MIS Quarterly Executive

Volume 23 | Issue 4 Article 7

December 2024

Experiences and Lessons Learned at a Small and Medium-Sized Enterprise (SME) Following Two Ransomware Attacks

Donald Wynn, Jr.

W. David Salisbury

Mark Winemiller

MIS Quarterly Executive

Experiences and Lessons Learned at a Small and Medium-Sized Enterprise (SME) Following Two Ransomware Attacks

Because of resource constraints compared to larger corporations facing similar threats, small and medium businesses face unique cybersecurity challenges. We describe the case of a small U.S. manufacturing company that suffered two ransomware attacks. After it had recovered from the first attack, it strengthened its cybersecurity but was still breached again four years later. In addition to highlighting the growing skill and adaptability of attackers, the lessons learned and our resulting recommended actions will help SMEs strengthen their cybersecurity concerns and recover from cyberattacks.[1,2]

Donald Wynn, Jr.
University of Dayton (U.S.)

W. David Salisbury
University of Dayton (U.S.)

Mark Winemiller
World Wide Technology, Inc. (U.S.)

Most Ransomware Attacks Target Small Businesses

Though large corporations receive the lion's share of attention concerning cyberattacks and the importance of cybersecurity preparedness, in the U.S., small businesses with less than 500 employees account for over 99% of businesses, over 46% of private sector employees and 63.3% of net new jobs over the past several years.[3] Like large corporations, small to medium-sized enterprises (SMEs) have increasingly digitalized their processes and interactions with customers, suppliers and other business partners, exposing them to growing sources of cyber threats to their valuable information resources (e.g. personally identifiable information and intellectual property). SMEs, however, often lack the capacity in terms of resources and expertise to implement and maintain adequate technical controls and workforce training to effectively secure their information systems and data. It is therefore not surprising that 63%

1 Stuart Madnick is the senior accepting editor for this article.

2 The authors would like to thank Stuart Madnick and the members of the review team for their excellent feedback and suggestions through the special issue review process.

3 *Facts & Data on Small Business and Entrepreneurship*, Small Business & Entrepreneurship Council, 2023, available at http://sbecouncil.org/about-us/facts-and-data/.

DOI: 10.17705/2msqe.00106

of reported data breaches in 2023,[4] including 82% of ransomware attacks,[5] involved small businesses.

In this article, we consider the various cybersecurity challenges faced by SMEs, illustrated by a case of one that first suffered a ransomware attack in 2017. We describe this attack, its discovery, its impacts, the firm's recovery and changes it made to its cybersecurity as a result of lessons learned from the experience.

This would have been a fairly straightforward story, except that, in 2021, the same firm suffered a second ransomware attack, despite dramatically strengthening its defenses, increasing resources for information security and changing the organizational structure to emphasize the importance of IT security.[6] A review of the second attack (in particular, given improvements to the firm's cybersecurity after the first) is instructive because it reflects the change in the "state of the art" of ransomware attacks over a four-year period.

We discuss both attacks, how they were different from each other, how the company changed between the first and second attacks and the implications for the company, and identify the lessons learned from both experiences. We then provide recommended actions for SMEs (which may be challenged by limited resources) to address the threats to information and system security, which can enable them to gain a better grip on securing their online information assets.

Cybersecurity Challenges Faced by Small Business

Like any business, SMEs need to protect their valuable information assets. The three key aspects of information protection are confidentiality, integrity and availability,[7] commonly referred to as the "CIA triad." *Confidentiality* means that information (especially sensitive information) should not be disclosed or available to unauthorized persons or processes. *Integrity* means that throughout its life cycle, information should be kept consistent, trustworthy and accurate. *Availability* means that the people who need to see the information should be able to access it whenever they need it to do their jobs.[8]

Like their larger counterparts, more and more of SMEs' valuable information is available online in systems that have known (and some unknown) vulnerabilities, with threat agents seeking to capture, alter or deny access to this information. A key challenge for a small business is that the range of threats isn't smaller because the firm is smaller.

SMEs obviously need cybersecurity controls. Basic technical controls include anti-malware, firewalls and so forth. Deciding which controls are necessary can be challenging for SMEs because keeping up to date with the latest and greatest is rather like an arms race in which one must keep ahead of current and emergent threats to information resources. Procedural controls (e.g., rules and training) can also be helpful, but they require making time for training, which can also strain the more limited resources of SMEs.

The NIST Cybersecurity Framework, or CSF (V2.0),[9] outlines six interrelated core functions that should be present in any cybersecurity program:

4 *2023 Data Breach Investigations Report*, Verizon, 2023, available at https://www.verizon.com/business/en-gb/resources/2023-data-breach-investigations-report-dbir.pdf. Verizon gathers data from a variety of sources and analyzes it to identify patterns of attack vectors prevalent in data breaches. In this 2023 report, there were a total of 608 incidents with confirmed data disclosure, of which 63% were in small and medium enterprises (1,000 employees or less) and the remainder in larger firms.

5 Drapkin, A. *82% of Ransomware Attacks Target Small Businesses*, Report Reveals, Tech.co, February 7, 2022, available at https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals.

6 At the time of the attacks, one of the authors of this article was IS Director then VP of IS (and later of Marketing as well) at Gosiger, the case study company.

7 *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard, National Institute of Standards and Technology, February 2024, available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

8 The CIA triad is a common model that forms the basis for the development of security systems. The confidentiality, integrity and availability aspects are used for finding vulnerabilities and methods for creating solutions. Other cybersecurity models could be applied along with the CIA model, including: 1) the DIE model (see Heller, M. *Experts Say CIA Security Triad Needs a DIE Model Upgrade*, March 24, 2022, available at https://www.techtarget.com/searchsecurity/feature/Experts-say-CIA-security-triad-needs-a-DIE-model-upgrade); and 2 the Parkerian Hexad (see Turab, N. and Kharma, Q. "Secure Medical Internet of Things Framework Based on Parkerian Hexad Model," *International Journal of Advanced Computer Science and Applications* (10:6), January 2019, pp. 54-62.

9 *The NIST Cybersecurity Framework (CSF) 2.0*, National Institute of Standards and Technology, February 26, 2024, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. NIST 2.0 was released very close to the time that the initial version of this article was submitted for review; it added a sixth function, Govern, and included some updates to the other five core functions.

1. *Govern:* Organizational cybersecurity risk management strategy expectations, and policy are established, communicated and monitored
2. *Identify:* The organization's current cybersecurity risks are understood
3. *Protect:* Safeguards to manage the organization's cybersecurity risks are used
4. *Detect:* Possible cybersecurity attacks and compromises are found and analyzed
5. *Respond:* Actions regarding a detected cybersecurity event are taken
6. *Recover:* Assets and operations affected by a cybersecurity incident are restored.

The governance, identification and protection of an organization's online assets implies that the controls in place to protect information should be commensurate with the impact that would be experienced should a breach occur. This is why categorizing the likely impact of a breach is important; the more valuable and sensitive the information, the more rigorous the controls should be; conversely, information that is less sensitive or valuable does not merit the expense of highly rigorous (and expensive) security controls.

Compared to larger firms with more resources, one challenge faced by SMEs is a lack of comprehensive understanding of their threat environment. Small enterprises lack the resources to fully address *every* domain in which they operate, and implementing a full information governance program requires both expertise and commitment, which must compete for time with trying to attract and service customers, operate the payroll and other reasonable concerns. However, the threats are real and are becoming ever more significant as time passes.

