The Cybersecurity Watchlist for Association and Nonprofit Executives

delcor

TABLE OF CONTENTS

INTRODUCTION 3

THE NIGHTMARISH IMPACT OF A SECURITY BREACH 4

SECURITY AWARENESS BEGINS IN THE C-SUITE 5

A WORD ABOUT DATA 6

WATCH LIST: 17 THINGS TO LOOK OUT FOR 7

FINAL THOUGHTS 22

INTRODUCTION

When it comes to security, what you don't know can hurt you. No one expects association and nonprofit executives to be security experts, but you need to know whether your organization's departments are doing all they can to protect your data and systems.

Why would a hacker go after your association when more enticing targets are out there? Because hackers aren't picky. Ransomware is easy and affordable to deploy: They use automated tools that crawl the web seeking vulnerabilities wherever they exist. It is so easy that "Ransomware as a Service" is now a viable business model, where hackers can buy ransomware products to attack whomever they please. When a weak link is found, they go in and grab data. Your organization has exactly the type of sellable data wanted by cybercriminals: personal and financial information of employees, members, donors, and customers. But more frequently, it's all about the money. Criminals are counting on you to pay ransom to get your data back. While espionage and "advanced persistent threats" (APT) get a lot of press, 86% of breaches are simply financially motivated (according to Verizon DBIR).

It's not only data they seek. Sometimes they simply want to use one of your servers or workstations to attack someone else. Your own infrastructure (servers, Microsoft 365) can be leveraged as a vector to spread ransomware to others.

Even more troubling, your organization might not even be their target—one of your members might be. The hackers could use one of your systems to infiltrate a member's network.

And sometimes, it is personal. A 'hacktivist' group attacks your network to cause harm or embarrassment to your industry in the most public manner possible.

THE NIGHTMARISH IMPACT OF A SECURITY BREACH

SECURITY BREACHES HAVE DAMAGING CONSEQUENCES:

- Websites and e-commerce sites go down
- Data assets must be restored
- Credit card information is stolen
- Confidential or proprietary information is compromised
- Data is lost—even something as innocuous as member names or emails
- Embarrassment
- Average cost of security breach in 2020: $3.86 million (according to an IBM report)

THE IMMEDIATE IMPACT HURTS, BUT THE LONG-TERM IMPACT CAUSES EVEN MORE FALLOUT:

- Business interruption
- Communication crisis
- Loss of data and other information
- Weakened brand reputation
- Loss of member and donor trust
- Loss of online revenue and other financial assets
- Costs of forensic investigation, crisis management, legal counsel and damages, regulator penalties, and credit monitoring

This report will help you prepare your organization for this new worrisome security landscape. We identify the most likely security threats for associations and nonprofits, their cause and impact, and the questions you need to ask your IT team to ensure your organization is protected.

SECURITY AWARENESS BEGINS IN THE C-SUITE

Before we get into specific threats, let's step back to take a wider look at security in your organization. Security is not an IT concern only. **Security is everyone's concern**, starting with your organization's staff leadership.

ADD THESE QUESTIONS TO YOUR NEXT SENIOR STAFF MEETING AGENDA:

- Do we have multifactor authentication (MFA) in place protecting ALL remote access? (MFA is no longer a "nice to have" – it is the best protection you can add to defend against account compromises)
- We used to ask "Does our IT team have sufficient security training? Do they have the budget and time to regularly attend security training?" This is still important, but the question should now be: Do ALL OUR EMPLOYEEES have sufficient training, especially those responsible for member data, financial data, and the websites?!
- Do we have an IT security policy? Who wrote it? How often is it reviewed and revised? Has our staff read it? How do we measure compliance?
- What steps have we taken to nurture a culture of security awareness?
- Do we provide regular security awareness training for staff?
- When was the last time we had a security audit, and did we complete the resulting recommendations and remediations?
- Do we have an incident response plan?
- Should we invest in cybersecurity insurance?

