based on ”**Purpose Specification**”, ”**Collection Limitation**”, **Data Minimization** and ”**Use, Retention, and Disclosure Limitation**”.

3. *Privacy Embedded into Design:* Privacy should be embedded into the design and architecture of IT systems in a holistic, integrative and creative manner and should not be added on later. It should be incorporated holistically by considering the context, integrative by including all stakeholders and creative as to re-defining preceding designs.

4. *Full Functionality - Positive-Sum, not Zero-Sum:* the accommodation of all legitimate interests and objectives of the organization in a win-win manner by a multi-functional solution, instead of the old zero-sum approach in which privacy trade-offs are made.

5. End-to-End Security - Lifecycle Protection: Strong security practices should be implemented throughout the whole lifecycle. Entities should assume responsible management of personal information and principles, for example, by destroying data in a timely fashion.

6. *Visibility and Transparency:* this principle ensures all stakeholders in business practices and technologies operate according to objectives and stated promises. In this, visibility and transparency are crucial to achieve accountability and trust. This principles highlights three Fair Information Practices: ”Accountability”, ”Openness” and ”Compliance”.

7. *Respect for User Privacy:* the architects and operators should always keep the design user-centric by prioritizing users’ needs and interests. Four Fair Information Practices are considered: ”Consent” - The individuals specific consent is needed for collection, processing, or disclosure of personal data; ”Accuracy” - Personal information should be accurate, timely and complete; ”Access” - Users should be provided access to their personal data and should be informed regarding its uses and disclosure; ”Compliance” - Organizations should take measures (e.g. complaint and redress) and communicate these to the public.

This pre-existing framework for privacy has already been used by organizations to implement privacy. However, a legal binding law that encapsulates this concept of ’Data protection by design and by default’(Regulation, 2016; Kurtz et al., 2019) is the General Data Protection Regulation (GDPR). The GDPR is the most comprehensive online privacy approach up to this point (European Commission, 2018). According to the GDPR, four main entities can be described: data subjects represent the users from which data is acquired; data controller which is the cloud service provider who aims to gather and process data; processor might be employed by the data controller to process user data (organizations); a third party might be authorized by the data controller to process user data (partially) with the goal of performing big data analytics for example.

Under the GDPR, several rights are granted to data subjects:

- They hold the right to be informed by the cloud service provider regarding privacy policies in a transparent and clear manner;
- They have to be communicated about data collection, processing and data sharing practices by the cloud service provider;
  - Contact information of the cloud service provider, purpose of data collection, the recipients of data sharing practices, period of retention and collected data types need to be informed
- Users hold rights of access to data, right of rectification and deletion, right to limit processing of data, right to object and the right to data portability.

These rules stress the notion of privacy in which the endeavouring of control over data is highlighted, in which informed consent is considered as a focal point (Warnier et al., 2015). However, practices carried out *with informed consent* and as acceptable under the GDPR may have discriminatory and unjust consequences (Padden and Öjehag-Pettersson, 2021). Even though consent has been designed to grant individuals control over their information (Recital 7 GDPR), it has been remarked to be an ill-suited legal basis for the act of data processing. People usually just tap the consent boxes for convenience and do not read and ponder over complicated privacy agreements (McDonald and Cranor, 2008; Koops, 2004). Padden and Öjehag-Pettersson (2021) draw attention to the business-like attitude of the European regulators as they bring the notion of ’surveillance capitalism’ (Zuboff, 2019) and ’platform capitalism’ (Srnicek, 2017) to light, which mainly focus on a business model centering around algorithmic profiling.

4.2.2. Neglecting regulatory stance

European inhabitants are obligated to the demands of data sharing in this platform capitalism and the European Commission see the lack of trust as a hindrance for the online economy of Europe (European Commission, 2010). Edward Snowden’s revelations in 2013 of mass surveillance of people’s online communications brought trust into greater attention (Zuboff, 2019). The hidden conspiracy between non-public providers and governmental organizations was responsible for new crisis management challenges with responding to the public outrage. The European Commission responded that safety measures needed to be strengthened in order for people to accept big data so that digital advantage can be seized and thus, economic benefits can be obtained (European Commission, 2014):

”Many of us were shocked by the recent revelations of online spying, and invading privacy... . But, serious though this issue is, our answer cannot be extreme. For one thing, it would be dangerous, as we turn our backs on a huge digital opportunity. Like the huge economic and social innovations of big data; it would be a disaster to turn those down, and we can’t afford that”. The revelations brought attention to privacy issues and enhanced the position of privacy defenders (Rossi, 2018).

However, the present-day GDPR regulation is vulnerable to certain risks as identified by Padden and Öjehag-Pettersson (2021): (1) the risk to personal data of ”a lock and key variety” and (2) the risk to people. The first revolves around the implementation of required technical measures to enable confidentiality and security of data processing activities and that data is only available to the intended persons (Recital 29 GDPR). In the GDPR, the concept of personal data of a data subject has been captured as (Article 4 GDPR): ”any information relating to an identified or identifiable natural person”. The problem this introduces is that anonymized data can still be used in profiling techniques (Mann and Matzner, 2019). Furthermore, there is an absence of consensus regarding whether the derived information should be classified as personal information (Mann and Matzner, 2019).

Data subjects have the right to be informed about data processing practices and purposes (Recital 60 GDPR) and also can access information regarding them (Article 15 GDPR). These regulations target existing information asymmetries and try to comply to the transparency principle (Article 15 GDPR; Padden and Öjehag-Pettersson, 2021). Besides information asymmetries, Daly (2016) argues that the current EU regulation is based on governing the private companies as they possess power, which in turn hinders autonomy of individuals. They stress that ”EU regulation does not address fully the negative impact that concentrations of private economic power have over the free flow information online and thus Internet users’ autonomy” (Daly, 2016). Furthermore, these power asymmetries threaten the concept that consent can be freely given by users, and that the user does not have room for bargaining as they are given a couldn’t-care-less attitude regarding privacy notices by platform giants (Bergemann, 2018).

4.2.3. The necessity to incorporate the constitutional privacy principles into European regulation

Personal information identifiers as highlighted in Table 3.1 can be denied access or granted access, which is referred by Padden and Öjehag-Pettersson (2021) as the lock and key perception. The GDPR’s approach to tackle the issue of lock and key variety is by providing a set of technical specifications and rules in order to secure prevent information loss, alteration of data or unauthorized exposure (Article 83 GDPR). The GDPR has adopted many fundamental principles, such as ’purpose limitation’ and ’data minimization’, and aims to increase control provided to users (Recital 68 GDPR). Regardless, these principles continue to be preferable, it is challenging to accommodate control over user data and data minimization. Especially, since more personal information than ever is being processed at the moment (Lynskey, 2015). Similarly, Koops (2014) emphasizes that it would be irresponsible to look at today’s situation and insist that data minimization prevails. Technical and organizational procedures such as ’data protection by design and data protection by default’ (Article 25 GDPR) are more distinct when identifiers as in Table 3.1 need to be protected. These measures however become impractical when core values such as ’fairness’ (Recital 71 GDPR) and ’rights and freedoms’ (Recital 78 GDPR) have to be guaranteed (Padden and Öjehag-Pettersson, 2021).

The risk to individuals can be seen as violation of ’social and mutable norms’, for example fundamental rights and freedoms (Article 1 GDPR), fairness (Article 5 GDPR) and public interest (Article 6 GDPR). These values can be ambiguous, clashing and variable over time. The guiding principle of data processing should focus on how mankind can be served (Recital 4 GDPR). We refer to constitutional privacy principles as followed by Diaz, Tene and Gürses (2013) under the European Convention of Human Rights, which entails that individuals should be protected from illegal (government) surveillance. Unlike, the concepts of informational privacy, constitutional privacy does protect against surveillance coming from private actors or governmental bodies (Diaz, Tene and Gürses, 2013). Thus, data controllers should be considered adversaries, as data revealed to data controllers is always compromised under this perspective and does not remain private. After disclosure of personal information to the controller, it becomes hard for the user to control how this data will be used by the controller. There-

fore, European regulators and policymakers should recognize the severity and apply proper regulatory mechanisms so that individuals can exercise 'their right to privacy as freedom from surveillance' (Diaz, Tene and Gürses, 2013).

4.3. Interference from US

As we already established, the GDPR contains several constitutional obligations (Hoofnagle, van der Sloot and Zuiderveen, 2019). Rodota (2009), a member of the writers of the Charter of Fundamental Rights of the European Union, elaborated that protection of personal information should be seen as a pledge made by kings to their knights in 1215, such as in the Magna Charta; they would not have to worry about being imprisoned or tortured in an illegal way. This pledge should also be refreshed and transformed from the substantial body to the digital body. The sanctity of the individual should be reinforced in the digital dimension, corresponding to the recent concentration put on respecting the human (Hoofnagle, van der Sloot and Zuiderveen, 2019). These responsibilities existed way before the rise of Silicon Valley data companies, but these values have become more essential since the dominance of these companies. However, the difference between the contextual US regulatory laws and the GDPR still differ, as the GDPRS's context can be vague and ambiguous in some places and has been written at a level of goal-oriented principles. Zuiderveen (2015) describes parts of the GDPR to be 'principles-based regulation' and its recitals based construction makes the provisions even more unspecified (Klimas and Vaičiukaitė, 2008; Hoofnagle, van der Sloot and Zuiderveen, 2019). And in turn these uncertainties vex US lawyers (Hoofnagle, van der Sloot and Zuiderveen, 2019). In contrast to the instrumental values in Europe, the US seems to interpret privacy as values that are morally important. For instance, they recognize the importance of liberty and moral concerns regarding governmental transgression in the personal life of individuals as the main principles of privacy (Whitman, 2003; Christen, Gordijn and Loi, 2020).

4.3.1. Data Location and transparency issues

Cloud service providers typically process and store information on multiple servers at various locations and thus, this email data is moving constantly between these servers spread all around the world. When personal data is collected and replicated in this way at an untrustworthy host, it is questionable whether consent can be given for a certain task. There can be a lack of understanding and awareness as to how the information is processed, because information about data's location is not disclosed or unavailable to the customer. This complexity makes it hard to estimate whether security safeguards are set up and consistency with laws and regulations is unclear and difficult to assess (Suresha and Vijayakarthick, 2020). This *lack of transparency* may lead to a lack of control over where data may be located (Kaur, Agrawal and Dhiman, 2012) and thereby impact organizations' decisions to employ cloud-based email service.

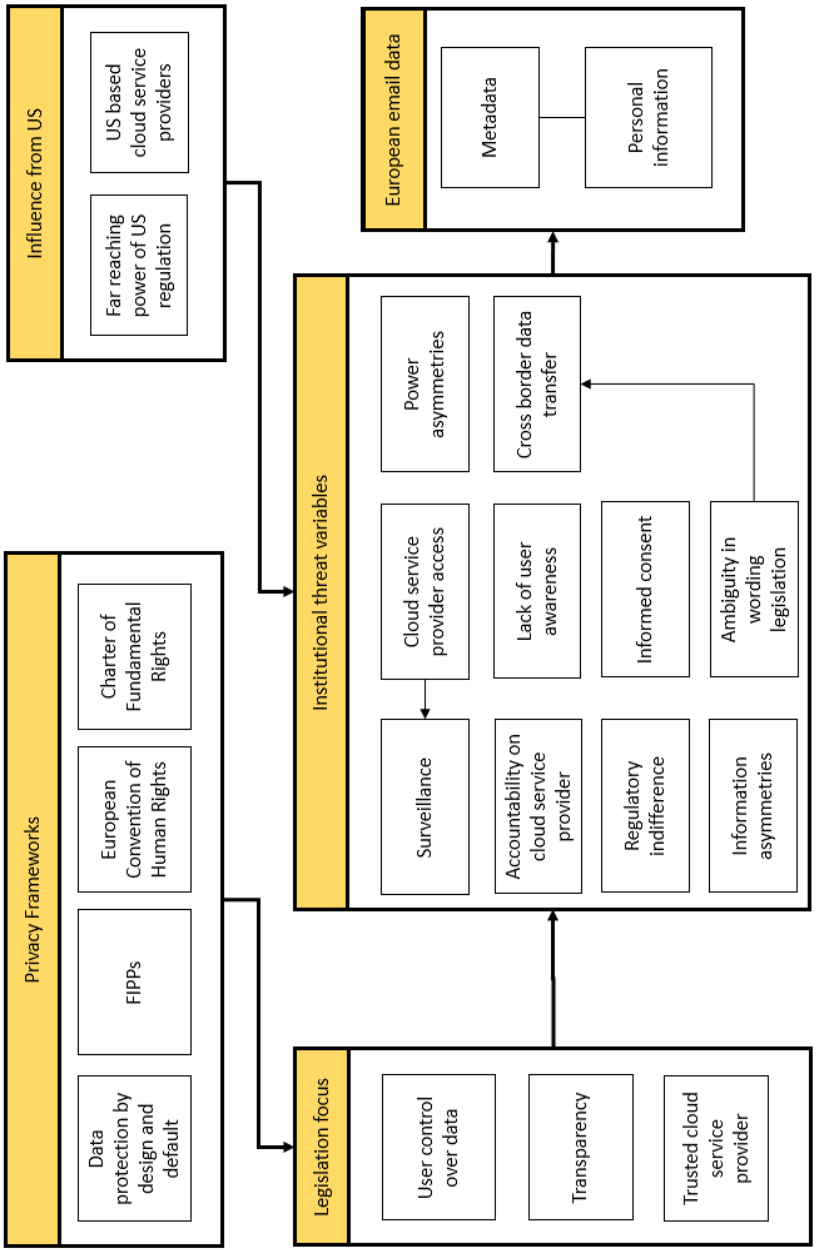
4.3.2. Cross border data transfer

If sensitive personal information comes to cross the borders of countries, it becomes challenging to promise safeguarding under international laws and regulations. One primary example of this concern is the far-reaching power of the USA patriot act, which has agitated foreign governments for the reason that it would permit the US government to retrieve sensitive data outsources to American companies, like medical records (Paquette, Jaeger and Wilson, 2010). Even though national and international laws have focused on limiting trans-border flow of data, several concerns are raised, for example whether regulations in the jurisdiction where information has been collected allows for data flow. The GDPR imposes additional responsibilities to European data transmitted to the US (Suresha and Vijayakarthick, 2020). A Lack of transparency in combination with uncertainty around legislation's of the cloud service providers' country may lead to a lack of trust (Zafar et al., 2014).

4.4. Institutional threat system

The literature about the institutional background has given insights about the institutional system in which the email ecosystem is presented. We identified privacy frameworks that influence the focus of the European legislation. Factors resulting from US interference, the current and future focus of the European legislation have impact on the institutional threat variables and can be found in Figure 4.1.

Figure 4.1: The institutional threat system



5

Towards a threat landscape for the process mail ecosystem

In this chapter, we tried to understand interests and objectives of different actors within this process mail ecosystem. We also discussed the triggering aspect of the threat landscape, which is the attack space. We first present the process that enabled us to gain the literature review we performed on the process domain. After this, we present the literature review.

5.1. Literature selection

In order to understand cloud service providers and the cloud computing environment in which they operate, we investigated Henze (2018), Pasquier and Powles (2015), Zardari and Bahsoon (2011) and Ghorbel, Ghorbel and Jmaiel (2017). We specifically noted that centralized cloud-markets means the market is dominated by several providers in papers by Leong, Petri, Gill and Dorosh (2016) and Barbaschow (2016). This can have implications as demonstrated by Microsoft (2017), Satzger et al. (2013), Opara-Martins (2017) and Körner (2020) which have been collected by database search. Opara-Martins, Sahandi and Tian (2016) and Baudoin et al. (2013) have been found by backward snowballing. These studies highlighted the issues with contractual agreements, therefore, we searched the database for understanding of SLA's and found Terfas (2019), Terfas, Suryn, Roy and Eftekhar (2018), Faniyi and Bahsoon (2015). We also searched the database for complications around SLA's which resulted in papers by Shimba (2010), Taddicken (2013) and Mulder and Tudorica (2019).

Further on, we analyzed sectors for its relevance, privacy and security relating threats. We used a combination of scientific and informal literature due to the actual nature of the sectors. The selected literature has been enlisted in Table 5.1.

Authors and date	Focus	Search method
Tweneboah-Koduah, Endicott-Popovsky and Tsetse (2014), Hartholt (2016), Ibestuur (2019)	Executive government	Database search
Healthaffairs (2020), Seh et al. (2020), Zafar et al. (2014), HIMSS (2019), Spamtitan (2019)	Healthcare	Database search and forwards snowballing
Palos-Sanchez (2017), Marston et al. (2011), Kaspersky Lab (2020)	SME's	Forwards snowballing and database search
Xu (2018), Fiebig et al. (2021), Srinivasan (2011), Matthew (2015), Aydin (2021), Hayhurst (2021)	Higher educational institutes	Forwards snowballing and database search
Zekrya (2011), Marston et al. (2011), Lokuge and Sedera (2017), The Guardian (2017)	Large companies	Forwards snowballing and database search
Zhou, Ghosho and Giyane (2014), Microsoft (2021), Shavell (2021)	NGO's	Database search
Mungai (2012), Afrika (2018), Research and Markets (2021), Mimecast (2021)	Financial services	Database search

Table 5.1: Overview of selected literature for sectors

After considering the mentioned threats, we tried to investigate different attacker profiles, which could benefit by attacking data stored in clouds. These attackers can be driven by different motivations. We found informal sources that suggested political motives in The Washington Post, The New York Times (2021) and BBC News (2021). Furthermore, we assessed a research by Ablon (2018) describing the monetary motivations of cyber threat actors. However, the most prominent attacker profile has been in the shape of legal extract by misuse of power. To research this, we looked at a combination of formal and informal sources found by database search and Google search. Research by Swire (2012), a news article by The Washington Post (2021) and Freedom of the Press Foundation (2020) focused on legal extraction by governmental bodies and law enforcers. A news article by Lawne (2020) described a controversial legal extraction case by threat intelligence agencies.

5.2. Cloud service providers

In Chapter 3.3.2, we already distinguished different type of cloud service providers. In particular, this research focuses on cloud service providers of the type: (1) cloud email hosters and (2) email security providers. The complex landscape in which these cloud service providers operate is not transparent towards its consumers. In the cloud computing infrastructure, the technical complexity of cloud-based email services is often secluded (Henze, 2018). This introduces the usage of indirect resources because cloud-based email services may be actualized resting on cloud infrastructure, and this in turn may lead to unfamiliar and indirect contractual interchange (Henze, 2018). Pasquier and Powles (2015) elaborate that cloud services often assign to other cloud services or depend on cloud infrastructure, for example to speed up scalability, to evade having to operate own cloud infrastructure or to increase resilience against cyber attacks. For instance, cloud service providers may outsource different services, like security services (anti-spam filtering etc) and data processing to external parties. This outsourcing of services and data proliferation is not controlled by the cloud service providers (Zardari and Bahsoon, 2011). Thus, a lack of transparency in the technical and contractual implementation of cloud-based email services causes consumers to 'forcibly' trust an unknown number of third party cloud service providers with their personal information. This state has become too tangled for service developers and consumers to comprehend (Ghorbel, Ghorbel and Jmaiel, 2017). Especially in a situation in which European legislation is centred around trusting the data controller, e.g. the cloud service provider, this could lead to serious privacy risks for users.

5.2.1. Dominance of cloud service providers

The current marketplace of cloud-based email service providers can be described as a centralized market, in which several number of services are dominating (Henze, 2018). In previous years, technology and research consultancy Gartner (Leong, Petri, Gill and Dorosh, 2016) already saw the prevalence of Microsoft and Google in the cloud-based email adoption among companies belonging from various sectors and of different sizes (Barbaschow, 2016). The presence of centrality on the cloud services market can come at a considerable cost. First of all, an increase of 300% was observed in the number of targeted Microsoft user accounts ranging in the period from 2016 to 2017, and thus centralized services can be a beneficial target for cyber attackers (Microsoft, 2017). Therefore, the prevalence of certain cloud service providers can be a decisive factor in estimating future threats with regard to data hosted with the providers. Furthermore, the options to switch to alternative cloud service providers are rather limited. Especially when migration between cloud service providers has become more complicated due to absence of common standards and technical inconsistency (Satzger et al., 2013). This vendor lock-in by the cloud service provider can appear in different forms: lock-in of data, lock-in of application and lock-in of contract (Opara-Martins, 2017; Körner, 2020). A vendor lock-in can occur when the cloud service user seeks to integrate supplementary cloud services from other vendors or when the user wants to switch their cloud service provider (Opara-Martins, Sahandi and Tian, 2016). A data lock-in entails that users are incapable of getting their user data out of the bounds of the cloud service provider, as the company data is usually stored by the cloud service provider (Mell and Grance, 2011; Körner, 2020). The lock-in of application occurs when the application has become deeply ingrained within the functioning of the cloud users' organization and they might be hesitant to turn to another provider because of challenges such as required retraining for staff (Opara-Martins, 2017; Körner, 2020). In the case of a lock-in by contract, inflexible and poor contracts between cloud service providers and users can buildup the burden of enterprises in search of additional services from other vendors or to switch to an alternative provider (Körner, 2020). In that situation, specific details regarding measures that fall under the cloud service providers' responsibility, are often issued vaguely in standard formal agreements (Baudoin et al., 2013) such as service level agreements.

5.2.2. Implications around Service Level Agreements (SLA's)

Cloud-based email service users typically encounter SLA's when they first decide to employ the service (Terfas, 2019). The agreement between the cloud service provider and user pursues to specify the level of service desired by the user and aims to set out their requirements (Terfas, Suryn, Roy and Eftekhar, 2018). Clearly defined SLA's can lead to an increased level of service and reduced violations of service (Terfas, 2019). However, a very foremost problem is that SLA's in cloud based ecosystem are not yet mature to a point where vital applications can be deployed in a reliable manner (Faniyi and Bahsoon, 2015).

Users often base the selection of cloud providers on the reputation of the cloud providers, their service level agreements, past experiences and subjective ad hoc inputs. SLA's are expected to act as a mediator between consumers' expectations with regard to the cloud service provision. An issue arises when SLA's are non-negotiable and static and do not address the individual requirements of the users (Zardari and Bahsoon, 2011). SLA's are considered to representing the level of trust that an organization has in the cloud service provider (Zafar et al., 2014). In addition, (Shimba, 2010) found that a challenge can be observed in meeting the requirements of SLA's by the cloud service providers. Another facet of this problem is the privacy paradox: most users give consent to privacy policies without actually being aware of what the consequence will be for their personal data. In this paradox, people hold their privacy in high regard, they do not act on that account (Taddicken, 2013; Mulder and Tudorica, 2019). Therefore, typical concerns for organizations are:

- To whom is their email data accessible?;
- How many backups of the email data exist on the cloud servers?;
- How can organizations be certain their data has been deleted upon request?;
- And most importantly, how can you be sure whether privacy policies are respected by all involved parties?

5.3. Sectors moving to cloud-based email

The previous literature has shown the complex environment in which threats are posed on email data privacy and security in the cloud. In this section, an overview is presented of identified sectors who may come to face such threats as a consequence of email outsourcing to cloud-based services.

5.3.1. Executive government:

The executive government consists of different bodies spread over layers, such as the national level, the provincial level and the municipal level. These governmental bodies may employ cloud based email services for lower operating costs, high scalability possibilities, no need for up-front investment or easy access through applications (Tweneboah-Kuoduah, Endicott-Popovsky and Tsetse, 2014). However, cloud based email systems can pose several risks for privacy and security of involved governments and involved individuals. Such is the case with 35 Dutch municipalities, that came under pressure for their weak security standards. A report by the domestic administration (Hartholt, 2016) that almost no municipality satisfied the mandatory security standards, such as DKIM, SPF and DMARC. This made the municipalities vulnerable to phishing attacks. An even bigger danger is the use of webmail. It has proven to be hard for civil servants to differentiate the forged webmail from the original mailbox, when adequate security measures are not present. The executive government has been moving (parts) of its operations to the cloud, albeit their move is quite reluctant (Ibestuur, 2019). Therefore, we analyze briefly what this move may entail for privacy and security of citizens and governmental employees.

5.3.2. Healthcare:

In the US healthcare system, about 90% of the physicians deploy an electronic health record (EHR) (Healthaffairs, 2020). These EHRs have caused healthcare data to be more digital, distributed and mobile (Seh et al., 2020). Historically, these EHRs ran on site, within a hospital data center. In a more recent move, the EHR system vendors now provide cloud services which shift the management and hosting of EHR's to a third party (HealthAffairs, 2020). The challenges in healthcare organizations' IT infrastructure are for example, scalability, an increased need for collaboration with other organizations and accessibility. Cloud based services improve this situation with its elasticity of resources, broad access to the network and measured service according the the demand. Email is an aspect of medical collaboration tools or medical teaching and learning (Zafar et al., 2014) and thus is a fundamental service.

The rise of cloud adoption in healthcare has lead to serious concerns, as medical information is of high value. A majority of healthcare facilities seem to fall behind in terms of protecting this data considering the responsibility they have. According to the HIMSS Cyber security survey in 2019, 59% of the IT experts in healthcare have stated that the most common area of compromise was email. In addition, more than 64% of health data from EHRs has been compromised from 2005 to 2019. Furthermore, in the preceding years from 2015 to 2019, hacking incidents uncovered about 92% of the total records with email and network servers being the main target (Seh et al., 2020). One notable incident occurred with a large healthcare insurance provider Anthem inc., which experienced a data breach due to a spear-phishing attack in 2015. This has been one of the most expensive phishing attack targeted at healthcare organizations (SpamTitan, 2019).

5.3.3. SME's:

SME's can obtain direct access to cloud computing resources. They can set operations in motion without a large investment, which enforces speed to the market (Palos-Sanchez, 2017). Cloud service providers carry responsibility about licensing and upgrading. Also, scalability improves the need for time resources and SME's can use exactly the computing resources they require by calibrating resources according to the demand (Marston et al., 2011). Moreover, the Kaspersky Lab (2020) found that about 37% of SME's are currently thinking of increasing the use of cloud based services. Despite this move, SME's are worried about the safety of their sensitive data in the hands of cloud service providers. The study revealed that 33% of the total incidents in which hosted infrastructure has been affected, were caused by phishing attacks in particular.

5.3.4. Higher educational institutes:

Email is considered as one of the primary means for information exchange by educational institutes, such as universities (Xu, 2018). Especially, since the occurrence of COVID-19 universities have had to switch to remote education (Fiebig et al., 2021), which in turn partly relies on communication through e-mail. As valuable data of these universities or colleges is carried by email, its security is of utmost importance (Xu, 2018). Two primary ways for the higher educational institutions to manage the email of its users is either (A) on premise or (B) cloud services. The former approach has mainly been the traditional way in which email has been managed, resulting into many challenges such as high storage requirements and expensive investments (Srinivasan, 2011). In a recent study of Fiebig et al. (2021), a migration to cloud services by universities can be observed.

