

How to identify and leverage Lead Users as a stepping stone to bring Bilog's user authentication product to market?

Author
Sushant Narang

Master Thesis
TU Delft

Graduation Committee
Chairs: prof.dr. P.J. French, Professor Dap Hartmann, Arjan van Genderen
Mentor: Jesus Kallegis

Acknowledgement

Firstly, many thanks to the graduation committee. I would like to thank Professor Paddy French and Professor Dap Hartmann for their timely guidance and support. I would like to thank Jesus Kallergis and Bilog for mentoring and helping with the timely completion of this project.

1. Introduction	6
2. Research Question	8
3. Literature Review	10
3.1 Trends in Authentication Technology	10
3.2 Entrepreneurial Concepts	19
3.2.1 Startup Definitions	19
3.2.2 Lead Users	21
3.2.3 SPIN Model	23
4. Company Overview	25
4.1 About Bilog	25
4.2 Product Innovation	27
4.3 Cybersecurity Market Landscape	29
5. Methodology Design	46
5.1 The Approach	46
5.2 Semi-structured Interviews	46
5.3 Data Collection and Analysis	47
5.4 Reasons for using the interview method	47
6. Methodology Execution	49
6.1 Semi-structured Interviews	49
6.2 Collection of Data (post-interviews)	52
7. Conclusion	61
7.1 Future Work	61
8. Self Reflection	62
9. References	63
10. Appendix	74
Appendix A: Questionnaire	74

Abstract

Recently, data breaches have been increasing in many organisations, causing a spotlight to be put on the security practices such as 2 Factor Authentication(2FA) technology and the methods used to protect cyberspace. This has resulted in an opportunity for passwordless authentication technologies. Biloq is an early stage venture which aims to develop hardware and software to provide continuous authentication without the burden of extra login steps that are present in existing technologies such as 2FA. This project aims to identify lead users for Biloq's new product in the cybersecurity space. To answer this research question, first desk research was done to identify current trends in authentication technologies. This was followed by a stakeholder analysis to identify the people who are involved in ensuring the cybersecurity of their organisation, specifically with respect to the robustness of digital systems and how their staff perform authentication on a daily basis. After this, semi-structured interviews were conducted with the identified stakeholders to spot behavioral and preference patterns and narrow down as precisely as possible the type of persona which would most likely be interested to adopt Biloq's new products and services. The final outcome of the project is identification of lead users for this new paradigm of authentication.

Keywords: User Authentication, New Product Launch, Lead Users

Executive Summary

In today's digital world, cloud technology is an integral part of every sector of our economy. The importance of "Data" has risen exponentially in the past decade and has become so important that companies go to great lengths to collect and analyse customer data. The more the data; the result is more insights to offer a better product to gain competitive advantage. As a result of this trend, privacy protection has become a major concern for individuals, organisations and governments, who are deeply invested in ensuring the security of private information stored on computers, the internet and within corporate networks.

In the past couple of years Europe has seen costly data breaches to the tune of up to 2.5 Million Euros. While stories of vigilante groups have floated around the internet, claiming breaches and hacks, reality shows that most breaches have been for the sake of financial gain. Emails and passwords are the easiest targets for these breaches. Sectors such as Healthcare, Finance and Information are the most attractive targets to malicious actors. Specifically, in the Health sector methods such as phishing and ransomware were most commonly used to breach sensitive data.

Within the above mentioned sectors, employees often prove to be a weak link in the overall security operations. For example, when they use their devices on an insecure network, malicious actors can use emails to trick them into revealing their information. Attack vectors such as spear phishing can be used to target careless employees. Another way employees are targeted is when they use the same passwords on multiple accounts increasing the risk of data exposure.

Biloq, an early-stage venture, aims to tackle these security vulnerabilities. It aims to develop technology for making authentication more secure, by offering true 3 Factor Authentication reducing the number of login steps for B2B customers. Motivated by this goal, this thesis tries to answer the question,

Who are the lead users for Biloq's authentication product in the cyber security space and what are their characteristics?

To do so, this thesis implemented the following approach. Investigation of the state of the art authentication technology. This was done to identify current trends and comprehend potential improvements to these existing technologies. Next, the stakeholder identification. This was done to identify potential users using a stakeholder map. Interviews of potential users - This was done to support and validate assumptions that Biloq has about its product development, by further understanding the cybersecurity

ecosystem. These stakeholders consisted primarily of business users and cybersecurity experts ranging from junior level with 2-3 years of experience to experts having 20+ years of experience.

1. Introduction

Ever felt insecure about sending an e-mail to your colleagues? Are you frustrated about recalling too many passwords or your data being misplaced when you send an email. You are not the only one! The theme of this project is to solve the issues of friction and vulnerability that companies and employees face when it comes to existing authentication technologies, such as less passwords to remember, not conducting multiple steps when using biometrics, and being assured that human biometric data is ethically used and equally protected

We live in a hyperconnected world (i.e from businesses to governments) run on data. Everyday terabytes of data is produced. In this data-driven world, identity/verification of the user becomes important. It is important because one needs to be sure the service is given to the appropriate person, while maintaining privacy of other people (for example in the case of health records).

At the same time, bad actors are realizing this (the importance of data) and are attacking more frequently, attacking more businesses (of all types) hence the concept of cybersecurity was born. Cybersecurity can mean many things depending on infrastructure and end points. For interfaces related to people interacting with a digital system, we see user authentication. The evolution of user authentication can be traced back to passwords and today we have biometrics which utilize unique markers of the human being such as fingerprint and eye retina scanning. Following this trend, now we have a combination of biometrics and passwords which is termed as multi-factor authentication. The future is envisioned as exploring new ways in authentication. This blocks and prevents the success of bad actor hack attempts to materialize a breach.

Biloq is an early-stage deeptech venture (startup) which operates in the authentication space and is introducing a novel method of user authentication specifically for the Banking and Financial sector. As part of being a startup it has many challenges such as developing technology, building products and addressing the market.

This paper will focus on the elements required to bring this innovation to market. Specifically, in identifying the lead users/buyers and formulating a persona sketch.

To minimise security risks which all organisations face, extra layers of security are added with a method such as Multi-Factor Authentication(MFA). This has been around

three decades and is used to secure data and provide sufficient authentication. In addition to enhancing security this method is also cost effective. MFA as a concept has been around for some time, but its implementations have differed according to the criticality of the data it is being used to protect(Aaron et al., 2019).

In view of these security vulnerabilities and protection concepts such as MFA, enter Biloq. It is an early stage venture focusing on developing biometric markers, sensor technology, intelligent algorithms and secure access software. They envision a new paradigm of digital security, enhancing the existing user authentication scheme. While most vendors today claim multi factor authentication methods, they actually use multiple steps within a 2 factor setup such as asking a security question and a password. This is not true multi-factor (2FA) as it is just asking something the user knows, multiple times. Thus this is better described as multi-step authentication of a single factor.

On the other hand, Biloq uses a true 3 Factor Authentication(3FA) setup in which they offer 3 distinct accepted identity-confirming factors. A true 3 FA comprises the following components, a Knowledge factor(something to know) such as password, secret question; a Possession(something to have) Factor such as tokens, One-Time-Password(OTP); and an Inherence factor(something to be) such as fingerprint, retina and voice (Mihailescu et al., 2015).

Being an early-stage venture, Biloq has developed a demo product that proves their concept corresponds to Technology Level Readiness (TRL) 5 as per the definition in Mankins et al., 1995. It is seeking to introduce the product into the market in the most effective way in terms of adoption and profitability. To achieve this they want to understand the market characteristics of digital security products focused on user authentication/identification. The challenge has resulted in this project, aiming to find the needed answers and produce a lead user persona sketch for Biloq.

This report is structured as follows, for the first phase, a literature review is conducted into the technological aspects of cybersecurity such as different kinds of authentication systems. The purpose of the literature review is to give an indication what kind of authentication technologies already exist. This is followed by a review and introduction of entrepreneurial concepts such as a startup and lead users. This is done to give the reader an idea about what a startup is and its different stages of growth. For the second phase, the overview of the company, Biloq, is described in its capabilities. This is followed by the execution of market research through semi-structured interviews and analysis of those interviews. Semi-structured interviews are conducted with the relevant stakeholders to know about their digital status quo in terms of behavioral patterns and preferences. Finally, a conclusion is presented along with future work and self reflection.

2. Research Question

Given the introduction of this project, the main problem Bilq is trying to solve is more secure authentication by offering true Three-Factor Authentication(3FA). The introduction of this offering in the market, gave rise to the following question,

Who are the lead users for this novel authentication product, such as one presented by Bilq?

What are their characteristics that a company like Bilq needs to be aware of when planning and executing its go-to-market strategy?

This is a relevant question because Bilq is an early stage startup in the cybersecurity space, specifically working on authentication technology. Being at an early stage and working with an innovation has challenges such as, too much focus on the technology which may lead to the risk in over-engineering or too much focus on the market, that's why at the early stage it is important to balance and find product market fit which means systematically finding those lead users by focussing on the behavioral aspects of potential customers. Its primary task at this stage is to find its first ever customer which has many intricacies. For example, in the case of Nokia's downfall, one of the reasons was temporal myopia(Vuori and Huy, 2015). It was too concerned with the technology and having too many product variants and were too focussed on the sales numbers that they didn't take into account the customers' behavioral preferences.

Given this example of a downfall, Bilq needs to focus on finding the customer with the right characteristics, who will help in developing its innovation and be a great aid in bringing it to the market. To do that it needs to go out in the field of cybersecurity and get to know about the people's behavioral patterns and preferences with authentication technologies. This will help in identifying a potential first customer and lay the foundation for the adoption of its innovative embedded system into the majority market. This first customer is also known as a lead user who is representative of the mass majority which form the authentication market. A lead user is powerful because they help in co-creating the first product. They have this ability since they are first to experience this problem. In addition to helping in the product development they also decrease the risk of failure. They are the first ones to benefit from the innovation. They can also design the innovative product themselves, which makes them an integral part of the innovation process. Some real examples of products that were developed by

these users themselves are, the World Wide Web(WWW), the mountain bike and the sports drink Gatorade(ZAPFL, 2022).

The process of finding these special users is to actually go out in the field and interview people about their behavioral patterns. In modern times, a tool to find and contact relevant people is a social media channel called LinkedIn, which is a professional networking service provider. For the purpose of this project this service provider was chosen and utilised to contact and interview relevant people in the cybersecurity space.

Another aspect, which makes this a relevant project question is that, existing authentication technologies are increasingly proving to be vulnerable to cyber threats which presents a unique opportunity for Bilq to introduce its security embedded system which utilises a 3 Factor Authentication scheme. Focusing on behavioral aspects for a company like Bilq is crucial. The existing technologies clearly seem to be incomplete given the increasing breaches, so Bilq needs to focus on the behavioral aspects of its potential customers, for its innovation to be effective.

3. Literature Review

To begin addressing the question of this project, it is important to discuss certain concepts that would help readers form a well-rounded context of the problem. For this paper, two major concepts are discussed. First, cybersecurity and its aspects are defined. This is followed by a definition of entrepreneurial concepts such as an early stage startup, and lead users which is the central subject of this project.

3.1 Trends in Authentication Technology

Cybersecurity is a broad term. It is defined as the organisation and collection of resources, processes and structures used to protect cyberspace and cyber physical systems misaligned occurrences that injure the existing property rights (DIAKUN-THIBAUT, & PURSE, 2014). This definition of Cybersecurity provides a comprehensive view of cybersecurity and makes its scope as interdisciplinary and not just a technical field.

Within the broader umbrella of cybersecurity, Authentication technology exists to protect cyberspace from cyberthreats. One such threat is called data breaches. Biloq with its innovative embedded system is addressing these threats which plague organisations of all kinds. Let's first look at what are data breaches and what are some protection techniques that organisations are adopting to mitigate such risks.

Data breaches are a threat to all organisations. While they may differ in their type, the impacts are similar which are mostly financial. Over the last decade large organisations have been the primary targets of these attacks. Among the most popular data breaches are fatal attacks called ransomwares, which operate by locking through encryption and asking the organisation for a ransom. The direct impact is mainly financial. The indirect impact is the organisation contacting the victims for investigations. This also causes loss of customers (Hicham et. al. 2019).

Another type of data breach is data leakage, which is a threat to enterprises. This is the loss of sensitive information which can lead to reputational damage in addition to financial losses. This is a detriment to the organisation's long term health. Common types of leaked information include employee data and intellectual property. These breaches have caused serious financial damage, with the average reaching up to 4

million dollars. The Target Corporate network was breached by bad actors and it incurred 248 million dollars in financial loss. The rising volume of data has given rise to data leakages which mostly land in the hands of unauthorised persons. The perpetrators of these illegal activities can be both external and internal. Internal causes include, sabotage by insider attackers and data theft by intruders. External causes include unintended exposure by careless employees (Cheng, et. al. 2017).

In today's highly digital world, these breaches and losses are increasing. Companies are adopting several protection techniques such as multi factor authentication, privileged access control and firewalls which minimise such risks albeit anything can be hacked and security is a cat and mouse scenario. Many large companies which have suffered consequences of such attacks--Equifax, eBay, JPMorgan, Yahoo. These companies were targets of hackers where they were able to access company records in spite of these companies investing significantly in IT infrastructure(Juma'h, et. al. 2020).

Recently the dutch healthcare system has fallen prey to data breaches. Data containing names, telephone numbers, email addresses of thousands of Dutch citizens has been illegally traded on the internet. According to this news all employees had access to the data so anyone could have leaked it. This incident has taken place due to outdated security systems(Loohuis, 2021).

While modern technology has made collection and storage of massive amounts of data convenient and provided economic benefits, this has led to a whole new area of data security and regulations. A survey suggests that an identity theft can cost up to USD 50 Billion, which has been caused by decreasing cost of information technology. (Roberds, 2008).

There have been multiple instances of data leaks, and best practices for how companies should deal with these incidents are still to be formalised. One of the ways to remediate a breach is that companies notify the victims. But this remediation doesn't always happen in a timely manner. For example Uber waited over a year before disclosing a USD 100,000 thousand ransom payment to a breach. There clearly seems to be a tradeoff between timely remediation and a company wanting to safeguard its reputation from these attacks. There doesn't seem to be any standardised way to responsibly handle leaked data (Karunakaran S. et al., 2018).

During the marketing changes, it has become highly essential to enhance the information security system to protect important data and information from theft issues and several types of third-party access. The trend of authentication has helped various marketing industries, especially the information technology sector, to enhance their

working sustainability (Medium.com, 2021). The information technologist has become capable of mitigating critical data breach and theft challenges through severe and crucial authentication techniques. As stated by Shah and Kanhere (2019), technological advancements have developed authentic devices to scan and secure the information of multinational organizations. Figure 1 illustrates the multiple use cases of authentication technology. These use cases are in the domain of Personal Devices, Online Services such as the bank and smart spaces such as co-working spaces.

According to authentication techniques, there are several types of authentication technology, although five major authentication techniques are based on passkeys, multi factor, certificates, biometric and token system authentication methods. Security teams have become able to enable superior firewall techniques against the easier access from third party and hacking groups. These techniques have become highly trendy in current marketing circumstances.

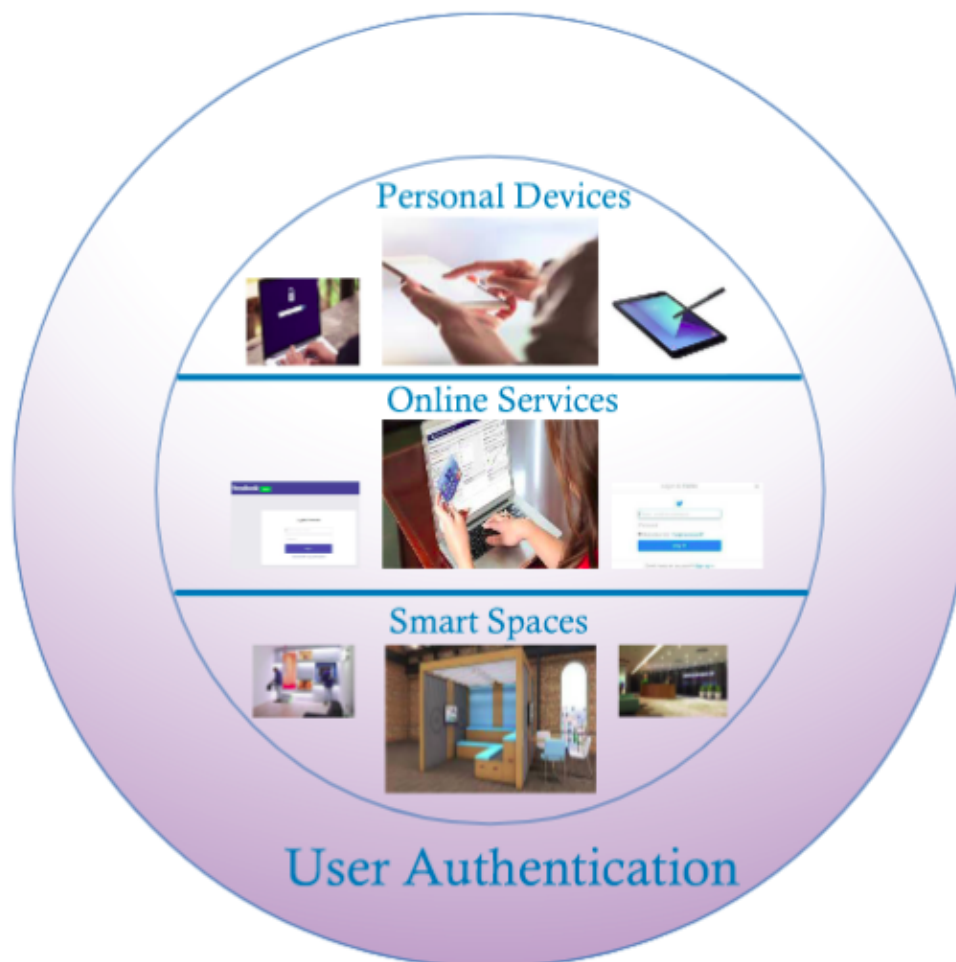


Figure 1: User Authentication
(Source: Shah Kanhere, 2019)

According to *passcodes and passkey authentication techniques*, people and users should use separate passcodes for several online portals and accounts. Utilization of separate passcodes has helped to secure personal and important information from data breach issues (Msp360.com, 2021). However, in the global research, half of the online portal users have utilized similar passcodes for various types of online portals and websites. *Multi factor authentication techniques* have helped to secure the information through two or more authentication techniques in order to build up sufficient security. As discussed by Rui and Yan (2018), multi-factor authentication has helped to construct biometric techniques in reducing the complexities regarding passcode authentication techniques. Figure 2, illustrates the system architecture of a Biometric authentication technology. This architecture consists of three parts, viz., the User Agent(UA) that performs the identity request from the user, The Identity Provider(IdP), which is responsible for verification of the user's identity and finally the Relying Party(RP), which decides the access control method.