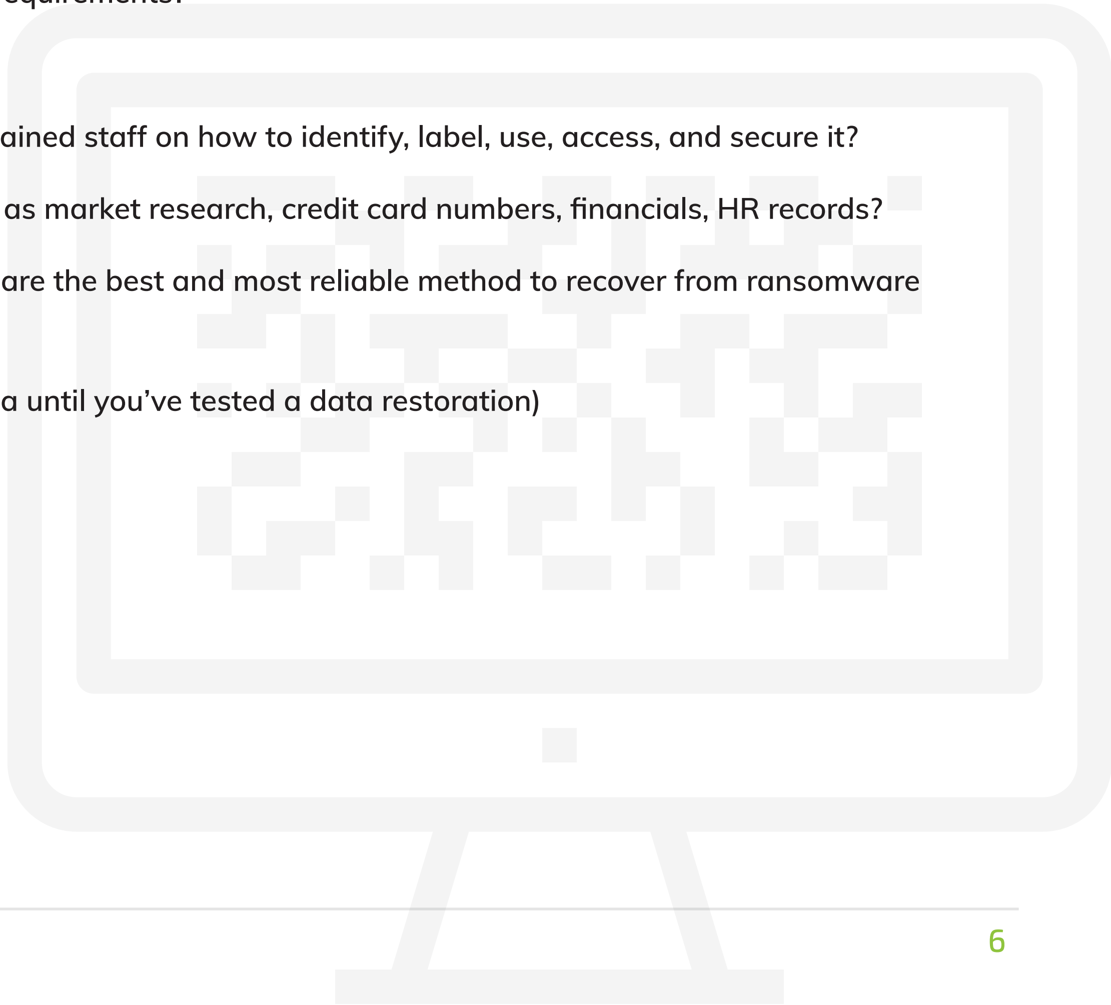
If you need someone to guide you through the changing and confounding world of cybersecurity and the decisions you must make to survive and thrive in that world, our DelCor consultants can help. In a trusted partner like DelCor, you get the assurance of knowing we're always on the lookout for you, assessing systems, solutions, and threats.

A WORD ABOUT DATA

Before we dive any deeper into security threats, we must first address the information entrusted to your organization's care by your members, customers, donors, and staff. Cybercriminals have sophisticated tools at their command (or easily bought on the black market) to wrest this valuable data from your safe-keeping. And you'd be surprised at all the varying levels and types of data they're after.

