CYBER LIABILITY INSURANCE:
Protect Yourself in 2023

Unions, multiemployer and governmental benefit funds, and joint apprenticeship training committees (JATCs) should review the latest cybersecurity risk management guidance to protect their data in addition to purchasing broad cyber liability insurance.

Ullico Casualty Group offers the following brief as a tool to help insureds plan their next steps. The sooner that brokers, clients and vendors begin discussions about risk mitigation, the smoother the policy renewal process will go.

MORE CYBER ATTACKS THAN EVER

Cyber attacks increased dramatically as organizations shifted to remote work environments during the pandemic. It's more important than ever to understand the types of attacks that occur and how to minimize your organization's vulnerabilities to them.

Types of attacks:

PHISHING

Phishing is the most common method of attack. Phishing involves the sending of a phony email with the goal of getting the recipient to provide sensitive information (like Social Security number or credit card information) and/or tricking them into clicking a link designed to trick the user into providing their password or downloading malicious software.

RANSOMWARE

Ransomware is usually the result of a phishing attack. Ransomware is software that gets loaded onto a machine, and then locks the machine and the data on it. The only way to unlock the machine and the information on it is to pay the ransomer, typically in an anonymous currency such as Bitcoin.

SUPPLY-CHAIN ATTACK

The most recent breaches of both government and private sector entities involve a supply-chain attack. In this case, attackers were able to add malware into a known software manufacturer's product. When that vendor released their standard upgrade, it contained the malware, which proliferated it to all that vendor's customers. The attackers could then use that malware to attempt to steal credentials and information from that entire customer base.

HOW TO MINIMIZE YOUR RISK

Cyber security is a constant arms race between security providers and bad actors looking to circumvent defenses. A layered security approach is essential to mitigating your risk; in the event one layer fails, the other layers in place can prevent or at least mitigate the possible damage.

MULTIFACTOR AUTHENTICATION:

Passwords are only a single factor of defense, and they can be easily stolen or cracked. Having multiple factors to access information is now critical, and already in place by many organizations such as banks. The additional factor is typically linked to something you own that cannot be shared, like a fingerprint or phone (SMS or mobile app verification). Key vendors in this area are Duo and Okta.

FIREWALLS:

At one time, firewalls were the only requirement for cyber security. Now, many more components are required for truly robust cyber protection, but firewalls are still a necessity. They exist as both physical and virtual hardware and act as a barrier between your network and the internet, only allowing trusted connections to come in or out. They have also transformed over time to perform a multitude of other functions, such as website filtering, intrusion detection, etc. Key vendors in the area include Cisco and Fortinet.

ANTI-VIRUS/ANTI-MALWARE SOFTWARE:

Like firewalls, anti-virus (A/V) was once all that was needed on a computer to prevent harm. Also like firewalls, this software has undergone a number of changes to become more robust and handle a variety of different functions, such as virus and malware detection, protection, and prevention, data leakage prevention, encryption, and device control. This solution has gone through so much change that it even has a new name: Endpoint Detection and Response (EDR). Key vendors in this area include CrowdStrike, SentinelOne, Carbon Black, Symantec, Sophos and Malwarebytes.

PHISHING EMAIL TESTING & TRAINING:

The proliferation of phishing emails is so prevalent that testing and training has earned its own category. There are systems that allow you to create your own test phishing emails to send to employees, as well as supply training on how to identify and deal with these types of emails. This is critical as many phishing attacks can fool email filters and still be delivered to the recipients. Having a knowledgeable staff is key to identifying and avoiding any damage caused by phishing. A major standalone testing and training vendor in this space is KnowBe4. Mail security vendors, like Mimecast and Proofpoint, also offer testing and training tools as part of their platforms.

ADVANCED THREAT PROTECTION:

If you use cloud-services such as Microsoft Office 365 and Google G-Suite, you should activate the features known as advanced threat protection as soon as possible. These features allow the services to provide additional security checks such as anti-malware and anti-phishing inside of the email services before the messages are even delivered. While these features are built in, they need to be properly configured to function correctly. Third party vendors can also supply and supplement these features, such as Mimecast, Proofpoint and Symantec.

BACK-UP AND OFFSITE STORAGE:

A critical part of data protection is backing up that data, as well as proper storage. A good backup can allow you to recover from an accidental or malicious destruction of data. Storage of the backup is important as well; if your network is compromised and all your backups are stored in the same place as your affected infrastructure, you may not be able to use those backups at all. Keeping a copy of your backups in an off-site or out-of-band area is key to being able to quickly recover from breaches, particularly ransomware attacks. For example,

some organizations back up key data to a server, then back up that server to alternate media such as tape, DVD, etc. and keep it physically separate from the main equipment. This strategy allows you to recover even in the event your main site is inoperable. Key vendors in this space are CommVault, Veeam and Veritas.

DATA SECURITY:
This is the base layer needed to protect your data. This can be anything from a simple password on a file to more complex forms of encryption. Some tools are even built into the operating system, such as Microsoft's Bitlocker.

POLICIES AND PROCEDURES:
All the features above need some form of policy to dictate their use, along with a procedure guide on how to use them. Think of it this way: The procedures are like the user manual for a new blender, explaining how to use it properly.

The policy tells you when it is the right time to make a smoothie or a Bloody Mary. All security policies should undergo a periodic review to make sure they are kept current and meet your security needs. Firms such as Accume Partners can assist with creating and reviewing, as well as testing these policies.

CYBER LIABILITY INSURANCE:
Insurance is a critical part of the arsenal against breaches. The insurance policy acts as the last line of defense and will cover the costs associated with a breach: remediation, recovery and/or implementing new preventative measures. That said, many insurance carriers will require you to have other security layers in place before they issue the policy.