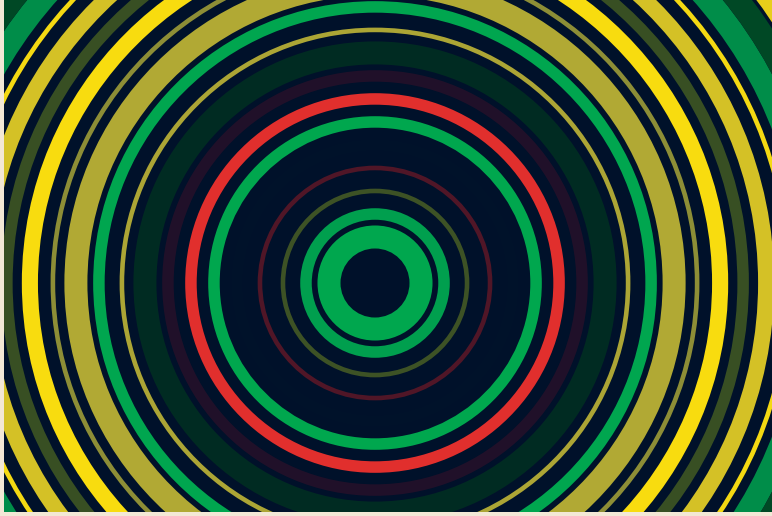
# Cybersecurity threats proliferating for midsize and smaller businesses

Smaller organizations are targets for hacking and phishing attacks to get information that can harm them or bigger companies they do business with.

By Russ Banham



IMAGES BY FRANKRAMSPOTT/ISTOCK



Why would cyberthieves target a company other than the very largest—big enterprises with big payoffs? It's a question that many small and medium-size businesses (SMBs) ponder, arriving at the wrong answer.

Hackers have SMBs in their crosshairs as much—if not more so—than the world's biggest enterprises. Here's one reason: Small companies in the business-to-business space that serve large organizations often connect to the latter's networks and systems. In effect, the SMB is a potential conduit to the larger company's data assets. Case in point: The massive data breach of Target in 2013 was widely reported to have begun with the hacking of the retailer's HVAC vendor.

Another reason SMBs have a bull's-eye on their backs is that just like larger businesses, they are repositories of sensitive customer and employee information like credit card numbers. These data can be stolen and sold on the darknet, the anonymous network used for illegal peer-to-peer file sharing. In its shadowy corners lurk the plunder of many data breaches, including the spoils taken from SMBs.

"Small businesses are a prime target of cybercriminals," said Larry Ponemon, Ph.D. (accounting), chairman and founder of the Ponemon Institute, a research think tank dedicated to advancing data protection practices. "Hackers know that smaller organizations don't have the wherewithal to develop a defensive security strategy. But the companies themselves tend to erroneously believe that the bad guys only target big companies."

This was true for a long time, Ponemon added, "until smart hackers realized they could get into a large business through a small one. Just because you're small doesn't mean you don't have access to a huge amount of valuable information."

A 2016 study by the Ponemon Institute found that 55% of SMBs experienced a cyberattack in the previous 12 months, and 50% experienced a data breach over the same period. Nearly 600 respondents participated in the research, which looked at companies with a headcount of fewer than 100 employees up to 1,000.

## PROTECTING THE STORE

There are several types of information that many SMBs are required by law and industry regulations to protect. They include protected health information (PHI) that is shielded by the HIPAA privacy and security rules, personally identifiable information (PII), and credit card data. The latter security standard is known as PCI DSS ▸

### GET THE COMPLETE PICTURE

For information on how to defend your small business from cyberattacks, the Federal Trade Commission rolled out a webpage on May 10 (ftc.gov/SmallBusiness) that offers free risk management tips and other advice to small and medium-size businesses. The site is designed to help smaller companies protect their networks, systems, and customer and employee data from cybercrimes. Among the FTC tips is compiling the following information:

- **Who sends sensitive personal information to your business.** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Job applicants? Other businesses?
- **How your business receives personal information.** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
- **What kind of information you collect at each entry point.** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
- **Where you keep the information you collect at each entry point.** Is it in a central computer database? On individual laptops? On a cloud-computing service? On employees' smartphones, tablets, or other mobile devices? On disks or tapes? In file cabinets? In branch offices? At employees' homes?
- **Who has—or could have—access to the information.** Which of your employees has permission to access the information? Do they need access? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Are contractors operating in your call center?