Hocking (2010) mentioned that security is based on three fundamental elements: something a person knows, something they own, or something that they are. Both knowledge and possession-based security rely on the user, who is intrinsically the weakest link. The first makes use of a piece of important or memorable information that is frequently forgotten or written down; the second makes use of the physical presence of a key or token at the appropriate time. Since people are more likely to carry many portable devices and interact with, or at least be aware of, other technology in their immediate area at any one moment, there are opportunities to leverage this security potential. Enhanced assurance of security is achieved by utilizing the user's interaction with these many devices and linking the identification knowledge that each device holds separately.

Kennedy & Olmsted (2017) stated that the most important component of any safe cooperative computing system is user authentication. In many cases of multifactor authentication, both a mobile device as well as a desktop are required for proper authentication and must be used together. One of the disadvantages of multifactor authentication is that user IDs and passwords are plentiful, with many users claiming to have more than they can remember. Kennedy & Olmsted (2017) conducted research on a methodical approach to the development of a secured three-factor authentication software that protects user privacy in the most time-efficient and easy manner possible. The study's premise was that a three-factor authorization app could be created without being unduly difficult or time-consuming. The program made use of three-factor authentication, which combines the benefits of authentication based on a password, username, and face recognition with the usage of a mobile device. The results showed that the software worked as expected, with user involvement consisting of entering a

username and password and then having their photo taken, all with a single mouse click. This three-factor authentication tool outperformed expectations for ease of use with its convenience and simplicity.

Velásquez et al. (2018) mentioned that analyzing authentication schemes and multi-factor authentication methods allow for the identification of the main contexts in which they were recommended and even used, as well as providing insight into the criteria used when deciding which scheme or method to be used in multiple settings and the existing frameworks that perform this task. The inherence factor is the most investigated of the three well-known authentication factors, but the knowledge factor is the least explored, maybe due to the prevailing paradigm that the most typical scheme of this component (text passwords) is not very safe.

Gunson et al. (2011) explained that while passwords and PINs remain an effective instrument in the security of automated services when it is used appropriately, the cognitive load of memorizing many passwords and PINs across various apps may become burdensome. When implementing new security processes, caution should be exercised because the changes may affect the service's perceived usefulness. This is significant because consumer adoption of security measures is dependent on usability; if security processes are complicated to use, users will reject them or fail to utilize them appropriately.

Barkadehi et al. (2018) mentioned that given the large number of novel ways to authenticate users, password-based authentication remains one of the most popular. The latest authentication system trends include a mix of two or more approaches. These systems utilize a mix of techniques to differentiate genuine users from imposters. Authentication systems may be classified into three categories: what you know, what you have, and what you are. The summaries of sample types of authentication based on their categories are presented:

Ownership model

1. Physical keys 2. Smart card 3. NFC 4. RFID 5. Hardware-token 6. Cell-phone

Knowledge-based model

1. Passwords 2. PIN code 3. Lock pattern 4. Graphical password 5. Rhyme-based 6. Challenge-response

Inherent-based model

1. Fingerprints 2. Palm 3. Iris 4. Voices 5. Gestures 6. Face

Mix models

1. Two factors 2. Multi-factor

Barkadehi et al. (2018) concluded that authentication systems appear straightforward at first sight, but they are actually rather sophisticated in terms of security, usability, and availability. As badly picked passwords could not adequately protect users, multi-factor authentication systems were introduced in a variety of methods to improve authentication system dependability.

Abhishek et al. (2013) stated that the advancement of information technology has created new difficulties and possibilities for new authentication methods and protocols in recent years. When more components are included in the verification process, the faith in authenticity grows dramatically. Strong Authentication or Multifactor Authentication is when a security architecture uses two or more separate and diverse categories of authentication procedures to strengthen the protection for proper authentication. Multifactor authentication systems are more dependable and effective fraud deterrents when properly developed and deployed.

Sajjad et al. (2019) mentioned that many hybrid approaches exist that combine various aspects to provide comprehensive data and information security. Spoof attacks are methods for fooling a biometric system by delivering a fictitious sample of the individual for authentication. In finger spoofing, on the other hand, the attacker employs molds to fool the biometric system. Various strategies have been explored to address these issues. Sajjad et al. (2019) developed a novel hybrid approach for ensuring the user's authenticity to the system and monitoring if the user has passed the biometric system as a genuine or faked one. Tier-I employed fingerprint, palm vein print, and facial recognition to match with the respective databases, whereas Tier-II used anti-spoofing convolutional neural networks (CNN) based models to identify spoofing.

It can be stated that multi-factor authentication techniques have helped to create several types of layers in overall information security to protect data from breach and theft issues (Searchsecurity.techtarget.com, 2021). Generating particular coding techniques, people and users can easily find out their lost information and personal devices.

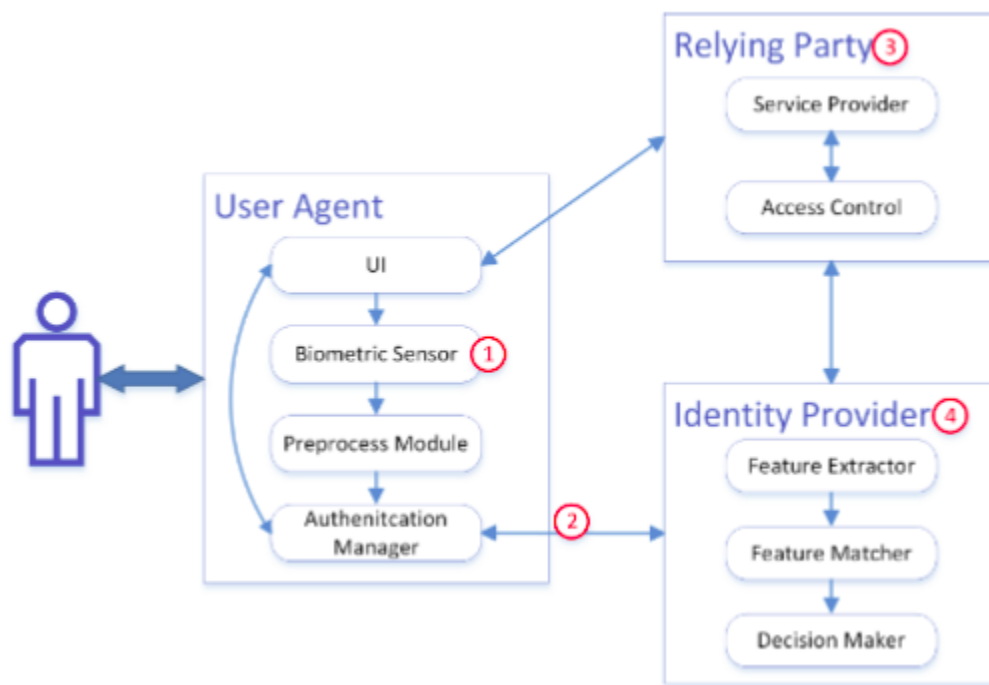


Figure 2: Biometric Authentication structure
(Source: Rui and Yan, 2018)

Besides that, various online devices have become secured through *digital certificates* which have unique coding structures. Moreover, this digital certificate has been owned by multinational organizations and information technology sectors. According to Hummer *et al.* (2018), IT infrastructure technologists have become able to build up IAM techniques to reduce the impact of digital challenges regarding data breach and theft. IAM stands for Identity and Access Management, and it is a technique used to tackle misuse of access by insiders. Figure 3 illustrates the IAM scheme, whose function is twofold, first it confirms user identity, with username and password credentials. Next to that, it provides a layer of authorization by categorising access into editor, viewer and commenter("What is IAM?", 2022).

Another technique which is used is, the Ge-certificate specialisation technique has been used in various Dutch organizations through smartphone and smart devices techniques. One of the most trendy and efficient authentication techniques is biometric procedure, which has been conducted based on facial and fingerprint realisation, eyeris scanning technique and speaker recognition procedure. These techniques have helped to reduce time consumption and the complex structure of passcode authentication procedures (Pciguru.wordpress.com, 2021).

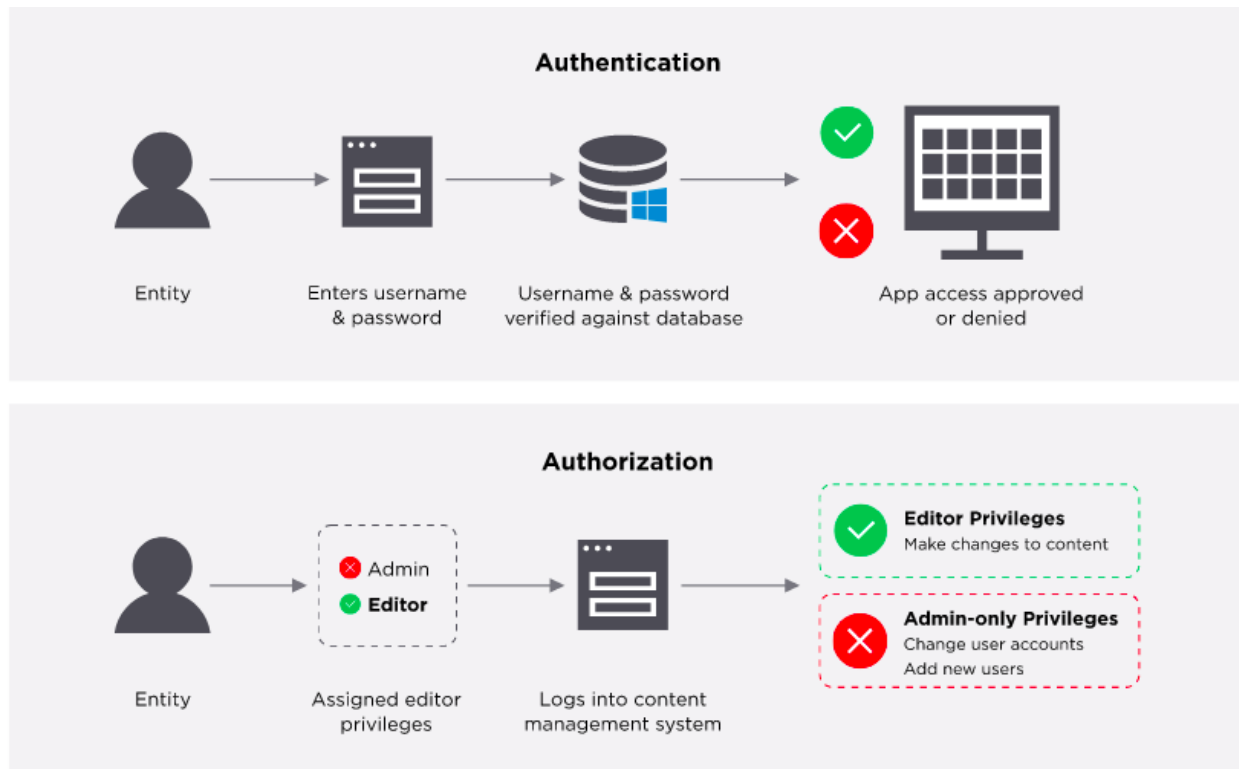


Figure 3: IAM Authentication
(Source: <https://www.onelogin.com/learn/iam>)

Due to obtaining a separate fingerprint, eyeris structure, voice and biometric structure, it has become the most competitive and secured authentication technique for the information technology sector and other industries. As argued by Wang *et al.* (2020), traditional multi-factor authentication techniques can create vulnerable situations that can be declared as a reason for task and effort disruption. *Token system authentication* techniques have assisted in building up separate encrypted strings for users to utilize devices and online portals. This has guided the REST API technique to become generalized through authentic data structure and to gather access to digital portals and websites. Considering the current trends of authentication technique, it can be constructed that the trends of biometric authentication procedures will be highly beneficial in the upcoming future generation. Superior technological innovation has helped to stabilize the efficiency of biometric procedures.

Biometric Technology

Biometrics as a technology has been there since 1960, the accuracy of scanning was almost 100%. In 1975 the FBI in the USA funded the first scanners. By the 1990s other

government organisations funded the biometrics containing face recognition algorithms. The 1990s was the flourishing time for biometrics. In the 2000s, facial recognition was being used to scan travel and other machine readable documents. The shift towards consumers using biometrics took place in 2013, when Apple came up with its new iPhone 5S. Their TouchID technology allowed customers to unlock their devices and make payments. In 2010, Samsung also made their smartphones with fingerprint scanners. Biometrics have been given a huge boost, biological traits are almost impossible to replicate. The individual technologies which bundled together to form biometrics in its current form, are scanning sensors and the smartphone, which became ubiquitous. Experts suggest that there would be more options with biometrics such as, heart-rate detection and devices which can identify a person based on their walking style. (LoginID, 2021)

Jain & Kumar (2010) explained that biometrics is defined as the process of automatically recognizing people on the basis of their distinctive physiological (fingerprint, face, iris, and others) or behavioral (voice, stride, signature, and others) characteristics. Any physiological or behavioral trait can be classified as a biometric trait if it meets the following criteria: i) Universality: possessed by all humans, ii) Distinctiveness: discriminative among the population, iii) Invariance: the selected biometric attribute must be invariant over time, iv) Collectability: easily collectible in terms of the acquisition, digitization, and feature extraction from the population, v) Acceptability: refers to the population's willingness to submit that attribute to a recognition system and the imposition of real constraints in terms of data collection and guaranteeing high accuracy. vi) Performance: refers to the availability of resources and the imposition of real constraints in terms of data collection and guaranteeing high accuracy. vii) Circumvention: someone who is prone to imitating or mimicking others in the scenario of fraud attacks against the identification set-up.

Unar et al. (2014) mentioned that Verification, Identification, and Screening are the three modes in which a biometric technology works. Positive recognition is a term that is frequently used to describe verification. After providing the biometric signatures to the system, the user claims a specific identity using a PIN, login username, and other methods. In return, the recognition system verifies or invalidates the user's claim by comparing the provided biometric signature to the registered biometric signature linked with that specific identity in a 1:1 (one-to-one) matching. In identification mode, the system seeks to identify the user by matching the provided biometric signature to all of the enrolled signatures throughout the database using 1:N (one-to-many) comparisons but without the user claiming a particular identity. In negative recognition, where the user denies having a certain identity, identification is critical. Screening is an extension to identification and by doing 1:N (one-to-many) comparisons throughout the database,

the biometric system ensures that a specific individual does not belong to a watch list of identities.

Hamidi (2019) stated that the Internet of Things (IoT) is a new trend in wireless connectivity between objects. The essential premise of the Internet of Things is the widespread existence of many types of objects in the local environment. Integration, privacy, and availability are the three primary elements of data security on the Internet. Biometric technology is one of the most important technologies for keeping Internet medical devices secure. Biometric technology has a wide range of applications for the protection of personal and organizational assets, with the primary goal of serving as a suitable replacement for traditional access control systems. Hamidi (2019) suggested a continuous security solution for smart healthcare devices based on IoT and biometrics. In addition, combining biometrics with IoT raises questions for user-friendly design implementation. The study proposed a new standard for integrating biometric technology to construct smart healthcare using the Internet of Things, which includes a high capacity for data access as well as ease of use.

Iqbal & Qadir (2012) mentioned that different biometric systems are utilized for a variety of applications. The first approach is focused on facial expressions. A standard camera may be used to capture a facial image. It is the most widely used biometric for establishing identification. The holistic or global method and the feature-based approach are the two basic approaches being used to accomplish face recognition. The feature-based strategy is focused on identifying particular fiducial spots on the face that are less vulnerable to change, such as the points around one's cheekbones, the sides of one's nose and mouth points around the eyes, and so on. Without localizing particular locations, the holistic method analyzes the complete facial image at the same time. Fingerprints are the earliest biometric approach and a forerunner in identity authentication, having been used for criminal identification since 1896. The basic concept is inspired by fingers with corrugated skin and ridges that go from one side of the finger to the other. These ridges have a non-continuous flow that generates a pattern. Generally, fingerprint recognition can attain a high level of accuracy, which is good enough for both verification and identification. It is a popular consumer product due to its low cost and compactness. The third biometric technique is the image of the hand which is captured from above by a camera when the user places his or her hand on a selected surface. Reference markers or pegs can be used to align the user's hand. A monochrome camera with visible and near-infrared light is typically used to capture the iris picture, which is another biometric technique. The colorful component of the eye, the iris, is made up of trabecular meshwork, a kind of tissue. When inspected attentively, the iris seems to have layered radial lines or mesh. Rings, striations, furrows, crypts, and other features make up the visible mesh, which gives the iris its distinct pattern. A

microphone is used to capture a person's voice for speaker recognition or voice authentication which facilitates voice-based biometrics. The recorded voice must be digitized in order to be authenticated.

