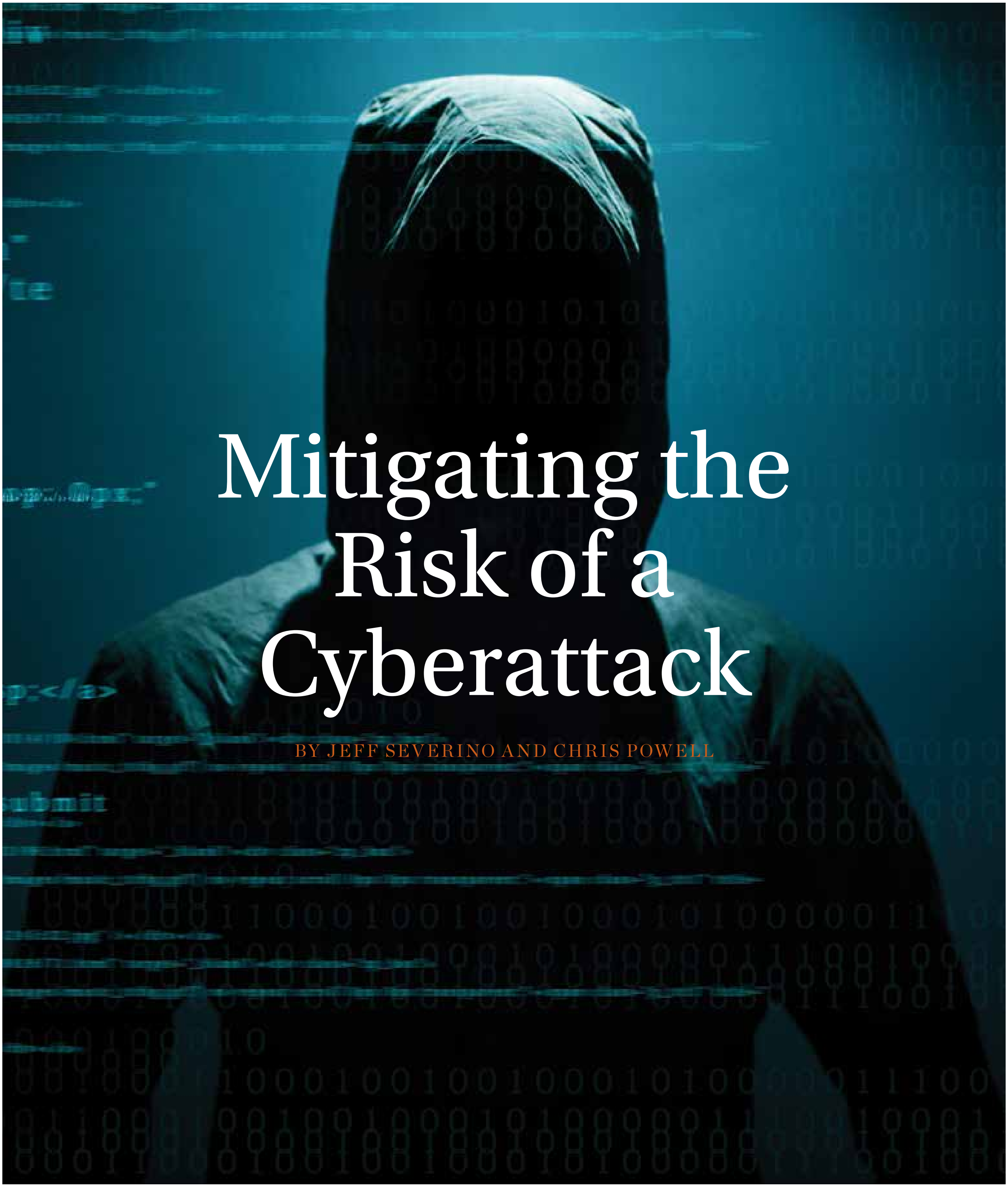


Mitigating the Risk of a Cyberattack

BY JEFF SEVERINO AND CHRIS POWELL

WHOOPS, our firm chose not to evaluate and purchase cyber insurance coverage. What could go wrong? A civil suit? An investigation by the Office of Attorney Regulation Counsel? Or worse, losing business for days or weeks or longer because a ransomware hacker locked us out of our files? The following discussion is presented courtesy of CNA and Lockton Affinity, the CBA's endorsed malpractice carrier and broker.

Over the last few years, the number of serious cyberattacks targeting law firms has surged, with hacks costing hundreds of millions of dollars and exposing sensitive client data. A cyberattack can cripple a firm's ability to operate and cause lasting harm to its reputation. Unfortunately, many advanced cybersecurity solutions are costly and difficult to implement, making the typical law firm a prime target for cybercriminals.

One way to mitigate the increased risk of cyberattacks is to look to no-cost and low-cost solutions that can offer an immediate risk management benefit without added expense or complexity. Below are 12 no-cost or low-cost ways to help prevent cyberattacks on your business.

