FDD | CCTI Center on Cyber and Technology Innovation

Cyber Hygiene 101 for Small- and Medium-Sized Businesses

By RADM (Ret) Mark Montgomery and Theo Lebryk

July 28, 2021

Introduction

Industry reports and surveys paint a frightening picture of the cybersecurity landscape for small- and medium-sized businesses (SMBs): Between 2019 and 2020, cyber intrusions increased by 400 percent around the world, while the FBI received up to 4,000 cyberattack-related complaints per day.[1] Forty percent of cyberattacks target SMBs, and up to half of all SMBs experience a breach each year.[2] In 2020, the total cost of ransomware payments was $350 million, a 311 percent increase from the previous year.[3] In 2020, the average cost of repairing a data breach was $2.64 million for companies with fewer than 500 workers.[4] A report on critical infrastructure SMBs found that 46 percent of hacked companies lost customers and 59 percent reported losses in daily productivity because of a breach.[5] No wonder 60 percent of small businesses go out of business within six months of a cyber incident.[6]

SMBs are often unprepared to respond to cyberattacks. Nearly two-thirds of SMB CEOs confess that their companies lack an active, up-to-date cybersecurity strategy.[7] This report consolidates advice from industry and the U.S. government on cyber best practices. It provides SMBs a high-level overview of how to integrate investments in people, processes, and technologies to mitigate the risk of the most common types of cyberattacks. For a more comprehensive list of industrial cybersecurity standards and technological controls, the Foundation for Defense of Democracies has also released a "Comparison of Cybersecurity Guidance for Critical Infrastructure Sectors."[8]

1. Maggie Miller, "FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic," *The Hill*, April 16, 2020. (https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic); Tonya Riley, "The Cybersecurity 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds," *The Washington Post*, February 22, 2021 (https://www.washingtonpost.com/politics/2021/02/22/cybersecurity-202-cybercrime-skyrocketed-workplaces-went-virtual-2020/)

2 Gabriel Bassett et al., 2021 Data Breach Investigations Report," *Verizon*, May 2019. (https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/); "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses," *Ponemon Institute*, October 2019. (https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf); "2021 Cybersecurity Survey: Critical Infrastructure Small and Medium-Sized Businesses," *USTelecom*, March 2021. (https://www.ustelecom.org/research/2021-cybersecurity-survey-critical-infrastructure-small-and-medium-sized-businesses)

3. "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," *Chainalysis*, January 26, 2021. (https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021); "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," *Institute for Security and Technology*, April 2021. (https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf)

4. "Cost of a Data Breach Report 2020," *IBM*, July 2020. (https://www.ibm.com/security/data-breach)

5. "2021 Cybersecurity Survey: Critical Infrastructure Small and Medium-sized Businesses," *US Telecom*, March 2021. (https://www.ustelecom.org/research/2021-cybersecurity-survey-critical-infrastructure-small-and-medium-sized-businesses/)

6 Robert Johnson, III, "60 Percent Of Small Companies Close Within 6 Months Of Being Hacked," *Cybercrime Magazine*, January 2, 2019. (https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/)

7. "Cyberthreats and Solutions for Small and Midsize Businesses," *Vistage*, May 2018. (https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912)

8. Georgianna Shea, "Comparison of Cybersecurity Guidance for Critical Infrastructure Sectors," *Foundation for Defense of Democracies*, July 22, 2021. (https://www.fdd.org/analysis/2021/07/22/comparison-of-cybersecurity-guidance-for-critical-infrastructure-sectors/)

Cyber Hygiene: People, Processes, and Technology

All businesses face a choice when it comes to technology management, cybersecurity, and risk acceptance: Should the company employ a dedicated, in-house security operations center or outsource these tasks to a managed service provider? In general, outsourcing is the cheaper and more practical solution for SMBs. Regardless of who manages security functions, however, businesses have to understand the risks that stem from the combination of people, processes, and technologies, and weigh their tolerance for those risks.

Cyber hygiene entails persistent due diligence and comprehensive due care. Due diligence is the continual evaluation of security practices; due care is the action taken to ensure security. While the practices listed below should help reduce risk, it is equally important for businesses to be ready to adapt to new exploits presented by the adversary. It is worth noting, then, that enterprise cybersecurity is as much about mindset as it is about any single person, process, or product.

