IT Security Improvements for Small and Medium Size Businesses

Sponsor: ARCO IT Security Services

Authors:

Meghan Brady

David Leandres

Eric Schmid

Nadia Singh

Advisors:

Ulrike Brisson

Blake Currier

I. Table of Contents

II. List of Figures

III. Authorship

Section	**Author**	**Editor**
Title Page	Nadia Singh	All
Table of Contents	Eric Schmid	All
Abstract	David Leandres	Eric Schmid, Nadia Singh
Acknowledgements	Meghan Brady	Eric Schmid, David Leandres
Executive Summary	Eric Schmid, Meghan Brady, Nadia Singh	Eric Schmid, Meghan Brady, Nadia Singh
Authorship	Meghan Brady	All
Chapter 1: Introduction	All	All
Chapter 2: Background		
Large Businesses Aren't the Only Targets	Nadia Singh	Eric Schmid
Types of Cyber Attacks	All	Eric Schmid
The Effect of Cyber Attacks	Nadia Singh	David Leandres
Why are SMBs Underprepared	Meghan Brady	Nadia Singh
Cyber Insurance	Meghan Brady	David Leandres, Eric Schmid
SMBs Undervalue IT Security Measures	Meghan Brady	David Leandres, Eric Schmid
Behavior Change	Nadia Singh	Meghan Brady
Conducting Surveys	David Leandres	Eric Schmid
Conducting Interviews	Meghan Brady	Eric Schmid
Our Goal	Eric Schmid	Meghan Brady
Chapter 3: Methodology		
Objective 1: Assess the state of SMBs IT Security	David Leandres	Eric Schmid
Objective 2: Understand SMBs knowledge of IT security	Nadia Singh	Meghan Brady

Chapter 4: Findings and Analysis		
Lack of Skill and Awareness	Nadia Singh, Meghan Brady	Eric Schmid
Optimism Bias	Meghan Brady, Nadia Singh	David Leandres
Benefits of Having Cybersecurity Training	Meghan Brady, Nadia Singh	David Leandres
Relationship to Country	Meghan Brady	Eric Schmid
Differences Amongst Industries	Eric Schmid	Meghan Brady
Interview Results	Meghan Brady	David Leandres, Nadia Singh
Conclusion	Nadia Singh	Eric Schmid
Chapter 5: Conclusions and Recommendations		
Recommendations	David Leandres	Eric Schmid
Expectations vs. Findings	Meghan Brady, Nadia Singh	Eric Schmid
Future Improvements	David Leandres	All
Appendices		
Appendix A: Sponsor Description	Meghan Brady	David Leandres
Appendix B: Preliminary Survey	All	All
Appendix C: Interview	David Leandres	All
Appendix D: Post-Interview Survey	David Leandres	All
Appendix E: Website	David Leandres, Eric Schmid, Nadia Singh	All

IV. Abstract

Our project aims to identify why some small and medium-sized businesses lack suitable IT security standards and how to better support them in updating their IT security systems. We surveyed and interviewed employees from different companies in Switzerland, Germany, and the US. Major inhibitors/obstacles were lack of skill and awareness as well as optimism bias. We recommended more frequent and better training for all employees.

V. Acknowledgements

Our team would like to thank our sponsors, Amy Vaillancourt and Bertram Dunskus of Arco IT GmbH. Amy Vaillancourt and Bertram Dunskus aided our team throughout this project and offered unparalleled information about the IT industry in Switzerland. Their contacts allowed us to distribute our survey and collect interview candidates all around Switzerland and into bordering countries. Both Ms. Vaillancourt and Mr. Dunskus were instrumental in our completion of this project and development of the final deliverable. We could not have done this without them.

We would also like to thank those who participated in our survey and extend an additional thank you to those who took the time out of their day to interview with us. Any project is dependent upon the participation of community members, and so our team wishes to address the fact that our project could not have been successful without the input of respondents.

Additionally, we would like to thank our advisors, Professors Blake Currier and Ulrike Brisson from Worcester Polytechnic Institute, for all of their time spent helping us with our website, report, and presentation. Their continued efforts to guide us in the right direction even after the many setbacks stands out to us tremendously.

Lastly, we would like to thank Worcester Polytechnic Institute. Although we were not able to travel overseas to Zurich, Switzerland, the opportunity to work with a company in Zurich is an experience we would not have been able to experience without the IQP Process.

VI. Executive Summary

Many businesses store sensitive customer data, such as names, addresses, credit card information, and social security numbers. Companies can not only create a profile on customers with necessary information but also predict where and how customers will spend their money. They can also create targeted advertisements and improve customer experience; however, this information can be leveraged to steal customers' money and identities. Therefore, cybercriminals have targeted these businesses to gain access to this information. Some criminals have also taken to disrupting the services of businesses to seek a ransom. Despite these threats, only in recent years have companies begun to invest in effective data security measures.

VI.i Background

In the wake of increased cyberattacks, many large businesses have increased their cybersecurity, however, some small to medium-sized businesses (SMBs) have opted to forgo these security improvements (UK: Support for small businesses against cyberattacks., 2012). They display optimism bias, as they believe they are smaller targets and are not subject to an attack (Appleby, 2019). This belief ironically drives up the number of attacks perpetrated against them.

VI.ii Project Goal

This project looked at the state of SMB IT Security through surveys and interviews to better understand underlying feelings of public opinion. Having this knowledge provided a better understanding of how to help SMB's implement security measures and training. With this generalized information, we conducted an informed interview process and created data graphics.

VI.iii Methodology

The team first sent out a survey to several companies, aimed at seeing how the respondents felt about IT security at their company. The survey consisted of 27 questions (Appendix B) and asked participants to rate these statements on a scale of applicability to their company. Answers were collected through our website (wpicybersecurity.com, Appendix E), and participants were asked if they were willing to participate in a follow-up interview.

Upon completion of the interview, we asked participants to briefly take a 5-minute survey to rank activity. We had the participants rank a number of IT security scenarios to understand how they perceived different threats on a scale of 1 (worst) to 10 (best). These data comparisons are important in illustrating if companies' perceived threats are valid and if their level of concern for these threats align with the measures their company currently has in place (see appendix D for post-interview questions).

VI.iv Findings and Analysis

When collecting our data, we focused primarily on two questions:

- How well are small and medium-sized businesses equipped to handle cyberattacks?
- How can these businesses be better prepared for cyberattacks in the future?

We collected survey responses for two weeks and received 29 replies. In week 3, we then set up interviews with five respondents. 70% of our survey respondents worked for a company based in the United States, and 20% worked for companies based in Switzerland. The remaining 10% of respondents worked for a variety of countries, mainly based in Germany.

Our survey showed the biggest inhibitors to adopting good cybersecurity practices are due to lack of skill, awareness, and optimism bias. Lack of skill and awareness feed into each other and cause an uninformed workplace, which can also be exacerbated by the belief that a company is safe from attacks. This can be easily mitigated by increased training for employees. We also found that these businesses opted not to improve their security programs even after falling victim to attacks, possibly due to financial concerns. Through our interviews, we learned that those most opposed to advanced security measures were senior members in the office.

The biggest trend we noticed was the importance of employees receiving cybersecurity training. This training could range from occurring in a classroom setting to completing online training modules. Numerous other positive factors were linked to a company that actively trained its employees, such as increased confidence in their IT infrastructure.

VI.v Conclusions and Recommendations

One of the most glaring constants across our surveys and interviews is that cybersecurity measures are often seen as a hindrance to many employees. This can be attributed to a lack of training and technical knowledge. 50% of those surveyed do not have a specific cyber-security program in place, and 45% of respondents are given no training in good security practices from their company.

We found that not enough people invest in enough holistic IT security procedures, such as antivirus software, incident protocols, employee training, and scheduled security updates. Pairing these measures with simulated network penetration tests allow companies to audit their systems and training efficacy.

We recommend that every company provide IT cybersecurity training and additional materials such as videos or guides. We also recommend companies to have a dedicated resource solely concerned with the organization’s cybersecurity and IT infrastructure. This could be either an in-house employee who is proficient in IT security or an outside consultant. This will ensure that the organization maintains good cybersecurity practices.

Ultimately, we are hopeful that this project made a contribution to improve cybersecurity measures in small to medium-sized businesses by defining threats, addressing barriers, and proposing changes.

Chapter 1: Introduction

In the modern era, people have transitioned from guarding troves of gold to developing hard drives with terabytes of data, worth more than their weight in gold. Many businesses store customer data such as names, addresses, credit card information, and social security numbers. With customer data, companies can create targeted advertisements and improve customer experience. However, this information can be leveraged to steal customers' money and personal identities. Therefore, many cybercriminals have targeted these businesses to gain access to this information. Some criminals have also taken to disrupting the services of businesses to seek a ransom. In many cases, this is merely annoying; however, if the target is a power plant, distribution center, hospital, or other essential service, there can be serious consequences. Despite these threats, only in recent years have companies begun to invest in effective data security measures.

Many businesses have increased their cybersecurity because of increased cyberattacks. A lot of small to medium-sized businesses (SMBs), however, have opted to forgo security improvements (UK: Support for small businesses against cyberattacks., 2012). They display optimism bias, as they believe they are smaller targets and are not subject to an attack (Appleby, 2019). This belief ironically drives up the number of attacks perpetrated against them. For example, in Switzerland, SMBs make up 99.6% of all companies, and employ two-thirds of all Swiss citizens. This poses a substantial threat to the country (SME Policy 2019). Many companies also try to cover up their data breaches in an attempt to maintain public trust, furthering the narrative that security breaches are not common (Thompson, 2014). 73% of small businesses say a safe and trusted internet is critical to their success, but most do not have an internet security policy. 87% of small businesses do not have a formal internet policy, and 69% are without a basic informal internet security policy (Thompson, 2014). To understand how companies view their cybersecurity goals, we assessed our respondents' knowledge through opinion based survey questions. We then released our findings through our website to stress the importance of good cybersecurity practices.

Chapter 2: Background

Throughout this chapter, we aim to show how cyberattacks are a risk to small and medium-sized businesses which typically range from 1 to 250 employees. Many of these businesses remain unprepared due to the high cost of cybersecurity and the fact that many businesses place a low value on cybersecurity. 50% of small businesses reported experiencing a data breach in the past 12 months, proving that optimism bias on this topic is unfounded (Appleby, 2019). Many SMBs continue to believe that security breaches only happen to large enterprises, partly due to the media focus on massive security breaches like Equifax and Marriott, with limited media exposure on smaller hacks (Zou, Mhaidli, McCall, Schaub, 2018). These attacks can be very expensive for small businesses, many of which may be unable to recover (Kujawa, Zamora, Segura, et al., 2017). Even though cyberattacks are prevalent for SMBs, numerous are still underprepared due to their optimism bias and the fact that they undervalue these security measures.

2.1 Large Businesses Aren't the Only Targets

With their copious amounts of private data, it is easy to assume that large businesses require the most protection. Due to the long history of cyberattacks conducted against them, bigger businesses have stepped up their IT security measures. In contrast, SMBs have neglected this step, making them more susceptible to attacks. (Banham, Russ, 2017). SMBs have left themselves open to data breaches, which can cost them both customer trust and a large portion of their earnings (Manning, 2015). The 2013 Information Security Breaches Survey shows that 87% of small businesses across all sectors experienced a breach in 2012. This is up more than 10% from the previous year and costs small businesses up to 6% of their earnings (UK: Support for small businesses against cyberattacks, 2012).

A small California-based company aimed at teaching children how to think like engineers was hit with an attack that first shut down their website (Widjaya, 2018). At this time, they only had seven full-time employees. They were then attacked with ransomware and had to rebuild from the ground up. Throughout this process, they lost thousands of dollars but were able to stay in business (Widjaya, 2018). In another case study, someone planted malicious software in the cash registers of a small magazine shop located in Chicago. Customer credit card information was sent to Russia, costing the shop $22,000 (Fowler and Worthen, 2011). The Efficient Services Escrow

Group was hit by a cyber attack in 2012 that forced it to shut down. It started with a fraudulent wire transfer to Russia, and one month later, another followed, this time to China. These wire transfers cost the company over 1.5 million dollars. They attempted to get this money back, but when they were unable to do so, the California Department of Corrections shut them down (Harris K. D., 2014).

While SMBs may not have the same quantity of data as larger companies, they still have sensitive data such as customer and employee information, and credit card numbers. This information can be held ransom or sold to the highest bidder, both of which can cost SMBs a nontrivial sum of money, which may be difficult to recover from (Banham, Russ, 2017). Many SMBs serve larger organizations and are additionally connected to their networks and systems. Therefore, the SMBs can provide hackers a back door to access the larger company's sensitive data (Banham, Russ, 2017).

There was a massive data breach of Target in 2013, and this is just one instance of cyber attacks occurring across multiple companies (Banham, Russ, 2017). After an investigation, it was determined that the attackers gained access to Target's computer gateway through credentials stolen from a third-party vendor. This third party, Target's HVAC (Heating, Ventilation, and Air Conditioning) vendor, was an SMB. Using the stolen credentials, the hackers gained access to Target's customer service database and installed malware on their servers. This malware captured full names, phone numbers, email addresses, credit card numbers, and verification codes, among other sensitive data. In the end, Target had to pay $18.5 million for this data breach, which affected 41 million consumers (Manworren, Letwat, Daily, 2016). This illustrates the value for hackers to compromise SMBs in the hopes that it will provide an easy opportunity to compromise a larger enterprise.

2.2 Types of Cyber Attacks

There are many different types of cyberattacks, ranging from random to targeted. The ultimate cybersecurity goal of securing all points of access from a hacker is extremely challenging because of this large variety of attacks. Based on reports from the Ponemon Institute, the most common attacks are phishing, malware, viruses/worms/trojans, spyware, ransomware, and Denial of Service (DOS) (Akbari Roumani, Fung, Rai, Xie 2016).

2.2.1 Social Engineering and Phishing

Phishing is a type of network attack where a replica of an existing Web page is created to trick users into submitting personal, financial or protected data to what they think is a secure website (Chen and Guo). These attacks have recently become more sophisticated, and in turn, have been getting more press (Ludl, McAllister, Kirda, Kruegel 2007). According to a study by Gartner, 51 million US Internet users have received emails that were a part of phishing scams, and about 2 million of them are estimated to have been tricked into giving away sensitive information (Chen and Guo).

In social engineering attacks, attackers pretend to be something that they are not. They may pose as utility companies, government agencies, banks, and much more. Using publicly available information sources such as social media, websites, government databases, compromised emails, or from previous phishing attacks, the attackers can gain victims' trust and trick them into revealing personal information. Some examples may include Social Security Numbers, credit card numbers, security questions, passwords, and other forms of sensitive information (Krombholz, K., Hobel, H., Huber, M., & Weippl, E., 2015). Although it seems easy to avoid such an attack, research indicates that people perform poorly on detecting these lies and deceptions (Qin and Burgoon, 2007, Marett et al., 2004).

2.2.2 Malware

Malware is a broad term used to describe many different types of malicious programs with the sole purpose of infecting and disrupting the target. The most common type of malware is a virus, which is typically attached to legitimate software. Once someone runs the infected code it spreads as a virus would in an animal, causing rapid damage.

The computer virus began in the 1980s, but today almost every Fortune 500 company has experienced computer viruses. The current rate of virus incidents is about one every 2-3 months. They have been known to cause physical harm to computer hardware in addition to erasing and destroying data. The increased connectivity among individuals, companies, and governments will allow a computer virus to wreak havoc. In a general sense, the virus must perform an intended function or a function the user or operator did not intend, like making it difficult for the user to access the files, moving a file to a new location, or deleting files. More malicious viruses may intend to hurt a competing business through sabotage, espionage or financial loss (Schnurer, Klemmer, 1998).

Other types of malware include: worms, trojans, and spyware. Worms specialize in infecting entire networks by connecting to as many computers as quickly as they can. Trojans disguise themselves in legitimate software, then provide a backdoor for other malware to infect the computer. Unlike other forms of malware, Spyware seeks to hide on your computer undetected, collecting data. The spyware may behave as a keylogger, recording all keyboard entries on a computer.

Ransomware is a threat to data files of individuals and businesses. It encrypts and locks files on an infected computer or network and holds the key to unlock the files until the owner pays ransom. This malware is responsible for hundreds of millions of dollars lost annually (Richardson, Ronny, and North, 2017). This type of extortion has been around since 2005, but new versions appear very frequently due to their success (Zetter, 2015). These updates allow ransomware to bypass some antivirus software and detection methods.

2.2.3 Denial of Service Attacks

Denial of Service attacks occur when users are not able to access information on their devices or network because of a malicious cyber threat (Roumani, Fung, Rai, and Xie, 2016). This type of attack can affect emails, websites, and online accounts. There are two common DOS attacks: a Smurf Attack and a SYN flood. In a Smurf attack, the attacker sends a broadcasted message from a spoofed IP address that matches that of the target. People will respond and the targeted host will be flooded with their responses. In a SYN flood, “an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server” (Roumani, Fung, Rai, and Xie, 2016). The server then has to waste resources waiting to complete these fraudulent connections, slowing its performance down and can prevent legitimate users from connecting as all the connections are occupied.

