An Extension of Small Business Cybersecurity Into the Classroom and Community

Ellen M. Raineri
Penn State University

Erin A. Brennan
Penn State University

Small business owners often feel immune to hackers because of their business's size and consequently do not have adequate security training, safeguards, policies, or insurance. Accordingly, small businesses are easy and frequent cybercrime targets because of limited budgets, technical personnel, and awareness. To increase small business owners' awareness, a university conference for Cybersecurity and Small Business was offered with PCI DSS, Social Engineering, and Company Cases topics. To augment such cyber knowledge generation, this paper contains cybersecurity outreach activities for small businesses and cybersecurity learning activities for entrepreneurship students who aspire to be small business owners.

Keywords: small businesses education, cybersecurity, entrepreneurship education, small mid-size enterprise, entrepreneur, entrepreneurship

INTRODUCTION

Small businesses often have limited resources, and entrepreneurs may not have cybersecurity backgrounds that allow them to understand cybersecurity best practices (U.S Small Business Administration, 2024). Nonetheless, small businesses utilize technology and are responsible for maintaining and securing data (Rahmonbek, 2024). As a result, small business owners need a basic understanding of cybersecurity to effectively reduce cybersecurity risks and comply with cybersecurity laws (U.S Small Business Administration, 2024).

This paper builds on the foundational learning components of the November 15, 2023 cybersecurity conference at Penn State Hazleton. In so doing, it explores the context of cybersecurity concerning small businesses. It offers practical learning activities and resources for entrepreneurs and small business owners who do not have a technology background. These resources will help small business owners and entrepreneurs become more informed and more secure. These resources also provide the foundation for colleges and universities to provide educational outreach to the small business community and aspiring entrepreneurs.

LITERATURE REVIEW

Cybersecurity Legal Compliance

Small business owners are already tasked with learning about and adhering to a variety of organizational, operational, and employment laws. Small business owners are obligated to stay informed of legal updates and ensure compliance (Forbes Business Council, 2020). As new technology evolves and small businesses continue relying on technology, small business owners need to expand their knowledge base to understand the basic laws that apply to cybersecurity to protect against data privacy breaches and cyberattacks (Cybersecurity: Challenges and Opportunities for Small Businesses, 2023). This can be challenging since the laws pertaining to cybersecurity, data security, and reporting are not a model of clarity and come from various sources (Bandler, 2023).

The United States does not have a single federal law addressing cybersecurity. The Federal Trade Commission (FTC) administers the Federal Trade Commission Act (FTCA), which prohibits deceptive business practices related to data security in business. Additionally, the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) regulate further aspects of cybersecurity (Brands, 2024). All 50 states, Puerto Rico, Guam, and the District of Columbia also have current or pending laws pertaining to data security, privacy, and/or cybersecurity (Cybersecurity 2023 Legislation, 2024).

The Biden Administration has recognized the need for the United States to develop a robust cybersecurity legal framework and as a result has prioritized promulgation of a comprehensive regulatory scheme and enforcement of the same (Joshi & Dobrygowski, 2024). The U.S. Small Business Administration (SBA) Office of Advocacy recognizes small businesses as those which employ fewer than 500 people. There are approximately 33 million small businesses in the United States, which collectively employ 61.7 million Americans while generating 36.2 percent of the private sector payroll (2023). Clearly, small businesses have a significant impact on the U.S. economy. If the cybersecurity of even one business is breached, it will not only impact that individual business but will also have a ripple effect. Developing laws recognize the vital role that small businesses play in the national economy and will impact small businesses (Kreps & Arsenault, 2023).

Small business owners not only have a legal responsibility to protect against cyberattacks but can further be legally required to report any attack that inevitably occurs. Every state has laws that establish a reporting duty when there is a data breach. The specifics of these laws vary, but they all require reporting to consumers and government agencies when a cybercrime data breach occurs (Bandler, 2023). Since the legal landscape is constantly being redefined, small businesses and entrepreneurs must build foundational knowledge of resources that will help provide up to date guidance.

Cybersecurity Challenges for Small Businesses

Several cybersecurity challenges exist for small businesses. Small business owners often do not think that a hacker would have an interest in attacking them and instead think that hackers would choose large businesses for attacks. Accordingly, small business owners do not feel the need to invest time and money to implement preventative security measures -- 59% of such owners believe attackers would bypass them since their businesses are too small (Rahmonbek, 2024). Yet, small businesses can be an easy target for hackers since adequate security measures are not utilized due to lack of knowledge or funding. Small businesses cannot afford to hire a full-time cybersecurity professional or to keep that employee current with training and certifications. Consequently, important security patches may not be applied; hardware and software may also not be updated for proper security defense. Small businesses are therefore often selected as targets for hackers. For example, 82% of ransomware attacks occurred in small businesses having under 1,000 employees, and hackers frequently selected small businesses as targets for malicious emails (Rahmonbek, 2024).

