Academic Paper

Austin Cupp

Old Dominion University School of Cybersecurity

WCS 494: Entrepreneurship in Professional Studies, Cybersecurity and World Languages and Cultures

Professor Porcher

October 26th, 2023

Abstract

The purpose of this paper is to examine and explain a problem regarding what cybersecurity threats, vulnerabilities, and attacks can affect small businesses and the damages they can cause. Further in the paper is our proposed innovation, known as EzDetection, that will be a solution to solving the aforementioned problem in an effective and affordable manner for small businesses, and how EzDetection can be used as a training tool for the business owners and staff. Included in the study is courses related to our innovation outside of cybersecurity, how to determine if our innovation is effective, how our group intends to turn the innovation into reality, and the next steps regarding the innovation and myself.

Problem and innovation overview.

As technology continues to become a major influence in today's society, more organizations and businesses are beginning to incorporate technology or add on to present technology in their enterprises. While having more technology present is a good thing, the problem is that as small businesses begin to incorporate systems, networks, and applications into their enterprises, critical cybersecurity vulnerabilities that can lead to threats may arise, which if not addressed, can lead to a cyberattack affecting the business. Vulnerabilities that can affect small businesses include weak or broken access controls, misconfigurations, weak passwords, and missing encryptions of confidential data (Alshayeb et al., 2020). Threats that can hinder a small business include phishing, ransomware, and malware (Alshayeb et al., 2020). Attacks that small businesses can fall victim to include SQL injection attacks and Denial of Service (DoS) attacks (Alshayeb et al., 2020). These are all major cybersecurity incidents that can handcuff a small business both socially and financially if they are not properly addressed. Cyberattacks are difficult to detect without a cybersecurity tool or team, and unfortunately most small businesses are unable to afford cybersecurity resources, making our innovation the perfect solution for small businesses.

The innovation my group and I are proposing is a form of software named EzDetection that will help remedy any vulnerabilities and threats small businesses can face and help combat against cyberattacks. EzDetection will run a scan and be able to generate a report that will let users know what vulnerabilities and threats are present anywhere in a system, network, or application, and what cyber-attacks the business could fall victim to due to the present vulnerabilities and threats. EzDetection will have an option for the business to scan the system, network, or application anytime they want at the click of a button, or they can schedule the scan to automatically occur daily or weekly. The report will go into detail as to what specifically is causing the vulnerability or vulnerabilities, for example if the system has a weak password. The report will then list what is required to correct the vulnerability, what threats are present due to the vulnerabilities, and what attacks could be successfully launched against the business due to the vulnerabilities. The report will also be able to indicate whether human error was involved with causing the vulnerability to arise. Some vulnerabilities, threats, and attacks may have the ability to be solved in a quick and timely manner, while others may take a long time to remedy. The report will indicate the expected time it will take to remedy the vulnerability or threat, and it will be able to determine what the specific threats are present.

The business that uses the EzDetection software can also use the report as a training tool to help educate themselves and their employees as to why it's important they practice proper cybersecurity etiquette and maintain systems, networks, and applications. Since the report lists out each vulnerability, goes into detail about the vulnerability, and indicates if human error was a factor, the user of the software can teach themselves or help the employee learn how to prevent the vulnerability from arising again, what threats are associated with the vulnerability, and how the business is at risk of an attack because of the vulnerability. The overall goal of EzDetection is to be an affordable, strong cybersecurity defense system to help small businesses bolster or start up their cybersecurity infrastructure by keeping them constantly informed about vulnerabilities, threats, and attacks before they arise, when they occur, and how to resolve them after the fact. With small businesses being very susceptible to cybersecurity incidents, EzDetection is a must have for small businesses.