Source: Federal Trade Commission, *Protecting Personal Information: A Guide for Business*.

for the payment card industry that created the data security standard. Similar regulations are in place for businesses in specific industry sectors, such as small banks or insurance agencies.

In all cases, a business must protect the information from loss, theft, or damage and notify relevant authorities in the event of a data breach. Noncompliance can result in fines and penalties. The challenge for SMBs is the cost of protecting these data. "Large organizations have ample resources dedicated to this; smaller organizations typically do not," said Mark Burnette, CPA, shareholder at audit and advisory firm LBMC, where his focus is client cybersecurity. "Their resources generally are constrained. They just have less attention to provide the matter."

Other cyber experts agree. "Small companies typically don't have a formal cybersecurity policy, much less a chief information security officer like many large companies have in their employ," said Rod Smith, CPA, managing director of audit and advisory firm Crowe Horwath. "It's also considered overly expensive by many SMBs to implement a program that prevents, detects, mitigates, and helps a business recover from cyber incidents."

Aside from the expense, many small businesses believe there is scant risk of something bad happening if they skirt the rules. While Smith noted that the regulatory scrutiny of SMBs is not as assiduous as the inspections accorded larger businesses, complacency can backfire. Ponemon agreed: "The statistics indicate that very few small companies will avert a cyberattack."

This may explain why many large enterprises that conduct business with smaller companies are now requiring them to provide evidence of their cybersecurity practices. "More and more smaller businesses serving *Fortune* 500 and large publicly owned companies are coming to us to report on their cybersecurity practices," said Smith. "The main reason appears to be that their customers are demanding it."

SMBs that do not confront such pressure nonetheless cannot be cavalier about a risk that can severely disrupt and even doom their business. Hackers are aware that many SMBs collect customer credit card data. Knowing this, the thieves attack a small retailer's point-of-sale system to make their way into the payment card data. "A small retailer on Main Street also may have access to all sorts of people, buying mailing lists that could contain sensitive data like login information," Ponemon said.

Other threats include payment card skimmers that physically tamper with ATMs and fuel-pump terminals. "Being small doesn't mean you're free from worry," he added.

Aside from a data breach, SMBs also face the threat of ransomware. This malicious software is embedded within infected email links, email attachments, and compromised webpages that either lock up a computer screen so users can't access their applications, or encrypt files so they can't be opened. To unlock or reopen, the company must pay a ransom, typically in bitcoin. Once hacked, most companies pay the ransom, which for smaller businesses is in the range of a few thousand dollars.

The common entryway for a cyber extortionist is a phishing scam that entices an employee to click on something he or she shouldn't. According to the U.S. Department of Justice, ransomware attacks quadrupled from 2015 to 2016, averaging an astonishing 4,000 attacks each day. The United States is the region most affected by ransomware, recording 28% of infections globally. "When we first looked at ransomware in our SMB survey, only 11% of small companies had been victims," Ponemon said. "In 2016, the percentage jumped to 46%—nearly half of all attacks."

### CYBERSECURITY RISK MANAGEMENT REPORTING FRAMEWORK

The AICPA unveiled a new framework for cybersecurity risk management reporting designed to help businesses meet a growing challenge.

The AICPA's framework is voluntary and designed to enable all organizations to communicate about the effectiveness of their cybersecurity risk management programs and to communicate effectively about cybersecurity activities. Two resources that support reporting under the framework were released in April:

- Description criteria that management can use to explain an organization's cybersecurity risk management program in a consistent manner. CPAs can use these criteria to report on management's description of its cybersecurity risk program.
- Control criteria that CPAs providing advisory or attestation services can use to evaluate and report on the effectiveness of the controls within a client's program.