Before describing the information security controls the case study firm had in place at the time of the first breach, we first provide a brief primer on ransomware and background information on the firm. We then describe what happened during and after the first attack, which took down critical systems that were unavailable to legitimate users for nearly two weeks. Next, we highlight the changes that were implemented as a result of the first attack, before discussing the second attack and the actions taken after it.

A Ransomware Primer

Ransomware is defined as "malicious software that allows a hacker to restrict access to an individual's or company's vital information in some way and then demand some form of payment to lift the restriction."[10] A ransomware attack often involves the encryption of vital data, which is then held for ransom, with payment usually required in the form of Bitcoin, primarily because it's fast, reliable, verifiable and hard to trace.[11] The ransomware may be distributed either by mass mailings (i.e., phishing emails) or it may be targeted. Modern encryption algorithms make it nearly impossible for ransomware victims to decrypt their files, so the choices are basically to pay the ransom, rebuild and restore systems from scratch or do without the encrypted data.

Ransomware is not new. The first example occurred in 1989 and involved code distribution largely via floppy disk with a ransom of $189 to be sent to Panama.[12] Though there are a variety of so-called "ransomware business models,"[13] nearly all of them involve certain key elements. One is the distribution of, infection by and execution of the ransomware, resulting in the target system's critical files being encrypted. In the case study firm, the first attack appeared to have come from Iran; the second from Russia. As discussed below, dealing with foreign entities complicates matters further.

Because of the difficulty of purchasing Bitcoin, an industry has emerged consisting of consulting firms that have large caches of Bitcoin, which they will sell and use on behalf of the ransomware

10 Brewer, R. "Ransomware Attacks: Detection, Prevention and Cure," *Network Security* (2016:9), September 2016, pp. 5-9.

11 Agrawal, N. *Why Ransomware Criminals Use Bitcoin and Why That Could Be Their Undoing*, May 16, 2017, Coin Center, available at https://coincenter.org/link/why-ransomware-criminals-use-bitcoin-and-why-that-could-be-their-undoing.

12 See: 1) Ismail, N. *The Ransomware Business Model. Information Age*, April 11, 2017, available at http://www.information-age.com/ransomware-business-model-123465658/; and 2) *AIDS Trojan or PC Cyborg Ransomware*, KnowBe4, Inc., 2024, available at https://www.knowbe4.com/aids-trojan.

13 For examples of ransomware business models, see: 1) *Threat Research Report: The Anatomy of a Ransomware Attack*, Exabeam, 2016, available at https://docs.media.bitpipe.com/io_13x/io_131500/item_1334136/Exabeam_Ransomware_Threat_Report_Final.pdf; 2) Bartle, B. *Three Phases of a Ransomware Attack*, Techspective, May 8, 2017, available at https://techspective.net/2017/05/08/three-phases-ransomware-attack/; 3) Ismail, N., op. cit., April 11, 2017; and 4) *The 2024 Ransomware Threat Landscape*, Symantec Enterprise Blog, January 2024, available at https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf.

victim to pay the ransom if desired. Moreover, demanding payment in Bitcoin has likely had some impact on the market price of Bitcoin itself, if for no other reason than increased awareness.[14] In terms of supply and demand, it only stands to reason that increasing numbers of successful ransomware attacks would make the demand for a difficult-to-trace currency exchangeable online increase. For example, the emergence of significant Windows XP ransomware breaches (e.g., the "WannaCry" attack) that occurred in the summer of 2017 coincided with an increase in Bitcoin prices.[15]

Sadly, but predictably, ransomware attacks have become more sophisticated over time.[16] Once potential victims started to put in protections to keep their data safe from being encrypted (enabling them to simply rebuild systems), ransomware attackers moved from simply extorting firms by encrypting their data to first downloading it and threatening to release it publicly if the target didn't pay the ransom—the so-called double-extortion attack. The University of Utah was an early high-profile victim of this sort of attack. Though it had sufficient backup and recovery facilities to recover the data, the attackers had copied the data (including student data protected by FERPA [Family Educational Rights and Privacy Act]) forcing the university to pay the ransom to avoid its release.[17]

It gets worse. Ransomware attackers are now, in some instances, deploying so-called triple-extortion attacks. In addition to exfiltrating the data, encrypting it and threatening to release it, the triple-extortion model threatens *the individuals about whom data is stored*, promising to release *their data* if they don't pay. The first triple-extortion attack was at a Finnish psychotherapy clinic in 2020, with its patients being threatened that data about their treatments would be released if they didn't pay the ransom.[18]

The next evolution of ransomware is the quadruple-extortion attack, which involves distributed denial-of-service (DDoS) attacks against public-facing servers at the target organization unless a ransom is paid. Thankfully, these are still somewhat rare.

Case Study Firm Background and Its Pre-Attack Approach to Cybersecurity

Gosiger is a family-owned machine tool distributor and manufacturer headquartered in Dayton, Ohio. By the time our story begins it had been in business for over 90 years, and is by any measure a typical successful enterprise in its domain, with 13 U.S. locations, just under 500 employees and roughly $400 million in annual revenues. It specializes in technical metal working machines and manufacturing automation, and provides sales, service and engineering expertise to customers.

Because of the firm's history and industry focus, many Gosiger executives originally viewed computers as a convenience rather than a necessity. As such, it was sometimes difficult to procure funding to advance the IT capabilities of the firm. This included funding for cybersecurity efforts, despite Gosiger's increasing reliance on interconnected technologies across the firm.

At the time of the first attack, as well as the IS director, there were just five IT personnel who were perhaps somewhat more sophisticated than is typical in this industry space. Two worked on the help desk, two were assigned to assist with various specific applications, and there was a systems administrator.

Gosiger's IS director was tasked with maintaining the operation and security of various systems and networks while also sustaining significant levels of accessibility and ease of use for members of the organization to do their jobs. His repeated pleas to corporate leadership that ease of use (which the leadership required)

14 See Jenkinson, G. *Fearing Ransomware Attacks, Companies Preemptively Buying Bitcoin*. Cointelegraph, December 20, 2017, available at https://cointelegraph.com/news/fearing-ransomware-attacks-companies-preemptively-buying-bitcoin. For a detailed report about ransomware, see *The 2024 Ransomware Threat Landscape*, op. cit., January 24, 2024.

15 Fung, B. "What you need to know about bitcoin after the WannaCry ransomware attack," *Washington Post*, May 15, 2017, available at https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/?utm_term=.dfe797583665.

16 For more information, see *The Rise of Quadruple Extortion Ransomware and How to Protect against It*, Acronis, March 31, 2023, available at https://www.acronis.com/en-us/blog/posts/quadruple-extortion-ransomware/.

17 Cimpanu, C. *University of Utah Pays $457,000 to Ransomware Gang*, ZDNet, August 20. 2020, available at https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/.