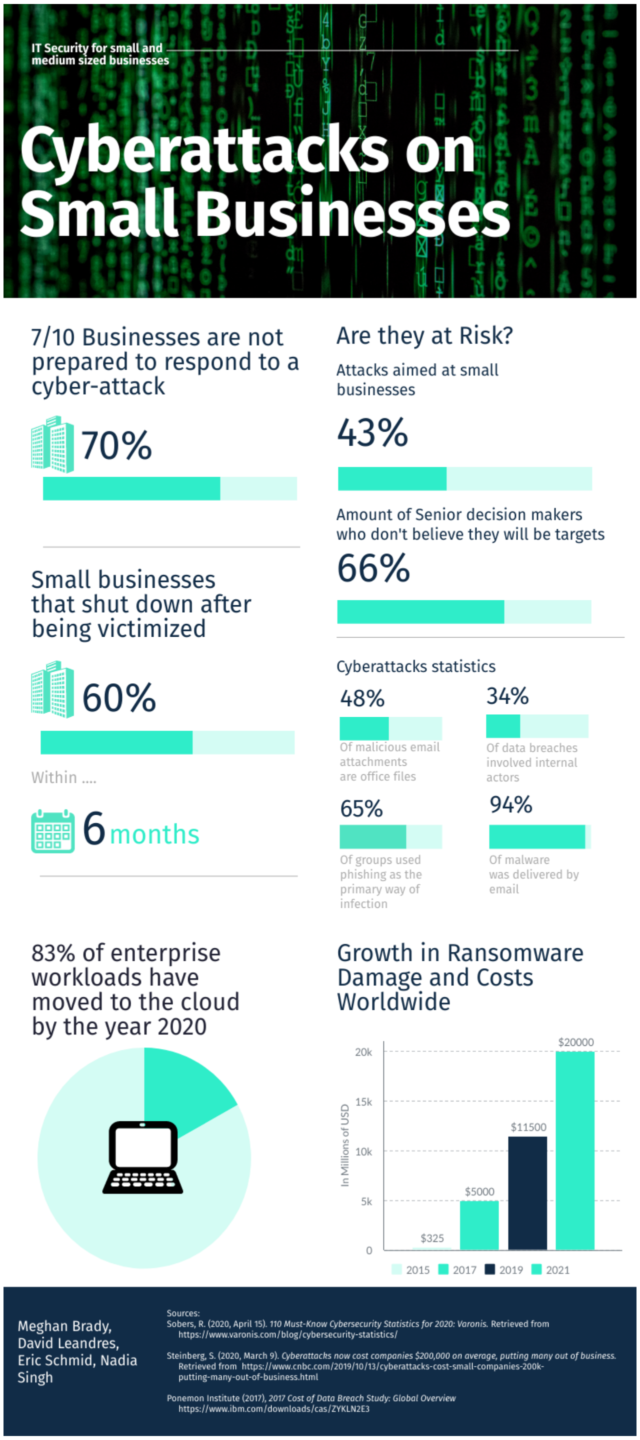
2.3 The Effect of Cyber Attacks

When cyber-attacks are not handled effectively, adverse effects can start to pile on, and they aren't limited to a loss in revenue. When a company falls victim to these attacks, they open up their sensitive information to be taken or held hostage. This can result in a loss of business operations, customer trust, and can harm their reputation.

An example of attackers taking advantage of an SMB's critical data is shown with a large data breach in a psychiatric hospital. The hospital network stored a vast quantity of sensitive data, including medical records, addresses, payment information, and records of the medications each patient uses, and conditions they were afflicted with. The attackers used ransomware to hold hostage the hospital's data. This was a big problem for the hospital, as they lost access to information regarding medications. The hospital paid a lot of money in ransom to get the data back to continue serving their patients (Dunskus and Vaillancourt, personal interview).

When comparing the monetary loss across various nations, the enormous cost of dealing with cyberattacks is made apparent. From research in 2013 which compiles data collected from seven studies, the average annualized cost of these attacks: The United States of America with 11.56 million USD, The United Kingdom with 2.99 million GBP, and Germany with 5.67 million euros (Johnson, 2015).

In both the Target and psychiatric hospital instances, customer and patient trust was lost (Greene and Stavins, 2017). In a study by the Ponemon Institute, we see that there is, in fact, a relationship between customer turnover and a strong security posture. 51% of consumers in this study were victims of a data breach, and 52% of these respondents say they were the victims of more than one data breach. Multiple breaches have had a serious impact on the relationship the consumer had with the organization. 65% of respondents say these incidents did cause them to lose trust in the organization experiencing the data breach (Ponemon Institute, 2017). According to individuals surveyed in the Ponemon Institute study, a data breach is one of the top three negative effects on brand reputation. Both IT security representatives and upper management participants revealed that they believe a data breach and product recall would hurt their brand reputation, even ranking it above the potential impact of a scandal involving the CEO. As found in their study, 65% of upper management individuals and 63% of IT representatives felt that the most serious threat to reputation is poor customer service caused by security breaches (Ponemon Institute, 2017).



IT Security for small and medium sized businesses

Cyberattacks on Small Businesses

7/10 Businesses are not prepared to respond to a cyber-attack

70%

Small businesses that shut down after being victimized

60%

Within ....

6 months

83% of enterprise workloads have moved to the cloud by the year 2020

Are they at Risk?

Attacks aimed at small businesses

43%

Amount of Senior decision makers who don't believe they will be targets

66%

Cyberattacks statistics

48%
Of malicious email attachments are office files

34%
Of data breaches involved internal actors

65%
Of groups used phishing as the primary way of infection

94%
Of malware was delivered by email

Growth in Ransomware Damage and Costs Worldwide

Meghan Brady, David Leandres, Eric Schmid, Nadia Singh

Sources:
Sobers, R. (2020, April 15). *110 Must-Know Cybersecurity Statistics for 2020: Varonis.* Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/

Steinberg, S. (2020, March 9). *Cyberattacks now cost companies $200,000 on average, putting many out of business.* Retrieved from https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Ponemon Institute (2017), *2017 Cost of Data Breach Study: Global Overview* https://www.ibm.com/downloads/cas/ZYKLN2E3

Figure 1: Infographic Depicting Statistics of Cyber Attacks on Small Businesses.

2.4 Why are SMBs Underprepared

A main reason SMBs lack the proper security measures is because the upgrade or establishment of a security system could cost more than they are willing to spend (Wirth, 2017). The lack of a fixed cost for information security is a large deterrent, even as the volume of data and information these businesses protect doubles each year (Johnson, 2015; Bojanc and Jerman-Blažič, 2012). A PriceWaterhouseCoopers survey in the UK reports that incidents can cost £15000 - £30000 per small organization, around $16,000 - $32,5000 (Ng, Ahmed, and Maynard, 2013).

Proactive SMBs have been shifting the focus away from what is technically feasible to what is fiscally responsible (Bojanc and Jerman-Blažič, 2012). However, a drawback to this trend or strategy is figuring out what is "economically optimal" for one specific SMB compared to another. There are, however, specific guidelines that businesses must follow. The 1998 UK Data Protection Act is the standard that UK businesses follow, and most U.S. businesses have agreed to follow. The most important principle outlines the need for personal data to be secure (Manning, 2015). This principle details that a business must take all "appropriate measures" to keep personal data safe, including educating themselves and their employees through training sessions (Manning, 2015). Switzerland, along with more than thirty other countries, is a part of the Council of Europe's Convention on Cybercrime, held in November of 2001. This Convention seeks to combat cybercrime by creating national laws that work together, improving investigative abilities, and boosting international cooperation.

Regulation and policies can only go so far when it comes to cybersecurity. Companies must implement security features to assist these policies, but sometimes this is difficult due to the expenses associated with these features. It is hard to know if implementing security features will pay off because a company can't predict what will happen in the future. The cost of an investment includes the price of the required hardware, software, and labor to install, but it is hard to quantify the benefits (Bojanc and Jerman-Blažič, 2012). Return on investment is based on an assessment of the cost savings related to potential events that haven't happened yet, deterring smaller businesses from making that leap. SMBs also have to think about their investment value not being higher than the value of the data they are trying to protect, and sometimes this can lead a business owner to decide not to protect their data (Bojanc and Jerman-Blažič, 2012).

To begin managing a security risk assessment the owner or IT department of a SMB needs a thorough analysis and evaluation of the company's assets, the kinds of threats that can attack the company, the consequences if an attack is successful, the probability of a successful attack, and the costs and benefits of investing in a higher level of security. A study conducted by Deloitte and the Financial Services Information Sharing and Analysis Center revealed that on average, businesses spend 10% of their IT budgets on cybersecurity. That would account for approximately 0.2% to 0.9% of a company's revenue, which could be a lot of money for businesses with smaller revenues (Crawley, 2019). Developing better security systems is typically a large project that takes more time and money than an SMB is willing to put out (Bojanc and Jerman-Blažič, 2012).

2.5 Cyber Insurance

Cyber insurance is an insurance product designed to help businesses hedge against the devastating effects of cybercrimes. Cyber insurance is an effective way to prepare for cybersecurity attacks because the premium is a fixed price that can be budgeted for since SMBs may be unable to set aside large arbitrary sums of money for security. Cyber insurance offers broad coverage, which can help protect businesses from technology-related risks. Two main types of cyber insurance include cyber liability insurance and data breach insurance. Cyber liability insurance is mainly used by larger businesses and offers more coverage to help prepare for, respond to and recover from cyberattacks, whereas data breach insurance helps businesses respond to breaches and can offer protection for small business owners (The Hartford, 2020). If a small business is the victim of a breach, data breach coverage can help pay to: notify affected customers, patients, or employees, hire a public relations firm, offer credit monitoring services to data breach victims, and help cover extortion costs (The Hartford, 2020). For larger businesses, cyber liability insurance can help cover: legal services to help meet state and federal regulations, notification expenses to alert affected customers that their personal information was compromised, extortion paid to recover locked files in a ransomware attack, and lost income from a network outage and much more.

The cost of cyber insurance is not the same for all businesses. Different factors such as the number of customers, clients or patients, type of sensitive data, information stored, revenue, and claims history all affect your ability to get cyber insurance as well as its cost. When comparing costs from various companies, some stated that based on the factors mentioned above, some annual policies might cost around $500, while others cost $5,000 or more (Progressive Commercial, 2020). Only about 35% of firms in the United States said they carry cyber insurance, which is up from 31% in 2018, leaving the other 65% of firms with a lack of support if a breach occurs (J.D Power, 2019). While cyber insurance is a useful way to mitigate an attack's damages, coverage does not help prevent a cyber-attack or data breach. Moreover, the level of IT security that a business has can greatly affect the price of coverage (Progressive Commercial, 2020). Cyber-insurance makes IT security investment less cost prohibitive, reduces risk to a company, and can create incentives for research and development (Böhme, 2005). Therefore, cyber insurance should not replace traditional security measures, but rather provide a safety net in the event of a breach.

2.6 SMBs Undervalue IT Security Measures

Even if an SMB has the money to put towards a security upgrade or implementation, many business owners undervalue these measures (Wirth, 2017). A business owner needs to know what is at stake to make an educated decision about the security of their company. 12% of the worst security breaches were partly caused by senior management giving insufficient priority to security (UK: Support for small businesses against cyber-attacks). In two studies conducted in 2017 and 2016, Malwarebytes found that ransomware attacks against businesses are on the rise and that nearly a quarter of SMBs that suffer these attacks don't have the resiliency to recover (Appleby, 2019). Knowing what can be done to protect the company and what will happen if it is under threat helps make this decision easier. However, many businesses don't do anything until it is too late.

Upper management of a company often believes that attacks are highly sophisticated and require equally sophisticated defense systems. However, systems are ultimately breached from the internet through vulnerabilities that can be easily identified and mitigated (Appleby, 2019). These "vulnerabilities" are a mix of a system's weaknesses or flaws, an attackers' awareness of these weaknesses, and the attackers' capability to exploit these weaknesses (Appleby, 2019). Organizations can handle risk by implementing controls to prevent the potential breach from occurring (risk avoidance), reducing the impact after the breach has taken place (risk mitigation), doing nothing at all (risk acceptance) or outsourcing to an external party and obtaining insurance (risk transfer) (Ng, Ahmed, and Maynard, 2013). However, to maintain an effective IT security program, policies and procedures need to be developed to match the company's growth. Along with undervaluing these measures, some businesses assume they will not be targeted due to an optimism bias and/or a lack of education on the subject.

2.7 Surveys

A survey is a systematic way of getting information on a specific topic by asking questions and then generalizing the answers to those questions to represent the entire population surveyed. They are an effective way to get information from many people, and the first thing needed to know before conducting a survey is the goal (Rossman and Rallis, 2003). Figuring out what this is will help to make clear and relevant questions. These questions must be crafted to avoid bias, and answers should be multiple-choice, mutually exclusive, and clear. “Double-barreled” questions, with two or more subjects in them, should also be avoided so neither the surveyor nor respondent questions which subject the response is referring to (Schensul and LeCompte, 1999). If respondents were confused during the survey, there will not be useful data to take away from the survey.

2.8 Interviews

The main objective of an interview is “to gain enlightenment on a topic which we as individuals could not gain on our own” (Beebe, J., 2014). While preparing to interview our respondents, we had to keep in mind different tactics to get the most in-depth and honest answers. The first major influence on an interview is the location and environment in which it is taking place. We wanted to ensure that the environment was professional when talking to respondents, yet casual enough where the interviewees felt comfortable sharing information. When interviewing the clients or the average consumer, our interviews were professional. Since all of our interviews were conducted online, we had to adjust some of our interview practices and methods to the virtual medium.

2.9 Our Goal

This project aimed to assess the state of SMBs’ IT Security through surveys and interviews. With the information we received, we created data graphics and looked for similarities and differences. Having this knowledge has given us a better understanding of what the barriers for improvements to SMB’s security needs are.

Chapter 3: Methodology

With SMBs making up 99.6% of all Swiss companies, and being increasingly targeted by hackers, it is more important than ever to find ways to improve the cybersecurity of these businesses that play such a large role in the Swiss and world economy (SME Policy 2019). Even in the face of increasing attacks, many SMBs have yet to make the investments and changes necessary to fend off these attackers and reverse this harmful trend. Business owners often underestimate the threats they face and undervalue the benefit of even basic IT security programs, procedures, and policies. Without informing SMB owners/CEOs, these attacks will continue to occur, affecting the bottom lines of various businesses and their partners.

Working in partnership with the Swiss company Arco IT GmbH, we aimed to develop a publicly available deliverable displayed on our website which was based on our research. It showed the public the importance of implementing strong information security measures and practices (see Appendix A for a description of our sponsor). In addition, we hoped that our research would help to generate a positive change in behavior at these companies. Through presenting security as a cost preventative measure, we aimed to cater to most SMBs' biggest interest, their return on investment (ROI).

This Interactive Qualifying Project (IQP) aimed to understand the different ways small and medium-sized businesses (SMBs) approach IT security. To achieve this goal, we developed two objectives.

1) Assess the state of small businesses' IT security
2) Understand SMBs knowledge of IT security

To accomplish these objectives, our team collected information from surveys and interviews from different companies.

3.1 Objective 1: Assess the state of SMBs' IT Security

The team first sent out a survey to several companies based on their size and industry. We did not limit our research to a certain industry type and monitored our data very closely as it created more variability in our data. This survey was sent out in both English and German and aimed to find out how participants felt about the handling of IT security at their company and the risks that come with not having enough security. The survey consisted of 27 questions (Appendix B) and asked participants to rate these statements on a scale of applicability to their company. Answers were collected through the website (wpicybersecurity.com) using google forms, and participants were asked if they were willing to participate in a follow-up interview. This provided a sample size of 29 participants and offered an opportunity for follow-up interviews where open-ended questions were asked. These surveys yielded a few interview participants that provided more thorough data.

After gathering our data, and using T-Tests and Pearson's correlations, we determined if specific answers are related. T-Tests and Pearson's correlation uses a P-value or an R-value to determine the probability that a result is not due to random chance and to see how strong a correlation is. If $p < 0.05$, it is considered statistically significant. The R-value is between 1 and -1. If it is 1, there is a strong positive correlation, and if it is -1, there is a strong negative correlation.

3.1.1 Conducting Surveys

Our surveys kept questions relevant to the topic and avoided including negatively and positively phrased items (Schensul and LeCompte, 1999). Below are some sample survey questions; the full set is available in appendix B.

A. How confident are you in your organization’s overall security posture? (Select one)
   a. Extremely confident
   b. Very confident
   c. Moderately confident
   d. Slightly confident
   e. Not at all confident

B. If you already have a cybersecurity program in place, is it: (Select all that apply)
   a. In house
   b. Outsourced / Through a managed service
   c. No security program in place
   d. Don’t know

e. Other (please specify)

C. Who ultimately determines the security budget in your organization? (Select one)
   a. Owner
   b. Manager
   c. Accountant
   d. Production Staff
   e. Marketing Team
   f. Security Leader
   g. Other (please specify)

3.2 Objective 2: Understand SMBs knowledge of IT security

We aimed to understand the knowledge of IT security that SMBs have through in-depth interviews. We transcribed this information to be sure that we were addressing the most important data points.