Compared to traditional ICT infrastructure in universities, cloud based services introduce possibilities to access online resources on-demand e.g. e-learning platforms, digital archives, database repositories, e-mail, portals and research applications (Matthew, 2015). As most universities deal with budget shortages, cloud computing provide an efficient alternative for systems management in a cost saving manner (Aydin, 2021). However, as valuable data is moved to cloud service providers, target setting by attackers will move along. In 2017, the Westminster College in London had fallen prey to a phishing scam. In this scam, an employee clicked on an email link, which appeared to be originating from staff. This resulted in the compromise of W-2 statements, which were then used to file fake tax returns. Even though the situation was severe, this breach was an eye-opener for the Westminster college, as they reassessed their approach to data security. For this reason, we highlight the security and privacy challenges for higher educational institutes (Hayhurst, 2021).

5.3.5. Large companies:

Cloud based services offer the main advantages of flexibility and prompt accessibility for large companies. Also, it brings along the benefit of having to maintain a smaller IT department (Zekrya, 2011). Cloud based services allow larger organizations to strengthen efficacy and productivity to achieve competitive advantage (Marston et al., 2011; Lokuge and Sedera, 2017). Despite the much promising benefits of cloud based services, we have seen clear privacy and security related risks for large enterprises. One example is the cyber attack on one of the world biggest accountancy firms, Deloitte. The data breach occurred in 2016 and hackers gained access to varieties of data including confidential emails. They potentially had access to usernames, passwords, business diagrams, IP addresses and health details. On top of that, certain emails contained attachments with design information and sensitive security. The hacker could accomplish this by gaining access to the companies' universal email server via an administrator's account. Emails belonging to staff were cached on the Azure Cloud service, hosted by Microsoft. This cyber incident set Deloitte into re-evaluating its security approach (The Guardian, 2017). One particular noteworthy aspect of this incident is the interrelation with different sectors and its impact on their privacy and security. For example, Deloitte provides, inter alia, tax consultancy services to media, governmental organizations, some of the biggest banks and other multinational companies.

5.3.6. NGO's:

The mission of NGO's is to encourage certain causes e.g. in healthcare, education, governance or education. ICT is a relevant element in the execution of these missions. Like the case with universities, NGO's have been facing challenges with regards to maintaining their current ICT infrastructure due to a restricted budget being available. Therefore, the characteristics of cloud based services, such as low upfront expenditure, scalability and payment for what service you consume are interesting investments for NGO's (Zhou, Ghosho and Giyane, 2014). Regardless of these features, the security and privacy of their data is something to consider seeing the growth in phishing attacks. One particular example is the threat posed by NOBELIUM, who has been continuously launching phishing attacks by specifically targeting for numerous types of organizations, among which NGO's. The Microsoft Threat Intelligence Center (MSTIC) has confirmed this activity in which the threat actor NOBELIUM attempted to access cloud service providers that are employed by such NGO's. After gaining access to the cloud environ-

ments, the attackers aim to to reach customers and achieve further access to other systems (Microsoft, 2021). The CEO of a privacy company, Rob Shavell, observes that more than 50% of NGO's have been set under attack by cyber criminals and can be classified as easy targets for cyber criminals (Shavell, 2021).

5.3.7. Financial services

Cloud based services allow banking institutions to approach their customer in an interactive manner; innovation can be achieved in a more efficient way. Also, multiple benefits are offered by cloud computing services for banks, such as a smaller continuous operational cost instead of large expenditures (Mungai, 2012). Due to the eruption of mobile cloud based banking, services can be brought closer to users, through e-payments for example (Afrika, 2018). Even though many banking organizations make use of cloud adoption for their email services, this industry has been increasingly targeted by attackers. For example, a large UK bank TSB became the victim of a phishing incident. The phishing emails resembled original emails and were sent to customers to ask for verification of their account due to security problems. As a consequence of this attack, 1300 clients reported cases in which their bank accounts had been emptied (Research and Markets, 2021). Mimecast, a cloud security company, highlights the danger for the Banking industry in their email security report, because of their vulnerable nature. Financial service organizations often deal with money, have a large clientele and their sensitive data such as income, bank and contact details (Mimecast, 2021).

5.4. Attacker Profiles

Within the scope of this research, we differentiate between insider access and outsider access. Insider access occurs by legal extraction by governmental bodies. Outsider access on the other side stem from political motives and financial gains. We convey these scenario's in this section.

5.4.1. Insider access: misuse of power by legal extraction

A research by Swire (2012) explains how the rise in adoption of encryption lead to a greater emphasis on access of stored records in the cloud by law enforcement and national security lawful access. Due to the strong encryption at the Internet Service Provider's (ISP) level, a lawful order to access these messages by government agencies does not reveal the content of the communication. However, it is crucial to note for the upcoming strategies of lawful access, that emails saved by consumers on the webmail's servers are not always strongly encrypted. The cloud service provider (server owner) always holds the ability to decrypt the plaintext of the email message. Therefore, a lawful access order made by government agencies may result in successful disclosure of emails. When these agencies fail to access email data at local ISP's, then they have a strong incentive to find unencrypted email data, which can be either from a third party in the communication or a third party system owner between the parties. For example, majority of email data held by Gmail or Hotmail is unencrypted at server level, thus governmental agencies have motives to request access from Microsoft or Google. Such incentives from various involved stakeholders on different levels could increase the complexity of the problem, especially when stakeholder values clash on certain domains.

One relevant example of such clashing values are the recent attacks of the US government to access email data of journalists of The Washington Post in order to uncover the identity of their sources. The government used Proofpoint, a firm that offers data security services, as a method to gain the reporters' email records and this implies that the attorneys tried to think cleverly where the needed reporter's data might be found apart from the standard email service providers like Google or Microsoft. The struggle of to what lengths the government can go in its pursuit is conflicting with the constitutional protections of the free press (The Washington Post, 2021).

Another situation is the retrieval of a journalist's email content obtained in a leak investigation in 2015, without her being aware of it. The US Department of Justice (DoJ) obtained journalist Ali Watkin's email metadata of previous years without her consent. The aim for this action by the DoJ was to gather evidence against the now retired Senate Intelligence Committee aide James Wolfe. He was suspected

of issuing classified information to other journalists. In doing so, the guidelines of the DoJ in which they do not have to inform journalists that their records have been obtained, do not have the force of the law. Thus, the DoJ can potentially break rules without accountability. Also, Watkins had no opportunity to withstand the legal order before the request was permitted by the email service provider (Freedom of the Press foundation, 2020).

The case of Edward Snowden is one of the controversial issues. Snowden is a former National Security Agency (NSA) contractor, who revealed how the US government has been collecting data, among which emails, on millions of Americans using servers of Google, Microsoft and Facebook. Furthermore, he has issued a statement that he would be able to retrieve raw data, IPs, email headers etc., if he would target for a certain email address under the FAA702 law. This law allows for electronic information collection of people outside the US (Lawne, 2020). This case certainly demonstrates the need for a debate on privacy and ethics.

5.4.2. Outsider access: political motives

Email attacks due to political unrest have become quite common in the recent years. Such is the email compromise case in 2016, during the US presidential election, when emails of Hilary Clinton and her campaign manager John Podesta had been released through WikiLeaks. The release of these documents has brought significant harm to her campaign (The Washington Post, 2016).

In a recent hacking campaign in January 2021, thousands of email records of businesses and government agencies have been compromised from the Microsoft email service. Microsoft has stated that these attacks were probably sponsored by the Chinese government. The US government's cybersecurity institution issued an emergency warning, as the hacking campaign had affected a large number of targets, which is estimated to be about 30000 Microsoft customers. The hackers were even able to collect emails and install malware to continue monitoring of their targets, and Microsoft said it had no sense of the extensiveness of the theft. The Microsoft systems are used by a broad range of organizations, from small businesses to state and local governments, and even military contractors, large banks and healthcare (The New York Times, 2021). Also, the European Banking Authority's email servers have been targeted by the attack and its personnel's email data has been compromised (BBC News, 2021).

5.4.3. Outsider access: financial gains

Cybercriminals can perform attacks on email systems with the aim of making money. In such attacks, they attempt to access, for example personal data, health information or financial data, and sell this on underground black markets. These cybercriminals often rely on known vulnerabilities in a system. Also, phishing and spear-phishing are quite common. In such attacks, credentials such as usernames, email addresses or passwords can be obtained and allow the attacker to access the contact list of the victim to carry out further spam or phishing campaigns. When the attacker has access to company email addresses, the attacker can act as a legitimate employee and demand for a presumably legitimate transfer. The funds will get transferred in the account of the money mule, who will probably send it further to the attacker or withdraw it (Ablon, 2018).

5.5. Threat Assessment Framework

The background has produced relevant insights regarding actors, their complex processes and implications as a result of their interdependencies. We identify crucial sectors that might use cloud-based email services and outsource email services to cloud service providers. This may bring implications for their European data as they might outsource services to external providers. In addition, factors from the attack space have influence on how cloud service providers operate. These relationships produce threats we aim to look further into. Essentially, it is important to investigate what the level of cloud adoption is in combination with prevalent cloud service providers to estimate the future threat landscape. We capture most important relationships within the subsystem in Figure 5.1.

5.5.1. Process threat system

The different actors in this process subsystem introduced various threats, which can be initiated by the adversaries in the attack space. We identify vulnerable sectors, cloud service providers, which collaborate with third party providers and an attack space containing adversaries with different motivations. The process threat system has been depicted in Figure 5.1.

5.5.2. Overall threat assessment framework

The prevalence of cloud service providers and the level of cloud adoption can be considered as factors that trigger the cloud-based email threat landscape. Thus, these factors strongly determine the future threat scenario for the mentioned crucial sectors. In Figure 5.2 we present the overall threat assessment framework resulting from the combination of the technical, institutional and process subsystem.

Figure 5.1: The Process threat system

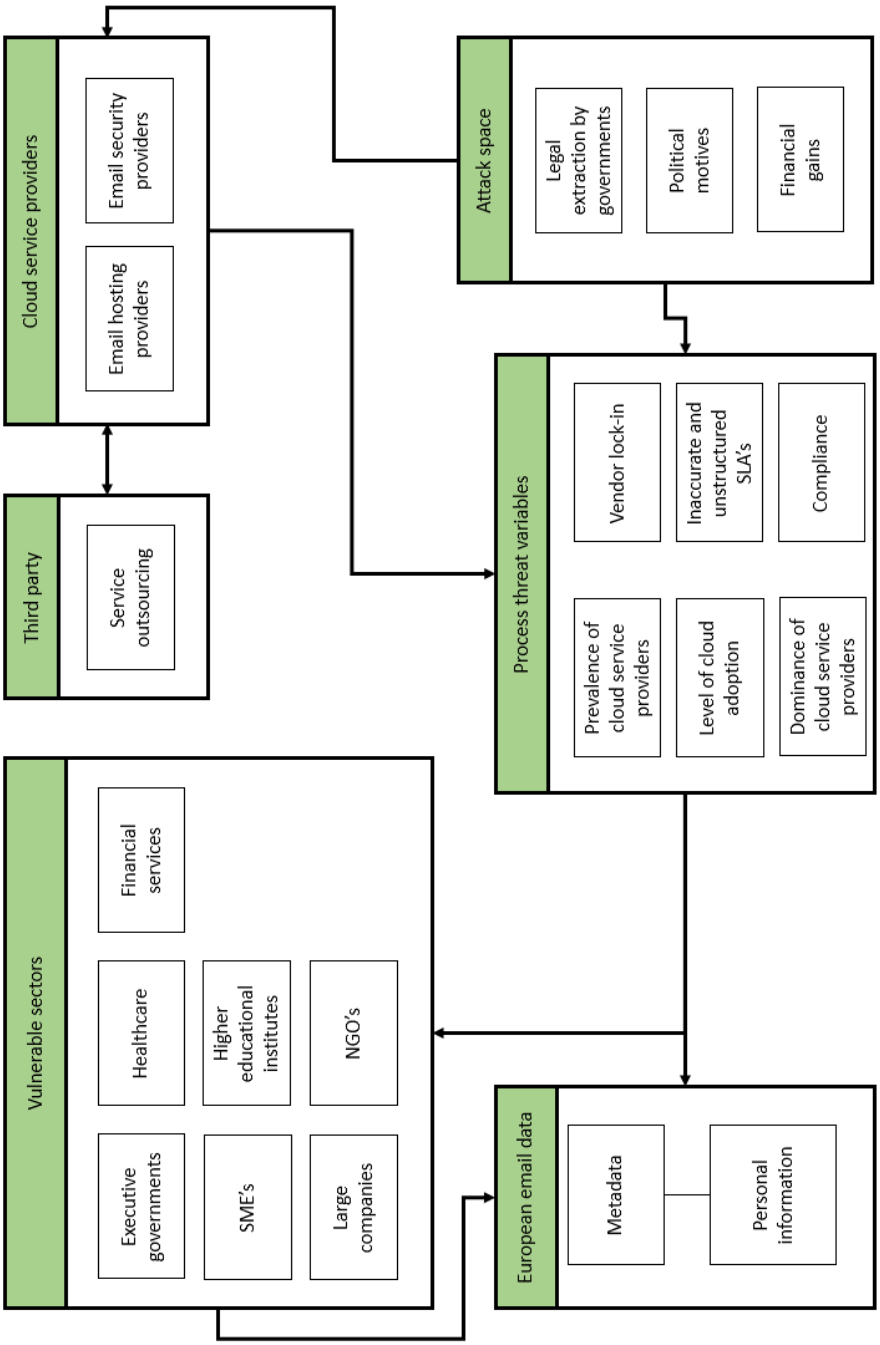


Figure 5.2: The threat system

6

Data analysis

In this Chapter, we will discuss the process of the data analysis. We commence with the data collection process in which we gather input data for the measurements. After this, we review the presented results. The aim of this Chapter is to gain more insight into the current level of adoption of cloud-based email services among sectors, and which cloud service providers may have become prevalent over the past years.

6.1. Data collection

We describe the procedures for selecting organizations and cloud service providers.

6.1.1. Selection of organizations

In accordance with the data analysis approach as described in Chapter 2.4, we first collected data for organizations which constitute the crucial sectors. We focused on collecting domain names for seven sectors in Europe, namely: executive governments, healthcare, SME's, higher educational institutes, large companies, NGO's and financial services. The organizations have been selected manually by inspecting the each organization for its relevance. The selection of organizations has been based on predefined online available lists. In total, we limited the search on 352 organizations per sector. The domains for these organizations will be used to filter the data.

Executive governments: Executive governments can consist of different layers of departments. In this research, we focused strictly on municipalities. Municipalities are situated at a level that has close contact with its citizens, especially through email. Therefore, they possess enormous amounts of personal information regarding the citizens. We looked at 352 municipalities retrieved from Ministry of the Interior and Kingdom Relations (2021), which is a Dutch register containing a list with all municipalities in the Netherlands. Even though, this research is focused on Europe, we have chosen to select municipalities from the Netherlands only. This is thus a limitation to the study, however, a more reliable list containing municipalities throughout Europe is not present at the time. The complete list containing domains of municipalities can be found in Appendix A.

Healthcare: The healthcare sector can also exist of different healthcare facilities like clinics, medical offices and hospitals. We chose to center the research around hospitals within Europe. This is mostly due to the fact that hospitals are the most common type of healthcare facility, which also directly engages with its patients. Thus, hospitals also possess sensitive patient/personal data through email, which is not only shared by patients with their assigned doctor but also among staff. We selected 352 hospitals throughout Europe and comprised the list from the Ranking Web of Hospitals (n.d.). This website ranks hospitals throughout the whole world and per continent. During the selection, we specifically picked hospitals from different countries in Europe in a balanced manner in order to ensure reliability of the results. The complete list containing domains of hospitals can be found in Appendix B.

SME's: Small and medium enterprises across are firms that account for 90% of Europe's businesses (European Commission, 2021). The European Commission defines small and medium firms as an enterprise that has (1) a staff headcount of less than 250 and (2) a yearly revenue of maximum €50M. We used the fifth annual list of Europe's fastest growing enterprises comprised by the Financial Times (2021). Their list provides the opportunity to select companies based on revenue and staff headcount. Therefore, we carefully selected firms that satisfy both conditions (1 and 2). Also, during the selection we aimed to select companies across different countries in Europe. The resulting domains of the companies are presented in Appendix C.

Higher educational institutes: The higher educational institutes sector can consist of universities, colleges and diverse professional schools. However, in this study we will focus on universities across Europe. We decided to follow universities because of the ample availability in predefined lists as there are many rankings available for universities. We investigated universities from the QS World University Rankings (2021), which we filtered for universities in Europe. The domains have been collected and are presented in Appendix D.

Large companies: For large companies, we looked at Europe's top companies based on high revenue. We gathered domains for the largest companies from Value Today (2022). Value Today offers lists of companies in various sectors which can be filtered on time span, company business and company name. We collected domains for organizations that had headquarters in Europe and included different company businesses such as luxury goods, clothing, medical equipment and food products for example. During the composition of the list, we deliberately excluded companies with business fields that intersect with other sectors in this research, for example financial services. The selected domain can be found in Appendix E.

NGO's: For finding domains of NGO's in Europe, we used a combination of two sources. The NGO Branch of the United Nations Department of Economic and Social Affairs (n.d.) published several lists of accepted NGO's which can be filtered on organization type, region, country and development goals. We selected NGO's from throughout Europe, by ensuring that the number of NGO'S selected from one country are in proportion with NGO's selected from other countries. However, as some countries are smaller and NGO's seem less innovative in terms of digital transformation, they do not offer the same level of reliability. Therefore, we also based the selection on the NGO list provided by the European Youth Foundation (n.d.). The comprised list of domains can be found in Appendix F.

Financial services: We based the search for finding domains owned by financial services on the list provided by Value Today (Value Today B, 2022). The results after filtering European financial services revealed several big organizations. We reviewed the resulted financial services organizations for company business, in which we included banking services, insurance companies and investment companies. Also, we specifically looked for companies with headquarters in Europe and took into account what the annual revenue was, and checked its worldwide ranking before including the company in the domains list. The final list can be found in Appendix G.

6.1.2. Selection of cloud service providers

To constitute a list containing relevant cloud service providers, we used several predefined lists and previous researches to collect input data for cloud service providers. We compiled the list using email hosting providers and email security providers. For each of the providers, we searched for MX domains that point towards the cloud service provider. We based the search on providers and MX domains reported by Fiebig et al. (2021), Trost (2020) and Henze, Sanford and Hohlfeld (2017). The final results have been presented in Table 6.1.

Email hosting providers	Hosting providers domains	Email security providers	Security provider domains
Microsoft	outlook.com hotmail.com	Proofpoint	pphosted.com ppe-hosted.com
Google	google.com googlemail.com smtp.goog	Mailguard Mimecast	mailguard.com mimecast.com mimecast.co.za mimecast-offshore.com
GoDaddy	secureserver.net		
Bluehost	bluehost.com	Spamtitan	spamtitan.com
Zohomail	zohomail.com zoho.eu	Protonmail	protonmail.ch mailanyone.net
Rackspace	emailsrvr.com	Symantec	messagelabs.com
Greatmail	greatmail.com	Barracuda	barracudanetworks.com barracuda.com
Hostinger	hostinger.com		
Dreamhost	dreamhost.com	FireEye	fireeyecloud.com fireeyegov.com
iCloud	icloud.com		
Yahoo	yahoodns.net yahoo.com	Trendmicro	trendmicro.eu trendmicro.com
GMX	gmx.net	Forcepoint	mailcontrol.com
Yandex	yandex.net yandex.com	Spamhero	spamhero.com spamhero.net mxthunder.net mxthunder.com
AOL	aim.com		
Intermedia	severdata.net		
Fastmail	messagingengine.com	CSC	cscdns.net
Ionos	1and1.com ionos.com schlund.de	McAfee	mcafee.com
		Deteque	deteque.com
		Hornetsecurity	everycloudtech.com everycloudtech.us hornetsecurity.com futurespam.com
Hushmail	hushmail.com		
Amazon Workmail	amazonaws.com awsapps.com		
Gandi	gandi.net	SiteGround	mailspamprotection.com
MXroute	mxrouting.net	Mailgun	mailgun.org
Sendgrid	sendgrid.net	Appriver	appriver.com arsmtp.com
Hostgator	hostgator.com		
Strato	rzone.de	Solarwinds	spamexperts.com antispamcloud.com
A2hosting	a2hosting.com		
Postmark	postmarkapp.com	Reflexion	reflexion.net
		Sophos	sophos.com
		Cyren	ctmail.com
		Edgewave	rcimx.com rcimx.net
		Vadesecure	vadesecure.com
		Tutanota	tutanota.de

Table 6.1: Overview of cloud service providers

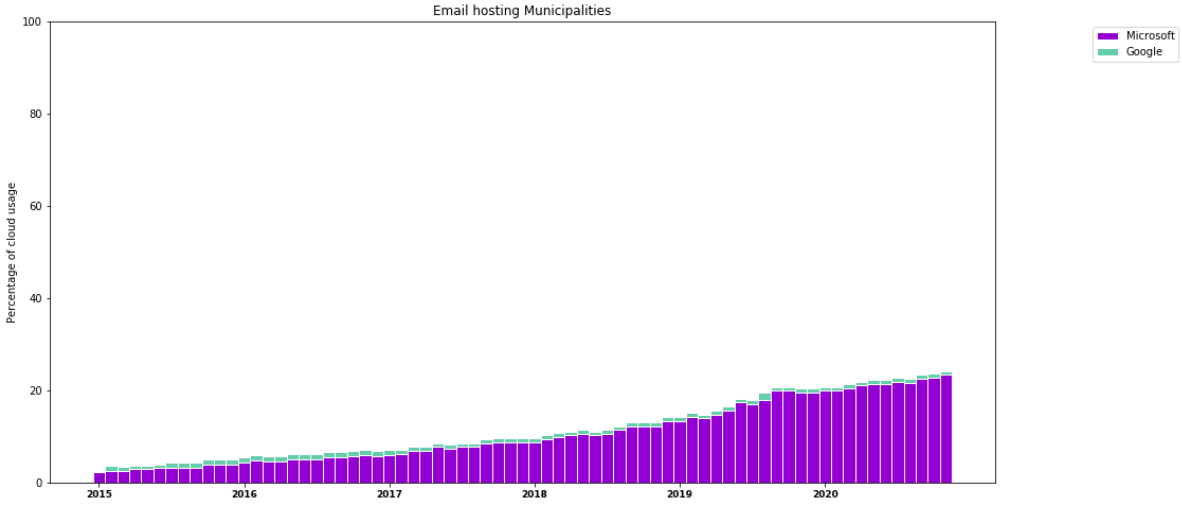
6.2. Measuring the level of adoption of cloud-based email services in sectors

In this section, we will discuss the findings resulting from the performed measurements. The measurements have been executed by following the methodology as described in Chapter 2.4.1.

6.2.1. Prevalence of cloud-based email services in executive governments

The measurement study concerned the prevalence of all email hosting providers mentioned in Table 6.1. The results for the prevalence of email hosting services among municipalities have been visualized in Figure 6.1. Although we evaluated the dataset for an occurrence of all email hosting domains, we can observe a prevalence of only two email hosting providers: Microsoft and Google. A notable feature is the significantly low adoption of cloud-based email services in 2015, which is about 2% for Microsoft and 1% for Google. Over the years up till mid 2019, we can note a rather gradual increase in the use of Microsoft services while the employment of Google services remains at the consistent pace of upmost 2%. We suspect this may eiter be explained by one or two organizations that may have decided to adhere to the provider or are facing issues such as a vendor lock-in (Opara-Martins, Sahandi and Tian, 2016). However, we see a steadfast increase in the use of Microsoft services, especially from mid 2019 on to the end of 2020 which is about 23%. As we solely followed municipalities in the Netherlands, we can observe the move in various digital innovative programs that allow for Dutch municipalities to work together in a more efficient way. In 2017, Dutch municipalities Ouder-Amstel, Diemen and Uithoorn formed a DUO+ alliance in order to achieve administrative collaboration (Microsoft, 2017B). With this initiative, they aim to better cope with the effects of new regulation. Also, they strive to tackle the extra costs and workload that resulted after the delegation of governmental responsibilities by the national government. Microsoft Azure Cloud services provided possibilities for them to merge their existing IT infrastructures into a sole architecture.

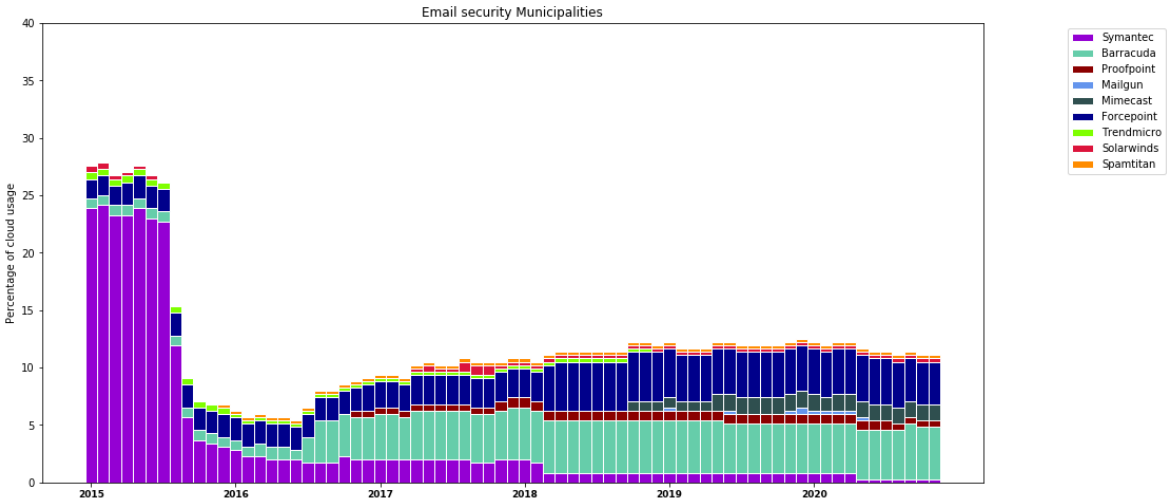
Figure 6.1: Email hosting use among municipalities



We have also tried to detect the use of email security services among municipalities. The results have been depicted in Figure 6.2. The measurements revealed that certain email security providers have been employed over the years: Symantec, Barracuda, Proofpoint, Mailgun, Mimecast, Forcepoint, Trendmicro, Solarwinds and Spamtitan. A first remarkable characteristic is the quite high use of Semantic security with 25% in 2015, which decreases rather significantly in 2016 and ends up to be almost non-existent. The drastic decrease in deployment of Semantic may be explainable by the enormous data leaks in 2015 that compromised millions of data in the Netherlands (Radar, 2018). It did not end with data breaches only, Symantec also revealed that Utrecht had the most DDOS attacks in 2017. The list with DDOS attacks also included Amsterdam and The Hague (Verburg, 2017). This could potentially explain a consequential decision of municipalities suspend the use of Semantic services. We also notice a significant use of Barracuda and Forcepoint, that starts with a low percentage but slowly increases to about 5%. Earlier in 2015, we saw the municipalities of Giessenlanden, Leerdam and Zederik opting for Barracuda firewalls (Infosecurity Magazine, 2019). Also, the municipality of Drechtsteden moved to email security services of Forcepoint (Motiv, 2019). They use Forcepoint email and web filtering services. Other than this, we see a constant use of spamtitan, solarwinds, trendmicro, proofpoint and mimecast, albeit in a superfluous quantity.