Another challenge is that small businesses owners do not have adequate security knowledge to fully understand threats or security proactive measures. Based on a study by Furman, Theofanos, Choong, and Stanton, only 8% of small business owners participated in cybersecurity training (2012). Additionally, the deficiency in cybersecurity knowledge even occurs with university entrepreneurship students who are depending upon universities to prepare them to be small business owners (Raineri & Fudge, 2019). As a result of inadequate cybersecurity knowledge, only 49% of small businesses have implemented cybersecurity safeguards within their businesses (Rahmonbek, 2024).

A final challenge is that most small businesses are unaware of or do not feel the need to purchase cyber insurance. Only 36% of small businesses are familiar with cyber insurance, and of those, only17% have purchased such insurance (Rahmonbek, 2024). Yet, cybersecurity insurance is vital to small businesses if attacked, especially since small businesses may retain customer data (personal and financial) and may also be governed by regulations related to customer data (PCI DSS or HIPAA). Cyber insurance is beneficial because it assists with costs such as fees for forensic investigations, crisis management costs; financial assistance with ransomware demands, fines and penalties associated with regulatory agencies (PCI DSS) or banks; legal fees; and crisis management costs. Last, although the purchase of cyber insurance is not legally required, all states require customers to inform their customers if a cyber breach has occurred that impacts customers' data (Simply Business, 2024).

CYBERSECURITY CONFERENCE BACKGROUND

On November 15, 2023, the Hazleton campus of Penn State University hosted a half-day cybersecurity conference designed to help small businesses learn about the dangers and impact of potential cyberattacks. The event was funded by Penn State's Center for Security, Research, and Education (CSRE), the Hazleton LaunchBox, and Penn State Hazleton. CSRE is an interdisciplinary hub that supports 13 Penn State units and focuses on interdisciplinary cybersecurity outreach activities, education, and research to positively impact individuals, infrastructure, society, and institutions (Penn State University, 2024). The Hazleton LaunchBox supports its local community by functioning as "a no-cost startup accelerator and coworking space designed to provide early-stage startup companies with the support and resources needed to build a sustainable business and a viable growth plan" (Penn State Hazleton, 2024, para. 1). Eighty individuals registered for the event and attended in-person and through Zoom from national and international locations.

Four sessions were included as part of the conference. Topics included "Law Enforcement Response to Emergent Cybersecurity Challenges"; "Achieving Zero Trust within Retail (Redner's Markets)"; "PCI Payment Card Industry Data Security Standard (DSS) – What is it? Why Should You Care"; and "Social Engineering – Why Human Weakness may be the Biggest Threat to Your Small Business" (Penn State Hazleton, 2023). Functioning as the keynote speaker was the Chief of Police from the Bloomsburg Police Department whose session was "Law Enforcement Response to Emergent Cybersecurity Challenges." The keynote speaker reflected upon the "Development of Pennsylvania Cybersecurity Threat and Intelligence Communications Unit; law enforcement challenges in adapting to the changing landscape as it pertains to technology and cybersecurity evolution; and a case study discussing a breach suffered by a local nonprofit" (Penn State Hazleton, 2023, para. 11).

The second session was co-presented by the Senior Information Security Engineer and the IT Security Analyst from Redner's Markets and was titled "Achieving Zero Trust within Retail (Redner's Markets)." The zero-trust model presumes that no individual or access point can be trusted inside or outside of the network perimeter (Cloudflare, 2024). Accordingly, proper security measures must be utilized. The speakers explored "Traditional cybersecurity challenges"; "What is zero trust?"; "Retail zero trust example,"; "Why it matters; Know your threat landscape"; and "Implementation for small businesses" (Senesap & Hozella, 2023).

The Chief Executive Officer of Backbone Security presented the third topic in a session called "PCI DSS – What is it? Why Should You Care?" The regulations of PCI DSS pertain to any company that receives, processes, and stores customers' credit card information. Yet, data shows that "27% of small businesses with no cybersecurity protections at all collect customers' credit card information" (Rahmonbek, 2024, para. 13). The Chief Executive Officer helped participants to understand "'What is the PCI DSS?'; 'Who needs to be PCI Compliant?'; 'Why are small businesses easy targets for credit card fraud?';

‘Common attack vectors’; ‘What will it cost my business to clean up after a breach?’; and ‘What can I do to help to keep my business and my customers’ data secure?’” (Penn State Hazleton, 2023, para. 13).