QUESTIONS TO ASK YOUR DATA TEAM:

- Have you documented the types of data we have, where it's located, who owns it, and who has access to it?
- Do you segregate data by its level of importance and security requirements?
- Is sensitive data encrypted?
- Have you established clear definitions of 'sensitive' data and trained staff on how to identify, label, use, access, and secure it?
- Do you know where you are storing sensitive information such as market research, credit card numbers, financials, HR records?
- Is data automatically backed up and stored off-site? (Backups are the best and most reliable method to recover from ransomware attacks)
- Have you tested a data restoration? (Don't rely on back-up data until you've tested a data restoration)



WATCH LIST: 17 THINGS TO LOOK OUT FOR

Throughout this report, we'll share some of the stories we've heard via our secret IT backchannel about associations and nonprofits that have been victimized by hackers.

1. PHYSICAL THEFT AND LOSS

Our first story took place last year in a friendly Midwestern city. Two backup hard drives belonging to a state association were stolen while on their way to an offsite storage facility. The details of the theft weren't revealed but, most likely, the drives were taken from an employee's vehicle. These drives contained the association's group health and life insurance databases including the medical history, social security numbers, and personal information of 39,000 members. Ouch.

Employee-owned vehicles are the location of 22% of data equipment thefts. Work areas are the most common location for thefts—55% of them. Storage drives, computers, laptops, tablets, and phones are tempting targets because of the data they hold and/or the access they provide into your organization's network.

Smartphones are essentially mini-computers that provide access to your organization's accounts and data. Bring-Your-Own-Device (BYOD) practices increase the risk of theft or loss because phones and tablets could be in use around the clock. The security risk increases when employees travel through airports, leave belongings in rental cars, or use their devices on public transit or in coffee shops—going mobile means more opportunities for devices to get lost or stolen.

QUESTIONS TO ASK YOUR IT TEAM:

- Do we have a method for tracking endpoints including laptops and smartphones?
- Does our workplace culture (and IT policy) encourage prompt reporting of loss or theft within a specific number of hours?
- Are you able to remotely wipe any device that stores organizational data? Have employees signed an agreement authorizing the remote wipe of personal devices if a data breach is possible?
- How are phones handled when employees are terminated?

- Are computers in the office physically secured?
- Are computers in the office logged off and locked automatically after a set period of time?
- Are passwords and encryption required and activated on all devices?
- Is MFA required to access data on the server or in the cloud?

2. INSIDE JOBS: EMPLOYEE MISUSE AND ERRORS

Thirty percent of incidents are caused by insiders abusing their privileges. Employees or other individuals who have access to your network or data can take advantage of that privilege and cause harm. Their actions are usually motivated by convenience, not crime.

EMPLOYEES (AND FORMER EMPLOYEES) PLACE ORGANIZATIONS AT RISK BY:

- Retaining log-in privileges or access after termination
- Taking shortcuts or using unapproved workarounds to do their job
- Sending sensitive information to the wrong recipient
- Publishing nonpublic data to public web servers
- Disposing personal data insecurely
- Ignoring password protocol
- Human error, or just plain carelessness

Surprisingly, system administrators are the culprits in 60% of insider misuse incidents, according to a Verizon study. The practice of giving administrative privileges by default to employees who don't need them is one reason for this high number. Operate on the principal of least privilege: only assign administrator rights when absolutely necessary.

QUESTIONS TO ASK YOUR TEAM:

- Who has administrative privileges? Why does each one need those privileges? If they do need admin rights, are they always logged in as ‘admin’ (bad) or do they log in as an unprivileged user whose permissions are elevated only when needed (good)?
- Do you practice “separation of duties”? Is the person in Finance who requests wire transfers the same person that approves them?
- Are you aware of employees using risky workarounds? Why do they resort to them? How can this be prevented? Is there a problem with a process, software, or lack of training?
- What is our password policy? Where are the keys?
- Is our password policy enforced? Do you regularly check to make sure there are no forgotten exceptions, such as a clicked “Bypass MFA” checkbox?
- Do you audit user accounts and access controls regularly?
- Do we have procedures for disposing sensitive data that’s no longer needed?
- What are the exit procedures for people leaving our employ?