A crucial point that can be derived is that email hosting seems to increase over the years almost hitting 25% by the end of 2020, while email security use seems to start at 27% and decreases significantly to come to balance at around 13%.

Figure 6.2: Email security use among municipalities



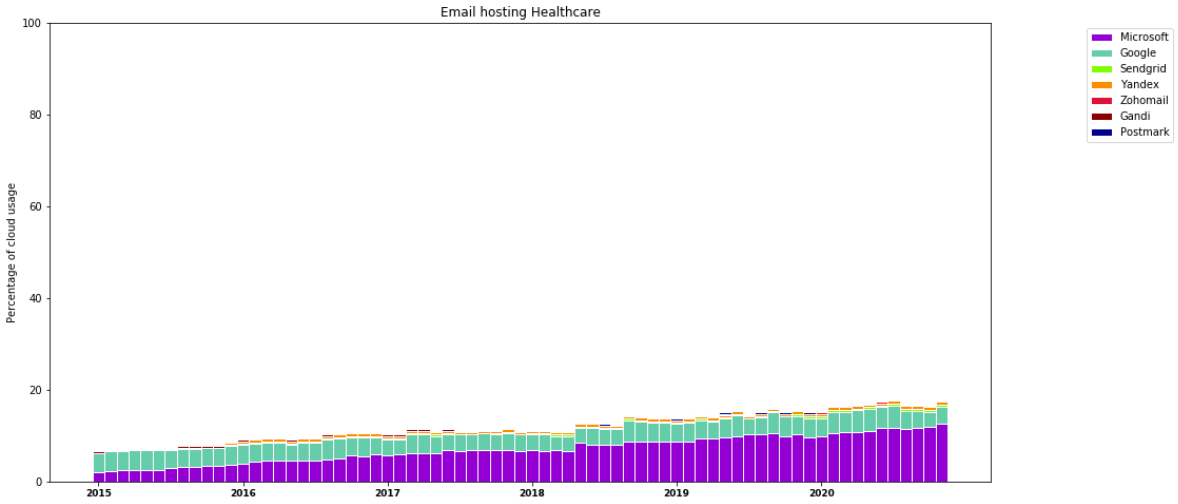
6.2.2. Prevalence of cloud-based email services in healthcare

We measured the prevalence of email hosting in hospitals and presented the results in Figure 6.3. The most common providers are Microsoft and Google, as expected since they are dominant cloud service providers. The pattern can also be traced back from the observations of cloud-based email hosting in the executive governments sector. However, we observe a slight difference in the results. At the beginning of 2015, both Microsoft and Google are present, with a share of respectively 2% and 4% just as we saw in the case of municipalities. Whereas the employment of Microsoft services grows over time up till 11% by the end of 2020, we spot a consistent use of Google over time of about 4%. We assume that this might be the same hospitals using Google email service, however, this does not have to hold. Google offers the Google Cloud for Healthcare to enable better care of patients and encourages collaboration between healthcare professionals using Google Workspace (Devoteam G Cloud, 2021). The increase in the use of Microsoft services might be explained by the novel cloud platforms offered by Microsoft such as the Microsoft Cloud for Healthcare. This platform enables healthcare organizations to scale the management of healthcare data, supports engagement with patients and enhances collaboration between healthcare teams (Microsoft, 2021). Furthermore, Microsoft continuously aims to ease healthcare integration. For example, Microsoft customers and its partners introduced an initiative to bring healthcare to home, so that patients can manage their conditions from their homes via their platforms (Fischer, 2020). We also see a negligible detection of Sendgrid, Zohomail, Postmark, Yandex and Gandi.

Another noteworthy aspect is that move towards employment of cloud-based email services is slower than we have seen in the case of municipalities, but albeit, the move seems more stable. In general, we discover that 6% of hospitals of European hospitals used cloud-based email services in 2015 and this percentage increases up to 18% in 2020.

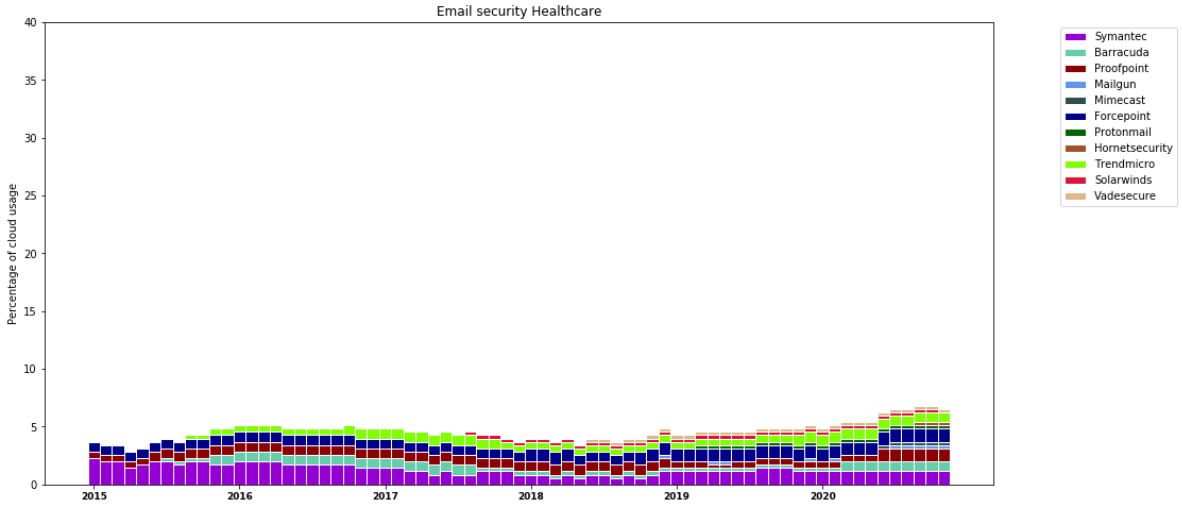
If we look at the use of email security services in healthcare in Figure 6.4, we see the appearance of Symantec, Barracuda, Proofpoint, Mailgun, Mimecast, Forcepoint, Protonmail, Hornetsecurity, Trendmicro, Solarwinds and Vadesecure. Something that immediately strikes is the low percentage of cloud-based email security services in general. By the end of 2020, the extreme can be found with a total use of 6.5%. We notice a slightly dominant presence of Symantec, Barracuda, Proofpoint, Forcepoint and Trendmicro, however, this seems more like a consistent pattern over the years. The observed lack in the use of email security services could possibly be explained by the fact that dominant email

Figure 6.3: Email hosting in healthcare



hosting providers such as Microsoft offer an entire cloud platform that allows for management of the whole system from one single infrastructure.

Figure 6.4: Email security use in healthcare



6.2.3. Prevalence of cloud-based email services in SME's

The results for the use of cloud-based email hosting in the SME's sector have been presented in Figure 6.5. As immediately can be reflected, a large percentage of cloud hosting can be observed among SME's with an initial percentage of 30 in 2015 and ending with 75% in 2020. This value is significantly higher than previous analyzed sectors. We note that a majority of the cloud-based email hosting occurs through Google and Microsoft. However, unlike the previous sectors, Google can be seen to be dominant over Microsoft. The use of Microsoft seems to begin with a low percentage of 3% and evolves gradually over the years up till 22%, which is in line with the use of Microsoft in executive governments. Google services on the other sides are being used by 26% of SME's in 2015 but increase to a use of 50% by the end of 2020, which is extremely high. The fact that more SME's have been opting for Google instead of Microsoft could be due to dominant behaviour of Microsoft. The European Digital SME Alliance has welcomed an initiative by German SME Nextcloud, who has filed a complaint on behalf of European SME's with the Directorate-General for Competition from the European Commission regarding anti-competitive exercises of Microsoft (Low, 2021). This behaviour of Microsoft led SME's

to be pushed aggressively towards signing and entrusting their data to Microsoft. Microsoft's bundling of OneDrive Cloud, Teams and other Windows services restricts customer's surface of choices and therefore makes it hard for SME's to opt for other services. Google on the other side has been actively investing in SME's across Europe in terms of finance and providing functionalities that enable SME's to enhance the growth of their business (Google, 2015).

Among the less significant occurrences, we spot several different providers Sendgrid, Strato, GoDaddy, Yandex, Rackspace, Amazon Workmail, Gandi and Postmark. The deployment of Strato seems more constant over the years compared to others.

Figure 6.5: Email hosting use among SME's

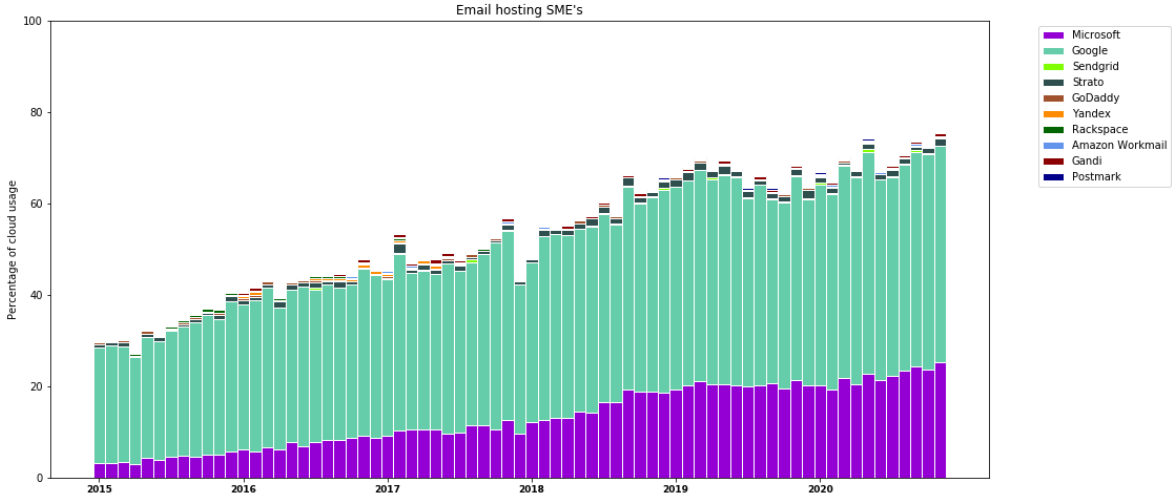
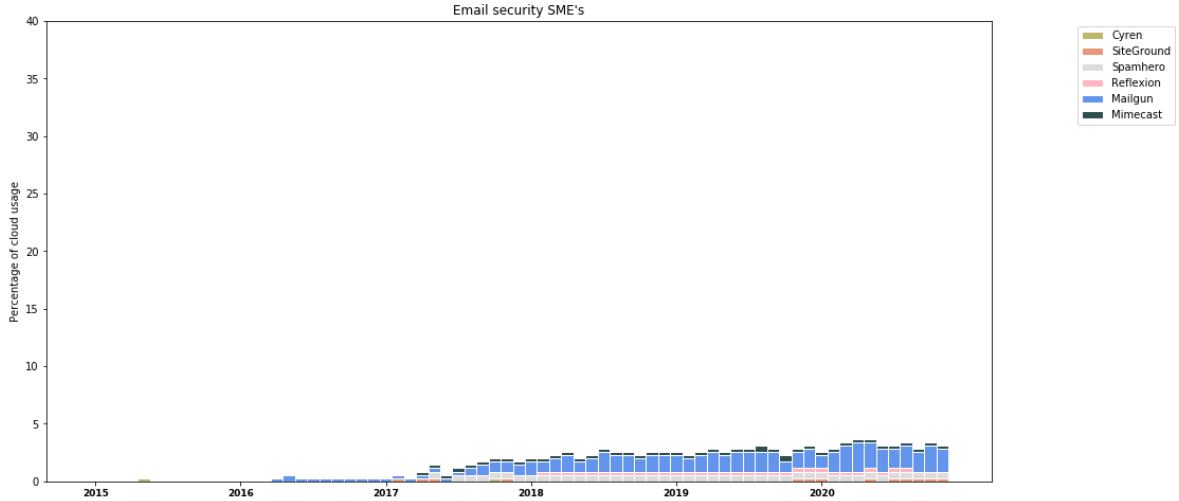


Figure 6.6 shows the use of cloud-based email security services among SME's. It becomes obvious that that most SME's have not been open to email security services, especially in 2015. However, we can see that the adoption of security services increases slightly over the years to a maximum of 4%. Within this, providers such as Cyren, Siteground, Spamhero, Reflexion, Mailgun and Mimecast have a share. Regardless, Mailgun and Spamhero have the largest ratio.

Figure 6.6: Email security use among SME's

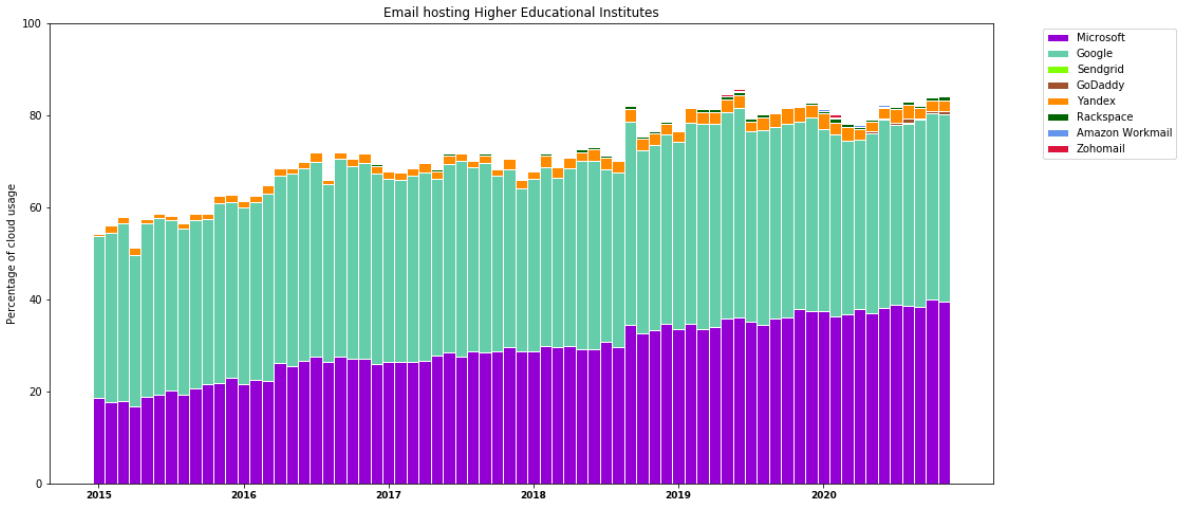


6.2.4. Prevalence of cloud-based email services in higher educational institutes

The findings for the adoption of cloud-based email hosting in universities have been presented in Figure 6.7. The results are resembling to the findings in the SME sector. Although, universities have been using email hosting in 2015 to a considerable large extent. The adoption pattern in 2015 points to a cloud implementation of 52% and progressively 82% approaching the end of 2020. Thus, so far we have seen the highest adoption rate of cloud-based email services. Similar to previous sectors, a domination of Microsoft and Google can be observed with Google being moderately more prevailing. Microsoft services have an adoption rate of 19% in 2015 and increasingly rises to 37% in 2020. Google services have been used by 33% of universities in 2015 and reach up to 41% around the end of 2020. While we have seen a preference for Microsoft services in universities in 2014 an on, for instance the University of Cantabria in Spain (Microsoft, 2014) and University of Lodz in Poland (University of Lodz, 2020), the use of Microsoft Office 365 has been banned from schools in Germany because of privacy concerns (European Digital Rights (EDRi), 2020). Despite this, we see a steadfast increase in the employment of Microsoft email services. The same holds for Google: the Dutch Personal Data Authority (AP) urges universities to stop using Google's email services as they are not compliant with the European privacy regulations (Fabrizi, 2021). However, with the current ongoing trend of adoption of email services, we do not expect this to take effect in the near future.

Apart from Microsoft and Google, we also find occurrences of Sendgrid, Zohomail, GoDaddy, Yandex, Rackspace and Amazon Workmail. The use of Yandex seems to be the most prominent among these, as the proportion increases somewhat over the time.

Figure 6.7: Email hosting use among higher educational institutes

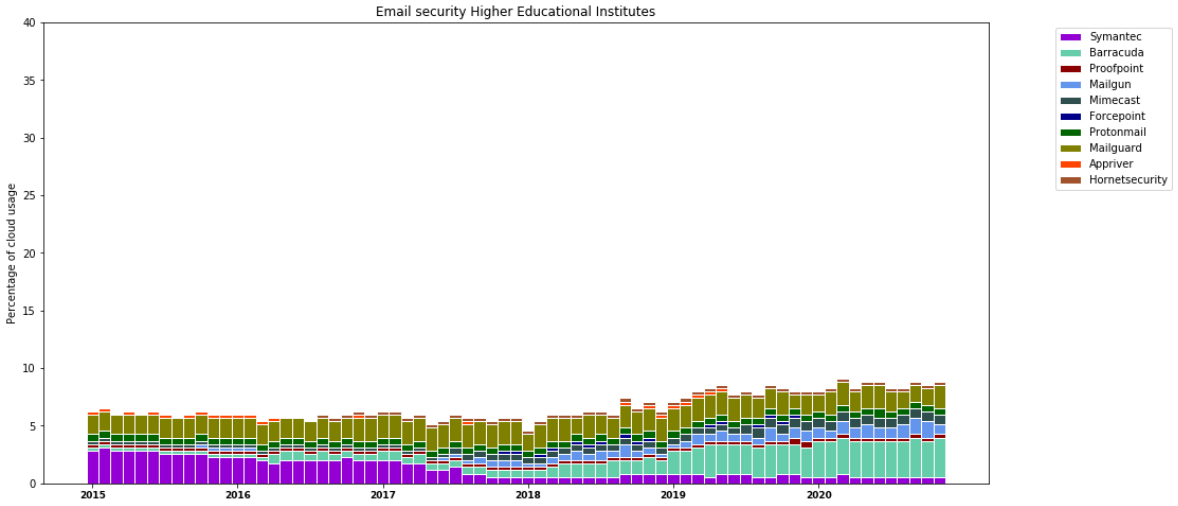


The visualization for the employment of email security services at universities has been depicted in Figure 6.8. It is immediately evident that not many investigated universities have been using cloud-based email security services. The total share of email security usage in 2015 is 6% and ends with 8.5% in 2020, which is extremely low compared to the extent of cloud-based email hosting as observed at universities. There is an appearance of the following email security providers: Symantec, Barracuda, Appriver, Mailguard, Proofpoint, Mailgun, Forcepoint, Mimecast, Protonmail and Hornetsecurity. However, the use of Symantec seems to be decreasing over the years, with an resemblance to the observations in the executive governments sector and in the healthcare sector. At the same time, Barracuda seems to be filling the developed gap. Furthermore, we notice a constant use of Mailguard.

6.2.5. Prevalence of cloud-based email services in large companies

The overview of email hosting in large companies is shown in Figure 6.9. A considerable upsurge in the level of email hosting can be seen which starts with 24% in 2015 and increases to 52%, which is quite a significant increase especially considering email hosting in previous sectors. Also, Microsoft and Google services are dominant players, similar to other sectors. Microsoft is clearly more superior

Figure 6.8: Email security use among higher educational institutes



as it starts off with an adoption rate of 12% in 2015 and advances towards 31% by the end of 2020. At the same time, we observe the adoption pattern of Google to be more constant over the years. It starts with a usage of 11% and gradually reaches 14% in 2020. We speculate that this could be the same enterprises that invested in Google services and remained committed to the provider. We also see the emergence of Sendgrid, Postmark, GoDaddy, Yandex, Rackspace and Amazon Workmail. Sendgrid seems to be more prevalent from 2019 and on.

Figure 6.9: Email hosting use among large companies

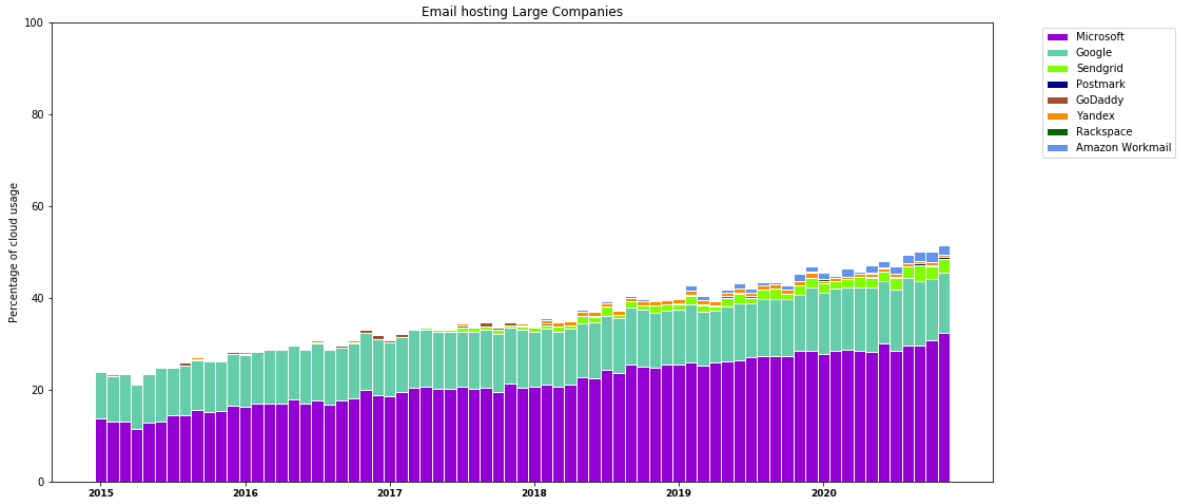
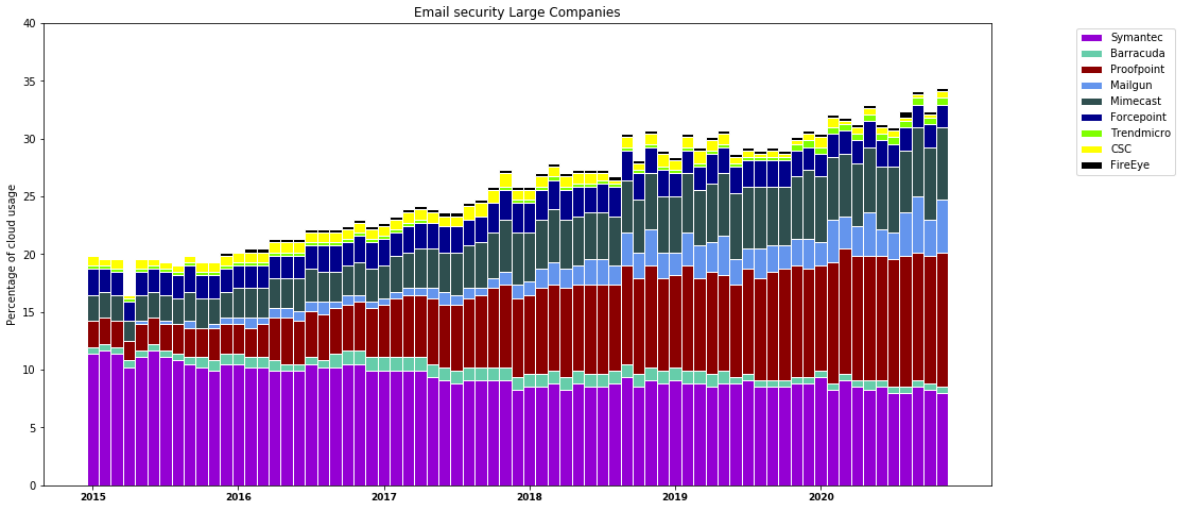


Figure 6.10 illustrates the use of email security over the past five years in the large companies sector. In comparison with previous sectors, we immediately see a different development as the extent to which large companies adopt email services is quite exceptional. Even in 2015, we can spot a total adoption rate of 19% which continues to increase and eventually becomes 34%. A strong prevalence of Symantec, Proofpoint and Mimecast can be observed over the years. However, the use of Semantic security seems to decrease over the years, with 11.5% employment in 2015 and 8% usage by the end of 2020. This phenomena is equivalent to the decrease of Semantic use in the executive governments, healthcare and higher educational institutes sector. On the other side, the use of Proofpoint services can be seen to increase over the years, with a 2% adoption rate in 2015 and a 10% rate in 2020. The use of Mimecast has been 2% in 2015 and increases a bit over time to 6% in 2020. Furthermore, among the less leading email security providers, we find Trendmicro, Barracuda, Mailgun, Forcepoint,

CSC and FireEye. It is interesting to note that unlike in other sectors, the use of Barracuda has been scant in this sector. Also, the use of Forcepoint is consistent over the years with 2% usage and Mailgun use increases in the beginning of 2018. In addition, we see the appearance of relatively unfamiliar providers such as CSC and FireEye.

A significant use of email security can so far be inferred compared to previous sectors. However, large companies such as the companies listed in the Fortune 500 had been found to be prone to phishing attacks in 2017 (Whittaker, 2017). This was due to the fact that they do not implement basic security features that intercept email spoofing. The research by cybersecurity firm Agari pointed to a poor use of DMARC email security. Furthermore, our finding that the use of Proofpoint has increased over the years is line with an article by Microsoft Cybersecurity firm that says that the use of Proofpoint has managed to gain a market share increase of 12% among top companies (Stocker, 2020).

Figure 6.10: Email security use among large companies



6.2.6. Prevalence of cloud-based email services in NGO's

We present the use of cloud-based email hosting in the NGO sector in Figure 6.11. In general, we perceive a relevant utilizing of email hosting over the years. The pattern we observe seems quite consistent as time passes with an adoption of 37% in 2015 and ending with 48% in 2020. However, there is an oscillation in the end of 2018 until the end of 2019. Among the occurrences, Microsoft and Google clearly have a major role confirming the patterns we saw in preceding sectors. One essential difference however is the extremely ruling position of Google in relation to Microsoft. The adopted email hosting level of Microsoft is 3% in 2015 and slowly magnifies to 10% by the end of 2020. This increase in use of Microsoft services could be explained by the improved availability of productivity solutions for non profit organizations such as NGO's (Microsoft, n.d.). Despite Microsoft's extensive effort to satisfy NGO's demands in terms of productivity software, we do not detect a movement of NGO's aligned with these efforts. Google on the other hand is present to an extent of 29% in the beginning of 2015 and stays somewhat constant over the time, but gradually reaches 34% by the end of 2020. Google also offers tools that encourage growth and efficiency of non-profit organizations, which is called 'Google Workspace for Nonprofits' (Google, n.d.). Among the trivial occurrences, we distinguish several providers: GoDaddy, Zohomail, Dreamhost, Yandex, Gandi, Strato and Rackspace. Within these, Yandex and GoDaddy have a leading position.