The fourth session was presented by the Chief Operating Officer of Backbone Security in a session called “Social Engineering – Why Human Weakness may be the Biggest Threat to Your Small Business.” The Chief Operating Officer increased cyber awareness by examining “‘Why are small businesses vulnerable to social engineering?’; ‘What could be the impact on your business if exploited?’; ‘What specific types of attacks should we look out for?’; ‘Examples of social engineering attacks and where the victim went wrong’; ‘How is AI changing the game?’; ‘How can small businesses/entrepreneurs prepare/protect themselves?’; ‘Is there a technical solution to defend against social engineering attacks?’” (Penn State Hazleton, 2023, para. 14). Participants received many take-away practical strategies to implement in their workplaces to assist their organizations in thwarting a social engineering attack.

DISCUSSION

In a study completed by Raineri and Fudge (2019), data shows that since university entrepreneurship students are not adequately prepared with cybersecurity knowledge and safeguards from academic classes, a majority of these students have instead needed to self-educate on various cybersecurity topics. In other instances, entrepreneurship students did not self-educate and were at risk when becoming small business owners. The study’s data suggests that cybersecurity self-education and deficient knowledge largely occurred within the topics of strong password creation, computer viruses, social engineering, employees as insider threats, BYOD, phishing, cybersecurity policies, physical security of data, network attacks, network vulnerability safeguards, and disaster recovery plans. Because of these findings, the authors recommended that university professors augment their entrepreneurship courses with cybersecurity learning activities which are incorporated in this paper. Last, small businesses can receive cybersecurity assistance from groups such as Small Business Development Centers (SBDCs) and university support centers. The authors also developed outreach activities incorporated in this paper to assist those outreach organizations.

CYBERSECURITY LEARNING ACTIVITIES

Entrepreneurship students are wise to begin to think through the broad implications of cybersecurity issues on small businesses. These learning activities are directed to an audience that does not have a technology or cybersecurity background. They are framed to allow entrepreneurship students to build a foundational awareness of cybersecurity issues through practical application. These activities can also serve as a continuing resource for entrepreneurs to review and apply as they build and grow their businesses. These learning activities can easily be adapted from classroom delivery to delivery in a community outreach setting.

Learning Activity 1: Social Engineering Team Assignment

Background Information

Social engineering uses technical or psychological approaches to exploit an employee and/or an organization (Wang, Sun, & Zhu, 2020). Phishing is a common technical tactic in which a hacker deploys emails that look credulous but instead deceive individuals into clicking on links that solicit personal information based upon fictitious but believable rationale. Phishing emails can also encourage recipients to download a file that contains malicious code. Mouton, Leenen and Venter (2016) contend that hackers rely on several strategies to influence email recipients to take action. For example, if the content of social engineering emails appears to be written by an authority figure (i.e. a workplace supervisor), then the recipient may take action. Also, a hacker may utilize reciprocity (i.e. sharing positive words with the recipient to build up trust and later exploit) to induce action. A hacker may also utilize scarcity ideas to imply limited availability and may encourage the recipient to act now to download a file or click on a link (Mouton, Leenen, & Venter, 2016).

Sawant (2022) refers to psychological and social engineering as a hack on humans. This type of social engineering is manipulative because it preys on employees' emotions, naivety, and trust; employees are deceived into divulging confidential information or providing unauthorized security access to the building or data (Aldawood & Skinner, 2019; Wang, Sun, & Zhu, 2020). For example, a hacker may impersonate a delivery person, cleaning personnel, or repair person to gain unauthorized access. Additionally, the hacker may tailgate by closely following an employee into a building as that employee swipes their badge. Such vulnerable employees yield to social pressure which could be remedied by providing proper cybersecurity training (Choi & Rubin, 2023). Identifying social engineering attacks is especially important for small businesses because employees of small businesses encounter 350% more social engineering attacks than employees who work at large companies (Rahmonbek, 2024).

Team Assignment

As a team, find or develop your own psychological social engineering narrative that you will role play in class. The social engineering narrative must be convincing and applicable to a small business. Choose roles representing the perpetrator, employee(s), narrator, or other roles as appropriate. Use props and uniforms as needed. Your role play should incorporate the perpetrator's goal, such as obtaining confidential information, getting secure access within the organization, or exploiting one or more of the organization's systems.

At the end of your role playing, debrief by summarizing the psychological techniques utilized and the ethical theories that are pertinent. Peers, small business owners who will be joining by Zoom, and the instructor will evaluate your team's role-playing in creativity, social engineering narrative believability, and your social engineering narrative's relatability to a small business.

