Best Practices for Institutional Cybersecurity

Introduction

The events of 2020 forced a significant portion of the working world into "work-from-home" status. Institutions needed to shift their operations virtually, whether they were ready or not. In many cases, the logistics of distributing laptops and other office supplies as quickly and with as little disruption to operations as possible took center stage. This did not leave much time to think about the importance of cybersecurity, much less put safeguards in place. In this paper, we discuss the current cybersecurity landscape, identify common vectors for attack and offer a five-step approach to cyberhygiene.

Current Landscape

Large corporation data breaches are typically the ones that make the news, but small businesses, nonprofits, higher education institutions, healthcare systems and other institutions are an increasingly attractive target of cyberattacks. Global losses from cybercrime now total over $1 trillion, according to a December 2020 McAfee Report.

While large corporations typically have the budget to maintain cutting-edge technology and dedicate entire departments to security, criminals expect smaller institutions to have limited resources for cybersafety. Almost a third (28%) of data breaches in 2020 involved small businesses, according to Verizon 2021 Data Breach Investigations Report.

Consider a local religious organization such as a church, synagogue or mosque. The organization relies on its members, financial donors and volunteers to keep the lights on. Over time, the organization collects a treasure trove of sensitive personal information. For example, the organization might have the names, addresses, phone numbers and even the credit card numbers of members who have donated money in the past.

Generally, would this small nonprofit have security-focused database software or a vendor to protect this sensitive information? Or is it more likely that the person responsible for the organization's finances has a simple Microsoft® Excel spreadsheet saved on their unsecured shared drive? In this case, cybercriminals would probably be right about the vulnerabilities of smaller organizations. The smaller religious institution most likely does not have the resources for a security-focused database, and its Excel spreadsheet of donor information is much easier to reach than a large corporation with multiple lines of cyberprotection.

A successful cyberattack has far-reaching implications for institutions large and small, whether for-profit or not-for-profit. A breach harms an institution's reputation and deters partners, employees, donors, volunteers and other associates from working with the organization. An institution's most sensitive asset is its data, and it is the institution's responsibility to protect it. Financial ramifications are also significant.

Unfortunately, there is no panacea to make an institution cybersafe. Cybercriminals are always finding new ways to cause damage. But a commitment to ongoing education, employee training and a few best practices can go a long way toward upholding an institution's responsibility to protect its data. The cyberhygiene methods discussed here are affordable and can go a long way toward keeping an institution's assets safe.

Three Common Vectors for Cyberattacks

A crucial part of protecting against cybercrime, especially with limited resources, is understanding and focusing on mitigating the common threats. Three common vectors for cybercrime are email, business networks and mobile devices.

Email

Cybercrime accomplished by email is sometimes referred to as "phishing." According

to 2020 AFP Payments Fraud and Control Survey, 75% of companies were exposed to business email fraud in 2019, and phishing accounted for 22% of breaches in 2020, according to Verizon 2021 Data Breach Investigations Report. In this scenario, a cybercriminal sends what appears to be a legitimately business-related email. The email instructs the employee to complete a task that seems innocuous but enables the criminal to complete their crime (e.g., initiating a wire transfer or other financial transaction by gaining access to the organization's system).

One common line of attack is for a fraudster to pose as a senior executive and attempt to have the employee send sensitive personal information by email. Another is for the cybercriminal to pose as an outside vendor and ask the recipient to click on a link and fill out a form of information about the institution's financial accounts. While the approach may differ, fraudulent business emails usually contain some detectable red flags, including:

- a generic, awkward greeting;
- use of number in the place of a letter, like using "1" instead of "L";
- a demand for an immediate response;
- an offer that is too good to be true; and
- an address that has a small variation from the company's actual address.

If the criminal is successful, they might gain access to sensitive client information, access to the institution's financial information or other valuable information.