People

Cyberattacks cut across the targeted organization, meaning that every employee needs to understand his or her role in preventing attacks. Employees are both the primary line of defense against cyberattacks and often the weakest link targeted by malicious actors. In fact, IBM estimates that human error contributes to 95 percent of security breaches.[9] The best technology in the world today still cannot always prevent employees from clicking on a phishing scam or stop security professionals from neglecting to install a critical security update.

Therefore, businesses should train and educate all of their employees on the importance of:

Using Secure Passwords

Reports indicate that 81 percent of cyber breaches involved weak or reused passwords.[10] Increasing password complexity and incorporating additional good password habits make it harder for hackers to access accounts, sign into other accounts that share the same password, and establish persistent access to computer networks and devices. Some examples of good and poor password habits include:[11]

9. Frank Ohlhorst, "IBM Says Most Security Breaches Are Due to Human Error," *TechRepublic*, October 8, 2014. (https://www.techrepublic.com/article/ibm-says-most-security-breaches-are-eue-to-human-error)

10 Thu T. Pham, "Stop the Pwnage: 81% of Hacking Incidents Used Stolen or Weak Passwords," *Duo Security*, May 2, 2017. (https://duo.com/decipher/stop-the-pwnage-81-of-hacking-incidents-used-stolen-or-weak-passwords).

11. U.S. National Institute of Standards and Technology, "Digital Identity Guidelines: Authentication and Lifecycle Management," June 2017. (https://pages.nist.gov/800-63-3/sp800-63b.html#appA); U.S. Federal Communications Commission, "Cybersecurity for Small Business," January 2020. (https://www.fcc.gov/general/cybersecurity-small-business); U.S. Small Business Administration, "Stay safe from cybersecurity threats," accessed June 30, 2021. (https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats); U.S. National Security Agency, "NSA's Top Ten Cybersecurity Mitigation Strategies," March 5, 2018. (https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf?v=1); U.S. Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-002): Choosing and Protecting Passwords," November 18, 2019. (https://us-cert.cisa.gov/ncas/tips/ST04-002)

Poor Passwords Habits	Good Passwords Habits
• Common passwords (e.g., password123) • Human-readable, dictionary words • Repeat passwords • Short passwords (less than eight characters) • Default passwords	• Password managers • Long, random, unique passwords • Multifactor authentication • Changing default passwords

Avoiding Email Scams

According to the cybersecurity company Proofpoint, 88 percent of organizations worldwide experienced spear-phishing attempts in 2019.[12] Spear phishing is the act of sending emails containing malware to individuals, often appearing to be sent from a trusted email account. By carefully inspecting the source of the email, or the email sender, and not clicking on suspicious links or download prompts, users can avoid falling victim to email-based scams and attacks.[13]

Practicing Good Physical Security Habits

In addition to monitoring cybersecurity threats from external sources, SMBs should also be vigilant about physical threats to technology assets.[14] A recent study reported that almost 30 percent of businesses do not regularly conduct regular reviews of physical security as part of their cybersecurity practices.[15] Employees should be reminded never to leave a computer unlocked or unattended in a public setting.

Updating Software

In a 2019 survey, 60 percent of respondents reported breaches as a result of "unpatched" software for which a patch was available for download.[16] Employees should turn on automatic updates where possible and follow

12. "2020 State of the Phish: an in-depth look at user awareness, vulnerability and resilience," *Proofpoint*, 2020. (https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf)
13. U.S. Federal Trade Commission, "How to Recognize and Avoid Phishing Scams," May 3, 2019. (https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)
14. U.S. Department of Education, "Data Security: Top Threats to Data Protection," June 2015. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf); U.S. Federal Communications Commission, "Cybersecurity for Small Business," January 2020. (https://www.fcc.gov/general/cybersecurity-small-business); U.S. Small Business Administration, "Stay safe from cybersecurity threats," accessed June 30, 2021. (https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats)
15. "Seventh Annual Study: Is Your Company Ready for a Big Data Breach?" *Ponemon Institute*, February 2020. (https://www.experian.com/blogs/ask-experian/wp-content/themes/exp/pdf/experians-seventh-annual-data-breach-preparedness-study.pdf)
16. "Costs and Consequences of Gaps in Vulnerability Response," *Ponemon Institute*, 2019. (https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html)

guidance from system administrators to ensure updates are safely incorporated into the network environment.[17] Additionally, employees should not download software from unknown sources and should verify the update's authenticity with network administrators before proceeding with the download.