Learning Activity 2: Building a Toolkit of Free Resources

In the United States, the legal landscape related to cybersecurity is rapidly evolving, and small businesses may find it daunting to stay current. Small businesses often are an easy target for cybercriminals because they lack the financial and time resources to protect themselves against an attack (Clark, 2024). Small business owners not only need to secure electronic information from attack, but they also need to be aware of increasing duties to report cyber-attacks. By way of context, President Joseph Biden recently issued an Executive Order that prioritizes data security (Executive Order No. 14117, 2024), and laws will certainly develop in response to this. In March 2024, The Cybersecurity & Infrastructure Security Agency issued draft rules that require mandatory reporting of cyber-attacks by businesses that own and operate critical infrastructure and carve out potential exceptions for small businesses (Rundle, 2024). Keeping up with the rapid pace of developing technology and law can be challenging. Using free resources is an effective way for a small business to protect itself and build its cybersecurity knowledge base.

1. The Cybersecurity and Infrastructure Security Agency offers great resources for small businesses (Cybersecurity and Infrastructure Security Agency, 2020). These resources are current and presented in a user-friendly manner. Take a moment to explore and bookmark the resources/references that are most relevant to you. Be sure to check back frequently. Create a list of resources and share it with your fellow students to compare the resources you have found to those they have found. Remember that one way to ensure current information is for a business to designate an employee to provide regular updates.
    - https://www.cisa.gov/secure-our-world
    - https://www.cisa.gov/audiences/small-and-medium-businesses
    - https://www.cisa.gov/secure-our-world/secure-your-business
2. Small Business Administrations (SBA) and local Chambers of Commerce also offer helpful cybersecurity resources. Review this resource from the U.S. Small Business Administration.
    - https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

Research and identify resources that your local SBA and or Chamber of Commerce may have. Bookmark these resources for easy reference. Create a list of resources and share it with your fellow students to compare the resources you have found to those they have found.

3. Remember to reach out to college students who have the benefit of specialized academic study to share. You may find fellow students who have an information technology (IT) or cybersecurity background and can help you think of ways to protect your data. As you launch and grow your business, remember that local colleges/universities may even offer free cybersecurity clinics like the ones referenced in this recent *Wall Street Journal* article.
    - https://www.wsj.com/lifestyle/careers/small-businesses-look-to-college-students-to-help-guard-against-hackers-61181777?mod=cybersecurity_more_article_pos4

    Contact local colleges/universities, including your own, to see if they offer free community resources. Create a list of resources and share it with your fellow students to compare the resources you have found to those they have found.
4. Reporting cybercrime helps to create a safer society and better information security. Never hesitate to report a crime. The FBI provides a centralized way to report cybercrimes through its Internet Crime Complaint Center (IC3). Other government agencies also offer ways to report cybercrimes and fraud. Review these websites to learn more about reporting. Create a list of resources and share your list with your fellow students to compare the resources that you have found to those that they have found.
    - https://www.ic3.gov/
    - https://www.justice.gov/criminal/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime
    - https://reportfraud.ftc.gov/
    - https://www.identitytheft.gov/

Learning Activity 3: Cybersecurity and Business Ethics

The law relative to cybersecurity is dynamic and developing. Many gaps still exist in the legal landscape as federal and state laws evolve and individual agencies enact regulations (Jaffries & Brazinski, 2023). Responsible business owners must keep themselves updated and comply with all legal requirements but in the absence of clearly stated laws, it becomes even more crucial to define and prioritize the ethical obligations of a business related to cybersecurity. Prioritizing ethical obligations to employees, customers, and stakeholders benefits businesses and society more broadly (Boyles, 2023).

By identifying stakeholders, business owners can begin to fully appreciate the impact of unethical business action on them. Using ethics to guide IT and cybersecurity decision-making, contributes to a sustainable business by mitigating legal liabilities and building stakeholder confidence (Farayola & Olorunfemi, 2024). You should consider your current business or, if you do not currently have a business, you should consider a hypothetical future business and answer these questions based on that hypothetical entity.

Use this learning activity to identify business stakeholders and assess your ethical obligations to each group you identify.

Step One

1. What type of business do you operate and what services/goods does it supply?
2. What type of electronic information do you maintain as part of your business?

Step Two

Now that you have defined your business and the electronic information that you are responsible for, you next need to consider your stakeholders.

1. Identify your stakeholders. Specifically, identify every broad group of stakeholders that is connected to your business –for example, employees, customers, and/or third parties.

2. For each category of stakeholders, identify the electronic information maintained by your business that impacts each category of stakeholders.

Step Three

Working with the information you have already identified, consider what might happen if there was a cybersecurity breach in your business. Project realistic worst-case scenarios and how any such scenario would impact each identified group of stakeholders.

Final Step

With your prior responses in mind, define the ethical obligations that you owe to each group of stakeholders and think through ways to enact cybersecurity policies and protections that will allow you to serve the ethical priorities of your business.