Literature review

As previously mentioned, with technology becoming a major influence in society today, more organizations, including small businesses, are beginning to implement or add onto present technology in their enterprises. While there is a litany of benefits that are tied to implementing technology, as well as adding onto present technology that is in the business, the problem is that as small businesses begin to incorporate systems, networks, and applications into their enterprises, critical cybersecurity vulnerabilities that can lead to threats may arise, which if not addressed, can lead to a cyberattack affecting the business (Alshayeb et al., 2020). Small businesses for example, do not always have a strong cyber defense system due to the cost that the business would incur from the defense installation process (Berry & Berry, 2018). Hence, a vulnerability, threat, or an attack may be undetected for months if there is no method of a cyber defense in place (De Haro et al., 2017). A cybersecurity vulnerability is any flaw that is in a business's systems, networks, or applications. If a vulnerability is present, a business's important confidential data and assets will be exposed, leading to cybersecurity threats forming. If a threat is not addressed, a cyber-attack has a much larger chance of affecting a business, which can lead to financial losses, and social impacts such as employee's losing their job.

One paper outlines the main forms of cybersecurity vulnerabilities that can affect businesses, which include weak or broken access controls, misconfigurations, weak passwords, and the missing encryption of confidential data (Wang et al., 2021). The broken access control vulnerability is a type of cybersecurity flaw present in a system, network, or application that allows an unauthorized user to easily bypass any standard security procedures, which would grant the unauthorized user the ability to access any restricted resources, such as those that contain an employee's personal information and confidential business information (Clancy, 2022). Most computer systems and applications have an authentication system present, such as a push notification or a code that would be able to authenticate a user who is trying to gain access to it, however if the broken access control vulnerability is present, the authentication system would in essence be incapacitated, and the malicious actor could then bypass it (Clancy, 2022). The malicious actor then would be able to access the sensitive data they are looking for or make changes that could harm the system, application, and the business itself.

Studies show that small businesses are very susceptible to having misconfigurations, as the configuration process for systems, networks, and applications can be complicated (Shinde & Ardhapurkar, 2016). Misconfigurations are a form of cybersecurity vulnerability that arises when a system, system component, application, cloud storage function, or security tool has an improper or incorrect configuration or no configuration (Shinde & Ardhapurkar, 2016). Misconfigurations enable systems, networks, and applications to become more susceptible to attacks and breaches, as a misconfiguration will cause security protocols to not function properly, or to not function at all (Shinde & Ardhapurkar, 2016). Because many systems, networks, and applications need to be manually configured, this allows for misconfigurations to occur if they are not properly configured or if they are not configured at all (Shinde & Ardhapurkar, 2016).

Research has shown that weak passwords are another common cybersecurity vulnerability, especially in small businesses that can affect every kind of system, software, or application (Harris & Teymourlouei, 2020). A weak password is a type of authentication password which is set by the user that is either very commonly used, an easy to guess word or string of numbers, is short in length, or is a default password set by the product vendor that is unchanged. Weak passwords are considered the weakest link when it comes to any form of authentication method because a malicious actor can easily exploit a weak password by using a brute force attack, dictionary attack, rainbow table attack, social engineering, spidering or by even guessing the password (Azadi et al., 2018). Malicious actors also have help when it comes to being able to exploit small businesses and their weak password vulnerability. Various tools that cybercriminals can use to help aid them in executing exploitations or attack methods against weak password vulnerabilities include John the ripper, Cain and Abel, and Hashcat (Azadi et al., 2018).

Another cybersecurity vulnerability that can arise is the missing encryption of confidential data, which may lead to security breaches and the loss of data in small businesses. When confidential data is not properly encrypted, or is not encrypted at all, it is left vulnerable to a malicious actor having unauthorized access to the data or allows the malicious actor to intercept the data (Iny, 2022). Encryption is a method of scrambling, converting, or encoding data and information in a manner that only those who are communicating or those who are deemed an authorized party can access the information and data to ensure its security (Nagaraj et al., 2015). Data and information are encrypted to ensure that it maintains its confidentiality and integrity and has not been tampered with or viewed by a third party (De Capitani di Vimercati, 2023). If a malicious actor is able to intercept and view the businesses confidential data, they can use the data to commit malicious acts such as identity theft and financial fraud.