El-Abed & Charrier (2012) explained that despite the apparent benefits of biometric systems, their adoption is not as widespread as it should be. The biggest disadvantage is the unpredictability of the verification outcome. The biometric authentication procedure is broken down into three parts. The first is enrolment, which is the act of gathering biometric data samples from a person and then creating a reference template reflecting a user's identification that can be compared afterward. The user's biometric sample and his or her template are matched in the second phase verification, resulting in a score. The third phase in the identification process is identifying the identity of an unknown person from a database of people. Biometric technology, on the other hand, has a number of limitations that may limit its usage in real-world applications. As a result, evaluating such systems is seen as a major issue.

Hamid (2015) explained that biometric technology, as well as passwords, have a long history. With vastly expanded issue areas and huge numbers of possible deceivers online, the shortcomings of every one of these methods have become obvious in current security implementation. Biometrics have indeed been offered as a password replacement, addressing some of password technology's fundamental weaknesses. However, putting entire faith in biometric technology might lead to its own set of issues. Biometrics, which range from voice recognition to fingerprint technology, address some of the problems in current password systems, but they also pose new issues in a number of areas. The majority of these issues boil down to one major flaw, which is also one of biometric technology's major strengths: people are naturally messy, living creatures.

3.2 Entrepreneurial Concepts

In this section, entrepreneurial concepts are defined which are applied to the context of bringing Bilog's new technology to the market. These concepts are defined for the purpose of clarifying that Bilog is a startup in the incubation stage.

Firstly, let's define a startup.

3.2.1 Startup Definitions

Entrepreneurs define a startup in myriad ways. These definitions are as follows,

"A startup is a human institution designed to create a new product or service under conditions of extreme uncertainty." - Eric Ries - Entrepreneur and Author The Lean Startup

"A startup is the living embodiment of a founder's dream," - Wil Schroter - Co-Founder and CEO Startups.co

Technology Entrepreneurship

This concept is creatively outlined by Bailetti as follows:

"Technology entrepreneurship is an investment in a project that assembles and deploys specialised individuals and heterogeneous assets that are intricately related to advances in scientific and technological knowledge for the purpose of creating and capturing value for a firm." The definition of Bailetti is based on four different elements (Bailetti, 2012b)

1. Ultimate goal. Capturing and creation of value are identified as goals of tech business development. This is so, since there can be different sources of value capture and creation.
2. Target of the ultimate goals. The company is the target organisation for which value is created and captured.
3. Mechanism used to deliver the goals. A company is an inventory of resources(employees and assets). It delivers the ultimate goals over time.
4. Interdependence with science and technology advances. The employees immersed in a project are affected by the creation of scientific and technological knowledge. The company utilises science and technology knowledge. Individuals external and internal to the company produce its outputs.

New Technology Venture

Another concept associated with technology entrepreneurship is a New Technology Venture(NTV).

The concept of NTV's can be defined as:

"Emerging business entities during their early development and growth with exploitation of technologies and transforming such technologies into new products or services for rapid business growth and development." - IGI Global

Some criteria for an enterprise to be qualified as an NTV, are as follows, it should be in early development phase, there should be a technology involved, it must be bringing a new product or service to the market and finally there should be business growth associated with its new solution. Song et al. (2007) uses the following creative terms: new, adolescent, young, emergent and high technology, technology-intensive and technology-based to present NTVs.

Startup Phases

Startups have different phases according to their maturity. Santisteban and Mauricio (2017) give the following overview. Startups create different phases as they grow and progress. Santisteban and Mauricio (2017) give the following overview. When the enterprise is just starting, it is considered to be in the phase of Incubation also known as Seed or Emergence. After this comes the phase of Early/Young, finally followed by the phases of Growing/Post-Incubation heading towards Maturity and Expansion. In the project, this definition is preferred as it clearly distinguishes the phase of Incubation, which matches the case of Biloq.

For the purpose of this project a boundary has been drawn between early stage and later stage startups. The following terms characterise the early and later stage startups; at the early stage, there product development along with extensive testing with some revenue and mostly depending on external funding and grants. This is followed by the later stage, in which the revenue streams have been established, and there are multiple product lines along with product implementation.

Definition of Success

The literature review of Santisteban and Mauricio (2017) discusses the different aspects such as the growth aspect present in most definitions and concludes with the following definition for success:

"A successful startup is considered a new company that offers products and/or services capable of being well received in the market, looking for a repeatable, profitable and scalable business model, generating jobs or managing to transform the way people do things." Throughout this research, the definition of Santisteban and Mauricio (2017) for success will be used.

This is a comprehensive definition which encompasses both profit and success in product implementation. In the context of an early stage startup the definition of success is more focussed on product development and adoption in the market. The aspect of profit and scale become important for later stage companies.

3.2.2 Lead Users

This section defines the concept of a lead user which is a great aid in finding Bilog's first customer. This concept also gives an indication of who to interview during the lead user development process and what are their characteristics.

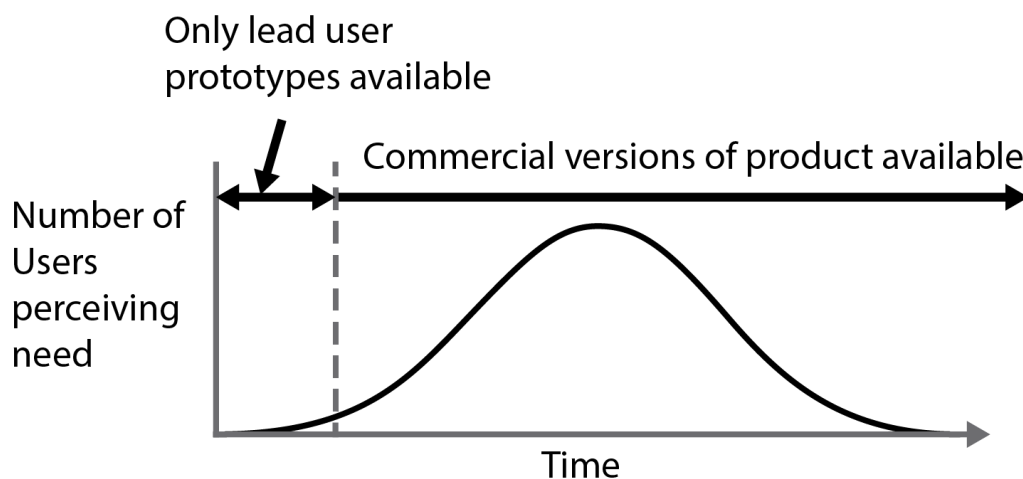


Figure 4: Lead Users Overview
(Source: <http://www.leaduser.com/#research>)

Lead users(LUs) are the ones who display strong needs before the mass majority of the market. They serve as a needs-uncovering laboratory for market research as shown in Figure 4. This figure provides a zoomed out overview of lead users who are ahead of the mass majority of the market in experiencing the need for a solution. They also act as potential customers which provide valuable product development insights. Lead users do not have to be the ones to use the entire product, they can be leading with respect to just a few product attributes (E. Hippel, 1986).

LUs are characterised by, firstly they have needs years earlier than the mass market. Secondly, they receive benefits from this initial solution, thus contributing to the innovation (Marzouki et al., 2019).

Churchill et. al., 2009 suggest three types of lead users,

- 1) Lead users in the target market;
- 2) Lead users of similar applications;
- 3) Lead users that have attributes of the main problem faced by target market users.

Churchill et. al. 's definition of Lead User's comprehensively covers aspects of lead users. In this project, lead users for Bilog's cybersecurity novelty are interviewed with the technique of semi-structured interviews. The importance of lead users is that they represent the majority target and help in gaining insights for a commercially successful

product.

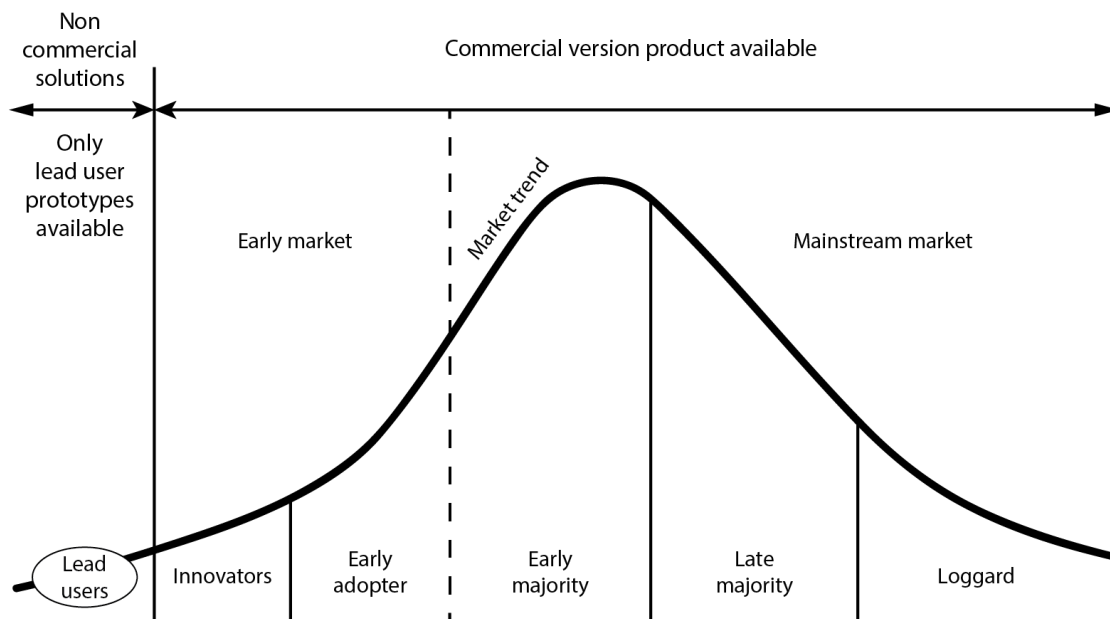


Figure 5: Lead Users (von Hippel, 2005)(Zoomed in)

Lead users(Figure 5) often start innovating on their own and their ideas are more attractive and successful(Globocnik & Faullant, 2021). Figure 5 gives a zoomed in view of lead users clearly highlighting that these users are even before the innovators. Now that the concept of a lead user has been defined. The purpose of this project is to actually find lead users for Bilog's novelty.

The most common approach to finding lead users is to conduct semi-structured interviews, so this method was chosen for the purpose of this project(Pajo et. al., 2015)

3.2.3 SPIN Model

To analyse the conversations with potential lead user(s), various frameworks exist in literature. Frameworks such as, contextual, reveal the situation and problem of the interviewee. The evaluative and the diagnostic frameworks reveal the implications of the problems identified, for the interviewee(Ashton, 2014). After finding these frameworks in literature, the company supervisor also suggested investigating selling frameworks.

Upon further research, the SPIN model was found, which seemed to comprehensively cover the attributes of the aforementioned frameworks.

This model is useful because it helps in decomposing the behavior of the interviewee and provides insights for product development. The SPIN model stands for; Situation(S) of the interviewee. The S questions ask about the buyer's existing situation i.e. how and what is their current way of working in solving problems. Problems(P) faced by the interviewee. The P questions are asked to uncover pain points that the customer is facing along with the hidden problems and implied needs. Implications(I) for the interviewee, the implication questions are for investigating what are the effects of the problems, such as a time or a financial loss. N stands for needs of the interviewee; these questions help in evaluating the effectiveness of the solution. The questions about needs are also for offering solutions in the buyer's words with products/services of the seller (Rackham, 1988). The way this model works is after receiving the responses, they are categorised into S, P, I or N to get a clearer picture of the interviewee's situation.

The SPIN model was chosen because it consists of asking the interviewee open-ended questions. The S questions ask about the buyer's existing situation i.e. how and what is their current way of working in solving problems. The P questions probe into the customer's pain and aid the prospect to identify their problem. These questions also give an insight into implied needs of the customer which sets the stage for the next set questions. The I questions, talk about the consequences and effects of the problem, aid in developing a motivation to buy from the buyer's perspective. The N questions, ask the buyer to explain their explicit needs and match with the benefits the solution is offering. Through these questions, the buyer realises the benefits of the solution themselves.

Next, the young company Biloq is introduced along with its innovative offerings, and its use cases and benefits.

4. Company Overview

4.1 About Biloq

This early stage venture, Biloq, wants to serve financial institutions as their lead customers. These institutions include both big and small banks and trading houses. This company wants to make the IT Directors, COOs, CISOs sleep more peacefully at night by solving data breaches. These breaches lead to considerable financial losses along with reputational damage. They claim to provide stronger authentication which is easy to install, easy to use and does not delay workers. They want to help their customers solve their security needs by redesigning existing hardware. This hardware will have multiple sensors so that the device captures both more layers of authentication and stronger identity factors.

At present, their potential customers haven't been able to solve this problem because no one is offering true 3FA. Current authentication platforms provide limited functionality when it comes to checking identity factors. They only check one other factor and are not able to check multiple at the same time. From a hardware device perspective, these devices are limited to one or two factors. These devices are only compatible with mainstream authentication schemes such as One Time Password(OTP) and Fingerprint(FP). From a data communication standpoint the server calls that occur are outdated. To check multiple factors, it would happen sequentially which further delays this process.

In view of the above mentioned issues, Biloq has identified the following measurable outcomes that their potential customers will achieve:

1. Save time from Authentication process
2. Provide more security checks during authentication by
 - a. Authenticating more times in a given day
 - b. Verify identity of user with more factors during an authentication event
3. Reduce time/occurrence of lock out
4. Transparent logs of authentication
5. Storing/handling of private data (identity, or biometrics) is fully encrypted, not part of network
6. Provide savings to companies, by preventing loss of millions of dollars due to disruption or fines

To acquire these customers, Bilog aims to undertake customer acquisition through the following channels. They plan to approach IT suppliers and supply chain partners of System Integrators within the domains of Identity Management and User Administration. They also plan to approach partners of Cyber Security Operational Centres. They assume their beachhead market will be Financial Services, specifically, the IT departments in those organisations. However, the exact persona that should be targeted is unclear and is the subject of this project.

After acquiring customers through these channels, Bilog wants to offer their value proposition through a Subscription Pricing Model. They will offer a software license, with a one-off fee on the hardware. Along with that they will charge a consulting fee for project assessment and setting up the project.

Cybersecurity is a competitive landscape with many offering a particular product with a combination of services. Figure 6 illustrates the vastness of cybersecurity with its myriad verticals.

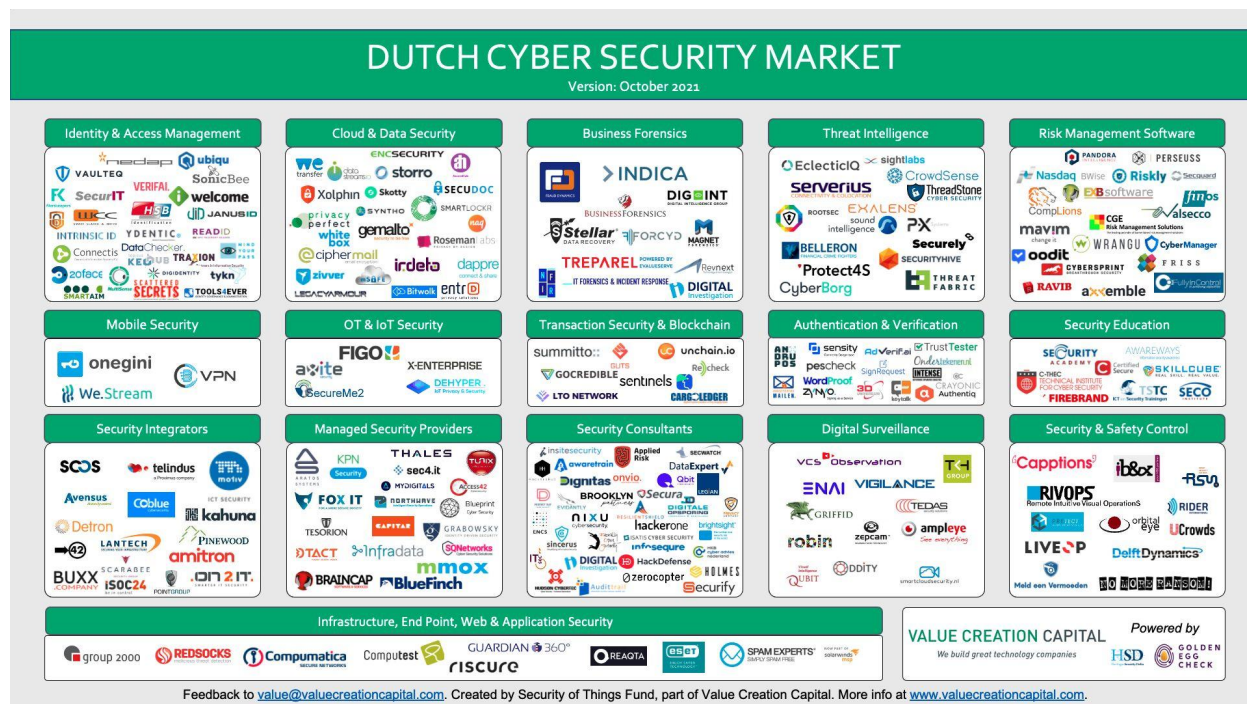


Figure 6: Dutch Cyber Security Market
(Source: Security of things Fund)

Bilog sees the following firms as their competitors. These are mainly authentication

software platforms such as password managers and generators, for example, LastPass. Other software platforms include DUO and Authy which offer 2 Factor Authentication. In terms of biometrics, Thales is a big competitor. Finally, their primary competitor is Yubico, which offers a strong 2 Factor Authentication(2FA).