CYBERSECURITY OUTREACH ACTIVITIES

These activities help current business owners with limited or no technology or cybersecurity background. They provide the framework for small business owners to think through practical approaches to ensuring cybersecurity in their existing businesses. While these exercises can be used in a classroom setting, they are specifically directed to small business outreach efforts.

Outreach Activity 1: Defining Your Cybersecurity Culture

59% of businesses do not use security awareness training to educate their workforce (Hiscox, 2023) and a business is only as strong as its weakest link. Training employees can be impactful in preventing cyberattacks (U.S Small Business Administration, 2024). This can help accomplish the important task of establishing a workplace culture that prioritizes security and evidences ownership dedication to staying up to date on cybersecurity issues.

Use this learning activity to inventory and assess your current training by working through the following list of questions:

Training Inventory

1. Do you have an employee on-boarding process that includes cybersecurity basics?
2. Do you offer cybersecurity training to employees?
3. Do you regularly remind employees of the need to be vigilant in identifying phishing emails?
4. Do you update employees on developing cybersecurity issues?
5. Do you have policies that limit the use of employer owned laptops?
6. Is employee internet access restricted or limited to work related topics?
7. Do you require regular password updates for all employees?
8. Are employees informed of the process by which to report suspected security breaches?

Looking Ahead

1. Use free resources to protect yourself. You can build a custom Cybersecurity Plan by using the Federal Communications Commission (FCC) Cyberplanner. https://www.fcc.gov/cyberplanner
2. Check out free training resources that are available through the U.S. Small Business Administration. https://www.sba.gov/events?keyword=cybersecurity
3. Work through free learning modules offered by the Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/cyber-essentials-toolkits
4. Challenge yourself as an owner to update your knowledge base on an annual basis.

Outreach Activity 2: Cybersecurity Roundtable Discussion Topics

An additional outreach activity is for universities to organize and host monthly cybersecurity roundtable discussions for small business owners. Numerous benefits exist. Participation in a roundtable can help business owners increase their awareness of cybersecurity knowledge, issues, and safeguards. Being with peers can create a comfortable and confidential environment to candidly discuss internal cybersecurity roadblocks and share knowledge. Additionally, peers can hold each other accountable by defining specific cybersecurity goals and objectives and then providing updates at meetings. Last, participation in such roundtables provides networking and collaboration and the opportunity to obtain referrals (Bada & Nurse, 2019; Louisiana Economic Development, 2024).

Audience

Participants in the cybersecurity roundtable can include CEOs from small businesses who are directly contacted through local Chambers of Commerce, SCORE, SBDCs, University Incubator Centers, and university small business assistance programs (SCORE, 2024). Once CEOs indicate an interest in the roundtable, screening can be done by having CEOs complete a form with questions that can determine if the CEO is appropriate for the group. Such questions can focus on the name and address of the CEO's company, years in business, type of industry, number of employees, types of cybersecurity measures implemented, and requested cybersecurity topics (Louisiana Economic Development, 2024).

Topics

The topics for the cybersecurity roundtable discussion can be driven by preferences as indicated by participants on an initial screening form. Additionally, the initial discussion can focus on an overview of cybersecurity (definitions, buzzwords, compliance with regulations (PCI DSS, HIPAA), security awareness training, types of threats, types of protection, and security policies) since some CEOs may have little or no cybersecurity knowledge. Monthly topics can include the purpose and use of firewalls, creating and managing complex passwords, templates for cybersecurity policies, free and inexpensive education for employees, types of anti-malware software, industry regulations, and insider employee threats (RiskXchange, 2024). Including a segment on lessons learned would be beneficial as peers interrelate and learn from each other (Graves, 2022). Pertinent cybersecurity current events can be discussed at each meeting. Guest speakers can also be invited to showcase best practices from similar firms. If CEOs are considering cybersecurity product and service purchases, then vendors can be invited to showcase their offerings such as network monitoring, policy writing, or other areas of need (Graves, 2022; Kelly, 2011).

Speakers

University representatives would be moderators for each of the roundtable meetings. Free or inexpensive speakers can include university IT staff; university IT students; local IT business staff; Toastmasters' speakers; Chamber of Commerce members; Government agency employees; cybersecurity service providers; cybersecurity software and hardware providers; LinkedIn members; and SBDC speakers. The university moderator should request an outline for the guest speaker's talking points to determine if the content applies to the audience or if revisions are necessary. Last, to ensure availability when guest speakers are being utilized, a 6-month schedule can be developed to permit sufficient time for content review and coverage for all meetings.