Practicing Safe Browsing

When possible, employees should avoid using public Wi-Fi, which attackers can use to steal passwords or company information.[18] When employee use of public Wi-Fi is unavoidable, the businesses should provide a virtual private network (VPN) to encrypt traffic. Additionally, any URL can potentially be used to install malware on a device, so employees need to be careful not to browse untrusted websites and should never disclose passwords over unsecure sites. Browsers such as Google Chrome, Mozilla FireFox, and Microsoft Edge warn users that a website is unsecure by placing an open lock by the URL.

Practicing Safe Social Media Habits

Social media can provide hackers with a significant amount of information, including names, birthdays, spouse and pet names, and places of employment. Given that much of this information is often used to create usernames and passwords, it is highly valuable to hackers. By avoiding the disclosure of personal information over social media and using password managers to increase password complexity, employees can make it more challenging for hackers to access their accounts.

Backing up Data

The recent uptick in ransomware attacks has shown that a failure to back up data can significantly impact a company's ability to withstand a cyberattack. Regularly backing up files and programs, either through cloud services or through physical hard drives, will facilitate recovery efforts from cyberattacks such as ransomware.[19] For larger companies, sophisticated network configuration can render ransomware ineffective.

---

17. U.S. Federal Bureau of Investigation, "OPS Cyber Awareness Guide," July 2016. (https://www.fbi.gov/file-repository/cyber-awareness-508.pdf/view); U.S. Federal Emergency Management Agency, Ready, "Cybersecurity," March 16, 2021, (https://www.ready.gov/cybersecurity); U.S. National Security Agency, "NSA's Top Ten Cybersecurity Mitigation Strategies," March 5, 2018. (https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf?v=1); U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Essentials," accessed June 30, 2021. (https://www.cisa.gov/cyber-essentials); U.S. Department of Education, "Data Security: Top Threats to Data Protection," June 2015. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf); U.S. Federal Communications Commission, "Cybersecurity for Small Business," January 2020. (https://www.fcc.gov/general/cybersecurity-small-business)

18. U.S. Federal Bureau of Investigation, "Simple Steps for Internet Safety," October 11, 2016. (https://www.fbi.gov/news/stories/simple-steps-for-internet-safety)

19. Ready.gov, "Cybersecurity," March 16, 2021. (https://www.ready.gov/cybersecurity); U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Essentials," accessed June 30, 2021. (https://www.cisa.gov/cyber-essentials); U.S. Department of Education, "Data Security: Top Threats to Data Protection," June 2015. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf); U.S. Federal Communications Commission, "Cybersecurity for Small Business," January 2020. (https://www.fcc.gov/general/cybersecurity-small-business).

Processes

A number of frameworks provide high-level ways of ensuring good cybersecurity. These include the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework,[20] the Center for Internet Security's Security Controls,[21] and the International Organization for Standardization's 27001 document,[22] as well as industry-specific security frameworks.

Every framework consists of a set of "controls," which are processes or best practices to secure an organization's assets. These controls can be grouped into methods used to plan for, protect against, detect, respond to, or recover from attacks. Organizations should have clear policies and procedures on cybersecurity. These policies should include designating people in charge of tasks to oversee a set of predetermined steps to be taken throughout the response and recovery process.

Anticipating and Preventing Attacks

To plan for attacks and anticipate threats, companies should conduct threat modeling.[23] This entails analyzing a company's digital infrastructure, identifying threats, ranking which threats are most important, and determining countermeasures.

Analyzing a company's infrastructure means breaking down a network and understanding how each individual section operates. With the network's architecture in mind, businesses can examine every section of it and identify weaknesses as part of a systematic vulnerability assessment.[24] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency provides free scanning and assessments to most businesses upon request.[25] Penetration testing (a term often used synonymously with "red teaming") is the practice of stress testing a system by utilizing a dedicated team to attempt to break into the system or exploit potential vulnerabilities. This testing can further identify weaknesses in the network.[26]

Businesses can also participate in information sharing schemes to better understand recent developments in the threat landscape. The U.S. government promotes membership in Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). These institutions allow firms in similar