Cybersecurity threats are a cyber event that is carried out by a malicious actor towards a business with the intent to exploit any vulnerabilities and cause harm to a system, network application, or individual within the business (Ghelani, 2022). A study by the Acronis software organization found that phishing scams are the most common cybersecurity threat that is levied towards businesses, with email-phishing based attacks increasing by over 400% during the 2023 calendar year (Law, 2023). Phishing occurs when an attacker sends an enticing email, text message, or attempts to call the victim in order to coerce the victim into divulging personal or business information, clicking on a malicious link, or downloading a form of malicious software or application (Wang et al., 2021). Once the victim has revealed confidential information or has had their systems compromised, the attacker then has the ability to gain unauthorized access into the network, compromise unencrypted confidential data, commit intellectual property theft, or disable systems (Aggarwal, 2019).

Research shows that malware is a cybersecurity threat that harms small businesses across the globe (Hall, 2021). In Australia, malware is one of the most common cybersecurity threats that affects small businesses (Hall, 2021). Malware is a form of a malicious software, program, or code that is installed on the victim's computer without their consent and is harmful to networks, systems, and applications that are on the system (Agarwal et al., 2020). Malware can be transmitted to a computer by a malicious actor via an email, removable media device such as a USB drive, and by the victim visiting a website that is infected with malware (Holmes, 2023). Forms of malware include viruses, spyware, and worms, with each having the ability to monitor the victim's computer activity, modify the affected networks, alter, or take control of internal computing functions and steal, encrypt, and delete confidential data (Lutkevich, 2022).

Ransomware is another form of malicious software that heavily impacts small businesses. One journal points out that there are two main forms of ransomware that businesses fall victim to, which are classified as crypto-ransomware and locker-ransomware (Alsayat et al., 2021). Crypto ransomware is a form of malicious software that encrypts a file and data to hold it hostage (Alsayat et al., 2021). If the victim attempts to access the file or data, a message is displayed with the malicious actor demanding payment in exchange for the victim to have access to the encryption key, which is used to decrypt the file or data (Alsayat et al., 2021). Locker ransomware is a form of ransomware that disables a system or an entire network, but like crypto ransomware, requires a payment to restore functionality (North & Richardson, 2017). If a business decides to not pay the ransom or is unable to afford the ransom, the disabled technology or encrypted data may be locked permanently, forcing the business to purchase new resources, and recreate the file or data that was stolen (Alsayat et al., 2021).

Cyber-attacks are a malicious and intentional effort by a bad actor to disrupt or disable a computer or network in order to harm organizations financially, disrupt production and task completion, and use collected information and data to commit a different cybercrime (Kim et al., 2014). Malicious actors aim to use cyber-attacks to take advantage of any vulnerabilities that are present within any networks that are used by a business. A Denial-of-service (DoS) attack is an example of a cyber-attack that affects small businesses. A DoS attack is a cyberattack that is launched by a malicious actor who aims to disrupt or render a business's technological resources inaccessible to its intended user (Alshayeb et al., 2020). DoS attacks affect a business by flooding the victim with network traffic, which triggers a crash that weakens or eliminates a network's capacity to perform its expected function (Alshayeb et al., 2020).

SQL injection attacks are a cyberattack where the malicious actor injects an SQL input string through the application's data-plane to change or manipulate the SQL statement to their advantage (Alshayeb et al., 2020). SQL injection attacks harm the application's database in several ways by allowing the malicious actor to gain unauthorized access to the database, manipulate data, and disclose confidential data (Alshayeb et al., 2020). Data that is present in a database affected by an SQL injection attack also loses its confidentiality, integrity, and functionality (Alshayeb et al., 2020). Furthermore, if the malicious actor can enter system-level administration commands while injecting the SQL input string, they can enable the authorized users to no longer have access to the data and the entire database (Alshayeb et al., 2020).

Almost anything negative in the cybersecurity ecosystem, such as vulnerabilities, threats, and attacks, can easily affect small businesses due to their lack of training regarding cybersecurity and the small businesses' thinking that a cybersecurity incident would only affect a large business (Raineri & Resig, 2020). Small business employees are also less likely to be trained in cybersecurity compared to those in a large business, and thus combined with little to no cybersecurity infrastructure, means small businesses are almost always not ready for a cybersecurity incident (Raineri & Resig, 2020). A study conducted by Verizon Communications in 2019 found that 43% of small businesses experience a cyberattack, and a further 60% of those businesses closed within 6 months of the attack (Raineri & Resig, 2020). Businesses that do survive a cybersecurity event, however, often suffer from negative effects, such as reputation loss, employee, and financial losses, fines, legal and credit monitoring fees, and fees to diagnose and determine what cyber incident affected the business (Raineri & Resig, 2020). Recovery costs are also significant for small businesses, with small business owners reporting that the average cost was $20,000 per cyber incident, with some being as high as $44,000, and then a further $8,000 to take measures against cybersecurity incidents (Raineri & Resig, 2020).