18 Ralston, W. *They Told Their Therapists Everything*. Hackers Leaked It All, WIRED, June 2021, available at https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/.

and more effective security (a growing concern for the IS director) were at times in opposition went unheeded. Decisions concerning system configuration routinely prioritized ease of use over security. This conundrum came as no surprise to the IS director. It is not uncommon for enhanced security controls to make accessibility and ease of use more complicated. Resolving this conundrum on a limited budget is a massive challenge. Moreover, the firm was not fully convinced prior to the first breach that it was an attractive target for hackers, making the "sell" for costly security measures even more challenging. In the words of the IS director: "The general opinion of the most senior leaders of Gosiger was that the firm was not in the financial industry and therefore would not be a target of would-be hackers." Management simply didn't see the threat at that time; the firm believed in "security by obscurity" (because it was small in size and not working with financial data), which probably contributed to it not being fully prepared for what was about to hit.

The First Ransomware Attack

Detection of the Attack

Detection of the first ransomware attack occurred late one evening in the spring of 2017. The IS director was contacted at home by the systems administrator because employees could not access one of the organization's servers. However, there were numerous scripts running on the server that weren't being run by Gosiger employees. Further examination revealed that most of the other servers in the firm had been affected by some sort of ransomware; encrypted files and a ransom note were found on each machine.

With a dearth of insight about the attack, when the systems administrator found the ransom note on his computer, he believed his machine was the point of entry. This fear caused substantial panic on his part; indeed, on several occasions, the IS director had to sternly instruct him to calm down—though, in fairness, he was not the only one in the firm to panic over the next few days. "At this point, we had no choice but to try to figure out what was happening, and freaking out didn't help at all" (IS director, Gosiger).

The attack employed the ransomware package SamSam (aka Samas), which is believed to have been written by Iranian hackers. SamSam is designed as a targeted ransomware attack that is deployed manually, as opposed to ransomware that is automatically distributed.[19] This means that at its core, it is a targeted attack. Hence, Gosiger's conviction that it was not an attractive target was unfounded, though the specific reason for this targeting (aside from the ransom itself) was unclear. At that time, the "business model" for those using SamSam tended to be a targeted attack. After gaining remote access, the attackers often deployed shell scripts (e.g., perhaps to change file modification date information to make it difficult to identify files that have been changed), connect via a remote desktop protocol and then run batch scripts to deploy the payload to various machines.

The specific vector[20] for a typical SamSam attack (such as that in the Gosiger case) compromises a server, either by entering via some exploit or other means of directly accessing the server. With this sort of access, directory information is collected, after which a list is built and targets tested for access. Resources targeted successfully are added to the target list, after which public and private keys are deployed. Processes with locked files are killed and backups are sought. Psexec.exe (part of the Microsoft-owned Windows Sysinternals package) is used to encrypt files with the RSA 2048 encryption, after which all files are deleted and the private keys removed.

During this attack, the primary attack vector was existing and online machines, with several hundred individually attacked. Gosiger was able to determine that the threat agent gained access to a domain controller, but was not able to determine how it entered its IT environment. At that time, the firm had no partnership with a threat response team, so remediation consisted primarily of simply getting everything running again. Gosiger also lacked sophistication from a

19 SamSam and how it works is described in Ragan, S. *SamSam Explained: Everything You Need to Know about This Opportunistic Group of Threat Actors*, CSO Online, April 18, 2028, available at https://www.csoonline.com/article/564908/samsam-explained-every-thing-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html.

20 In cybersecurity, an "attack vector" is the path or means a hacker uses to gain access to a computer or network in order to bring about some malicious outcome.

security or logging standpoint, which limited the ability to make comparisons or identify when and where malicious traffic appeared. With no ability to review logs, the company determined it would be time- and cost-prohibitive to determine the point of entry in any great detail. However, the method of attack and artifacts were all identified.

While there was some evidence of script execution on a customer relationship management (CRM) server, there was no evidence that this was the initial point of compromise, which would be consistent with removing traces to limit the effectiveness of forensic analysis. The point of entry may have been some unpatched servers or an internal user PC. The attackers were able to gain administrative privileges through brute force attacks, with the script to launch the attack written into the system directories of over 200 local machines. Curiously (though thankfully), shared drives were not attacked because universal naming convention (UNC) pathed shares were ignored. (UNC is a standard for naming resources on a local area network that are shared by computers.)

Gosiger identified several artifacts that proved the attack was SamSam. The first was a script called "Test.txt" that ran on a machine and returned a result of "OK" if it was successfully able to write to a system-secured directory. Second were the more problematic files, including Psexec.exe, which permits the remote launch of applications, including the ransomware binary files (i.e., Samsam.exe). Third, public keys were found, along with encrypted files. Fourth, there was a ransom note in the file LET-ME-TRY-DEC-FILES.html that was left behind in every directory where encryption had taken place. This note specified what the ransom would be, how to purchase Bitcoin, how to pay the ransom, and a threat of access being denied forever by removal of the keys if the Bitcoin was not paid in seven days. After that time, the private encryption keys would be destroyed. The ransom was 1.7 Bitcoin for each key, or 28 Bitcoin to get all of the keys.

Response to and Recovery from the First Attack

The first response was initiated very shortly after the attack was detected: unaffected systems were shut down to limit the spread of the damage. The local police department and the FBI were made aware of the attack. Though helpful, the police and FBI are really only useful in going after the attackers and in collecting threat intelligence to help others evade future attacks. Management pondered whether to pay the ransom. Gosiger also considered whether to hire one of the several consulting firms that could help by acquiring the required Bitcoin needed to pay the ransom, coordinating recovery with the attackers and decrypting the data. After much debate and risk analysis, this course of action was rejected as the damage had been done, and the IS director believed that the attackers were no longer in the IT environment. Instead, the firm now embarked on the process of recovery in earnest.

After being informed of the attack, the CEO was bewildered: "How did this happen? How were we targeted? What can we do?" Everyone was out of their comfort zones, and the firm was literally unable to conduct business for a few days. The IS director called all five members of the IT group into the firm's headquarters to assist with recovery efforts.

The primary phase of the recovery began by contacting several incident response vendors, the most useful of which turned out to be AT&T Incident Response. Its experts were sent a user virtual machine (VM) and a VM server for analysis. AT&T's expertise turned out to be quite helpful. Indeed, much of the forensics that identified artifacts and provided a more detailed timeline of the attack was done by AT&T.

Conference rooms became makeshift IT labs. End user computers were reimaged and redeployed as rapidly as possible. The help desk staff largely carried out these tasks and were even helped by employees having nothing to do with the IT team. Meanwhile, the IS director and systems administrator set about rebuilding and restoring all of the servers. Terabytes of data had been encrypted. Backups, stored locally on various servers were identified by the attack and had been deleted. Large databases had been entirely encrypted. Domain controllers were rendered unusable and, in most cases, would not reboot successfully. The entire infrastructure had to either be restored or rebuilt.

At the time of the first attack, Gosiger's disaster recovery process was to own multiple identical storage area networks (SANs) and take

snapshots of logical unit numbers,[21] replicating them to the off-site SAN. This meant that in most instances, a clean version of either the data, the server or both was available for recovery. However, while the data structure was large enough to allow the restoration of a partial failure (that of a few systems) it was not adequate to perform a full restoration of all systems simultaneously, which meant that the IS director had to quickly acquire additional SAN drive shelves.

The recovery involved long days. The attack occurred late on a Tuesday evening and by Thursday, when all IT staff members were on site, their working hours stretched from 5 a.m. to midnight. One exception was when the IS director was able to acquire and bring online the SAN drive shelves. For him and some of his staff members, this day ended at nearly 3 a.m.