Our main investigation method focused on interviews with employees at various businesses, with different sizes and industries. We did this to try and elucidate their varying extent of understanding, which in turn, aided us during the development of our final research summary. We had a more structured interview using both the points raised by our sponsors and our research.

3.2.1 Interview Approach

When we conducted our interviews, we opened with a question that was broad to get the conversation going. Examples included, “How would you describe your company's cybersecurity?” or “Are you content with the current measures in place?” When getting into more specific questions, we phrased our questions in a non-invasive manner. For example, we asked employees about where they feel they need improvements, rather than asking them to list their weaknesses. We listened more than we spoke and planned our interviews around a few big questions. We planned to keep our interviews to a maximum of 20 minutes, as to not lose the interests of our interviewees. Conducting these interviews with these tactics increased our responses and their depth. (See appendix C for interview topics and discussion questions). We actively wrote meeting notes during our interviews and pulled significant pieces of information from there to add to our results.

3.2.2 Post-Interview Ranking Survey

Upon completion of the interview, we asked participants to briefly take a 5-minute survey sent using Google Forms. Here the participants ranked a number of IT security scenarios to understand how they perceive different threats as compared to statistics displaying the actual threat. These data comparisons were important in illustrating if threats perceived by the companies were valid and if their level of concern for these threats aligned with the measures, they said they'd implement in the interview. (See appendix D for post-interview questions). We used the data we got from this survey to create a graphical depiction and display our findings.

Risk Scenarios:	Participants ranking: (From 1 (lowest) to 10 (highest) each number must appear only once)
Risk of unauthorized access by insiders E.g. Employees attaining something that they shouldn't have access to.	
Risk of deliberate act of sabotage E.g. An employee uses their insider access and/or knowledge to harm the business.	
Risk of deliberate act of data extortion E.g. A hacker stealing data and extorting the company for money to keep it private or using making their data inaccessible until a ransom is paid.	
Risk of compromising intellectual property E.g. Sensitive data related to the company's intellectual property gets stolen and then published.	

Risk of an act of human error or failure E.g. Employees or workers making a mistake that leads to a breach in security.	
Risk of exporting money without taking information E.g. Hackers specifically target the company with a cyber-attack to steal money not data.	
Risk of technical software failures or errors E.g. Due to a failure related to software being used in the business operations, company data is compromised.	
Risk of deliberate act of theft E.g. Data is stolen for its intrinsic value.	
Risk of internal network error E.g. Due to a failure of the company's network security, company data is compromised.	
Risk of forces of nature (flood, fire, earthquake) E.g. A natural disaster wiping out data.	

Table 1- Post-Interview Survey

3.2.3 Adjustments due to a global pandemic

Due to the global COVID-19 pandemic, we conducted our research remotely. We created a project website, which contained both our survey, information about our team, our sponsors, our plan, our project goals, and our results. We then asked our sponsors to distribute the website to their contacts on LinkedIn and Facebook. For those who chose to interview with us after completing the survey, we used the Zoom, and Microsoft Teams platforms. We wrote a condensed version of our final report for our sponsor, Arco IT GmbH, which was displayed on our website (wpicybersecurity.com) at the end of our project.

Chapter 4: Findings and Analysis

We focused primarily on questions to evaluate cyber security:

- How well are small and medium-sized businesses equipped to handle cyberattacks?
- How can these businesses be better prepared for cyberattacks in the future?

To begin, we collected survey responses for two weeks, receiving 29 replies. In week 3, we then set up interviews with five respondents. We asked our interviewees to answer questions during the meeting and to fill out our post-interview survey immediately afterwards. 70% of our survey respondents worked for a company based in the United States and 20% worked for companies based in Switzerland. The remaining 10% of respondents worked for countries based in Europe, mainly Germany. We feel that the main reasons small and medium-sized businesses are underprepared for cyber-attacks are due to lack of skill, awareness, and optimism bias.

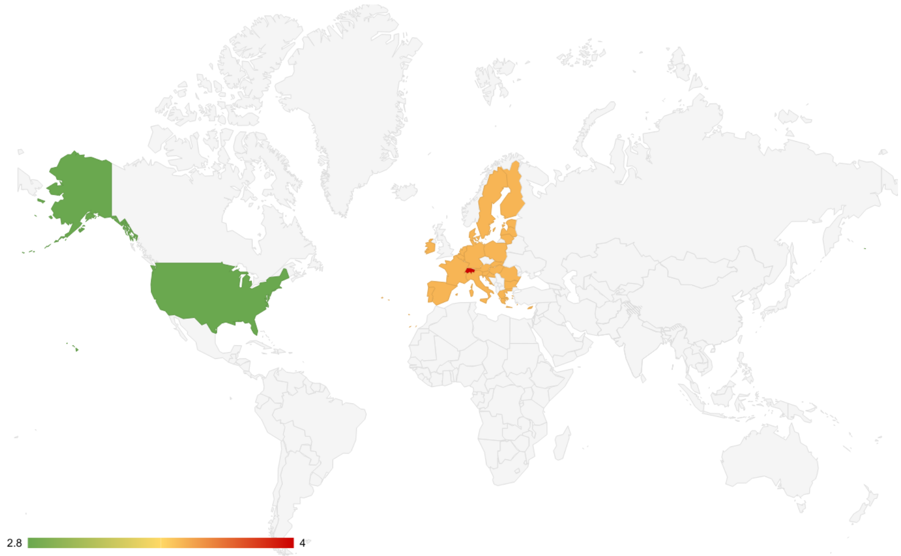


Figure 2: Map detailing the country of our survey respondents.

4.1 Lack of Skill and Awareness

Through our research we found that many companies have employees which lack the cybersecurity skills needed to identify when they have been compromised or differentiate between regular and phishing emails, leading to less awareness of potential threats. The Center for Strategic and International Studies (CSIS) conducted a survey in 2019 of IT decision-makers across 8 countries. In this survey, they found that “82% of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organizations” (Crumpler, W, Lewis, J. A., 2020).

Shown in the survey results, 58% of respondents said that the barriers that inhibit their organization from having exceptional security are related to lack of skill and awareness. 41% of respondents said a shortage of skilled personnel inhibits their organization from adequately defending against cyber-threats, and an additional 41% said lack of awareness inhibits their organization from adequately defending against cyber-threats.

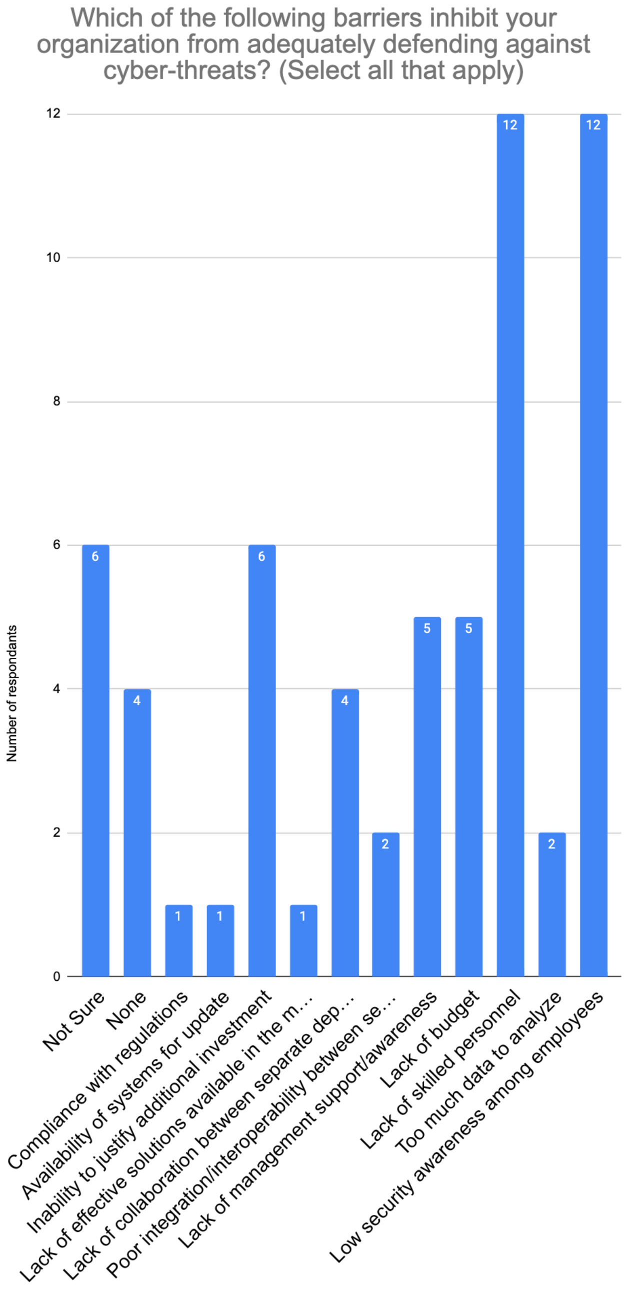


Figure 3: Bar Chart showing which barriers inhibit organizations from adequately defending against cyber-threats.

This explicitly shows that most companies' biggest problem is low security awareness and a lack of skilled personnel. This was addressed in the background chapter, where it was said that education is one of the most important things to address when trying to develop better cybersecurity practices. One participant who interviewed with us said that they had consultant IT professionals come in and train their staff about good IT practices and what to do when faced with something harmful. They liked this but would rather have an educational training video to be brought to the office. Since their company is mainly staffed with older workers, they often cannot keep up with the person training them and refrain from asking questions. To further this point, the interviewee even remarked that if there was a video paired with the training, employees could reference it later as a refresher, instead of just disregarding their training.

The blame cannot solely be placed on employees and their lack of knowledge of beneficial practices. 12% of the worst security breaches were partly caused by senior management giving insufficient priority to security (UK: Support for small businesses against cyber-attacks). 62% of respondents replied that their cybersecurity practices were put in place by the owner of their company, not someone trained specifically in IT security. Lack of education and lack of priority tie into each other and cause a cycle of inadequate security practices.

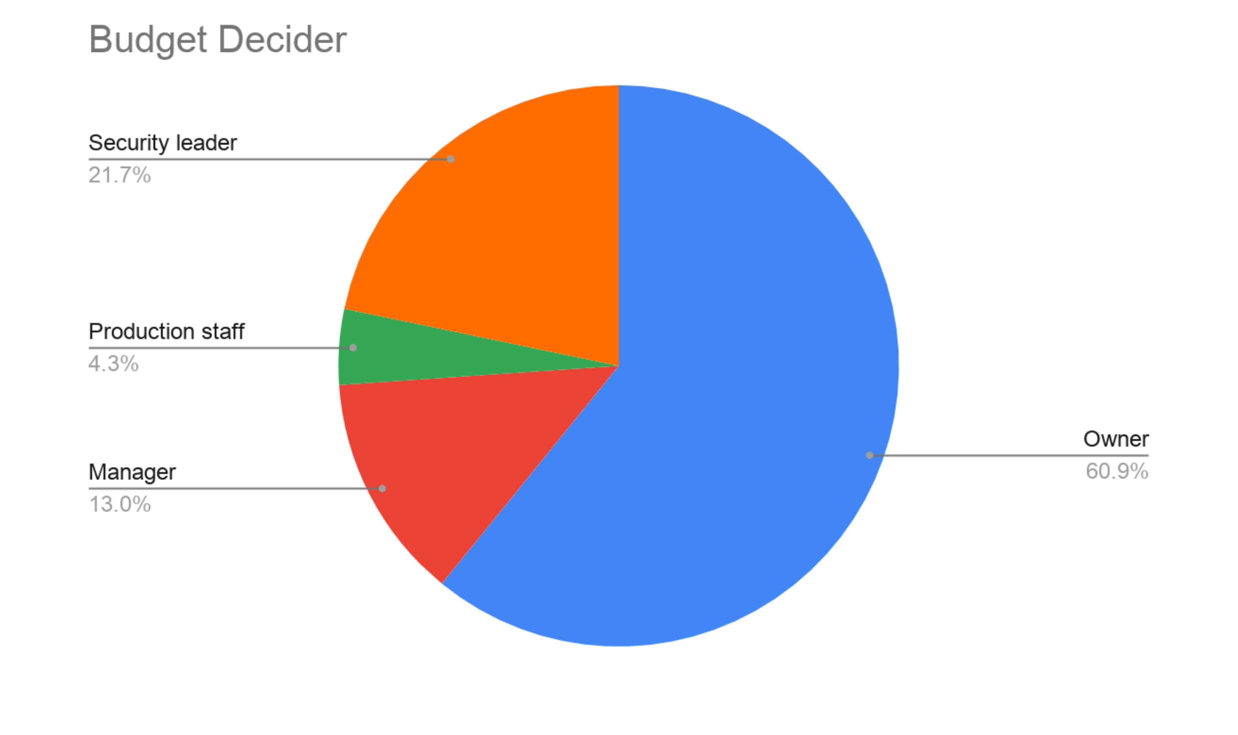


Figure 4: Pie chart of who decides the budget in the businesses surveyed.

4.2 Optimism Bias

Another harmful misconception is the belief that a company is above being targeted by a hacker. When thinking about data breaches and hacks, we often think about large businesses, but that is not the case. Small and medium-sized businesses are also targeted due to their lack of cybersecurity, making them easy targets. A study conducted by DNG technology found that 43% of all cyberattacks target small businesses but only about 16% of small business owners are concerned about potential cyberattacks (Your Optimism Bias Will Impact Your Website Security, 2019). This gap is significant because it shows the difference between the small number of businesses that take cybersecurity seriously and the larger number of businesses that get attacked.

Data breach statistics suggest that 60% of them will go out of business within 6 months of a successful attack (Your Optimism Bias Will Impact Your Website Security, 2019). This can be because of the debt incurred from it, a loss of customer trust, or a loss of significant data. It was found that the best way to combat this type of optimism bias is to put the risk faced in easy enough language for any organization to understand. This does not necessarily mean making a large financial investment, but rather focusing on updating policies which can mitigate the security threats (Hay, 2018).

50% of the people who responded to our survey and said that a cybersecurity-related incident had impacted them in the past 2 years also said they had no concern that it would happen again in the next year. Additionally, 50% of the people affected within the last year said they had no plans to change their approach to cyber security.

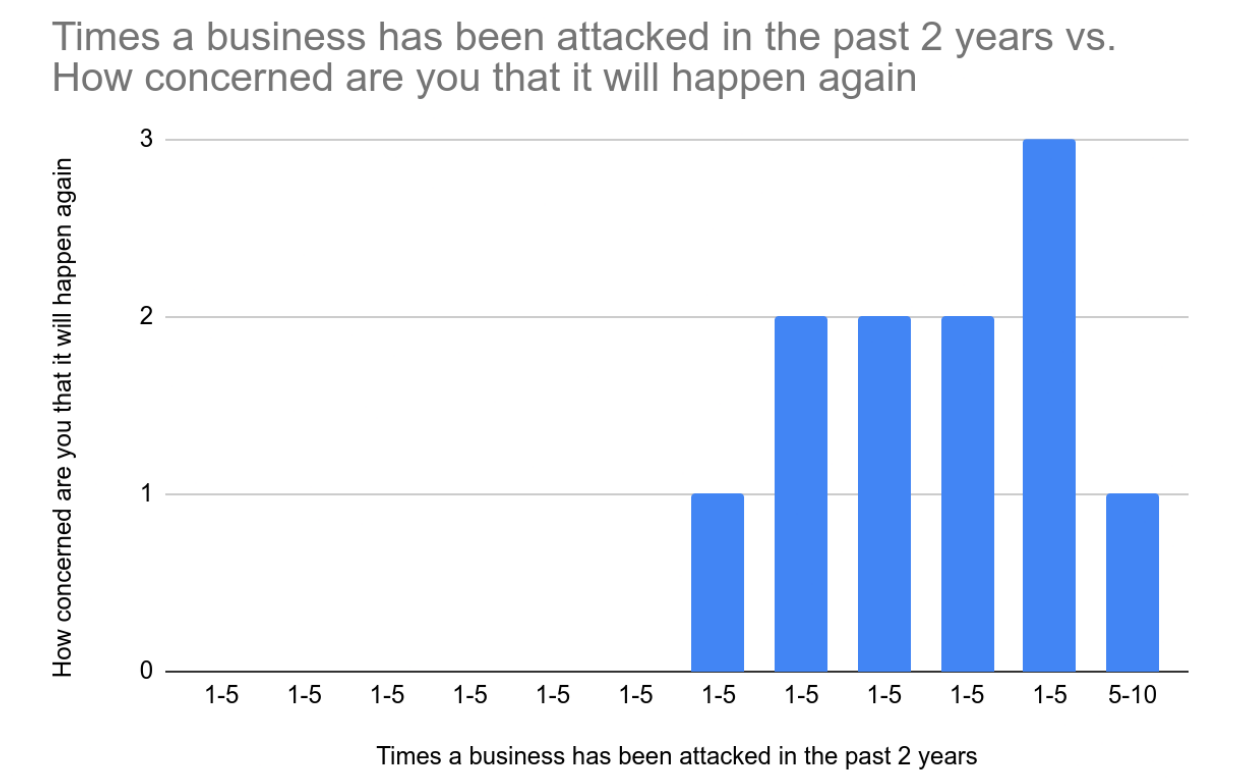


Figure 5: Bar Graph depicting the amount of times a business has been attacked compared to how concerned they are that it will happen again.

