Fred C. Church
INSURANCE
EST. 1865

A CYBERSECURITY GUIDE:
Six ways to protect your business from cyberattacks and how they impact your organization's cyber insurance.

BY TOM O'NEIL, MANAGEMENT LIABILITY COVERAGE SPECIALIST, FRED C. CHURCH

Whether you have already gone through your business insurance renewal this year, or it is upcoming, you have likely heard about the challenges taking place in the cyber insurance marketplace. The frequency and severity of business cyberattack claims, particularly ransomware claims, have forced cyber insurance providers to respond by imposing significant changes to policy terms, pricing, and underwriting requirements.

With cyberattacks occurring more frequently and the implications so severe, network security is no longer just an IT issue. Much like employee safety or safe driving programs, network security is an enterprise-wide risk management concern where management, IT, and staff all play an important role.

To help guide our clients and business associates, Fred C. Church pulled together six of the top network cyber risks and the cybersecurity implementations that insurers are most concerned with today.

1. Securing your email.

Email is how most businesses communicate both internally and externally with employees, clients, vendors, and other outside contacts. Running your business without it is next to impossible. Unfortunately, it's one of the most vulnerable access points in your system and how many bad actors get in.

According to the 2020 Internet Crime Report published by the FBI, business email compromise (BEC), also called email account compromise (EAC), is the No. 1 loss reported ($1.8 billion) of all online scams, surpassing phishing scams ($54 million) by more than 3,000%. Addressing email security is an important tactic that carriers will look at when you enter the cyber insurance marketplace.

Risk Management Guidance

Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are forms of email authentication that help protect email users from phishing attacks, spoofing, or spam by verifying the legitimacy of the email sender. Make sure these are implemented in your email system.

For additional security, enable Domain-Based Message Authentication, Reporting and Conformance (DMARC), which ties SPF and DKIM together and provides instructions for how a receiving email server should handle the data found in your SPF and DKIM configurations. DMARC can also be configured to send reports to you on email spoofing attempts.

2. Using multi-factor authentication.

Multi-factor authentication (MFA) is a system for securing your accounts by requiring multiple forms of verification to prove your identity when logging into an application. In a time when bad actors are targeting businesses based on their security controls (or lack thereof) rather than on the information that they might have stored on their network, MFA is the best means for keeping the cybercriminals out.

Risk Management Guidance

Carriers will look to see MFA implemented on all business-critical systems, but with a particular focus on MFA for remote access to email, remote network access, and privileged/administrative access.

Organizations using Google and Microsoft 365 for email can implement MFA on employee accounts simply by changing the settings through their administrative account (see Google Instructions or Microsoft 365 Instructions). Many third-party accounts have a setting that allows you to require MFA when logging in. And finally, consider an MFA solution from a reputable security provider, such as Microsoft's Azure, Duo Security, or Okta.

3. Backing up your data.

Maintaining timely and comprehensive data backups is something that many cyber insurance carriers require. Implementing a good data and system backup plan is a critical step to recovering from and reducing the severity of a ransomware attack.

Risk Management Guidance

Data backups should be encrypted. If a bad actor can gain access to your systems and start manipulating data, it can cause even more problems when you go to restore your systems.

Separate data backups from the primary network. You can do this in two different ways, using either an offline backup that is different from the primary network or a cloud backup solution. You can also use a combination of the two.

Test your backups. It's good to know how quickly you can restore the data and your systems, in the event of a cyberattack. Implementing a routine test to ensure that everything works properly after restoring a full system backup is a critical step in your mitigation efforts.

4. Implementing security awareness training programs.

Cybersecurity requires a culture that holds employees, IT teams, and management alike accountable for their role in protecting their company, its data, and any client information they hold. Any organization is one momentary lapse in judgement away from opening the door to a bad actor who could ultimately carry out a ransomware attack. Cyber insurance carriers often require ongoing employee cybersecurity training.

Risk Management Guidance

Implement a monthly training for your employees to identify and report suspicious emails using a combination of training videos, simulated phishing attacks, and a suspicious email reporting plugin to your email system. There are several vendors who provide these services, including KnowBe4, Proofpoint, and Curricula.