3. STRANGER DANGER: SOCIAL ENGINEERING AND PHISHING

No one likes to be conned, but it happens all the time. Social engineering, a non-technical tactic for tricking people into breaking security procedures, can look something like this:

- “Comcast” calls to verify your account information before they run a speed test
- A person wearing an official-looking badge needs access to your server room for an electrical inspection
- A “CEO” emailing asking you to send a gift card to a “customer”
- A “board member” calls asking you to reset their account because they forgot their username and password

More than two-thirds of cyberespionage incidents reported in the last two years involved phishing. More than two-thirds! In phishing attempts, people are tricked into downloading malware (malicious software) via a bad attachment or link, or providing access to network or account information by emails, text messages, and websites that look real but are actually fake.

Associations have been and continue to be victims to phishing attacks. Staff received short, simple emails from the “CEO” requesting account information for wire transfers or W-2 information. More recently, staff have been asked by the “CEO” to send a membership list to a legit work email address but also to a phony hacker-owned address.

Another common phishing tactic is to send the victim an email that appears to be from a co-worker. The “co-worker” asks the victim to review an attached memo or to check out a website URL. Too often, the phishing target opens the infected email attachment or clicks on the link to the compromised website, thus exposing their computer and their association’s network to malware.

Any one of us could fall for a phishing ploy. The security company McAfee sent a ten-question Phishing Quiz to more than 30,000 of their customers. 80% of them fell for at least one phishing email in the quiz—only 3% aced the test. You can have the strongest perimeter defense possible, but it only takes one person to click on a malware link for an outside agent to get into your network.

QUESTIONS TO ASK YOUR IT TEAM:

- Should we hire a company to provide social engineering training for our staff?
- Should we educate our members about phishing? Should we tell them to be wary of attempts to request private information, such as usernames and passwords?
- Are we using modern email security practices such as SPF, DKIM, DMARC?
- Do we appropriately label external (read: potentially dangerous) email coming into our organization?
- What are the risks of publishing staff titles and email addresses online?

4. BRING-YOUR-OWN-DEVICE (BYOD)

IT departments must find the right balance between the organization's need for security and the staff's need for productivity. A good BYOD policy walks this fine line. Because mobile devices are entry points into your network, employees must understand their BYOD responsibilities (and rights) and comply with your BYOD security policies, especially the procedures to follow if their device is lost or stolen.

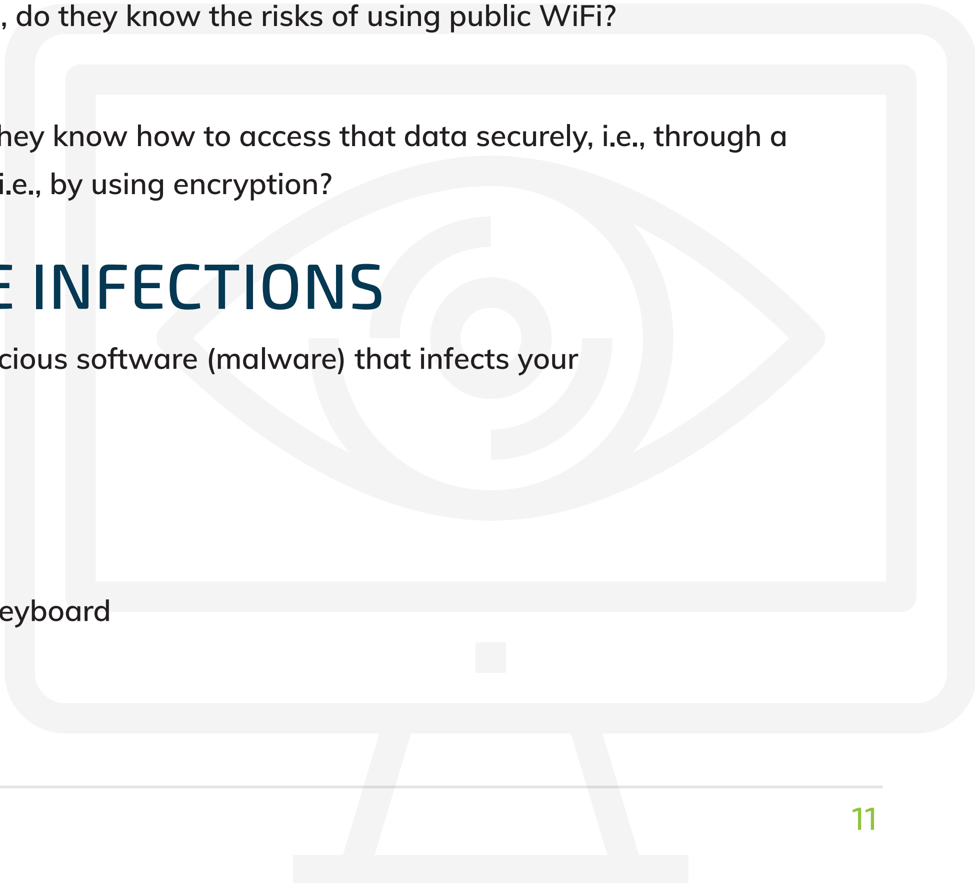
QUESTIONS TO ASK YOUR IT TEAM:

