Cyber Attacks More Serious and More Sophisticated Each Year

Cyberattacks can do more than steal data or money. They can drive a business out of business, due to loss of assets or loss of customer trust. SMEs are particularly at risk, meaning every business needs a cybersecurity strategy.

The number of cyber threats continues to grow, threatening businesses with the loss of customers, assets, innovations, and proprietorial information. These cyberattacks are directed at all sizes of businesses and consumers. According to the Small Business Administration, 88% of small businesses believed their business was vulnerable. Threats include malware or malicious software, ransomware, viruses, and phishing. In 2020, it is estimated that global losses due to cybercrime were more than one trillion dollars, and the number of cyber threats grew by 17% as of September 30, 2020, compared to September 2020.

Rapid Technology Changes Create Vulnerabilities

A Deloitte survey of cybersecurity for financial institutions found the top cybersecurity challenge is managing “rapid IT changes and rising complexities.”1 The utilization of technology is accelerating across industries, and the adoption of each new technology presents a new set of cybersecurity challenges. For example, consumers now shop with their smartphones, creating a new way for cyber thieves to steal personal information and perhaps gain access to a company’s software. Cybercrime costs people and businesses more than money, as well. It can lead to lost sales, customer distrust of the brand, business downtime, missed deliveries to customers, loss of intellectual property (IP), and in some cases, loss of worker wages when the company must temporarily shut down.

The reasons for the attacks vary too. Criminal attackers are seeking financial gain through data or money theft or business disruption. Socio-political attacks are seeking attention for a cause. Personal attacks could target the theft of data or money, or could focus on disrupting the business, and the motivation is usually retribution. Spying attacks are intended to gain an unfair competitive advantage.

A joint study by Stanford University Professor Jeff Hancock and Tessian, a security firm, found that 85% of data breach incidents are the result of employee mistakes.2 The U.S. government says that manufacturers are increasingly threatened by cyberattacks, and most are small businesses that do not have IT security practices to combat cyber incidents.3 There are also supply chain attacks which are also called third-party attacks. Someone either steals supplier innovation or gains access to a customer of the supplier.

Challenge of Securing IT Systems

The attack on SolarWinds, a U.S. information technology firm, was undetected for months, and in that time the attackers were able to spy on private companies and government agencies. Malicious code was added to SolarWind's software system called Orion, used by companies to manage IT resources. When SolarWinds sent software updates to its customers, the update included the hacked door. This gave the hackers access to the technology systems of SolarWinds' customers, so the hackers could install more malware on approximately 18,000 customers.

Once hacked or breached, it can be difficult to secure systems once again. Even if secured, the damage can be long-lasting, especially for small and medium-sized businesses (SMEs). The National Cyber Security Alliance found that 60% of SMEs that are hacked will go out of business within six months. A cyberattack goes beyond the initial loss. The company must pay for mitigation, hardware or software upgrades, lost productivity, lawyer fees, and employee retraining. Attacks on businesses also directly affect consumers. When customer identity theft occurs, the data is often sold on the dark web, which leads to further thefts or theft attempts. It is very difficult to regain customer trust, especially for an SME, so it is not surprising so many businesses go out of business due to a cyberattack. ArcServe's research of global consumers found that half of the respondents would avoid doing business with a business that experienced a cyberattack in the past year.

Cybercrime is going to accelerate. Cybersecurity Ventures predicts cybercrime costs will increase by 15% annually over the next five years, which in terms of money is an estimated $10.5 trillion hacked by 2025.6 Any business not taking the threat of cyberattacks seriously is leaving the business extremely vulnerable.

Shutting the Door on Hackers

How does a business keep hackers out? The first step is auditing the current IT system, followed by developing a cybersecurity strategy. Every organization needs someone in charge of cybersecurity, but it is important to involve other people from across the organization. Human Resources, finance, sales, and other functions should provide input into the cybersecurity process. Identifying vulnerabilities is critical, and some companies utilize third-party suppliers to conduct an audit or manage the cybersecurity system. Should a cyberattack occur, the supplier will assist with mitigating damage as quickly as possible. Cybersecurity experts can periodically perform stress tests to determine loss exposure. Another major defense against cyberattacks is the choice of a reliable, experienced cybersecurity vendor.

ProWriters insurance company offers cyber insurance and recommends several ways to limit cyber risks. Employee training is critical since employee mistakes account for a large majority of data breaches, and they need training in areas like password management and recognizing phishing emails. Social engineering attacks are on the rise, too, in which someone tricks another person into bypassing security measures. This is a growing threat that is difficult to stop, which is why other measures are so important, such as keeping software updated, using cloud security technology, and

ensuring all the risk management tools are in place, like multi-factor authentication and endpoint protection.

Preventing cyberattacks is nearly impossible, but ignoring the growing threat can put the business out of business. It is important to invest in cybersecurity as a major asset needed for business continuity.