Alexandra Ellis

Academic Paper

Security Werks: Cybersecurity Simplified

As our society leans heavily into technological dependence, the need for a robust cybersecurity program has evolved into a primary need for businesses and organizations of all sizes. Small businesses, specifically startups and those in the early stages of growth, are particularly vulnerable to cyber-attacks. Limited by financial constraints, these businesses often struggle to invest in cybersecurity, leaving them exposed to a range of cyber threats that could disrupt or even derail their operations. This challenge is made worse by a cybersecurity industry that tends to cater to the more substantial financial capabilities of larger organizations. This lack of protection has led to small businesses becoming known easy targets for cybercriminals.

According to the U.S. Small Business Administration (SBA), in 2020 there were over 700,000 attacks against small businesses, with damages totaling 2.8 billion dollars. Furthermore, a recent survey conducted by the SBA determined that “small business owners felt their business was vulnerable to a cyber-attack. Yet many businesses can’t afford professional IT solutions, have limited time to devote to cybersecurity, or don’t know where to begin.” (Madrid). The range of cyber threats is extensive, and small businesses frequently underestimate the risks they face. This leaves them vulnerable to cyber-attacks such as data breaches, phishing scams, and ransomware. These attacks can have serious financial consequences, rupture the trust between business and client, and in certain situations force a business to close.

Addressing these challenges requires a proactive approach that is both affordable and effective for small businesses. This approach should not only focus on implementing advanced cybersecurity measures but also on building a culture of cyber-awareness amongst a team who may not know the impact they have on their organizations cyber posture. This pressing need led to the creation of Security Werks, a company that provides cybersecurity solutions designed specifically to meet the needs of small business within three years of startup and/or with less than $125k annual revenue. Our mission emphasizes the power of awareness as the first line of defense and integrates affordable and scalable cybersecurity services aimed at our communities most vulnerable targets.

At the core of what we offer, Security Werks provides customized training to help business owners and their teams develop an acute awareness of cyber threats. These programs are designed to accommodate all levels of technical proficiency- anyone from a first-year employee to a seasoned cybersecurity veteran. We focus on creating an environment where continuous learning and adaptability are at the forefront, ensuring that our training remains relevant as cyber threats evolve. Furthermore, we perform vulnerability assessments, penetration tests, and risk evaluations scaled to match the size and complexity of the clients' network. These assessments, coupled with our incident response planning, allow for targeted improvements, and give clients the tools they need to respond quickly and confidently to vulnerabilities and threats. For those businesses looking to add a final layer of protection, Security Werks also specializes in continuous monitoring services, offering real-time threat detection and response. This service is especially useful for businesses without resources available for 24/7 network surveillance.

As we educate small businesses on the critical importance and urgency of cybersecurity, Security Werks is committed to establishing longstanding partnerships with our clients. With our support, small businesses gain more than just cybersecurity; they acquire an ally that will ensure their cyber defenses remain as robust and dynamic as the digital landscape they navigate.

Small businesses are becoming increasingly vulnerable to cyber threats. Despite their smaller size, cybercriminals consider these businesses to be easy targets due to their limited budgets and lack of specialized IT support. The aforementioned 2020 SBA study highlighting the combined $2.8 billion in damages to small businesses who fell victim to cyber-attacks underscores the need for cybersecurity solutions tailored to their unique constraints and capabilities. The rapid growth of cybersecurity threats facing small businesses can be attributed to various factors, including technical deficiencies and a lack of organizational, financial, and legal expertise. A 2022 study published by IEEE Access found that, " the three main challenges faced by small businesses identified were: (i) not having the in-house expertise to mitigate cyber risk; (ii) IT budget constraints; and (iii) a general lack of understanding of how to protect against cyber-attacks" (Chidukwani, et. al., 7). Given these challenges, it is evident that in order to safeguard small businesses against the increasingly sophisticated landscape of cyber threats there is an urgent need for accessible and effective cybersecurity solutions tailored to the limitations of small businesses. As technology and cyber threats continue to grow more advanced, many small business owners find themselves ill-equipped to keep pace, highlighting a pressing need for risk management strategies that cater specifically to the small business sector.