- Are we using mobile management software?
- Do employees understand their security responsibilities?
- Do employees know how to use their mobile devices safely? For example, do they know the risks of using public WiFi? Are their devices password-protected?
- Do they know what type of data may be accessed on their devices? Do they know how to access that data securely, i.e., through a secure network? Do they know how to store and transmit data securely, i.e., by using encryption?

5. TERMINAL CONDITION: MALWARE INFECTIONS

One consequence of a successful phishing attempt is the installation of malicious software (malware) that infects your computer and network, for example:

- Viruses—malware that infects and modifies other programs
- Worms—stand-alone, self-propagating malware
- Keyloggers—malware that surreptitiously records the keys struck on a keyboard
- Trojan horses—malware that misleads users of its true intent



- Spyware—malware that tracks and stores web activity

Malware was a factor in more than 50% of data breaches over the past three years. It's used for all types of mayhem, including data extraction, extortion, and the manipulation of computers and servers so they can be used for another attack.

MALWARE IS DOWNLOADED WITHOUT YOUR KNOWLEDGE OR CONSENT WHEN YOU:

- Open an infected email attachment
- Click on an infected advertisement (malvertising)
- Visit a compromised website that downloads a malicious executable file—a file that instructs the computer to perform specific tasks
- Use an infected removable device, like a thumb drive
- Use a network that's connected to an infected computer
- When one computer on a network is infected, malware spreads quickly, especially if users are logged in with administrative rights.

Take note: Java, Adobe Flash, and Internet Explorer are frequently exploited targets for malware because of 'security holes' in the software that hackers exploit before the software companies can fix them. These holes are called 'zero day vulnerabilities.'

QUESTIONS TO ASK YOUR IT TEAM:

- Do users have local administrative rights? Why?
- Is endpoint security (antivirus, antimalware) software centrally managed? Can you get reports on individual machines?
- Do you have antivirus on servers too?
- Do you have a software-based firewall enabled? (A firewall is a security system that monitors and controls incoming and outgoing network traffic)
- Firewalls are still important, but in the age of remote-work, mobile-first, cloud-first IT, the "action" is happening at the endpoint. Do we

have the software and staffing in place to detect breaches at the endpoint and contain them quickly?

- How old is our firewall software? (You should replace firewall software every three to four years to take advantage of new security technology)
- Does the firewall have deep packet inspection (DPI)? (DPI means the packets of data being sent and received by network users are inspected)
- Does the firewall have an intrusion detection and prevention system? (This technology leverages DPI to identify and block known exploits)
- Do you have gateway antivirus software installed? (This perimeter-based protection controls access to all entry and exit points of the network)
- Are we using the same password for multiple accounts, for example, firewall, switches (used to receive, process, and forward data within your network), and such?
- How are we protecting our IT assets outside the local network?
- Have we implemented a multi-layered approach to security with multiple security solutions in place? (Relying on only antivirus and firewall software will not get the job done)

6. WEB OR BROWSER ATTACKS

Has your browser ever delivered the message, “This site may harm your computer,” before taking you to a website?
Sometimes you’ll even see this warning in Google search results. This warning occurs when a legitimate website has been compromised by malware.