> In its 2021 Benchmarking Report on phishing, KnowBe4 reported 31.4% of users with no security awareness training clicked a simulated phishing attempt email. That means almost 1 in 3 users clicked when they should not have – alarming, considering it only takes one click for the bad actors to get in. KnowBe4 also reported that, for users after 90 days of participating in their security awareness program, 16.4% clicked when they shouldn't have. And, after one year, only 4.8% clicked when they shouldn't have.
>
> Verizon's 2021 Data Breach Investigations Report shows that phishing continues to be the top threat action used in successful breaches. About 85% of breaches were linked to stolen login credentials that were obtained using social engineering schemes. The FBI reported that the frequency of phishing incidents nearly doubled from 114,702 in 2019 to 241,324 in 2020. All indications are that frequency is worsening in 2021, and this unfortunate trend shows no sign of changing.

5. Scanning for malicious software.

With the increase in the number of endpoints that an organization has (instances where a device such as a desktop, laptop, or phone is connected to the network), coupled with more sophisticated cyberattacks, insurance carriers are looking for businesses to require more advanced antivirus protection programs that can identify and prevent threats.

Risk Management Guidance

Endpoint detection and response (EDR) is a relatively new technology that addresses the need for 24/7 monitoring and response of your network's endpoints. Examples of companies offering this software include Sophos, SentinelOne, McAfee, Carbon Black, FireEye, and Microsoft Defender for Endpoint.

6. Having an incident response plan.

Despite your best efforts and security implementations, cybercriminals can still get in. When they do, it is important that the organization know how to manage the response. Having a cyber incident response plan can help reduce the chaos brought on by a cyberattack and can potentially reduce the severity of the loss, as well. Plans like these are looked upon favorably in the cyber insurance marketplace.

Risk Management Guidance

Your incident response plan should incorporate reporting a breach to your insurance agent and carrier as soon as possible. Many carriers have incident response teams standing by 24/7. The sooner they are aware of the breach, the sooner they can help you bring in experts who can potentially mitigate the damages.

You should regularly test your incident response plan. One way to do this is by facilitating a tabletop exercise with those team members who are a part of the incident response plan. Make sure everyone knows their role and that the plan is keeping up with any developing best practices or new security implementations you may have added.

In their Incident Response white paper, "You've Been Breached—Now What?", CrowdStrike, a leading provider of incident response services, says not to unplug your system when you become aware of a breach. It's likely that the bad actor has been in the system for some time, and unplugging will either tip them off and cause them to install additional malware or can damage important forensic evidence needed for remediating the damage.

It's important to note that this is an evolving marketplace and these six steps are just a sampling of ways you can improve your company's cybersecurity measures and be more attractive to cyber insurance carriers. The lack of a particular security implementation at your business four months ago may have been of no consequence at renewal, but today it could be a requirement on a cyber insurance policy.

While the cyber insurance marketplace is facing unprecedented changes, insurance policies with broad coverage terms are still available for those businesses that are taking care to keep up to date with these cyber security implementations and risk management steps. While the guidance outlined is a good place to start to help prevent a cyberattack, we are now at a point where such security controls and procedures must be continually assessed and adapted as a part of your organization's overall risk management in order to safeguard your company from becoming a victim of cybercrime.

About the Author

Tom O'Neill joined Fred C. Church in 2019 as the coverage specialist for Cyber, Management Liability, and Professional Liability coverage lines. In coordination with the commercial insurance marketing team, he consults with clients about their risk management strategies and negotiates coverage programs with our partner carriers.

About Fred C. Church

Fred C. Church Insurance is one of the largest firms in the Northeast and one of the top 100 full-service brokerages in the United States. We offer property & casualty and employee benefits solutions, risk management consulting services, and private client asset protection. With over 155 years of industry experience, multiple locations throughout New England and Colorado, and 165 full-time insurance professionals, risk consultants, and claims advocates, we deliver a superior customer experience. Through our hands-on approach, strategically developed to identify, assess, and address risk, we provide personal and business clients of any size and specialty with the advice and guidance they need to make informed decisions about their insurance.