While the initial investment into cybersecurity is a significant financial impact on small businesses, it is a critical defense measure. Forgoing cybersecurity investment is a risky gamble, and those who opt out are increasingly finding themselves targets of cyberattacks, a costly consequence of underestimating online threats. In 2022, IBM Security's Data Breach Report reveals the average cyber-attack in the United States cost $4.35 million. This report also indicates that destructive attacks are even costlier, averaging $5.12 million, 16.3% higher than the overall data breach average. These attacks are something that small businesses often lack financial resources to mitigate. Additionally, the financial repercussions of these attacks go beyond monetary losses. Indirect costs such as potential legal action, harm to a brand's reputation, and a decline in customer trust are just as important. "Rectifying a data breach or cyber-attack could cost SMEs companies millions of dollars. When there is a data breach in SMEs companies' systems it is not just the financial loss that is a concern. A breach of extremely sensitive personal data could have disastrous consequences for a SMEs companies' reputation and people's privacy" (Wallang, et. al., 5). Fixing a cyber incident can cost small businesses millions of dollars, jeopardize their reputation, and threaten their customers privacy.

The resource and knowledge gap in cybersecurity is a major contributing factor to the growing cyber risks that small businesses are facing. A 2021 CNBC survey revealed a concerning level of overconfidence among U.S. small business owners. Despite the growing national cybersecurity threat, 56% are not concerned about being the victim of a hack in the next 12 months, and 24% express no concern at all. This is particularly troubling considering that, according to research conducted by Bob Duncan for the University of Aberdeen, "many signs indicate that SMEs underestimate cyber threats by not using efficient security measures"

(Duncan, et. al., 3). This overconfidence is contrasted with the fact that while 59% believe they can quickly resolve any cyberattack, only 28% have a response plan in place, and 42% have no plan at all.

Although it is concerning that small business owners believe a cyber-attack isn't a real possibility, most people simply don't know any better. A lack of internal IT specialists and a general unawareness of threats and best practices for prevention and response are both contributing factors. Furthermore, small businesses struggle with the complicated demands of risk assessments and implementing best practices. This problem involves more than just technical expertise; it also involves management and staff members being made at least somewhat aware of cyber best practices and procedures. Unfortunately, the speed at which cyber threats are evolving makes this undertaking especially challenging. JM Olejarz for Harvard Business Review explains, "hackers can change their tactics far faster and more easily than we can update our defenses. They can sidestep security simply by changing their IP addresses or adding a few lines of code to their malware, and they relentlessly pick apart apps, websites, and devices to find security holes they can exploit." For small businesses, closing the knowledge and resource gap in cybersecurity is essential. To preserve their survival and safeguard the privacy and data of their clients, they need to become aware of the need and have access to cost-effective and cybersecurity solutions that work with their resource limitations.

Another challenge faced by small businesses is the complex legal landscape of cybersecurity and compliance. Cybercriminals take advantage of the confusing legislation that can span across multiple jurisdictions, often going without punishment because the speed in

which they develop new attacks and techniques is faster than legislation can keep pace. Small businesses are left to navigate a tangled web of legal procedures that vary across countries. This process is often a disincentive for seeking legal action, ultimately contributing to low conviction rates of cyber criminals. The underreporting of cybercrimes due to embarrassment or uncertainty of the correct reporting channels masks the true severity of this issue. This situation calls for international collaboration and a unified approach to combat cybercrimes, as explained by Jennifer Saber in “Determining Small Business Cybersecurity Strategies to Prevent Data Breaches”. Saber notes, “If global laws do not advance and take precedence, a catastrophic cyber event would ensue," (Saber, 40). The current lack of a universal law over cybercrime leaves the world in a vulnerable position where "cybercriminals threaten individuals' economies and nations." (Saber, 40).

A lack of adequate cyber protection has the potential for not only immediate financial losses but also subsequence lawsuits, compensation demands, and regulatory fines. Compliance with a variety of data protection standards and privacy laws is critical for small businesses who expect to remain in business. For example, regulations that dictate the secure handling of personal health information, consumer data, and financial transactions are integral parts of a business model. Conducting a thorough cost-benefit analysis highlights the value of investing in cybersecurity measures against these potential financial and legal consequences. Proactive investment in cybersecurity is not merely a shield against cyber threats, but a strategic business decision essential for maintaining operational integrity, upholding customer trust, and safeguarding the enterprise's viability in the face of diverse and evolving legislation.