The results for the depiction of email security use within the NGO's sector have been presented in Figure 6.12. As instantly becomes clear, the use of email security in the NGO sector is below average. We can observe minor occurrences of email security providers Symantec, Cyren, SiteGround, Solarwinds, Proofpoint and Mailgun. The email security adoption starts at 0.6% in 2015 and ends with 1.4% in 2020. Compared to other sectors, this level of adoption is extremely deficient.

Figure 6.11: Email hosting use among NGO's

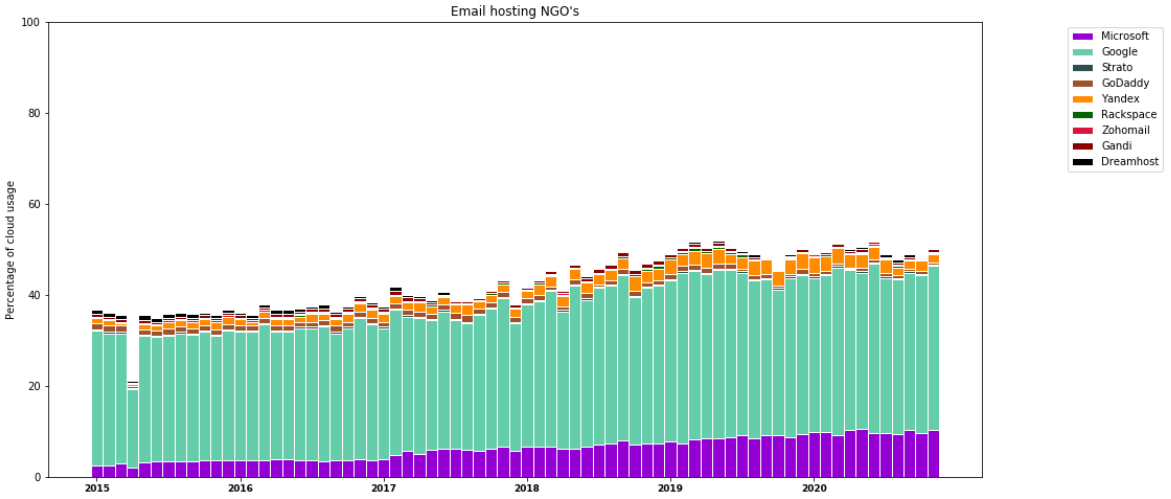
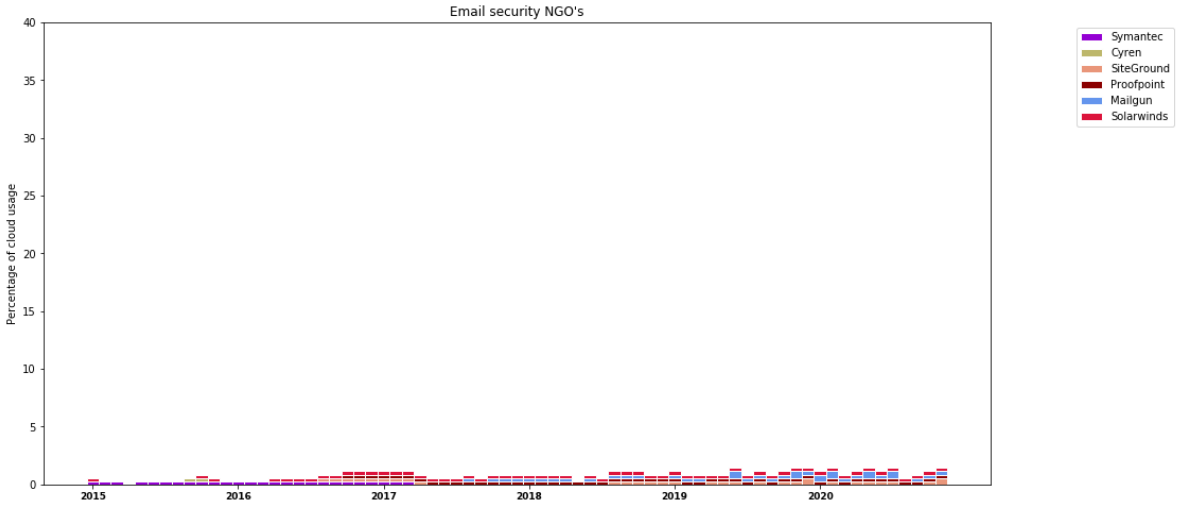


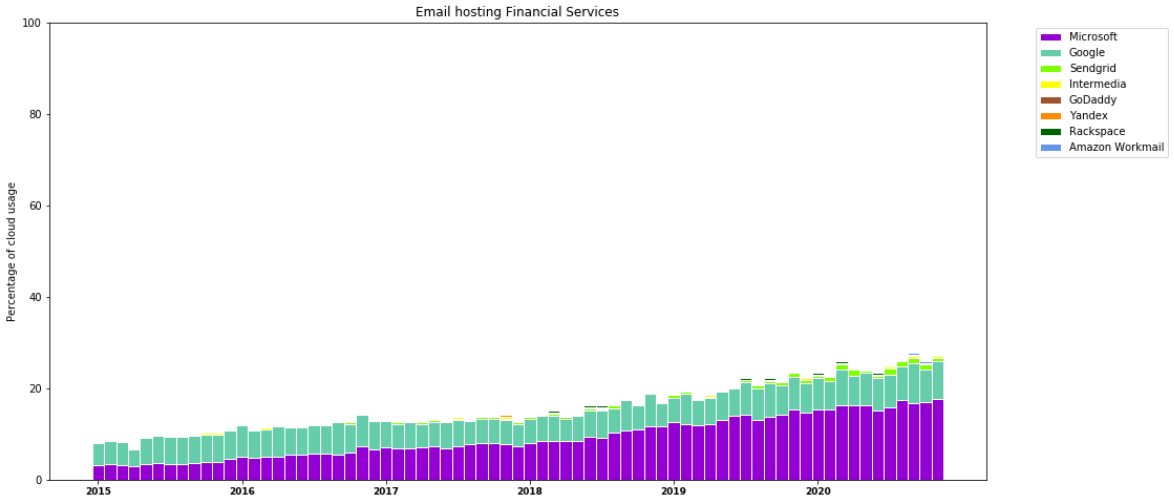
Figure 6.12: Email security use among NGO's



6.2.7. Prevalence of cloud-based email services in financial services

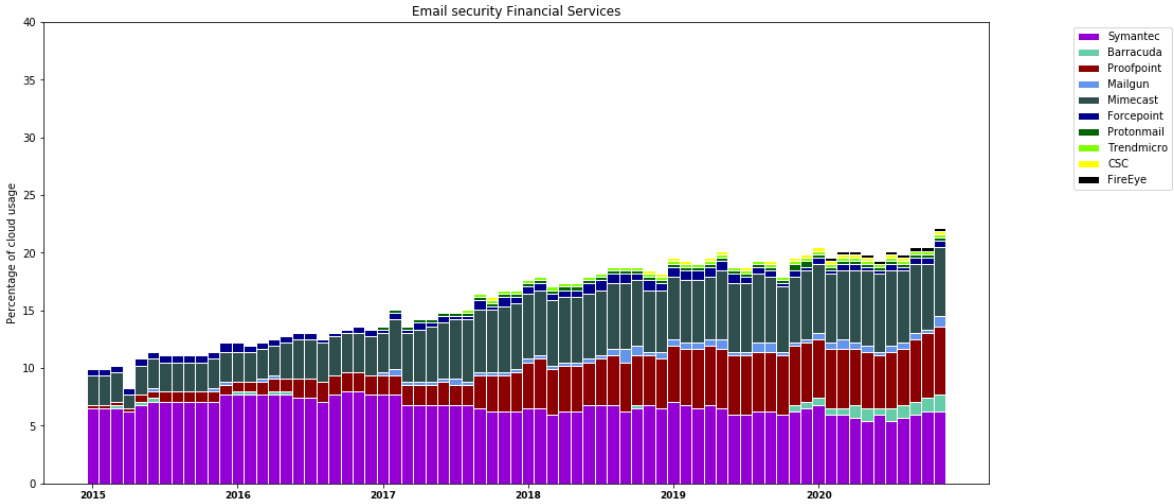
The results for the adoption of cloud-based email hosting in the financial services sector can be found in Figure 6.13. We spot a significant increase in the use of email hosting in this sector. Mainly prominent email hosting providers that are once again Microsoft and Google, with these findings being consistent with prior discussed sectors. Especially the rise in the usage of Microsoft services is remarkable over the years, while the use of Google services remains somewhat constant. We see a total email hosting adoption of 8% in 2015, only consisting of Microsoft and Google. In 2020, 28% percent of financial service organizations have been using cloud-based email hosting. This also includes several minor cloud market players such as Sendgrid, Intermedia, GoDaddy, Yandex, Rackspace and Amazon Workmail. Among these, we can observe Sendgrid to be the most prevalent from the beginning of 2019 and on. Microsoft has been by only 3% of financial service organizations in 2015. This movement increased rapidly to 17% usage by the end of 2020. Google however starts with a higher usage of 5% in 2015, yet increases only to 9% in 2020. This motion could be ascribed to the focus of Microsoft which has been partially on improving operations for financial services sector since 2015 (Tognela, 2015). They even collaborate with consulting companies Accenture and Avanade in order to optimize business and technology with a based upon Microsoft infrastructure. The main aim of this cooperation is to support financial services organization to understand their requirements and challenges.

Figure 6.13: Email hosting use in financial services



The email security employment in the financial services sector has been illustrated in Figure 6.14. A significant level of email security adoption can be identified which increases over the past five years. Altogether, 10% of the financial services had been using email security in 2015. This adoption rate snowballed to 23% by the end of 2020. We see some similarities with the adoption movement in the large companies sector, e.g. the dominance of cloud players such as Symantec, Proofpoint and Mimecast is clearly evident. Just like the case with large companies, the movement of Symantec seems to be somewhat constant over time, in contrast with email security in higher educational institutes, healthcare and executive governments, where it seems to decrease strongly. Semantic has been used by 6.5% of financial services organizations in the start of 2015 this use decreases somewhat to 6% nearing the end of 2020. Furthermore, Proofpoint has hardly been present in the start of 2015, but slowly appears and turns out to one of the most crucial providers as it has a share of 5% by the end of 2020. Mimecast has been used by 3% of financial organizations and this percentage increases to 5% in 2020. Less dominating email security providers are Barracuda, Trendmicro, Mailgun, Forcepoint, CSC, FireEye and Protonmail.

Figure 6.14: Email security use in financial services



7 Discussion

This chapter contains an analysis of found results in the context of framing the societal implications of the move to cloud-based email service adoption. These implications will act as input for managerial decision making in organizations belonging to crucial sectors. We will synthesize these perspectives using existing theories. Lastly, we will highlight limitations of the study.

7.1. Dominance of cloud service providers and its impact on the sovereignty of European data

In Chapter 6, we have discussed the findings of our data analysis. This resulted into insights about the prevalence of several cloud service providers in the sectors. In order to sketch an overview of the most dominant cloud service providers, we analyze the most relevant occurrences of the cloud service provider per sector. In Table 7.1 we present an overview containing the most major occurrences.

Email hosting provider	Executive government	Healthcare	SME's	Higher educational institutes	Large companies	NGO's	Financial services
Microsoft	X	X	X	X	X	X	X
Google		X	X	X	X	X	X
Yandex		X		X		X	
Strato			X				
Sendgrid					X		X

Table 7.1: Dominant email hosting providers per sector

Within this overview, we highlight the most dominant providers in dark blue as they are present in the majority of the sectors. We also mark sectors using a multitude of these email hosting providers in light blue. Microsoft, Google and Yandex are the most dominating email hosting providers in Healthcare, SME's sector, higher educational institutes, large companies and Financial services. In executive governments however, there is a stronger prominence of Microsoft. In the same way, we have analyzed the most major occurrences of email security providers and presented these findings in Table 7.2. We can note a strong prevalence of email security providers Symantec, Barracuda, Forcepoint and Mimecast in general since we have seen a significant use of these providers in multiple sectors. Executive governments, healthcare and large companies have been using many email security providers and have therefore been marked light blue.

Email security provider	Executive government	Healthcare	SME's	Higher educational institutes	Large companies	NGO's	Financial services
Symantec	X	X		X	X		X
Barracuda	X	X		X			
Forcepoint	X	X			X		
Proofpoint		X					X
Trendmicro		X					
Mailgun			X		X		
Mailguard				X			
Mimecast	X				X		X

Table 7.2: Dominant email security providers per sector

So far, we find a strong prevalence of already accepted cloud service providers such as Microsoft and Google with a maximum usage of 82%. Apart from this, we also notice prominence of several email security providers that dominate the market to a considerable extent with an upper bound of 40%. Thus, cloud service in the context of email is an actively ongoing advancement, albeit varieties can be observed in different sectors. This phenomena in which there is prominence of certain cloud players is referred to as centrality as described in Chapter 5.2.1. In all critical sectors, we have seen a strong increase in the use of cloud-based email hosting in the past five years. Similarly, in most sectors we have noticed a significant level of email security use over the years. While these cloud solutions may have countless benefits which enhance efficiency, growth and reduce costs (Rashid and Chaturvedi, 2019) for enterprises in these sectors, this trend seems to be moving forwards. Therefore, we expect an even enhanced movement in the years from 2021 and on. Especially, as Microsoft and Google have been focusing on the improvement of business operations such as email services, for specific customer groups like financial services or NGO's (Microsoft, n.d.; Google, n.d.; Tognela, 2015).

A dominated cloud market does not raise only economic concerns. When cloud giants especially not originating from Europe, manage to gain dominance over the cloud market, they consequently possess an extent of power. In 1890, the antitrust bill had been introduced to the US Senate by Senator John Sherman in concern of the rising power of private company Standard Oil and related trusts. In this bill (US Congress, 1890; Moore and Tambini, 2018), he described to power of private combinations to be parallel to "a kingly prerogative, inconsistent with our form of government". He further elaborated to other senators that "If we will not endure a king as a political power, we should not endure a king over the production, transportation and sale of any of the necessaries of life". This motivation of the senator reflects his fear of the power of dominating companies. This bill was introduced as a solution to tackle the back then "great evil" that was endangering to society. However, today we are not far away from this threat.

The significant level of cloud-based email adoption has shown that cloud service providers, particularly Microsoft and Google, are primarily in charge of managing email services for crucial firms. This position of dominant in sectors has not only granted them a "kingly" privilege, but also allowed them ownership of the complete and raw flow of data through their platform. More concretely, the production of data, transportation and sale thereof is actively placed in the hands of mainly Microsoft, Google and Yandex. In the seven cases, we observed a strong prominence of Microsoft and Google, with other providers mostly owning a minor share of the cloud market. Sherman argued that monopolists in an environment without competition, will always aim for the highest price possible that will not be conform the demand (US Congress, 1890). This economic concern could be allied with the position of Microsoft and Google, which could also mean this position might be abused as they may or may not hold high regard for the European demand.

After Sherman, Louis Brandeis also had criticism of large companies, however his criticism found its base in political and moral objections (Urofsky, 2009). Brandeis was of the opinion that size of a company is not a crime by itself, however size could become harmful because of the means by which

it has been gained and the way in which it is being utilized (Brandeis, 1914). This threat of emergent political power resulted into the introduction of legislation that aimed to challenge the combined power of the private organizations (Moore and Tambini, 2018). In the same way, Europe has introduced the European Competition Law in order to avert collaborations between dominant enterprises, to interfere when dominant positions are impending and grants power to prevent large companies from merging (Moore and Tambini, 2018). However, in reality the EU institutions are often left with no power to handle the dominance that aftereffects internal expansion of foreign enterprises; these enterprises do not abuse their dominant position in terms of increasing prices (Moore and Tambini, 2018).

Regardless, when European crucial sectors outsource their sensitive personal information retrieved from email services to the extent that we found in Chapter 6 and this adoption level only keeps increasing, cloud giants Microsoft, Google, Yandex, Symantec and other security providers will obtain an undemocratic powerful position. Especially, size of these companies becomes an important factor as it determines how their position has been maintained throughout the years. It could give these cloud companies a free pass to abuse their position to threaten European digital sovereignty. The German Federal Ministry for Economic Affairs and Energy defines digital sovereignty as the states' and its organizations' ability to be independently self-determined in terms of the employment and arrangement of digital systems, produced and stored data in these systems, and processes resulting from it (BMWi, 2019). However, as American cloud companies dominate European markets, it becomes a challenge to preserve the unique European DNA of values and human rights (Celeste, 2021). Therefore, it becomes hard for Europe to govern and control its data transferring through a space that surpasses physical boundaries.

Currently, Microsoft is working on The EU Data Boundary for the Microsoft Cloud plan (2021) that improves existing data processing in the cloud for Europe and enhance their existing commitments about data storage. While Microsoft affirms that it already complies to and exceeds existing EU regulation, this initiative aims to offer data processing and storing in the EU itself which can be configured by customers belonging to commercial and public sectors. Furthermore, they implement data encryption that meets regulatory objectives in rest and transit. They declare that many services enable control to be put in the hands of customers by the use of customer-managed keys for encryption. An interesting point to note is their focus on defending their consumers' data from inappropriate access by any government to provide added confidence to consumers regarding their data. To achieve this they assure consumers that (1) they are committing to oppose every request received from *any* government for commercial or public sector data, *where lawful basis gives space to do that* and (2) compensation will be offered to consumers if their data has been disclosed in answer to a government request that violates the GDPR (Brill, 2021).

We notice that their vision is strongly based on the compliance to the GDPR and thus incorporates principles of privacy by default as described in Chapter 4.2.1. However, we fail to see principles related to 'Collection Limitation' and 'Data Minimization' implemented in their data strategy. Thus, these principles only remain desirable. The current version of the GDPR can be subject to surveillance by governments. Furthermore, they aim to provide trust to consumers regarding any type of legal extraction, but do not exclude such situations in present day. While they try to restore public trust with the alternative to store data locally in Europe, it should still be noted that the personal data they process remains within their physical infrastructure and thus possibly accessible to Microsoft itself. The main concern still remains: the GDPR focuses at implementing informational principles relying on trust, out of which some can not be evaluated for compliance, where the actual risk of Microsoft's access to data is neglected.

Google Cloud on the other hand has a vision for digital sovereignty to guarantee privacy and security requirements of their customers in Europe specifically, that has a foundation on three main pillars: data sovereignty, operational sovereignty and software sovereignty (Kurian, 2020). Data sovereignty ensures that consumers can keep all control over access to data and encryption. This principle provides access to the provider for specific behaviors deemed necessary by the customer and allows for management and string of encryption keys outside the cloud environment and permits access to these based on descriptive justifications. Operational sovereignty includes having visibility and control over

provider operations. Software sovereignty provides the ability to run workloads without having to depend on the providers software.

Whereas we saw that Microsoft has been concentrating more on following the privacy and security fundamentals prescribed by the European regulation, Google does not necessarily put emphasis on following regulations. Rather, Google comes with a somewhat more detailed strategy that aims to provide control over technical processes in Google Cloud. For example, they allow customers to store encryption keys in a separate External Key Manager (EKM) that enables the user to manage the access to the keys using advanced cryptographic protocols. However, when data in the Google Cloud needs to be decrypted, the Google Cloud project needs to be granted access. Services like these however, put users in a situation on which they have to make a trade off between availability and privacy (Google Cloud, 2022). Furthermore, they encourage independence from the provider and data lock-ins by embracing open API's.

Thus, it comes down to the fact that especially policies of dominant cloud service providers are based on the principles of trust of the user in the cloud system. Where they can take some control into their own hands, such as in the case of encryption keys, they are placed in a difficult situation that either leaves them with a fast and reliable system and otherwise, a system that allows for completely encrypted data. Furthermore, protection from surveillance is not guaranteed, especially when the law is more powerful. One example is the overarching reach of the Cloud Act, that allows American authorities to request data stored on American and overseas grounds as well (Mevissen, 2018). Therefore, storing email data at Microsoft in Europe does not provide reassurance. Furthermore, none of these dominant providers integrate the principles: eliminating a single point of failure, data disclosure minimization and public scrutiny of protocols and software. Rather, their objectives seem based on the principle of privacy as a control, which strives to protect information collection, processing and dissemination as mentioned in Tabel 3.2.

A very crucial point to note is that no emphasis at all is placed on encouraging users to encrypt their email data using (advanced) cryptographic protocols prior to the process of information collection by the cloud platform. Both Microsoft and Google seem to be using encryption in rest and transit such as TLS and S/MIME. Also, in the findings in Chapter 6, we have seen that in all cases, Microsoft and Google have been dominant consistently over the years. This might have implications for companies that have been using Microsoft and Google, because new policies such as software sovereignty to restrict vendor lock-in problems have just been implemented. It might be hard for these firms to migrate their data or applications to another provider or bring it on-premise due to lacking technical standards. Also, relationships between Microsoft/Google and their consumers are mainly based on SLA agreements, for example the Google Cloud EKM SLA (Google Cloud, 2022). SLA's are mostly used represent the level of trust between the parties, however, the dominant position of these providers might not leave space for individual consumers to negotiate.

7.2. Societal implications for sectors moving to cloud solutions

In this section, we analyse the current threat landscape of the seven crucial sectors following the relevant foundations as presented in the threat landscape in Figure 5.2.

7.2.1. Executive governments

In Chapter 6.2.1, we have seen a quite significant move towards Microsoft services and that email security service use has decreased over time. Microsoft 365 and Government is a Microsoft edition specialized for governments (Microsoft, n. d.). However, due to the nature of this research, we can not determine whether executive governments in the Netherlands have been using this governments plan or not. The increasing move to Microsoft may be problematic in the future, because the government has a responsibility to protect data of citizens and data entrusted to the government by others. To achieve this they need to maintain the critical infrastructure and its availability to different sectors. Governments increasingly face security attacks that have impact on citizen data confidentiality, integrity and accessibility (Tweneboah-Kuoduah, Endicott-Popovsky and Tsetse, 2014). The governments may also not be interested in sharing citizen email data with third parties such as Microsoft as it may lead

to a loss of control. Especially, since this can have a negative impact on their services and reputation (Tweneboah-Koduah, Endicott-Popovsky and Tsetse, 2014).

Meanwhile, Microsoft does not guarantee freedom from legal extraction by US governments, this can pose severe risks to private email data maintained in the Microsoft cloud. Furthermore, if this trend of moving towards Microsoft in the executive governments section keeps moving forward, this can then indeed mean that European governments may be losing ownership over their crucial infrastructure and sensitive data to dominant foreign companies. The threat of surveillance might be the most integral, because Microsoft does not offer freedom from it. Especially, since European law and regulations do not acknowledge this risk. Also, we saw a significant share of Forcepoint use, this may provide higher email security levels. However, it does not save European governments from legal extraction regulations. Therefore, executive governments would need to re-evaluate their decision to move their email services to Microsoft cloud. However, as Microsoft and Google have been actively improving their cloud service for governments, they would need to minimize their data disclosure as this decreases the risk of surveillance. Furthermore, perspective of looking at a provider as a centralized trusted party needs to be eliminated. Trust should then be divided over multiple system components, such as Google is already implementing in their External Key Manager (EKM). The cloud system allows the user to manage the access to the keys using advanced cryptographic protocols in a separate cloud (Google Cloud, 2022).

7.2.2. Healthcare

In healthcare, we have seen a a quite slow but consistent move towards Microsoft and Google. This means that majority of the healthcare organizations have not been moving to cloud-based email services at all. However, in healthcare several threats can be identified; a research by Seh et al. (2020) revealed an increase in email and network server locations breach incidents from 2016 to 2019. Outdated security, database servers having no passwords and email accounts without (strong) passwords have been identified as the core reason for these breaches. While the adoption of Microsoft services has been quite slow in 2020, the level of cloud adoption has been increasing and will probably continuously grow in this manner. Especially since the launch of Microsoft's Cloud for Healthcare (Microsoft, 2021) this might be more appealing to organizations in the future compared to email security services. The attack space for healthcare firms more or less consists of outsider attacks that exploit security vulnerabilities for monetization of healthcare data for example. When healthcare organizations decide to opt for Microsoft services, they will have to delegate the security of their data to Microsoft. Furthermore, they will have to consider threat factors such as data loss and data migration issues (Zafar et al., 2014), holding for both Microsoft and Google. These risks can have disastrous consequences for patients and healthcare professionals as well, for example when patient health data is lost by the provider and no back up is present. Also, Google seems to be used by a certain group of organizations, that might be facing issues relating to migration and lock-in.

7.2.3. SME's

SME's are small to medium sized companies typically perceived as having relatively bounded resources and casual management style. Consequently, applicable practices theories for larger organizations may not hold for SME's. This means that security measures and infrastructure may be critical issues for SME's (Mijnhardt, Baars and Spruit, 2016; Osborn and Simpson, 2018) and therefore, security requirements need to be considered separately before adoption of cloud based email services. However, this may also be the cause of the heavy extent of email service adoption of Google and Microsoft as we have seen in Chapter 6.2.3. This huge dependency on Google and Microsoft could place SME's in a critical situation:

- In general, employees of SME's have little knowledge and expertise about processes and procedures of Microsoft and Google. SME's can differ greatly in size and industry, meaning that they unquestionably possess a lot of varying type of email information relating to the industry field. We note that a lot of SME's are dependent on Microsoft and Google, which means that a lot of trust is put in them. We thus observe a lack of employee awareness regarding privacy and security of data at the side of SME's.
- Such organizations that rely heavily on Google and Microsoft cannot control the information stored

on the cloud servers (Alkhater, Wills and Walters, 2018) due to lack of knowledge. As SME's are usually smaller firms, this phenomena leads us to believe that at some point, they will have to compromise their privacy and security requirements in SLA's against these dominant cloud players. And migrating from these providers might turn out to be a challenging task, especially due to data lock-ins.

- Laws pertaining to protection of data and confidentiality are concerns. For instance, SME's need to meet legal requirements and integrate SLA's to ensure compliance with legal responsibilities (Asiaei and Rahim, 2019).

7.2.4. Higher Educational Institutes

Like in the SME's sector, we have seen a strong dependency on Microsoft and Google. Universities particularly considered the risk of transferring of sensitive data to a third party provider in 2015, which hosts in a remote datacenter. This results into the loss of control due to employing cloud based services and unknown data location (Matthew, 2015). However, this fear cannot be inferred from the extent of dependency on Microsoft and Google as we saw in Chapter 6.2.4. Universities are vigorously allowing Microsoft and Google to obtain their sensitive student data, such as student's records or accounts (Chandra and Borah, 2012). This actual scenario poses several threats to which universities should be vigilant.