For small businesses, many cybersecurity tools can be difficult to navigate, are expensive, and sometimes are inefficient, (Berry & Berry, 2018). Therefore, most small businesses avoid using any cybersecurity tools, leaving them at a great risk of having their systems and networks compromised (Berry & Berry, 2018). However, unlike most cybersecurity tools, EzDetection is an efficient, affordable, easy to use, and easy to navigate solution for small businesses who struggle to maintain or do not possess a cybersecurity infrastructure.

EzDetection is a software that scans systems, networks, and applications to detect if any vulnerabilities are present, what threats are associated with the vulnerabilities, and what attacks the business is at risk for due to the vulnerabilities. EzDetection has a monthly plan that is $13, and a yearly plan that is $150, but also has a one-month free trial period that is included for small businesses upon signing up for an EzDetection subscription plan. Users will be able to run an EzDetection scan at the click of a button, however, users also have the option to set a schedule for the scan to run automatically either every day, or once a week. If no vulnerabilities are present, EzDetection will generate a report with a printed message that reads “no vulnerabilities present”. If a vulnerability or multiple vulnerabilities are present, EzDetection will still generate a report, but will print a message that says, “vulnerabilities detected, please read below”, and the report will have a list of what vulnerabilities are present, what threats can affect the business due to the vulnerabilities being present, and what attacks the business is at risk for. The report will also organize the vulnerabilities by level of risk. If a vulnerability poses a major threat to the business, then the risk level will be marked as high, however, if the vulnerability is essentially a non-threat, then the risk level will be marked as low, although there will be a notice about the vulnerability on any further generated reports. EzDetection will also be able to determine if an attack is currently taking place or has taken place. If the user runs an EzDetection scan while an attack is taking place or after an attack has affected the business, the report will print out what attack is currently being launched against the business or has affected the business.

EzDetection also informs the business on how to remedy and eliminate any vulnerabilities that are present, and how to take the necessary steps to remedy a cyber-attack. For example, studies show that most small businesses do not use strong passwords to protect their systems, networks, and applications, which allows the weak password vulnerability to arise

(Berry & Berry, 2018). However, if a business owner runs a scan through EzDetection and a network has a weak password, the report will print out a list noting that the vulnerability is due to a weak password on the network, and the solution to the vulnerability is to change the password to a more complex password. This feature is key for business owners who are not tech-savvy, as EzDetection can help steer the user and employees in the right direction into protecting their cyber ecosystem.

Furthermore, the same study shows that most small businesses are unable to afford cybersecurity knowledge and the training to secure their systems (Berry & Berry, 2018). Another way EzDetection is very helpful to small businesses is the business can use the report as a training tool to help educate themselves and their employees as to why it's important they practice proper cybersecurity etiquette while maintaining systems, networks, and applications. Since the report lists out each vulnerability and goes into detail about the vulnerability as well as the associated threats and potential attack risks, while indicating if human error was a factor, the user of the software can teach themselves or help the employee learn how to prevent the vulnerability from arising again, what threats are associated with the vulnerability, and how the business is at risk of an attack because of the vulnerability. This feature, as well as the other previously discussed features, allows EzDetection to be an "all in one" cybersecurity tool that is excellent for small businesses.

Courses OUTSIDE of Cybersecurity That Relate to the Innovation.

While the bulk of the courses taken in the Cybersecurity major are cybersecurity courses, there are also courses taken outside of cybersecurity that help students become successful cybersecurity professionals, and in some cases also successful entrepreneurs. Courses such as these are considered general education courses but contributed much more than even I realized to my cybersecurity and entrepreneurial efforts. Personally, both an Economics and college English composition course played a key role in helping me become a well-rounded cybersecurity professional, and helped me become a better entrepreneur, which played a key role in the research, development, and implementation of EzDetection and our business strategy.