Key Defenses:

- **Empower your people.** The top defense against cyberattacks is an institution's employees. Employees can spot the anomalous behavior indicative of a malware infection, phishing or another social engineering attack. Empowering employees to pause and report suspicious activities will protect your customers and your business.
- **Establish Domain-based Message Authentication and Reporting Conformance (DMARC) on all your email domains.** DMARC is a way to electronically sign emails and tell email providers *how* to identify when *your institution* sends an email versus when a *criminal* is pretending to be your institution when sending an email. DMARC also tells the email providers what to do with those impersonations: delete or quarantine. You can also get reports on who is trying to impersonate your institution and how often. This can help you build communications for your customers and/or employees so they can better protect the company and themselves.
- **Separation of duties leads to a far harder target.** For example, an approval process (e.g., for a cash distribution request) that requires the requestor and the approver to be different people can make it more difficult for criminals, requiring them to compromise multiple people.
- **Multi-factor authentication (MFA) prevents a criminal from being able to access your emails just by knowing or guessing your password.** MFA is supported by all major email providers and offers a significant security boost over just use of a username and password.

Network Security

Another type of fraud occurs when a cybercriminal gains access to an institution's sensitive information by entering the company's network. In 2020, 45% of breaches were caused by hacking tactics like this.

There are different ways for hackers to enter an institution's internal business network. As remote work becomes even more common, employees need to be vigilant about how and where they connect to the internal network remotely.

If the computer is connected to a business's network, and the cybercriminal has access to the computer, then the cybercriminal has access to the business's network. And if all of the content of the entire business network is available from a single entry point, not requiring different passwords to different secured areas, then the cybercriminal has immediate, easy access to everything.

Key Defenses:

- **Virtual Private Networks (VPN).** Using a VPN limits the ability of a criminal to intercept communications between an organization's employees' disparate systems and its core network. When MFA is enabled on a VPN, it becomes even more difficult for any criminal to attain access to the business's network.
- **Apply system patches as soon as possible.** Unpatched systems have been at the heart of many of the largest breaches, costing companies hundreds of millions of dollars. Taking a system offline to patch it will never cost as much as unpatched systems have cost breached companies. Ransomware actors in particular like to target unpatched systems.
- **Segregate systems and only allow people access to data that they need to conduct their business.** Every employee of an organization should not have access to all of the organization's data. Even enforcing password protection of folders can limit a criminal's ability to steal or weaponize a company's data.

Mobile Devices

More people than ever before are using mobile devices and tablets to conduct business online. In addition to being vulnerable to nonphysical actions like email compromise and network hacking, mobile devices are also vulnerable to physical interference. While it might sound like the plot of a spy movie, physical actions are present in 4% of breaches.

Starting with the obvious example, if a phone is lost or stolen, all of the business data and access on the mobile device goes with it. Even without password access, sophisticated hackers are able to "jailbreak" phones by installing software that allows them to bypass password prompts.

Other types of physical interference can be less obvious. For example, how often have you been traveling or otherwise away from home and needed to charge your mobile device? Knowing this, some hackers have set up charging stations to perform "juice jacking." When the device is plugged in to charge, the hackers use the charging cable to access the phone's data or install malware on the device.

Key Defenses:

- **Establish MFA on mobile phones.** This will prevent unauthorized changes.
- **Screen-lock phones.** Even a simple, four-digit PIN can thwart a criminal's attempt to use your phone against you.
- **Carry your own charger** or use a write-blocker when travelling.
- **Establish strong procedures** so no one will act based on a voicemail, text message, or a simple phone call. This prevents a criminal impersonating one employee to create havoc in your enterprise.

Five-Step Approach

Cyberhygiene will look different for different organizations, but the different approaches can share common best practices. We recommend a five-step approach that is customized to the needs (and resources) of your organization.

STEP 1: Educate yourself

The first step of any problem-solving exercise is to understand the problem. Commit time to understanding the scope of the issue and what policies and procedures your organization has in place today. The paragraphs above are a good start, but there is more to learn. Research the common

vectors we looked at above. Does your organization engage in activities that put it at risk? Some key questions to consider include:

1. Your organization is more vulnerable to phishing attacks if your employees are not actively engaging in training on how to spot and respond to fraudulent emails. Is regular cybersecurity training for employees being provided?
2. An organization is more vulnerable to network breaches if the network is being accessed using unsafe Wi-Fi connections. Provide users with a way to protect their connection by issuing safety tools like VPNs?
3. Are employees are allowed to conduct work using mobile devices that are not issued by the company? Do you know what devices they are using, and whether they protect them with passwords and tracking capabilities?

It may seem obvious, but it bears saying: working with a cybersecurity firm can help you to identify and understand the scope of what your organization needs to be successful in implementing cybersecurity solutions.