The Microsoft vision is more or less an implementation based on European privacy laws such as GDPR. These laws do not focus on the untrusted cloud provider perspective as we have defined for this research. For example, the task of encrypting user data is still put on the shoulders of Microsoft (Microsoft, 2021). Promises are made that governments will not be able to reach data. Furthermore, they implement data processing with consent only and claim no data mining will take place as per contractual agreements. Even though this is in line with the prescriptions of the GDPR, this still means that most involved students and staff might not read the complicated privacy agreements. Also, even if they manage to read these agreements, they have to face a situation in which they have to choose between maintaining their privacy and having access to their student work/academic work. Furthermore, the GDPR's vague terminology allows for profiling, which also needs to be considered by universities in Europe. Also, an increase in the use of smaller security providers, such as Mailguard and Barracuda has been noticed. These providers aim to follow the concepts of GDPR, however, extensive privacy policies to protect data from the provider itself or other adversaries are absent.

7.2.5. Large companies

In the large companies sector, we have also noticed a significant advancement towards Microsoft, Google, Sendgrid, Symantec, Proofpoint and Mimecast. Seeing the extent of email security adoption, we speculate that large companies care and are seemingly are more heedful of their email data security. Also, existing literature points towards this threat along with other existing threats. Compared to SME'S, the security concern is much greater for larger organizations then for SME's. Such concerns are for example, the environment with shared resources or management of identity (Alkhater, Walters and Wills, 2018). While we observe that large companies do value the security of their data to an high extent, they seem not be careful with the use of dominant email hosting services such as Google or Microsoft. They seem to be trusting these service providers with their data, not careful of how services like Microsoft may be impacted by legal extractions or how hosting data at a universal provider may make it potentially easier for attackers to reach, as providers as Sendgrid, Microsoft or Google may not offer extensive email security features that companies like Proofpoint may offer. For example, Google and Microsoft use plain TLS for email in transit, instead of STARTTLS or an added security feature for authentication such as DANE.

Furthermore, large enterprises worry about the exposure of their private information to third parties without them granting permission for it. This flows into the critical point that they may not be aware of the location where their data resides. Also, large sized organizations typically have more users and stakeholders and thus, their reputation is of utmost importance (Alkhater, Walters and Wills, 2018). This is an especially crucial point to notice, because of the extent of email hosting and email security hosting we have seen. Whereas larger providers like Google and Microsoft actively improve their

privacy strategies, smaller security firms such as Proofpoint do not seem to be following that move. Also, sometimes when add on security features of firms like Proofpoint is used on top of major cloud providers as Google and Microsoft, new concerns come up. For example, in a phishing attack in 2021, hackers posed as Proofpoint to get access to users' Microsoft and Google email passwords (Din, 2021). Such attacks may have disastrous consequences for security of large companies' data and therefore damage their reputation. And even though SLA's aim to guarantee quality service, the reputation of large companies may suffer greatly in case of a data breach or data loss (Khan and Malluhi, 2010).

7.2.6. NGO's

NGO's have also been using Microsoft, Google and Yandex to a large extent. In general NGO's are mainly concerned about the integrity and confidentiality of their organizations' data. More precisely, entrusting private company data to a provider for security and storage is challenging for them. NGO's want to be assured that their cloud service provider follows at least standard security practices which entail data disclosure and inspection (Rop, 2015). As Google and Microsoft both offer these standard security features, the pattern we saw in Chapter 6.2.6 can be explained. NGO's can possess diverse sensitive data regarding social/political issues and figures. A prior study by Nyakeya (2010) found that a lack of control and data ownership had been concerns.

It is essentially important for NGO's to consider hosting to providers with such a dominant position. Due to the nature of the sensitive data possessed by NGO's, they have to consider moving their email operations to providers from American origin or Russian origin in the case of Yandex. Hosting with these companies is mainly established on the basis of trusting these cloud service providers, as we discovered earlier. For example, when European NGO's possess actual information regarding a very sensitive topic such as the ongoing war between Russia and Ukraine in mutual email conversations in February 2022 (Kirby, 2022), this will then typically be hosted in Google, Microsoft or Yandex. This brings complications for privacy of this data. Especially as US legal extraction allows goverments to retrieve data in such situations. Also, a more devastating risk could be posed when the Russian government requests such information from Yandex. A lack of expertise in managing IT operations (Techsoup, 2012) further intensifies the danger. This means that it would be hard for NGO's to leave cloud hosting. Also, when they would want to leave they can face severe migration challenges. Therefore, if NGO's would want to keep moving this way, a sensible first step would be to follow principles regarding minimization of data disclosure and for example take encryption procedures in their own hands before information collection by the provider as these providers should not be trusted.

7.2.7. Financial Services

In the financial services sector, we have seen a somewhat balanced pattern in adoption of email hosting and email security services. However, Microsoft, Google, Symantec, Proofpoint and Mimecast are the major cloud service providers. These findings are in line with concerns found by Masons (2016), who also notes the reluctance of banks to switch to cloud services due to data breach reporting. The found increase of email security services stems from security issues. For example, 60% of financial services respondents have encountered an increase in phishing attacks with malicious attachments and 42% of the respondents have faced spoofing in 2021 (Mimecast, 2021). In these spoofing attacks, a financial organization's website is often replicated, and contains fake log in portals. Especially emerging institutes who are trying to build a reliable brand, are facing security related challenges. These security violations have resulted into reputation damage and business disruption for 89% of financial service organizations. At the moment, the challenge after adoption of cloud based email services is the in place setting of additional security software (Mimecast, 2021). Therefore, the susceptible nature of this sector requires additional security services. While many financial service organizations have been implementing security providers such as Mimecast, Barracuda and Proofpoint, they do not seem to consider the risk as a consequence of employing dominant cloud service providers.

Financial services organizations often possess sensitive financial data belonging to individuals. However, public or political figures involved in corruption cases in Europe use these financial services, and their data moves to providers like Microsoft, Google and Proofpoint, who are subject to legal extraction by US governments. Even though, these service providers promise top-notch security features, data access management for customers and separate storing of encryption keys for example,

there is still no guarantee that unauthorised individuals cannot access the information. Also, in most cases users have to grant access to their data if they want to use certain services, which if they do not use, may limit their enterprise efficiency. Furthermore, Microsoft and Google mainly use standard security for email in transit and rest, such as TLS and S/MIME. The security may still be vulnerable to attacks as the attack vectors continuously shift with novel technology. See for example, the hack of the European Banking Authority with Microsoft that compromised employee's email data in 2021 (BBC). To avoid such threat scenario's, financial service organizations would have to adopt their own encryption procedures to limit surveillance risks and other attacks due to political motives and financial gains.

7.3. Responsibilities for decision-makers

The societal implications of a centralized cloud-market have produced several responsibilities for on European governmental level as well as for decision-makers within the crucial sectors. These responsibilities form a gap for which it is essential to be filled to counteract new powers given dominant cloud players.

7.3.1. European Commission

The aim of the European governing body should be to prioritize the European digital sovereignty by preservation of European DNA of rights and values (Celeste, 2021). The concept of sovereignty in this entails that a state has the power over its territory and guarantees independence from external parties. We have discussed various risks and challenges that hinder the preservation of European rights and values. Especially, as the focus of the European Commission had been mostly on encouraging a data-driven economy in the preceding years with the introduction of the GDPR in 2018. Thus, so far we have seen many situations in which European data can still be compromised, even when dominant cloud service providers are following all prescribed procedures to ensure data privacy and security. In order to grant European sectors and citizens the right of freedom from surveillance from foreign governments and to gain control over the process of free data flow, the European Commission would have to change its perspective on digital governance. In the current prospect, we have seen a critical dependency on foreign infrastructure. Initiatives to store data within Europe should be imposed, such as Microsoft already implemented. In addition, the European Commission should take the responsibility of promoting European cloud service providers, which might help to regain control over their own infrastructure and data it carries. Furthermore, the European Commission should encourage a certain degree of sovereignty from foreign cloud service providers (Celeste, 2021), by enforcing PETs principles as mentioned in Table 3.3 in their law and regulations.

7.3.2. Decision-makers in sectors

In order to decrease the current dependency on dominant cloud service providers belonging from foreign countries, managers and high level decision-makers in organizations within the crucial sectors would need to implement change. Currently, sectors are diligently dependent on foreign infrastructures. We have noticed that many enterprises have been focusing on primarily security threats resulting from adversaries with monetary and political motives. However, the risk due to insider access by the cloud service provider, especially as a consequence of legal extraction by US governments has not or hardly been considered, especially in the SME's sector, higher educational institutes, large companies and NGO's.

This moves us to the point where (1) awareness has be raised regarding these privacy issues and (2) enterprises have to take partial responsibility in the light of data disclosure minimization. In the case of high dependency raising awareness within the enterprises includes training the (IT) personnel according to the required level of privacy such as the correct tuning of SLA's, management of encryption keys by the firms itself and having complete understanding of data locations. However, in order to decrease the level of dependency, training the enterprises own staff would enable the company to eventually turn to on-premise architecture, which would provide freedom from governmental surveillance. Furthermore, enterprises should take some part of the responsibility of their own data in their own hands by implementing security principles before data collection by the cloud service provider as we saw in Table 3.3. For example, encrypting their own emails using advanced cryptographic protocols would ensure that the cloud service provider cannot decrypt the information. Furthermore, this principle

will allow for data to be accessible to only intended recipients. However, this would require these firms to have awareness about this privacy and security risk.

7.4. Scientific relevance

A research by Celeste (2021) analysed question of the boundaries of digital sovereignty in Europe. In the context of the dominating effect of foreign cloud service providers they have found two relevant findings. Firstly, they find that the unbounded sovereignty between different states, such as Europe and the US, can create pressure and eventually increase the chance of dominant cloud players which control certain parts of the digital infrastructure. This is in accordance with the findings in this research. However, they also found that when excessive pressure is put on alignment of data and infrastructures in compliance with territorial jurisdictions, this could lead to a sense of being isolated and protectionism. However, we argue that seeing the threat landscape resulting from this study, we certainly see a necessity to protect European data from foreign surveillance performed by governments and intelligence agencies.

Barwise and Watkins (2018) found dominant tech giants such as Apple, Google, Microsoft, Amazon and Facebook, to hold a significant level of control over digital markets. This leads to high dependency for consumers. However, these dominant players are found to use this market power by implementing a monetizing business model in which they charge users and advertisers, which ultimately lead to steady supernatural growth. Reflecting back to Sherman's imperative of the "kingly" privilege and Brandeis' threat of size, we notice that these companies have managed to grow the size of their platform in a manner, namely by using their power and position, to an extent that it has become harmful to European society. This power has mainly been achieved by the competitive variety and flexibility of their products along with their monetizing business model. Due to the highly innovative range of services, consumers have been locked into using Microsoft and Google for example. This phenomena granted these providers a "kingly" advantage, in which they have ownership and control over any data that flows through them. Furthermore, this permitted Microsoft and Google to monetize their business models in which they can ask peak prices to further improve their position, without considering threats concerning censorship for example.

van Dijck (2020) investigated the governance of public values in data-driven digital societies. They concluded that US based infrastructures in ecosystems mainly take commercial values with higher regard than public values. Therefore, if Europe wants to secure their public values, they would have to understand the concrete underlying mechanisms of the American ecosystem before designing and adjusting their legal structures upon that. They found that Europe needs to recognize confines and opportunities of the networked digital infrastructures that span over borders and express their new position by virtue of the virtual superpowers. Similar to this research, they reason that governance of digital societies requires effort on levels varying from municipalities to governments and universities. However, in this research we aim for the European regulatory bodies to recognise the risk of surveillance among others and adopt privacy perspectives that take this risk into account in their laws and regulation. This would shift the attitude of dominating powers like Microsoft and Google. Eventually, we should promote independence from these digital infrastructures, as van Dijck (2020) mentions that US based digital infrastructures are built upon the ideology of American privacy that supports commercial values over public values.

7.5. Limitations of the research

In this research, we only measured the use of cloud service providers that provide email hosting solutions and email security solutions. Thus, we did not include the use of cloud email providers as defined in Chapter 3.3.2 e.g. these services provide email addresses bound to the domain of the provider such as '@gmail.com' for Google. However, the fact that we did not include these services may entail that the approximated use of cloud-based email services may be moderately underestimated. For instance, small scale firms like NGO's and SME's may have a rather limited budget assigned for digital innovation, thus they may use free email service options. Furthermore, we investigated the use of strictly popular cloud service providers as mentioned in Table 6.1. Therefore, the use of cloud-based email services could also be underrated, as organizations could also use other less known cloud service providers.

Also, for the collection of organization domains for the analysis we included most crucial type of organizations. For example, for executive governments, we only collected domains for municipalities in the Netherlands. This could give a slightly biased view with respect to all executive governments organizations throughout Europe. Especially, since some counties' municipalities might be more advanced than others. Also, for healthcare, we decided to focus only on hospitals throughout Europe. Especially, since these hospitals might be the most crucial large scale organizations within these sectors that are in close contact with patients.

8

Conclusion

In this chapter, we will translate the concrete interpretations into conclusions. We will also provide recommendations for future research.

8.1. Concluding impression about the threat landscape of European sectors

Cloud-based email services have been a popular option for organizations who wish to outsource their on-premise email service systems. In particular, among European organizations this has been a trend for the past few years. This movement introduced a novel threat landscape for the European data sovereignty. Namely, the use of foreign cloud service providers by critical European sectors initiated new challenges in terms of essential public values such as privacy and security. In this study, we strive to analyze the prominence of cloud service providers among DNS records on the internet to structure implications it may bring for sensitive European data that has been hosted with these cloud service providers. Therefore, we will answer the following research question:

How does the future threat landscape look like for different sectors in Europe as they adopt cloud-based email services?

An indicative level of cloud-based email service adoption in sectors like executive governments, SME's, higher educational institutes, large companies, NGO's and financial services have shown an increasing level of prevalence of cloud service use. In healthcare, this level of cloud-based email service usage is present in less significant volume, albeit the use is constant and persistent. This threat measure elevated previous threat models we defined to analyze the threat scenario of the cloud-based mail ecosystem.

The analysis resulted into finding extremely dominant cloud hosters in Europe: Microsoft and Google. These two major cloud hosters entirely transformed the cloud market of Europe by the end of 2020. Among less dominant cloud providers, we found Yandex, Symantec, Barracuda, Forcepoint and Mimecast. Albeit being less dominant, the use of these services seems to have been growing and we expect them to take in an integral share in the upcoming cloud market of Europe if the situation is not transformed by intervention.

The threat landscape for these sectors has many facets: (1) the dominance of Microsoft and Google, (2) the manner in which this position is being maintained, (3) the obtained (digital) power as a result of 1 and 2, societal complications for European sectors due to weak regulatory focus. Microsoft and Google have managed to achieve a dominant position in the cloud market of the previous years by partially using monetizing business models, and partially by locking customers in using for example data lock-ins. Even though Sherman and Brandeis had warned against this power of private enterprises, Europe has landed itself in a situation where critical organizations such as hospitals, municipalities,

large companies and banking facilities heavily rely on American companies.

Not only does this entail that any data that enters the infrastructure encrypted or unencrypted falls under the ownership of Microsoft and Google, but also that European firms will have no control over who accesses it. American tech giants are subject to legal extraction under the American Cloud Act for example, that orders them to present certain email records in highly sensitive or political cases. Data collected by these cloud service providers is vulnerable to censorship performed by foreign intelligence agencies, as Microsoft and Google both cannot counteract these orders by governments presently. This rising threat can be extremely endangering to privacy of organizations and involved individuals residing in Europe. Even though cloud giants like Google and Microsoft continuously aim to provide better privacy and security protections, novel attack vectors still manage to compromise the security of these systems, often resulting in the infringement of privacy. For example, data kept in these infrastructures is subject to traffic analysis by adversaries or profiling which is allowed as per European privacy laws. Also, a lack of advanced security measures and protocols seem to further enhance the attack space. This concretely means that if Europe continues on this track, it will lose sovereignty over its data.

Regardless of many security and privacy threats, Europeans still actively opt for these cloud solutions. We identified two critical factors that are the reason behind this motion: (1) weak regulatory focus in Europe and (2) lack of awareness at management level in organizations. In order to improve the situation, Europe would have to restore the sovereignty over digital infrastructures. Currently, actual legislation in Europe is centred around the informational privacy perspective, that encourages trusting the cloud service provider and support data collection by platform. The focus of this legislation would have to move towards the constitutional perspective, that incorporates values centred around not trusting the cloud service provider and promotes encryption by the client itself and supports minimization of data disclosure principles. In order to reconstruct Europe's public values and individual rights, the European Commission should take a leading position in the delineation of a novel regulatory focus within the European socio-technical system. This concretely means that on the long term, Europe should work towards decreasing reliance on foreign cloud service providers. This can be implemented by promoting digital initiatives of European origin. Managers belonging from the crucial sectors should on the other hand implement measures that increase awareness among (IT) employees within the enterprises. For example, they should encourage performing email data encryption before the cloud platforms collects the data.

8.2. Recommendations for future research

This research brings various insights about the current level of cloud-based email adoption in sectors in Europe. However, these insights also bring new domains that still remain unknown and could potentially enhance this field of study.

1. the extent of dependency on foreign cloud service providers: further research should evaluate the extent of dependency on these cloud service providers, in terms of which services are mostly being used and opportunities to move all data from certain cloud service providers. This field could provide insights about the actual practicability of moving email services to European based cloud service providers.

2. the acceptance of relative new Europe based email services: in order to investigate whether the reliance on foreign cloud service can potentially be decreased in the future, European regulatory institutes would have to perform a qualitative acceptance assessment towards novel cloud service providers originating from Europe. This initiative could return data ownership and control over the European infrastructure. Also, this research could provide more insight about the openness of sectors and this could prove to be vital measure in determining the chances to migrate to new cloud service providers.

Bibliography

Aaron, G., & Rasmussen, R. (2010). Global phishing survey: Trends and domain name use in 2h2009. *Lexington, MA: Anti-Phishing Working Group (APWG)*.

Ablon, L. (2018). Data thieves. *The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*.

Acevedo, L. (2016). The advantages of email in business communication. *Demand Media*.

Adeyinka, O. (2008). Internet attack methods and internet security technology. *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, 77–82.

Afrika, R. (2018). Adoption of cloud computing services for sustainable development of commercial banks in uganda. *Global Journal of Computer Science and Technology*.

Agrawal, P., Kaur, S., Kaur, H., & Dhiman, A. (2012). Analysis and synthesis of an ant colony optimization technique for image edge detection. *2012 International Conference on Computing Sciences*, 127–131.

Aisch, G., Huang, J., & Kang, C. (2016). Dissecting the #PizzaGate Conspiracy Theories. https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html?mtrref=en.wikipedia.org&gwh=79802C125E6C25C7051D085E30B26FDF&gwt=pay&assetType=PAYWALL

Alge, W. (2012). Email in the cloud: The challenges and benefits. *Computer Fraud & Security*, *2012*(7), 10–12.

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*, *35*(1), 38–54.

Angel, S., & Setty, S. (2016). Unobservable communication over fully untrusted infrastructure. *In 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, 551–569.

Anwar, U., Umair, H. A., Sikander, A., & Abedin, Z. U. (2019). Government cloud adoption and architecture. *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 1–8.

Apwg, A. (2014). Global phishing survey: Trends and domain name use in 2h2014.".

Asiaei, A., & Rahim, N. Z. A. (2019). A multifaceted framework for adoption of cloud computing in malaysian smes. *Journal of Science and Technology Policy Management*.

Aydin, H. (2021). A study of cloud computing adoption in universities as a guideline to cloud migration. *SAGE Open*, *11*(3), 21582440211030280.

Barbaschow, A. (2016). Microsoft trumps Google in ANZ cloud email market: Gartner. https://www.zdnet.com/article/microsoft-trumps-google-in-anz-cloud-email-market-gartner/

Barwise, P., & Watkins, L. (2018). The evolution of digital dominance. *Digital dominance: the power of Google, Amazon, Facebook, and Apple*, 21–49.

Baudoin, C., Flynn, J., McDonald, J., Meegan, J., Salsburg, M., & Woodward, S. (2013). Public cloud service agreements: What to expect and what to negotiate. *Cloud Standards Customer Council*.

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of general psychology*, *1*(3), 311–320.

BBA, P. M. (2016). Banking on cloud a discussion paper by the bba and pinsent masons.

BBC News. (2021). European Banking Authority hit by Microsoft Exchange hack. https://www.bbc.com/news/technology-56321567

Beato, F., Kohlweiss, M., & Wouters, K. (2011). Scramble! your social network data. *International Symposium on Privacy Enhancing Technologies Symposium*, 211–225.

Bergemann, B. (2017). The consent paradox: Accounting for the prominent role of consent in data protection. *IFIP International Summer School on Privacy and Identity Management*, 111–131.

Bezemer, C.-P., & Zaidman, A. (2010). Multi-tenant saas applications: Maintenance dream or nightmare? *Proceedings of the joint ercim workshop on software evolution (evol) and international workshop on principles of software evolution (iwpse)*, 88–92.

Brill, J. (2021). New steps to defend your data. https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

Camp, L. J. (1999). Web security and privacy: An american perspective. *The Information Society*, *15*(4), 249–256.

Casalini, F., & González, J. L. (2019). Trade and cross-border data flows.

Cavoukian, A. et al. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, *5*, 12.

CBS News. (2016). The phishing email that hacked the account of John Podesta. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

Cecchinato, M. E., Sellen, A., Shokouhi, M., & Smyth, G. (2016). Finding Email in a Multi-Account, Multi-Device World. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2858036.2858473

Celeste, E. (2021). Digital sovereignty in the eu: Challenges and future perspectives. *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, 211–228.

Chandra, D. G., & Borah, M. D. (2012). Cost benefit analysis of cloud computing in education. *2012 International Conference on Computing, Communication and Applications*, 1–6.

Chhabra, G. S., & Bajwa, D. S. (2015). Review of e-mail system, security protocols and email forensics. *International Journal of Computer Science & Communication Networks*, *5*(3), 201–211.

Cidon, A., Gavish, L., Bleier, I., Korshun, N., Schweighauser, M., & Tsitkin, A. (2019). High precision detection of business email compromise. *28th USENIX Security Symposium (USENIX Security 19)*, 1291–1307.

Columbus, L. (2014). 83% Of Healthcare Organizations Are Using Cloud-Based Apps Today. https://www.forbes.com/sites/louiscolumbus/2014/07/17/83-of-healthcare-organizations-are-using-cloud-based-apps-today/?sh=54c3ebd3b729

Conley, C. (2014). Metadata: Piecing together a privacy solution. *Available at SSRN 2573962*.

Courage Snowden. (2014). https://edwardsnowden.com/

Creswell, J. (2022). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th). SAGE Publications, Inc.

Crocker, D., Hansen, T., & Kucherawy, M. (2011). Domainkeys identified mail (dkim) signatures. *ser. RFC6376*.

Dabbish, L. A., Kraut, R. E., Fussell, S., & Kiesler, S. (2005). Understanding email use: Predicting action on a message. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 691–700.

Daly, A. (2016). *Private power, online information flows and eu law: Mind the gap* (Vol. 15). Bloomsbury Publishing.

De overheid zit met haar hoofd in de cloud | iBestuur. (2019). https://ibestuur.nl/podium/de-overheid-zit-met-haar-hoofd-in-de-cloud

Deloitte Switzerland. (2021). Cloud adoption with Non Governmental Organisations NGOs and International Development Organisations: recommendations to succeed. https://www2.deloitte.com/ch/en/pages/public-sector/articles/cloud-adoption-with-non-governmental-organisations-ngos-and-international-development-organisations-recommendations-to-succeed.html

Devoteam G Cloud. (2021). Healthcare. https://gcloud.devoteam.com/industries/healthcare/

Dey, R. K., Roy, S., Bose, R., & Sarddar, D. (2021). Assessing commercial viability of migrating on-premise mailing infrastructure to cloud. *International Journal of Grid and Distributed Computing*, *14*(1), 1–10.

Diaz, C., Tene, O., & Gurses, S. (2013). Hero or villain: The data controller in privacy law and technologies. *Ohio St. LJ*, *74*, 923.

Diffie, W., & Landau, S. (2010). *Privacy on the line: The politics of wiretapping and encryption*. The MIT Press.

Din, A. (2021). Hackers Impersonate Proofpoint to Collect Microsoft Office 365 and Google Credentials. https://heimdalsecurity.com/blog/hackers-impersonate-proofpoint-to-collect-microsoft-office-365-and-google-credentials/

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316.

Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bursztein, E., Lidzborski, N., Thomas, K., Eranti, V., Bailey, M., & Halderman, J. A. (2015). Neither snow nor rain nor mitm... an empirical analysis of email delivery security. *Proceedings of the 2015 Internet Measurement Conference*, 27–39.

Europe | Ranking Web of Hospitals. (n.d.). https://hospitals.webometrics.info/es/ranking_europe
European Commission. (2000). *CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION* (tech. rep.).
European Commission. (2010). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Agenda for Europe. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%5C%3A52010DC0245R%5C%2801%5C%29
European Commission. (2018). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/
European Commission. (2021). SME definition. https://ec.europa.eu/growth/smes/sme-definition_en
European Digital Rights (EDRi). (2020). Microsoft Office 365 banned from German schools over privacy concerns. https://edri.org/our-work/microsoft-office-365-banned-from-german-schools-over-privacy-concerns/
European Youth Foundation. (n.d.). NGO - European Youth Foundation. https://fej.coe.int/WebForms/ONG/PublicONGsPage.aspx
Fabrizi, G. (2021). Regulator: 'Universities, ban Google'. https://ukrant.nl/regulator-universities-ban-google/?lang=en
Faniyi, F., & Bahsoon, R. (2015). A systematic review of service level management in the cloud. *ACM Computing Surveys (CSUR)*, *48*(3), 1–27.
Farsight Security, cyber security intelligence solutions. (n.d.). https://www.farsightsecurity.com/
FBI. (2020). Business Email Compromise. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise
Federal Ministry for Economic Affairs and Energy (BMWi). (2019). *Project Gaia-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem* (tech. rep.). https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4
Fiebig, T., Gürses, S., Gañán, C. H., Kotkamp, E., Kuipers, F., Lindorfer, M., Prisse, M., & Sari, T. (2021). Heads in the clouds: Measuring the implications of universities migrating to public clouds. *arXiv preprint arXiv:2104.09462*.
Financial Times. (2021). FT 1000: the fifth annual list of Europe's fastest-growing companies. https://www.ft.com/content/8b37a92b-15e6-4b9c-8427-315a8b5f4332
Fischer, M. (2020). How Microsoft customers and partners in Europe are bringing health care home. https://news.microsoft.com/transform/how-microsoft-customers-and-partners-in-europe-are-bringing-health-care-home/
Fitzgerald, K. J. (1995). Information security baselines. *Information Management & Computer Security*.
Franceschi-Bicchierai, L. (2015). Teen Hackers: A '5-Year-Old' Could Have Hacked into CIA Director's Emails. https://www.vice.com/en/article/8q84gx/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails
Freedom of the Press. (2020). How reporters' emails get got: Case studies in legal requests and hacking. https://freedom.press/training/blog/how-reporters-emails-get-got-case-studies-legal-request-hacking/
Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2017). Privacy in cloud computing environments: A survey and research challenges. *The Journal of Supercomputing*, *73*(6), 2763–2800.
Google. (n.d.). Google Workspace for Nonprofits: Collaboration Tools - Google for Nonprofits. https://www.google.com/nonprofits/offerings/workspace/
Google. (2015). Google is a growth engine for European business. https://europe.googleblog.com/2015/02/
Google Cloud. (2022). Cloud External Key Manager | Cloud KMS Documentation |. https://cloud.google.com/kms/docs/ekm
GREWAL, P. S. (2013). Optiver Australia Pty. Ltd. v. Tibra Trading Pty. Ltd. https://casetext.com/case/optiver-australia-pty-ltd-v-tibra-trading-pty-ltd
Gritzalis, D., Stergiopoulos, G., Vasilellis, E., & Anagnostopoulou, A. (2021). Readiness exercises: Are risk assessment methodologies ready for the cloud? *Advances in core computer science-based technologies* (pp. 109–128). Springer.
Gürses, S., & Diaz, C. (2013). Two tales of privacy in online social networks. *IEEE Security & Privacy*, *11*(3), 29–37.