Outreach Activity 3: Interviewing Cybersecurity Consultants

Importance

Many small or midsize businesses do not have the funds to hire their own cybersecurity staff (Jordan & Hannahs, 2013; Raineri & Fudge, 2019). Instead, such businesses may utilize security consultants on an as-needed basis in numerous areas such as conducting a cybersecurity assessment to identify vulnerabilities and create a remediation plan. These businesses must have foundational knowledge to ask the appropriate questions to determine which consulting firm to hire.

Outreach Activity

Cybersecurity outreach centers such as the SBDCs or University centers may assist small businesses by initially explaining to small and midsize business owners (who have no cybersecurity background) what a cybersecurity assessment is, the process used, and its importance. Then, such outreach centers can share important questions that small and midsize firms can plan to ask cybersecurity firms that they are interviewing to conduct a cybersecurity assessment.

As an example, here are some types of questions that might be considered:

1. How long has your firm been in business?
2. What types of cybersecurity services have you provided to small and mid-sized clients?
3. Have you provided cybersecurity services to clients in the same industry as mine?
4. Do you have any references or testimonials in the small and mid-size marketplace?
5. Would employees or consultants be performing the assessment?
6. How do you screen your employees/consultants before hiring?
7. What types of technical certifications or industry memberships are held by your employees/consultants?
8. Do you have experience with regulatory compliance with HIPAA, SOX, PCI DSS…. (if applicable)?
9. What does your firm do to conduct a cybersecurity assessment?
10. What tools does your firm use to conduct the assessment?
11. What people, processes, systems within my company do you need to access?
12. Can you discuss what will be included in the cybersecurity assessment report?
13. Do you have a sample generic cybersecurity assessment report I can review?
14. How long does an assessment take?
15. What is the cost and when is it due?
16. How is pricing determined for any recommendations contained in the assessment report? (VC3, 2023).

Outreach Activity 4: Non-Disclosure and Confidentiality Agreements

The safety of electronically stored data and information should be a priority regardless of a business's size and/or financial resources. In 2023, up to 73% of small businesses reported experiencing a data breach or cyber-attack (ITRC, 2023). As small businesses do their best to turn a profit, it can be tempting to overlook robust cybersecurity protections, but that decision can prove to be costly (Hiller, 2024). There can be a tendency to think primarily of outside threats to data security, but threats can also come from within a business. Businesses voluntarily and purposefully allow employees and third-party vendors to access confidential electronic information. These "inside" parties can also significantly threaten electronic information. In 2023, third-party vendors and malicious insiders accounted for over 50% of cybercrimes against small businesses (ITRC, 2023). Controlling insider access to confidential information and managing how that information can be used are important. One way to do this is by ensuring that your third-party contracts include language addressing information security and that your employees are bound by confidentiality or non-disclosure agreements. These contracts should be used as one part of your cybersecurity measures.

Part One of this exercise offers a step-by-step approach that will help you identify and inventory the third-party people/businesses who have authorized access to your data. You will then assess the contractual protections that your business has in place related to each of these third-parties. In Part Two, you will work through the same process focusing on employees.

Part One – Third Party Vendors

A. **Identify your Vendors**
   1. List all third-party vendors with whom you currently have a contract or with whom you anticipate you will have a contract.
   2. Determine and list whether you have a current contract with the vendor or if you have not yet entered into a contract.
   3. For each vendor, identify the service the vendor provides.

4. For each vendor, identify what, if any, access to confidential information/data the vendor needs to render its services.
5. If the vendor requires access to confidential information/data, then identify what particular information is needed and for how long access is required.

TABLE 1
VENDOR INFORMATION

Vendor Name	Current or Anticipated Contract	Service Provided	Is confidential access needed?	Confidential information that will be accessed	Frequency and Duration of Access

Now you know who the players are. Good work! The next process may involve some footwork on your part.

B. Review your vendor contracts

1. Collect your contracts with each vendor.
2. Review the language in each of those contracts. If there is a clause addressing data security, are you comfortable with it? Review the service provided and the data being accessed that you listed in Part A. Do you think the contract language sufficiently protects your data and access to your networks/information?
3. Does the contract language identify the specifics of what/who/how/why/when? Who will have access to the confidential information and/or your network? For what purpose will they have access? How will they gain access? When will access be granted and/or denied?
4. If you do not yet have a contract with a particular vendor, identify what language should be included in a future contract to protect your data and/or your network.

C. Looking Ahead

1. Remember that contracts are reached through negotiation. If you are not comfortable with the current language in any contract, consider negotiating new terms when your current contract expires or consider using a different vendor.
2. Be prepared. When you enter negotiations with new providers be sure to do your homework so you can come into negotiations with an informed position. You want to know what data needs protection so you can negotiate effectively from the start.
3. When a contract ends, remember to change passwords and access settings to ensure that access to your data/network is no longer available.