Slowly, systems were restored and systems functionality returned. Domain controllers allowed users to log into the network and begin to access local data repositories (which were miraculously untouched by the attack). The ERP system was restored, followed by the customer relationship management and customer service databases being returned to functional states, albeit with some data loss. Mail servers were recovered and, with the help of several consultants, all utility servers were returned to their former functional state. It took 12 days and 580 IT-person hours to reach this point.

The cyber response team was relatively small. One on-site engineer worked to ensure that the attackers were gone from the network and then determined what weaknesses or failed processes were exploited. Two remote engineers reconstructed the virtual server machines to determine if any "time-released" threats remained and dug into the source of the breach. Two additional remote engineers were tasked with executing intrusion testing to determine if there were other weaknesses that could still be identified.

Several pre-attack security weaknesses were discovered. Whitelisting[22] of server software was not in place, allowing nearly any program to be executed by anyone with access. However, in the pre-attack environment, the method of execution was Psexec.exe, a Winternals product that the IT staff found useful for many routine tasks, and it would have likely been included in any whitelist. No central or automated log analysis was in use, allowing server logs to hold critical data about potential issues that were not being captured. The domain administrator account was allowed to have remote desktop protocol (RDP) login access, making a login hack of the servers that much easier because the username was already known.

There were three possibilities for the initial point of entry. The first was that an external user's computer had been compromised and then introduced to Gosiger's network. The second was that a user had received a phishing email or visited a malware-infected website that allowed an attacker to have access to the user's PC, ultimately giving the attacker local access. The third possibility was an exploit of an operating system bug that allowed a user to acquire access through the network address translation[23] of forward-facing ports on servers. Given the cost of the cyber response team and the relatively small number of possibilities, Gosiger decided to mitigate all three rather than spend considerable engineering hours on determining the precise cause.

Counting the Cost of the First Attack

Gosiger came to view this attack as a learning experience, albeit a painful and expensive one. Direct tangible cost for AT&T's efforts was roughly $48,000 for multiple network engineers, both on- and off-site. Other costs included rebuilding a customer relationship management system (about $5,000) and a service database ($20,000, due to lost customizations). However, these systems took substantial time to recover and redeploy, making the "soft" cost substantially greater. In addition, the targeted user computers and the majority of user virtual machines were reimaged.

21 A storage area network is a computer network that allows servers to access data storage devices, such as tape libraries and disk arrays, as if they were directly attached to the server. A logical unit number is a unique identifier for a storage partition in a storage area network.

22 Whitelisting is the process of securing a device or network by allowing trusted IP addresses, software or emails to access it.

23 Network address translation is a service that enables private IP networks to use the internet and cloud.

Other less direct costs included approximately 580 person-hours of work spent on remediation in the first 12 days after the attack (full recovery took a few months), and loss of functionality over a period of about a week (email, ERP, other minor systems). In sum, the data loss was comparatively minimal, but the recovery cost was significant.

Lessons Learned from the First Attack and Resulting Cybersecurity Improvements

After the first ransomware attack, several cybersecurity weaknesses were identified, including those involving local user accounts and their permissions. This attack didn't leverage these weaknesses, but fixing them would help mitigate future attacks.

The lack of whitelisting was addressed by implementing a product on servers for executables. The lack of centralized logging was also addressed. Antivirus was in place but was not relevant for stopping this particular attack. Another point of weakness involved the server domain administrator accounts. These accounts tend to be susceptible to brute force attacks and are a plausible candidate for the entry point. In retrospect, allowing the remote desktop protocol to remain as a permitted user was an unwise choice. Because Gosiger saw the risk to the networks as minimal, intrusion testing was not a priority, nor was traffic analysis or blocking IP addresses by geolocation, all of which were implemented after this first ransomware attack.

Like many small businesses, Gosiger had limited funding and other resources for cybersecurity initiatives. The small number of IT staff focused mainly on keeping things running rather than defending against attacks. Storage available for backups was acceptable for daily operations and an occasional outage, but the backups proved to be inadequate for rebuilding, restoring and redeploying all systems simultaneously.

However, the lessons learned from the first ransomware attack did lead to better preparation for preventing future attacks. This incident empowered the IS director to ask for things that previously would not have been feasible for systems that were not seen as viable targets by management. More complex passwords and routine password changes were mandated. Administrator privileges were removed from local machines that did not need this. On the server side, the domain administrator access via the remote desktop protocol was eliminated, and the firm adopted automatic updating of patches. It also implemented central logging along with analysis of the logs. Default port numbers were changed. Firewalls were replaced with far more capable next-generation firewalls, automatic local sandboxing of unknown files for testing was adopted, and network sniffing and packet analysis were put in place for all core devices. Though none of these features would offer absolute security, it did make the systems a harder target.

The firm also made significant changes to processes related to external networking. It implemented regular intrusion testing, in combination with an annual security audit performed by a reputable penetration tester. It also deployed software for network analysis and threat detection, along with firewall tools able to block IP addresses by location. In terms of personnel, Gosiger now employed several vendor-certified network security experts. Other newly acquired resources included access to on-demand consulting, and an incident response team was put on retainer.

However, the most significant change was the mindset of the firm's leadership, which enabled everything else. The IS director was charged with ensuring that something like this never happened again. Every aspect of cybersecurity was placed under scrutiny, and the firm was willing to spend the necessary dollars on any corrective and preventative action. After the first ransomware attack, the IS director no longer had to explain how dangerous and extraordinarily disruptive cybersecurity breaches could be, even at firms in this particular industry. Everyone remembered. The IS director was promoted to vice president of IS (VP/IS hereafter), and later to vice president of IS and Marketing, with significant increases in both funding and staffing dedicated to protecting the firm's information assets.

> *"Every portion of the firm's cybersecurity was under scrutiny and the firm was willing to spend necessary dollars on any corrective action to ensure this event was not repeated. Finding cybersecurity dollars was no longer difficult, as everyone now*

knew we were clearly a target. Everyone is a target." (VP/IS, Gosiger)

The Second Ransomware Attack

Sadly, despite the significant effort that Gosiger put in to strengthen its defenses, it was successfully attacked again in Spring 2021. The attacker this time was an affiliate of REvil (also known as Sodinokibi), which is a malware developer that employs a Ransomware as a Service (RaaS) model. With this model, REvil contracts to provide its software to affiliates, who select the targets and execute the attacks, in exchange for a share of the takings.[24] Though its origin is somewhat murky, REvil is believed to have originated in Russia, a belief supported by the fact that it didn't tend to launch attacks against Russian organizations.[25]

Detection of the Second Attack

On the morning of the second attack, the VP/IS was unable to connect to the company's Outlook server on his phone. At this time, his home was actually an extension of the Gosiger network via a permanent internet protocol security virtual private network (IPsec VPN,) so he sat down at his home machine and attempted to ping the Microsoft Exchange server from there, receiving no reply. As this server was a virtual machine, he attempted to log into VMWare's vCenter server to see the status of the server. He discovered that every VM in the environment was in a powered-off state. He then attempted to power up a VM but received a datastore error message. By now, convinced something was amiss, he alerted his technical staff and hurried to the office.