Haq, M. (2015). A comparative analysis of qualitative and quantitative research methods and a justification for adopting mixed methods in social research.

Hariharan, N. K. (2021). Financial data security in cloud computing.

Hartholt, S. (2016). Gemeentelijke e-mail “gˆenant slecht” beveiligd. https://www.binnenlandsbestuur.nl/gemeentelijke-e-mail-genant-slecht-beveili-gd.9539030.lynkx

Hayhurst, C. (2021). What It Takes to Secure the Cloud. Technology Solutions That Drive Education. https://edtechmagazine.com/higher/article/2021/08/what-it-takes-secure-cloud

Healthaffairs. (2020). The Risks Of Moving Health Care Delivery To The Internet. https://www.healthaffairs.org/do/10.1377/forefront.20201202.453916/full/

Help Net Security. (2020). How does COVID-19 impact cloud adoption? https://www.helpnetsecurity.com/2020/06/08/covid-19-impact-cloud-adoption/

Hentschel, R., Leyh, C., & Petznick, A. (2018). Current cloud challenges in germany: The perspective of cloud service providers. *Journal of Cloud Computing*, *7*(1), 1–12.

Henze, M. (2018). *Accounting for privacy in the cloud computing landscape*. Shaker Verlag GmbH.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., & Wehrle, K. (2014). User-driven privacy enforcement for cloud-based services in the internet of things. *2014 International Conference on Future Internet of Things and Cloud*, 191–196.

Henze, M., Hiller, J., Hohlfeld, O., & Wehrle, K. (2016). Moving privacy-sensitive services from public clouds to decentralized private clouds. *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, 130–135.

Henze, M., Hummen, R., & Wehrle, K. (2013). The cloud needs cross-layer data handling annotations. *2013 IEEE Security and Privacy Workshops*, 18–22.

Henze, M., Sanford, M. P., & Hohlfeld, O. (2017). Veiled in clouds? assessing the prevalence of cloud computing in the email landscape. *2017 Network Traffic Measurement and Analysis Conference (TMA)*, 1–9.

Hildén, J. (2021). Mitigating the risk of us surveillance for public sector services in the cloud. *Internet policy review*, *10*(3), 1–24.

Hiller, J., Kimmerlin, M., Plauth, M., Heikkila, S., Klauck, S., Lindfors, V., Eberhardt, F., Bursztynowski, D., Santos, J. L., Hohlfeld, O., et al. (2018). Giving customers control over their data: Integrating a policy language into the cloud. *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 241–249.

HIMSS. (2019). 2019 HIMSS CYBERSECURITY SURVEY. https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks’ use of cloud services. *Computer law & security review*, *34*(1), 4–24.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The european union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98.

Idoga, P. E., Toycan, M., Nadiri, H., & Çelebi, E. (2019). Assessing factors militating against the acceptance and successful implementation of a cloud based health center from the healthcare professionals’ perspective: A survey of hospitals in benue state, northcentral nigeria. *BMC medical informatics and decision making*, *19*(1), 1–18.

Infosecurity Magazine. (2019). GLZ gemeenten kiezen voor Barracuda NG Firewalls. https://www.infosecuritymagazine.nl/artikelen/glz-gemeenten-kiezen-voor-barracuda-ng-firewalls

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud! privacy concerns for consumer cloud storage. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 1–20.

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3-4), 40–71.

ISO/IEC 27032:2012. (2012). https://www.iso.org/standard/44375.html

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Review*, *25*(3), 270–274.

Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). “we’re being tracked at all times”: Student perspectives of their privacy in relation to learning an-

alytics in higher education. *Journal of the Association for Information Science and Technology*, *71*(9), 1044–1059.
Karunagaran, S., Mathew, S. K., & Lehner, F. (2019). Differential cloud adoption: A comparative case study of large enterprises and smes in germany. *Information Systems Frontiers*, *21*(4), 861–875.
Kaspersky Lab. (2020). Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns. https://www.kaspersky.com/blog/understanding-security-of-the-cloud/
Khayer, A., Talukder, M. S., Bao, Y., & Hossain, M. N. (2020). Cloud computing adoption and its impact on smes' performance for cloud supported operations: A dual-stage analytical approach. *Technology in Society*, *60*, 101225.
Kirby, B. P. (2022). Why is Russia invading Ukraine and what does Putin want? https://www.bbc.com/news/world-europe-56720589
Kitterman, S. (2014). Sender policy framework (spf) for authorizing use of domains in email, version 1. *RFC7208*.
Koh, J. S., Bellovin, S. M., & Nieh, J. (2019). Why joanie can encrypt: Easy email encryption with easy key management. *Proceedings of the Fourteenth EuroSys Conference 2019*, 1–16.
Koops, B.-J. (2014). The trouble with european data protection law. *International data privacy law*, *4*(4), 250–261.
Körner, N. (2020). Institutionalized cloud clients.
Kucherawy, M., & Zwicky, E. (2015). Domain-based message authentication, reporting, and conformance (dmarc). *ser. RFC7489*.
Kumar, S. N., & Vajpayee, A. (2016). A survey on secure cloud: Security and privacy in cloud computing. *American Journal of Systems and Software*, *4*(1), 14–26.
Kurian, T. (2020). How Google Cloud is addressing the need for data sovereignty in Europe in 2020. https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-addressing-data-sovereignty-in-europe-2020
Kurtz, C., Wittner, F., Semmann, M., Schulz, W., & Böhmann, T. (2019). The unlikely siblings in the gdpr family: A techno-legal analysis of major platforms in the diffusion of personal data in service ecosystems. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
Lawne, R. (2020). US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM. https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups
Lee, H., Gireesh, A., van Rijswijk-Deij, R., Chung, T., et al. (2020). A longitudinal and comprehensive study of the {dane} ecosystem in email. *In 29th {USENIX} Security Symposium ({USENIX} Security 20)*.
Leong, L., Bala, R., Lowery, C., & Smith, D. (2017). Magic quadrant for cloud infrastructure as a service, worldwide. *Retrieved on November*, *24*, 2017.
LII / Legal Information Institute. (2018). 18 U.S. Code § 2701 - Unlawful access to stored communications. https://www.law.cornell.edu/uscode/text/18/2701
Limoncelli, T. A., Hogan, C. J., & Chalup, S. R. (2016). *The practice of system and network administration: Volume 1: Devops and other best practices for enterprise it* (Vol. 1). Addison-Wesley Professional.
Lindh, M., & Nolin, J. (2016). Information we collect: Surveillance and privacy in the implementation of google apps for education. *European Educational Research Journal*, *15*(6), 644–663.
Lokuge, S., & Sedera, D. (2017). Turning dust to gold: How to increase inimitability of enterprise system. *Proceedings of the 21st Pacific Asia Conference on Information Systems (PACIS 2017)*.
Low, F. (2021). European SMEs stand up to Microsoft, urging the EU to open antitrust investigation. https://www.digitalsme.eu/european-sme-stands-up-to-microsoft-urging-the-eu-to-open-antitrust-investigation/
Lundin, L. (2020). Head in the clouds: A quantitative study on cloud adoption in a industrial setting.
Lynskey, O. (2015). *The foundations of eu data protection law*. Oxford University Press.
Mandal, S., & Khan, D. A. (2020). A study of security threats in cloud: Passive impact of covid-19 pandemic. *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 837–842.
Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, *6*(2), 2053951719895805.

Marek, M. W., & Skrabut, S. (2017). Privacy in educational use of social media in the us. *International Journal on E-Learning*, *16*(3), 265–286.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—the business perspective. *Decision support systems*, *51*(1), 176–189.

Matthew, F. T. (2015). Cloud computing in education–a study of trends, challenges and an archetype for effective adoption in nigerian universities. *Information communication technology (ICT) integration to educational curricula: a new direction for Africa*, 296.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543.

Mell, P., & Grance, T. (2014). The nist definition of cloud computing, september 2011. *Accessed on May*.

Messaging, Malware and Mobile Anti-Abuse Working Group. (2016). *Introduction to Traffic Analysis* (tech. rep.).

Metheny, M. (2017). *Federal cloud computing: The definitive guide for cloud service providers*. Syngress.

Mevissen, C. (2018). The CLOUD Act and its consequences. https://www.ictrecht.nl/en/blog/the-cloud-act-and-its-consequences

Microsoft. (n.d.-a). Empowerments begin with trust. https://www.microsoft.com/en-ww/trust-center

Microsoft. (n.d.-b). Microsoft 365 Nonprofit | Microsoft 365. https://www.microsoft.com/en-us/microsoft-365/nonprofit

Microsoft. (2014). The University of Cantabria in Spain prepares students for the world of work with Microsoft Office 365. https://news.microsoft.com/europe/2014/02/11/the-university-of-cantabria-prepares-students-for-the-world-of-work-with-microsoft-office-365/

Microsoft. (2017a). *Microsoft Security Intelligence Report* (tech. rep. No. 22).

Microsoft. (2017b). Three Dutch cities build an alliance on the Microsoft cloud. https://customers.microsoft.com/fr-fr/story/duo

Microsoft. (2021). Cloud for Healthcare. https://www.microsoft.com/en-us/industry/health/microsoft-cloud-for-healthcare

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing sme information security maturity. *Journal of Computer Information Systems*, *56*(2), 106–115.

Mimecast. (2021a). Email Security in Finance. https://www.mimecast.com/resources/ebooks/email-security-in-finance/

Mimecast. (2021b). Email Security in Finance. https://www.mimecast.com/resources/ebooks/email-security-in-finance/

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2021). Contactgegevens Gemeenten | Overheid.nl. https://organisaties.overheid.nl/Gemeenten/

Mockapetris, P., & Dunlap, K. J. (1988). Development of the domain name system. *Symposium proceedings on Communications architectures and protocols*, 123–133.

Mohammed, M. T., Rohiem, A. E., El-moghazy, A., & Ghalwash, A. (2013). Chaotic encryption based pgp protocol. *International Journal of Computer Science and Telecommunications*, *4*(2).

Moore, M., & Tambini, D. (2018). *Digital dominance: The power of google, amazon, facebook, and apple*. Oxford University Press.

Motiv. (2019). Gemeente Drechtsteden. https://www.motiv.nl/case/gemeente-drechtsteden/

Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the gdpr. *Information & Communications Technology Law*, *28*(3), 261–274.

Müller, J., Brinkmann, M., Poddebniak, D., Böck, H., Schinzel, S., Somorovsky, J., & Schwenk, J. (2019). {“johnny}, you are {fired!”}–spoofing {openpgp} and {s/mime} signatures in emails. *28th USENIX Security Symposium (USENIX Security 19)*, 1011–1028.

Mungai, B. (2012). The relationship between business management training and small and medium-sized enterprises’ growth in kenya. *Unpublished PhD Thesis, Kenyatta University*.

Nanos, I., Manthou, V., & Androutsou, E. (2019). Cloud computing adoption decision in e-government. *Operational research in the digital era–ict challenges* (pp. 125–145). Springer.

Nationaal Cyber Security Centrum. (2019). National Cybersecurity Agenda. https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda

Newman, I., Benz, C. R., & Ridenour, C. S. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum*. SIU Press.

NGO Branch. (n.d.). United Nations Civil Society Participation – Advanced Search. https://esango.un.org/civilsociety/displayAdvancedSearch.do?method=search&sessionCheck=false

Nissenbaum, H. (2013). Privacy Enhancing Technologies Symposium 2013. https://petsymposium.org/2013/program.php

Nurse, J. R., Erola, A., Goldsmith, M., & Creese, S. (2015). Investigating the leakage of sensitive personal and organisational information in email headers. *Journal of Internet Services and Information Security*, *5*(1), 70–84.

Nyakeya, D. M. (2010). *Adoption of cloud computing by the ngo sector in kenya* (Doctoral dissertation).

Opara-Martins, J. (2017). *A decision framework to mitigate vendor lock-in risks in cloud (saas category) migration.* (Doctoral dissertation). Bournemouth University.

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing*, *5*(1), 1–18.

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue—a uk case study. *The Computer Journal*, *61*(4), 472–495.

Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? problem representations of risk in the general data protection regulation (gdpr). *Critical Policy Studies*, *15*(4), 486–503.

Palos-Sanchez, P. R. (2017). Drivers and barriers of the cloud computing in smes: The position of the european union. *Harvard Deusto Business Research*, *6*(2), 116–132.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government information quarterly*, *27*(3), 245–253.

Pasquier, T. F.-M., & Powles, J. E. (2015). Expressing and enforcing location requirements in the cloud using information flow control. *2015 IEEE International Conference on Cloud Engineering*, 410–415.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 44–52.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702.

Poddebniak, D., Ising, F., Böck, H., & Schinzel, S. (2021). Why {tls} is better without {starttls}: A security analysis of {starttls} in the email context. *30th USENIX Security Symposium (USENIX Security 21)*, 4365–4382.

QS World University Rankings 2022. (2021). https://www.topuniversities.com/university-rankings/world-university-rankings/2022

Radar. (2018). Recordaantal grote datalekken in 2015. https://radar.avrotros.nl/nieuws/item/recordaantal-grote-datalekken-in-2015/

Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: A brief review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421–426.

Research and Markets. (2021). ReCloud Security in Banking Market - Growth, Trends, and Forecast (2019 - 2024). https://www.businesswire.com/portal/site/home/

Rodotà, S. (2009). Data protection as a fundamental right. *Reinventing data protection?* (pp. 77–82). Springer.

Rop, T. K. (2015). *A framework for adoption of cloud computing in non-govermental orgarnization in nairobi-kenya* (Doctoral dissertation). University of Nairobi.

Rose, S., Nightingale, J., Garfinkel, S., & Chandramouli, R. (2019). Trustworthy email. https://doi.org/https://doi.org/10.6028/NIST.SP.800-177r1

Rosenquist, M. (2009). Prioritizing Information Security Risks with Threat Agent Risk Assessment. *Intel Information Technology*.

Rossi, A. (2018). How the snowden revelations saved the eu general data protection regulation. *The International Spectator*, *53*(4), 95–111.

Samonas, S., & Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Sanchez, J. (2017). Obama Backs Off Real NSA Reform. https://www.thedailybeast.com/obama-backs-off-real-nsa-reform

Satzger, B., Hummer, W., Inzinger, C., Leitner, P., & Dustdar, S. (2013). Winds of change: From vendor lock-in to the meta cloud. *IEEE internet computing*, *17*(1), 69–73.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133.

Sharma, M., & Sehrawat, R. (2020). A hybrid multi-criteria decision-making method for cloud adoption: Evidence from the healthcare sector. *Technology in Society*, *61*, 101258.

Shavell, R. (2021). It's time or NGOs and nonprofits to tighten their cybersecurity standards. https://philanthropynewsdigest.org/columns/the-sustainable-nonpro-fit/it-s-time-or-ngos-and-nonprofits-to-tighten-their-cybersecurity-standards

Shen, Y., & Pearson, S. (2011). Privacy enhancing technologies: A review. *Hewlet Packard Development Company. Disponible en https://bit. ly/3cfpAKz*.

Shimba, F. (2010). Cloud computing: Strategies for cloud computing adoption.

Shitole, H. P., & Divekar, S. (2019). Secure email software using e-smtp.

Smith, B. (2021). Answering Europe's Call: Storing and Processing EU Data in the EU. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. l. Rev.*, *154*, 477.

SpamTitan. (2019). Spear Phishing Attack Results in $16 Million Anthem Data Breach Settlement. https://www.spamtitan.com/blog/anthem-data-breach-settlement/

Srinivasan, M. (2011). Cloud-based email architecture for higher education institutions. *Issues in Information Systems*, *12*(1), 339–345.

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Steenhuisen, B. (2019). Complex Systems Engineering – revisited the struggle to design in a multi-actor setting. https://brightspace.tudelft.nl/d2l/le/content/195046/viewContent/1562029/View

Stocker, J. (2020). Fortune 500 Email Security Vendor Market share. https://thecloudtechnologist.com/2020/05/13/fortune-500-email-security-vendor-market-share/

Suresha, K., & Vijaya Karthick, P. (2020). Enhancing data security in cloud computing using threshold cryptography technique. *Advances in cybernetics, cognition, and machine learning for communication technologies* (pp. 231–242). Springer.

Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: A review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297–302.

Sweeney, L. (2000). Simple demographics often identify people uniquely. *Health (San Francisco)*, *671*(2000), 1–34.

Swire, P. (2012). From real-time intercepts to stored records: Why encryption drives the government to seek access to the cloud. *International Data Privacy Law*, *2*(4), 200–206.

Taddicken, M. (2013). 13 privacy, surveillance, and self-disclosure in the social web. *Internet and Surveillance: the challenges of Web 2.0 and social media*, *16*, 255–272.

Techsoup. (2012). *The Significance of Cloud Computing in the Social Benefit Sector: A Survey of 10,500 Nonprofits, Charities, and NGOs from 88 Countries on Barriers and Motivators in Cloud Computing.* (tech. rep.). https://www.techsoup.bg/sites/default/files/2012%5C%20Global%5C%20Cloud%5C%20Survey%5C%20Full%5C%20Report_2.pdf

Teddlie, C., & Tashakkori, A. (2012). Common "core" characteristics of mixed methods research: A review of critical issues and call for greater convergence. *American behavioral scientist*, *56*(6), 774–788.

Terfas, H. (2019). *The analysis of cloud computing service level agreement (sla) to support cloud service consumers with the sla creation process* (Doctoral dissertation). École de technologie supérieure.

Terfas, H., Suryn, W., Roy, J., & Eftekhar, S. M. (2018). Extending iso/iec 19086 cloud computing sla standards to support cloud service users with the sla negotiation process. *SQM XXVI*, *127*.

The Guardian. (2017). Deloitte hit by cyber-attack revealing clients' secret emails. https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

The New York Times. (2021). Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China. https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

The Washington Post. (2021). Trump Justice Dept. effort to learn source of leaks for Post stories came in Barr's final days as AG, court documents show. https://www.washingtonpost.com/national-security/washington-post-trump-reporter-emails/2021/07/13/27c1f04e-e41f-11eb-b722-89ea0dde7771_story.html

The Washington Times. (2008). Hacker wanted to 'derail' Palin. https://www.washingtontimes.com/news/2008/sep/19/hacker-wanted-to-derail-palin/

Tognela, A. (2015). In financial services data is the business. https://cloudblogs.microsoft.com/industry-blog/financial-services/2015/01/06/in-financial-services-data-is-the-business/

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human resource development review*, *4*(3), 356–367.

Trost, J. (2020). Mining DNS MX Records for Fun and Profit. http://www.covert.io/mining-mx-records-for-fun-and-profit/

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to government cloud adoption. *International Journal of Managing Information Technology*, *6*(3), 1–16.

University of Lodz. (2020). International Relations Office » Microsoft Office 365 at the University of Lodz – new email accounts for students. https://iso.uni.lodz.pl/microsoft-office-365-at-the-university-of-lodz-new-email-accounts-for-students/

Urofsky, M. (2009). Louis d. *Brandeis: A Life*.

US Congress. (1890). Our Documents - Sherman Anti-Trust Act (1890). https://www.ourdocuments.gov/doc.php?flash=false&doc=51

Value Today. (2022a). Europe Top Companies by market cap as on Sep 1st 2021. https://www.value.today/europe-top-companies?title=&field_company_category_primary_target_id=All&page=0

Value Today. (2022b). Europe Top Companies by market cap as on Sep 1st 2021. https://www.value.today/europe-top-companies?title=&field_company_category_primary_target_id=7412

Van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, *36*, 105377.

van Gelder, P. (2020). Lecture 1: Introduction to Cyber Space. https://brightspace.tudelft.nl/d2l/le/content/279937/viewContent/1730337/View

Velte, A. T., Velte, T. J., & Elsenpeter, R. C. (2011). *Cloud computing: Praktickỳ pr vodce*. Computer Press.

Verburg, M. (2017). Beveiligingsbedrijf Symantec: 'Geen verklaring voor grote aantal computerbesmettingen in Utrecht'. https://www.ad.nl/utrecht/beveiligingsbedrijf-symantec-geen-verklaring-voor-grote-aantal-computerbesmettingen-in-utrecht~a8187fc6/?referrer=https%3A%2F%2Fwww.google.com%2F

Voorsluys, W., Broberg, J., Buyya, R., et al. (2011). Introduction to cloud computing. *Cloud computing: Principles and paradigms*, 1–44.

Warnier, M., Dechesne, F., & Brazier, F. (2015). Design for the value of privacy. *Handbook of ethics, values, and technological design: sources, theory, values and application domains. Springer, Dordrecht*, 431–445.

Westin, A. F. (1967). Privacy and freedom atheneum. *New York*, *7*, 431–453.

Whittaker, Z. (2017). Most Fortune 500 companies aren't using this basic email security feature. https://www.zdnet.com/article/most-fortune-500-companies-arent-using-a-basic-email-security-feature/

WikiLeaks - Sony Archives. (2018). https://wikileaks.org/sony/emails/

Willett, M., & Solms, R. V. (2014). Cloud-based email adoption at higher education institutions in south africa. *Journal of International Technology and Information Management*, *23*(2), 2.

Wood, D. (2007). Gao-07-737 data breaches are frequent, but evidence of resulting identity theft is limited; however, the full extent is unknown. *Government Accountability Office*.

Xu, Q. (2018). Research on Security Construction of University Email System Based on Information Security Classified Protection. *Proceedings of the 2018 International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018)*. https://doi.org/10.2991/tlicsc-18.2018.51

Yvonne Feilzer, M. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of mixed methods research*, *4*(1), 6–16.

Zafar, Z., Islam, S., Aslam, M. S., & Sohaib, M. (2014). Cloud computing services for the healthcare industry. *Int J Multidiscip Sci Eng*, *5*, 25–29.

Zaki, T., Uddin, M. S., Hasan, M. M., & Islam, M. N. (2017). Security threats for big data: A study on enron e-mail dataset. *2017 international conference on research and innovation in information systems (icriis)*, 1–6.

Zardari, S., & Bahsoon, R. (2011). Cloud adoption: A goal-oriented requirements engineering approach. *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing*, 29–35.

Zdrnja, B., Brownlee, N., & Wessels, D. (2007). Passive monitoring of dns anomalies. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 129–139.

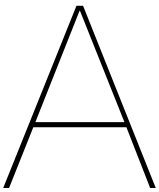
Zekrya, M. (2011). *Le cloud computing en Suisse: R´esultats de l'enquˆete aupr‘es des entreprises:* (tech. rep.). Haute Ecole de Gestion, Geneva.

Zhong, L., Mu, L., Li, J., Wang, J., Yin, Z., & Liu, D. (2020). Early prediction of the 2019 novel coronavirus outbreak in the mainland china based on simple mathematical model. *Ieee Access*, *8*, 51761–51769.

Zhou, T. G., Gosho, C., & Giyane, M. (2014). Cloud computing adoption and utilization amongst zimbabwean ngos: A case of gweru ngos.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack obama's books of 2019*. Profile books.

Zuiderveen Borgesius, F. (2015). Improving privacy protection in the area of behavioural targeting. *Available at SSRN 2654213*.



Appendix A: Overview of Municipalities

aaenhunze.nl.
aalsmeer.nl.
aalten.nl.
achtkarspelen.nl.
alblasserdam.nl.
albrandswaard.nl.
alkmaar.nl.
almelo.nl.
almere.nl.
alphenaandenrijn.nl.
alphen-chaam.nl.
gemeentealtena.nl.
ameland.nl.
amersfoort.nl.
amstelveen.nl.
amsterdam.nl.
apeldoorn.nl.
arnhem.nl.
assen.nl.
asten.nl.
baarle-nassau.nl.
baarn.nl.
barendrecht.nl.
barneveld.nl.
gemeentebeek.nl.
beekdaelen.nl.
beemster.net.
beesel.nl.
bergendal.nl.
bergeijk.nl.
bergen.nl.
bergen-nh.nl.
bergenopzoom.nl.
gemeenteberkelland.nl.
bernheze.org.
gemeentebest.nl.
beuningen.nl.
beverwijk.nl.
bladel.nl.
blaricum.nl.
bloemendaal.nl.
bodegraven-reeuwijk.nl.
boekel.nl.
borger-odoorn.nl.
borne.nl.
borsele.nl.
boxmeer.nl.
boxtel.nl.
breda.nl.
brielle.nl.
bronckhorst.nl.
brummen.nl.
brunssum.nl.
bunnik.nl.
bunschoten.nl.
buren.nl.
capelleaandenijssel.nl.
castricum.nl.
coevorden.nl.
cranendonck.nl.
cuijk.nl.
culemborg.nl.
dalfsen.nl.
dantumadiel.frl.
debilt.nl.
defryskemarren.nl.
derondevenen.nl.
dewolden.nl.
delft.nl.
denhaag.nl.
denhelder.nl.
deurne.nl.
deventer.nl.
diemen.nl.
dinkelland.nl.
doesburg.nl.
doetinchem.nl.
dongen.nl.
dordrecht.nl.
drechterland.nl.
drimmelen.nl.
dronten.nl.
druten.nl.
duiven.nl.
echt-susteren.nl.
edam-volendam.nl.
ede.nl.
eemnes.nl.
eemsdelta.nl.
eersel.nl.
eijsden-margraten.nl.
eindhoven.nl.
elburg.nl.
emmen.nl.
enkhuizen.nl.
enschede.nl.
epe.nl.
ermelo.nl.
etten-leur.nl.
geertruidenberg.nl.
geldrop-mierlo.nl.
gemert-bakel.nl.
gennep.nl.
gilzerijen.nl.
goeree-overflakkee.nl.
goes.nl.
goirle.nl.
gooisemeren.nl.
gorinchem.nl.
gouda.nl.
grave.nl.
gemeente.groningen.nl.
gulpen-wittem.nl.
haaksbergen.nl.
haarlem.nl.
haarlemmermeer.nl.
halderberge.nl.
hardenberg.nl.
harderwijk.nl.
hardinxveld-giessendam.nl.
harlingen.nl.
hattem.nl.
heemskerk.nl.
heemstede.nl.
heerde.nl.
heerenveen.nl.
heerhugowaard.nl.
heerlen.nl.
heeze-leende.nl.
heiloo.nl.
hellendoorn.nl.
hellevoetsluis.nl.
helmond.nl.
hendrik-ido-ambacht.nl.
hengelo.nl.
s-hertogenbosch.nl.
hethogeland.nl.
heumen.nl.
heusden.nl.
hillegom.nl.
hilvarenbeek.nl.
hilversum.nl.
gemeentehw.nl.
hofvantwente.nl.
hollandskroon.nl.
hoogeveen.nl.
hoorn.nl.
horstaandemaas.nl.
houten.nl.
huizen.nl.
gemeentehulst.nl.
ijsselstein.nl.
kaagenbraassem.nl.
kampen.nl.