What differentiates Biloq from their competitors is, they offer a holistic solution which is a combination of software and hardware. Their solution is easy to use and faster to authenticate. They incorporate privacy by design instead of storing biometric data.

While it has a clear competitive advantage, its risk to financial viability comes from a complex solution requiring multiple partner suppliers resulting in a dispersed supply chain. The complex solution also leads to a high cost of time and effort to present a comprehensive solution with total integration. Further, unclear MVP requirements add to the high costs of making assumptions.

4.2 Product Innovation

Biloq has redesigned the verification process, so that the user knows that the device is performing authentication without experiencing any delay in their workflow, while making it exponentially more complex for bad actors. There is no reliance on existing security markers, or methods of implementation. Instead, Biloq uses proprietary sensor technology and intelligent algorithms to introduce multiple, next-generation (behavioral, physiological) types of identity-confirming markers across the full spectrum of authentication factors (knowledge, possession, inherence) that are distinct, obscure, dynamic and encrypted.

Biloq is able to combine ultimate security with unmatched simplicity by optimally embedding its sensors in devices dominating the human-to-machine interaction and are most-used by knowledge workers, ensuring that markers are retrieved simultaneously and continuously.

Finally, Biloq is committed to delivering stronger connectivity through “trusted” integrations with the most common business applications and services for establishing their privacy-grade verification decision during the login process.

Biloq is developing the needed hardware and software together, ultimately making an ecosystem designed to protect critical business assets from unauthorized access in real time. This protects network owners and users from cyber attacks and data breaches.

Biloq provides continuous liveness user verification through sophisticated and adaptable Multi Factor Authentication(MFA) methods in ways that fit well with people's existing habits of use. This ultimately prevents hackers from exploiting the weaknesses of human nature to gain unauthorized access to entry points or resources required to execute an attack.

Biloq's solution provides a robust framework designed to improve trust through strong authentication, verification and identity management. Their first product to market is the B-mouse, an intelligent authentication mouse establishing a new verification standard to protect critical business assets. In the B-mouse 2 physical biometric markers are recorded and combined for identification: the fingerprint and the finger vein. The goal is to continuously identify the correct user and to reduce the number of identification attacks. After all, the finger vein can only be traced back to the correct user. The product has a hardware component and a software component. The development concerns an optical computer mouse with multiple sensors to identify and record the required characteristics/attributes of 2 physical biometric markers (fingerprint and finger vein) in one movement. The captured biometric data is then processed separately and jointly (fusion method) using advanced identity matching algorithms in 3 layers of authentication and integrated into a multi-factor authentication system to provide access to digital systems. In a successful development, Biloq wants to further expand the authentication system with other authentication layers such as behavioral factors.

However, it is important to note that their software products are compliant with existing software standards and are developed with an open systems architecture. This means customers are not tied to one technology or device but can mix and match devices, yet enjoy the increased authentication service from their software.

Use case and benefits

Biloq is developing technology (hardware and software) that will allow authentication to happen in a more secure yet more frequent manner but also become unnoticeable, so much so that an employee will not be able to notice it.

For companies to adopt and use Biloq's solution will be required to configure Active Directory or other digital system to authenticate with Biloq's software. Then they will provide a Biloq compatible hardware to each employee, who will perform work and access digital systems through that device, but be simultaneously authenticated.

The way this benefits the customers is, companies will be certain that the data in their corporate systems will be accessed only by employees whose identity is checked in a stronger manner, and is also checked frequently.

Biloq's solution makes user authentication 4 times more secure, 6 times faster, and available in real-time. With this companies benefit from limitless productivity of their employees, and reduce their exposure to data breaches thereby avoiding the cost of operation disruption and fines.

Initially, they are bringing a complete solution including a smart device and an authenticator software platform which will shift the way user authentication is provisioned in corporations, employees and their digital systems. Once launch is successful it will give way to an ecosystem and new approaches of authentication broadly. At first, more devices can be used from other vendors to be compatible with the Biloq authenticator. Then, they can look at applying the authenticator platform to additional scenarios (mobile, wearables etc).

The working principle of finger vein recognition and finger vein matching has made its way into the literature. The novelty lies in combining biometric data from fingerprints and finger veins (and eventually behavioral factors) in a multi-factor authentication system to find out the identity of the correct user. This concept does not yet exist and is not known in the literature. In this way, the security system can find out at all times whether the person operating the mouse should actually have access.

4.3 Cybersecurity Market Landscape

This project started to get a broader view of the cybersecurity landscape. First a desk research was conducted about the latest trends in the cybersecurity space covering different industries. The research question mentioned above also required an understanding of the various stakeholders present in this space.

In less than a decade, cybersecurity has turned into one of the extremely critical systemic issues in the global economy. Cybersecurity is more often interpreted as a strategic problem of the state, which affects the country's economy and the interaction of national developers of software and control systems, manufacturers of equipment, and components to provide information and communication technologies (ICT) infrastructure. At the same time, the digital economy is developing, and this economy's formation and development are due to the active use of modern ICT in economic processes.

In 2020, according to Mordor Intelligence (2021), the size of the information security or cybersecurity market amounted to 156.24 billion US dollars. It is predicted to attain \$352.25 billion by 2026, with an average annual growth rate of 14.5%. The highest market share is in North America due to the high economic and technological development of the United States. Trends in IoT (Internet of Things), BYOD (bring your own device), AI (artificial intelligence), and machine learning in information security will grow. According to the US Center for Strategic and International Studies and McAfee (2018), cybercrime, which includes data corruption and destruction, theft of money, loss of property, theft of intellectual property, and others, currently made up the world approximately \$600 billion annually, which is 0.8% of the world's GDP.

As the number of Internet users increases in emerging economies (Silver, 2019), the same problems of disinformation and cyberattacks will arise like in more advanced cyberspace countries. The Internet world is becoming more complex and threatening. Many organizations find it difficult to reconcile the level of their investment in cybersecurity innovation with the results of cyber resilience for their business. Even worse, choosing the wrong strategy for investing in cybersecurity technology can cost an organization far more than wasted money. It can damage the organization's brand, reputation, and future prosperity.

There is already a global cybersecurity capacity gap (specialists and workforce in general) (Lewis & Crumpler, 2019), and as new technologies emerge, the gap in cybersecurity skills will widen. In this regard, at present, activities in the field of cybersecurity are becoming a priority and are associated with a business strategy - minimizing damage to IT resources. The growing need for strong authentication methods, especially after the booming remote work trend, provides a lucrative opportunity for the cybersecurity market.

The digital reaction to the COVID-19 virus has also formed new security vulnerabilities. Hackers try to manipulate the gaps that open up when remote workers employ insecure appliances and networks. Threat performers also operate available attack methods to influence people's fears associated with COVID-19. The response to the pandemic has highlighted the vital role that cybersecurity plays in enabling remote operations both during and after the crisis. Cybersecurity teams are being re-imagined as companies rethink their processes and redesign their architecture in response to COVID-19. They should no longer be seen as impediments to growth but should be recognized as strategic partners in technology and business decision-making. It can be concluded that the cybersecurity of the digital economy in a broad sense is determined not only by its protection from cyber attacks and the availability of resources in it that allow it to function in the conditions of their successful implementation but also by the quality of the software of its constituents.

In this regard, Biloq as a 3 Factor Authentication (3FA) solution in the Banking and Financial sector will only benefit the business. Despite the already existing software solutions with AI to ensure banks' cybersecurity, their relative primitiveness and high cost should be noted. Only large banks and financial institutions have enough budget and staff to use AI technologies, while the programs' quality of tasks is still far from being perfect. As financial services organizations increasingly use cloud-based applications and infrastructure, the security architecture must be flexible enough to provide fast, secure, and interoperable public, private, and hybrid cloud services while protecting traditional on-premises services.

1. Breach trends - global

Industry verticals such as banking, education, logistics and information technology industry that have been managing data and information in their organisational system have faced a significant amount of data breaches with their current security approaches for data management (Mordor Intelligence, 2021).

According to Jentzen (2019), 88% of organizations worldwide experienced phishing attempts. This is not just about mass spam mailings but about well-prepared actions aimed at a specific victim. Against the background of the increased activity of various scammers, managers are beginning to abandon the principle that this does not concern us and recognize a problem. The medical and financial sectors remain the most tidbits. For example, according to SafeAtLast (2021), in 2019, the healthcare industry in the US lost about \$25 billion due to ransomware attacks. In 2021, the overall loss provoked by ransomware attacks exceeded \$157 million since 2016. In turn, financial institutions remain the leader in the amount of stolen data and the cost of one leak. According to Accenture, one information incident costs banks about \$18.3 million (Walters, 2020).

According to Mordor Intelligence (2021), the amount of data lost because of breaches grew by 4.7 times in 2020 compared to 2017. According to DLA Piper's latest GDPR (General Data Protection Regulation, 2020) statistics report, the Netherlands, Germany, and the UK rank in the top three for the number of data breach notifications reported to the regulator. From January 28, 2019, to January 27, 2020, the number of notifications per day increased from 247 to 278 compared to May 25, 2018, to January 27, 2019. The increase was 12.6%.

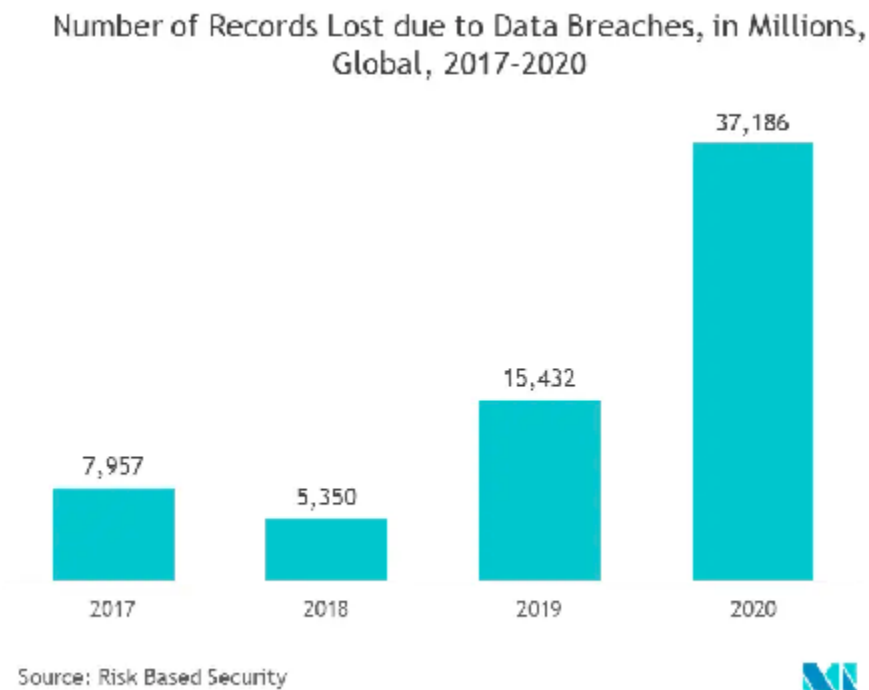


Figure 7: The Chart of Global Data Breaches (in millions) (Mordor Intelligence, 2021)

If 2019 was affected by hacks from Elastics, MS SQL, and other server databases, then in 2020, these breaches gradually became the background, apart from several major incidents and a new scheme implemented by cybercriminals in 2020 to delete the contents of found databases and extort a ransom to restore it. Whatever the ultimate destructive actions of cyberattacks, the most common tools that hackers use to enable an attack to take place are phishing with attachments and fraudulent URLs, the exploitation of vulnerabilities, and not some marginal ones, but relatively high-profile, for example, Zerologon, and weakly protected network-published services, such as RDP, poorly configured security tools (Mordor Intelligence, 2021).

According to Morris (2021), in 2021, 1,291 breaches were recorded, showing a 16.5% increase compared to 1,108 in 2020. However, the largest number of breaches was in 2017, with 1,529 cases. The author highlighted that phishing and ransomware remain the two most widespread hackers' methods. Data from researchers at F5 Labs recorded a 220% increase in phishing attacks during lockdowns in 2020 above the norm in previous years, with 72% of incidents using TLS encryption, making them difficult to

block (Warburton, 2020). The Dutch cyber security industry raises rapidly every year by 14.5%. Among 66,000 IT organizations in the Netherlands, 3,600 retain cyber security as their essential operation, and over 2,500 provide cyber security solutions on the market (Cisco, 2020).

2. Breach trends - per industry

According to Johnson (2021), in the US, in 2019, the Business segment had 43.7% of breaches, followed by the Healthcare sector, with 525 cases out of 1,473, and the Educational share of 7.7%. The Banking segment had 7.3% of breaches, or 108.

Characteristic ↕	Business ↕	Medical/Healthcare ↕	Educational ↕	Banking/Credit/Financial ↕	Government/Military ↕
2013	194	271	54	35	60
2014	263	332	57	38	91
2015	312	275	58	71	63
2016	497	373	97	51	72
2017	907	384	128	134	79
2018	575	369	78	135	100
2019	644	525	113	108	83

Figure 8. The Number of Data Breaches by Industry in the US (Johnson, 2021)

According to the Data Breach Investigations Report by Verizon (2021), the largest number of data breaches was found in the Public sector (885 cases of 5,258), followed by the Professional (630), the Healthcare (472), and the Finance (467) segments.

Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Figure 9. The Number of Data Breaches by Industry (Verizon, 2021)

As the market emerges toward digital innovation in their organisational practices the need for cyber security has increased. The effect of covid-19 in organisational practices has moved the workforce toward work from home opportunities and remote database access. Therefore, all organisations that have been practising digital workforce management have considered innovative approaches and reformed their security management approaches (Duca, 2020).

Figure 8 helps this study to interpret that the market practising digital transformation has gone through data breaches therefore a huge amount of data loss globally and the graph has been increased in 2020, Suggesting that the new transformation towards digital growth needs a better infrastructure in terms of cyber security management as the whole economy has shifted to word industry 4.0. In the time of this covid affected economy, the growth of cybercrime on a global scale has increased significantly (Carataş et al., 2019). Therefore, the new approaches for IoT Security, Identity and Access Management, Unified Threat Management, Endpoint Security, Security Information and Event Management and firewall management can be a possible attribute of adapting better security among the organisational practices for the industry verticals.

3. Consequences of hacks/breaches

Hackers no longer pose a danger to information security in the financial sector since it no longer makes sense to hack into the bank's information system to obtain financial information about a client. Today, search tools are used for searching for an insecure database where information was exposed by mistake, for example, by an insurance organization.

Operators, in turn, who have leaked personal data, will bear the following liability (Sharma et al, 2020):

- Civil, in the form of recovery in a court of losses incurred by citizens and moral damage;
- Administrative, in the form of imposing a fine, suspension, or prohibition of activities related to the processing of personal data;
- Criminal, in case of illegal distribution of Personal Data, which caused significant damage and the transfer of information to law enforcement agencies.

The most substantial damage that a data leak causes is reputational. People begin to perceive the organization as compromised. The changed consumer psychology played a unique role in the new trends - now everyone is aware of the damage that the publication of personal data in the public domain can cause. As a result, buyers and potential customers are ready to vote against companies that do not save data by completely abandoning their products or services. Financial losses from leakage can be direct and indirect. The former include violation of activities, sanctions from counterparties, and fines from regulators. Indirect negative consequences are associated with the outflow of customers.

What can suffer quite seriously is the internal reputation of the security department. Information security specialists will be considered responsible for the incident, regardless of its real causes. This can be bad for the team's effectiveness and introduce additional risks in the long run. The most common decisions of employers in data breaches are reducing the IT department or the security service to a minimum, cutting salaries or bonuses, laying off everyone even remotely involved in the incident (Ettredge et al., 2018).

After a major leak, the chief information officer is usually expected to leave his/her post since he/she is the one responsible for the failure. However, complex systemic problems cannot be solved by removing one person. It will take months and even years for the new leader to reach the same level of experience and understanding of the company, build relationships with colleagues, etc. Like any other top manager, the new chief information officer is likely to make changes to prove him/herself. This will inevitably affect the usual processes and create an additional burden on the IT security department. Usually, such measures have sharply negative consequences. In the best case, the morale of the staff, and as a result, efficiency and profits, seriously drops. At worst, employees begin to quit en masse, losing faith in the employer.

4. Cost of Breaches

According to IBM (2021), the average loss per company from a data breach in 2021 amounted to \$4.24 million. This is 10% higher compared to 2019 data. Within 2015-2021, this amount is the highest.