In order for small businesses to combat the unique cybersecurity challenges they face, a proactive, affordable, and effective strategy is required. Similar to the approach of Security Werks, this strategy must be specifically designed for the needs of small businesses. These solutions should be affordable and effective, focusing on leadership, risk management, cyber policies and procedures, training and awareness, incident response, compliance, and ultimately establishing a culture of security within the business. Additionally, to ensure success it is important to develop strategies that cater to both immediate cybersecurity needs and long-term development. By identifying important assets and understanding the risks, protective measures can be designed around any budget to be as effective as those used by larger corporations with more disposable income. As explained in "Integrated Framework for Information Security Investment and Cyber Insurance" by Shaun Wang, "SMEs generally lack access to knowledge and expertise to help them to prioritize their security investments" and would benefit from "basic cybersecurity measures that provide them with a minimal toolbox responding to easily correctible areas of vulnerability" (Wang, 6). This research supports the importance of a tailored approach that addresses the specific vulnerabilities and resource limitations of small businesses, enabling them to implement effective and sustainable cybersecurity measures.

Effective communication is a foundational element in building cybersecurity awareness among small businesses. It is through clear and relatable communication that business owners who are less technically inclined can become fully aware of the cybersecurity services available to them and understand how to implement these practices effectively. To build this awareness, the language and channels used to disseminate information must be carefully considered to ensure that they resonate with employees and management alike. "Information is at times

conflicting, causing confusion and uncertainty amongst SMBs. It is possible the overwhelming availability of cybersecurity information hinders rather than helps SMEs." (Chidukwani, et. al., 8). When cybersecurity concepts are communicated in a way that is clear, consistent, and constructive, it fosters an environment where each member of the organization becomes a proactive participant in defending against cyber threats. This approach strengthens both the cyber culture and security posture of the business.

Collaboration amongst small businesses is another key strategy that can support their cybersecurity defenses. By sharing strategies, successes, and failures, small businesses can strengthen their security measures. This communal exchange of information can help in developing best practices that are both effective and practical for businesses with similar profiles and challenges. Additionally, this approach allows for the pooling of resources, which is especially beneficial for businesses that may lack the financial capability to invest heavily in cybersecurity. Engaging with local business communities and industry associations can further amplify these efforts, providing a structured platform for collective cybersecurity initiatives and access to shared expertise.

Government intervention is another important aspect in steering small businesses toward a resilient cybersecurity infrastructure. By ensuring they provide new businesses with education on resources available to them, such as Security Werks and others designed to help small businesses, state government can assist in strengthening cyber defenses of those most vulnerable. It is not only about providing the tools but also ensuring that small business owners and their employees understand how to utilize them effectively. Training and awareness programs funded

or facilitated by government agencies can play a huge role in this educational process. In addition to education on services available to them, the availability of special loans and grants dedicated to cybersecurity improvements can motivate small businesses to invest in their cyber health. Financial incentives are a huge benefit to small businesses, many of which operate with limited budgets and may otherwise deprioritize cybersecurity due to cost concerns. As explained in "The severity and effects of Cyber-breaches in SMEs" by Ignacio and Juan De Arroyabe, "most small and medium-sized businesses feel that IS security is not their primary concern... This is due to the fact that SME managers evaluate that the level of risk is very low as compared with large companies, therefore having a false sense of security" (De Arroyabe, 5). This inaccurate perception can be shifted with the help of government-backed programs and financial support, which can highlight the importance of cybersecurity and provide the means to achieve it. By combining education with financial assistance, both state and federal government can improve the overall cyber culture of small businesses throughout the country. This approach would help bridge the gap between the perception of cybersecurity as an unnecessary or luxury investment and the reality of it being a critical business necessity.

In my research into the cybersecurity problems faced by small businesses and the solutions developed by Security Werks, I've discovered the unexpected relevance of past courses unrelated to the field of Cybersecurity. As part of my work towards earning a Bachelor's in Cybersecurity I've studied principles of public speaking, as well as survey of economics. Despite being unrelated to my main field of study, these courses equipped me with knowledge that was essential in developing the concept and business strategy for Security Werks.

Small businesses and startups often struggle with limited resources, making strategic financial decisions extremely important. Survey of economics introduces students to the fundamental concepts of cost-benefit analysis and externalities, both of which are relevant to the cyber challenges faced by small businesses. Cost-benefit analysis, a key economic tool, is particularly relevant in considering the services offered by Security Werks. Small businesses must weigh the cost of cybersecurity against the potential effects of a cyber-attack. This type of analysis can lead to a greater appreciation of Security Werks' value proposition. Additionally, the economic concept of externality can be seen in many areas of cybersecurity. Cyber-attacks can affect not only the targeted business but also its customers, partners, and the broader economic landscape. The solutions offered by Security Werks help mitigate these negative externalities, thus contributing to a more secure economic environment.