20. U.S. National Institute of Standards and Technology, "Cybersecurity Framework," November 19, 2019. (https://www.nist.gov/cyberframework)
21. "CIS Controls," *Center for Internet Security*, accessed June 30, 2021. (https://www.cisecurity.org/controls)
22. "ISO/IEC 27001: Information Security Management," *International Organization for Standardization*, accessed June 30, 2021. (https://www.iso.org/isoiec-27001-information-security.html)
23. There are a number of ways to approach threat modeling, such as STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege), DREAD (damage potential, reproducibility, exploitability, affected users, and discoverability), PASTA (process of attack simulation and threat analysis), and NIST's data-centric threat modeling. For an overview of threat modeling, see: Josh Fruhlinger, "Threat Modeling Explained: A Process for Anticipating Cyber Attacks," *CSO Online*, April 15, 2020. (https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html)
24. Jeff Goldman, "How to Conduct a Vulnerability Assessment: 5 Steps toward Better Cybersecurity," *ESecurityPlanet*, April 17, 2019. (https://www.esecurityplanet.com/networks/how-to-conduct-a-vulnerability-assessment-steps-toward-better-cybersecurity)
25. U.S. Cybersecurity and Infrastructure Security Agency, "National Cybersecurity Assessments and Technical Services," accessed June 30, 2021. (https://us-cert.cisa.gov/resources/ncats)
26. Wayne Rash, "DIY Penetration Testing to Keep Your Network Safe," *PCMag*, March 28, 2019. (https://www.pcmag.com/news/diy-penetration-testing-to-keep-your-network-safe)

sectors to collaborate and share information about relevant threats. ISACs are geared toward larger businesses with in-house cybersecurity defense capabilities. ISAOs are more suitable for small businesses but may not provide as frequent or high-quality information.[27]

Having identified potential threats, teams should evaluate the costs of improving defenses. The reality of cybersecurity for SMBs is that there are more threats than an SMB can feasibly defend against. Therefore, the threat modeling framework is a tool to conduct a cost-benefit analysis of threats so an organization can prioritize where to spend its resources.

Detecting Threats

Network administrators need to know as soon as possible when their company has been hacked. A 2020 IBM report found that the average breach goes undetected for 207 days. The report also found that detecting and containing a breach in under 200 days saved the hacked organization $1.12 million on average.[28] Businesses should set up tools to detect suspicious activity, especially around high-priority assets. For instance, any changes to sensitive files should be logged and flagged for network administrators.[29]

Meanwhile, employees throughout an organization should know the common signs of a cyberattack. These include unexpected installations on a device; frequent browsing redirects or pop-ups while browsing the web; changed or broken passwords; and disabled anti-malware, task manager, or registry editor programs.

Responding to Threats

Based on the threat modeling's results, SMBs should establish protocols for reacting to attacks. All employees should know the protocol for how to report and take initial steps when they become aware of a breach. Each attack demands a slightly different response, but the short-term response to a cyberattack generally involves isolating the affected parts of the system, revoking the access or privileges of compromised users, purging the hacker from the system, and alerting law enforcement and any affected parties.[30] While there currently is no national breach-notification law, states have their own data-breach notification laws, and regulated industries may have additional reporting requirements. Accordingly, SMBs need to develop procedures and policies in line with these requirements.

Recovering From Attacks

On the software side, the most common step toward recovery is restoring computers to a previous backup. Online guides can provide instructions on how to restore prior working states.[31] These instructions are especially helpful in the event of a ransomware attack.

27. Jaikumar Vijayan, "What Is an ISAC? How Sharing Cyber Threat Information Improves Security," *CSO Online*, July 9, 2019. (https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html)
28. "Cost of a Data Breach Report 2020," *IBM*, July 2020. (https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
29. Traci Spencer, U.S. National Institute of Standards and Technology, "How to Detect a Cyber Attack Against Your Company," November 7, 2019. (https://www.nist.gov/blogs/manufacturing-innovation-blog/how-detect-cyber-attack-against-your-company)
30. When a hacker steals personal information, follow the procedures laid out in: U.S. Federal Trade Commission, "Data Breach Response: A Guide for Business," April 29, 2019. (https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business)
31. Kyle Chivers, "How to remove malware from a Mac," *Norton Antivirus*, October 1, 2020. (https://us.norton.com/internetsecurity-malware-how-to-remove-malware.html)

