WA GROUP
100% Employee Owned

CYBER LIABILITY

HOW THE CURRENT ENVIRONMENT HAS CHANGED BUSINESS TODAY

INTRODUCTION

Cyber Liability has become increasingly popular over the years. A large and significant uptick in organizations shifting to “work from home” platforms might be opening pandora’s box for cyber breaches.

NETWORK SECURITY/CYBER EXPOSURES

As each year passes, organizations and individuals become more reliant on technology. From day to day interactions to running an organization, technology is all around us. It’s no secret that an increase in technology use goes hand in hand with security breaches. In fact, the University of Maryland’s Clark School discovered there is a hacker attack every 39 seconds. Turn on the local news and it’s impossible to go more than a few days without learning about a new cyber breach that an organization has experienced.

According to the Cyber Risk Analytics report performed by RiskBased Security, data breaches exposed 4.1 billon records in just the first half of 2019! Cybercriminals prey on organization’s networks and systems and seek out vulnerabilities only to turn around and make a profit on what they have exploited. But it’s not just the well-known organizations that fall victim to these breaches.

According to Verizon’s 2019 Data Breach Investigations Report, 43% of breach victims were small businesses. The theory behind this number is that even though the target is not as large, smaller businesses do not have the IT infrastructure or “back room support” that larger, well-known organizations have, making them an easier target.

The information contained herein is for informational purposes only. It may not be appropriate for your particular situation and should not be taken as legal advice. You should contact an advisor or legal professional for advice about your situation.

There are several different ways an organization can experience a breach in security or disruption in their business, ranging from a physical loss of information (paper files, etc.) to systems interruption (disablement of an IT platform or system). A network security breach is when an individual gains unauthorized access to private information. When the individual has access to this information, they can cause destruction or manipulation to the information, or even permanently destroying it. Legally it is an organization's responsibility to keep private information protected, so when there is a breach it is that organization's responsibility to notify individuals when their identifiable information (birthdate, social security number, credit card information, etc.) is breached. These types of breaches can be costly from a financial standpoint. The average cost of a data breach is $3.92 million according to a 2019 survey conducted by Security Intelligence. This study only focuses on the financial impact and doesn't even touch the reputational impact a breach can also have on an organization.

Malware, malicious viruses, and Trojans are just a few examples of how an organization's network can be exploited. These malicious codes can not only affect an organization, but they can be transmitted unintentionally through an organization's system to a third party. According to Verizon's study, 52% of the hacking featured breaches, 28% involved malware and 32 – 33% included phishing or social engineering. Exploitation is not only virus transmission, it can also be in the form of ransomware, where the cyber-criminal is demanding a sum of money or some type of "ransom" and will hold your computer or network "hostage" until the ransom has been paid. The average cost of a ransomware attack on businesses is $133,000, according to a SafeAtLast report.

KEY RANSOMWARE STATISTICS

*Information taken from SafeAtLast's Ransomware Statistics

- **Ransomware cost businesses more than $8 billion in the past year.**
- **The average cost of a ransomware attack on businesses is $133,000.**
- **The global spending on cyberseurity is over $14 billion.**
- **Ninety-five percent of ransomware profits went through the cryptocurrency trading platform BTC-e.**
- **Cybersecurity Ventures predicts businesses will fall victim to ransomware attacks every 11 seconds by the year 2021.**
- **In 2018, more than 77% of the businesses affected by ransomware were using up-to-date protection.**

If an organization is highly dependent on their IT infrastructure to run their business, they are also at a high risk of falling victim to system interruption. System interruption is where an IT system becomes disabled, one of the most common ways of achieving this is through Denial of Service attacks, where a malicious third party overwhelms a system with access requests, to the point with the system shuts down. 51% of businesses experienced denial of service attacks in 2018, according to Cybint Solutions. If an organization cannot operate without their IT system, they are now losing revenue until their system is back up and running.