An Economics course, such as ECON 200S is a course that is key for helping students understand the impact a cybersecurity vulnerability, threat, and attack can have on a small business, and how important it is for a business to have countermeasures against them. Businesses that have a strong cybersecurity infrastructure help save themselves from major financial losses including legal fees, cost to determine vulnerabilities, threats, and attacks, and company information loss. Economics also stressed how important it is that a business has a business plan. An effective business plan can help the business focus on expenses, have clear goals, understand their target market, and maximize profits. Each choice a business makes can determine their expenses and profits, and understanding economics and having an effective business plan can help a business make the right choices. Economics was very much involved with the thought process behind EzDetection. Understanding economics also allowed us to create a budget table to help our group and determine our expenses for our business, and how much we needed to make to earn a net profit.

A course that most people would not necessarily expect to be related to Cybersecurity and our EzDetection software but plays a major role into developing an understanding of the software and Cybersecurity is a college writing course, such as ENGL 110C. This course is effective in helping students understand how to communicate their ideas in writing and helps the student develop their entrepreneurial skills. Research is a requirement for this course, which teaches the student how important research is, and for us was very beneficial when it was time to research material related to market trends, cybersecurity trends and incidents, and statistics relating to small businesses. Without knowing how to conduct proper research, an entrepreneur has a strong likelihood to fail from the start. An entrepreneur who does not conduct proper research is unlikely to understand the problem their product will solve, their target market, and market trends. A lot of the research I was able to conduct enabled me to understand that EzDetection with the right marketing can be a very viable cybersecurity tool for small businesses. Research showed that almost half of small businesses can experience a cyberattack, and more than half of small businesses that experience a cyberattack end up closing their doors. Through research, these studies showed that EzDetection can be help small businesses prevent a cyberattack from taking place. The writing aspect will also be very important when pitching and marketing EzDetection and when communicating with clients. An effective marketing campaign is essential for drawing in new customers who need some cybersecurity infrastructure "assistance" for their small business. Once small businesses understand how EzDetection can help them, we need to communicate effectively through clear and concise emails to help retain them as a user of our product.

How to determine whether your innovation is effective.

Research has shown that EzDetection is very much suited for and needed in our target market, which suggests there are a few ways to analyze and measure if our innovation is successful or not. One of the main ways to determine if EzDetection is effective is if the business has made a net profit each year. If our sales bring in more money than all our combined expenses on the innovation, and we are continuing to make more of a profit each year, then this will help us realize our innovation is successful in one way. Another way to measure the effectiveness of EzDetection is by sending a follow up email to clients after their one-month free trial period has ended. In the email, the user would be asked to provide feedback about EzDetection, inform us if they notice an improvement in their cybersecurity infrastructure, and to include any suggestions that could improve EzDetection. These emails would allow us to hear from the businesses on how we can improve EzDetection and add features based on their needs. After a six-month period, we would send out another follow up email to businesses asking if there are any new features and improvements we can provide, and to help them determine if any vulnerabilities or threats are present in their systems. If the user feedback is positive and businesses report seeing fewer or no vulnerabilities in their systems and networks, as well as the elimination of threats, then we can determine that EzDetection has been an efficient and overall effective product for them.

A reporting feature is another way for us to analyze if EzDetection is effective for our clients. Included in EzDetection will be a button that the user can click on and report any issues they may encounter. If clients are consistently having to use the reporting feature due to bugs, crashes, or other issues, then we can understand that EzDetection is not operating in an efficient manner, and we need to work on an update or patch to release to the clients, so that it does operate properly. Meanwhile, if clients are not needing to use the reporting feature, then we can assume EzDetection is operating in an efficient manner.

What is needed to turn the innovation into reality.

While there are a few ways to make sure EzDetection is effective and successful, there is a step-by-step basis needed to turn EzDetection from a thought into a reality. Almost all successful businesses have a business plan, so the first step to turn EzDetection into reality would be to craft a well-rounded business plan to determine the necessary resources and expenses for our business. Included in the plan would be our goals, target market for EzDetection, the market plan, staff roles, and financial projections. The plan would also feature a budget, so we know what expenses we expect to incur regarding our business location, marketing tools, utilities, staff pay, and the expenses needed for developing EzDetection.