Recovering from business interruption is more complicated. Cyber insurance is becoming increasingly common for businesses of all sizes, but SMBs have still been slow to purchase cyber insurance.[32] A 2020 study found that more than half of all SMBs lack cyber insurance despite the prevalence of cyberattacks affecting them.[33]

A recent Government Accountability Office report noted that while demand for cyber insurance policies has continued to increase year over year, the cost of insurance premiums increased 10 to 30 percent in the third and fourth quarters of 2020.[34] The increase in premiums is reportedly attributed to higher losses from the increasing number of cyberattack insurance claims. The increase in price has effectively shifted cyber insurance policies from an affordable $1,000 investment for a basic policy to a price that is likely out of reach for some SMBs.[35] Even if affordable, these basic insurance policies may not provide coverage for revenue lost while fixing a breach.[36] Needless to say, cyber insurance is not a substitute for other best practices.

Technology

There is no single software suite that will work for every business. Businesses need to weigh their specific needs, risks, and constraints when purchasing technologies. Businesses must also ensure their employees can easily adapt a given technology to their work. This means clear company policies, easily installable software, and basic training so employees know how to use the tools and products provided. For example, a password manager is useless if employees never use it or if they use it only to fill in the same password over and over again. While not exhaustive, the following list provides 12 technologies that can assist SMBs in their cybersecurity efforts.

Password Managers, Single Sign-On, and Multi-Factor Authentication

Password managers generate random, hard-to-guess passwords.[37] They require an employee to remember only a single secure password to access the full collection of advanced passwords for all his or her accounts. Most modern web browsers have built-in password managers that can generate and store hard-to-guess passwords.

Single sign-on is a similar solution in which employees need to log in only once to access an entire suite of apps for a set period of time.

32. Nour Aburish, Annie Fixler, and Michael Hsieh, "The Role of Cyber Insurance in Securing the Private Sector," *Foundation for Defense of Democracies*, September 13, 2019. (https://www.fdd.org/analysis/2019/09/11/cyber-insurance)
33. "Small Business, Huge Risks Cyberattacks among Largest Risks SMBs Face Today," *CyberScout*, October 6, 2020. (https://cyberscout.com/en/press-releases/majority-of-us-small-and-medium-sized-businesses-do-not-have-cyber-insurance)
34. U.S. Government Accountability Office, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," May 2021. (https://www.gao.gov/assets/gao-21-477.pdf)
35. Nour Aburish, Annie Fixler, and Michael Hsieh, "The Role of Cyber Insurance in Securing the Private Sector," *Foundation for Defense of Democracies*, September 13, 2019. (https://www.fdd.org/analysis/2019/09/11/cyber-insurance)
36. Trevor Logan, "The Time for Cyber Insurance: Coverage Improves Supply Chain Resiliency," *Foundation for Defense of Democracies*, September 2, 2020. (https://www.fdd.org/analysis/2020/09/02/the-time-for-cyber-insurance)
37. U.S. Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-002): Choosing and Protecting Passwords," November 18, 2019. (https://us-cert.cisa.gov/ncas/tips/ST04-002); U.S. Department of Homeland Security, "Cyber Lessons," May 23, 2018. (https://www.dhs.gov/be-cyber-smart/cyber-lessons)

Multi-factor authentication means requiring verification from a second "factor," which may be either a separate login step or a physical token.[38] Even if attackers guess a password, they will still need to get access to the second factor, which makes it harder to gain unauthorized access to the targeted network.[39]

Access Control

Most networks have some form of built-in login or access-control system to keep out unauthorized users.[40] Businesses should configure their login systems so that users cannot use weak passwords and will get locked out after a certain number of failed attempts. Accounts and devices should be configured to lock automatically after a certain period of inactivity. Companies should also consider configuring their access-control systems to apply other security measures, such as preventing logins from foreign countries or unusual locations. Finally, employees should have access only to the information they need for their jobs. For instance, most employees should not be able to access or alter sensitive customer information.

Most often, a dedicated network administrator determines how to configure the network. Therefore, it is especially crucial that network administrators practice good cyber hygiene, as an attack that compromises an administrator potentially gives the attacker control over the entire network. Administrators should use their administrator accounts only when necessary; they should have a separate account for all other functions, such as browsing the web.

