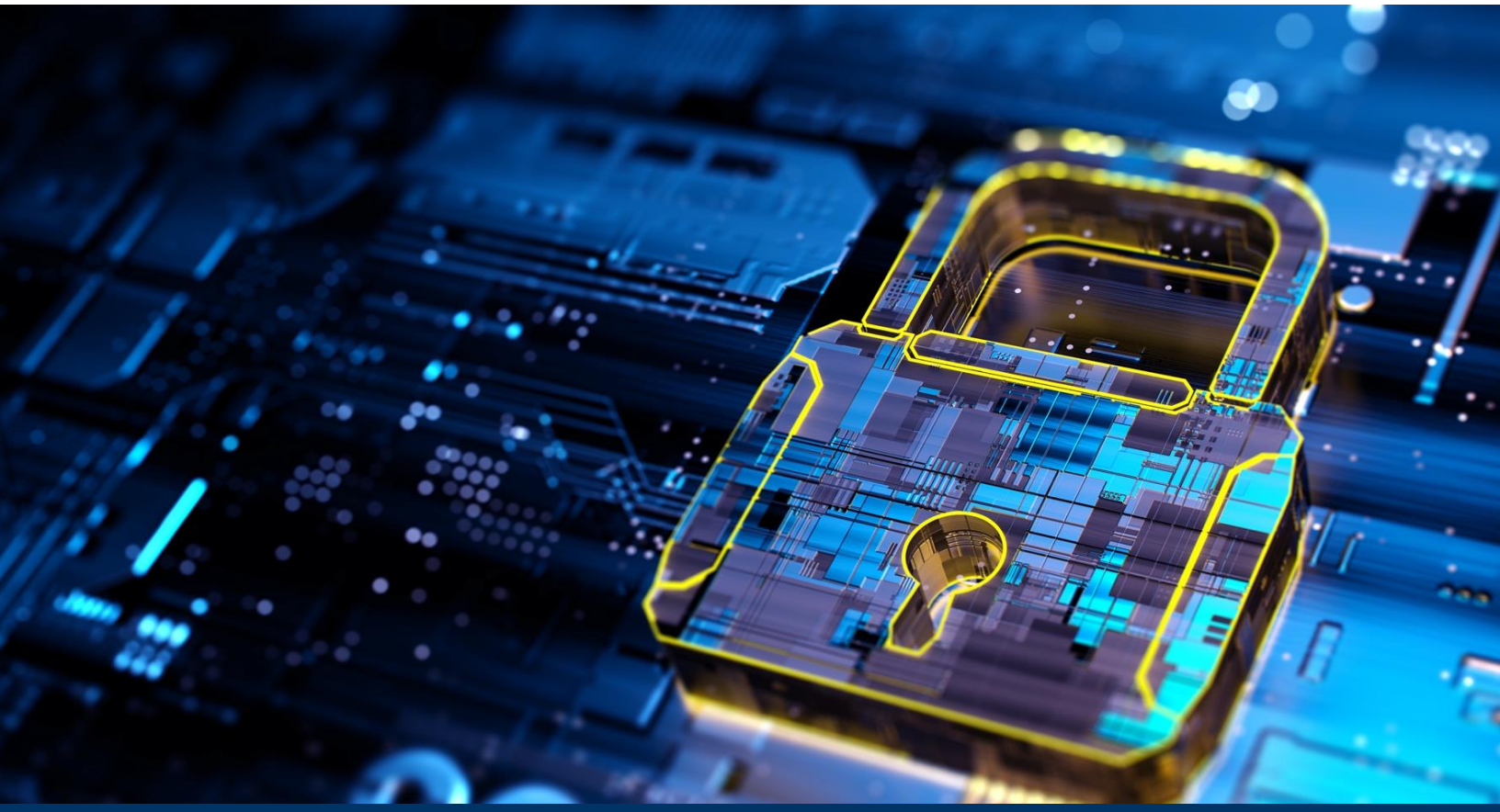
Eastern insurance
JOIN US FOR GOOD®



Cybercrimes Peak Amid Pandemic – Cyber Insurance Offers Protection

March 2021
Eastern Insurance Group

As businesses of all sizes rushed to move operations online in 2020, cybercriminals capitalized on the confusion and uncertainty brought on by the pandemic; cybercrime reports almost quadrupled in 2020.[1] Sensitive types of information, such as customer credit card numbers and employee social security numbers, are hot items for cybercriminals. For the victims, retrieving this lost data, notifying customers and employees, and coordinating with government entities and forensic specialists can be an extremely lengthy and expensive process.

Most common property and liability policies do not provide coverage for most losses and expenses related to cybercrimes. However, cyber privacy and security insurance coverage **can** protect your organization.