0: Not Concerned

1: Slightly Concerned

2: Moderately Concerned

3: Extremely Concerned

Optimism bias is often unfounded and counterproductive, as a study showed that 50% of small businesses reported experiencing a data breach in the past 12 months (Appleby, 2019). In one interview conducted, a participant said that not everyone in his office takes cybersecurity practices seriously. Often, when on breaks, their receptionists "surf the internet" on the company's wifi, opening up the possibility of a malicious attack on the office. Optimism bias can also be related to the perception of being able to control security threats. The only way to overcome this is to increase security awareness training and "systematic treatments" of security threats rather than reactive security responses (Rhee, Rhu, and Kim, 2012). This ties back into the previous point on the importance of education and increasing awareness regarding good practices.

4.3 Benefits of Having Cybersecurity Training

Having cybersecurity training in place is one of the most proactive and important things a company can do to protect themselves. The benefits of having security awareness training include: reducing errors, enhancing security, increasing compliance, protecting a company's reputation, possibly saving the company itself, boosting morale, saving time and money, and having peace of mind (Moramarco, 2019).

Since many small and medium enterprises do not have a training program in place, governments and local industries in Europe have provided guidance to help these businesses start. For example, in the UK, the Cyber Essentials scheme was launched in 2014. This is a government-backed industry-supported scheme put together to help organizations, especially small and medium-sized businesses, protect themselves against common online threats (Bada, Nurse, 2019). Another great resource for these small and medium-sized businesses is the Information Assurance standard (IASME). This is designed to be simple, affordable, and help improve the cybersecurity practices of SMBs (Bada, Nurse, 2019). The IASME Governance Standard includes information regarding people and processes like training and managing employees (Bada, Nurse, 2019).

The development of good cybersecurity posture and culture in a company is crucial as it can help mitigate the number of attacks businesses face. By increasing awareness and cybersecurity training, businesses can support themselves and face fewer cyber-attacks.

Our survey responses have shown us statistically significant correlations between having a training program in place and increased confidence. It also showed us that most companies either have no formal training of staff or internal staff training.

The first test run was to find a correlation between having training and how confident respondents are with their current organization's security standards. Statistical analysis returned a p-value of less than 0.01 and an R-value of 0.49. This R value shows that there is a positive correlation between the two data points, however it is moderate instead of strong. This statistically shows that as employees are trained in good cybersecurity practices, their confidence in their organization's cybersecurity posture also increases. This increased confidence is different from the confidence seen in optimism bias, as confidence gained from good cybersecurity practices is founded. This is important to note because it shows one of the tangible benefits of training employees.

A second test was done between employee training and having a cybersecurity program in place, whether this is in-house or outsourced. Only 27% of those who do not have a security program in place are training their employees, while 92% of those with a security program are training their employees. This test came back with a p-value of less than 0.0005. This shows a strong significance between the relation of employees being trained and having a security program in place. It makes sense, because a security program costs money and is more effective with trained employees. Additionally, when a company has a program in place to deal with cyber attacks, they are more likely to have informed employees.

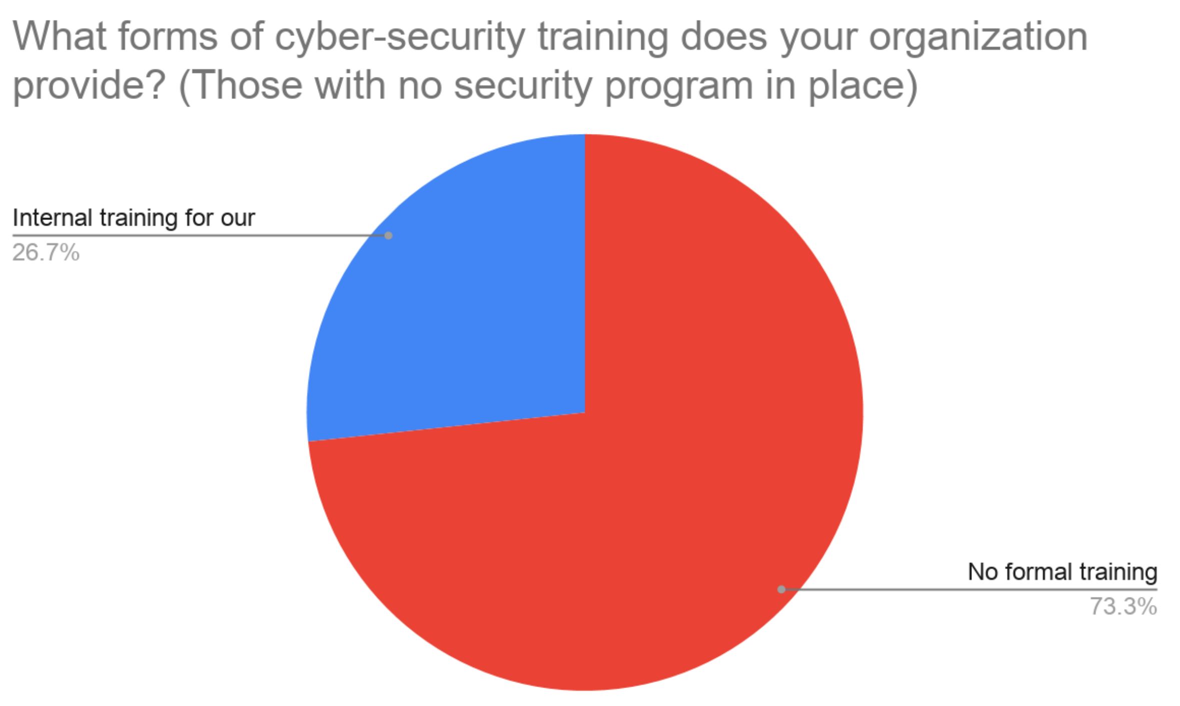


Figure 6: Forms of cybersecurity training when there is no security program in place.

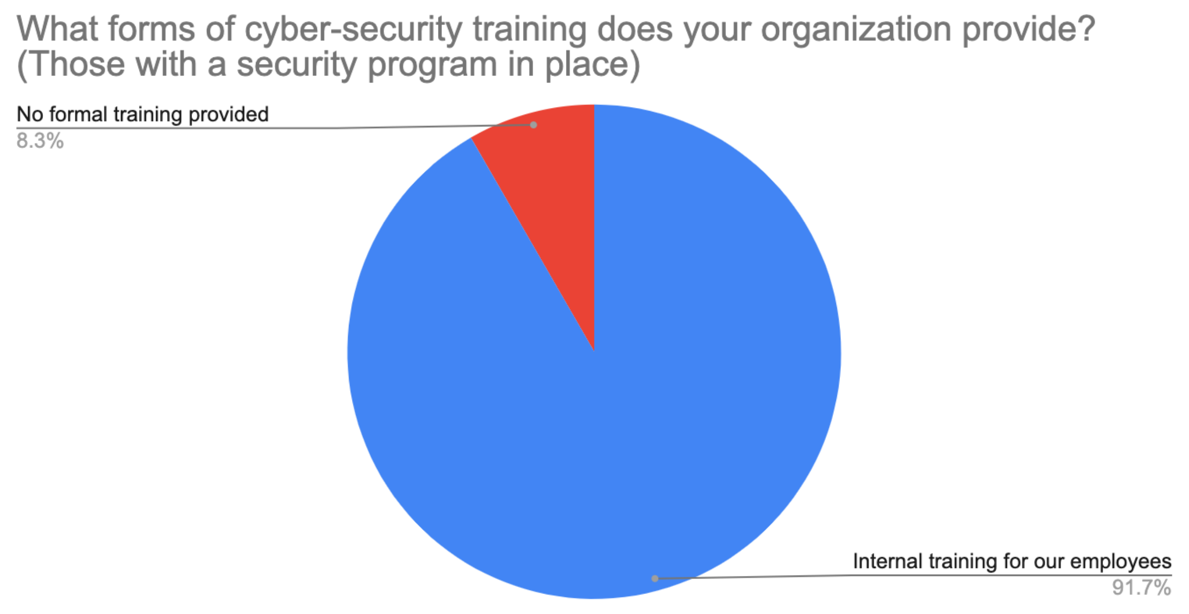


Figure 7: Forms or cybersecurity training when there is a security program in place.

The final test was conducted to better understand the correlation between training employees and a company's culture around cybersecurity decisions. It was found that there is more likely to be training when a security leader is in charge. This test came back with a P-value of 0.00007, showing a strong significance tying the two pieces of data together. This emphasizes that when technically informed people are in managerial positions, employees are more likely to get trained. Prioritizing technical training for those in managerial positions may positively influence the companies' attitude towards cyber security.

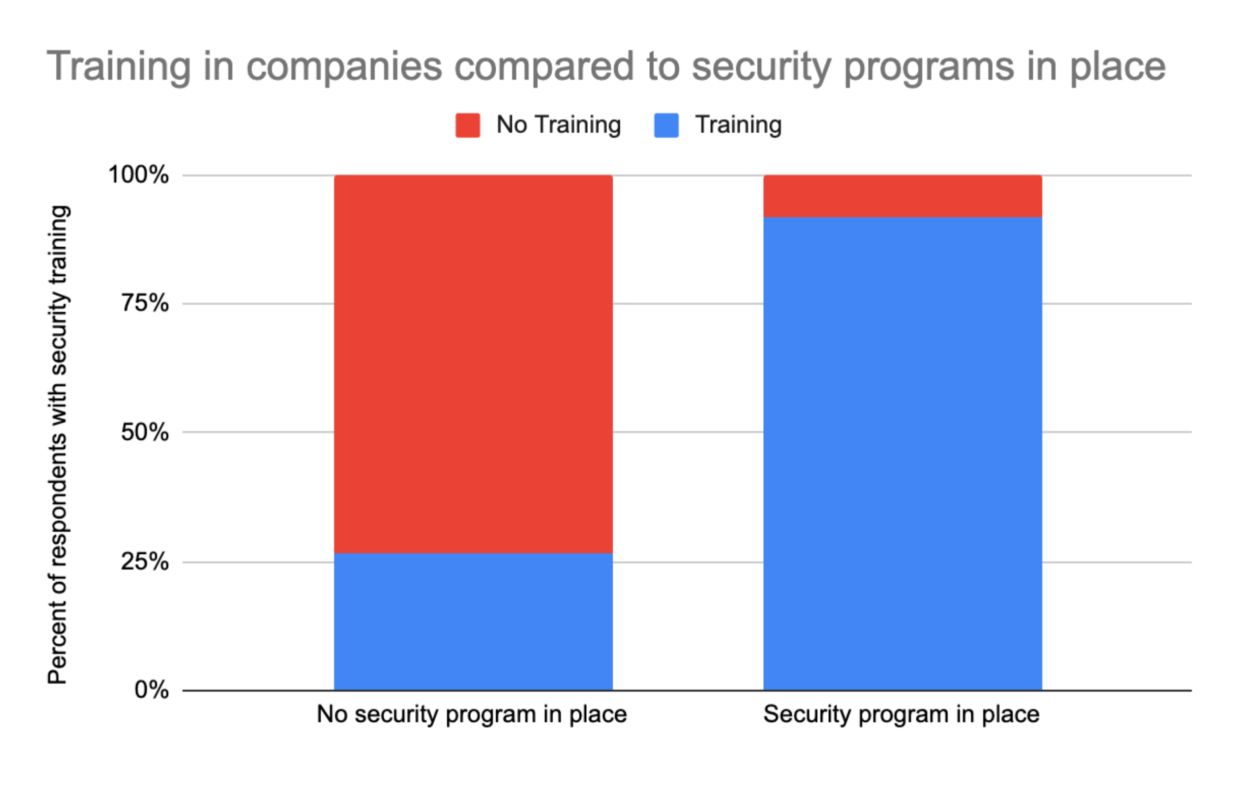


Figure 8: Training depending on Security Programs.

4.4 Relationship to Country

We found a difference between the countries companies are based in and their confidence in their IT security. From our survey, we found that companies based in the United States are slightly more confident in their cybersecurity than companies based in Switzerland or the European Union. We can confidently state this because the T-Test run resulted in a p-value of less than 0.0001. We found no significant difference between the US, Switzerland, and the European Union when comparing the number of cybersecurity incidents to the country. However, on average, companies in the United States take less time to recover than companies in Switzerland or in the European Union. This is proven through the survey data because a T-Test run resulted in a p-value of 0.0002. We believe that the United States elevated confidence might be tied to their decreased time to recover from these attacks.

4.5 Differences Amongst Industries

When looking at the differences in cybersecurity training among different industries, we noticed that companies in manufacturing, engineering, and education were two to three times more likely to have cybersecurity training in place than companies in other fields, such as IT services, residential services or health and engineering. Through a T-Test, we found a p-value of less than 0.0001, proving the correlation is significant. We attribute the lower training rates at IT security companies to a high level of expected understanding amongst their employees. The high rates of training in manufacturing and engineering are likely due to large levels of intellectual property that these businesses protect. We also found that businesses in manufacturing, IT services, or education were also almost 2 times as likely to have plans to update their cybersecurity software, training, or resources in the upcoming 12 months.

4.6 Interview Results

The survey yielded eleven respondents willing to interview with us, and after reaching out, we scheduled five interviews. The participants were from various countries: four from the United States and one from Germany.

The first interviewee was the manager of an IT service provider to law firms, construction companies, and medical providers. He described his approach to cybersecurity as proactive: working to prevent attacks and implementing measures to make recovery easier. Although his clients want to be proactive, the cost of these measures and the time required to implement them often limit what changes they end up making. The systems that he ultimately installs have a good return on investment, which he says, is a very important selling point to his clients. When an attack does occur, he has a specific procedure that he follows. Typically, he receives automatic security notifications, as about 75% of his clients do not have enough knowledge regarding what to do if they have been attacked. Once notified, he then follows up with the company to deploy a solution. Lastly, he believes that user training is essential because a company can have an abundance of security measures, but if employees make a mistake, the effectiveness of these security measures could be negated.

The second interviewee was the president of a manufacturing company and described his approach as proactive. His company employs an outside consultant to update programs and processes. He dislikes the extra security measures because of the extra time it adds to his day-to-day life. This sentiment is shared by his employees, all of which are over 50 and have difficulties learning or are unwilling to learn the new security measures. Currently, his company doesn't offer any training to educate his employees on security best practices. His company does, however, ask employees to forward suspicious emails to the company's security manager. This policy was implemented after they were sent a job application containing a virus which resulted in a four-day period where the company was down. He suggested that emphasizing the return on investment of security procedures could be beneficial when convincing companies to install security systems.

The third interviewee was a local IT manager of a very large engineering company which is proactive about their security measures, providing yearly training for their employees. She ensures that employees in her region comply with all national rules, such as updating their computer whenever new security updates are released. Her main concerns lie with senior engineers who do not want to take the time out of their work schedule to commit to a full update of their computer.

The fourth interviewee is the head of a small cybersecurity company based in Germany, with a very proactive approach to cyber security. They deem this approach necessary because all of their data are in the cloud, therefore their company could not operate if their IT infrastructure were offline. She is worried about her reputation and her clients' application systems if her business were to be attacked. The companies she works with believe that the systems she implements are both a hindrance and too expensive. However, she convinces them that these systems are worthwhile by showing examples of companies that were attacked and by emphasizing the cost of getting hit with a cyberattack. This cost would be much greater than what the company would be spending to prevent such an attack. This return on investment is often hard to estimate, as it is a measure of something trying to be prevented.

The fifth and final interviewee is part of a drop shipping company that takes vendor products and sells them on Shopify. Their response to cybersecurity is reactive, rather than proactive and could not run if their core IT infrastructure went offline. This has happened to them several times in the past few months when they lost their wifi due to router problems, resulting in a day and a half of lost work. Their company does not prioritize cybersecurity because they believe that their small size does not make them a target. Instead, their main priority is to ensure they have a stable internet connection, and their customers receive products on time. His company has no defined protocol for if they are attacked and no security training for employees either. Ultimately, he believes that a higher baseline of cyber security knowledge for all employees is a good starting point to begin protecting themselves.

He also mentioned that he knew of another company close to him that suffered a ransomware attack. The hackers were in their systems for three months, encrypted all of their data, preventing them from doing business, and held all the company's data for a ransom of 3 million dollars. They hired an outside company to retrieve the lost data, investigate how the hackers got in, and set up a consulting process to prevent another attack. They ultimately had to spend about 1.5 million US dollars and their business was down for about two weeks. They now send regular simulated phishing emails to their employees to continually evaluate their ability to detect potential security threats.

There were many similarities between the first four interviews, with the fifth interview being an outlier. Our first four interviewees were all in the IT department of their company and described their companies' approach to cybersecurity as proactive. The last interviewee differed, as he was not a part of the IT department and described his company's approach to security as reactive. Most interviewees believed that the return on investment of a security system was a key factor when convincing clients to invest. Additionally, they all believed that training was important to secure their company.