The information contained herein is for informational purposes only. It may not be appropriate for your particular situation and should not be taken as legal advice. You should contact an advisor or legal professional for advice about your situation.

INCREASED VULNERABILITIES (WORKING REMOTE)

In early March of this year, we saw organizations do a “scrambled rush” to get as many employees working from home as possible. While this is something that can take months, if not years to get an entire workforce of employees organized from an IT standpoint to work from home (ensuring proper equipment is being used, workstations are secure, etc.), we saw this shift happen almost overnight. Cybercriminals have viewed this as a huge opportunity, they have seen individuals move from a secured enterprise that is closely monitored, to a largely unmonitored and often unsecured home Wi-Fi networks. These cybercriminals are outside the reach of perimeter-based security tools and will likely have higher exposures to phishing and network attacks.

When organizations send their employees to work outside the normal perimeter, managing device sprawl, and patching and securing hundreds of thousands of endpoints become a bigger challenge. Add to that, most organizations did not have time to give any “last minute” security training to their employees on how to avoid phishing scams or ransomware, or what to look for. This has also opened the “flood gates” for cybercriminals. Capitalizing on individuals during a vulnerable time, sending out links in phishing emails that look like updates from the Centers from Disease Control (CDC) or the World Health Organization (WHO) that look like emails coming from someone within the organization (ex. Management or HR). Verizon’s report also notes a whopping 94% of malware was delivered by email. This eye-popping statistic shows how successful cybercriminals are at preying on the element of human error.

The information contained herein is for informational purposes only. It may not be appropriate for your particular situation and should not be taken as legal advice. You should contact an advisor or legal professional for advice about your situation.

PREVENTION

Fortunately, there are some steps organizations can take right now to help tighten security. Take an inventory of all business applications used and identify the most critical ones. For SaaS applications (third-party provider host, ex. Cloud computing), follow up with the service provider and inquire about their business continuity plans. For any on-premises applications that would require VPN connectivity, test and validate that VPN connectivity for higher utilization than usual. Make risk-assessments of remote workers' computing setups. Ask employees how they will connect to the organization's systems, and what devices will they be using to connect. Have employees "brush up" on their training and awareness of cybercriminal activity, remind them of how phishing scams and ransomware work, and to never click on links sent in emails before further investigating the email and the source of the email.

CYBER LIABILITY INSURANCE

Organizations can have the best safeguards, state of the art firewalls, continuous employee training, and still fall victim to a cyber security event. Cyber Liability insurance is a great tool for organizations to utilize when an event occurs. A Cyber Liability policy will not only assist in making the organization "whole" again after a loss, it provides tools that an insured heavily relies on when organizing a breach response (notification letters, IT Forensics, call centers, credit monitoring for affected individuals, replacing lost income during an IT shutdown, etc.). IBM's most recent Cost of a Data Breach report states that the average lifecycle of a breach was 314 days (from the breach to containment). Having an insurance policy that provides the above-mentioned tools provides great value to an organization, when considering the amount of time it takes to contain a breach.

There are also insurance carriers in the market that offer several services with their policy, such as an evaluation of an insured's IT network, or IT penetration testing where a "professional hacker" will try to gain access to the insured's IT network from outside the organization.

These services, and several others, assist insured organizations in tightening up their IT controls, as well as policies and procedures, which, in turn, will aid in claims prevention.

Underwriting for a Cyber Liability policy has tightened up due to recent global events, but it is not impossible to obtain coverage. Underwriters are looking at revenues, IT safeguards, policies and procedures that have been put in place, etc. to underwrite a quote. WA Group plays an active role in the insurance industry in assisting organizations place Cyber Liability coverage that compliments their organization's needs and ensuring the coverage fits their exposures. WA Group is here to help you determine your exposures, your need for coverage, and answer any questions along the way!

WA GROUP
100% Employee Owned

The information contained herein is for informational purposes only. It may not be appropriate for your particular situation and should not be taken as legal advice. You should contact an advisor or legal professional for advice about your situation.