Second, EzDetection will need multiple teams of software developers to produce and help maintain the software so that EzDetection and its features operate in an efficient manner. The software developers will also be tasked with adding or changing any features and publishing updates for EzDetection. Having two seperate cybersecurity teams will also be a necessity for our business. One cybersecurity team will be needed to ensure all networks and systems that contain our businesses information and data is protected, and this team will also be tasked with making sure our users' reports that are present within our business are protected as well. The other cybersecurity team will help guide the software developers to ensure the proper cybersecurity features, such as the vulnerability and threat list, are included in the reports generated by EzDetection.

A marketing team will be tasked with making sure EzDetection is promoted on various websites and social media, such as Twitter, Facebook, and Instagram, and through physical means such as newspapers and billboards. They will also be tasked with ensuring our product reaches a wide audience, specifically those who own a small business. A human resource team will be needed to handle all employee related concerns, but our business will also need a customer service team to help answer any questions or concerns our users may have. This will ensure that our business keeps user satisfaction at the top of our priority list. Also, a quality control team will be needed to test EzDetection before it is released, after new or additional features have been implemented, and before updates and patches are released to ensure our users do not encounter any bugs or issues when using EzDetection,

Externally, for us to help turn our innovation into reality, we will need to establish trust between us and the small businesses we are targeting in our marketing campaigns. We want the small businesses who consider using EzDetection to understand how and why it is beneficial for them, and how EzDetection can help bolster their cybersecurity infrastructure. Once the small businesses begin to show interest in EzDetection, we will need to help retain them by establishing a connection with them. Moreover, we can do this by offering a one-month free trial period to first time users, referral discounts, and send follow up emails requesting feedback from the businesses. Having connections will also be a key factor to help us turn our innovation into a reality. I personally know two family friends who own small businesses, both of which are restaurants, and we can have them become our first users of the EzDetection software. This will also enable us to have our product marketed through “word of mouth”, which is a form of marketing where individuals organically spread the word about a product and business through conversations.

Finally, to help turn our innovation into reality, we will need to have a strong work ethic and understand that there will be challenges each step of the way. It will be a difficult process to find the necessary staff to fill out the roles in our business, and there will be challenges along the way regarding EzDetection itself, but with a strong work ethic we can overcome the challenges and provide small businesses an effective and innovative product that will remain viable for years to come.

Next Steps

As the cybersecurity landscape continues to change, businesses will need to adapt to keep their systems and networks safe while combating against malicious actors. Therefore, EzDetection is the perfect tool to help business startup and maintain a secure cyber environment. The next steps for EzDetection are to fine-tune and add features that will help ensure it remains a viable and effective product for small businesses. Automated patching is one of the first features we would like to implement in EzDetection, which would allow the software to stay up to date and include any new features we have released. The option to have a 24/7 constant scan is another feature that we would like to implement in EzDetection. Users who have a 24/7 constant scan would allow the user to have their systems, network, and any applications constantly scanned to check for any vulnerabilities and threats. A push notification that alerts the user when a scan is taking place, when a scan is completed, and if the scan has detected any abnormalities in the system and network is another key feature we would like to implement in EzDetection. Within the push notification would be a description indicating if the system is “all clear” or if there is a vulnerability and a threat present.

Personally, for me, this innovation and course has helped me fulfill the capstone section of my degree and has taught me what is necessary for a business and innovation to be successful and effective. I learned how important a business plan is for a business to achieve success, and how it is necessary businesses determine the problem they are going to solve when considering what their innovation is going to be. Completing the EzDetection innovation with my group has also helped prepare me to be a great candidate, and a great leader in the cybersecurity job force. We were able to create a software that would benefit small businesses both financially and socially and is something that would remain viable as technology continues to become more of an influence on small businesses. The main thing I would have done differently is communicate with my group members more at the beginning stages of our course, as the lack of communication affected our innovation at the beginning stages.