The art of communication is often as critical as the science of cybersecurity, especially when engaging with the small business sector where the stakes are high, and knowledge often limited. The skills and strategies taught in a principles of public speaking course- specifically audience analysis, informative speaking, and persuasion- were important in developing the business plan and will continue to be crucial moving forward. Through audience analysis, Security Werks can identify the unique cybersecurity needs and comprehension levels of each client. This approach not only ensures that the technical nature of our training services is adjusted to avoid overwhelming clients, but also focuses on the specific threats and preventative measures most relevant to the client. For example, a local retailer would receive guidance on securing transaction systems, while a med spa would learn how to protect patient data. This approach makes cybersecurity advice both relevant and actionable.

Alongside audience analysis, Security Werks deploys informative speaking to minimize the complexities of cybersecurity into understandable information. This skill is particularly important in a time when cyberthreats are developing and evolving at an alarmingly high rate. By translating the latest developments in cyber threats into clear, manageable information, Security Werks equips small businesses with the power to anticipate and counteract potential cyber threats. Additionally, persuasive communication is used to emphasize the risks of cyber negligent behavior. Through engaging, data-driven narratives Security Werks can stress the importance of investment in cybersecurity measures. This approach allows us to change a client's perspective of cybersecurity from an optional expense to an essential component of their business plan.

The interdisciplinary knowledge gained from both economics and public speaking courses has been extremely valuable in developing the Security Werks business model. Moving forward, the information from both courses will continue to influence and drive the services Security Werks has to offer.

Determining the efficacy of Security Werks cybersecurity products will require a multifaceted approach. We will utilize an extensive evaluation methodology that gather both quantitative and qualitative data to make sure our services are in line with the needs of small businesses and startups. Our primary metric is a careful examination of the improvements made to our client's cybersecurity posture. This will begin with an initial security assessment to establish a baseline against which future improvements are measured. Subsequently, periodic evaluations will be performed to track the progress in strengthening the network infrastructure,

adherence to updated policies, and the promptness of incident response handling. A decline in both the number and severity of vulnerabilities, combined with a decrease in reported suspicious activity or incidents, are signs of the increased security that our services have produced.

Client testimonials serve as another component of our assessment by providing insights into the user experience. By actively seeking client feedback we can focus on the effectiveness of our communication, the usefulness of the cybersecurity measures we deploy, and the overall value perceived by our customers. This qualitative feedback is instrumental in refining our services to ensure they remain impactful. Additionally, we monitor important business metrics such as revenue trends and customer retention rates following use of our cybersecurity solutions. For example, a client experiencing fewer business interruptions due to cyber threats is likely to see improved customer loyalty and potentially an increase in revenue, which can be attributed to the services provided by Security Werks.

By utilizing these methods of evaluation Security Werks can ensure we are providing the protection that is promised of our services, and support that promise with tangible and measurable results. The data we collect will allow us to determine how well our services are working, as well as help us to continuously improve our company.

To fulfil the vision of Security Werks, a strategic and resource-intensive startup plan is necessary. Being the true backbone of the entire operation, building a strong technical foundation is the first step in the process. This involves an investment in at least four servers to form the central hub of operation, hosting our security tools and managing network traffic. Additionally, at least 10 laptops and 2 desktops are needed to equip our cybersecurity analysts

with the tools necessary for in-house and on-site assessments. Supplementary equipment such as monitors, printers, desks, server racks, and secured storage equipment must also be considered when developing a lab environment. Finally, specialized equipment like hard drive cloners is also essential to reproduce data for analysis and reporting. Maintaining the integrity of these systems requires a continuous investment in software updates, security patches, and licenses. This proactive approach in updating and securing our systems assures our commitment to the highest standards of cybersecurity practices. While the initial investment for such a lab is considerable- estimated between $20,000 and $50,000- it is an essential investment that establishes Security Werks' ability to offer exemplary cybersecurity services.

In addition to the creation of our network infrastructure, there are several costs that will come with ensuring the success of Security Werks. The projected costs listed below are based on research into the average cost of first year business expenses. One of Security Werks most important resources will be the people behind the curtains. The initial team will consist of myself and my business partners as both the administrative support and cybersecurity talent, as well as legal counsel. In support of our market plan to establish an online presence, engaging with small business communities, and participating in business expos an estimated budget of $5,000 will be expected. Legal counsel and guidance will be necessary to ensure adherence to industry standards and regulations. We expect to invest approximately $10,000 in legal fees in the first year. Finally, the estimated operational expenses are expected to include software licenses, equipment maintenance, and staff development. Software licenses for the three founders, to include cybersecurity, incident response, and digital forensic tools, are expected to be anywhere between $7-18,000/annually. This number is dependent on type of tools we purchase and number

of employees. Equipment maintenance is also dependent on the upkeep of our devices, but we expect to spend between 5-10% of the initial cost of our network infrastructure. Finally, staff development such as training courses and certificated, workshops, and conferences are expected to be anywhere between $5-20,000/annually. This range is based on the type of training we participate in, the frequency of training, and the number of employees.