Top Four Cybersecurity Threats

The media focuses primarily on larger cyberattacks such as the breaches at Netflix and JP Morgan; however, the most frequent threats have been to small and midsized businesses — and the threats don't stop there. Cybercriminals don't discriminate on industry or organization type. In fact, health care organizations in the U.S. recently experienced a 37% increase in attacks,[2] and local and state governments have seen an increase of 50%.[3]

While all cyberattacks are detrimental to organizations, not all cyberattacks are the same. There are four major categories of cybersecurity threats: 1. Malware attacks, 2. Phishing, 3. Ransomware attacks and 4. Data breaches.

1. MALWARE ATTACKS

Malicious software is installed on a device without the owner's knowledge by a cybercriminal usually looking for financial gain. These attacks can include ransomware, spyware, and viruses.

> "In 2015, the global cost of malware was an already-staggering $500B. Fast-forward to 2021, and cybercrime is costing an estimated **$500B every month.**"
>
> Safety Detectives

In early December 2020, IT software firm SolarWinds experienced a malware attack that exposed thousands of corporate customers, the U.S. Treasury, the State Department, and the Department of Homeland Security. Based on SolarWinds' legal filings, more than 30,000 organizations use the SolarWinds' platform that was attacked and the compromised update was installed by more than 18,000 customers.[4] It's estimated that the insured losses of the attack were upwards of $90M — including incident response and forensic services for those who were impacted by the attack and had cyber insurance coverage.[5] While the losses to uninsured companies affected are still unknown, it's a wake-up call for all organizations and sectors to ensure they have adequate cybersecurity insurance, detection capabilities and incident response plans.

2. RANSOMWARE

Ransomware is a form of malware that encrypts a victim's files – the attacker demands ransom to restore data access and does so after payment is received. Ransom costs can range from several hundred dollars to thousands and are most often payable in cryptocurrency.

Recently, a customer of Eastern Insurance Group (EIG) fell victim to a ransomware attack. The customer's files, software and other technology mediums were locked, and a ransom note was embedded in their systems. The customer's cyber insurance carrier immediately assembled a team of professional negotiators and forensic computer systems experts. Thankfully, our claims division was able to facilitate the immediate threat response promptly and successfully.

> "Ransomware attacks rose **148% globally** in March 2020."
>
> - Fintech News

In this example, the "ransom" ended up being negotiated and paid within three days with digital currency. Once paid, the restoration process began, and the costs associated with the threat were determined. The customer had paid a premium between $15,000 and $20,000 for its policy and the insurance carrier ended up paying out more than $1M.

3. PHISHING ATTACK

A cybercriminal disguises an email or text message as a "weapon." The goal is to trick the recipient into believing the message is important and valid – for example, a bank request or an email from the CEO that leads the victim to click a link or download an attachment.

In one example of a phishing attack, an asset and wealth management firm received a fraudulent invoice for $80,000.[6] The attacker impersonated a known client asking for payment of a recent home renovation project — even attaching a real invoice from the contractor. It was thankfully discovered to be a scam when an employee contacted the client for confirmation. Luckily, the firm had a cybersecurity plan in place to catch this attempted attack — otherwise, depending on its insurance policy, the company could have lost $80,000.

4. DATA BREACH

Confidential or sensitive information is exposed to cybercriminals, which is then viewed and/or shared without permission. Stolen data may include credit card numbers, customer data, trade secrets or matters of national security and can compromise organizations of all sizes.

Trinity Health recently experienced a data breach on the health care system database they utilize, Blackbaud. Patient and donor data was compromised, including names, addresses, donation-date, patient room number and patient insurance information. Blackbaud now faces more than 20 class action cases in the U.S. and Canada related to this attack. Consumers are seeking financial compensation for the time and effort involved in the breach. Consumers hope to push Blackbaud to adopt security practices to safeguard data and prevent issues like this in the future. Blackbaud has already incurred more than $6M in costs and has received roughly $3M in insurance recoveries to date.[7]

How to Protect Your Business and What to Consider

It's no longer a matter of "if" but "when" a business will be the target of a cyberattack. Despite this, many organizations have yet to purchase a cyber insurance policy. Whether that's due to budget constraints amid the pandemic, the assumption that only larger organizations are susceptible or lack of knowledge around cybersecurity insurance — any business that falls victim to an attack will still face consequences.

It was recently reported that only 14% of small businesses have the resources to defend against a cyberattack. Yet 50% of all companies reported a breach in the last year and 60% of companies that suffer an attack are unable to recover and are forced to close their doors within six months.[8]

"In The FBI recently reported that the number of complaints about cyberattacks…is up to as many as **4,000 a day**."