Firewalls, Intrusion Prevention Systems, and Endpoint Protection Platforms

Most networks should have comprehensive schemes to prevent malicious cyber activity from ever reaching a computer or device (known as an endpoint). At a minimum, this means employing a standard firewall that filters out malicious traffic.[41]

Many companies employ multiple layers of protection, such as an intrusion prevention system[42] underneath the main firewall.[43] These systems provide a second line of defense in filtering out malicious traffic and can alert administrators to any suspicious activity.

---

38. U.S. Department of Education, "Identity Authentication Best Practices," July 2012. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Identity_Authentication_Best_Practices_0.pdf); U.S. Department of Education, "Data Security: Top Threats to Data Protection," June 2015. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf); U.S. Federal Communications Commission, "Cybersecurity for Small Business," January 2020. (https://www.fcc.gov/general/cybersecurity-small-business); U.S. Small Business Administration, "Stay safe from cybersecurity threats," accessed June 30, 2021. (https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats); U.S. National Security Agency, "NSA's Top Ten Cybersecurity Mitigation Strategies," March 5, 2018. (https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf?v=1)

39. Joel Witts, "The Top Multi-Factor Authentication (MFA) Solutions for Business," *Expert Insights*, January 1, 2021. (https://expertinsights.com/insights/the-top-multi-factor-authentication-mfa-solutions-for-business)

40. Vincent Hu, David Ferraiolo, and Richard Kuhn, U.S. National Institute of Standards and Technology, "Assessment of Access Control Systems," September 29, 2006. (https://doi.org/10.6028/NIST.IR.7316)

41. Karen A. Scarfone and Paul Hoffman, U.S. National Institute of Standards and Technology, "Guidelines on Firewalls and Firewall Policy," September 28, 2009. (https://www.nist.gov/publications/guidelines-firewalls-and-firewall-policy)

42. Karen Scarfone and Peter Mell, U.S. National Institute of Standards and Technology, "Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology," February 20, 2007. (https://doi.org/10.6028/NIST.SP.800-94)

43. "What Is an Intrusion Prevention System?" *Palo Alto Networks*, accessed June 30, 2021. (https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips)

Endpoint protection platforms serve a similar function by scanning files and checking them against extensive, externally maintained threat databases to prevent malware from ever reaching the computer.[44]

The precise differences between firewalls, intrusion prevention systems, and endpoint protection platforms are less important than the general need for products that can filter out malicious traffic. As businesses grow and encounter more sophisticated attacks, their endpoint security should also become more sophisticated. However, everyone, from the smallest businesses to individual contractors, should have at least some software to filter out harmful traffic.

Anti-Malware

Malware is short for *malicious software*, which is specifically designed to damage data or a computer system. It is software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Malware typically comes in the form of malicious code hidden in computer systems and is often installed without the knowledge or consent of the computer's owner, using viruses, worms, or trojan horses. Anti-malware is software that scans incoming files and downloads to prevent a user from being infected.[45] It should regularly scan the computer to find any malware that slipped past that first line of defense. Anti-malware software uses techniques such as signature-based detection, behavior-based detection, and sandboxing to protect systems from malicious software. The value of anti-malware applications goes beyond simply scanning files for viruses. Anti-malware programs can also detect advanced forms of malware and offer protection against ransomware attacks.

VPNs and Zero-Trust

Many companies use VPNs to encrypt and help authenticate remote traffic.[46] VPNs operate by creating a tunnel between a user and the network. Instead of having data go directly from the user to the end location, VPNs act as a middleman, encrypting traffic between the two parties to make it harder for attackers to intercept or impersonate a user.

However, cybersecurity experts increasingly see VPNs as insufficient protection against unauthorized traffic. They instead recommend building zero-trust networks, which do not give automatic access to the network merely through a VPN. Zero-trust networks operate under the mantra "never trust, always verify." No user or device is trusted by default, meaning that even within a network, users must constantly verify their identity.[47] This paradigm helps isolate and identify breaches but is still a relatively new phenomenon. Therefore, transitioning toward a zero-trust network will likely take time for many organizations.

---

44. "What Is an Endpoint Protection Platform?" *McAfee*, accessed June 30, 2021. (https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-an-endpoint-protection-platform.html)

45. U.S. Department of Education, "Data Security: Top Threats to Data Protection," June 2015. (https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Issue%20Brief%20Data%20Security%20Top%20Threats%20to%20Data%20Protection_0.pdf); U.S. Small Business Administration, "Stay safe from cybersecurity threats," accessed June 30, 2021. (https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats); Jon Martindale, « What is antivirus software, and how does it work?," *Digital Trends*, August 26, 2020. (https://www.digitaltrends.com/computing/what-is-antivirus-software/).