The VP/IS and his staff confirmed that the VMs were still in the powered-off state and all data stores in the environment were showing either with errors or as file not found. He attempted to log into the ESX servers via Secure Shell (SSH)[26] but neither his credentials nor the administrator credentials would work. He reached out to his most senior technical employee, who was able to find a machine on the network and started looking through local storage, where he found encrypted files and a ransom note. These artifacts confirmed there had been an attack by an, as yet, unknown attacker.

Analyzing and Recovering from the Second Attack

The VP/IS called the CEO and shared his discovery of another attack on the Gosiger IT environment. The CEO instructed him to advise the chief financial officer and ask him to initiate a conversation with the insurance company (Traveler's). The VP/IS also called a few partners with whom he had built rapport after the first attack. One of them suggested that he call the Dayton police as well as the Secret Service. The Dayton police took a report, but without the technical resources needed to perform an advanced forensic investigation they were unable to offer much assistance.

The Secret Service sent an agent to Gosiger's office, and, again, one of the conference rooms was turned into a war room. The agent asked a lot of questions and asked for mirror images of a few affected drives to take back to the Secret Service lab. (The Secret Service has a specialized group that tracks threat agents and their attack methods.)

In the war room, there was a conference call including the CEO, president, chief financial officer, systems administrator, the VP/IS, an agent and another representative from the insurance company, a breach coach and a few employees from Arete, an incident response (IR) company. After introductions, the IR team asked that SentinelOne, an end-point detection and response package, be installed on every machine on the network to ensure that the threat agent was no longer in the environment.

During the conference call, the systems administrator received a text message from an employee in Pittsburgh. The message included

24 Fokker, J. *McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service—The All-Stars*, McAfee.com, October 2, 2019, available at https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/.

25 Saarinen, J. *No Let Up on REvil Ransomware-as-a-Service Attacks*, itNews, January 29, 2020, available at https://www.itnews.com.au/news/no-let-up-on-revil-ransomware-as-a-service-attacks-537189.

26 VMware's ESX Server, now known as ESXi, is a virtualization tool that allows users to create multiple virtual machines on a single physical server; SSH is a network protocol that allows users to securely access and manage remote computers and devices over an unsecured network.

a screenshot of an email that said: "We are the group that infected your corporate network." As the VP/IS explained, "This user received this email in her personal yahoo.com email [account]. At this point, we at least had heavy suspicion of the origin of the attack."

The IT staff began restoring the environment from the backups as per the disaster recovery plan. This was a complex and long endeavor, given that 10 terabytes of data needed to be restored and much of the email services and other infrastructure had to be moved to the cloud. While the restoration process was ongoing, the VP/IS was able to reset the passwords to access the console of the vCenter Server and all eight ESX hypervisor servers. He then began exploring the various datastores that were accessible. Every directory contained ransom notes and files that had obviously been affected.

Encrypted files had their file names changed, with a randomly generated set of characters inserted as a prefix to the file name. Every time the datastore was encrypted new random characters were added to the file name. This was the first time the VP/IS had heard of a file being encrypted more than once and the first time he had ever heard of ESX servers being encrypted. Because of the vCenter setup and vMotion,[27] all the servers had access to all datastores. So, when Sodinokibi was executed on each ESX server it encrypted every datastore it could access. This meant that, for all eight ESX servers, there were eight Sodinokibi executions and eight encryptions on each file.

For an external application to execute on ESX servers, it must be designed specifically for ESX. One cannot, for example, install Apache on an ESX server and then run a web server; it simply will not work. The threat agent in this attack built the encryption tool (Sodinokibi) specifically to run on ESX servers. That, along with the speed with which this application could render a file useless, was very impressive from a technical standpoint. As the VP/IS exclaimed, "I was blown away by the technical prowess and speed that this would require."

The IR team agreed to a minimum of two meetings daily to create a strategy and provide any necessary updates. During the second meeting, it was revealed that the attacking group was REvil (REvix). The IR team followed instructions from the ransom note to reach the threat agent on the dark web and found a "shaming site"[28] that announced who the threat agent was and had a screenshot of a corporate directory structure showing that it had exfiltrated data from several sensitive repositories, including finance, HR, marketing, engineering and automation.

Interestingly, the shaming site had a link that allowed the IR team to assume the identity of Gosiger and communicate with the attacker, essentially via an encrypted chat window. During these communications, the attacker made the first ransom demand of $1.7 million, to be paid in Bitcoin.

The next step for the VP/IS was to carry out a forensic analysis of known attacked computers. The technical staff chose an affected domain controller and the suspected PC (from Pittsburgh) and had an employee drive this PC to Dayton from the Pittsburgh office. Using forensic software, the technical staff created compressed archives and sent them to the IR team. The next day, the war room meeting included full technical details of the attack.

The threat agent had reached out to the employee's personal email account with a spear phish having an attachment containing Cobalt Strike, which is a beacon software that will open a tunnel that allows anyone to get remote control of a device where the beacon is installed. Once the threat agent was on the targeted device, the agent was able to see that there were cached credentials on this computer from someone working at the help desk holding administrative privileges. From here, the agent began to laterally move throughout the network. The network was not micro-segmented at the time and the threat agent was easily able to get to the Dayton data center from the Pittsburgh office using the acquired credentials. From there, the agent set up a beacon on the data center and began reconnaissance of the environment.

The threat agent continued this reconnaissance for exactly one month. During this time, the agent examined the available file shares in the environment and exfiltrated valuable data

27 VMware's vMotion technology enables the live migration of virtual machines from one physical server to another without downtime.

28 This shaming site was created on the dark web, and a couple of days later it was reported via hacknotice.com.

for a double-extortion play—even if Gosiger was able to rebuild easily without a decryption key and didn't pay the ransom, this sensitive data could simply be released. After a month, the threat agent executed Sodinokibi on the ESX servers as well as a few available computers on the network. In the previous attack, massive numbers of client machines were encrypted. In this attack, no more than 30 physical computers were affected and the VMs were not affected directly but their datastores were. No shared user or group data was encrypted. Clearly, the method of this attack was broader and more sweeping than the original attack with SamSam.

While these investigations into how the attack happened were ongoing, the IT environment was slowly being brought back online. The VP/IS and technical staff moved services to the cloud where they could and installed the SentinelOne package on all endpoints. All systems were restored within a couple of weeks except for archived email, which involved terabytes of data.

The next task for Gosiger was to work with the IR team and breach coaches to determine what to do about the stolen data. The firm had a responsibility to keep employee information and other sensitive data confidential. It decided to purchase identity theft protection for its employees. Two-year coverage was quoted by LifeLock, costing several thousand dollars:

> *"We had a responsibility to keep our employee information confidential. The data that was taken from the HR share contained not only sensitive information about employees (past and present) but also their mates and dependents. The threat agent was threatening to sell this information on the dark web if we did not pay the ransom."* (VP/IS, Gosiger)

The Arete team continued to negotiate prices with the threat agent for both the decryption application and the destruction of data. Because the attacker did not speak English natively, communication was broken and very unsophisticated. The negotiation team began making offers. The threat agent first asked for $1.7 million. Arete countered with an offer of $4,000. The negotiations progressed through several rounds. On more than one occasion, the threat agent indicated that "the offer has to be taken to my boss," suggesting that there was also a negotiation going on between the developer of Sodinokibi and the affiliate. This continued for a few days until an agreement was reached to pay approximately $225,000 in Bitcoin, which was acceptable to both Gosiger and the insurance company.