An attest guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, has been published to assist CPAs who are engaged to examine and report on an entity's cybersecurity risk management program.

The engagement for reporting on a cybersecurity risk management program and controls grew out of an emerging need identified by the AICPA Assurance Services Executive Committee. Using the framework, CPAs can provide cybersecurity-related assurance services while applying their experience in auditing information technology controls.

More information is available at aicpa.org/cybersecurity.

### LOCKING DOWN THE HOUSE

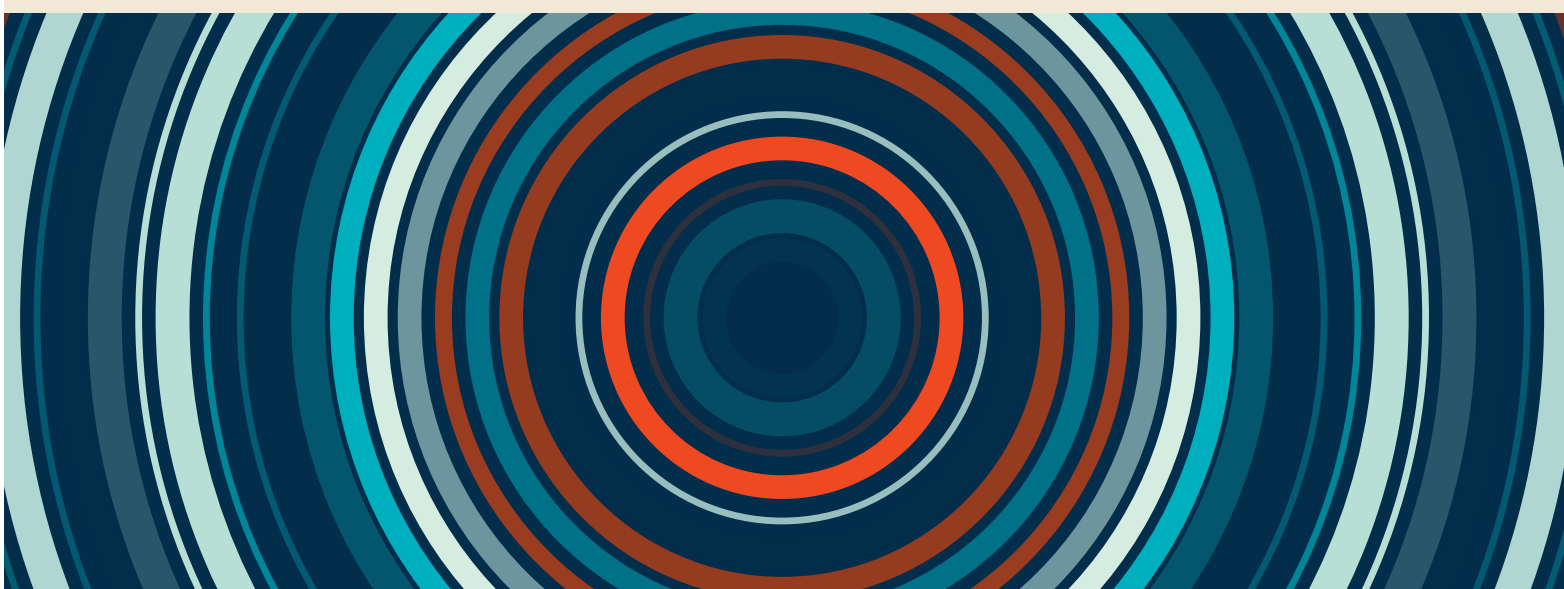
According to the Ponemon study, the most prevalent cyberattacks against SMBs today are web-based and phishing/social engineering scams. Negligent employees and third parties such as outside vendors are the primary cause of most breaches. Nearly six in 10 respondents said they did not have visibility into employees' password practices, indicating the possibility of weak password protections. Of small businesses that have developed a password policy, 65% do not strictly enforce it.