We found that across the board there were various levels of training in each company and varying procedures for when an attack occurs. The third interviewee, the only person we interviewed which was part of a large company consisting of more than 250 employees, viewed cybersecurity as a loss that they could handle because they had the capital to do so. Those that we interviewed which were a part of a smaller company emphasized that cybersecurity investments were not a financial loss because of its return on investment.

The post-interview survey was administered directly after we concluded the interviews, and respondents were asked to rank ten scenarios from most to least likelihood of occurrence. We found that "risk of human error" and "risk of software failure" were ranked the highest, and that the "risk of compromising intellectual property" and "risk of forces of nature" were ranked the lowest. This reiterates our argument that training is important in reducing human error and having an individual that is knowledgeable in IT security is important for the success of businesses.

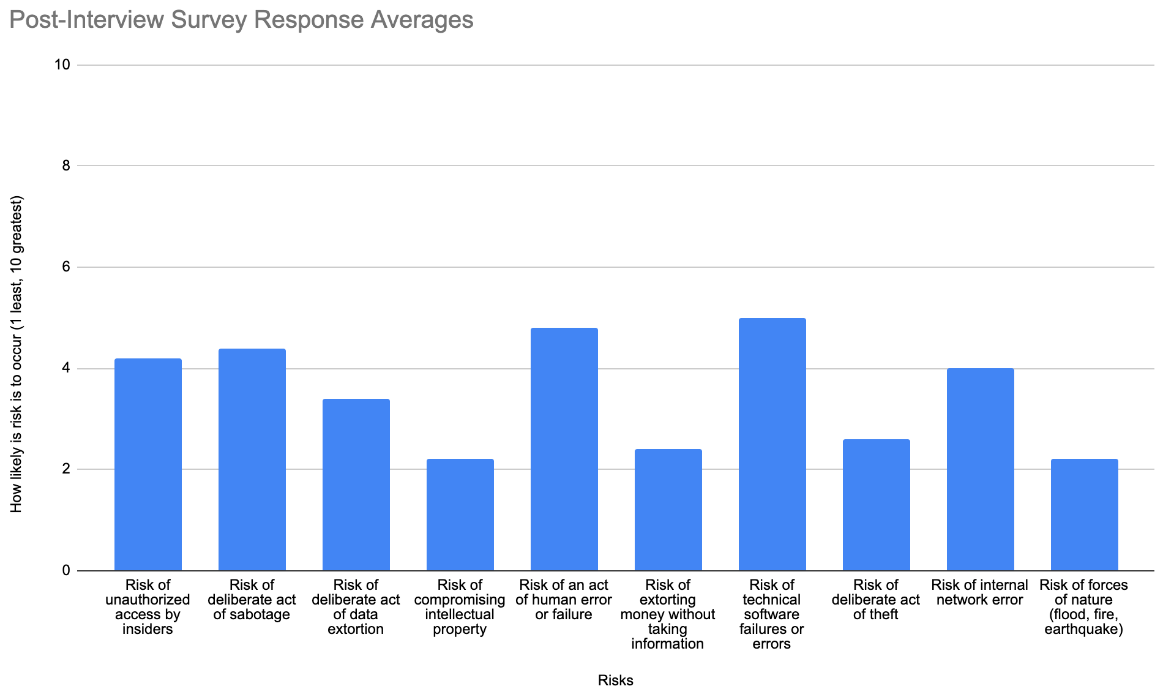


Figure 9: Averaged responses of our post interview survey ranking how respondents viewed various risk scenarios.

4.7 Result Conclusions

Our survey showed us that the biggest inhibitors to adopting good cybersecurity practices are due to lack of skill, awareness, and optimism bias. Lack of skill and awareness tie into each other to create an uninformed workplace, which can additionally be exacerbated by the misconception that one business is above the threat of cyber-attacks. Ultimately, this can be mitigated by increasing workplace training. We also found through our survey results that these businesses opted not to improve their security programs even after falling victim to attacks. This could be due to a myriad of reasons, such as budget deficiencies or lack of priority. However, everyone we interviewed had a good system in place and was happy with their company's cybersecurity stance. Additionally, through the interviews, we learned that those most opposed to advanced security measures were older and more senior level employees, who were reluctant to learn or keep up with skills. The biggest trend we noticed was the importance of employees receiving cybersecurity training. Numerous other positive factors were linked to a company that actively trained its employees, such as increased confidence in their IT infrastructure.

Chapter 5: Conclusions and Recommendations

After having analyzed the data collected through our surveys and interviews, we drew conclusions from what we found. One of the most glaring constants across our surveys and interviews is that cybersecurity measures are often seen as a hindrance to many employees. This can be attributed to a lack of training and technical knowledge. 50% of those surveyed do not have a specific cyber-security program in place, and 45% of respondents are given no training in good cyber security practices from their company. Since many companies do not offer any formal IT training to their employees, they are all significantly slowed down by security measures, especially less technically savvy employees, due to the extra time imposed by two-factor authentication or single sign-on. Furthermore, through an interview conducted we found that when employees receive training, some have too much pride to ask for clarifications or inform the trainer if they need additional training.

Individuals with more knowledge of IT security practices also view cybersecurity as a return on investment rather than as a cost of business. This knowledge makes them more likely to allocate additional resources to their cybersecurity as they see the monetary benefits of being proactive. Having this knowledge also helps gauge what the necessary expenses are versus what is unnecessary. However, explaining return on investment in cybersecurity to SMBs is sometimes difficult because it measures what is trying to be prevented.

Through our interviews, we gained some critical information. We found that not enough people invest in holistic IT security procedures: antivirus software, incident protocols, employee training, and scheduled security updates. Doing so would create a well-rounded security system which protects against many different avenues of attack. Additionally, we confirmed that it is easier for larger businesses to invest in quality cybersecurity measures because they have the capital to do so.

5.1 Recommendations

To remedy some of the barriers SMBs face when trying to adopt IT security measures, we recommend that every company provide IT cybersecurity training and supporting materials such as videos or guides. As mentioned in the interview section, videos explaining proper procedures can be referenced at any time, whenever needed. These can be generic videos, but they should also be supplemented with detailed training videos from informed consultants, catered to their companies' IT environments. This is imperative, as training can teach employees why there is a need for these security measures and how to carry out these procedures accurately.

Another recommendation is to conduct simulated phishing attacks on employees to assess their current cybersecurity knowledge and to determine if they need additional training, such as those mentioned in the interview section. Doing this regularly allows businesses to target employees that pose the greatest liability and assess if their previous training was effective.

Our next recommendation is to have an employee dedicated to reviewing the organization's cybersecurity and IT infrastructure. This could either be an in-house employee who is proficient in IT security or an outside consultant. In certain circumstances, outside consultants can be paired with cyber insurance to cover data recovery measures after a breach has occurred. They can train employees, deploy countermeasures if an attack is encountered, and handle any concerns along the way. This is because having a dedicated employee will ensure that an organization maintains good cybersecurity practices. Through a T-Test, we found a P value of less than 0.0001, confirming the statistical significance correlation showing that having an educated employee in IT security made it more likely that businesses had training in place for employees. Additionally, everyone we interviewed said they could not continue their work efficiently if their IT infrastructure were down, reiterating why having an informed IT security staff member is important.

Finally, we recommend that each company hold annual IT seminars. These can foster good cybersecurity practices and additionally reinforce knowledge already possessed by employees. If companies are too small to conduct their own, we recommend finding a regional information session to have employees attend. Seminars can give employees intensive exposure to expert knowledge, the opportunity to network with others in their field, and a renewed motivation for upholding proficient security practices (Chemers, Hu, and Garcia, 2001).

5.2 Expectations vs. Findings

When collecting our data, we noticed a few surprising things. When initially going into our research, we believed that everyone would have suffered a cyberattack within the last two years. In reality, we found that only 44% of respondents had fallen victim to a cyber-attack in the last two years. This contrasts a survey by the Ponemon Institute in 2017, which found that a typical firm experienced 130 security breaches a year. According to the survey, it was also found that 40% of respondents indicated the number of cyber "incidents" associated with malware had increased each year, starting from 2014 (Council of Economic Advisers, 2018).

We also believed that every company would have a technically informed member in charge of their IT security. This again was a mistake, as only 19% of those interviewed had a specific security leader in charge of their budget. According to McAfee, even though 480 new high-tech threats are introduced every minute, human error is still the number one greatest threat to a business's well-being. This is confirmed through our post interview survey results as well, where "human error" was ranked the most likely to occur. They have also found that not all businesses have enough IT security knowledgeable employees in house, with only 3 out of 10 individuals receiving annual cybersecurity training (Steinberg, 2019). However, 59% of our respondents replied that they had received some sort of cybersecurity training, whether this be internal training, classroom training, or through handbooks.

We initially believed there to be a direct correlation between size and amount of times attacked, however, after running statistical analyses, we could not prove this. We found that over 70% of cyberattacks administered in the United States are pointed at small businesses (Koulopoulos, 2017). Along with this, another T-Test determined that there is no significant relationship between confidence in cybersecurity practices and the number of times the company had been impacted. We thought that being attacked less would be connected to having higher confidence in their company's security. However, a T-test proved this was not the case.

Another T-Test was run on the significance of the correlation between the change of risk within the past year and any attempts to change security measures. We thought that if a company believed that their risk had increased within the past year, they would also plan to evolve their security measures, but again this was unfounded. Overall, we have found no correlation between the confidence a business has in their cybersecurity posture and how many times they have been impacted in the last 24 months. Although we found no correlation between confidence and impact for these businesses, a study conducted by the Ponemon Institute and Switchfast Technologies, found that 51% of SMB leaders say that they are not a target of cyberattacks. However, 61% of these businesses surveyed experienced a cyberattack in the last year (Gendre, 2019). This is contrasted in our survey results where only 40% of respondents experienced an attack in the past two years.

5.3 Future Improvements

Looking back on our project, there are a few things we would choose to do differently. Had we made our project scope more thorough and outlined our critical path to success, there would not have been an overestimation in the project's slack time. We would have created the website over the summer, so we could have gotten it approved earlier in the term. Due to delays caused by requests for website revisions, we had a smaller window for data collection than initially anticipated. Additionally, we would refrain from any translations until everything in English is finalized instead of wasting time translating infographics and our websites text multiple times unnecessarily. These changes would have allowed us to send out our survey earlier, and in turn, would have enabled us to conduct more interviews. Our compressed project schedule did not affect the project's completion but did diminish our sample size.

The other area of improvement would be the asynchronous communication between the team and the project sponsor. Due to the global COVID-19 pandemic, the project was made fully remote. This unforeseen change initially seemed pretty manageable, however it exacerbated the delays mentioned above. Virtual meetings were difficult to organize due to time zone differences and email responses often took longer due to differing schedules. Had we leveraged faster means of communication like instant messaging groups and collaborative document editing means, this issue could have been mitigated.

Ultimately, we are hopeful that this project has made a modest contribution to improve cybersecurity measures in small to medium-sized businesses by defining threats, addressing barriers, and proposing changes.

References

Appleby, A. (2019, January 31). *Three reasons why small and medium-sized businesses fail at cybersecurity - and what they can do about it*. Explore Our Thinking: Plante Moran. https://www.plantemoran.com/explore-our-thinking/insight/2019/01/three-reasons-why-small-and-medium-sized-businesses-fail-at-cybersecurity.

Akbari Roumani, M., Fung, C. C., Rai, S., & Xie, H. (2016). Value analysis of cyber security based on attack types. *ITMSOC: Transactions on Innovation and Business Engineering*, *1*, 34-39.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393-410. doi:http://dx.doi.org/10.1108/ICS-07-2018-0080

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy, 224*(1), 75.

Beebe, J. (2014), pgs. 55-56. *Rapid qualitative inquiry: a field guide to team-based assessment* (2nd ed.). Lanham, Maryland: Rowman & Littlefield.

Bojanc, R., & Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija*, 45(6), 276-288. https://doi.org/10.2478/v10051-012-0027-z

Chemers, M. M., Hu, L.-t., & Garcia, B. F. (2001). Academic self-efficacy and first year college student performance and adjustment. *Journal of Educational Psychology, 93*(1), 55–64. https://doi.org/10.1037/0022-0663.93.1.55

Crawley, K. (2019) *How to justify your cybersecurity budget in 2019.*

https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget

The Council of Economic Advisers. (2018, February). *The Cost of Malicious Cyber Activity to the U.S. Economy*. The White House. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Crumpler, W., & Lewis, J. A. (2020, May 22). *The cybersecurity workforce gap*. https://www.csis.org/analysis/cybersecurity-workforce-gap.

Davis, J. (2019, March 27). *71% of ransomware attacks targeted small businesses in 2018*. https://healthitsecurity.com/news/71-of-ransomware-attacks-targeted-small-businesses-in-2018**.**

de Ternay, G. (2020, April 4). *Convince your boss: 11 ways to make them say "Yes!"* https://guerric.co.uk/convince-your-boss/.

Fowler, G., Worthen, B. (2011) Hackers Shift Attacks to Small Firms. Wall Street Journal. https://www.wsj.com/articles/SB10001424052702304567604576454173706460768

Gendre, A. (2019, November 5). *How MSPs can sell cybersecurity to overly optimistic SMBs*. Vade Secure. https://www.vadesecure.com/en/how-msps-can-sell-cybersecurity-to-overly-optimistic-smbs/.

George, J. F., Marett, K., & Tilley, P. (2004, January). Deception detection under varying electronic media and warning conditions. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the* (pp. 9-pp). IEEE.

Greene, C., & Stavins, J. (2017). Did the target data breach change consumer assessments of payment card security? *Journal of Payments Strategy & Systems*, *11*(2), 121-133.

Harris, K. D., General, A., & Lookout, A. (2014). Cybersecurity in the Golden State. *California Department of Justice*.

Hay, A. (2018, September 27). *Do you suffer from breach optimism bias?* Forbes. https://www.forbes.com/sites/andrewhayeurope/2018/09/27/do-you-suffer-from-breach-optimism-bias/

J. Chen and C. Guo, "Online Detection and Prevention of Phishing Attacks," 2006 First International Conference on Communications and Networking in China, Beijing, 2006, pp. 1-7, doi: 10.1109/CHINACOM.2006.344718.

Johnson, T. A. (2015). Economic Cost of Cybersecurity. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, *255*, 286.

Kevelighan, S., Lynch, J., Pieffer, D. (2019). *Smaller doesn't mean safer* [White Paper]. Insurance Information Institute. https://www.iii.org/sites/default/files/docs/pdf/small_business_cyber_wp_102319.pdf

Koulopoulos, T. (2017, May 11). *60 Percent of companies fail in 6 months because of this (it's not what you think).* https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Kujawa, A., Zamora, W., Segura, J., Tsing, W., McNeil, A., Artnz, P., Boyd, C., Umawing, J., Collier, N., Reed, T., Rivero, M. (2017). *Cybercrime tactics and techniques: 2017 state* *of malware* [White Paper]. Malwarebytes. https://www.malwarebytes.com/pdf/white-papers/CTNT-Q4-17.pdf.

Ludl, C., McAllister, S., Kirda, E., Kruegel, C., (2007). On the effectiveness of techniques to detect phishing sites. *Secure Systems Lab.* https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.437.232&rep=rep1&type=pdf

Loftis, J. (2018, June 18). *4 scientific ways to convince your boss to say yes every time*. https://coschedule.com/blog/convince-your-boss/

Manning, A. (2015), *Databases for small business: Essentials of database management, data analysis, and staff training for entrepreneurs and professionals.* Apress.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257-266.

McAfee. (2016, July). *Hacking the skills shortage.* McAfee.com. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. *USA Today*. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Moramarco, S. (2019, February 11). 7 *benefits of security awareness training*. https://resources.infosecinstitute.com/7-benefits-of-security-awareness-training/

Morse, E., Raval, V., and Wingender Jr., J. (2011) Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263-273, https://doi.org/10.1080/19393555.2011.611860

Ng, Z., Ahmed, A., Maynard, S. (2013). *Information security management: Factors that influence security investments in SMEs.* Edith Cowan University.

Ponemon Institute (2017). The Data Breach: Business & Financial Impact Report.

Progressive Commercial. 2020. *Cyber Insurance Cost.* https://www.progressivecommercial.com/business-insurance/cyber-insurance/cyber-insarance-cost/

Qin, T., & Burgoon, J. K. (2007, May). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *2007 IEEE Intelligence and Security Informatics* (pp. 152-159). IEEE.

Schnurer, J., Klemmer, T. (1998). *U.S. Patent No. 5,842,002A.* Washington, DC: US Patent Office.

Rhee, H., Ryu, Y., & Kim, C. (2011, December 16). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221-232. https://doi.org/10.1016/j.cose.2011.12.001

Richardson, R., & North, M. M. (2017) Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10-21. https://digitalcommons.kennesaw.edu/facpubs/4276/

Rossman, G. B., & Rallis, S. F. (2003). *Learning in the field: An introduction to qualitative research*. Rowman & Littlefield.

Schensul, J., & LeCompte, M. (1999). *Structured approaches to ethnographic data collection: Surveys.* Rowman & Littlefield.