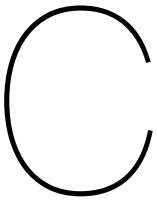
kapelle.nl.
katwijk.nl.
kerkrade.nl.
koggenland.nl.
krimpenaandenijssel.nl.
krimpenerwaard.nl.
laarbeek.nl.
landerd.nl.
landgraaf.nl.
landsmeer.nl.
gemeentelangedijk.nl.
lansingerland.nl.
laren.nl.
leeuwarden.nl.
leiden.nl.
leiderdorp.nl.
leidschendam-voorburg.nl.
lelystad.nl.
leudal.nl.
leusden.nl.
lingewaard.nl.
lisse.nl.
lochem.nl.
loonopzand.nl.
lopik.nl.
losser.nl.
maasdriel.nl.
gemeentemaasgouw.nl.
maassluis.nl.
gemeentemaastricht.nl.
medemblik.nl.
meerssen.nl.
meierijstad.nl.
meppel.nl.
middelburg.nl.
middendelfland.nl.
middendrenthe.nl.
midden-groningen.nl.
gemeente-mill.nl.
moerdijk.nl.
molenlanden.nl.
montferland.info.
montfoort.nl.
mookenmiddelaar.nl.
nederbetuwe.nl.
nederweert.nl.
nieuwegein.nl.
nieuwkoop.nl.
nijkerk.eu.
nijmegen.nl.
nissewaard.nl.
noardeast-fryslan.nl.
noord-beveland.nl.
gemeentenoordenveld.nl.
noordoostpolder.nl.
noordwijk.nl.
nuenen.nl.
nunspeet.nl.
oegstgeest.nl.
oirschot.nl.
oisterwijk.nl.
gemeente-oldambt.nl.
oldebroek.nl.
oldenzaal.nl.
olst-wijhe.nl.
ommen.nl.
oostgelre.nl.
oosterhout.nl.
ooststellingwerf.nl.
oostzaan.nl.
opmeer.nl.
opsterland.nl.
oss.nl.
oude-ijsselstreek.nl.
ouder-amstel.nl.
oudewater.nl.
overbetuwe.nl.
papendrecht.nl.
peelenmaas.nl.
pekela.nl.
pijnacker-nootdorp.nl.
purmerend.nl.
putten.nl.
raalte.nl.
reimerswaal.nl.
renkum.nl.
renswoude.nl.
reuseldemierden.nl.
rheden.nl.
rhenen.nl.
ridderkerk.nl.
rijssen-holten.nl.
rijswijk.nl.
roerdalen.nl.
roermond.nl.
roosendaal.nl.
rotterdam.nl.
rozendaal.nl.
rucphen.nl.
schagen.nl.
scherpenzeel.nl.
schiedam.nl.
schiermonnikoog.nl.
schouwen-duiveland.nl.
simpelveld.nl.
sintanthonis.nl.
sint-michielsgestel.nl.
sittard-geleen.nl.
sliedrecht.nl.
gemeentesluis.nl.
smallingerland.nl.
soest.nl.
someren.nl.
sonenbreugel.nl.
stadskanaal.nl.
staphorst.nl.
stedebroec.nl.
gemeente-steenbergen.nl.
steenwijkerland.nl.
gemeentestein.nl.
stichtsevecht.nl.
sudwestfryslan.nl.
terneuzen.nl.
terschelling.nl.
texel.nl.
teylingen.nl.
tholen.nl.
tiel.nl.
tilburg.nl.
tubbergen.nl.
twenterand.nl.
tynaarlo.nl.
t-diel.nl.
uden.nl.
uitgeest.nl.
uithoorn.nl.
urk.nl.
utrecht.nl.
heuvelrug.nl.
vaals.nl.
valkenburg.nl.
valkenswaard.nl.
veendam.nl.
veenendaal.nl.
veere.nl.
veldhoven.nl.
velsen.nl.
venlo.nl.
venray.nl.
vijfheerenlanden.nl.
vlaardingen.nl.
vlieland.nl.
vlissingen.nl.
voerendaal.nl.
voorschoten.nl.
voorst.nl.
vught.nl.
aadhoeke.nl.
aalre.nl.
aalwijk.nl.
addinxveen.nl.
ageningen.nl.
assenaar.nl.
aterland.nl.
eert.nl.
eesp.nl.
estbetuwe.nl.
estmaasenwaal.nl.
esterkwartier.nl.
gemeentewesterveld.nl.
estervoort.nl.
esterwolde.nl.
gemeentewestland.nl.
eststellingwerf.nl.
estvoorne.nl.
ierden.nl.
ijchen.nl.
ijdemeren.nl.
ijkbijduurstede.nl.
interswijk.nl.
oensdrecht.nl.
oerden.nl.
ormerland.nl.
oudenberg.nl.
zaanstad.nl.
zaltbommel.nl.
zandvoort.nl.
zeewolde.nl.
zeist.nl.
zevenaar.nl.
zoetermeer.nl.
zoeterwoude.nl.
zuidplas.nl.
zundert.nl.
zutphen.nl.
zwartewaterland.nl.
zwijndrecht.nl.
zwolle.nl.

B

Appendix B: Overview of Healthcare organizations

klinikum.uni-heidelberg.de.
erasmusmc.nl.
asklepios.com.
lumc.nl.
chuv.ch.
hug.ch.
uke.de.
medizin.uni-tuebingen.de.
sahlgrenska.se.
uniklinik-freiburg.de.
uniklinikum-jena.de.
lmu-klinikum.de.
ipin.edu.pl.
uzleuven.be.
usz.ch.
hirslanden.ch.
royalberkshire.nhs.uk.
insel.ch.
unimedizin-mainz.de.
vumc.nl.
med.uni-magdeburg.de.
guysandstthomas.nhs.uk.
umcg.nl.
curie.fr.
uniklinik-duesseldorf.de.
chu-lyon.fr.
rigshospitalet.dk.
uk-koeln.de.
norrbotten.se.
kssg.ch.
johanniter.de.
nhsggc.org.uk.
icr.ac.uk.
uniklinikum-dresden.de.
ukm.de.
uniklinik-ulm.de.
rhoen-klinikum-ag.com.
umcutrecht.nl.
ioveneto.it.
helios-gesundheit.de.
dornbirn.at.
uk-erlangen.de.
ukaachen.de.
karolinska.se.
nhsfife.org.
oslo-universitetssykehus.no.
huvn.es.
uniklinikum-saarland.de.
bmihealthcare.co.uk.
auh.dk.
sanita.puglia.it.
unispital-basel.ch.
chlc.min-saude.pt.
swisstph.ch.
parcdesalutmar.cat.
czd.pl.
royalmarsden.nhs.uk.
amc.nl.
medizin.uni-halle.de.
ifp.kiev.ua.
lf2.cuni.cz.
hus.fi.
mmc.nl.
chu-toulouse.fr.
chu-lille.fr.
fnbrno.cz.
nuffieldhealth.com.
chu-montpellier.fr.
chospab.es.
ausl.re.it.
rdkb.ru.
kgu.de.
vallhebron.com.
istituto-besta.it.
unn.no.
cuh.nhs.uk.
nbt.nhs.uk.
spirehealthcare.com.
ruh.nhs.uk.
ukw.de.
fnplzen.cz.
radboudumc.nl.
helse-bergen.no.
stolav.no.
kliinikum.ee.
nhslothian.scot.
bakulev.ru.
fr.ap-hm.fr.
onko-i.si.
ausl.mo.it.
chporto.pt.
uksh.de.
akademiska.se.
amphia.nl.
hvidovrehospital.dk.
uniklinikum-leipzig.de.
chu-bordeaux.fr.
mou.cz.
vma.mod.gov.rs.
ouh.dk.
osakidetza.euskadi.eus.
merseycare.nhs.uk.
santpau.cat.
ksa.ch.
scamilloforlanini.rm.it.
fraternidad.com.
iscare.cz.
uhs.nhs.uk.
cun.es.
unicancer.fr.
slam.nhs.uk.
qehkl.nhs.uk.
luks.ch.
mediclin.de.
ospedaleniguarda.it.
nuh.nhs.uk.
bispebjerghospital.dk.
psykiatri-regionh.dk.
tauli.cat.
nhsgrampian.org.
royalcornwall.nhs.uk.
median-kliniken.de.
policlinico.mi.it.
auslromagna.it.
sabes.it.
vsshp.fi.
leicestershospitals.nhs.uk.
gesundheitsverbund.at.
ulss.tv.it.
ncic.nhs.uk.
asl3.liguria.it.
royalpapworth.nhs.uk.
nki.nl.
asl.vt.it.
csr-dialogforum.at.
neurology.ru.
onclinic.ru.
auva.at.
ukbonn.de.
istitutotumori.mi.it.
helse-midt.no.
ouh.nhs.uk.

paracelsus-kliniken.de.
l.nhs.uk.
nelft.nhs.uk.
ospedalebambinogesu.it.
gosh.nhs.uk.
cardioweb.ru.
uhb.nhs.uk.
humv.es.
chu-besancon.fr.
klinikverbund-suedwest.de.
uhbristol.nhs.uk.
hsr.it.
christie.nhs.uk.
helse-sorost.no.
chu-amiens.fr.
saintluc.be.
fsm.it.
aslcagliari.it.
newcastle-hospitals.nhs.uk.
sth.nhs.uk.
klinikum-nuernberg.de.
rlbuht.nhs.uk.
ameos.eu.
fdoctor.ru.
herlevhospital.dk.
sh.nhs.uk.
leedsth.nhs.uk.
gvmnet.it.
fnkv.cz.
vest.rm.dk.
chelwest.nhs.uk.
hospitalsenhedmidt.dk.
uclh.nhs.uk.
chaux-de-fonds.ch.
swbh.nhs.uk.
mehilainen.fi.
gustaveroussy.fr.
ospfe.it.
hca.es.
co.pl.
malteser.de.
sath.nhs.uk.
gaslini.org.
hscboard.hscni.net.
kch.nhs.uk.
uzbrussel.be.
chguv.san.gva.es.
kzcr.eu.
aulss8.veneto.it.
vivantes.de.
salisbury.nhs.uk.
asl4.liguria.it.
maartenskliniek.nl.
sccs.pl.
praktikertjanst.se.
landspitali.is.
ch-chateau-thierry.fr.
santa.lt.
nemlib.cz.
gentoftehospital.dk.
stgag.ch.
ausl.fe.it.
mst.nl.
asst-fbf-sacco.it.
isala.nl.
ivi.es.
uza.be.
nnuh.nhs.uk.
ospedale.al.it.
fnhk.cz.
fnol.cz.
chu-nice.fr.
esthertshospitals.nhs.uk.
hagaziekenhuis.nl.
ramsaysante.fr.
stomed.ru.
northdevonhealth.nhs.uk.
medsi.ru.
ahus.no.
uk-augsburg.de.
sshf.no.
eurolab.ua.
vfn.cz.
bsuh.nhs.uk.
med.sumdu.edu.ua.
cwz.nl.
kb-merkur.hr.
uvn.cz.
cancercentrum.se.
ppshp.fi.
fnusa.cz.
chu-brest.fr.
nhsforthvalley.com.
ao.pr.it.
infomedula.org.
nordlandssykehuset.no.
chu-limoges.fr.
plymouthhospitals.nhs.uk.
ausl.pc.it.
kliniken-koeln.de.
groupe-sos.org.
galliera.it.
evkb.de.
ksw.ch.
nhstayside.scot.nhs.uk.
chu-st-etienne.fr.
gloshospitals.nhs.uk.
kbcsm.hr.
mft.nhs.uk.
ieo.it.
luxmed.pl.
stvincents.ie.
dbth.nhs.uk.
diakonessenhuis.nl.
klinikum-stuttgart.de.
homolka.cz.
muenchen-klinik.de.
giomi.it.
krh.de.
clinicbarcelona.org.
olvg.nl.
homerton.nhs.uk.
fno.cz.
ausl.pr.it.
policlinica.ru.
mavit.pl.
policlinicogemelli.it.
rbch.nhs.uk.
etz.nl.
klinika-golnik.si.
haaglandenmc.nl.
grupposandonato.it.
kantonsspitalbaden.ch.
teknon.es.
aslnuoro.it.
southwestyorkshire.nhs.uk.
chu-brugmann.be.
operapadrepio.it.
ortenau-klinikum.de.
asl2.liguria.it.
onk.ns.ac.rs.
cardio-tomsk.ru.
drk-kliniken-berlin.de.
stgeorges.nhs.uk.
aots.sanita.fvg.it.
gelreziekenhuizen.nl.
sana.de.
hopitaux-saint-maurice.fr.
klinikum-ingolstadt.de.
jeroenboschziekenhuis.nl.
hcahealthcare.co.uk.
uslsudest.toscana.it.
huderf.be.
helse-vest.no.
moorfields.nhs.uk.
bordet.be.
hnt.no.
ckbran.ru.
asst-spedalicivili.it.
northerntrust.hscni.net.
lscft.nhs.uk.
swlstg.nhs.uk.
salk.at.
immanuel.de.
mumc.nl.
chu-poitiers.fr.
oldharlowhealth.co.uk.
rnoh.nhs.uk.
polifvg.it.
burlo.trieste.it.
su.krakow.pl.
bellvitgehospital.cat.
asfo.sanita.fvg.it.
solothurnerspitaeler.ch.
aou.mo.it.
priorygroup.com.
clinicabaviera.com.
franciscus.nl.
emcmos.ru.
rdehospital.nhs.uk.
enherts-tr.nhs.uk.
sfh-tr.nhs.uk.
bk-trier.de.
antoniusziekenhuis.nl.
klinikumchemnitz.de.
ghu-paris.fr.
klinikumdo.de.
sthk.nhs.uk.
unhb.cz.
umm.de.
uzgent.be.
chru-strasbourg.fr.
kages.at.
bedfordshirehospitals.nhs.uk.
satasairaala.fi.
ausl.vda.it.
klinikum-braunschweig.de.
geldersevallei.nl.
porthosp.nhs.uk.
cnwl.nhs.uk.
dzhmao.ru.
unbr.cz.
balgrist.ch.
aslcarbonia.it.
bernhoven.nl.
mdanderson.es.
medicina.ru.
asz.nl.
nhsaaa.net.



Appendix C: Overview of SME's

crossflowpayments.co.uk.
landbay.co.uk.
safe4u.de.
nl.bunq.com.
de.scalable.capital.
gojob.com.
happybrush.de.
huma.com.
bonmea.com.
kickmaker.fr.
privitar.com.
amco.bg.
eocharging.com.
fastnedcharging.com.
footdistrict.com.
nisa.services.
velocity.black.
lmmlogistics.com.
gustavo-gusto.de.
gellify.com.
kavera.de.
mg-project.com.
grover.com.
spotawheel.com.
lehibou.com.
elvie.com.
mavoco.com.
tmtinternational.it.
j-pm-systems.com.
theras-group.com.
locumsnest.co.uk.
goldenbees.fr.
ferroamp.com.
deutsches-pm.de.
mycamper.ch.
stoyo.io.
etaca.com.
youmawo.com.
mercurio-group.com.
bdrnlicensing.com.
d-energy.it.
sigalsapiro.de.
makonis.de.
infratech-bau.de.
qmee.com.
memorypc.de.
itds.pl.
funnel.io.
mia-platform.eu.
rvi.immo.
nanushka.com.
makingscience.com.
creditshelf.com.
sneakers-jackets.com.
amarencogroup.com.
parcellab.com.
advarra.com.
chattermill.com.
idenergy.group.
saturnoappalti.com.
bettergov.co.uk.
lvsbrokers.com.
divido.com.
spcservice.it.
aixemtec.com.
researchpartnership.com.
omnisend.com.
bizaway.com.
bumper.co.uk.
aliasgroup.it.
livestorm.co.
eu.lestrangelondon.com.
itrinity.com.
mcule.com.
elogic.co.
feiniko.de.
novicap.com.
manitech.it.
eastcoastbakehouse.com.
messina-autotrasporti.it.
sirenum.com.
kivra.se.
quantexa.com.
yoyogroup.com.
frauandpartners.it.
airbeam.tv.
bambridgeaccountants.com.
apitalianluxury.com.
idesa.net.
sfc-industrieservice.de.
bluwalk.com.
biotyfullbox.fr.
holidu.de.
arquimea.com.
cybersprint.com.
qred.com.
spiideo.com.
delante.co.
sio.engineering.
templafy.com.
valvoleitalia.it.
semantive.com.
ubiquicom.com.
elliptic.co.
boosterboxdigital.com.
assi.tech.
signaturit.com.
ayesconsulting.com.
playdigious.com.
sabor-espana.com.
crowdproperty.com.
comodoitalia.it.
topfish.it.
laboutiquedelbiologico.it.
transporentsrl.it.
reinagreen.com.
instilla.it.
atecnica.it.
designerealization.com.
adpone.com.
virta.global.
3zehn.net.
sixth-sense.ai.
obido.pl.
earephenix.com.
domator24.com.
grupoherrerobrigantina.com.
peoplegrapher.com.
zaraimballaggi.nwksite.com.
truu.com.
contrader.it.
skills-rh.fr.
greenteamsrl.com.
groupe-nat.fr.
gpainnova.com.
remove-france.com.
frontify.com.
firstphone.hu.
artepassioneristorazione.it.
deutschewebdesign.de.
messengerpeople.com.
soorce.de.
asserneutral-gmbh.de.
dallenergy.com.
performance54.com.
mpfinance.it.
it.everli.com.
druck-media-service.com.
crest-investment.com.
agrivi.com.
abcostruzioni.it.
phrasee.co.
tesgroupsrl.it.
savvyinvestor.net.

intumind.de.
samont.com.
moments.pastbook.com.
krollcosmetics.com.
marwincar.com.
farmermobil.com.
nexumstp.it.
net-it-systemhaus.com.
supermetrics.com.
computersparts.it.
herrles-industriemontagen.de.
samyroad.com.
lendingworks.co.uk.
fimarsud.it.
parlem.com.
velvetmedia.it.
bk-retail.de.
levertouch.com.
fashion-commerce.it.
bluefinfitness.com.
labelexperience.com.
unicoenergia.it.
studapart.com.
global-work.it.
evondos.com.
nephostechnologies.com.
9y.co.
teamtailor.com.
mailtrack.io.
apsi.fr.
travelcompositor.com.
bus-bau.com.
mclabels.com.
bordonaro-it.com.
fundingoptions.com.
preomics.com.
fillupmedia.fr.
billiondollarboy.com.
nuevo.fr.
exscientia.ai.
virtuslab.com.
kumulusvape.fr.
sourcebreaker.com.
discovercars.com.
karma-partners.com.
hd-elektrotechnik.com.
newilbau.fi.
tistyleit.com.
assistec.cc.
vanmoof.com.
lenergetica.it.
activbilanz.de.
studioimmagineitalia.it.
brandongroup.it.
vmway.it.
nordicunmanned.com.
xcd.com.
myesmart.com.
veit-shopfitting.de.
bke-eisenbahn.de.
brainhub.eu.
digitalent-consulting.com.
isoltech.info.
cru-wine.com.
newgeneralservice.com.
ecovatios.com.
kuadracucine.it.
uqido.com.
ibanfirst.com.
tavan-tiefbau.de.
uplink-network.de.
visions-network.com.
deepki.com.
ahp-cm.com.
gpasplus.com.
solarplay.it.
vonmaehlen.com.
postex.com.
parisherbes.com.
rettel-projektbau.de.
laundryheap.com.
zinoxlaser.it.
revolutionrace.se.
cfe-finance.com.
superprof.fr.
nethive.it.
revegfruit.it.
sorted.com.
pomorskaplatformapracy.pl.
uniteflooringltd.com.
energytecno.com.
autologymotors.com.
fruugo.com.
oppobrothers.com.
adsmurai.com.
atmopur.fr.
smarketer.de.
consorzioartea.it.
expereo.com.
vecchierelli.com.
logipal24.de.
namelessmusicfestival.com.
dialecticanet.com.
bksolarezukunft.de.
cabinet-ares.com.
podium-tech.com.
eila.de.
chez-nestor.com.
vitl.com.
nanovo.tv.
beatly.com.
brandupgroup.it.
riskmethods.net.
tecmasolutions.com.
draga-aurel.com.
null-bar.de.
clemajob.fr.
stuckateur-raissle.de.
endomag.com.
emiliafoods.it.
documaster.com.
asigma.fr.
proplacement.de.
revive.de.
imperialgroup.it.
azuri-group.com.
adludio.com.
trencadis.ro.
theinnercircle.co.
endado.com.
enesco.it.
fairmat.com.
sis-systemy.cz.
materassiedoghe.eu.
zialucia.com.
uc2000.eu.
ngtsrl.it.
lazerlamps.com.
branchspace.com.
gruppodelbarba.com.
md6.fr.
oodboxscs.it.
84codes.com.
plasmapro.ee.
greenflux.com.
dsglass.it.
deaterra.net.
democom.it.
aquis.eu.
hpmitaly.it.
agriconomie.com.
al-one.it.
insax.com.
vismacontract.com.
groupehisi.fr.
sciant.com.
ecoco2.com.
opna.fr.
ncmauctions.co.uk.
glas.agency.
phenisys.com.
speechmatics.com.
easycarsbg.com.
snigel.com.
cominciadazero.com.
one-unity.de.
cemirsecurity.it.
sharpteam.fr.
multix-trolley.com.
convertgroup.com.
autosalon-hh.de.
brewshop.no.
agilelab.it.
offhealth.it.
sandsrl.it.
fodmobilitygroup.com.
master-dealer.it.
dw-trans.fr.
silicone-innovation.com.
maxxiengineering.it.
maginta.fr.
marfeel.com.
stufeapelletitalia.com.
schroderscapital.com.
gruppotera.com.
doit.zone.
airthings.com.
fs-group.com.
camping-kaufhaus.com.
dottorgrandine.com.
thermatik.de.
frg.eu.com.
awesome-software.de.
opera-energie.com.
erksraeder24.de.
ombea.com.
obiz-concept.fr.