STEP 2: Assign Key Owners and Key Performance Indicators

Cybersecurity prioritization starts with leadership; unfortunately, leadership is often committed to only the bare minimum. This is changing, though, as organizations recognize the consequences of poor cyberhygiene.

It is becoming increasingly common for organizations to name a Business Information Security Officer who is equipped to stay up to date on the organization's cybersecurity needs, and can then communicate concerns directly to their management team, board members and other key stakeholders.

Once key owners are defined, it is important to define what success will look like. No news is good news when it comes to cybercrime, but you can't leave your efforts on autopilot. Key performance indicators help to keep cybersecurity top-of-mind. "No breaches" isn't a quality performance indicator because the cybercrime landscape is evolving. What worked last quarter might not work this quarter.

Key performance indicators that seek to identify potential risks are preferable over relying on backward-looking data. What does security "success" look like to you? What corresponding measurables are feasible for your organization?

STEP 3: Develop a plan of action and key policies

Establish formal policies, procedures and controls for the specific threats that your organization is choosing to address. Employees can serve as a great first line of defense against attacks, as long as they know what to look for. Employees should be trained and empowered to recognize online activity that deviates from the norm. To create a culture of vigilance, it's important that the sentiment starts at the top. Be sure that your board and your executive management communicate and follow the policies and procedures.

To illustrate this point, consider that most organizations have to purchase software and/or hire outside vendors as part of the normal course of business. As part of the process of making purchasing/hiring decisions, does your organization have a policy to ask security-related questions? As an example, one important question might be to ask about their prior experience with data breaches. When was their last breach, and how did they respond? It's also helpful to know whether the third party has regular security audits performed by an outsider. These questions can help you to feel confident that your data, and potentially the data of your clients/customers, will be protected.

The policies should also identify key steps for handling a breach. If a breach does occur, moving quickly to secure your operations and fix vulnerabilities can be critical, and having a procedure in place can help to shorten your response time. The Federal Trade Commission's (FTC's) Data Breach Response Guide is a good place to start.

In putting a procedure in place to deal with a potential breach, it is important to consider a communication plan. The consequences of a breach generally reach beyond the office and can harm relationships with customers, vendors, volunteers, donors and others. Communications following a breach can help to preserve those relationships. The FTC's guide, above, includes a model letter that your organization can use to properly and timely notify all affected parties, including individuals, vendors and other organizations.

Finally, cyberinsurance is one option that can help you protect your business against losses caused by a cyberattack. Providers offer things like payments to consumers affected by a breach, litigation costs, crisis management and more. Given the variety of insurance providers, it is important to ask cyberinsurance providers what their specific policies cover and don't cover.

STEP 4: Set a review period

Should plans be reviewed once every 3, 6 or 12 months? The answer will correspond to an organization's action plan. Because the cybersecurity landscape changes rapidly, erring on the side of too much is probably prudent.

In order to serve as a first line of defense, employees need to see a culture of security. This can be fostered by a regular training schedule. In addition to relying on the culture of security, organizations can choose to block an employee's access to the network if they do not complete the trainings.

Shifting to an external focus, it is important to regularly monitor and review third-party vendors. Requirements for regular review should be included in the contract so that the vendor is continuously verifying compliance with an organization's rules to show that they are keeping their security updated.

Finally, we would recommend that the review period be tailored to the organization's action plan. Some plans will need more frequent reviews, whereas an annual review might suffice for others. This decision can also hinge on the scope of the organization's operations and a number of other factors that relate to the extent of the company's possible exposure to cybercrime.

STEP 5: Execute

Start your cybersecurity efforts now. It is imperative that institutions do not wait to become a victim before addressing this reality: cybercriminals are sophisticated, and their objective is to catch institutions off-guard. There is an old saying, "Trust takes a lifetime to build and a single day to lose." Taking steps now to implement best practices for cyberhygiene can help an organization to maintain the trust of its customers/clients, employees, and other key stakeholders.

Conclusion

The pandemic accelerated the world's digital transformation. We believe that the importance of the virtual environment — and the need for protection — is going to increase rather than fade.

The best practices we shared here serve as a good introduction to understanding the cybercrime landscape and how to position your organization more defensively. Cybercriminals will find new ways to commit online crimes, but protective resources will also continue to evolve. Cybersecurity experts can tailor plans to meet the unique needs of your institution.

For additional resources, please visit PNC's security and privacy center.