If you make the mistake of visiting a website that’s been infected by malicious code, usually you’re redirected without your noticing to a website controlled by hackers. This site hosts malware packaged in an ‘exploit kit’ that probes your computer’s operating system, browser,

browser plug-ins, and other software (like a PDF reader) to find a security vulnerability. You're then encouraged to download malware disguised as a software update.

QUESTIONS TO ASK YOUR IT TEAM:

- Is network activity being monitored? Are you using network security software to provide phishing protection and optional content filtering?
- Do you have the ability to block download executables? For example, are you using software to restrict the types of executables that can run on computers?
- Should we be using ad blockers? (Ad blocking software is used to remove or alter advertising content on a web page)

7. POOR PATCH MANAGEMENT PRACTICES

We heard a story through the grapevine about a professional society with an old version of web design software installed on a web server that was hardly used, and hadn't been patched (updated) in ages. And, you guessed it, the server was hacked. They got this bad news when the FBI called.

Most computer attacks exploit well-known vulnerabilities for which patches exist. A patch is a piece of software published by the developer to fix or improve a computer program, for example, to fix a security vulnerability or some other bug (error).
However, if your IT team isn't regularly and consistently updating patches, you leave your network exposed to security breaches.

QUESTIONS TO ASK YOUR IT TEAM:

- Are software patches and updates automatically downloaded and installed on all computers?
- How are you centrally managing Windows updates?
- How are you managing third-party updates, like Java and Flash, which are more likely to be exploited?
- How do we handle out-of-compliance machines?

8. UNSUPPORTED SOFTWARE

Microsoft ended support for 7 and Windows Server 2008 R2 in January, 2020. Support for Windows 2012 R2 ends in April, 2023. Since Microsoft no longer provides patches for security vulnerabilities, you're at risk of opening up your network to viruses and malware if you continue to use unsupported software. Likewise, VMWare ended support for ESXi 6.0 in March, 2020, with ESXi 6.5 and 6.7 ending in October, 2022.

QUESTIONS TO ASK YOUR IT TEAM:

- Are we using any software that is no longer supported?
- What is our plan to decommission old and vulnerable servers?

9. FRIENDS OR FRENEMIES: THIRD-PARTY NETWORK ACCESS

Think about the companies that have access to your network. How well do you trust their security practices? Well enough to trust them with your data? It's time to have a discussion about security with your website designer, web application developers, website host, and any other third-party support provider for business-line applications—such as your AMS, CRM, financial management, collaboration software, and other systems. We regularly see a vendor simply request, and receive, "domain admin" access when all they need is to install software on a single server.

Example related horror stories: A vendor was used to manage a phone system. The vendor used the same password for all customers! One customer got compromised and hackers used that same password to attack all the other customers. In another situation, a vendor was managing backups, got ransomwared, and the customer's backups got locked up. Both happened in 2019/2020.

Your organization should have the following policies and procedures in place to help administer vendor access and reduce the risk of a data breach.

- Do you have a vendor checklist that includes cybersecurity questions? Does security play a role in the vendor selection process and contract review process?

- Establish a documented method for vendors requesting access to your network
- Do not provide too many privileges. Vendors will most likely need administrator level access on the systems that host their applications, but they should not need elevated access across other systems in your organization
- Require resets for their passwords, just like all your other employees
- Request information from your vendors about how they store the credentials to access your system and who has access to those credentials

Review your vendor contracts to make sure they include data security commitments and warranties. Make it clear to your vendors that they must take security seriously.