State Secretariat for Economic Affairs SECO. (n.d.). *SME Policy.* https://www.seco.admin.ch/seco/en/home/Standortfoerderung/KMU-Politik.html

Steinberg, S. (2019, Oct 13). *Cyberattacks now cost companies $200,000 on average, putting many out of business*. CNBC. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

The Hartford. (2020). *Cyber Insurance, Cyber Liability. Data Breach Insurance.*

https://www.thehartford.com/cyber-insurance

Thompson, R. (2014). The small business cybersecurity blindspot. *Risk Management.* http://www.rmmagazine.com/2014/06/01/the-small-business-cybersecurity-blindspot/

UK: Support for small businesses against cyber-attacks. (2012). *Document News, 30*(1), 12-13.

DNG Technology. (2019, June 14). *Your optimism bias will impact your website security*. https://www.dngtech.com.au/item/your-optimism-bias-will-impact-your-website-security.html

Widjaya, I. (2018). *Five small businesses hit hard by hacking*; Resources and Knowledge for the Small Business CEO. Retrieved from http://www.smbceo.com/2018/01/05/5-small-businesses-hit-hard-by-hacking/.

Williams, O. (2019, October 7). *SMBs remain critically unprepared for cyber attacks.* https://tech.newstatesman.com/security/smbs-cyber-attacks

Wirth, A. (2017). *The Economics of Cybersecurity. Biomedical Instrumentation & Technology: Cyber Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World*, Vol. 51, No. s6, pp. 52-59.

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 197-216).

Zetter, K. (2015, September 17). Hacker lexicon: A guide to ransomware, the scary hack that’s on the rise. *Wired*. https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

Appendices

Appendix A: Sponsor Description

Sponsor Name: Arco IT GmbH

Website (German): New Website

Arco IT GmbH is a private company at Albulastrasse 34, 8048 in Zurich, with around 2-10 employees. They are an IT security consulting firm that gets hired by companies to assess their cybersecurity and then provide options for solutions. Their mission statement is “We support you in improving your IT security and in the further development of your IT strategy.”

Arco IT GmbH is independent of manufacturers and suppliers which enables them to objectively assess situations and give neutral advice on clients' decisions. With a focus on small and medium-sized companies, they take into account the operational, financial, regulatory, and personnel needs that are relevant to their clients. “Their team combines many years of experience in various industries with the application of international standards. This enables them to plan and implement projects efficiently and cost-effectively for their clients.”

Appendix B: Preliminary Survey

Informed Consent: We invite you to participate in our survey! We are surveying as a part of our research project to understand the knowledge and level of IT security in small to medium-sized businesses. We will be publishing this research through our university, Worcester Polytechnic Institute, located in Worcester Massachusetts. The objective of our survey is to find out how SMBs handle their cyber security and why they do so in that manner. This survey can be completed in 10 to 15 minutes. Individual responses may be published anonymously, and they will be coded into more general data. However, identifiable information you provide will not be published. This process is voluntary as you can refrain from participating in the survey as a whole or refrain from answering a certain question. Before we begin, I invite you to ask any questions regarding our study. Our team can be contacted through the email alias gr-switzerlanditsecuritya20@wpi.edu, and the internal review board of WPI can be contacted at: IRB Manager (Ruth McKeogh, Tel. 508-831-6699, Email: irb@wpi.edu) and the Human Protection Administrator (Gabriel Johnson, Tel. 508-831-4989, Email: gjohnson@wpi.edu.

Survey Questions:

1. How many people make up your organization?
2. What country are your operations based in?
3. What industry does your organization's work pertain to?
4. How confident are you in your organization’s overall cyber-security posture? (Select one)
    a. Extremely confident
    b. Very confident
    c. Moderately confident
    d. Slightly confident
    e. Not at all confident
5. Please rate your organization's security in the following areas:

Area:	Rating on a scale of 1 (Vulnerable) to 5 (Very Secure) (or no selection, N/A)

Business applications Ex. payroll software, active directory, email, etc.	
Laptops	
Proprietary applications/software	
Social media	
Desktop computing devices	
Mobile devices	
Datacenter (physical or virtual)	
Cloud applications	
Cloud infrastructure	

6. How many times has your company been impacted by cybersecurity related incidents in the last 24 months?
    a. 0
    b. 1-5
    c. 5-10
    d. 10-25
    e. 25-75
    f. More than 75
7. What if any negative impact have these incidents had on the organization (please select all that apply)?
    a. Reduced revenue / lost business
    b. Disrupted business activities
    c. Reduced employee productivity
    d. Increased helpdesk time to repair damage
    e. Regulatory fines

    f. Lawsuit / legal issues
    g. Deployment of IT resources to triage and remediate issue
    h. Loss/compromise of intellectual property
    i. Corporate data loss or theft
    j. Financial loss or theft
    k. Don’t know / unsure
    l. None
    m. Other (please specify)

8. How concerned are you that your organization will fall victim to a cyberattack in the next 12 months?
    a. Extremely concerned
    b. Very concerned
    c. Moderately concerned
    d. Slightly concerned
    e. Not at all concerned
    f. Don't know

9. How long does it take your organization to recover from a cyberattack (on average)?
    a. Less than an hour
    b. Less than a day
    c. Less than a month
    d. Up to three months
    e. Longer than three months
    f. No ability to recover
    g. I don’t know
    h. Can't disclose
    i. Not applicable

10. How has the risk of cybersecurity threats to your company changed?
    a. Greatly increased
    b. Increased
    c. No change
    d. Decreased

e. Greatly decreased

11. If you already have a cybersecurity program in place, is it: (Select all that apply)
    a. In house
    b. Outsourced / Through a managed service
    c. No security program in place
    d. Don’t know
    e. Other (please specify)
12. What types of sensitive data are you most concerned about protecting? (Select all that apply)
    a. Customer data (e.g. names, contact information, credit card data, email, health information)
    b. Sales & marketing data
    c. Employee data (HR, payroll, internal emails, health information)
    d. Contracts, invoices, orders
    e. Financial corporate data
    f. Intellectual property (designs, formulas, blueprints)
    g. DevOps / development data
    h. None
    i. Not sure
    j. Other (please specify)
13. Which of the following barriers inhibit your organization from adequately defending against cyberthreats? (Select all that apply)
    a. Low security awareness among employees
    b. Too much data to analyze
    c. Lack of skilled personnel
    d. Lack of budget
    e. Lack of management support/awareness
    f. Poor integration/interoperability between security solutions
    g. Lack of collaboration between separate departments
    h. Lack of effective solutions available in the market
    i. Inability to justify additional investment

j. Availability of systems for update

k. Compliance with regulations

l. None

m. Not sure

n. Other (please specify)

14. How do you plan to handle your evolving security needs in the next 12 months? (Select all that apply)

a. No change

b. Partner with a managed services provider who will provide the resources

c. Expand existing relationship with managed services provider

d. Add security staff headcount

e. Deploy additional security solutions from hardware/software vendors

f. Train and/or certify existing IT staff to become security experts

g. Use security software from independent software vendor(s)

h. Not sure

i. Other (please specify)

15. Who ultimately determines the security budget in your organization? (Select one)

a. Owner

b. Manager

c. Accountant

d. Production staff

e. Security leader

f. Other (please specify)

16. What forms of cybersecurity training does your organization provide? (Select all that apply)

a. Internal training for our employees

b. Classroom training courses by third-party providers

c. Handbooks

d. Online training courses by third-party providers

e. No formal training provided

f. Other (please specify)

Appendix C: Interview

Informed Consent: We invite you to participate in our follow up interview! We are surveying as a part of our research project to understand the knowledge and level of IT security in small to medium-sized businesses. We will be publishing this research through our university, Worcester Polytechnic Institute, located in Worcester Massachusetts. We are looking for elaboration on our preliminary survey questions on how, and why companies do or do not take certain IT security measures. The interview should take about 30 minutes to complete. Individual responses may be published anonymously, and they will be coded into more general data. However, identifiable information you provide will not be published. This process is voluntary as you can refrain from participating in the survey as a whole or refrain from answering a certain question. Before we begin, I invite you to ask any questions regarding our study. Our team can be contacted through the email alias gr-switzerlanditsecuritya20@wpi.edu, and the internal review board of WPI can be contacted at:
IRB Manager (Ruth McKeogh, Tel. 508-831-6699, Email: irb@wpi.edu) and the Human Protection Administrator (Gabriel Johnson, Tel. 508-831-4989, Email: gjohnson@wpi.edu.

General Thematic Sample Questions (Below are a few potential concerns for discussion):

1. What does IT Security mean to you?
2. Do you think your company needs IT security, why or why not?
3. What is your biggest concern regarding falling victim to a data breach?
    a. Company's reputation and credibility? Why?
    b. Monetary loss/Business operations continuity? Why?
    c. Data privacy? Why?
    d. Data accessibility? Why?
    e. Data integrity? Why?
4. Has your company experienced previous incidents?
    a. If Yes, can you explain what happened
        i. Protocol to define an incident
        ii. Protocol to handle them?
    b. If no, why do you think that is the case?
5. Do you consider security measures to be a help or hindrance?

6. Do cost or resource limits play a role in the security measures implemented?
    a. Is there a return on investment?
7. Are you content with your current IT security measures?
    a. Or do they need further improvement?
8. Do you know of other businesses that had cybersecurity incidents?
    a. How did they handle it/what was the result?
    b. Did that impact your attitude toward the issue?

Appendix D: Post-Interview Survey

Informed Consent: We invite you to participate in our post-interview survey! We are surveying as a part of our research project to understand the knowledge and level of IT security in small to medium-sized businesses. We will be publishing this research through our university, Worcester Polytechnic Institute, located in Worcester Massachusetts. We are looking to find out the perceived risk of these scenarios from our interviewees, this should take 5 minutes or less. Individual responses may be published anonymously, and they will be coded into more general data. However, identifiable information you provide will not be published. This process is voluntary as you can refrain from participating in the survey as a whole or refrain from answering a certain question. Before we begin, I invite you to ask any questions regarding our study. Our team can be contacted through the email alias gr-switzerlanditsecuritya20@wpi.edu, and the internal review board of WPI can be contacted by at:.
IRB Manager (Ruth McKeogh, Tel. 508-831-6699, Email: irb@wpi.edu) and the Human Protection Administrator (Gabriel Johnson, Tel. 508-831-4989, Email: gjohnson@wpi.edu.

Post-Interview Survey:

Risk Scenarios:	Participants ranking: (From 1 (lowest) to 10 (highest) each number must appear only once)
Risk of unauthorized access by insiders E.g. Employees attaining something that they shouldn't have access to.	
Risk of deliberate act of sabotage E.g. An employee uses their insider access and/or knowledge to harm the business.	
Risk of deliberate act of data extortion E.g. A hacker stealing data and extorting the company for money to keep it private, or using making their data	

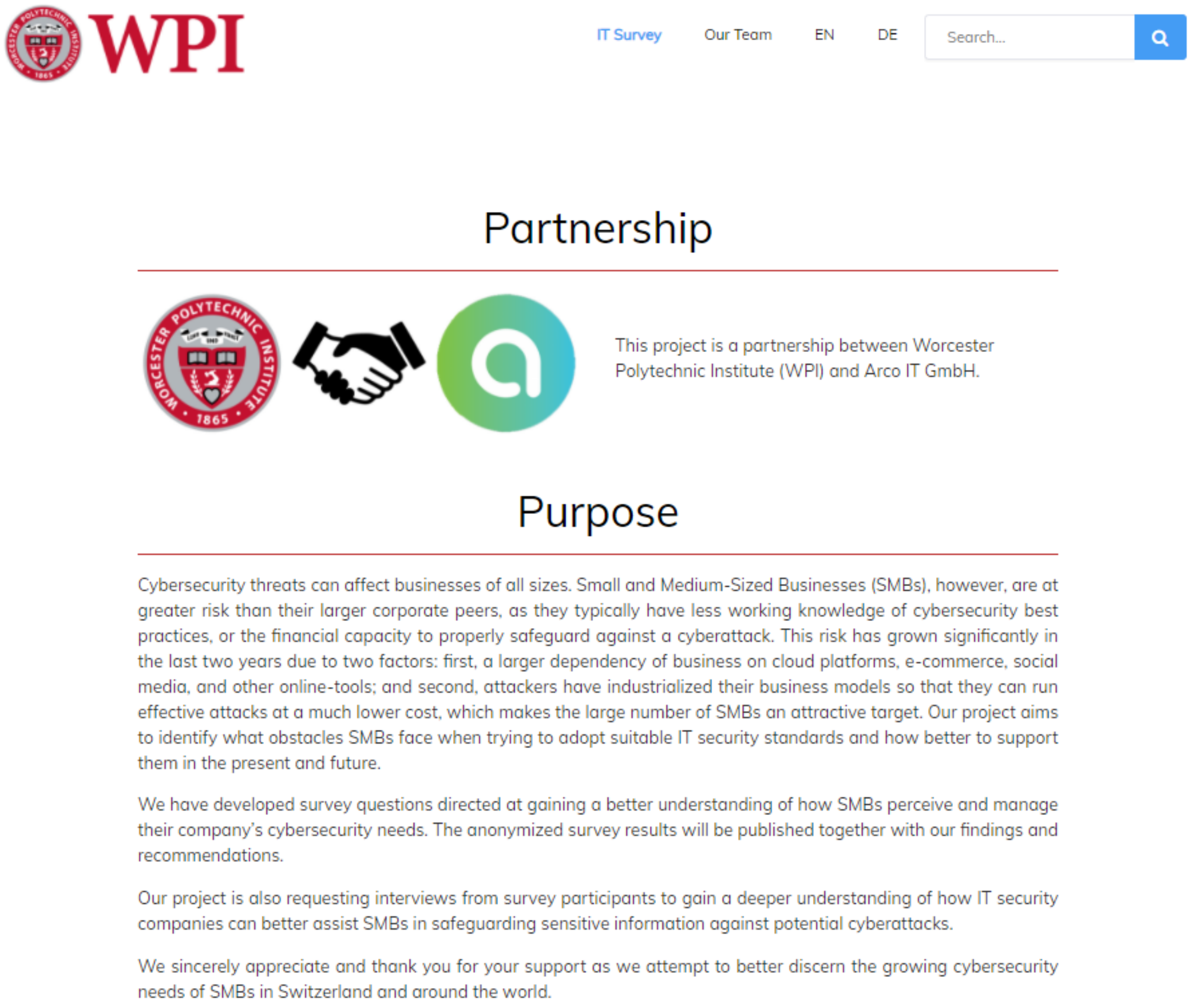
inaccessible until a ransom is paid .	
Risk of compromising intellectual property E.g. Sensitive data related to the company's intellectual property gets stolen and then published.	
Risk of an act of human error or failure E.g. Employees or workers making a mistake that leads to a breach in security.	
Risk of extorting money without taking information E.g. Hackers specifically target the company with a cyber- attack to steal money not data.	
Risk of technical software failures or errors E.g. Due to a failure related to software being used in the business operations, company data is compromised.	
Risk of deliberate act of theft E.g. Data is stolen for its intrinsic value.	
Risk of internal network error E.g. Due to a failure of the company's network security, company data is compromised. .	
Risk of forces of nature (flood, fire, earthquake) E.g. A natural disaster wiping out data.	

Appendix E: Website

We created a website to distribute our survey and display our results. This was created in English, and then translated to German as some of our respondents may have not been proficient in English. Our website was approved by our sponsors and our professors. It has a home page where our partnership, purpose, process and survey is displayed, and it has an additional "Our Team" page. This secondary page has information about our team, what an IQP is, who our sponsors are, and what they do. The third page of our website contains a summary of our report. At the end of our project, we replaced the survey with graphical depictions of the data we received. Below are pictures directly from our website and the URL itself.

Website: https://wpicybersecurity.com/

Landing Page



Partnership

This project is a partnership between Worcester Polytechnic Institute (WPI) and Arco IT GmbH.