Part Two – Employees

A. Identify your employees

1. List all employees (FT & PT).
2. Identify whether each employee is a contract employee or an at-will employee.
3. Identify whether each employee needs access to confidential information.
4. If the employee requires access to confidential information/data, then identify what particular information is needed and for how long access is required.

TABLE 2
EMPLOYEE INFORMATION

Employee Name	FT or PT?	Contract or at will?	Is confidential access needed?	Confidential information that will be accessed	Frequency and duration of access

B. **Review your employment contracts and/or non-disclosure agreements.**

Remember that a non-disclosure or confidentiality agreement can be entered into by any employee. A non-disclosure or confidentiality agreement is a contract that binds the employee and the employer, but it is NOT an employment contract.

1. Collect the employment contracts for all contract employees who have access to confidential information/data.
2. Review the language in each of those contracts. If there is a clause addressing data security, are you comfortable with it? Do you think the contract language sufficiently protects your data and access to your networks/information?
3. Does the contract language identify the specifics of what/how/why/when the employee will have access to the confidential information and/or your network?
4. Collect non-disclosure/confidentiality agreements for all employees who have access to confidential information/data (remember that these agreements are contracts).
5. Review the language in each of these non-disclosure confidentiality agreements. Do you think the language sufficiently protects your data and access to your networks/information?
6. Does the language in each of these non-disclosure confidentiality agreements include the specifics of what/how/why/when the employee will have access to the confidential information and/or your network?

C. **Looking Ahead**

1. Develop template language that you can use for all new hires. This will allow you to enter into a confidentiality/non-disclosure agreement with new employees at the point of hire and is an easy way to ensure the enforceability of the contract.
2. Review this process with an attorney but do your homework before consulting an attorney. Be sure to collect all the relevant information and facts so you can educate your attorney as to the needs of your business.

CONCLUSION

The majority of small businesses store data and information using information technology. As a result, aspiring and current small business owners must understand the risks inherent to information technology so that they can take steps to protect their business and its information (Cybersecurity, 2023). This paper recognizes that need and seeks to provide accessible learning and outreach activities for aspiring and current business owners who do not have a background in technology. These activities should be used to direct classroom activities or to foster community engagement and learning with the small business community.

REFERENCES

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

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. https://doi.org/10.1108/ICS-07-2018-0080

Bandler, J. (2023, September 19). Cybersecurity law, compliance, and protection. *Reuters*. Retrieved from https://www.reuters.com/legal/legalindustry/cybersecurity-law-compliance-protection-2023-09-19/

Boyles, M. (2023, July 27). What are business ethics and why are they important? *Harvard Business School Online*. Retrieved from https://online.hbs.edu/blog/post/business-ethics

Brands, M. (2024, May 6). Cybersecurity laws and legislation (2024 update). *Connectwise*. Retrieved from https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation

Choi, Y., & Rubin, J. (2023). Social engineering cyber threats. *Journal of Global Awareness*, *4*(2), 1–12. https://doi.org/10.24073/jga/4/02/08

Clark, A. (2024, April 29). During national small business week, take steps to secure your business. *Cybersecurity & Infrastructure Security Agency*. Retrieved from https://www.cisa.gov/news-events/news/during-national-small-business-week-take-steps-secure-your-business

Cloudflare. (2024). *What is zero trust security?* Retrieved from https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

Cybersecurity 2023 legislation. (2024, January 8). *National Conference of State Legislatures*. Retrieved from https://www.ncsl.org/technology-and-communication/cybersecurity-2023-legislation

Cybersecurity and Infrastructure Security Agency. (2020, December). *Cyber essentials toolkits.* Retrieved from https://www.cisa.gov/resources-tools/resources/cyber-essentials-toolkits

Cybersecurity: Challenges and Opportunities for Small Businesses, Field Hearing. (2023). (Testimony of Kevin Stine). Retrieved from https://www.nist.gov/speech-testimony/cybersecurity-challenges-and-opportunities-small-businesses-field-hearing

Exec. Order No. 14117, 89 F.R. 15421 (2014, February 28). Retrieved from https://www.federalregister.gov/d/2024-04573

Farayola, O.A., & Olorunfemi, O.L. (2024). Ethical decision-making in IT governance: A review of models and frameworks. *International Journal of Science and Research Archive*, *11*(02), 130–138. https://doi.org/10.30574/ijsra.2024.11.2.0373

Forbes Business Council. (2020, July 22). *15 actions to help your business stay compliant with changing laws*. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2020/07/13/15-actions-to-help-your-business-stay-compliant-with-changing-laws/?sh=294d28955261

Furman, S., Theofanos, M.F., Choong, Y., & Stanton, B. (2012, March–April). Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, *10*(2), 40–49. https://doi.org/10.1109/MSP.2011.180

Graves, B. (2022). IT pros share tales from the cybersecurity trenches. *San Diego Business Journal*, *43*(35), 24–24, 26, 28, 30. Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/trade-journals/pros-share-tales-cybersecurity-trenches/docview/2765926890/se-2

Hiller, J., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*, *61*(1), 5–29.