Measured in US\$ millions

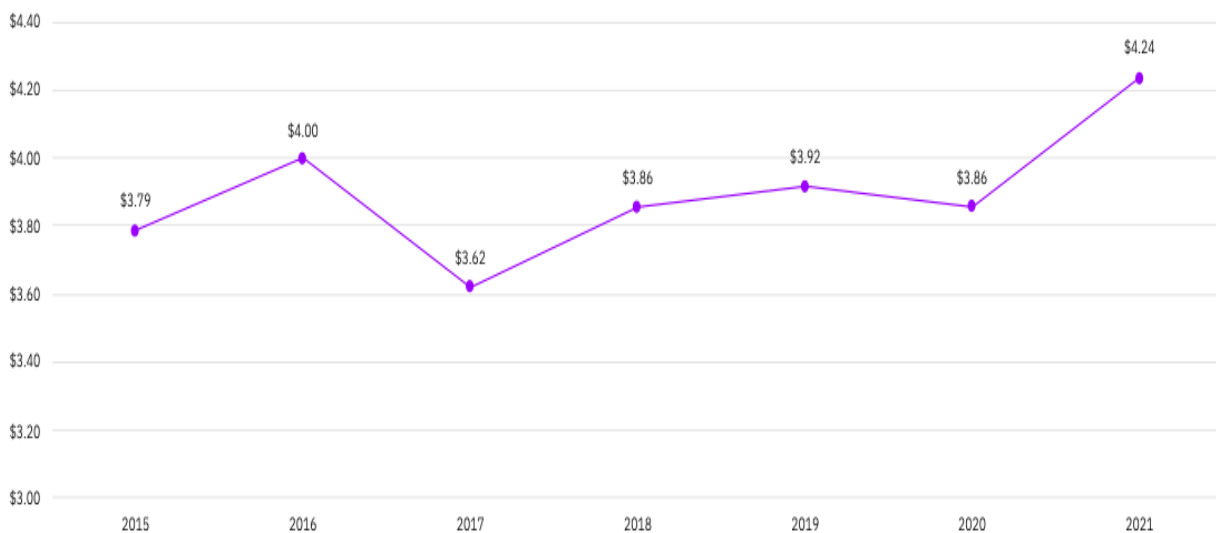


Figure 10. The Average Cost of a Data Breach, 2015-2021 (IBM, 2021)

According to Tunggal (2022), the leading most costly information leak attack types in 2021 are:

- Business email compromise - \$5.01 million;
- Phishing - \$4.65 million;
- Malicious insiders - \$4.61 million;
- Social engineering criminal attacks - \$4.47 million;
- Vulnerabilities in third-party software - \$4.33 million.

Other types are given in Figure 11 below.

Average total cost and frequency of data breaches by initial attack vector

Measured in US\$ millions

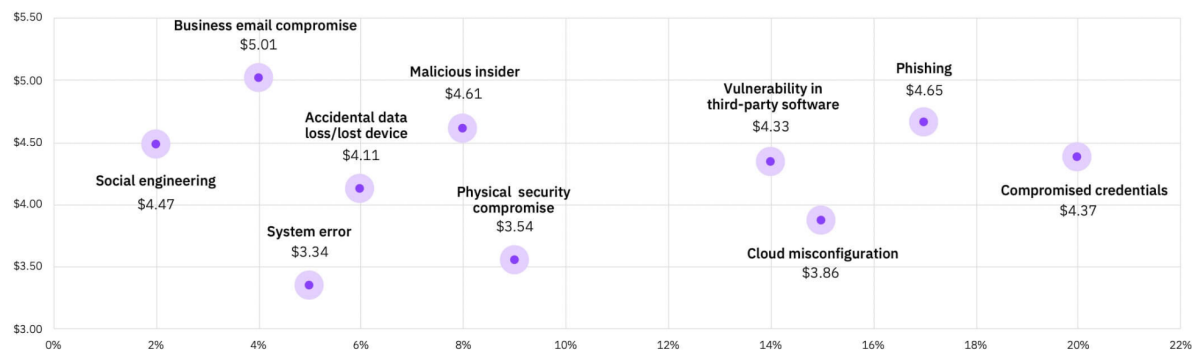


Figure 11. Average Total Cost and Frequency of Data Breaches by Initial Attack Vector

(Tunggal, 2022)

Considering various segments, Healthcare and Financial markets suffered the most in 2021 with \$9.23 million and \$5.72 million correspondingly (Figure 12, IBM, 2021).

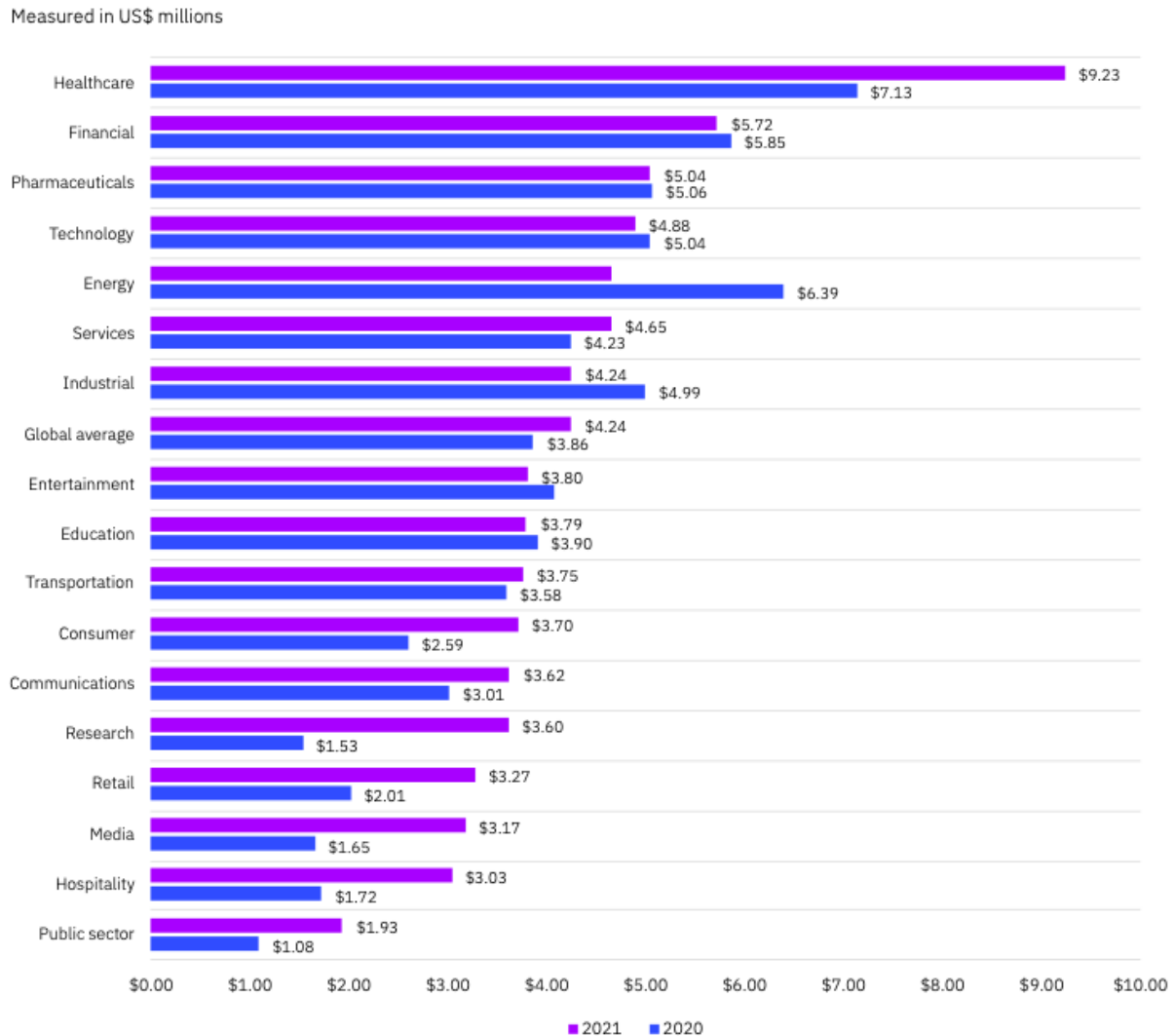


Figure 12. Average Overall Expenses of a Data Breach by Industry (IBM, 2021)

5. Spending on cybersecurity

According to IBM (2021), companies begin to use the Zero Trust model in security systems: a minimum of trust, a maximum of checks. The more devices connected to the network, the more relevant the issue of cybersecurity becomes. The Zero Trust strategic initiative is based on the postulate of never trusting and always verifying and aims to prevent data leaks, increasing the security level of modern information systems. The IT industry initially adopted the concept. Still, now its approaches are also being applied to physical security as security devices become a vital part of the IoT direction.

According to Mlitz (2022), in 2017, spending on cybersecurity globally was \$34 billion, and in 2021, it fluctuated within \$57.7-60.2 billion. According to Bernard & Nicholson

(2020), financial organizations spend 10% of their IT budget on cybersecurity, while medical institutions spend only 5% (West & Skahill, 2021).

The state or certain companies need to periodically take measures to increase the level of IT literacy of Internet users to avoid cybercrime due to human factors. Organizations should pay attention to training financiers and economists in the basics of cybersecurity, increasing their competence in protection against cyber attacks. It is essential to hold various conferences, forums and improve their quality. It is necessary to involve the top IT specialists of the event to share their experience.

Organizations are encouraged to develop economic and mathematical models for predicting the directions of cyberattacks and assessing potential damage (risks) to ensure cybersecurity. It is also necessary to develop information protection systems, optimize file sharing processes, and use special identification systems that determine the availability of information access rights to protect the company's internal network, along with powerful antiviruses and special hardware security modules. Popular developers of protective systems include such market leaders with extensive experience in this area as Group IB, Cisco, and Data Protection Systems.

The new economic development towards the digital revolution has taken the market strategy for more innovation in their organisational practices. Previous identification of data breaches and data loss among the organisational practices in the industry vertical indicates the growth of the cyber security market. Therefore by 2020, the growth of IoT security, machine learning, Firewall management, robotic technology and AI-based security management has emerged (Tewari, 2021). The market for cyber security was valued at 156.24 billion dollars by 2020 And the target expectation by 2026 is 35 2.25 million dollars. Therefore the trend indicates that by 2021 to 2026 the market is about to grow by 15%.

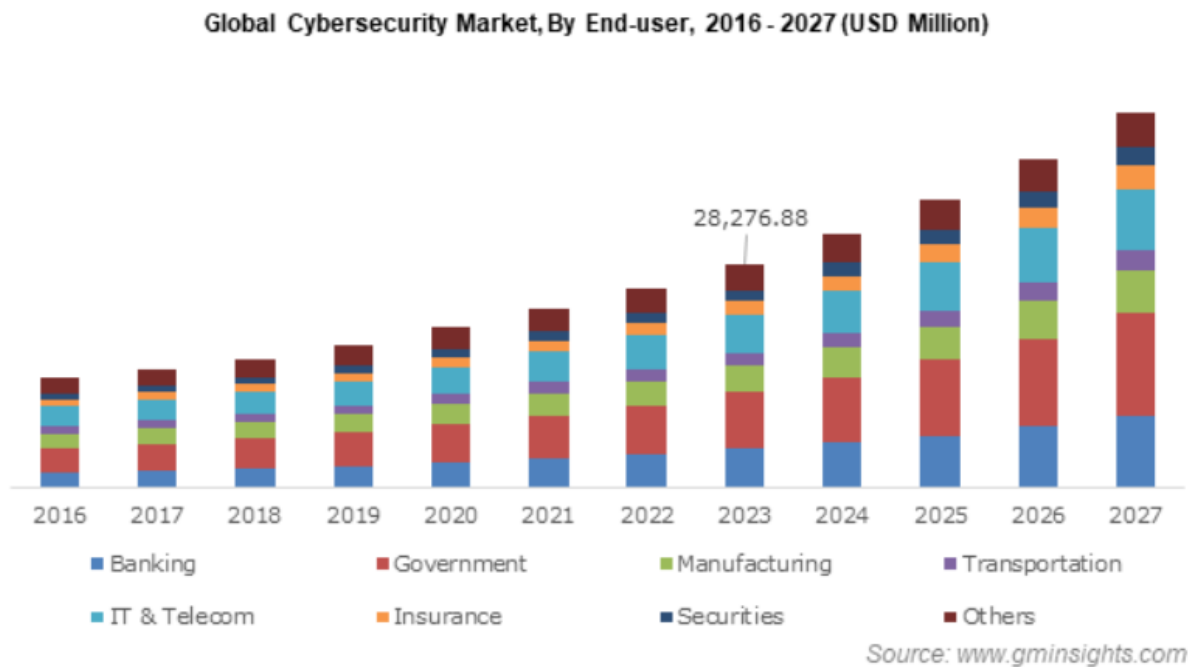


Figure 13. The Global Cyber Security Market with Industry Verticals (USD Million)

(Wadhwani, 2021)

With the increasing growth of Cybercriminal activities demand graph for cyber security and data protection has been increased therefore the graph suggest parameter of increasing growth in the cyber security market Trend as per the industry verticals such as government, banking, manufacturing, IT, insurance and securities (Wadhwani, 2021). Therefore in order to manage the cybercriminal activities in need of robotic Technologies and AI-powered data security management, it has become one of the necessities in overall organisational practices in industry verticals in order to establish better data securities. The covid-19 outbreak also has been one of the influences in the market growth for cyber security. As per Ferreira and Cruz-Correia (2021), the pandemic prevention approaches have moved the organisational workforce and its practices towards remote data management and workforce management, complete and preventive measures in order to manage the organisational workforce as well as employees and stakeholders data protection have become one of the trends in the new economic development.

Measurements for better cybersecurity management in order to avoid data theft, phishing, data losses, Malware and adware intervention has created an emerging platform for digital security companies and software developers.

Banking and Insurance: The increased amount of online activity in the Banking and Insurance sector has created scopes for better security management in order to protect clients' data and in order to protect against any financial loss that a client can face due to cyber security breaches (Jibril et al, 2020). Therefore, the need for a complete cyber security structure and revised organisational practices in the awareness of cyber security has become one of the necessities for the Banking and Insurance sector.

Government sector: The government sector in protecting the data and information must be one of the most important sectors around the globe. Therefore the security breaches in the military, Air Force and intelligence sector has created a great challenge in the overall security management of every country (Norris et al., 2021). Security breaches in the government sector can create great challenges in protecting confidential data and can direct the security system of a country emerging towards many devastating situations. Therefore mitigating the cyber attacks and adapting to better cyber security management has become one of the prime concerns for government and public sectors.

Education sector: As COVID-19 has emerged the whole education Sector towards e-learning and cloud-based data management and data access platform, cyber security in the education sector is on the demand. Data breaches in the education sector can lead the whole education system towards an uncertain future in terms of activities related to cybercrime. As the whole education approach has introduced a digital learning platform, availing computers, mobile phones and the internet has become unavoidable and therefore people of every age group, from kids to adult learners, are bound to access digital platforms in order to complete the education, The education sector must be concerned about the personal data safety of the students and the clients.

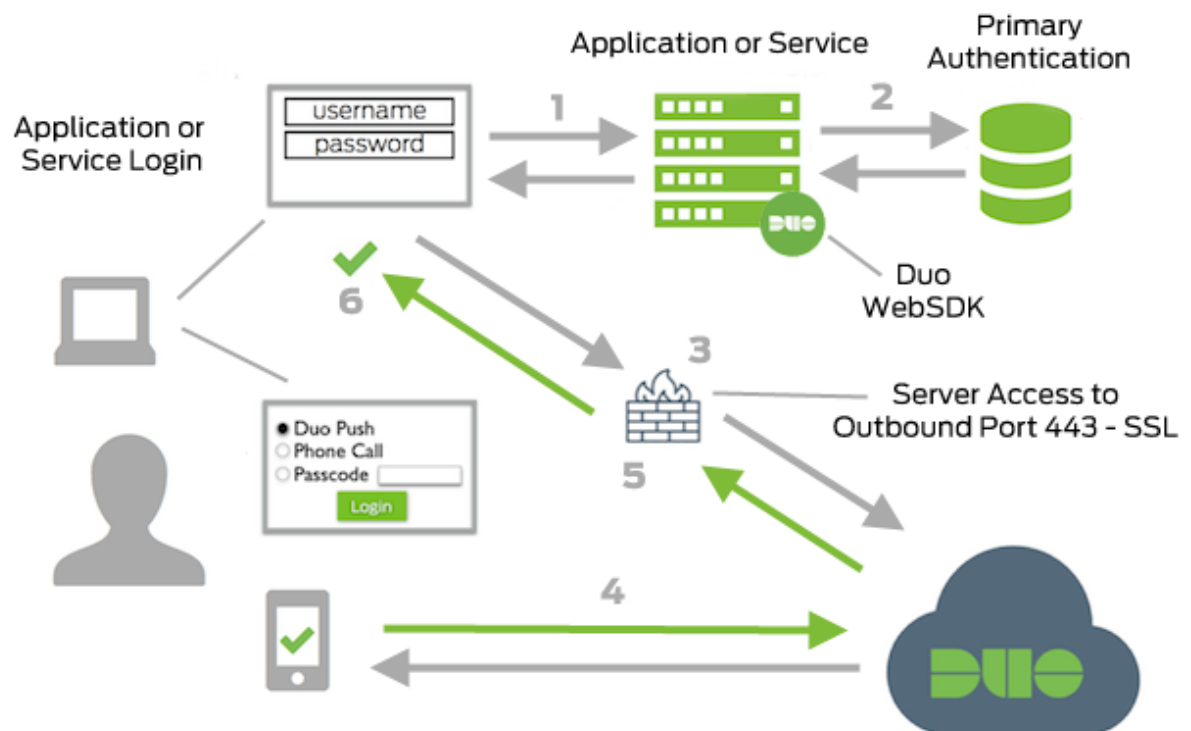
IT and telecom: One of the most suffered sectors in the industry vertical in terms of cybersecurity breaches has the Information Technology Sectors and the telecom sectors. As the Sector deals with the information of people, Security breach in the data management system can be an indicator of serious legal and consequential issues. The IT and Telecom sectors hold many informative and confidential data about the people of a country therefore the data breach can lead to identity theft, serious financial loss And can directly impact the government and public sector in their public welfare management approaches.