While the cost of starting a cybersecurity business such as Security Werks is high, our team plans to utilize several funding options and strategies. To optimize costs in the first year of business, operations will be run from our teams' home offices. This is a calculated risk that will save operational costs while allowing us to allocate funds to other critical areas. As our revenue increases and popularity grows, we will reevaluate the need for a dedicated office space that meets operational needs and strengthens our presence in the community. We intend on working with the Small Business Administration (SBA) to obtain our first business loan, as they are more likely to provide us with a low interest rate loan despite having less collateral available to secure the loan. In addition to a business loan, two of the three members of the Security Werks team qualify for specific federal grants and resources for veteran-owned, disabled-veteran owned, and women-owned small businesses. While the approval process is competitive, these grants will help immensely with the cost of startup.

While creating a comprehensive pricing plan for Security Werks, we've tailored a range of packages to suit the varied needs and resources of small businesses. Our Basic Cybersecurity Package, starting from $500, offers foundational risk assessments and essential cybersecurity training, perfect for new businesses looking to strengthen their security posture. The Standard

Package, ranging from $1,500 to $3,000, provides more detailed services, including comprehensive risk evaluations and advanced cybersecurity tools. This package is suitable for businesses with a dedicated budget for cybersecurity. Our premium package caters to businesses that prioritize cybersecurity at the core of their operations, and that require a more extensive suite of services. It is priced between $3,000 and $6,000, and delivers an in-depth risk assessment, tool setup, and advanced planning for incident response. Additionally, we offer flexible “A La Carte” services for targeted needs and a Subscription-Based Monitoring service to ensure ongoing network surveillance. This initial pricing plan ensures that Security Werks' solutions are accessible and adaptable to the needs of Hampton Road’s small businesses.

As Security Werks transitions from the planning stages towards full-scale operations, it is important for the team to reflect on our progress thus far to support how we strategize moving forward. The immediate future of Security Werks should be focused on refining our marketing approach and strengthening our finances. Moving forward, our marketing will involve utilizing digital platforms, such as social media and google ads, to reach a wider audience. Additionally, we will begin to engage with community services and events to help solidify our position locally. To better our finances our next step will be to seek out small business loans with reasonable terms, and explore grants tailored to veteran and women-owned businesses. With the influx of money, we will conduct a detailed review of our current budget and reallocate resources to maximize returns. This will guarantee that each investment we make moves us one step closer to being the leading cybersecurity company for small business in Hampton Roads.

In hindsight, developing Security Werks with my team has been a great learning experience. From the beginning, the importance of having a detailed business plan helped the project tremendously. From the business plan, it became clear to me that understanding market demands and legal compliance of having a cybersecurity business was just as important as being able to speak to the technical requirements of the business. The biggest lesson I learned was the significance of financial planning. Through research I learned about various funding avenues for small businesses, such as loans, grants, and venture capital. If I were to approach this project again, I would focus more on what it would take financially to start this type of business. In my opinion, funding the equipment alone for Security Werks would be a massive financial undertaking for new entrepreneurs. I may adjust my business model to start smaller, such as with the training aspect only, then branch into the technical side when more revenue was being generated.

References

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/access.2022.3197899

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES (SMEs). *Journal of Governance and Development (JGD)*, *18*(1), 75–87. https://doi.org/10.32890/jgd2022.18.1.5

IBM. (2022). *Cost of a Data Breach Report 2022*. https://www.ibm.com/downloads/cas/3R8N1DZJ

Rosenbaum, E. (2021, August 10). *Main Street overconfidence: America's small businesses aren't worried about hacking*. CNBC. https://www.cnbc.com/2021/08/10/main-street-overconfidence-small-businesses-dont-worry-about-hacking.html

The Evolving Cyberthreat. (2015, November 1). Harvard Business Review. https://hbr.org/2015/11/the-evolving-cyberthreat

Saber, J. (n.d.). *ScholarWorks Determining Small Business Cybersecurity Strategies to Prevent Data Breaches*. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=6270&context=dissertations

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2021). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, *17*(3), 1–27. https://doi.org/10.1080/17517575.2021.1942997

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580