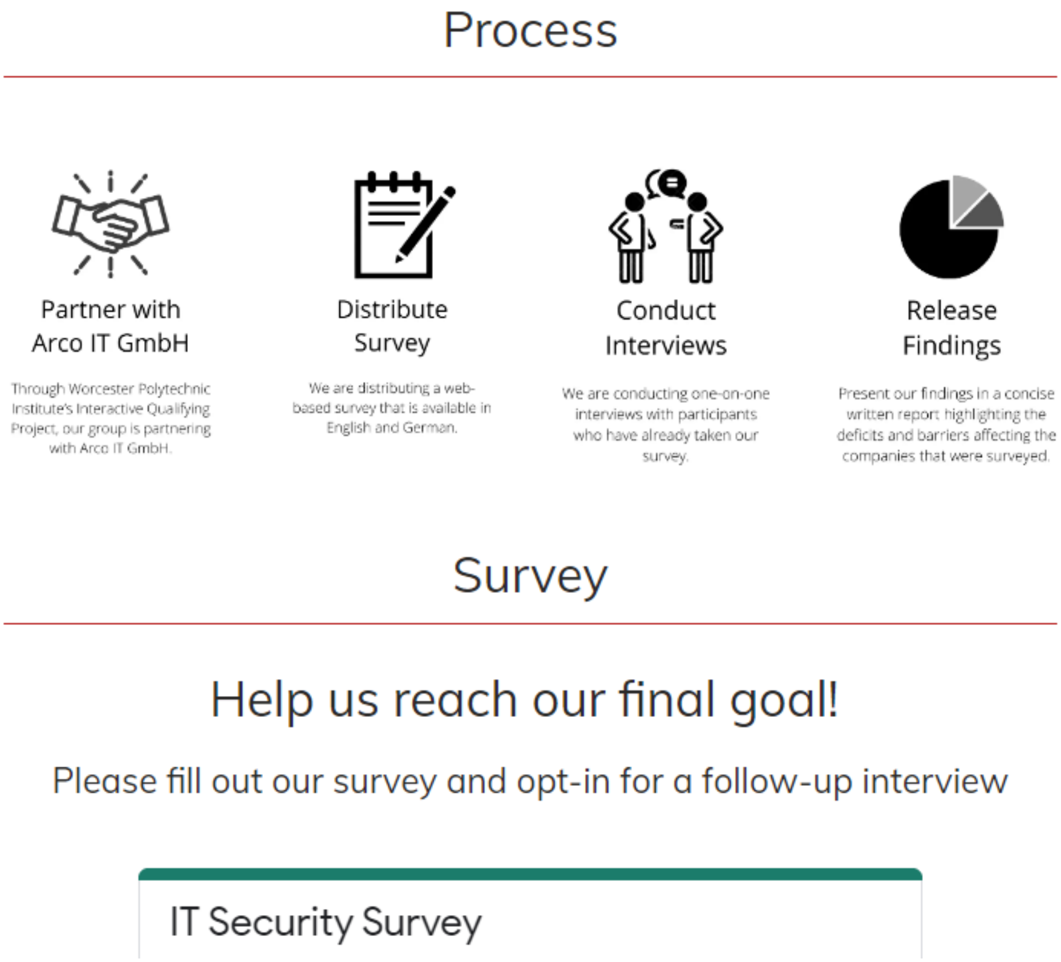
Purpose

Cybersecurity threats can affect businesses of all sizes. Small and Medium-Sized Businesses (SMBs), however, are at greater risk than their larger corporate peers, as they typically have less working knowledge of cybersecurity best practices, or the financial capacity to properly safeguard against a cyberattack. This risk has grown significantly in the last two years due to two factors: first, a larger dependency of business on cloud platforms, e-commerce, social media, and other online-tools; and second, attackers have industrialized their business models so that they can run effective attacks at a much lower cost, which makes the large number of SMBs an attractive target. Our project aims to identify what obstacles SMBs face when trying to adopt suitable IT security standards and how better to support them in the present and future.

We have developed survey questions directed at gaining a better understanding of how SMBs perceive and manage their company's cybersecurity needs. The anonymized survey results will be published together with our findings and recommendations.

Our project is also requesting interviews from survey participants to gain a deeper understanding of how IT security companies can better assist SMBs in safeguarding sensitive information against potential cyberattacks.

We sincerely appreciate and thank you for your support as we attempt to better discern the growing cybersecurity needs of SMBs in Switzerland and around the world.



Process

Partner with Arco IT GmbH

Through Worcester Polytechnic Institute's Interactive Qualifying Project, our group is partnering with Arco IT GmbH.

Distribute Survey

We are distributing a web-based survey that is available in English and German.

Conduct Interviews

We are conducting one-on-one interviews with participants who have already taken our survey.

Release Findings

Present our findings in a concise written report highlighting the deficits and barriers affecting the companies that were surveyed.

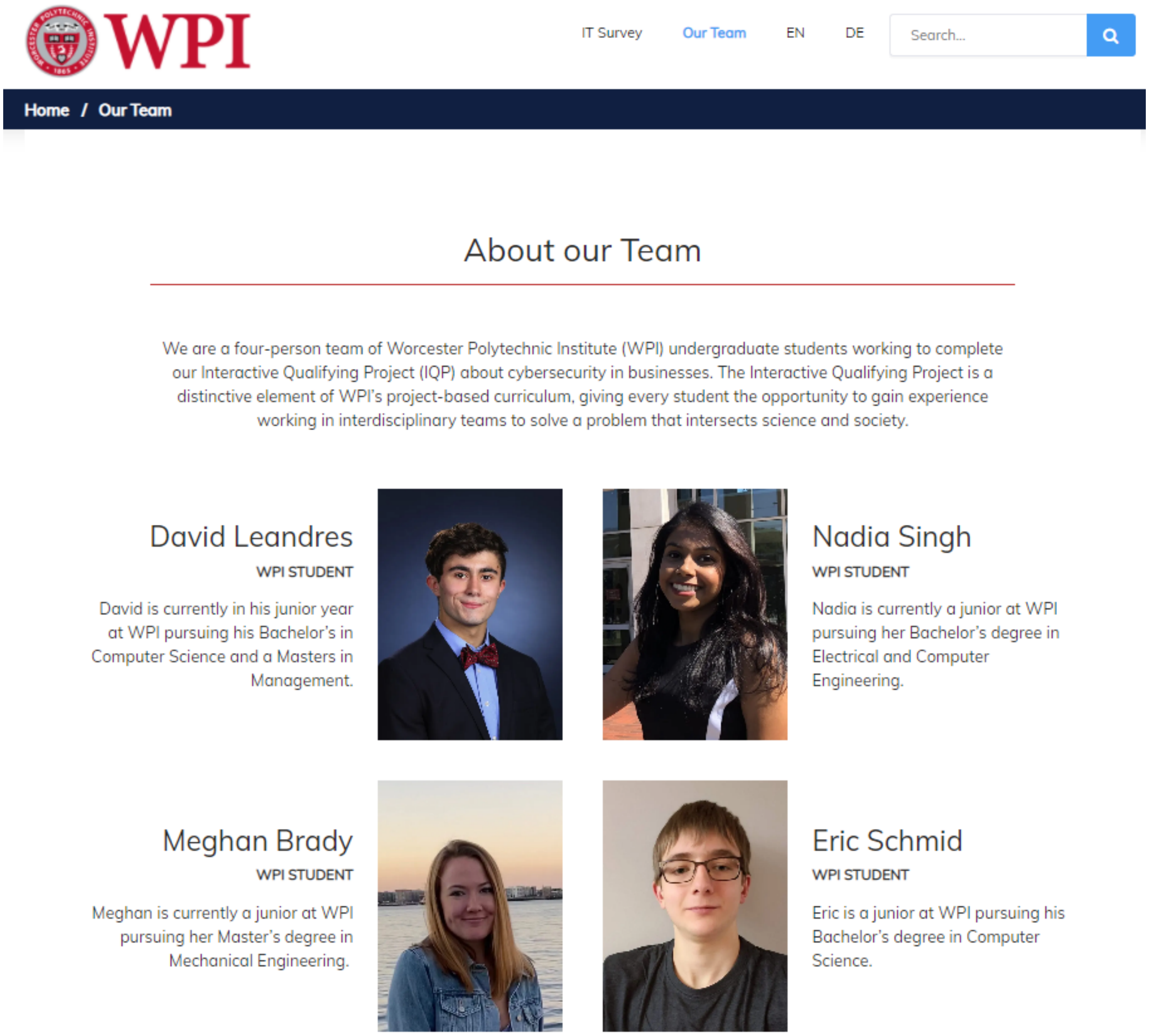
Survey

Help us reach our final goal!

Please fill out our survey and opt-in for a follow-up interview

IT Security Survey

Our Team



About our Team

We are a four-person team of Worcester Polytechnic Institute (WPI) undergraduate students working to complete our Interactive Qualifying Project (IQP) about cybersecurity in businesses. The Interactive Qualifying Project is a distinctive element of WPI's project-based curriculum, giving every student the opportunity to gain experience working in interdisciplinary teams to solve a problem that intersects science and society.

David Leandres

WPI STUDENT

David is currently in his junior year at WPI pursuing his Bachelor's in Computer Science and a Masters in Management.

Nadia Singh

WPI STUDENT

Nadia is currently a junior at WPI pursuing her Bachelor's degree in Electrical and Computer Engineering.

Meghan Brady

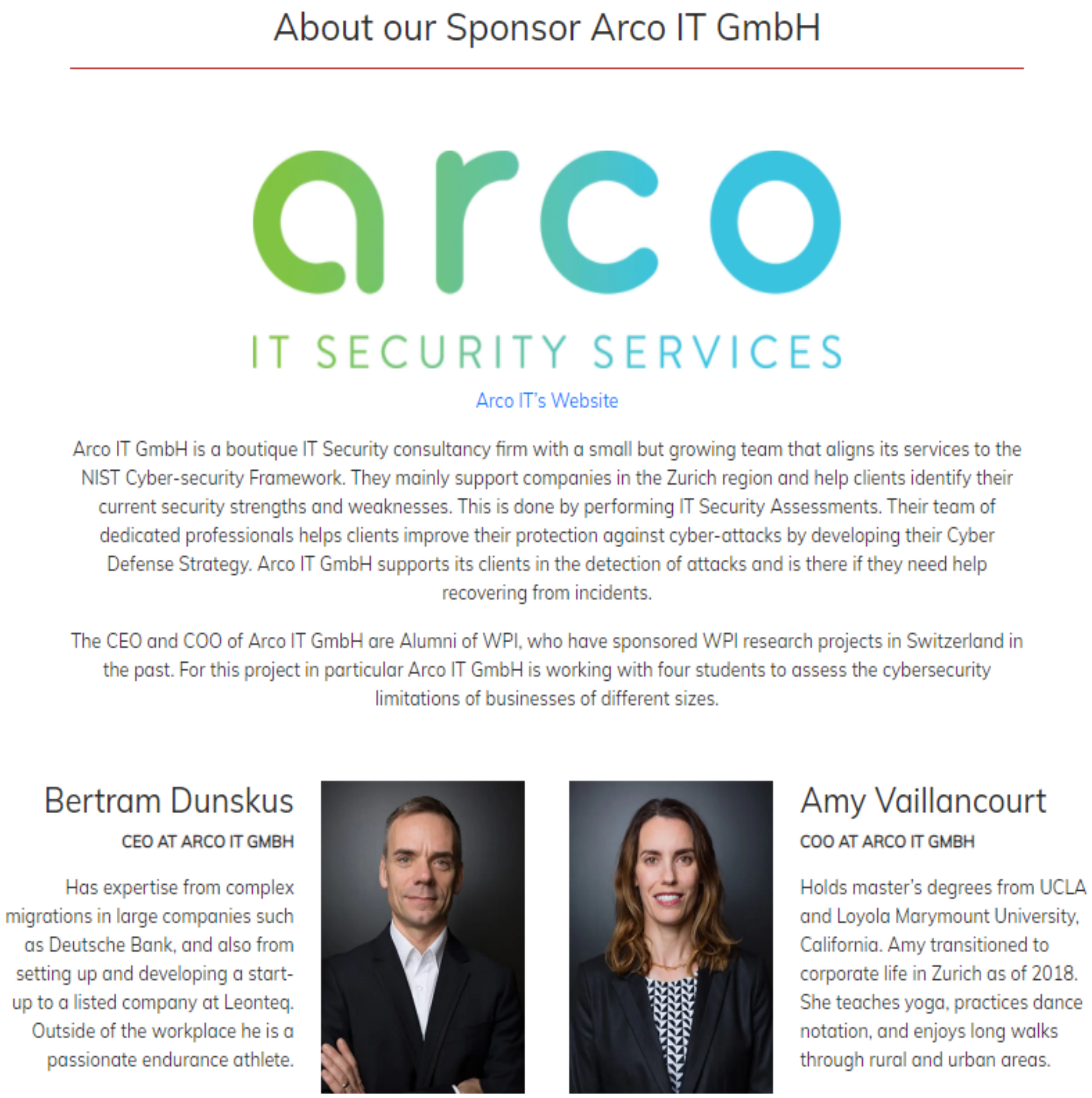
WPI STUDENT

Meghan is currently a junior at WPI pursuing her Master's degree in Mechanical Engineering.

Eric Schmid

WPI STUDENT

Eric is a junior at WPI pursuing his Bachelor's degree in Computer Science.



About our Sponsor Arco IT GmbH

arco

IT SECURITY SERVICES

Arco IT's Website

Arco IT GmbH is a boutique IT Security consultancy firm with a small but growing team that aligns its services to the NIST Cyber-security Framework. They mainly support companies in the Zurich region and help clients identify their current security strengths and weaknesses. This is done by performing IT Security Assessments. Their team of dedicated professionals helps clients improve their protection against cyber-attacks by developing their Cyber Defense Strategy. Arco IT GmbH supports its clients in the detection of attacks and is there if they need help recovering from incidents.

The CEO and COO of Arco IT GmbH are Alumni of WPI, who have sponsored WPI research projects in Switzerland in the past. For this project in particular Arco IT GmbH is working with four students to assess the cybersecurity limitations of businesses of different sizes.

Bertram Dunskus

CEO AT ARCO IT GMBH

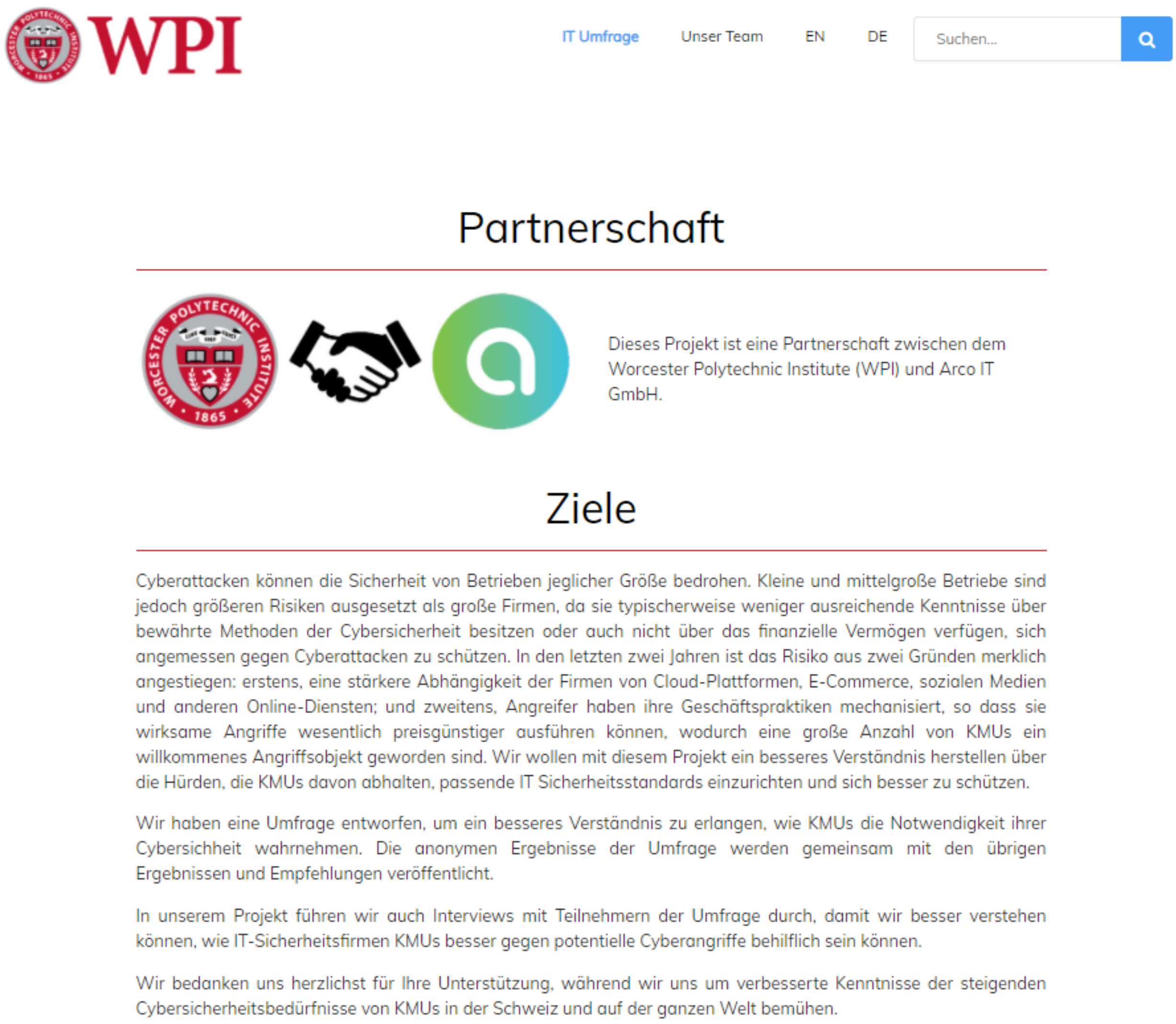
Has expertise from complex migrations in large companies such as Deutsche Bank, and also from setting up and developing a start-up to a listed company at Leonteq. Outside of the workplace he is a passionate endurance athlete.