Hiscox. (2023). *Hiscox Cyber Readiness Report 2023*. Retrieved from https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2023.pdf

Identity Theft Resource Center (ITRC). (2023). *2023 Business Impact Report*. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf

Jaffries, F., & Brazinski, A.G. (2023, October 9). Navigating the patchwork of U.S. privacy and cybersecurity laws: Key regulatory updates from summer 2023. *Reuters*. Retrieved from https://www.reuters.com/legal/litigation/navigating-patchwork-us-privacy-cybersecurity-laws-key-regulatory-updates-summer-2023-10-09/

Jordan, D.J., & Hannahs, J. (2013, March 21). *Collins subcommittee examines small business cyber-security challenges with new technologies*. Retrieved from https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=325180

Joshi, A., & Dobrygowski, D. (2024, January 1). The US has announced its national cybersecurity strategy: Here's what you need to know. *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

Kelly, L. (2011, September 13). IT security considerations for SMEs. *Computer Weekly*, pp. 19–20. Retrieved from https://search-ebscohost-com.ezaccess.libraries.psu.edu/login.aspx?direct=true&db=buh&AN=70124816&site=ehost-live&scope=site

Kreps, S., & Arsenault, A.C. (2023, April 14). What businesses need to know about the new U.S. cybersecurity strategy. *Harvard Business Review*. Retrieved from https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy

Louisiana Economic Development. (2024). *CEO Roundtables*. Retrieved from https://www.opportunitylouisiana.gov/program/ceo-roundtables

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Penn State Hazleton. (2023, October 27). *Cybersecurity for small business conference set for November 15 at Hazleton campus*. Retrieved from https://hazleton.psu.edu/story/16796/2023/10/27/cybersecurity-small-business-conference-set-nov-15-hazleton-campus

Penn State Hazleton. (2024). *Hazleton Launchbox: About*. Retrieved from https://hazleton.launchbox.psu.edu/about/

Penn State University. (2024). *Center for Security Research and Education: About*. Retrieved from https://csre.psu.edu/about/

Rahmonbek, K. (2024, February 1). *35 alarming small business statistics for 2024*. Retrieved from https://www.strongdm.com/blog/small-business-cyber-security-statistics

Raineri, E., & Fudge, T. (2019). Exploring the sufficiency of undergraduate students' cyber security knowledge within top universities' entrepreneurship programs. *Journal of Higher Education Theory and Practice*, *19*(4), 73–92. https://doi.org/10.33423/jhetp.v19i4.2203

RiskXchange. (2024). *Small to medium size business top 8 cyber security best practices*. Retrieved from https://riskxchange.co/285/small-to-medium-size-business-top-8-cyber-security-best-practices/

Rundle, J. (2024, March 27). U.S. publishes draft federal rules for cyber incident reporting. *WSJ Pro*. Retrieved from https://www.wsj.com/articles/u-s-publishes-draft-federal-rules-for-cyber-incident-reporting-c5c768d6?mod=tech_feat3_cybersecurity_pos5

Sawant, P. (2022, March 2). *Social engineering: The art of hacking humans* [Video]. YouTube. Retrieved from https://www.youtube.com/watch?v=lEK84lV6dxs

SCORE. (2024). *Score business owners roundtables*. Retrieved from https://www.score.org/newyorkcity/small-business-owner-roundtable

Senesap, J., & Hozella, J. (2023, November 15). Achieving zero trust within retail (Redner's Markets). [Conference presentation]. *Cybersecurity Conference for Small Business Conference*, Hazleton, PA, United States.

Simply Business. (2024). *Cyber insurance*. Retrieved from https://www.simplybusiness.com/business-insurance/cyber-liability-insurance/

U.S. Small Business Administration Office of Advocacy. (2023). *Frequently asked questions about small business, March 2023* [Data set]. U.S. Small Business Administration Office of Advocacy. Retrieved from https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf

U.S. Small Business Administration. (2024, March). *Strengthen your cybersecurity*. Retrieved from https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

VC3. (2023). Ten questions to ask when you're choosing a cybersecurity assessment provider. https://www.vc3.com/blog/cyber-security-assessment-provider

Wang, Z., Sun, L., & Zhu, H. (2020, January). Defining social engineering in cybersecurity. *IEEE Access*, *8*, 85094–85115. Retrieved from https://ieeexplore.ieee.org/document/9087851