- Yahoo! Finance

UNDERSTANDING YOUR NEEDS

There is no one-size-fits-all cyber liability policy. For each organization, the best choice depends greatly on industry, revenue and number of employees. It's also important to consider the entirety of the cybersecurity incident. Organizations may be faced with more than simply recovering information, including long-term business impacts and financial costs. Take time to evaluate your cyber risks, understand where gaps exist then implement measures to reduce cyber risks — and, ultimately, protect your investment.

"**93% of small businesses** reported having more reliance on technology since the start of the pandemic."

- PropertyCasualty360

When evaluating your risks, ask yourself the following questions:

- Does your business handle sensitive information, such as credit card or social security numbers?
- Is your organization following best encryption and data storage practices?
- Do customers log in to your website or web application where sensitive data resides?
- What third-party vendors do you use? How much access do they have to your IT infrastructure?

Measures to reduce cyber risks:

- Purchase and implement antivirus software, endpoint detection and firewalls.
- Segment your IT systems; it's less likely that cybercriminals will take down an entire system in one attack with segmented systems.
- Test attack response plans. Uncover poorly planned steps that could lead to more damage, expenses and business interruption.

CHOOSING A POLICY FOR YOUR BUSINESS

Taking the above risks into consideration and implementing measures to reduce them will be extremely helpful when determining your organization's cyber insurance needs with your insurance partner. The industry jargon and options available may at first seem overwhelming, but we at Eastern Insurance are here to help you navigate the process.

There are many coverage options to choose from, including:

- **Third-party coverage** – coverage that can pay for your business's legal expenses if a client files a lawsuit after experiencing a data breach. Includes: network security liability, privacy liability, regulatory coverage actions, website media liability and professional liability.
- **First-party coverage** – coverage that helps pay for lawsuits caused by breaches on your own network or system. Includes: privacy breach expenses/crisis management, business interruption, cyber extortion and data loss.
- **Pre-Breach Services** – provides education, protection and detection before a cyber threat. Includes: pre-breach planning, help line and information portal.
- **Post-Breach Services** – assists your company in recovering from a data breach. Includes: legal services, IT support, Identity repair and forensic accounting.

WHAT TO DO IF YOU'VE BEEN A TARGET OF A CYBERCRIME

Once an attack has been made known, time is of the essence to respond — organizations can quickly secure themselves from further damage or dig a deeper hole if they are slow to act. The foundation of a successful cyber incident response is one anchored in preparedness. Next steps should include:

- Report the cybercrime to parties, including IT, financial institutions and the FBI.
- Contain the attack. Determine what has been compromised and ensure additional servers/devices won't be affected. Preserve the confidentiality and integrity of data that has yet to be breached.
- Assess the attack. Identify those affected including employees, customers and third-party vendors. Notify law enforcement if necessary. If you have insurance coverage, contact your insurance carrier and potentially privacy counsel and forensics.
- Manage the fallout and begin recovery efforts. Communicate with staff and define a clear communication plan. Remove all unauthorized software from your network and disable access associated with those who committed the cybercrime.

Good Advises. Good Insures. Good Protects.

An unprecedented combination of circumstances has led to the current cybercrime boom that organizations of all sizes and industries face daily. The pandemic and increased use of technology have changed how businesses interact — and the new reality means greater cyber risks. Even when the pandemic ends and the economy begins to recover, remote work and security risks will remain.

Eastern Insurance Group's knowledgeable professionals have strong relationships with the insurance companies offering the most robust cyber coverage and we partner with our clients as they evaluate their ongoing and ever-changing needs. Contact us today for your cybersecurity insurance needs.

Sources

[1] 5 cybersecurity events that keep CEOs up at night | PropertyCasualty360 (ampproject.org)
[2] Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45% (healthitsecurity.com)
[3] Cyberattacks on state, local government up 50% -- GCN
[4] SEC filings: SolarWinds says 18,000 customers were impacted by recent hack | ZDNet
[5] SolarWinds Hack Could Cost Cyber Insurance Firms $90 Million (crn.com)
[6] How asset management companies are vulnerable to ransomware and phishing attacks - TechRepublic
[7] Blackbaud Expects Cyber Insurer Will Cover Most Attack Costs (careersinfosecurity.eu)
[8] Cyber Security Statistics: Numbers Small Businesses Need to Know - Small Business Trends (smallbiztrends.com)

Eastern Insurance Group LLC is the largest independently owned insurance broker headquartered in Massachusetts, and a wholly owned subsidiary of Eastern Bank.

The business entity now known as "Eastern Insurance Group LLC," was originally formed by Eastern Bank in December 2002. It has grown to become one of the premier insurance agencies headquartered in New England and is one of the top 50 largest insurance brokerage firms in the country. They have more than 400 dedicated, highly skilled employees in 25 locations ready to serve the personal, commercial, and benefits needs of its customers.