1. Identify Key Accounts and Systems.

An inventory of your vulnerabilities can help illuminate opportunities to protect them. Take a few minutes to think through all the key accounts and systems vital to your business. Ask yourself if you could continue to operate without issue if something were to happen to them. Jotting down a few notes about protecting these key vulnerabilities is a great place to start as you put your cyber risk management plan together.

2. Establish a Written Funds Transfer Policy.

Your digital financial transactions are a primary target for cybercriminals. A funds transfer policy can help minimize your risk. Follow these steps before any funds transfer:

- Require verbal verification of all new account numbers and any previously verified account number that has changed for any reason.
- Require the other party to recite their account number to your employee while on the phone.
- Train any employees that have the ability to transfer funds on behalf of the business to follow the policy according to these procedures.

> **Backups stored alongside your other data on the same network are little help in the event of a cyberattack. If your network is compromised, you want to make sure your backups remain unaffected.**

3. Implement Remote Access MFA.

Cybersecurity experts now recommend enabling multi-factor authentication (MFA) to mitigate the risk of unauthorized remote access to your computer network, accounts, and systems. This built-in security feature works by disallowing remote access without standard MFA verifications. For many networks, it's as easy as turning on a setting that enables MFA for anyone who will be remote accessing your computer network.

4. Carry Out Patch and Update Maintenance.

Patch and update maintenance is important for cyber risk protection as new software vulnerabilities are regularly discovered. Here are three ways to protect your firm:

- Take an inventory of devices, systems, and applications and update where needed.
- Create a process to regularly download, test, and install patches within 30 days of release on your computer network.
- Audit your network to ensure patches and updates are successful, and monitor for future releases.

5. Back Up All Computer Systems and Data.

A cyberattack can result in the loss or theft of your firm's trade secrets, client data, and financial credentials. This can cause a truly great deal of damage from which it's difficult to recover, so having adequate backup system protections in place is crucial. It's fairly easy to implement a system that will handle backups for you automatically. Back up all the systems and data on your network at least weekly.

6. Isolate Backups from Your Primary Network.

Backups stored alongside your other data on the same network are little help in the event of a cyberattack. If your network is compromised, you want to make sure your backups remain unaffected. It's best to keep multiple, redundant backups stored fully isolated from your primary network and in a separate geographic location to avoid contamination in the event of a network intrusion.

7. Remove Unsupported Operating System Versions.

Many popular operating system versions are no longer supported by their developers. That means companies no longer make or release updates to patch their security vulnerabilities. Examples of unsupported operating systems include Microsoft Windows 7 and Microsoft Windows Server 2008. It's important to depreciate these versions and upgrade to supported operating systems. Even one unsupported system connected to your network can compromise the whole network.

8. Scan and Filter Content on the Network.

Incoming emails and files can contain viruses that easily infect your computer and spread throughout your whole network. Often, all that's required is to open a suspicious email or download an attachment. A simple solution is to activate security features to scan and filter email and web content for malicious items. The security system can quarantine the item and alert your administrator that a problem has been detected.

9. Use Tools to Authenticate Incoming Mail.

Special tools such as Domain Keys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-Based Message Authentication, Reporting & Conformance (DMARC) exist that can authenticate incoming email and prevent phishing attacks. This one can be tricky, so don't despair if your first thought on seeing "SPF" is sunscreen. Your IT staff or network/server administrator should be able to recognize these options.

10. Secure or Disable All RDP Endpoints.

Remote Desktop Protocol (RDP) is a popular Microsoft Windows component used to connect to a computer remotely that can introduce serious security vulnerabilities if improperly configured. Either protect your RDP with MFA or disable it on all network endpoints.

11. Encrypt All Sensitive and Confidential Information.

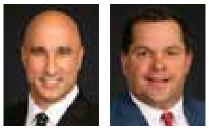
Data encryption is an essential tool that automatically scrambles data to protect it from prying eyes and unscrambles the same data so that authorized parties can work with it. Computer systems, software applications, and online services all have built-in settings to turn on encryption while data is "at rest" and "in-transit." In addition, most email providers can add specific encryption when needed.

12. Restrict Network Administrative Privileges.

Computer networks rely on a hierarchical system of access levels to help protect critical parts of the network from both accidental and intentional alterations. Having administrative privileges allows a user to make changes to the system, such as downloading software onto the computer network. Limit the number of employees with these high-level privileges to a select few to protect the system.

Conclusion

With these simple no-cost and low-cost solutions, you can significantly reduce the risk of a cyber-attack impacting your business. Your cyber risk management planning should also include purchasing the right cyber liability insurance policy.[1]



Jeff Severino and **Chris Powell** are senior vice presidents with Lockton Affinity, where they provide leadership to position Lockton Affinity at the forefront of the program insurance industry and deliver strategy to advance the Lawyers Professional Liability and Cyber Liability practices. Lockton Affinity has partnered with CNA to create an insurance program designed specifically for CBA members.

Coordinating Editor: Chris Little, clittle7892@gmail.com

NOTE

[1] CyberLock Lawyer, Lockton's law firm specific cyber insurance program, is designed exclusively for law firms. For more information, contact Jeff Severino, Lockton Affinity, LLC, at (913) 652-7520 or jseverino@locktonaffinity.com.