QUESTIONS TO ASK YOUR IT TEAM:

- Which vendors have access to our network? Have you discussed security with them?
- What warranties or protections do our vendors offer in the event of their negligence? Do they carry errors and omissions coverage to protect us against claims stemming from their negligence?
- Do we automatically give ‘domain admin’ access to any vendor?
- Do you enable and disable accounts as needed, or leave accounts open?
- Do you use audit logging? (An audit log records all ‘events’ in an IT system: resources accessed, destination and source addresses, timestamp, and user login information)

10. HOSTAGE SITUATION: RANSOMWARE

Ransomware accounts for 27% of all malware incidents, and the number keeps going up. The hacking of the Colonial Pipeline, an American oil pipeline system, in May of 2021 is a highly visible example. Ransomware is crippling malware that encrypts files on a computer’s hard drive and any external or shared network drives to which the computer has access. It directs the user to a personalized ransom page that announces the initial ransom amount, detailed instructions for purchasing Bitcoins to pay the ransom, and a countdown clock to notify victims how much time they have to pay before the ransom doubles.

Here's the rub: even if you pay, you may not get your files back. You can avoid having to pay ransoms by backing up all your data regularly. If you have backups, ransomware becomes an inconvenience, not a catastrophe.

QUESTIONS TO ASK YOUR IT TEAM:

- Do we have off-site and/or cloud backups of all critical data?
- Do we have multiple layers or systems of backups, for example, traditional online backups and server shadow copies? (Shadow copies are automated point-in-time copies of files located on shared resources, such as servers)
- Do we test data restoration regularly?
- How long does it take to do a full restoration of all files?
- Is our shared drive segmented and therefore limiting ransomware damage, or would our entire organization be affected by a ransomware attack?
- What about our vendors? What's the backup policy of our AMS or LMS vendor? How often do they test and restore? Are their recovery time objectives defined in our contract with them?

11. OUCH: SQL INJECTION

About half of all data breaches are caused by SQL injections—an especially common attack against credit card databases. When a web application (software that runs in a web browser) is not written securely, hackers can 'inject' malicious code (SQL commands) into it. These commands give the hackers access to the application's database. Because most application codes are proprietary and specific to the application, their vulnerabilities aren't known and, therefore, can't be protected by security defense systems.

The use of two-factor authentication by employees and customers for web applications adds a second layer of protection and is available on many of the most common applications we use today.

QUESTIONS TO ASK YOUR IT TEAM:

- Do you regularly test our SQL servers for vulnerabilities? Do you follow up on the results? Do you have a third party check them?
- What steps have we taken to harden (enhance the security of) our web/application server? How are we ensuring web app security? How are we protecting our members' and customers' data?
- Do you use input sanitization for web apps that integrate with databases? Input sanitization ensures that any input, such as a website login, is cleansed of harmful data and prevented from executing unauthorized actions
- Is traffic to and from our site encrypted?
- Do we have a web application firewall (WAF)?

12. ZOMBIE APOCALYPSE: BOTNETS

A botnet is a group of infected computers, also known as a zombie army, that are remotely controlled by a hacker. These computers are used to send emails containing viruses or malware to other computers, or to participate in attacks against other systems.

QUESTIONS TO ASK YOUR IT TEAM:

- Will you know if one of our computers becomes compromised and is being used for malicious activity?
- Do you have the ability to block suspicious outbound traffic?

13. DISTRIBUTED DENIAL-OF-SERVICE ATTACKS (DDOS ATTACKS)

When one of your computers becomes part of a network of zombie computers (botnet), a hacker can use it to inflict pain on others. For example, hackers could make an employee's hijacked computer (along with thousands, or even millions, of other zombie computers) inundate another network or server with useless external communication requests—a distributed denial-of-service attack (DDoS attack). The sole intent of these attacks is to bring a network or server down and make it unavailable to its users. You don't want any of your computers to be the cause of someone else's misery.

QUESTIONS TO ASK YOUR IT TEAM:

- What DDoS protection do we have in place?
- Do we have any DDoS protection on our web servers, for example, are we using Cloudflare?

