The NetWork

LeadingIT

Chicagoland CybersecurITy Support

March 2021

Why 2020 May Have Changed The MSP Industry Forever

Cybersecurity Is Still The #1 Risk For Manufacturers

The Big Problem In The Cybersecurity Insurance Industry

GoLeadingIT.com (815) 496-6300 @LeadingIT @LeadingIT-Solutions

Why 2020 May Have Changed The MSP Industry Forever

Last year (2020) was a challenging year for most of us. The pandemic affected many areas of our lives. Businesses also struggled to stay afloat, and business owners had to adapt to continue to operate. As businesses looked for ways to survive, they focused on various solutions that could help them. MSPs had to adapt to survive the pandemic's effects.

How MSPs Adapted To The Pandemic

• **Increased Remote Workforce**

Governments and businesses had to put worker's safety first. They developed various strategies to achieve this objective. One approach they had was encouraging people to work from home. Companies managed their employees to ensure most of them worked from home. This transition caused a few challenges. How would the firms' infrastructure support remote work? They needed the IT setup to handle users from different locations performing various tasks on the network.

MSPs played a crucial role in facilitating the transition to remote work. For example, companies asked MSPs to design user-friendly networks to support their employees working from home. Others asked MSPs to provide gadgets and secure their IT setups

• **Educating Remote Employees On Cybersecurity**

As companies adopted remote work, employees had an essential role in cybersecurity. Their home devices accessed the company's network. One of these gadgets could be an entry point for hackers if they breached the owner's cybersecurity measures. Companies partnered with MSPs to offer employees training and simulations to improve their cybersecurity awareness.

• **Remote Employees Also Had To Be Responsible For Data Security.** As most companies' remote workers had various credentials for the company's infrastructure. Firms partnered with MSPs to promote remote user responsibility. They encouraged employees to avoid saving passwords on their devices, being reckless with their gadgets, and using public networks to access the company's infrastructure.

• **Businesses Turned to MSPs To Help Them Adapt To The Pandemic's Developments:** MSPs that were proactive continued to earn revenue, despite companies prioritizing other functions. Companies needed the innovation to survive, and the proactive MSPs helped them with this goal.

• **Cost Savings:** These MSPs discovered better ways to do things. They were also proactive in finding and rectifying problems early. These actions helped the companies enjoy cost reduction, availing the cash flow they needed in other areas.

• **Improved Performances:** Changes in society meant that companies had to adapt. They had to do new things in excellent ways. Innovative MSPs helped them optimize these processes. For example, they helped them optimize remote work to ensure everything went on smoothly.

Cybersecurity Trends During The Pandemic

Cybercriminals took advantage of the pandemic to target organizations. According to PwC, cybercriminals targeted establishments with more attacks during the pandemic. They used social engineering to trick people through many attack patterns, such as phishing.

According to CSO, the Office of Foreign Assets Control (OFAC) in the Treasury Department issued new guidelines for ransomware attacks. The office controlled the ransom payments to attackers from various regions and groups. They believe that the new regulations will prevent ransomware attacks.

MSPs play a vital role in the wake of the increased cybersecurity threats to organizations. They have been proactive in their measures to prevent attacks, and they helped the attacked firms recover. Companies avoided or minimized losses and disruptions with reliable cybersecurity from MSPs.

MSPs will continue to get the recognition they deserve. Establishments will realize that they enable companies to enjoy various benefits. Working with an MSP can help businesses get expert, customized, and affordable managed IT services.

Cybersecurity Is Still The #1 Risk For Manufacturers

The manufacturing industry is a crucial sector that plays a foundational role in today's economic and technological innovations. One of the biggest risks manufacturers face is cybersecurity. It would help understand why cybersecurity is a risk, the threats cybersecurity poses, how to prevent and manage these risks, and get IT support. In Chicagoland, you can rely on LeadingIT to help you assess, manage, and respond to cybersecurity threats.

Why Is Cybersecurity The Top Risk For Manufacturers?

• **Cybersecurity Threats Can Halt Operations:** It is very costly for you, and concerned parties can experience other negative effects when manufacturing operations come to a halt. Some employees, especially those you pay by the hour, experience income shortages, others may go on unpaid leave, and others could even lose their jobs.

• **A System Hack Can Damage Your Reputation:** Cybersecurity threats can interfere with machinery and systems to create faulty products. If you fail to test them before they get into the market, you will have compromised your customers' quality standards. It can take time to rebuild a positive brand image once your customers associate you with faulty products.

• **Information Leak Poses Competitive Threats:** Information leak is another major cybersecurity threat. Your competitors can use sensitive information to gain a competitive advantage.

• **Most Manufacturers Are Small Firms:** Therefore, they are either not usually fully prepared to mitigate cybersecurity threats or lack infrastructure.

What Are The Top Manufacturing Cybersecurity Threats In 2021?

1. Phishing

Phishing is a fraudulent act of acquiring sensitive information to your organization like credit card details, passwords, and usernames. Cybercriminals usually trick you into revealing your sensitive information via email. You will find these emails very convincing because they have elements like letterheads to prove their legitimacy. However, you will notice that these emails address a general audience rather than you specifically.