References:

Alsayat, A., Jhanjhi, N., Humayun, M., & Ponnusamy, V. (2021). Internet of things and Ransomware: Evolution, mitigation, and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Alshayeb, M., Humayun, M., Niazi, M., Jhanjhi, N., & Mahmood, S. (2020, January 6). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Agarwal, A. T., Ngo, F., Govindu, R., & MacDonald, C. (2020, June 6). Malicious software threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793–813. https://doi.org/10.1007/978-3-319-78440-3_35

Aggarwal, P., Gonzalez, C., Rajivan, P., & Singh, K. (2019, November 20). Training to detect phishing emails: Effects of the frequency of experienced phishing emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 453–457. https://doi.org/10.1177/1071181319631355

Anu, V., Sultana, K. Z., & Samanthula, B. K. (2020). A human error-based approach to understanding programmer-induced software vulnerabilities. *2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 49–54. https://doi.org/10.1109/issrew51248.2020.00036

Ardhapurkar, S. B., & Shinde, P. S. (2016). Cyber security analysis using Vulnerability Assessment and penetration testing. *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, 1–5. https://doi.org/10.1109/startup.2016.7583912

Azadi, M., Zare, H., & Zare, M. J., (2018). Cybersecurity Vulnerabilities Assessment (A systematic review approach). *Information Technology - New Generations. Advances in Intelligent Systems and Computing*, *738*, 61–68. https://doi.org/10.1007/978-3-319-77028-4_10

Berry, C. T., & Berry, R. L. (2018). An initial assessment of Small Business Risk Management Approaches for Cyber Security Threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1–10. https://doi.org/10.1504/ijbcrm.2018.090580

Clancy, R. (2022, October 12). *What is broken access control vulnerability, and how to prevent it?* Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/broken-access-control-vulnerability/

De Capitani di Vimercati, S., Foresti, S., & Samarati, P. (2023). Protecting data and queries in cloud-based scenarios. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-01862-6

De Haro, G., Esteves, J., & Ramalho, E. (2017, March 6). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*.

Ghelani, D. (2022). Cyber security, cyber threats, implications, and future perspectives: A Review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19. https://doi.org/10.22541/au.166385207.73483369/v1

Hall, J., Rao, A., & Tam, T. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian Small Businesses. *Computers & Security*, *109*. https://doi.org/10.1016/j.cose.2021.102385

Harris, V. & Teymourlouei, H. (2020). Effective methods to monitor IT infrastructure security for small business. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 7–12. https://doi.org/10.1109/csci49370.2019.00009

Holmes, J. (2023, October 17). *Malware is a threat to businesses - here's what you need to know*. Stanfield IT. https://www.stanfieldit.com/malware/

Iny, N. (2022, May 16). *Polar Security (an IBM company) - sensitive data exposure: What is it and how to avoid it?* Polar security. https://www.polar.security/post/sensitive-data-exposure

Kim, Y., Kim, I., & Park, N. (2014). Analysis of cyber-attacks and Security Intelligence. *Lecture Notes in Electrical Engineering*, *274*, 489–494. https://doi.org/10.1007/978-3-642-40675-1_73

Law, M. (2023, September 1). *Top 10 cyber security threats*. Cyber Magazine. https://cybermagazine.com/top10/top-10-cyber-security-threats

Lutkevich, B. (2022, June 13). *What is malware? definition, types, prevention - techtarget*. Security. https://www.techtarget.com/searchsecurity/definition/malware

Nagaraj, S., Raju, G. S. V. P., & Srinadth, V. (2015). Data Encryption and authetication using public key approach. *Procedia Computer Science*, *48*, 126–132. https://doi.org/10.1016/j.procs.2015.04.161

North, M. M., & Richardson, R. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. Journal of Applied Business and Economics, 22(12), 13–23. https://doi.org/10.33423/jabe.v22i12.3876

Sun, L., Wang, Z., & Zhu, H. (2021, January 14). Social Engineering in cybersecurity: Effect Mechanisms, human vulnerabilities, and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/access.2021.3051633

Thakkar, M. (2022, January 9). *10 software development challenges every developer faces*. Synoptek. https://synoptek.com/insights/it-blogs/10-challenges-every-software-product-developer-faces/