### TAKING PRECAUTIONS

"Small companies need to do what large companies are doing; being small doesn't let them off the hook," said Mary Galligan, managing director, cyber risk services at audit and advisory firm Deloitte. "In both cases, the cyber hygiene is the same, whether you employ 10 people or 10,000."

How can SMBs begin this journey? Galligan advised they task someone within the organization to be responsible for the cybersecurity program. "It's basic human nature—once we put someone in charge of something, it gets looked at," she explained. "The person could be the CFO or in very small firms someone who is knowledgeable about technology. Once selected, the individual should be championed by the CEO or the business manager so everyone understands such supervision is in place and is important."

The cyber risk monitor's first assignment should be the development of a written cybersecurity policy that is signed by employees, who are then held accountable to the policy's rules, she added. This report should identify the organization's key cyber risks and most important data assets, as well as who in the organization has access to these data and on which devices, such as a personal laptop. (See the sidebar "Cybersecurity



Risk Management Reporting Framework" for information about guidance the AICPA has released to help organizations gauge the effectiveness of their cybersecurity efforts.)

"You can't protect sensitive data assets if you don't know what they are," said Burnette. "Once you know what it is and who should have access to it, you can then identify all the business processes involved in storing, transmitting, or processing the data to make well-informed decisions about how best to protect it."

Not that this is easy. Burnette pointed out that many SMBs have duplicates of data residing across the business. "An example is an attorney at a small law firm that exchanges sensitive files with clients, pulling information out of the firm's data repository and storing it on their laptops and phones using Dropbox, on flash drives, and possibly even backing it up on an external hard drive at home," he said. "There are now four copies of sensitive data floating around." And those methods of storage are not considered secure.

Other points to make in the cybersecurity policy include how the company's IT hardware is secured. For example, a key concern is the possibility of a nonemployee on the premises surreptitiously attaching a thumb drive to a desktop computer or a laptop to download files and other information. "If a device stores sensitive data, consider plugging the USB ports," Galligan said.

The security report also should address how the business is securing connected networks, cloud-based services, and other internet connections. Ditto company-provided mobile devices and those owned by employees that are used in a work context. Also spelled out clearly in the report are the company's security expectations of its employees and the third-party organizations providing services to the business.

In the case of a small business such as a café that hosts a Wi-Fi public access network, the report should identify how the wireless router is secured, such as through WEP, WPA, or WPA2 security software (each type offers a different level of security). According to a 2016 study of more than 31 million Wi-Fi hotspots across the world by Kaspersky Lab, more than one-quarter are not secured, lacking encryption or password protection.

Lastly, the report must have sharp teeth, with employees determined to be noncompliant at risk of losing their jobs. "Since phishing and other social engineering tactics are the root cause of so many data breaches, employees must be held accountable for their behavior," Galligan said.

## TRAINING AND EDUCATION

A tone at the top stressing the importance of cybersecurity and policies around strong passwords can help safeguard companies of all sizes. But that must be paired with training and education to regularly remind employees about the types of sensitive data the organization produces, transmits, and stores. Regular training also should be scheduled to ensure employees recognize new phishing scams and understand the actions they need to take when such tactics are evident. (See the sidebar "Get the Complete Picture" for tips from the Federal Trade Commission on protecting your business's sensitive data from cyberattacks.)

"Small companies' biggest risks like ransomware are caused by people clicking on things they shouldn't click on," Galligan said. "If a small business only had the resources to concentrate on just one thing, I would put it towards data access management."

Even the best cybersecurity policy is not perfect to thwart all cyberattacks, as large companies will attest. With the world increasingly interconnecting, companies of all sizes are becoming bigger targets.

"I tell clients they're going to be hacked at some point, which is why they need to have a plan in place of what to do when it happens," said Galligan. "Based on the size of the attack, they may need forensic, legal, and even crisis management support." Incident response planning is also key. "Knowing this beforehand, and having it clearly spelled out in the cybersecurity policy, will guide more-efficient and cost-effective mitigation and remediation tactics."

*Russ Banham, who specializes in technology risk management, is a veteran financial journalist and author of more than two dozen books.* ■