2. Identity Theft

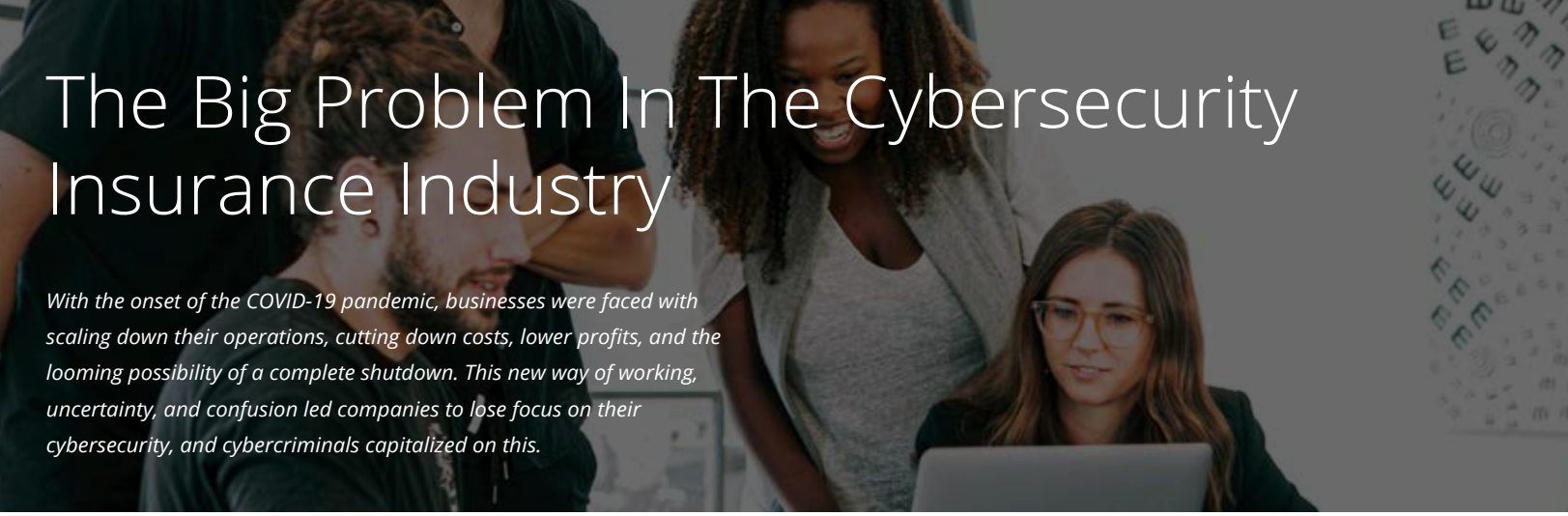
Identity theft involves acquiring and using someone's personal information illegally to obtain illegal access or sensitive information. Cybercriminals can use identity theft to access a manufacturer's sensitive information like their customer database.

3. Information Leaks

The European Union Networked Information Security Agency recognizes information leaks or intellectual property theft as a cybersecurity risk on its own. Your organization can experience information leaks from internal sources, which include employees or external hackers. Information leaks can cause you to lose your competitive advantage.

You can use various methods to prevent and manage the various cybersecurity threats you face as a manufacturer. They include:

• Train your employees or team on cybersecurity risks and how to avoid them.
• Always update your systems accordingly, especially software.
• Monitor and test security features of new technology.
• Ensure you implement real-time monitoring to systems prone to attack.
• Formulate a response plan for various cybersecurity threats and attacks.



The Big Problem In The Cybersecurity Insurance Industry

With the onset of the COVID-19 pandemic, businesses were faced with scaling down their operations, cutting down costs, lower profits, and the looming possibility of a complete shutdown. This new way of working, uncertainty, and confusion led companies to lose focus on their cybersecurity, and cybercriminals capitalized on this.

2020 Data Breaches Point To Cybersecurity Trends For 2021

According to Iomart, large-scale data breaches grew in frequency and intensity in 2020, with the number of breaches increasing by 273% in the first quarter of the year, compared to the same time in 2019. Deloitte has also reported a spike in email phishing, ransomware, and malware attacks as malicious attacks used COVID-19 as bait to impersonate brands.

With these statistics, it's only logical for a company to invest in cybersecurity insurance to protect itself against cyberattacks. Cybersecurity insurance is designed to help you mitigate your losses when you experience various cyber incidents ranging from data breaches, network damage, and business interruption. But what if the sector is suffering from a slow death?

What's The Problem In The Cybersecurity Insurance Sector?

According to Statista, cybersecurity insurance premiums are predicted to be valued at 20 billion US dollars worldwide by 2025. This is proof that the cybersecurity industry is rapidly growing. Or is it?

• Although the number of cyberattacks continues to rise, more companies are buying less or not buying cybersecurity insurance since the economic strain as a result of the COVID-19 pandemic has caused them to view cybersecurity insurance as a luxury.

• Additionally, there is no record of historical data loss, increasing the sector's unpredictability for all parties involved. All these problems boil down to one root problem — there might not be enough money in the cybersecurity insurance industry.

Costly Cyber Insurance Claims Could Lead To Higher Premiums In 2021

In the cybersecurity insurance industry, it appears that the pricing is low while the risk is high. There is no way this sector can continue to grow at its previous aggressive rate. On this basis, it may seem that it's not worth it for insurers to provide protection for cybersecurity risks — leading to a shortage of cybersecurity insurance.

What Should Businesses Do?

For companies worried about their cyber risks and cyber insurance availability, the ideal course is to have a plan and shift their thinking. Yes, you should still invest in cyber insurance, in part to help the sector grow, but you need to also look for alternative ways to cover your potential exposure. Buy a cover that you can currently afford and top it up with self-insurance mechanisms that range from carrying extra capital to cater to future cyberattacks by creating specific risk-financing activities that work like insurers. Over time, you may add to those partial programs, outplace self-insurance for external protection, and add to your overall insurance program.

WE ARE CELEBRATING!

Anniversaries

Jason Jimenez - March 4, 2013
Christa Gibbons - March 11, 2020
Steven Brimeyer - March 23, 2020

Birthdays

Steven Brimeyer - March 12th

Read Our Blog For More
https://www.goleadingit.com/blog