D

Appendix D: Overview of Higher Educational Institutes

ethz.ch.
cam.ac.uk.
imperial.ac.uk.
ucl.ac.uk.
epfl.ch.
ed.ac.uk.
manchester.ac.uk.
kcl.ac.uk.
lse.ac.uk.
tum.de.
psl.eu.
tudelft.nl.
bristol.ac.uk.
uva.nl.
polytechnique.edu.
arwick.ac.uk.
lmu.de.
uni-heidelberg.de.
uzh.ch.
msu.ru.
ku.dk.
gla.ac.uk.
sorbonne-universite.fr.
kuleuven.be.
durham.ac.uk.
birmingham.ac.uk.
southampton.ac.uk.
leeds.ac.uk.
sheffield.ac.uk.
st-andrews.ac.uk.
lunduniversity.lu.se.
kth.se.
nottingham.ac.uk.
tcd.ie.
dtu.dk.
helsinki.fi.
unige.ch.
uio.no.
unibe.ch.
qmul.ac.uk.
ur.nl.
hu-berlin.de.
tue.nl.
uu.nl.
uu.se.
aalto.fi.
universiteitleiden.nl.
rug.nl.
fu-berlin.de.
kit.edu.
lancaster.ac.uk.
ugent.be.
polimi.it.
centralesupelec.fr.
chalmers.se.
rwth-aachen.de.
international.au.dk.
tu.berlin.
unibas.ch.
univie.ac.at.
york.ac.uk.
ncl.ac.uk.
cardiff.ac.uk.
unibo.it.
ens-lyon.fr.
exeter.ac.uk.
unil.ch.
uniroma1.it.
tu-dresden.de.
bath.ac.uk.
cardioweb.ru.
uni-freiburg.de.
ucd.ie.
su.se.
liverpool.ac.uk.
ub.edu.
uclouvain.be.
tuwien.at.
uib.no.
uni-goettingen.de.
eur.nl.
utwente.nl.
uam.es.
vub.be.
gu.se.
reading.ac.uk.
ucm.es.
abdn.ac.uk.
qub.ac.uk.
uab.cat.
ru.nl.
unipd.it.
english.spbu.ru.
lboro.ac.uk.
english.nsu.ru.
uni-hamburg.de.
maastrichtuniversity.nl.
vu.nl.
nuigalway.ie.
uantwerpen.be.
uni-bonn.de.
ecoledesponts.fr.
sciencespo.fr.
le.ac.uk.
sussex.ac.uk.
en.tsu.ru.
ulb.be.
unav.edu.
cuni.cz.
uibk.ac.at.
tu-darmstadt.de.
surrey.ac.uk.
usi.ch.
tugraz.at.
u-paris.fr.
mipt.ru.
portal.uni-koeln.de.
ut.ee.
ucc.ie.
upf.edu.
pantheonsorbonne.fr.
utu.fi.
ens-paris-saclay.fr.
hse.ru.
strath.ac.uk.
hw.ac.uk.
unimi.it.
en.aau.dk.
universite-paris-saclay.fr.
uni-mannheim.de.
polito.it.
royalholloway.ac.uk.
uc3m.es.
goethe-university-frankfurt.de.
eng.mephi.ru.
upc.edu.
bsu.by.
fau.eu.
dundee.ac.uk.
en.uw.edu.pl.
uni-jena.de.
en.uj.edu.pl.
eng.rudn.ru.
upv.es.
ie.edu.
urfu.ru.

umu.se.
uni-stuttgart.de.
uea.ac.uk.
jyu.fi.
univ-grenoble-alpes.fr.
vscht.cz.
bbk.ac.uk.
uni-ulm.de.
soas.ac.uk.
english.mgimo.ru.
city.ac.uk.
sdu.dk.
uni-muenster.de.
um.es.
sigarra.up.pt.
en.itmo.ru.
ntnu.edu.
jku.at.
liu.se.
brunel.ac.uk.
tilburguniversity.edu.
eng.kpfu.ru.
kent.ac.uk.
brookes.ac.uk.
unipi.it.
international.unina.it.
unisr.it.
unistra.fr.
english.spbstu.ru.
tpu.ru.
uni-mainz.de.
unitn.it.
oulu.fi.
tuni.fi.
essex.ac.uk.
gold.ac.uk.
en.uit.no.
vu.lt.
u-bordeaux.com.
en.misis.ru.
unl.pt.
unisg.ch.
uc.pt.
cvut.cz.
unifi.it.
uni-wuerzburg.de.
dcu.ie.
ruhr-uni-bochum.de.
uni-konstanz.de.
upm.es.
uni-saarland.de.
uliege.be.
uhasselt.be.
lut.fi.
uni-halle.de.
swansea.ac.uk.
ntua.gr.
ucy.ac.cy.
univer.kharkov.ua.
uni-leipzig.de.
aber.ac.uk.
stir.ac.uk.
dvfu.ru.
uah.es.
uni-kiel.de.
ugr.es.
unizar.es.
u-szeged.hu.
aston.ac.uk.
unicatt.it.
en.uniroma2.it.
univ-amu.fr.
umontpellier.fr.
aau.at.
ul.ie.
pw.edu.pl.
sgu.ru.
en.unito.it.
uni-bayreuth.de.
edu.unideb.hu.
en.unimib.it.
uni-giessen.de.
muni.cz.
coventry.ac.uk.
insa-lyon.fr.
uni-bremen.de.
u-paris2.fr.
tu-braunschweig.de.
univ-tlse3.fr.
abo.fi.
asu.ru.
auth.gr.
uni-graz.at.
kingston.ac.uk.
us.es.
ua.pt.
upol.cz.
ssau.ru.
sfedu.ru.
uv.es.
uminho.pt.
bangor.ac.uk.
elte.hu.
unibz.it.
eng.unn.ru.
uni-sofia.bg.
univ.kiev.ua.
ulster.ac.uk.
usal.es.
eb.unipv.it.
url.edu.
uni-regensburg.de.
unifr.ch.
univ-cotedazur.eu.
bradford.ac.uk.
hull.ac.uk.
uni-lj.si.
port.ac.uk.
vut.cz.
uni-hannover.de.
en.uoa.gr.
kpi.kharkov.ua.
northumbria.ac.uk.
upjs.sk.
uni-marburg.de.
taltech.ee.
comillas.edu.
unige.it.
en.unisi.it.
uni-hohenheim.de.
eb.umons.ac.be.
international.pte.hu.
plymouth.ac.uk.
estminster.ac.uk.
vilniustech.lt.
uniba.sk.
keele.ac.uk.
maynoothuniversity.ie.
mendelu.cz.
mdx.ac.uk.
kpi.ua.
rtu.lv.
etu.ru.
int.sumdu.edu.ua.
usc.gal.
units.it.
uni-rostock.de.
univ-lyon1.fr.
gre.ac.uk.
hud.ac.uk.
bournemouth.ac.uk.
lsbu.ac.uk.
ntu.ac.uk.
plus.ac.at.
rea.ru.
poliba.it.
urv.cat.
tul.cz.
ehu.eus.
unive.it.
international.unimore.it.
unipg.it.
uni-due.de.
hhu.de.
univ-lille.fr.
brescia.edu.
upatras.gr.
international.amu.edu.pl.
agh.edu.pl.
aueb.gr.
ubbcluj.ro.
en.bntu.by.
bcu.ac.uk.
bme.hu.
uni-corvinus.hu.
pk.edu.pl.
czu.cz.
dmu.ac.uk.
napier.ac.uk.
pg.edu.pl.
gcu.ac.uk.
en.ktu.edu.
ljmu.ac.uk.
p.lodz.pl.
londonmet.ac.uk.
mmu.ac.uk.
lpnu.ua.
umk.pl.
en.nstu.ru.
en.psu.ru.
put.poznan.pl.
qmu.ac.uk.
rsu.lv.
shu.ac.uk.
polsl.pl.
stuba.sk.
susu.ru.
sziu.hu.
tlu.ee.
tuke.sk.
tu-dortmund.de.
tudublin.ie.
rgu.ac.uk.
ranepa.ru.
ua.es.

E

Appendix E: Overview of Large Companies

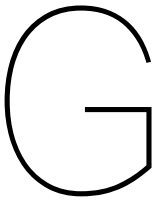
roche.com.
nestle.com.
asml.com.
prosus.com.
loreal.com.
novonordisk.com.
accenture.com.
novartis.com.
astrazeneca.com.
medtronic.com.
sap.com.
linde.com.
hermes.com.
shell.com.
volkswagenag.com.
unilever.com.
dior.com.
gruppe.schwarz.
siemens.com.
sanofi.com.
ab-inbev.com.
riotinto.com.
totalenergies.com.
diageo.com.
airbus.com.
inditex.com.
merckgroup.com.
gazprom.com.
gsk.com.
kering.com.
telekom.com.
se.com.
bosch.com.
adyen.com.
enel.com.
audi.com.
2.deloitte.com.
daimler.com.
luxottica.com.
bat.com.
dpdhl.com.
airliquide.com.
pwc.com.
bp.com.
atlascopco.com.
allergan.com.
arkema.com.
biontech.de.
siemens-healthineers.com.
iberdrola.es.
3ds.com.
global.abb.
novatek.ru.
swatchgroup.com.
rosneft.com.
basf.com.
ey.com.
adidas-group.com.
equinor.com.
aldi.com.
orsted.com.
gruppotim.it.
eaton.com.
sainsburys.co.uk.
vinci.com.
remy-cointreau.com.
richemont.com.
lonza.com.
bmwgroup.com.
dsv.com.
nxp.com.
glencore.com.
relx.com.
angloamerican.com.
home.kpmg.
pernod-ricard.com.
volvogroup.com.
infineon.com.
lukoil.com.
bayer.com.
reckitt.com.
safran-group.com.
maersk.com.
corporate.ferrari.com.
nornickel.com.
inpost.eu.
sika.com.
sartorius.com.
te.com.
edeka.de.
ihsmarkit.com.
neste.nl.
danone.com.
vodafone.com.
tranetechnologies.com.
omz.ru.
nationalgrid.com.
morrisons-corporate.com.
cellnextelecom.com.
givaudan.com.
hexagon.com.
spotify.com.
eni.com.
home.kuehne-nagel.com.
kone.com.
edfenergy.com.
philips.com.
stellantis.com.
vivendi.com.
crh.com.
vestas.com.
experianplc.com.
aptiv.com.
henkel.com.
alcon.com.
st.com.
hapag-lloyd.com.
ericsson.com.
verbund.com.
investoren.vonovia.de.
saint-gobain.com.
capgemini.com.
coloplast.com.
compass-group.com.
evolution.com.
deliveryhero.com.
eon.de.
assaabloy.com.
dsm.com.
hm.com.
ashtead-group.com.
flutter.com.
holcim.com.
engie.com.
fresenius.com.
aholddelhaize.com.
us.schindler.com.
corporate.arcelormittal.com.
nokia.com.
lyondellbasell.com.
home.sandvik.
ferguson.com.
straumann.com.
genmab.com.
porsche-se.com.

geberit.com.
legrand.com.
kerrygroup.com.
swisscom.ch.
orange.com.
nibe.com.
oltersklUwer.com.
vitol.com.
michelin.com.
peugeot.com.
telefonica.com.
lindt-spruengli.com.
amadeus.com.
zalando.se.
beiersdorf.com.
yandex.com.
tescoplc.com.
fortum.com.
unitedutilities.com.
eurofins.com.
theheinekencompany.com.
rwe.com.
carlsberggroup.com.
epirocgroup.com.
continental.com.
cocacolaep.com.
edpr.com.
teleperformance.com.
endesa.com.
baesystems.com.
orldline.com.
upm.com.
investor.ryanair.com.
naturgy.com.
polyus.com.
ems-group.com.
camparigroup.com.
enbw.com.
aena.es.
horizontherapeutics.com.
sonova.com.
sse.com.
kingspan.com.
telenor.com.
sgs.com.
essity.com.
akzonobel.com.
freseniusmedicalcare.com.
edp.com.
cnhindustrial.com.
novozymes.com.
ferrovial.com.
thalesgroup.com.
abf.co.uk.
nexi.it.
ucb.com.
irco.com.
steris.com.
ocadogroup.com.
segro.com.
deutsche-wohnen.com.
siemens-energy.com.
siemensgamesa.com.
nlmk.com.
iconplc.com.
imperialbrandsplc.com.
jdepeets.com.
zeiss.com.
veolia.com.
knorr-bremse.com.
antofagasta.co.uk.
snam.it.
severstal.com.
asm.com.
symrise.com.
hellofresh.com.
vantagetowers.com.
about.puma.com.
about.allegro.eu.
teliacompany.com.
omv.com.
alfalaval.com.
poste.it.
moncler.com.
bollore.com.
croda.com.
aveva.com.
heidelbergcement.com.
logitech.com.
jameshardie.com.
argenx.com.
surgutneftegas.ru.
sinch.com.
smith-nephew.com.
cez.cz.
repsol.com.
publicisgroupe.com.
spiraxsarcoengineering.com.
pp.com.
clarivate.com.
bouygues.com.
terna.it.
en.transneft.ru.
storaenso.com.
libertyglobal.com.
alstom.com.
entaingroup.com.
kesko.fi.
prada.com.
halma.com.
corporate.evonik.com.
atlantia.com.
brenntag.com.
swedishmatch.com.
group.bureauveritas.com.
smurfitkappa.com.
carrefouruae.com.
rentokil-initial.com.
traton.com.
suez.com.
jdsports.co.uk.
farfetch.com.
nextplc.co.uk.
biomerieux.com.
eng.alrosa.ru.
uniper.energy.
grifols.com.
kiongroup.com.
barry-callebaut.com.
novocure.com.
mowi.com.
lifco.se.
hydro.com.
demant.com.
solvay.com.
ise.com.
en.balder.se.
kpn.com.
recordati.com.
umicore.com.
randstad.com.
mondigroup.com.
rolls-royce.com.
adevinta.com.
jeronimomartins.com.
coca-colahellenic.com.
sca.com.
persimmonhomes.com.
allegion.com.
sagax.se.
mantruckandbus.com.
qiagen.com.
diasorin.com.
rational.nl.
covestro.com.
iliad.fr.
vatvalve.com.
indutrade.com.
skanska.com.
pandoragroup.com.
bunzl.com.
mtu.de.
chr-hansen.com.
curevac.com.
yara.com.
sodexo.com.
pik.ru.
urw.com.
embracer.com.
parisaeroport.fr.
intertek.com.
tenaris.com.
temenos.com.
corporate.amplifon.com.
evraz.com.
thg.com.
skf.com.
ihgplc.com.
getinge.com.
inwit.it.
rusal.ru.
gecina.fr.
mmk.ru.
informa.com.
nemetschek.com.
kabeldeutschland.com.
imcdgroup.com.
tele2.com.
iairgroup.com.
ree.es.
schibsted.com.
sage.com.
oatly.com.
rockwool.com.
ternium.com.
renault.co.in.
eiffage.com.
burberryplc.com.
barrattdevelopments.co.uk.
icagruppen.se.
kingfisher.com.
melroseplc.net.
elisa.com.
bachem.com.
boliden.com.
prysmiangroup.com.

Appendix F: Overview of NGO's

akmns-khab.info.
yhrm.org.
dobrovolets.ru.
shag-navstrechu.ru.
voginfo.ru.
myolymp.org.
atiso.ru.
detfond.org.
asf-ev.de.
amarodrom.de.
asla.de.
crisp-berlin.org.
cvjm.de.
go-epa.org.
drjug.org.
esw-berchum.de.
europeanfellowship.com.
bbyo.org.uk.
byc.org.uk.
childtochild.org.uk.
cisv.org.
communitycourtyard.org.
deaf-world.org.
euromernet.org.
papyrosn.com.
coexister.fr.
eedf.fr.
romans-international.fr.
y-nove.org.
cafebabel.com.
concordia.fr.
ccivs.org.
controventocatania.it.
acmos.net.
lunaria.org.
a-id.org.
alliance-network.eu.
amaita.it.
creativi108.com.
associazioneagrado.com.
aegeemalaga.org.
ser-joven.org.
aegeemadrid.org.
aheadedu.org.
cazalla-intercultural.org.
deamicitia.org.
eurodynamis.org.
ajovenes.es.
cent.dn.ua.
ekoart.org.
gcs.org.ua.
gurt.org.ua.
eu.sumy.ua.
uhrf.org.
p4ec.org.ua.
klitschkofoundation.org.
aiesec.pl.
europe4youth.eu.
krytykapolityczna.pl.
levelupngo.com.
federa.org.pl.
goinpro.org.
centrumwolontariatu.eu.
semperavanti.org.
educationstudio.ro.
a4action.ro.
geyc.ro.
youthcandoit.eu.
asociatiacris.ro.
atdd.ro.
cdcd.ro.
evocariera.ro.
adynenetherlands.nl.
aegee-utrecht.nl.
netherlandsromania.eu.
aegee-tilburg.nl.
ayape.eu.
eestec.net.
egea.eu.
estiem.org.
act4change.be.
adyne.eu.
ymcaeurope.com.
aegee.org.
best.eu.org.
beta-europe.org.
c4ep.eu.
connect-international.org.
eaicy.cz.
eyp.cz.
inexsda.cz.
iynf.org.
kuro.cz.
yeenet.eu.
aperio.cz.
artmill.eu.
goalive.eu.
antigone.gr.
aegee-athina.gr.
intermediakt.org.
skep.gr.
kidsinaction.gr.
ngokane.org.
elix.org.gr.
esnlisboa.org.
checkin.org.pt.
home.rotajovem.com.
futrua.org.
paraonde.org.
esnportugal.org.
refugees-welcome.pt.
ecos.pt.
activeeurope.org.
centralasien.org.
dromstort.com.
peaceworks.se.
yip.se.
globalutmaning.se.
kvinnatillkvinna.se.
iogt.se.
autonomia.hu.
best-budapest.hu.
kozpontegyesulet.hu.
elmenyakademia.hu.
ifjusagitanacs.hu.
szubjektiv.org.
haver.hu.
jeneialapitvany.hu.
ifmsa.org.
msanl.nl.
asri.nl.
buitendoor.nl.
belau.info.
est-east-fund.com.
unoy.org.
csr-dialogforum.com.
grenzenlos.or.at.
iusy.org.
generationeuropa.eu.
omen-without-borders.org.
bhakademiker.org.
elternkreis.at.
eard.at.
cse.rs.
intermedia.org.rs.
parlament.org.rs.
e8.org.rs.
tvojasrbija.rs.
ec.org.rs.
protecta.org.rs.
koms.rs.
eyp.ch.
global-changemakers.net.
oikos-international.org.

orldywca.org.
actfordev.org.
allianceforhealthpromotion.org.
alliancesud.ch.
africanfoundation.ch.
infopass.eu.
site.bbbsbg.org.
bulsport.bg.
trotoara.com.
yesbg.eu.
ifspd.org.
bgrf.org.
sozopol-foundation.com.
soholm4h.dk.
freemuse.org.
92grp.dk.
drc.ngo.
dignity.dk.
euromedrights.org.
fnforbundet.dk.
fig.net.
ifmsa.org.
ifhohyp.org.
nordung.org.
ykliitto.fi.
ruralyoutheurope.com.
peace.ax.
unwomen.fi.
ifsnetwork.org.
adelslovakia.org.
dobrovolnictvoba.sk.
dckk.sk.
ozviac.sk.
rmbrk.sk.
rmzk.sk.
skauting.sk.
studentskaunia.sk.
terrampacis.org.
yfu.no.
actis.no.
fhn.no.
humanrightshouse.org.
npaid.org.
lnu.no.
mirasenteret.no.
ymca.ie.
helplink.ie.
eyp.ie.
irishgirlguides.ie.
muintearas.com.
ywicork.com.
youthworkireland.ie.
eeg-turn.com.
mladi-eu.hr.
ya.net.
cnc.hr.
yihr.hr.
status-m.hr.
babe.hr.
status-m.hr.
synergy-croatia.com.
novageneracija.org.
fondacijazajednickiput.org.
proni.ba.
spin-okret.org.
cdmpl.net.
seeyn.org.
prevencija.ba.
humanityinaction.org.
liburnetik.org.
observator.org.al.
crca.al.
qendraimpakt.com.
hanacentre.org.
qendrasteps.al.
togetherforlife.org.al.
lda.al.
activeyouth.lt.
lijot.lt.
mjotas.lt.
darbdaviai.org.
laisve.lt.
youth-sport.net.
juruskautai.lt.
refugees.lt.
forum16.eu.
ekvalis.org.mk.
cid.mk.
sega.org.mk.
sppmd.org.mk.
dominium.mk.
napag.mk.
nms.org.mk.
mladiplus.si.
dsms.net.
socialna-akademija.si.
transparency.si.
zavod-voluntariat.si.
focus.si.
ifimes.org.
socialinnovation.lv.
jaunatnesmaidam.lv.
best.rtu.lv.
zalabriviba.lv.
eyl.ee.
shokkin.org.
yfu.ee.
trajectorya.ee.
fennougria.ee.
humanrights.ee.
sscw.ee.
youthrise.org.
umhcg.com.
cazas.org.
cgo-cce.org.
forum-mne.com.
mladiromi.me.
phirenamenca.me.
yihr.me.
young-pirates.eu.
alnu.lu.
dupainpourchaqueenfant.org.
gef.eu.
iaeste.org.
diplomacy.edu.
ioinst.org.
rarediseasesmalta.com.
ncwmalta.com.
amade-mondiale.org.
usme.org.
caritas.org.
roiip.ru.
vfunion.ru.
raipon.info.
academic-mobility.ru.
p4ec.ru.
interethnic.org.
centerpolit.org.
dumrt.ru.
eyp.org.
youthpress.org.
youth4media.com.
fzs.de.
iflry.org.
kurt-loewenstein.de.
loesje.org.
ayudh.eu.
migrafrica.org.
migrationmiteinander.de.
moviemiento.org.
pjr-dresden.de.
sci-d.de.
kommunikationskollektiv.org.
same-network.org.
skachem.com.
uaem.org.
yeni.org.
eypuk.co.uk.
migrantsrights.org.uk.
moishehouse.org.
mouththatroars.com.
mydg.org.uk.
operacircusuk.com.
peopleandplanet.org.
rethinkeconomics.org.
inspirefocus.co.uk.
ivsgb.org.
thewinch.org.
valleytheatre.co.uk.
vfcc.org.uk.
youact.org.
empow-her.com.
etudiantsetdeveloppement.org.
ficemea.org.
forumfrancaisjeunesse.fr.
hors-pistes.org.
radiocampus.fr.
interfaithtour.fr.
jecimiec.eu.
jeunes-agriculteurs.fr.
jeunes-europeens.org.
service-civique-europeen.com.
project-mirador.org.
mondepluriel.org.
mag-jeunes.org.
ymcasiderno.it.
maghweb.org.
terradimezzoaps.eu.
aicem.it.
iboitalia.eu.
linkyouth.org.
popolinsieme.eu.
bestbarcelona.org.
ciong.org.
redicnet.org.
plast.org.ua.
sii.org.ua.
yac.org.ua.



Appendix G: Overview of Financial Services

sberbank.ru.
allianz.com.
group.bnpparibas.
chubb.com.
investorab.com.
cooppank.ee.
axa.com.
zurich.com.
santander.com.
ubs.com.
lseg.com.
intesasanpaolo.com.
prudential.com.
ing.com.
eqtgroup.com.
nordea.com.
partnersgroup.com.
credit-agricole.com.
lloydsbankinggroup.com.
bbva.es.
home.barclays.
munichre.com.
3i.com.
kbc.com.
natwestgroup.com.
dnb.no.
generali.com.
deutsche-boerse.com.
sebgroup.com.
sampo.com.
illistowerswatson.com.
unicredit.it.
societegenerale.com.
bailliegifford.com.
swissre.com.
db.com.
credit-suisse.com.
caixabank.es.
ccpeol.com.
handelsbanken.com.
latour.se.
swedbank.com.
group.legalandgeneral.com.
hannover-re.com.
aviva.com.
sc.com.
exor.com.
about.amundi.com.
tinkoff.ru.
gbl.be.
otpbank.hu.
lundbergforetagen.se.
erstegroup.com.
euwax-ag.de.
nngroup.com.
tryg.com.
industrivarden.se.
swisslife.com.
halinvestments.nl.
natixis.com.
sofinagroup.com.
admiralgroup.co.uk.
juliusbaer.com.
danskebank.com.
edenred.com.
pkobp.pl.
schroders.com.
abnamro.com.
euronext.com.
sjp.co.uk.
cnp.fr.
kinnevik.com.
talanx.com.
allfunds.com.
finecobank.com.
gjensidige.no.
mediobanca.com.
rsagroup.com.
aegon.com.
ml.co.uk.
vtb.com.
ageas.com.
icgam.com.
thephoenixgroup.com.
dws.com.
santander.pl.
unipolsai.com.
abrdn.com.
commerzbank.com.
group.aib.ie.
rbinternational.com.
eurazeo.com.
bankofireland.com.
revolut.com.
ing.pl.
bmedonline.it.
janushenderson.com.
baloise.com.
mandg.com.
bcv.ch.
kb.cz.
pekao.com.pl.
klarna.com.
mapfre.es.
avanza.se.
endelgroup.com.
asrnederland.nl.
group.intesasanpaolo.com.
helvetia.com.
pzu.pl.
moex.com.
directlinegroup.co.uk.
scor.com.
ig.com.
bawaggroup.com.
vontobel.com.
bankinter.com.
tikehaucapital.com.
bancagenerali.com.
bancobpm.it.
n26.com.
greensill.com.
nordnetab.com.
apigroupinc.com.
topdanmark.dk.
alliancetrust.co.uk.
hypoport.com.
man.com.
uk.virginmoney.com.
unipol.it.
storebrand.no.
oaknorth.co.uk.
mbank.pl.
bancsabadell.com.
azimut-group.com.
lukb.ch.
ashmoregroup.com.
vermoegenszentrum.ch.
intrum.com.
oberbank.com.
kbcancora.be.
hsbc.de.
vig.com.
brederode.eu.
peugeot-invest.com.
reinet.com.
bure.se.
quilter.com.

eurobank.gr.
landbobanken.dk.
corporacionalba.es.
sparebank1.no.
tradegate.ag.
beazley.com.
mkb.ru.
closebrothers.com.
alpha.gr.
kentreliance.co.uk.
jyskebank.com.
bper.it.
temit.co.uk.
comdirect.de.
fondulproprietatea.ro.
flatexdegiro.com.
investec.com.
uniqagroup.com.
rothschildandco.com.
swissquote.ch.
sgkb.ch.
nbg.gr.
bnpparibas.pl.
hbmhealthcare.com.
unicajabanco.es.
janushenderson.com.
ajbell.co.uk.
ind.millenniumbcp.pt.
efginternational.com.
piraeusbank.gr.
gruppomol.it.
ratos.com.
hastingsgroup.uk.
moltenventures.com.
company.cerved.com.
credem.it.
banknorwegian.no.
cembra.ch.
arionbanki.is.
zugerkb.ch.
moneta.cz.
banknorwegian.no.
ww-ag.com
bankmillennium.pl.
bekb.ch.
jupiteram.com.
popso.it.
paragonbankinggroup.co.uk.
tipspa.it.
animasgr.it.
coface.com.
akerhorizons.com.
sparebank1.no.
monzo.com.
llb.li.
flowtraders.com.
creades.se.
bcvs.ch.
sydbank.com.
nibc.com.
btv.at.
financiere-moncey.fr.
rosbank.ru.
gimv.com.
cmcmarkets.com.
cattolica.it.
rgs.ru.
tiotechspac.com.
euromoneyplc.com.
aareal-bank.com.
valiant.ch.
nlb.si.
bff.com.
pfandbriefbank.com.
april.com.
citibank.pl.
aliorbank.pl.
lhv.ee.
atombank.co.uk.
vaudoise.ch.
credit-agricole.fr.
sparnord.dk.
octopusinvestments.com.
jtc.gov.sg.
intertrustgroup.com.
avgd.ua.
eq.fi.
effektengesellschaft.de.
justgroupplc.co.uk.
vostoknewventures.com.
liberbank.es.
bcge.ch.
mps.it.
providentfinancial.com.
almbrand.dk.
gkb.ch.
sbanken.no.
ch.leonteq.com.
vanlanschotkempen.com.
ukmity.com.
bankofgeorgiagroup.com.
eurohold.bg.
nuernberger.de.
baaderbank.de.
resursholding.com.
janushenderson.com.
spv.no.
aktia.fi.
traction.se.
creval.it.
dovalue.it.
mlp-se.com.
altamir.fr.
collector.se.
ca-indosuez.com.
aurelius-group.com.
svolder.se.
bancaifis.it.
tradition.com.
gruppocarige.it.
equiniti.com.
oresund.se.
permanenttsbgroup.ie.
cordiantdigitaltrust.com.
protectorforsikring.no.
credit-agricole.fr.
oekoworld.com.
pegasuseurope.com.
bancosardegna.it.
dbag.de.
tetragoninv.com.
ecclesiastical.com.
bks.at.
nbb.be.
argoblockchain.com.
sabreplc.co.uk.
d9infrastructure.com.
arrowglobal.net.
greshamhouse.com.
umweltbank.de.
bgholdingltd.com.
saga.co.uk.
alantra.com.
evli.com.
vpbank.com.
bois-sauvage.be.
bellevue.ch.
linc.se.
vestjyskbank.dk.
coinshares.com.
foresightgroup.eu.
polarcapitalglobalfinancialstrust.com.
asia-focus.co.uk.
diverseincometrust.com.
snb.ch.
pacific-assets.co.uk.
capman.com.
blkb.ch.
numis.com.
brooksmacdonald.com.
omasp.fi.
tm.org.
georgiacapital.ge.
northamericanincome.co.uk.
tincinvest.com.
alandsbanken.ax.
abgsc.com.
pegrocoinvest.com.
vef.vc.
corporate.fundingcircle.com.
mattioliwoods.com.
sb.lt.
fidelity.co.uk.
bancodesio.it.
bmogam.com.
abc-arbitrage.com.
b2holding.no.
investindustrial-acquisition-corp.com.
bspb.ru.
newdawn-trust.co.uk.
ussolarfund.co.uk.
jutlander.dk.
honeycombplc.com.
mutares.de.
group.tfbank.se.
tmtinvestments.com.
tkb.ch.
banklinth.ch.
eurologisticsincome.co.uk.
ipfin.co.uk.
abrdnchina.co.uk.
trianinvestors1.com.
sjova.is.
uralsib.ru.
invesco.com.
paretobank.no.
baikap.de.
unicornaimvct.co.uk.
pensionbee.com.
lendinvest.com.
xtb.com.
r4.com.
stelliscom.