Key market approaches: in order to provide better approaches for cyber security management, companies dealing with cyber security and software development have taken the necessary approach to input more security platforms and data management platforms. The key market approach for cybersecurity however has been segmented by user type and component, therefore companies like Cisco Systems, Inc., IBM, ProofPoint, have taken various preventative measures for different user requirements.

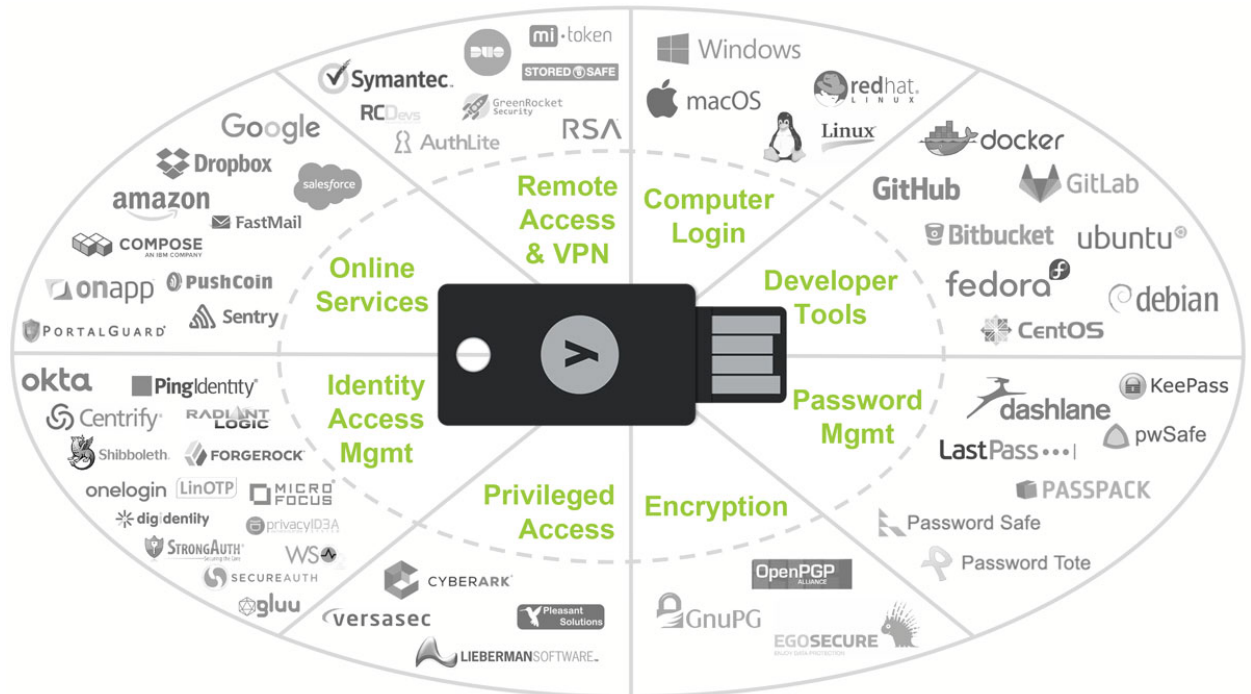
Competitors

Biloq has the following competitors in the user authentication space, namely DUO, Yubico, and Microsoft authenticator.

- Duo Security, Inc. (<https://duo.com>) is a user-oriented access safety solution that delivers two-factor authentication, endpoint protection, remote access programs, and more to save data. The company's software products and services include Two-Factor Authentication and Multi-Factor Authentication in various business sectors. The company has approximately 20,000 clients worldwide, including Facebook, Panasonic, Toyota, etc.



- Yubico (<https://www.yubico.com>) is a Swedish authentication organization, which provides software and hardware solutions and specific services, including YubiCloud, to legal entities, individuals, and developers. Various business sectors apply its products. It services over 4,000 enterprises, including Google, and more than ten (10) million customers in about 160 countries.



- Microsoft Authenticator (<https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a>) is a Two-Factor verification app for mobile tools developed by Microsoft Corporation. This app has over 786 thousand reviews on Google Play and over 146 thousand reviews on AppStore, meaning approximately one million users.








Microsoft Authenticator

Comparison chart

This chart outlines Bilq's advantages as compared to the competitors in the authentication space

Pushing the boundaries of what's possible

Security	Layers of Identity verification	2	2	2	3	One more layer
	Risk Reduction	Low	Low	Low	High	Stronger credential markers
Convenience	Frequent Verification	No	No	No	YES	Continuous
	Available productive time*	86.11%	89.58%	84.38%	97.92%	Unnoticeable

6. Relevance to Bilq

As digital technologies develop, the opportunities for attackers who seek to achieve any political goals or personal enrichment inevitably increase. This is what determines the importance of developing technologies that can provide cybersecurity and creating an

infrastructure aimed at training highly qualified personnel in this area. Knowing Bilq starts from the EU, it makes sense to continue so because market figures for EU and connected to US would allow it to focus in these regions. It makes sense for Bilq to consider the financial services as its beach head seeing the threat incidents, successful breaches, and cost spending in banking.

5. Methodology Design

5.1 The Approach

The approach of this project is designed as follows. It started with drawing up a timeline for all the tasks required to be done during the project. The timeline provided a clear overview of the whole project from start to completion. After this, Desk research was done to gather papers and other reports on the required concepts that serve as context for this project. The desk research also consisted of investigating current state of the art authentication techniques such as 2 Factor authentication and Multi-Factor authentication. These concepts have been there for quite some time but their implementations have changed over time. After this investigation into the problem of authentication, next came who encounters the problem on a day-to-day basis. To answer this question, a stakeholder analysis was done to identify the potential roles that are involved in deciding to buy and use new security solutions, such as that proposed by Biloq. This was followed by contacting the shortlisted stakeholders and interviewing them about their digital systems usage behavior. After analysing the responses, conclusions are drawn to finally present a lead user persona.

5.2 Semi-structured Interviews

The purpose of semi-structured interviews is to find and contact lead users to gain insights into product development for Biloq's innovation.

A semi-structured interview is a conversation between the selected interviewee and interviewer to collect data and information. This interview technique is used to gather the whys and hows of the current situation of the interviewee. The advantage of a semi-structured approach is it allows for flexibility to explore alternate lines of thought(Mannan, Capt. (2020). Semi-structured interviews can consume a higher amount of time and require sophistication from the interviewer's end (Adams, 2015). Additionally, this technique has helped to generalize various relevant aspects apart from few particular critical aspects of identified questions. According to Wan (2021), semi-structured interviews have helped to demonstrate experimental research techniques to generalize the information. Researchers can easily develop a two-way communication strategy to maintain transparency in the entire interview procedure. There is no particular format in building up a semi-structured interview, although the

interview conductor should follow a basic structure in achieving a superior outcome after execution of the entire interview procedure. Besides that, preparation of the interview has been conducted on past experiences and various other articles. Moreover, questionnaires of interview procedure can cover entire aspects from simpler to complex questions. Analysing several patterns, responses have been recorded to achieve sufficient information. As cited by Qu *et al.* (2019), semi-structured interview analysis is used to conduct thematic analysis and qualitative research for gathering productive information based on a research topic. Semi-structured interviews have followed a flexible framework in idealizing the aspects of questionnaires (McIntosh & Morse, 2015). According to this particular study, researchers can conduct semi-structured interviews on various managers and employees of information technology organizations in obtaining critical ideas and trends in authentication techniques.

5.3 Data Collection and Analysis

To collect data, the semi-structured interview method was chosen. The questionnaire is attached in the appendix. An interview session took 40 minutes to an hour. After an interview the responses were analysed and some interviewees were contacted again for follow ups to get further clarification on their answers to the questions. In these follow-ups more probing questions were asked about the interviewees' situation and their opinions about authentication technologies. A total of 11 respondents participated in the interviews.

The qualitative interview was transcribed and recorded with the consent of the stakeholders on the condition that the data be purged after graduation. Each interview helped in understanding the current user behavior and gave ideas for improvements.

From the learnings of the qualitative interviews, a SPIN summary was developed to analyse the responses and spot patterns in the responses.

5.4 Reasons for using the interview method

When searching for lead users for an innovation, conducting semi-structured interviews with potential customers in the product domain is the most common method(Pajo *et. al.*, 2015). The semi-structured interview approach was chosen because it provides insight into a complex situation by asking 'why' and 'how' questions. It also gives a comprehensive view from multiple perspectives. The combination of qualitative

interviews with the SPIN summary method gives a complete overview of the cybersecurity landscape and behavior of potential users.

The multiple perspectives in this project are the various stakeholders in the cybersecurity space who have 2 to 20+ years of experience in this field. The SPIN model helps to analyse and gain insights for product development from the responses given by these stakeholders.

The people that were contacted through the social media channel, LinkedIn were chosen based on the following criteria, firstly they should be in the cybersecurity domain, which is relevant to Bilq's product and/or secondly, they are in the Banking and Financial sector, which is Bilq's primary target market.

6. Methodology Execution

A semi-structured interview method was chosen to find lead users.

6.1 Semi-structured Interviews

Qualitative data was collected by conducting semi-structured interviews. To identify the candidates for these interviews, desk research into stakeholders was conducted and a stakeholder chart was made to give a clear view of the cybersecurity landscape.

Within the cybersecurity landscape, the various stakeholders identified ranged from 1 year to 20 years of industry experience. This was done to get a full picture of the cybersecurity space, specifically the space of authentication for logging in and file sharing tools. The questionnaire was designed based on the premise of how secure and convenient users feel about their current tools and is there a better way of doing their security.

To analyse the data collected, a SPIN model was used to gain insights into behavioral patterns. The SPIN stands for, Situation of the interviewee, Problems they are dealing with, Implications they face, Needs they have for solving their issues. The reason for using semi-structured interviews was it provides perspectives from multiple stakeholders in the field. It gives a clear picture of the cybersecurity context. A combination of semi-structured interviews and SPIN model gives a full overview of the authentication landscape.

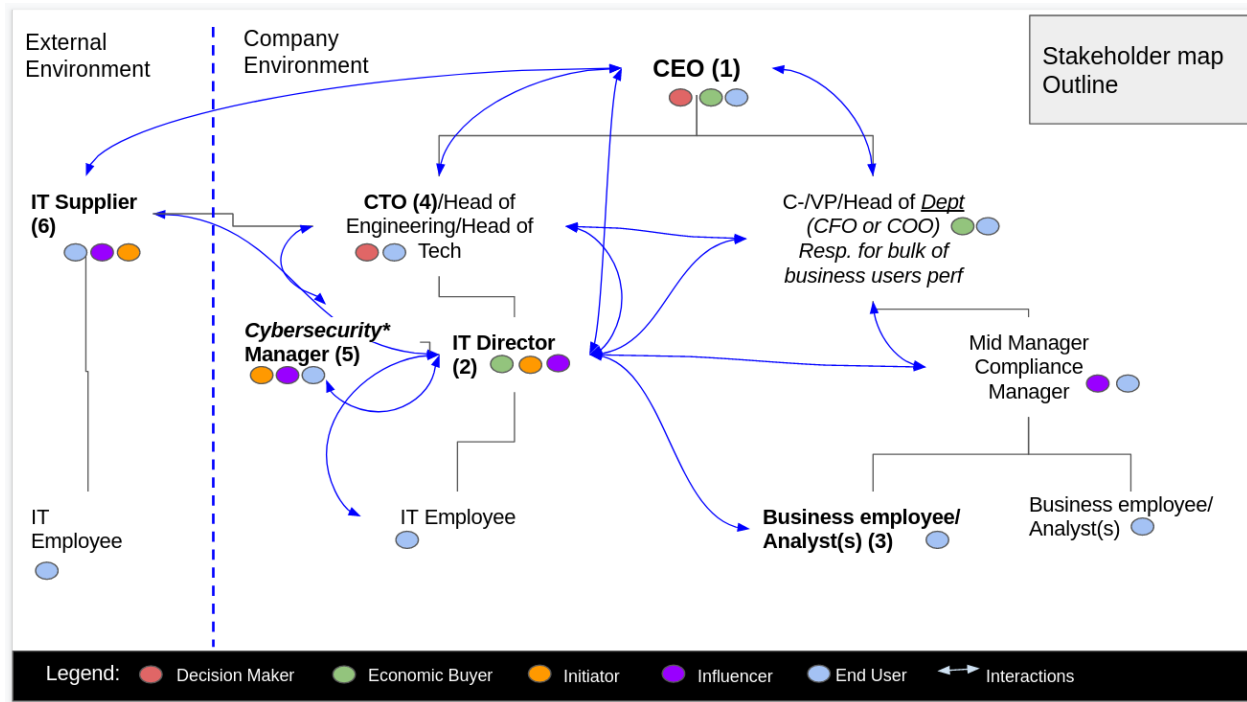


Figure 14: Cybersecurity Stakeholder Map

Figure 14 outlines the hierarchy of a large cybersecurity organisation. The arrows indicate verbal(also e-mails) communication among the various stakeholders. Based on this figure, the following stakeholders were prioritised as shown in Figure 15.

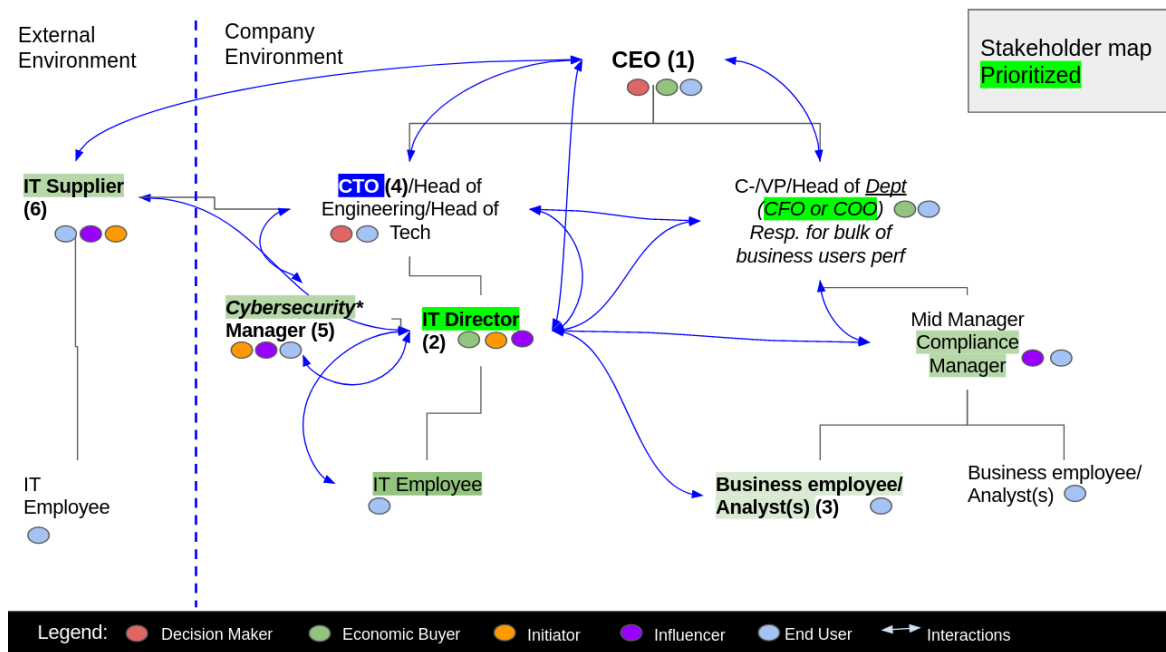


Figure 15: Cybersecurity Prioritised Stakeholder Map

Interviews were conducted with the following 11 stakeholders belonging to different organisations (Table 1.). Each stakeholder is from a different company. Every stakeholder had varying perspectives since they were shortlisted according to their level of experience to give a comprehensive view of the cybersecurity landscape.

The senior stakeholders were mostly annoyed with a lot of passwords and login procedures. While they were open to new technology they were challenged by their internal company stakeholders who were not as open to change. The mid-senior stakeholders were somewhat open to new technology. The junior interviewees appeared quite curious during the interview and seemed open to trying this novelty in their workplace.

Subject	Job Title	Years of Experience
Subject 1	Independent Consultant	20
Subject 2	Program Manager	20+
Subject 3	Associate	1.5
Subject 4	Consultant	3
Subject 5	Consultant	3.5+
Subject 6	Director	12+
Subject 7	CISO	20
Subject 8	Program Integrator	14
Subject 9	Head of Business Development	19
Subject 10	Security Systems Architect	15+
Subject 11	Associate	5

Table 1. Overview of interview subjects with their experience

6.2 Collection of Data (post-interviews)

After developing the persona and the company analysis followed by the product strategy, design of the interview questionnaire was done. For the scope of this project a semi-structured interview questionnaire was developed.

The interviewers were two, one person asking the questions(Biloq) and another person(intern) taking notes. These questions were based on the premise that currently the customers are not using a true 3-Factor Authentication (3FA) security setup, and they are losing revenue which is a cause for concern for both the internal stakeholders of the company such as the CEO and CTO/CISO, and their customers who are worried about their data privacy.

The line of investigation was that the questions start off with a broad view of the cybersecurity measures within its budget and then narrowed down to specific questions about the user authentication setup.

These questions provided a guideline. During the conversation, followup questions were mostly probing into the feelings of the users about their digital status quo to uncover their pains and frustrations.