46. Murugiah P. Souppaya and Karen A. Scarfone, U.S. National Institute of Standards and Technology, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," July 2016. (https://doi.org/10.6028/NIST.SP.800-46r2)

47. Scott Rose et al., U.S. National Institute of Standards and Technology, "Zero Trust Architecture," August 11, 2020. (https://doi.org/10.6028/NIST.SP.800-207); U.S. National Security Agency, "Embracing a Zero Trust Security Model," February 25, 2021. (https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF)

Data Loss Prevention

Data loss prevention (DLP) software is the opposite of a firewall: It ensures sensitive data does not leak out into the broader internet.[48] Many cybersecurity software providers (such as McAfee, Norton, et cetera) can bundle DLP, firewalls, data sanitization, and anti-malware software all in one. DLP software monitors business-critical data and identifies violations of policies defined by the SMB. If violations are identified, DLP software provides alerts and other protective actions to prevent end users from accidentally or intentionally sharing data that could put the SMB at risk. DLP software and tools monitor and control endpoint activities, filter data streams on business networks, and monitor data in the cloud to protect data at rest or in motion.

Email Protection Systems and Anti-Phishing Tools

Most email providers supply baseline spam filtering either by default or for purchase. Adding additional software on top of what the email provider offers can mitigate phishing attacks.[49] Specifically, email protection systems should have:

- Sender Policy Framework: Limits the number of internet protocol (IP) addresses using a business' domain, to prevent email spoofing.
- Domain Keys Identified Mail: Uses a digital signature to ensure no one tampers with an email after it is sent.
- Domain-based Message Authentication Reporting and Conformance: Verifies if a sender is legitimate, and manages the policy governing how to handle illegitimate emails.

Data Sanitization Tools

File recovery software can retrieve files that are merely deleted from a disk or drive. Companies can use a variety of free and paid tools to clean or purge sensitive data more securely so that the data do not fall into the wrong hands.[50] If all else fails, companies should have a policy of physically destroying hardware that previously housed sensitive material. Most cloud providers will automatically sanitize deleted data, but it is important to check their policies.[51] Furthermore, for cloud services that can be synced to local computers, deleting the cloud copy does not guarantee that the local copy has also been securely deleted. Therefore, companies should avoid syncing highly sensitive data to multiple local hosts if that data may need to be deleted quickly.

48. Simon Liu and David R. Kuhn, "Data Loss Prevention," Institute of Electrical and Electronics Engineers, Volume 12, Issue 2, March 29, 2010, pages 10–13. (https://doi.org/10.1109/MITP.2010.52)
49. J. S. Nightingale, U.S. National Institute of Standards and Technology, "Email Authentication Mechanisms: DMARC, SPF and DKIM," February 16, 2017. (https://www.nist.gov/publications/email-authentication-mechanisms-dmarc-spf-and-dkim); Scott Rose et al., U.S. National Institute of Standards and Technology, "Trustworthy Email," February 26, 2019. (https://doi.org/10.6028/NIST.SP.800-177r1)
50. Richard Kissel et al., U.S. National Institute of Standards and Technology, "Guidelines for Media Sanitization," December 17, 2014. (https://doi.org/10.6028/NIST.SP.800-88r1); "Data Sanitization & Disposal Tools," *Carnegie Mellon University Information Security Office*, accessed June 30, 2021. (http://www.cmu.edu/iso/tools/data-sanitization-tools.html)
51. Kenneth Hartman, "How Azure, AWS, Google Handle Data Destruction in the Cloud," *SearchCloudSecurity*, June 24, 2020. (https://searchcloudsecurity.techtarget.com/feature/How-Azure-AWS-Google-handle-data-destruction-in-the-cloud)

Security Information and Event Management Systems

To properly monitor a network and detect breaches, IT professionals should employ a security and event management (SIEM) system.[52] This software logs activity across the network. Attackers looking for persistent access to a network will often attempt to erase log files because their activity may appear in the log as anomalous activity. Thus, it is important that SIEM systems are configured to mitigate attackers' ability to cover their tracks.[53]

DNS Security

The domain name system (DNS) translates human-readable domain names (such as www.example.com) into computer-friendly numeric addresses (such as 12.345.67.890). Compromising the DNS opens the door to a variety of attacks, from stealing information to impersonating sites to redirecting users to malicious sites. Within an organization, DNS compromises pose a threat to any device connected to both the internet and the internal network.