The Bitcoin payment was fully handled by Arete once authorization from the U.S. Office of Foreign Assets Control was obtained. This is a critical step for legal compliance because of U.S. law mandating that funds cannot be transferred to terrorist organizations. Once payment was made, Gosiger received two things from the attacker. The first was the decryption software, which was built to run on a Windows machine that needed a shared connection to an ESX server. Once installed, it would find encrypted files and decrypt them. The second was an ASCII document that contained the attacker's "recommendations for security hardening." The threat agent provided recommendations for avoiding this type of ransomware attack in the future, as if this were a service the attacker was selling. This "service" is basically a "protection racket," where criminal groups threaten legitimate businesses if they don't make their "insurance payments." The contents of this document were not particularly insightful and contained suggestions such as "all administrators should browse in incognito mode." It also mentioned the training of users and "punishing with money" should anyone click on an unknown attachment, which was how the second ransomware attack began.

Further Strengthening of Cybersecurity in the Light of the Second Attack

> *"After payment, delivery of artifact, and execution of the agreement with Arete, we disengaged the IR team and began designing the next version of security in the environment that would include micro-segmentation and ZTNA (Zero-Trust Network Access)."* (VP/IS, Gosiger)

Though the second attack was successful, the good news is that, compared to the first attack, Gosiger was in a far better position to respond because of the steps it had taken after the first attack to strengthen its defenses in depth and implement traffic logging. This meant

Table 1: Summary of Attacks

	First Attack	Second Attack
Year	2017	2021
Threat Actor	Unknown	REvil
Threat Software	SamSam	Sodinokibi
Technical Level	Crude	Complex
Hardware Target	Network hosts	Hypervisors
Encryption Speed	Slow	Instant
Hosts Impacted	200+	30
Ransom Demand	28 Bitcoin (~$200 thousand)	$1.7 million
Ransom Paid	$0	$225 thousand
Third Parties Involved	Local police, FBI, AT&T	Local police, Secret Service, insurance company, incident response company, US Office of Foreign Assets Control
Full Recovery Time	1 Month	1 Month

it could identify the point of entry of the second attack and the type of attack. It was also able to determine that the threat agent carried out reconnaissance for a month before launching the attack and that the hackers' primary target was the VMWare ESX server datastores. Knowing how the attack was launched and how it progressed made recovery and restoration a little easier. Overall, the second attack was not nearly as disruptive as the first one, owing to the dramatically improved cybersecurity measures implemented after the first attack.

After the second attack, Gosiger further enhanced its cybersecurity. Specifically, it now has mandated credential expiration and complexity requirements, managed event detection and response on all endpoints, multi-factor authentication, and security information and event management (SIEM) software, and has adopted the zero-trust model, coupled with micro-network segmentation. Several of these enhancements were mandated by the insurance company that wrote the cybersecurity policy for the firm, including upgrades and enhancements that had been identified as future goals. For example, the firm is now required to hire consultants to perform penetration testing services. Gosiger also hired a third party to assist with migrating email services from the internal servers to a managed Microsoft solution, which would have been difficult for the IT staff to undertake due to staffing and resource constraints.

All in all, these changes increased the IT budget by approximately 30% in both upfront and recurring annual licensing. It is important to note that these changes (and their cost) were essential for even a relatively small firm to be able to defend itself against the increasing threats of cyberattacks. The arms race continues.

Summary of the Two Ransomware Attacks

Table 1 provides a summary of the 2017 and 2021 ransomware attacks on Gosiger.

Lessons from the Case Firm's Experiences

Within the cybersecurity field, learning is an ongoing process. Moreover, the two ransomware attacks show a significant evolution of hackers' methods and sophistication over the four years between the attacks. This is important information for SMEs because it shows just how

complex the hacker ecosystem has become and how sophisticated those involved in hacking organizations now are. In the cybersecurity arms race, SMEs need to know as much as possible about how threat agents "play the game."

The first attack was crude, slow, inefficient and only partially effective. The second attack was novel, complex, fast, cunning and purposeful, and required in-depth enterprise architecture knowledge. We set out below the general lessons learned from both attacks. These lessons will help other SMEs to strengthen their cybersecurity and respond effectively in the event of a breach.

Lesson 1. Everybody is a Target

Placing business processes and information resources on internet-linked devices means that they are potential legitimate targets, either by targeted attacks or by deployment of various forms of malware that cast a wide net. Coupled with the interconnectedness of the global economy, the presence of significant information resources online means that organizations must protect vital systems against cyberattacks. Though Gosiger was perhaps better prepared than most organizations of its size and industry, it was targeted. Its belief in "security by obscurity" was misplaced. If you're online, you're a target. Everyone is now a target, so SMEs should prepare for the inevitability of a successful attack: "It's not if you get breached, it's when you get breached, so get prepared" (VP/IS, Gosiger).

Lesson 2. Backups Must Include Everything

From the first attack. Gosiger discovered that, though the backups it had in place adequately covered the *data* on its systems, they did not include the *software* or *systems configurations*. By the time the second attack occurred, this gap had been filled, making recovery easier. But there must be a balance between the cost of prevention (e.g., additional backups and data storage costs) and the cost of recovering the various assets in the event of an attack. SMEs must carefully address this balance in their ongoing disaster recovery planning.

Lesson 3. The Importance of Adequate IT Staffing Levels

Despite having a small number of IT personnel and despite dealing with an issue that simply wasn't on their radar before the first attack, Gosiger's IT staff was flexible and resourceful enough to recover and was able to get the firm back to a semblance of normality fairly quickly after the first attack. With the benefit of hindsight, it is easy to identify the NIST framework that Gosiger should have adopted (and did adopt after the first attack), but the firm was able to recover and did survive. Not all firms are so lucky—one estimate from 2018 suggests that as many as 60% of small businesses fail after suffering a major cyberattack.[29]

By the time the second attack occurred, the IT staff was in a dramatically better position to defend critical systems. Even so, the attack was initiated via a simple phishing message. However, the resources needed for IT and security efforts were responsive in nature, which is not surprising given that IT at Gosiger is a cost center rather than a revenue-generating entity. As such, adding headcount was viewed as an expense that was not of the highest priority until the second attack made it clear that more staff were needed. The IT group doubled from two full-time employees (not counting help desk staff) to four, with additional consultants on retainer. This growth was required to manage the increasing complexity of the network and security resources necessary to defend the firm against future incursions.

Lesson 4. Technology Is Hard to attack, but People Are Easy

From all the evidence (admittedly poor given the limited logging Gosiger used then), the first SamSam-based attack was a more technology-focused attack. The second attack started with a phish that was received by a single employee in Pittsburgh. This highlights the significant challenge faced by organizations—no matter what they spend on technical controls, it only takes one person getting fooled by an email to bypass them. In larger organizations, it is commonplace to educate users through

29 Galvin, J. *60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack*. Here's How to Protect Yourself Online, Inc.com, May 17, 2018, available at https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html.

comprehensive training programs to recognize such attempts. Smaller organizations may not have the resources or staff to conduct such comprehensive programs, though they are just as necessary for SMEs. Phishing attacks are getting better and better, and generative AI will likely only serve to accelerate this trend. Hence, training users will still be imperative going forward, as will adopting Generative AI tools to help assess potential phishing messages.