14. MORE PAIN: SPAM OR EMAIL INJECTION

Hackers use search robots to scan the web looking for vulnerable website forms, for example, 'Contact Us' forms that are based on poorly written code or code that hasn't been updated with security fixes. In a spam or email injection, the attacker 'injects' or inserts malicious code into a form's email header fields (for example, the BCC, CC, and Subject fields) and then uses the victim's email server to send thousands of spam emails.

If your email server is hijacked in this way, it will likely get blacklisted. Your legitimate emails will be blocked by other servers until you can prove you've fixed the security issue and stopped the delivery of spam from your email server.

QUESTIONS TO ASK YOUR IT TEAM:

- Is our form app regularly updated by the developer? Are we applying those patches?
- Is the data submitted via forms validated or sanitized?

15. WEB SERVER HACKING

In the last year, we've read about hackers gaining access to the web servers of a few national trade associations. One incident involved the association's online bookstore. Hackers inserted malware on the server—a server maintained by a third party. Credit and debit card numbers, expiration dates, security codes, and cardholder names were compromised.

If hackers gains access to your web server, they can steal data, bring down your website, and/or use your server in a DDoS or some other type of attack. Don't assume your IT department is running your web server. If your marketing department runs the website, a third party could be hosting it.

QUESTIONS TO ASK YOUR IT TEAM:

- Are we protecting our web applications using WAF?
- Do you know about all the web servers and microsites our association is running?
- Who owns and manages those web servers?
- If a third party is hosting one of our web servers, are they responsible for breaches?
- Should we consider moving away from on-premise servers to hosted solutions that come with security experts?

16. BRUTE FORCE ATTACKS

If you Google "top 25 most common passwords" and see your password on the list, you need to change your password and your password habits immediately. 80% of data breaches involve exploitation of stolen, weak, or default passwords. Encourage employees to use a password management tool if that's what it takes to get them to use smarter and safer passwords. Don't be low-hanging fruit for bots.

Automated and malicious bots are constantly engaged in trial-and-error attempts to guess system passwords, otherwise known as brute force attacks. They keep trying username/password combinations until they hit upon one that works. If an attacker gains access to your email, they can then reset passwords for all your other accounts—locking you out.

QUESTIONS TO ASK YOUR IT TEAM:

- Do we use unique passwords for each account?

- Do we use two-factor authentication everywhere?
- Do we use lockout timers when possible?
- Do you get alerts when logins fail?
- Do we use and offer password management database tools to our staff?

17. POINT-OF-SALE (POS) INTRUSIONS AND PAYMENT CARD SKIMMERS

Although point-of-sale (POS) intrusions are increasingly more common in retail, restaurant, and lodging environments, you must guard your credit card readers when using them at conferences, tradeshows, and other events. Hackers have created sophisticated skimmers that fit inside credit card readers so they can steal credit and ATM card data, PCI card data, and PIN numbers.

In a typical POS intrusion, the hacker compromises the POS device, installs malware to collect the magnetic stripe data of cards, and then retrieves the data. In the past, only card issuers were liable for this type of fraud. However, as of October 2015, that liability shifted to merchants if they hadn't replaced or upgraded their card acceptance and processing systems to use EMV chip-enabled devices and applications.

QUESTIONS TO ASK YOUR IT TEAM:

- Are we using a third-party system to handle credit card information? Are we collecting and storing credit card information ourselves?
- Are we using the most secure solution?
- Have we upgraded our equipment to accept EMV chip-enabled cards?
- Is fraud monitoring in place?

FINAL THOUGHTS

Cybersecurity requires constant vigilance—you can't ramp up, set it, and forget it. Keeping your data and network secure requires a defensive and proactive approach from everyone on staff, not only the IT department. One person's careless or innocent slip could expose your data and network to catastrophic damage.

Maintaining your organization's cybersecurity is a multifaceted approach that requires vigilance. If, after reviewing this cybersecurity watchlist, you don't know where to start (or you're simply petrified), contact us for a security assessment.

DelCor Technology Solutions
8380 Colesville Road #550 Silver Spring, MD 20910
20 West Kinzie Street Chicago, IL 60654
877.4.DELCOR | 301.585.4222
www.delcor.com