DNS Security Extensions (DNSSEC), DNS over HTTPS (DOH), and Protected DNS (PDNS) provide enhanced protections against common DNS attacks while browsing the web. DNSSEC uses encryption to ensure that DNS queries are not altered (meaning no one can maliciously redirect traffic unbeknownst to the user).[54] DOH also uses encryption to secure the DNS, but this time to prevent hackers from spying on DNS queries.[55] PDNS works by configuring a policy for detecting malicious IP addresses to prevent users from landing on a malicious site even after the URL has been translated from a human-readable domain into a computer-readable address.[56]

DNS Registrars

Companies with websites need to ensure that users of their sites are not subject to DNS attacks. Normally, companies purchase domain names through a domain name registrar. While purchasing a domain name can be very cheap for some providers, businesses should consider investing in enterprise-level registrars that can guarantee better security. These providers offer more comprehensive protection against misspelled URLs and are better at protecting against common DNS attacks.[57]

52. "What Is Security Information and Event Management (SIEM)?" *McAfee*, accessed June 30, 2021. (https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-siem.html)
53. U.S. National Security Agency, "Hardening SIEM Solutions," October 29, 2019. (https://media.defense.gov/2019/Oct/30/2002203425/-1/-1/0/HARDENING%20SIEM%20SOLUTIONS_20191008-NSAGOV.PDF); Paul Cichonski et al., U.S. National Institute of Standards and Technology, "Computer Security Incident Handling Guide," August 6, 2012. (https://doi.org/10.6028/NIST.SP.800-61r2)
54. "DNSSEC – What Is It and Why Is It Important?" *Internet Corporation for Assigned Names and Numbers*, March 5, 2019. (https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en)
55. U.S. National Security Agency, "Adopting Encrypted DNS in Enterprise Environments," March 4, 2021. (https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF)
56. U.S. National Security Agency, "Selecting a Protective DNS Service," March 4, 2021. (https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_PROTECTIVE%20DNS_UOO117652-21.PDF)
57. UK Government, Central Digital and Data Office and Cabinet Office, "Choose a Good Registrar or DNS Provider," May 5, 2021. (https://www.gov.uk/guidance/choose-a-good-registrar-or-dns-provider)

Secure Socket Layer Certificates

Secure Socket Layer (SSL) certificates enable encryption between a website and the user, making it more difficult for hackers to steal private customer data passed over the web. These certificates also verify a website's identity and ownership to users. In most browsers, sites with SSL certificates have a closed padlock as well as text notifying the user that the site is secure. It is in an SMB's best interest to obtain an SSL certificate so that customers visiting its website do not turn away after receiving a message that the site is not secure. SMBs can obtain an SSL certificate by going through registration and verification by a certificate authority.[58]

Conclusion

SMBs will continue to face constant threats from malicious cyber activity. Meanwhile, the trend toward remote work and digitalization of operations will only further expand the attack space for businesses. However, according to a 2021 survey, only 18 percent of SMBs were confident that they are prepared for a cyberattack.[59] Going forward, efforts to mitigate risk must match the threat. Whether an SMB relies on a managed service provider or conducts its own security efforts, cybersecurity is a critical challenge that requires the attention of the company's senior leadership. Successful cybersecurity requires investments across three lines of effort: people, processes, and technology. The list of solutions above is not all-inclusive, but a cyber hygiene plan rooted in these recommendations stands a greater chance of success in an increasingly risky cyber environment.

58. U.S. CIO Council, "The HTTPS-Only Standard: Certificates," accessed June 30, 2021. (https://https.cio.gov/certificates)
59. "The Urgent Need to Strengthen the Cyber Readiness of Small and Medium-Sized Businesses," *Cyber Readiness Institute*, May 4, 2021. (https://cyberreadinessinstitute.org/resource/biden-whitepaper)

RADM (Ret) Mark Montgomery is the Senior Director of the Center on Cyber and Technology Innovation (CCTI) and a Senior Fellow at the Foundation for Defense of Democracies. **Theo Lebryk** was a CCTI intern during the spring of 2021. FDD is a Washington, DC-based, nonpartisan research institute focusing on national security and foreign policy.