Lesson 5. Management Must Understand the Importance of Cybersecurity and Fund It

Before the first attack, Gosiger's IS director had difficulties making the case for security expenditures and their importance to senior management. After the attack, senior management needed no further convincing. The IS director was promoted to VP/IS after the first attack, with significant increases in both funding and staffing dedicated to security. He was elevated to senior management, where these sorts of decisions are best made, with both the title and the organizational clout to do the job. That this didn't prevent the second attack, which was successful despite significant enhancements to cybersecurity, only highlights that security isn't a once-only exercise, though the enhancements meant the second attack wasn't nearly as disruptive.

Lesson 6. Recognize you Are in an "Arms Race" with Cybercriminals

The SamSam attack occurred at a time when both defenders and cybercriminals were not nearly as sophisticated as they are today. Despite dramatically strengthening its cybersecurity, Gosiger was hit a second time. REvil is a significant threat and demonstrates that attackers are only getting cleverer. The rapidity with which the criminals can copy and encrypt data means that response needs to be faster as well. The bad guys are definitely getting better, but so are the good guys, particularly those with deep pockets. The need for "deep pockets" to secure one's data creates a challenge for small businesses going forward.

As noted earlier, small businesses tend to have relatively limited resources compared to larger corporations. However, the threats to data confidentiality, integrity and availability are not diminished for SMEs. Indeed, it is more than likely that SMEs may be even more of a target than their larger counterparts. For example, hackers tend not to penetrate hardened defenses on primary resources but rather work in from peripheral systems, which is followed by attempts to gain elevated privileges on systems closer to the core of organizational operations. Such an attack is essentially what happened to U.S. chain store Target, where a heating, ventilation and air conditioning vendor's system was breached and used to gain access into Target's core systems.[30] Thus, even if the focal organization's systems are robustly defended from direct attack, an attack could originate from a partner's system, which obviously makes systems operated by business partners a target.

Much like larger organizations, SMEs have significant investments in various systems and software, and to simply mandate that everything be updated and/or patched immediately is infeasible from both cost and technical perspectives.[31] First, business-wide system updates take time and money, disrupt ongoing operations and are an unappealing prospect in an era of ever-increasing competition and financial pressures. As stated earlier, SMEs' limited financial resources compared to larger organizations may preclude them from installing stronger cybersecurity defenses, preferring instead to swallow the costs associated with recovery after an attack. Second, legacy systems may not work with updated operating systems or specific patches, which leaves organizations vulnerable. SMEs, in particular, have limited options for removing this vulnerability, short of radically redesigning their IT architectures.

Lesson 7. SMEs Face Increased Compliance Costs Due to Government Regulation

Consider, for example, the requirement for organizations handling so-called controlled

30 See Kassner, M. *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNet, February 2, 2015, available at www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned.

31 The cost of upgrading leads some organizations to forego the upgrades, with undesirable outcomes, as discussed in Barrett, B. *If You Still Use Windows XP, Prepare for the Worst*. WIRED, May 14, 2017, available at https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/.

unclassified information (CUI) belonging to the federal government to comply with NIST 800-171 (now in Revision 3, as of May 2024).[32] The impact of this is limited in the short term (DoD contractors were required to have this regime in place beginning on January 1, 2018). However, the broad definition of CUI implies that any organization that stores, processes or transmits federal data as part of its business operations may need to comply, including a great many SMEs doing contract work for federal or state governments, SMEs handling IRS data and universities (among others) would likely be required to comply with NIST 800-171.

Lesson 8. Cyber Criminals Are Becoming Increasingly Professional and Operate Like Businesses

The second attack at Gosiger used REvil ransomware. REvil uses a franchise model, not dissimilar to McDonald's. It recruits affiliates to distribute the ransomware. REvil provides the tools, the affiliate picks the targets and they split the revenue. The way attackers interact with their targets has taken on a transactional look and feel. When an organization is attacked via REvil, there are messages to contact what essentially serves as customer service to help negotiate the ransom, purchase Bitcoin to pay the ransom and provide the decryption keys. Indeed, the REvil group tends to refer to its victims as "customers" it is assisting in the recovery of their data for payment. The irony that the REvil group is the reason its "customers" have been denied access to their data appears lost to the cybercriminals, at least in terms of their public face.

It is worth noting that some kinds of cyberattacks will cause law enforcement, even in Russia, to at least go through the motions of enforcing international law. In January 2022 the Russian Federal Security Service (FSS) announced that it had dismantled REvil and charged several of its members after being provided information by the United States (and being subjected to no small amount of diplomatic pressure). It remains to be seen if these prosecutions will ultimately have any impact.

Recommended Actions for Strengthening Cybersecurity in Small Businesses

Though the experiences of the case study company provided some useful specific lessons, small businesses in general face significant resource constraints. Below, we provide six recommended actions that small businesses (and even larger ones) can take to protect their information assets against ransomware attacks and other malicious actions by cybercriminals.

1. Identify, Investigate and Implement State-of-the-Art Technical Solutions

There are a variety of technical solutions offered by software vendors and firms specializing in cybersecurity initiatives to deal with issues such as malware and other types of cyberattacks. Microsoft offers its Defender antivirus program and a firewall as part of the Windows 10 operating system, and there are a lot of web resources advising even those with limited technical skills on how to securely set up Windows 10 workstations. Most of these steps are fairly simple—e.g. password-protecting the screen saver, setting up the workstation as a user rather than as an administrator to protect from malware while on the internet and performing automatic patching and updates.

Other more turnkey anti-malware solutions are not free and the cost of one example we found was $2,000 per year for up to 30 devices (PCs, servers, etc.). This cost may seem to be excessive for an SME but it must be compared to the potential impact of an incident such as the ransomware attacks described in this article.

2. Continuously Train Users to Be Aware of Their Role in Cybersecurity

Though technical controls are important, training of the workforce is equally so, particularly with regard to passwords. Consider, for example, a technical control that requires a complex password to include at least one uppercase letter, lowercase letter, special character and number, with a length of at least eight characters. Such a control should be

32 NIST standards are mandated for U.S. government systems, and this requirement is now spreading to government contractors. See, for example, Ross, R. and Pillitteri, V. NIST 800-171. *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, National Institute of Standards and Technology, May 2024, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf.

administered carefully: "P@ssword1" would meet this requirement, but a 2015 study by Trustwave found "P@ssword1" was one of the most common passwords used on business computers.[33] Though the specific passwords may have changed since that study, the message is clear: users will develop workarounds to subvert procedures that make life less convenient for them. The benefits of complex passwords have been called into question, with more recent advice being to generate long phrases of random but easily memorable words strung together.[34] Another password-related issue is users repeating passwords on different sites, which is a bad, yet common, practice.[35]

As with many other aspects of cybersecurity, providing users with training and education on passwords represents one of the least expensive and perhaps most effective ways of improving online security. Some very good security training and user-awareness programs are free and available online. For example, "STOP.THINK.CONNECT." is a public awareness campaign led by the United States Department of Homeland Security that is aimed at improving the understanding of cyber threats and provides tools, approaches and strategies for individuals to use to enhance their safety online.[36] Free or low-cost resources such as this are a tremendously useful way for SMEs to overcome their resource constraints compared to large corporations.