After asking these questions (QUESTIONNAIRE IN APPENDIX), and analysing the responses the following conclusions are drawn:

1. Most people are frustrated with too many passwords
2. There is a tradeoff between security and usability
3. Not everything requires too much security for example 2FA
4. The level of security depends on the product, for example bank cards require higher security than laptop logins
5. A universal identity removing the use of multiple passwords is the vision for the future

Situation of interviewee	Client gives him PC, he checks mails, calendars, he uses FP on his phone
Key Problems interviewee is dealing with	FP sensor not working on work PC, multiple login procedures lot to handle, he got fed up with windows antivirus so switched to apple product
Implications they face because of the problems stated/ selected	Implication of multiple login procedures is it makes workflow tedious
Needs they have as part of solving the problem	Interpreted need: help him remember passwords, and work smoothly with multiple login procedures
Compelling quote from person to summarize call	"I am glad about FP sensor on private laptop"

SPIN Table 1: Subject 1

Situation of interviewee	Client gives him PC, he checks mails, calendars, he uses FP on his phone
Key Problems interviewee is dealing with	Office politics, too many passwords
Implications they face because of the problems stated/ selected	Too many passwords to remember, convenience security tradeoff, while many of the procedures make it more secure, it adds a load of recalling too many passwords.
Needs they have as part of solving the problem	Universal password linked to one identity
Compelling quote from person to summarize call	'Universal identity and universal password is the dream'

SPIN Table 2: Subject 2

Situation of interviewee	employer gives him PC, he checks mails, calendars, he uses FP on his phone, he uses FP on his work laptop
Key Problems interviewee is dealing with	Mostly new team on every project, takes time to onboard, new tools for every project because every project is different
Implications they face because of the problems stated/ selected	They have governance in place for misplaced files,
Needs they have as part of solving the problem	Good user interface, convenience,
Compelling quote from person to summarize call	'Password less login is trending, but still far away from it being mainstream on a global scale' - he specialises in id and access management so he talk about this for hours

SPIN Table 3: Subject 3

Situation of interviewee	Client gives him PC, he checks mails, calendars, he uses FP and facial recognition on his phone
Key Problems interviewee is dealing with	Keeping projects on track, preventing cyber attacks, cybersecurity is a cat and mouse situation
Implications they face because of the problems stated/ selected	Businesses are worried about ransomware and phishing
Needs they have as part of solving the problem	More awareness to the user
Compelling quote from person to summarize call	Multi Factor is better than multiple single factors

SPIN Table 4: Subject 4

Situation of interviewee	Lot of unstructured data with no one keeping track, this happens during file sharing
Key Problems interviewee is dealing with	Work and phone and laptop have standard security measures but he feels they are not enough from a security professional's point of view,
Implications they face because of the problems stated/ selected	With growing number of MS Team pages, no way to track which file went where so no control, implications may be data breaches and potential for bad actors to exploit unstructured data
Needs they have as part of solving the problem	Data structuring tool
Compelling quote from person to summarize call	He feels it is not enough yet convenient, Growing number of team pages, unstructured data, lying around, not everything needs 2FA, For high security products, security depends on what you are protecting, Be less attractive to the bad actors,

SPIN Table 5: Subject 5

Situation of interviewee	Flexible working even before covid,
Key Problems interviewee is dealing with	He doesn't like knowledge based logins
Implications they face because of the problems stated/ selected	Login to phone is easier,
Needs they have as part of solving the problem	A predictable customer journey
Compelling quote from person to summarize call	One size fits nobody - he believes, A customer journey which is predictable,

SPIN Table 6: Subject 6

Situation of interviewee	First CISO create and implement new cybersecurity policies,
Key Problems interviewee is dealing with	Vulnerability management Security on the phone is not optimal
Implications they face because of the problems stated/ selected	Know what he doesn't know, and put on them a map
Needs they have as part of solving the problem	Update IT infrastructure, Better security for MS tools, data structuring after a working relationship has ended with third parties,
Compelling quote from person to summarize call	Doing biometric is very convenient, Not a fan of passwords,

SPIN Table 7: Subject 7

Situation of interviewee	Laptop from client and employer, login to system, check the first meeting, then move forward, card and password login, password manager on laptop, fingerprint on his personal laptop
Key Problems interviewee is dealing with	He got locked out,
Implications they face because of the problems stated/ selected	Lost half a day in recovering his credentials,
Needs they have as part of solving the problem	Worry about transactional data in the bank, so need protection everyday

Compelling quote from person to summarize call	To him, it should be single sign on for all application and the access should be limited to the privilege level,
--	--

SPIN Table 8: Subject 8

Situation of interviewee	Personal laptop, doesn't work with employer's laptop, remotely connects to employer's work environment, checks her mobile first, she doesn't like employer smartphone
Key Problems interviewee is dealing with	Goes through remote application, requires password and authentication app to login to the bank's environment so one more password after the logging into bank's environment, she is not happy with 3 steps, but has become use to them
Implications they face because of the problems stated/ selected	Having too many passwords is an annoyance,
Needs they have as part of solving the problem	If she could have a single login, just click on, she wants an aggregator,
Compelling quote from person to summarize call	"Authentication As long as i dont realise it, Should be seamless,"

SPIN Table 9: Subject 9

Situation of interviewee	Mail check on company provided laptop, client gives him devices, outlook software for calendars, bitlocker to login, login via windows credentials, FP on his personal phone more secure than 4 digit pin
Key Problems interviewee is dealing with	Microsoft products, not secure, US law precedes EU law, the US govt can read your stuff, SaaS solutions, are not great, He hates office 365, virtual machines are not fast so very inconvenient,

Implications they face because of the problems stated/ selected	Security by obscurity is bad practice,
Needs they have as part of solving the problem	6 functions and beautiful design and usability is important,
Compelling quote from person to summarize call	Empower employees to do smart stuff through user friendly user interface

SPIN Table 10: Subject 10

Situation of interviewee	Uses usually laptop with external monitors, mobile phone for email communications, employer provided devices, uses google chrome, uses fingerprint on laptop and Face ID in the phone
Key Problems interviewee is dealing with	Face ID doesn't work with mask during covid, got locked out of her system
Implications they face because of the problems stated/ selected	She had to go to the office to recover her password.
Needs they have as part of solving the problem	Fingerprint mouse - will be helpful something in the future,
Compelling quote from person to summarize call	FP mouse but a privacy concern,

SPIN Table 11: Subject 11

The context of these statements in the SPIN tables(1 through 11) is cybersecurity, specifically, how employees in the Business-to-Business(B2B) space work with and experience authentication technologies in their day-to-day workflow. These SPIN tables(1 through 11) have been a great aid in decomposing the responses of the interviewees, by clearly categorizing the responses into respective situations, problems they face on a daily basis, the effects of those problems and what they need from a company like Biloq. The following pains and (in)conveniences are expressed by these stakeholders.

An independent consultant with over 20 years of industry experience expresses the convenience of using biometrics on their private laptop, "I am glad about the fingerprint sensor on my private laptop" and wishes it to be there on their work laptop as well. A program manager with 20+ years experience in the IT industry is exhausted by the number of passwords they have to use on a daily basis, "My Number one annoyance is too many passwords" They wish there was a universal identity with one password, which brought to light the security vs usability tradeoff which exists with current technology. There is a clear convenience of having a single password, however, if that one password is breached, it would be a serious concern of privacy and potential financial loss to the individual. An associate at a consulting firm seemed open to a continuous authentication product, however they opined that it is not very urgent; "Continuous authentication is not an urgent need". A consultant at a large firm suggests that the design steps should be seamless without the user realising they are happening;"Design steps so that operation is seamless". Another consultant indicates the need for a single sign on procedure for all their applications;"I prefer single sign on for all applications". This results from the fact that they use over 8 applications on a daily basis, which means a lot of passwords and a lot of time wasted in login procedures. A director of a multinational firm wants a more predictable customer journey, which enhances user experience of login applications;"Have a predictable customer journey". A C-level executive of a firm finds the use of biometrics very convenient;"Doing biometrics is very convenient". A program integrator in the banking sector wants to authenticate more with less interruptions"Authenticate more, interrupt less at the workplace". Login procedures when using multiple applications on a daily basis consumes a lot of time. A head of Business Development in the financial sector also expresses their annoyance with a lot of passwords,"Having too many passwords is an annoyance",and wants authentication to be seamless as long as they don't realise it is happening;"Authentication as long as I don't realise it, should be seamless". A System Architect wants a user friendly security application design, which empowers employees to do smart stuff,"Empower employees to do smart stuff through user friendly security systems design". An associate at a consulting firm seemed open to the

convenience of biometrics, however expressed concerns regarding its use in devices, "Fingerprint mouse is a privacy concern".

What I learned from these interviews is that, the lead user should have following characteristics,

1. They are frustrated with a lot of passwords.
2. They are open to trying new technologies.
3. They experience the usability benefits of biometrics such as its convenience

This boils down to the following lead users, the innovative head of business growth development in the financial sector, who is always looking to improve their daily workflow and the consultant at a large multinational firm who can recommend new technology to their clients. These characteristics allow Biloq to prospect smarter and qualify the prospects faster, for example, the initial assumption was approaching IT and cybersecurity professionals, which following this project transformed into IT and cybersecurity professionals who experience the benefits of biometrics and are frustrated by multiple passwords. The second advantage of this project has been in terms of better lead qualification. In sales qualifying a lead means talking to people who are open to purchasing the product quickly. By identifying these lead users through this project, now there are insights about the specific pain points and needs of the customers, which will mean high customer conversion rates and shorter sales cycles for Biloq. The identified lead users can now help promote Biloq's innovation to their organisation as they are in a position of influence within their teams. Biloq has already set up follow-up meetings with these specific users and is planning to launch a pilot with them. This acts a leverage for Biloq, which also helps them develop personas for their future customers as part of their go-to-market plan which is the next logical future work.

7. Conclusion

The answer to the question of what are the characteristics of lead users is the following:

1. There is frustration over a lot of passwords since most people worked with at least 8-10 business related applications on a daily basis.
2. The need to be open to trying new technologies to get their work done
3. They experience the benefits of biometrics in terms of usability

The person who has these characteristics is in the Banking and Financial Services industry. While the conclusion of this project has been that biometrics offer the benefit of convenience, recently a new concern has surfaced with this technology viz., fingerprint faking and deepfakes. These days with 3D printing anyone can pick up a fingerprint from a surface and print it with a 3D printer in minutes. Another way to steal biometric information is, deepfakes. Deepfake tech can easily make an online (picture or video) version of anyone in which they were never there. This technology has existed for some time and has been used in movies. Now, deepfakes can be made faster with the help of advanced computer-graphics combined with machine learning algorithms (Adee, 2021). Biloq with its innovative embedded system addresses the security of fingerprint faking.

This project assisted in being a stepping stone in the market introduction of Biloq's new product by identifying the core challenges the end-users face as part of single factor and 2 factor authentication. Moreover, the results indicated the actual expectations of end-users from a 3-factor authentication system where they need an effortless product and if possible a single login system. The product development of Biloq can be done based on these results.

7.1 Future Work

A definite topic for future research is a Go-To-Market plan by building on the current project of lead user development. For making a concrete market entry plan, more interviews need to be conducted over a longer span of time. Following these interviews, concrete buyer personas need to be constructed for an effective go-to market plan. In this project, over a hundred people were contacted via a social media channel called LinkedIn and 11 people were finally interviewed over a short timeline, however for the market entry strategy the same people can be contacted for follow ups. The questionnaire needs to be refined from its current version. The improved questionnaire

should probe more into, what kind of credential recovery methods are used, for example, how do the end users recover from providing incorrect biometrics?. The current questionnaire was more about what kind of problems, if any, that arise while working with existing authentication systems, a follow up questionnaire should include questions about the impact of time lost during recovery of lost user credentials. For example, another structured questionnaire could include a quantitative scale of pains and (in)conveniences expressed by the interviewees.

8. Self Reflection

An interesting learning in this project has been that cybersecurity professionals are very cautious in their behavior which is a result of being in such a profession. For example, an experienced professional wanted me to contact him via the student mail address just to verify if this project is a fraud or not.

What could have been done better by me is to start the project documentation along the process of this internship. This would have made the writing process easier. For example, while looking for references about existing technologies I could have summarised those references earlier and then just included them in the final document.

This was my first time conducting market research independently, which consisted of desk research and interviewing people. I enjoyed this process of interacting with different people, from different professional backgrounds, at various experience levels in their profession.

Through the process of this project I learned to make a gantt chart in an excel spreadsheet. I learned to design a semi-structured interview questionnaire. I learned to communicate with people in the B2B space with a social media channel such as LinkedIn.

9. References

22 shocking ransomware statistics for cybersecurity in 2021. (2021). SafeAtLast. Retrieved January 20, 2022, from <https://safeatlast.co/blog/ransomware-statistics/#gref>.

3 risks your healthcare data is exposed to daily - and how to minimize them. (2021). Legacy Data Access. Retrieved January 20, 2022, from <https://www.legacydataaccess.com/resources/3-risks-your-healthcare-data-is-exposed-to-daily/>.

Aaron Henricks and Houssain Kettani. 2019. On Data Protection Using Multi-Factor Authentication. In Proceedings of the 2019 International Conference on Information System and System Management (ISSM 2019). Association for Computing Machinery, New York, NY, USA, 1–4. DOI:<https://doi.org/10.1145/3394788.3394789>

Abhishek, K., Roshan, S., Kumar, P., & Ranjan, R. (2013). A comprehensive study on multifactor authentication schemes. In *Advances in computing and information technology* (pp. 561-568). Springer, Berlin, Heidelberg.

Adams, W. (2015). Conducting Semi-Structured Interviews. Handbook Of Practical Program Evaluation, 492-505. doi: 10.1002/9781119171386.ch19

Adee, S. (2021, June 24). What are deepfakes and how are they created? IEEE Spectrum. Retrieved December 5, 2021, from <https://spectrum.ieee.org/what-is-deepfake>.

AO Kaspersky Lab, (2021), What is Cyber Security? Retrieved 30 November 2021, from <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Ashton, David. (2014). Federally Qualified Health Center Transformation to the Patient-Centered Medical Home Model: A Qualitative Study of Provider Experiences.

Bailetti, A. J. (2012a). What technology startups must get right to globalize early and rapidly. Technology Innovation Management Review, 6(2):21–27.

Bailetti, T. (2012b). Technology Entrepreneurship: Overview, Definition, and Distinctive Aspects. Technology Innovation Management Review.

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, 35(5), 1491-1511.

Bernard, J. & Nicholson, M. (2020). Reshaping the cybersecurity landscape. Deloitte. Retrieved January 20, 2022, from <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>.

Carataş, M. A., Spătariu, E. C., & Gheorghiu, G. (2019). Privacy and Cybersecurity Insights. Ovidius University Annals, Series Economic Sciences, 19(2). <https://stec.univ-ovidius.ro/html/anale/RO/wp-content/uploads/2020/02/Section%20III/6.pdf>

Cheng, Long & Liu, Fang & Yao, Danfeng. (2017). Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 7. e1211. 10.1002/widm.1211. URL: https://www.researchgate.net/publication/318152978_Enterprise_data_breach_causes_challenges_prevention_and_future_directions_Enterprise_data_breach

Choi, J.B., Lee, S.J., Kang, S.R., Lee, S.S. and Choe, H.S., 2020. Analysis of bacterial community using pyrosequencing in semen from patients with chronic pelvic pain syndrome: a pilot study. *Translational Andrology and Urology*, 9(2), p.398.

Churchill, J. et. al. (2009). LEAD USER PROJECT HANDBOOK: A practical guide for lead user project teams.

Cooper, A. (1999). The inmates are running the asylum. Indianapolis, IN: Sams. Cost of a Data Breach Report 2021. (2021). IBM. Retrieved January 20, 2022, from <https://www.ibm.com/downloads/cas/OJDVQGRY>.

Cyber security - The Netherlands. (2020). Cisco. Retrieved January 20, 2022, from https://securitydelta.nl/media/com_hsd/report/185/document/NFIA-Cyber-Security-Brochure.pdf.

Cybersecurity market - growth, trends, COVID-19 impact, and forecasts (2022 - 2027). (2021). Mordor Intelligence. Retrieved January 20, 2022, from <https://www.mordorintelligence.com/industry-reports/cyber-security-market>.

Cyberstartupobservatory.com, 2021, The Netherlands Cyber Security Companies market map – Methodology, <https://cyberstartupobservatory.com/netherlands-cyber-security-companies/>, [Accessed on: 04.11.2021]

Delman, M. (2021). Are banks spending their cybersecurity budgets in the right place? Retrieved January 20, 2022, from <https://securityboulevard.com/2021/04/are-banks-spending-their-cybersecurity-budgets-in-the-right-place/>.

Diakun-Thibault, Nadia. (2014). Defining Cybersecurity. Technology Innovation Management Review. 2014. Accessed November 20, 2021 URL: https://www.researchgate.net/publication/267631801_Defining_Cybersecurity
DLA Piper GDPR data breach survey 2020. (2020). DLA Piper. Retrieved January 20, 2022, from <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>.

Duca, S. (2020). Security models of tomorrow for work from anywhere. Retrieved January 20, 2022, from <https://www.cio.com/article/302662/security-models-of-tomorrow-for-work-from-anywhere.html>.

El-Abed, M., & Charrier, C. (2012). Evaluation of biometric systems.

Ettredge, M., Guo, F. & Li, Y. (2018). Trade secrets and cyber security breaches. Journal of Accounting and Public Policy, 37(6), 564-585.