Amy Vaillancourt

COO AT ARCO IT GMBH

Holds master's degrees from UCLA and Loyola Marymount University, California. Amy transitioned to corporate life in Zurich as of 2018. She teaches yoga, practices dance notation, and enjoys long walks through rural and urban areas.

German Landing Page



Partnerschaft

Dieses Projekt ist eine Partnerschaft zwischen dem Worcester Polytechnic Institute (WPI) und Arco IT GmbH.

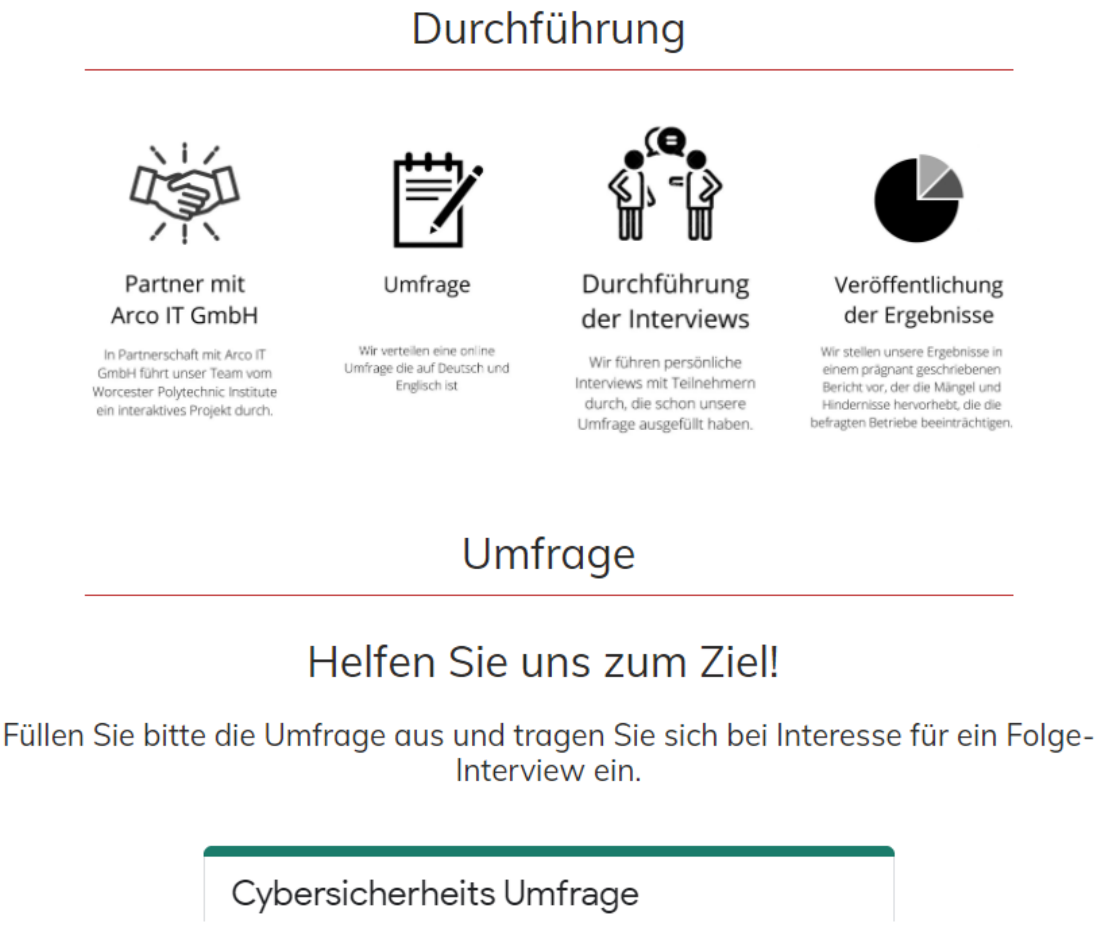
Ziele

Cyberattacken können die Sicherheit von Betrieben jeglicher Größe bedrohen. Kleine und mittelgroße Betriebe sind jedoch größeren Risiken ausgesetzt als große Firmen, da sie typischerweise weniger ausreichende Kenntnisse über bewährte Methoden der Cybersicherheit besitzen oder auch nicht über das finanzielle Vermögen verfügen, sich angemessen gegen Cyberattacken zu schützen. In den letzten zwei Jahren ist das Risiko aus zwei Gründen merklich angestiegen: erstens, eine stärkere Abhängigkeit der Firmen von Cloud-Plattformen, E-Commerce, sozialen Medien und anderen Online-Diensten; und zweitens, Angreifer haben ihre Geschäftspraktiken mechanisiert, so dass sie wirksame Angriffe wesentlich preisgünstiger ausführen können, wodurch eine große Anzahl von KMUs ein willkommenes Angriffsobjekt geworden sind. Wir wollen mit diesem Projekt ein besseres Verständnis herstellen über die Hürden, die KMUs davon abhalten, passende IT Sicherheitsstandards einzurichten und sich besser zu schützen.

Wir haben eine Umfrage entworfen, um ein besseres Verständnis zu erlangen, wie KMUs die Notwendigkeit ihrer Cybersichheit wahrnehmen. Die anonymen Ergebnisse der Umfrage werden gemeinsam mit den übrigen Ergebnissen und Empfehlungen veröffentlicht.

In unserem Projekt führen wir auch Interviews mit Teilnehmern der Umfrage durch, damit wir besser verstehen können, wie IT-Sicherheitsfirmen KMUs besser gegen potentielle Cyberangriffe behilflich sein können.

Wir bedanken uns herzlichst für Ihre Unterstützung, während wir uns um verbesserte Kenntnisse der steigenden Cybersicherheitsbedürfnisse von KMUs in der Schweiz und auf der ganzen Welt bemühen.



Durchführung

Partner mit Arco IT GmbH

In Partnerschaft mit Arco IT GmbH führt unser Team vom Worcester Polytechnic Institute ein interaktives Projekt durch.

Umfrage

Wir verteilen eine online Umfrage die auf Deutsch und Englisch ist

Durchführung der Interviews

Wir führen persönliche Interviews mit Teilnehmern durch, die schon unsere Umfrage ausgefüllt haben.

Veröffentlichung der Ergebnisse

Wir stellen unsere Ergebnisse in einem prägnant geschriebenen Bericht vor, der die Mängel und Hindernisse hervorhebt, die die befragten Betriebe beeinträchtigen.

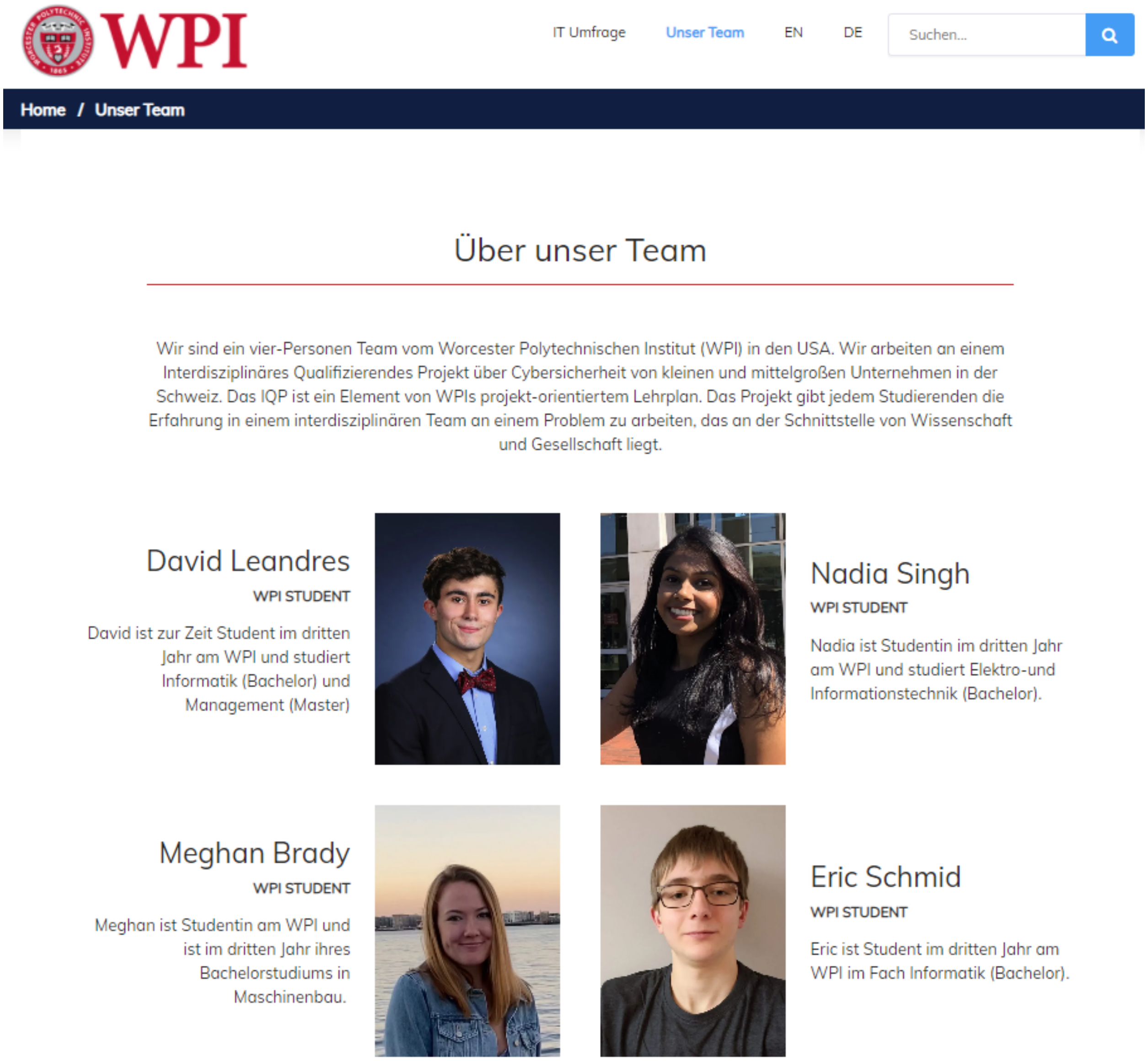
Umfrage

Helfen Sie uns zum Ziel!

Füllen Sie bitte die Umfrage aus und tragen Sie sich bei Interesse für ein Folge-Interview ein.

Cybersicherheits Umfrage

German Our Team Page



Über unser Team

Wir sind ein vier-Personen Team vom Worcester Polytechnischen Institut (WPI) in den USA. Wir arbeiten an einem Interdisziplinäres Qualifizierendes Projekt über Cybersicherheit von kleinen und mittelgroßen Unternehmen in der Schweiz. Das IQP ist ein Element von WPIs projekt-orientiertem Lehrplan. Das Projekt gibt jedem Studierenden die Erfahrung in einem interdisziplinären Team an einem Problem zu arbeiten, das an der Schnittstelle von Wissenschaft und Gesellschaft liegt.

David Leandres

WPI STUDENT

David ist zur Zeit Student im dritten Jahr am WPI und studiert Informatik (Bachelor) und Management (Master)

Nadia Singh

WPI STUDENT

Nadia ist Studentin im dritten Jahr am WPI und studiert Elektro-und Informationstechnik (Bachelor).

Meghan Brady

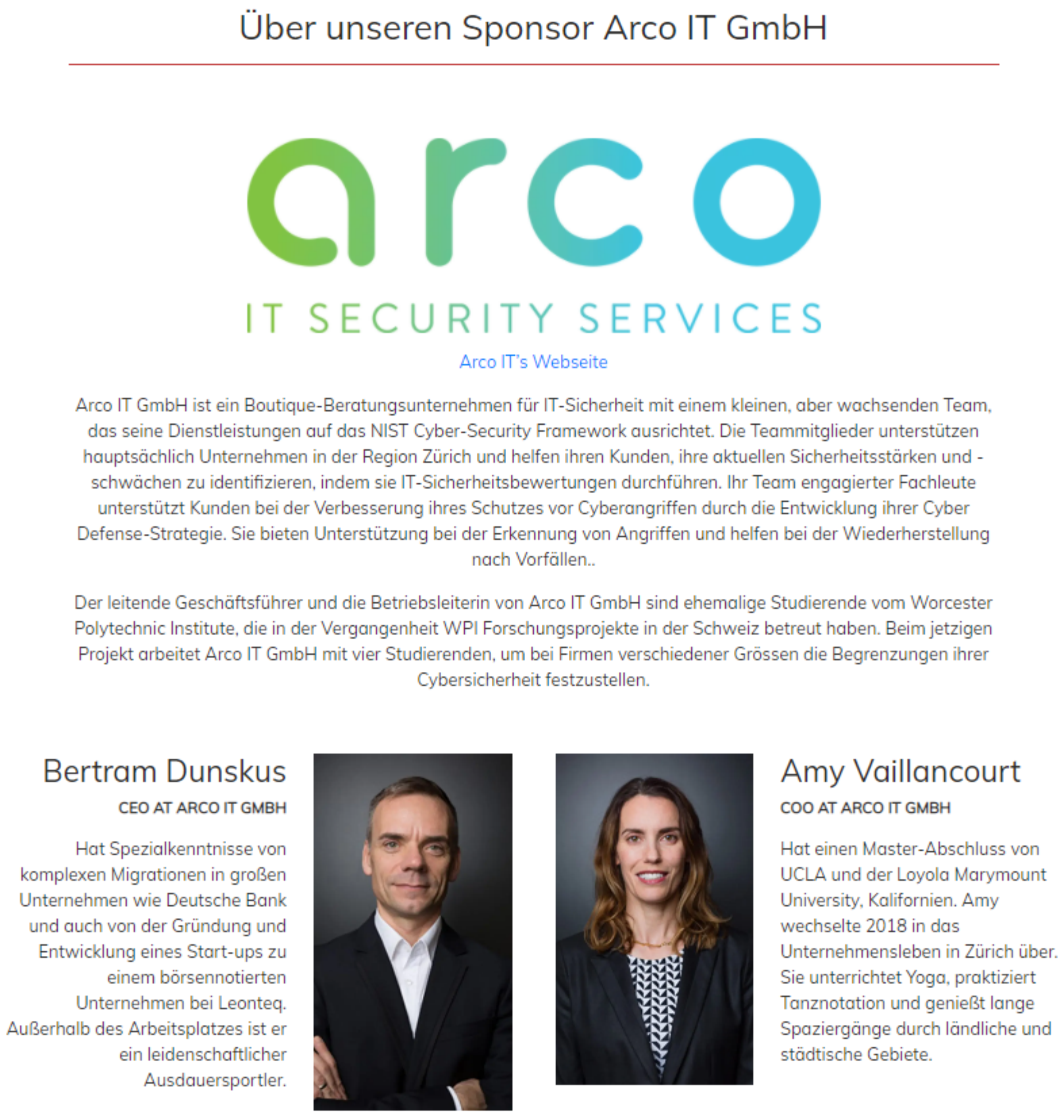
WPI STUDENT

Meghan ist Studentin am WPI und ist im dritten Jahr ihres Bachelorstudiums in Maschinenbau.

Eric Schmid

WPI STUDENT

Eric ist Student im dritten Jahr am WPI im Fach Informatik (Bachelor).



Über unseren Sponsor Arco IT GmbH

Arco IT's Webseite

Arco IT GmbH ist ein Boutique-Beratungsunternehmen für IT-Sicherheit mit einem kleinen, aber wachsenden Team, das seine Dienstleistungen auf das NIST Cyber-Security Framework ausrichtet. Die Teammitglieder unterstützen hauptsächlich Unternehmen in der Region Zürich und helfen ihren Kunden, ihre aktuellen Sicherheitsstärken und -schwächen zu identifizieren, indem sie IT-Sicherheitsbewertungen durchführen. Ihr Team engagierter Fachleute unterstützt Kunden bei der Verbesserung ihres Schutzes vor Cyberangriffen durch die Entwicklung ihrer Cyber Defense-Strategie. Sie bieten Unterstützung bei der Erkennung von Angriffen und helfen bei der Wiederherstellung nach Vorfällen..

Der leitende Geschäftsführer und die Betriebsleiterin von Arco IT GmbH sind ehemalige Studierende vom Worcester Polytechnic Institute, die in der Vergangenheit WPI Forschungsprojekte in der Schweiz betreut haben. Beim jetzigen Projekt arbeitet Arco IT GmbH mit vier Studierenden, um bei Firmen verschiedener Grössen die Begrenzungen ihrer Cybersicherheit festzustellen.

Bertram Dunskus

CEO AT ARCO IT GMBH

Hat Spezialkenntnisse von komplexen Migrationen in großen Unternehmen wie Deutsche Bank und auch von der Gründung und Entwicklung eines Start-ups zu einem börsennotierten Unternehmen bei Leonteq. Außerhalb des Arbeitsplatzes ist er ein leidenschaftlicher Ausdauersportler.

Amy Vaillancourt

COO AT ARCO IT GMBH

Hat einen Master-Abschluss von UCLA und der Loyola Marymount University, Kalifornien. Amy wechselte 2018 in das Unternehmensleben in Zürich über. Sie unterrichtet Yoga, praktiziert Tanznotation und genießt lange Spaziergänge durch ländliche und städtische Gebiete.