3. Adopt Compliance Standards

Compliance with security standards doesn't have the nicest of connotations; however, these standards can be used to help IT staff identify areas they should focus on. NIST 800-171, for example, offers a fairly straightforward and comprehensive list of control areas and specific controls that should be in place in order to comply with the standard and that auditors should be able to advise on and use to assess compliance. We recommend that SMEs consider adopting one of the public standards, even if not required, because the effort involved will help those responsible for both protecting data and assessing compliance to identify areas in which they should focus their energies. Though this is not a "compliance" requirement per se, the NIST Cybersecurity Framework (CSF) mentioned earlier is an excellent (and free) framework that small businesses can use to develop and maintain their cybersecurity approach.

However, none of the standards for cybersecurity that an organization might adopt offers a "cookbook" set of instructions that guarantee appropriate levels of cybersecurity. Given that SMEs have relatively limited resources (and possibly experience in IT governance), they need to approach cybersecurity in a way that does not create unrealistic expectations in the minds of non-technical organizational management.

We believe there are several reasons that the NIST CSF helps to address this issue. First, and to an even greater extent with the release of Version 2.0, its range of resources provide fairly straightforward guidance for organizations just starting out in building a cybersecurity program. The framework includes simple control examples that can be readily understood and implemented for each function (e.g., mapping business mission to cybersecurity needs, documenting legal and regulatory cybersecurity requirements, or implementing multi-factor authentication.[37] At Gosiger, multi-factor authentication in particular would have perhaps offered an additional measure of security in the second ransomware attack. Another NIST CSF resource, CSF Tiers,[38] could help any organization identify where they currently stand in terms of cybersecurity and what reasonable goals for future improvements might be.

33 *2015 Trustwave Global Security Report*, Trustwave, 2015, available at https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/13167_2015-trustwave-global-security-report.pdf.

34 McMillan, R. *The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!*, Wall Street Journal, August 7, 2017, available at https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118.

35 Howarth, J. *50+ Password Statistics: The State of Password Security in 2024*, Exploding Topics, October 31, 2024, available at https://explodingtopics.com/blog/password-stats.

36 *Stop. Think. Connect*., stopthinkconnect.org, available at https://stopthinkconnect.org/. The United States Department of Homeland Security provides the Federal Government's leadership for the STOP. THINK. CONNECT. campaign.

37 See, for example, *NIST Cybersecurity Framework 2.0 Quick Start Guide*, National Institute of Standards and Technology, February 2024, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

38 *NIST Cybersecurity Framework 2.0: Resource & Overview Guide*, National Institute of Standards and Technology, February 2024, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf.

4. Include Cloud-Based Assets in Cybersecurity Initiatives

Though the cloud is often viewed as an additional concern regarding compliance and cybersecurity, it doesn't have to be. Various cloud-based services are available for data that is particularly sensitive. While we are not advocating any specific vendor, Amazon (for example) has cloud services that comply with various cybersecurity standards (e.g., NIST 800-171), and at least some of these provide advice on how to put controls in place to help secure the client side (i.e., your organization). Using such services would simplify both the implementation of relevant controls for SMEs and the auditing process (both for internal assurance and compliance with any regulatory regimes).

5. Conduct Regular Security Audits

Security audits tend to be costly and time-consuming, whether done in-house[39] or by hiring external experts. The scanning tools often employed generate copious amounts of information that require expertise to make it actionable. However, as many companies have found out through experience, the cost and time involved in using these tools are generally insignificant compared to the cost and time spent remediating a security incident. Conducting regular in-house security audits could be incorporated as part of a firm's adoption of the NIST CSF. In the Gosiger case, especially prior to the first attack, it's fairly clear that an in-depth understanding of the threat environment and what could happen was lacking.

6. Build and Cultivate Relationships with Skilled External Parties

SMEs typically do not have enough in-house resources to adequately respond to every possible cyberattack, whether successful or not. A recent study suggests that 95% of SMEs do not employ any information security professionals.[40] Fortunately, there are an increasing number of businesses with the expertise to assist firms in their response to cyber incidents. The two ransomware attacks at Gosiger highlighted the growing ecosystem of specialized firms able to provide help. For instance, in the first attack, AT&T helped Gosiger with its mitigation efforts. In the second attack, there were other firms that assisted with tasks such as interacting with the attackers, assisting with recovery efforts, and more. This increasing availability of agile partners was a key factor in the firm's ability to respond, even with the increased sophistication of the second attack.

Hackers will continue to become more sophisticated. As they become more advanced, so too must the defensive efforts before an attack as well as the response efforts after an attack. Fortunately, cybersecurity professionals will also become more sophisticated and equally adept at combating hackers. SMEs and other firms should build and cultivate relationships with vendors, consultants and law enforcement partners that will enable a speedy and effective response to potentially enterprise-threatening incidents. Being able to draw on these resources is thus a critically important factor in an SME's preventative endeavors.

Concluding Comments

In this article, we described two ransomware attacks on a small business that prevented it from accessing its systems and data unless a cash payment was made to the attacker. After the first attack, no payment was made because of a combination of hard work (and a bit of luck), but the firm still incurred significant recovery costs. After the second attack, the firm had to pay a ransom to avoid the release of sensitive employer information, but, with the help of a third party, the amount paid was negotiated to a much lower amount than that originally demanded.

About the Authors

Donald Wynn, Jr.

Dr. Donald Wynn, Jr. (wynn@udayton.edu) is the Sherman-Standard Register Associate Professor of Management Information Systems at the University of Dayton. He received his Ph.D. in business administration from the University of Georgia, an M.B.A. from Middle Tennessee State

39 For an article that discusses the key components of an in-house security audit, see *How to Conduct Your Own Internal Security Audit*, Dashlane, April 16, 2021, available at https://www.dashlane.com/blog/conduct-internal-security-audit.

40 *Information Sharing in Cyber Supply Chain Risk Management—A New Model*, ISC2, June 27, 2024, available at https://www.isc2.org/Insights/2024/06/Information-Sharing-in-Cyber-Supply-Chain-Risk-Management-A-New-Model.

University, and a B.S. in electrical engineering from The University of Tennessee, Knoxville. Prior to pursuing a Ph.D., he worked for 15+ years in engineering, telecoms and information systems. His current research includes cyberattack methodologies, cybersecurity and software ecosystems.

W. David Salisbury

Dr. W. David Salisbury (salisbury@udayton.edu) is the Sherman-Standard Register Professor of Cybersecurity Management in the MIS, OSC and Business Analytics Department at the University of Dayton. He is the founding director of the UD Center for Cybersecurity and Data Intelligence, leading it during its early development and designation as a Regional Programming Center for the Ohio Cyber Range Institute. He is now a Senior Fellow at the center. Dave also teaches on the NIST Risk Management and Cybersecurity Frameworks, and holds the (ISC)2® Governance, Risk & Compliance Certification. He has commented on cybersecurity issues in local, national and international media outlets.

Mark Winemiller

Mark Winemiller (mwinemil@gmail.com) has over 25 years of experience as an information systems professional. He is currently a senior consulting systems engineer at World Wide Technology, Inc. (a U.S. technology services company), where he brings a depth of strategic technical insight to every project. Previously, he rose through several leadership roles at Gosiger, Inc., from IS manager to director, VP and, finally, VP of IS and Marketing. He is also an active member of multiple technical boards, driving impactful technology solutions across industries. Mark has a BS in computer information systems and an MBA from the University of Dayton.