Ferreira, A., & Cruz-Correia, R. (2021). COVID-19 and cybersecurity: finally, an opportunity to disrupt? Jmirx med, 2(2), e21069. <https://xmed.jmir.org/2021/2/e21069/>.

Ferreira, A., & Cruz-Correia, R. (2021). COVID-19 and cybersecurity: finally, an opportunity to disrupt?. Jmirx med, 2(2), e21069. <https://xmed.jmir.org/2021/2/e21069/>

Francisco Nunes, Paula Alexandra Silva, and Filipe Abrantes. 2010. Human-computer interaction and the older adult: an example using user research and personas. In Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '10). Association for Computing Machinery, New York, NY, USA, Article 49, 1–8. DOI:<https://doi.org/10.1145/1839294.1839353>

Garg J. (2021). Startupindia.gov.in, Early stage of growth stage, https://www.startupindia.gov.in/content/sih/en/bloglist/blogs/early_stage_to_a_growth_stage.html, [Accessed on: 04.11.2021]

Global Market Insights, Inc. Retrieved December 11, 2021, from <https://www.gminsights.com/pressrelease/cyber-security-market>

Globocnik, D., & Faullant, R. (2021). Do lead users cooperate with manufacturers in innovation? Investigating the missing link between lead userness and cooperation initiation with manufacturers. *Technovation*, 100, 102187. doi: 10.1016/j.technovation.2020.102187

Gorlewicz, J.L. and Jayaram, S., 2020. Instilling curiosity, connections, and creating value in entrepreneurial minded engineering: Concepts for a course sequence in dynamics and controls. *Entrepreneurship Education and Pedagogy*, 3(1), pp.60-85.

Grand View Research (2021). Identity and Access Management Market | IAM Industry Report, 2025. (2021). Retrieved 30 November 2021, from <https://www.grandviewresearch.com/industry-analysis/identity-and-access-management-iam>

Grant, M. (2020). Startup Definition.

Hamid, L. (2015). Biometric technology: not a password replacement, but a complement. *Biometric Technology Today*, 2015(6), 7-10.

Hicham Hammouchi, Othmane Cherqi, Ghita Mezzour, Mounir Ghogho, Mohammed El Koutbi, Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time, *Procedia Computer Science*, Volume 151, 2019, Pages 1004-1009, ISSN 1877-0509, URL: <https://www.sciencedirect.com/science/article/pii/S1877050919306064>

Hippel, E.V. (1986). Lead users: a source of novel product concepts. *Management Science*, 32, 791-805.

Hummer, M., Groll, S., Kunz, M., Fuchs, L. and Pernul, G., 2018, January. Measuring Identity and Access Management Performance-An Expert Survey on Possible Performance Indicators. In *ICISSP* (pp. 233-240).

IMARC Group (2021). Ipsnews.net, 2021, MULTI-FACTOR AUTHENTICATION MARKET 2021 SIZE, SHARE, GROWTH, TRENDS, COMPANIES, AND REPORT 2026, <https://ipsnews.net/business/2021/09/15/multi-factor-authentication-market-2021-size-share-growth-trends-companies-and-report-2026/>, [Accessed on: 04.11.2021]
Introduction to industries. (2021). Verizon. Retrieved January 20, 2022, from <https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/>.

Iqbal, I., & Qadir, B. (2012). *Biometrics Technology: Attitudes & influencing factors when trying to adopt this technology in Blekinge healthcare*.

Jentzen, A. (2019). The latest in phishing: First of 2019. Retrieved January 20, 2022, from <https://www.proofpoint.com/us/security-awareness/post/latest-phishing-first-2019>.

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270). Academic Conferences and publishing limited. https://www.researchgate.net/profile/Abdul-Bashiru-Jibril/publication/341215154_Customers'_Perception_of_Cybersecurity_Threats_Toward_e-Banking_Adoption_and_Retention_A_Conceptual_Study/links/5eb41ca9299bf152d6a28751/Customers-Perception-of-Cybersecurity-Threats-Toward-e-Banking-Adoption-and-Retention-A-Conceptual-Study.pdf

Johnson, J. (2021). Number of data breaches in the United States from 2013 to 2019, by industry. Statista. Retrieved January 20, 2022, from <https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/>.

Juma'h, Ahmad & Alnsour, Yazan. (2020). The Effect of Data Breaches on Company Performance. International Journal of Accounting and Information Management. 28. 10.1108/IJAIM-01-2019-0006. URL: https://www.researchgate.net/publication/335002124_The_Effect_of_Data_Breaches_on_Company_Performance

Jung, S.G., Salminen, J., Kwak, H., An, J. and Jansen, B.J., 2018, March. Automatic Persona Generation (APG) A Rationale and Demonstration. In Proceedings of the 2018 conference on human information interaction & retrieval (pp. 321-324).

Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018). Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. SOUPS @ USENIX Security Symposium. URL: <https://www.semanticscholar.org/paper/Data-Breaches%3A-User-Comprehension%2C-Expectations%2C-Karunakaran-Thomas/12d8071bde25e4dd1d28638281db630f245e7d82>

KBV Research (2021). Identity Verification Market Size, Share, Growth 2020-2026. (2021). Retrieved 30 November 2021, from <https://www.kbvresearch.com/identity-verification-market/>

Leatherbee, M. and Katila, R., 2020. The lean startup method: Early-stage teams and hypothesis-based probing of business ideas. Strategic Entrepreneurship Journal, 14(4), pp.570-593.

Lewis, J.A. & Crumpler, W. (2019). The cybersecurity workforce gap. Center for Strategic and International Studies. Retrieved January 20, 2022, from <https://www.csis.org/analysis/cybersecurity-workforce-gap>.

LoginID (2021). Biometric Technology: A Brief History - Retrieved 14 December 2021, from <https://loginid.io/blog/biometric-technology-a-brief-history>

Loohuis, Kim, 2021. ComputerWeekly.com. Data of thousands of Dutch citizens leaked from government Covid-19 systems. [online] Available at: <<https://www.computerweekly.com/news/252495983/Data-of-thousands-of-Dutch-citizens-leaked-from-government-Covid-19-systems>> [Accessed 14 December 2021].

Ltd, R. A. M. (2021). Cyber Security Market by Component, by Deployment Type, by User Type, by Industry Vertical - Global Opportunity Analysis and Industry Forecast, 2020 - 2030. Research and Markets Ltd 2021. Retrieved December 11, 2021, from [https://www.researchandmarkets.com/reports/5403217/cyber-security-market-by-component-by-deployment?utm_source=BW&utm_medium=PressRelease&utm_code=ch9nk&utm_campaign=1599502+-+Global+Cyber+Security+Market+\(2021+to+2030\)+-+by+Component%2c+Deployment+Type%2c+User+Type%2c+Industry+Vertical+and+Region&utm_exec=jamu273prd](https://www.researchandmarkets.com/reports/5403217/cyber-security-market-by-component-by-deployment?utm_source=BW&utm_medium=PressRelease&utm_code=ch9nk&utm_campaign=1599502+-+Global+Cyber+Security+Market+(2021+to+2030)+-+by+Component%2c+Deployment+Type%2c+User+Type%2c+Industry+Vertical+and+Region&utm_exec=jamu273prd)

Mankins, John. (1995). Technology Readiness Level – A White Paper.

Mannan, Capt. (2020). Best practices of Semi-structured interview method.

Marzouki, Reem & Belkahla, Wafa. (2019). The impact of lead users on innovation success: The mediating impact of knowledge sharing case of IT companies. *Innovation & Management Review*. ahead-of-print. 10.1108/INMR-12-2018-0093.

McCormac, M. (2021). Pain chain. Retrieved 29 November 2021, from <https://www.slideshare.net/MikeMcCormac/pain-chain-8120532>

McGowan, E. (2018). What Is a Startup Company, Anyway?, *Startups.com*, Accessed October 20, 2021, URL <https://www.startups.com/library/expert-advice/what-is-a-startup-company>

McIntosh, M., & Morse, J. (2015). Situating and Constructing Diversity in Semi-Structured Interviews. *Global Qualitative Nursing Research*, 2, 233339361559767. doi: 10.1177/2333393615597674

Mihailescu, M.I., Racuciu, C., Grecu, D., & Niță, L. (2015). A MULTI-FACTOR AUTHENTICATION SCHEME INCLUDING BIOMETRIC CHARACTERISTICS AS ONE FACTOR.

Mlitz, K. (2022). Global cybersecurity spending 2017-2021 (COVID-19 adjusted). Statista. Retrieved January 20, 2022, from <https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/>.

Mordor Intelligence. (2021) Multifactor Authentication Market | 2021 - 26 | Industry Share, Size, Growth. Retrieved 29 November 2021, from <https://www.mordorintelligence.com/industry-reports/multifactor-authentication-market>

Mordor Intelligence. (2021). Mobile Devices User Authentication Services Market | 2021 - 26 | Industry Share, Size, Growth Retrieved 29 November 2021, from <https://www.mordorintelligence.com/industry-reports/mobile-devices-user-authentication-services-market>

Mordorintelligence.com, (2021)., Cybersecurity Market Trends, Size| Industry Growth 2021 to 2026 With COVID Impact – Mordor Intelligence. (2021). <https://www.mordorintelligence.com/industry-reports/cyber-security-market>. Retrieved December 11, 2021, from <https://www.mordorintelligence.com/industry-reports/cyber-security-market>

Morris, Ch. (2021). The number of data breaches in 2021 has already surpassed last year's total. Fortune. Retrieved January 20, 2022, from <https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/>.

NIST. (2021). MFA - Glossary | CSRC. (2021). Retrieved 29 November 2021, from <https://csrc.nist.gov/glossary/term/MFA>

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, 43(8), 1173-1195.
https://ebiquity.umbc.edu/_file_directory_/papers/1110.pdf

Pajo, Sanjin & Verhaegen, P.-A & Vandevenne, Dennis & Duflou, Joost. (2015). Towards Automatic and Accurate Lead User Identification. *Procedia Engineering*. 131. 10.1016/j.proeng.2015.12.445.

Perini, S. (2021) Security Spending in Europe Remains Strong in 2021, with Banking and Manufacturing Maintaining Top Positions, According to IDC. Retrieved 30 November 2021, from <https://www.idc.com/getdoc.jsp?containerId=prEUR247561221>

PR Newswire. (2021) Reports, V. Biometric Technology Market Size is USD 11490 Million by 2026 at CAGR 11.0% | Valuates Reports. Retrieved 30 November 2021, from <https://www.prnewswire.com/in/news-releases/biometric-technology-market-size-is-usd-11490-million-by-2026-at-cagr-11-0-valuates-reports-858312448.html>

Qu, H., Hu, X. and Singh, J.A., 2019. Factors influencing implementation of a computerized, individualized, culturally tailored lupus decision aid in lupus clinics: a qualitative semi-structured interview study. *Clinical rheumatology*, 38(10), pp.2793-2801.

Rackham, Neil (1988), *Spin Selling*, USA: McGraw-Hill.

Ravi. (2021). Medium.com, 2021, What is Authentication?
<https://medium.com/demystifying-security/identification-authentication-696fd4dd6c3e>,
[Accessed on: 09.11.2021]

Roberds, W., Schreft, S.L., 2008. Data Breaches and Identity Theft. *SSRN Electronic Journal*.. doi:10.2139/ssrn.1296131. Accessed November 20, 2021 URL:
<https://click.endnote.com/viewer?doi=10.2139%2Fssrn.1296131&token=WzMyNDg2MDIsIjEwLjlxMzkvc3Nybi4xMjk2MTMxIi0u9uWHDNdGHi-Cm3EJM83fezZIVBo>

Rui, Z. and Yan, Z., 2018. A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE access, 7, pp.5994-6009.

Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A. K., Castiglione, A., ... & Baik, S. W. (2019). CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters*, 126, 123-131.

Salazar, C. (2021). How to Use a 'Pain Chain' to Add Customer Value. (2021). Retrieved 29 November 2021, from <https://www.channelpronetwork.com/blog/entry/how-use-pain-chain-add-customer-value>

Salminen, J., Guan, K., Jung, S.G., Chowdhury, S.A. and Jansen, B.J., 2020, April. A literature review of quantitative persona creation. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

Sanction Scanner. (2021). | 6 Identity Verification Methods Retrieved 29 November 2021, from <https://sanctionscanner.com/blog/6-identity-verification-methods-272>
Santisteban, J. and Mauricio, D. (2017). Systematic literature review of critical success factors of information technology startups. Academy of Entrepreneurship.

Sean Duca, (2020)., Security Models of Tomorrow for Work from Anywhere. (2020). Palo Alto Networks. Retrieved December 11, 2021, from <https://www.paloaltonetworks.com/cxo-perspectives/security-models-of-work-for-work-from-everywhere>

Shacklett, M. (2021) What is Authentication?. Retrieved 29 November 2021, from <https://www.techtarget.com/searchsecurity/definition/authentication>

Shah, S.W. and Kanhere, S.S., 2019. Recent trends in user authentication—a survey. IEEE access, 7, pp.112505-112519.

Sharma, N., Oriaku, E.A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, 8(1), 33-41. <https://doi.org/10.20448/2001.81.33.41>.

Silver, L. (2019). 1. Digital connectivity growing rapidly in emerging economies. Retrieved January 20, 2022, from <https://www.pewresearch.org/global/2019/02/05/digital-connectivity-growing-rapidly-in-emerging-economies/>.

Sobers, R. (2021) | 98 Must-Know Data Breach Statistics for 2021 | Varonis. (2021). Retrieved 30 November 2021, from <https://www.varonis.com/blog/data-breach-statistics/>

Song, M., Podoynitsyna, K., Van Der Bij, H., and Halman, J. I. M. (2007). Success Factors in New Ventures: A Meta-analysis*. *Journal of Product Innovation Management*, 25(1):7–27.

Tang, S., Jing, H., Huang, Z., Huang, T., Lin, S., Liao, M. and Zhou, J., 2020. Identification of key candidate genes in neuropathic pain by integrated bioinformatic analysis. *Journal of cellular biochemistry*, 121(2), pp.1635-1648.

Techopedia Inc. (2021). What is Identity and Access Management (IAM)? - Retrieved 30 November 2021, from <https://www.techopedia.com/definition/23922/identity-and-access-management-iam>

Tewari, S. H. (2021). Necessity of Data Science for Enhanced Cybersecurity. *International Journal of Data Science and Big Data Analytics*, 1(1), 63-79. [https://www.svedbergopen.com/files/1614613601_\(5\)_IJDSBDA15112020MTN003_\(p_63-79\).pdf](https://www.svedbergopen.com/files/1614613601_(5)_IJDSBDA15112020MTN003_(p_63-79).pdf)

The economic impact of cybercrime - No slowing down. (2018). McAfee. Retrieved January 20, 2022, from <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>.

Tunggal, A.T. (2022). What is the cost of a data breach in 2021? Retrieved January 20, 2022, from <https://www.upguard.com/blog/cost-of-data-breach>.

von Hippel, E. (2005) *Democratizing innovation*. Cambridge: MIT Press.

Vuori, T. and Huy, Q., 2015. Distributed Attention and Shared Emotions in the Innovation Process. *Administrative Science Quarterly*, 61(1), pp.9-51.

Wadhwani, P.S.L. (2021, June 28). Cybersecurity market worth over \$400 Bn by 2027. Global Market Insights, Inc. Retrieved January 20, 2022, from <https://www.gminsights.com/pressrelease/cyber-security-market>.

Walters, H. (2020). 6 cyber-related stats in financial services. Retrieved January 20, 2022, from <https://www.finextra.com/blogposting/19411/6-cyber-related-stats-in-financial-services>.

Wan, S., 2021. Research Methods in Second Language Acquisition---An Application Test of Semi-structured Interview. Sch Int J Linguist Lit, 4(7), pp.204-212.

Wang, C., Wang, Y., Chen, Y., Liu, H. and Liu, J., 2020. User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, p.107118.

Warburton, D. (2020). Phishing attacks soar 220% during COVID-19 peak as cybercriminal opportunism intensifies. Retrieved January 20, 2022, from <https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal>.

West, D.M. & Skahill, E. (2021). Hospitals and health care face increasing cybersecurity risks. Retrieved January 20, 2022, from <https://www.brinknews.com/the-evolving-cybersecurity-risks-in-hospitals-and-the-health-care-industry/>.

What is IAM?. OneLogin. (2022). Retrieved 24 January 2022, from <https://www.onelogin.com/learn/iam>.

ZAPFL, D. (2022). *Definition: What is a LEAD User?*. Lead-innovation.com. Retrieved 24 January 2022, from <https://www.lead-innovation.com/english-blog/what-is-a-lead-user>.

10. Appendix

Appendix A: Questionnaire

An outline of the questionnaire is as follows:

1. How do you start your work day?
 - How do you feel about your current login procedure in terms of convenience?
 - How do you feel about your current login procedure in terms of security?
2. Which devices do you use?
 - How many devices do you use for your work environment?
 - How many devices do you use for your home environment?
 - How do you feel about the convenience of home and work devices?
 - How do you feel about the security of home and work devices?
3. How do you collaborate in a team?
 - How do you feel about the convenience of the collaboration tools?
 - How do you feel about the security of the collaboration tools?
 - What are your worries and annoyances about these tools?
 - What are your worries and annoyances about collaboration processes?
4. What other tools have you used for security?
 - Why these tools?
 - How do you feel about these tools in terms of convenience?
 - How do you feel about these tools in terms of security?
5. Now that we have discussed multiple procedures and tools for security, what do you think about any improvements specifically in your work environment?
 - Would these improvements make you less worried?
 - Would these improvements make you more secure?