A GUIDE ON

COMMON SECURITY RISKS AND HOW TO SOLVE THEM

Wilson Consulting Group

- Cybercriminals always find new and effective ways to infiltrate sensitive and confidential corporate information and security systems.

- From malware to online ransoms, different companies of different levels have reported security risks that we often hear and see but never thought would ever happen to us.

- In 2019, IBM Security conducted research, finding that organizations reported an average of 279 days to identify and contain a data breach. Hackers gained access to information on an average of 500 million customers, compromising the companies' assets, security and trust.

Businesses are often vulnerable to different threats. With the advent of Internet of Things (IoT) connecting any device to the Internet and to other connected devices, the threats from hackers and cyber criminals increase and the weakest link defines the strength and potential exploitation of the network. In addition to allowing the infiltration of core systems, the IoT expands channels where cybercriminals can rattle company security. Social media, for example, has experienced an increasing number of predators. Social media platforms have been used to scout for high net worth professionals and business owners with the intention of extortion once sensitive information is obtained. External cloud services have also been a victim of cyberattacks. Data breach and hacking impact businesses negatively.

With this in mind, risk assessment and cybersecurity are now more important than ever. The use of information by organizations, including employee information, customer data, payment methods, and cloud services, necessitates the implementation of secure cybersecurity measures. To begin understanding the process, we must look at cybersecurity as part of a business plan and examine the common threats businesses have faced and how they solved it.

THE IMPORTANCE OF CYBERSECURITY IN BUSINESS

Most, if not all, businesses have some sort of basic cyber protection. These include passwords, authorized access, and device protection. While these are expected and required, as your company grows and interacts with more people and more devices, your assets become more vulnerable to cyberattacks. Cyber protection programs can be installed, like anti-malware, anti-virus, multi-factor authentication (MFA), and bot checkers. However, most of these are generic to all businesses and aren't tailored to what your business may need.

Recent technological innovations have also allowed more unauthorized access to business assets. Tools like APIs with poor configuration and security, third-party/fourth-party services providers that collect information, and cloud services make your business more susceptible to hacking and cyberattacks. Additionally, services like monetary transactions are expected to happen in real-time. The increasing demand for faster services affects security protocols and increases the chances of cyberattacks.

These cyberattacks can come from multiple sources as well. Foreign hostile powers, competitors, organized criminals and hackers and third-party service providers are just a few examples. While these are factors a business cannot control, the importance of cybersecurity in businesses, whether a start-up or high-profile, lies in identifying possible sources of cyberattacks, channels that could be attacked, and possible preventive and restorative solutions in case of an attack. Something as common as a data breach impacts businesses negatively, often running them into the ground and causing bankruptcy.

COMMON BUSINESS CYBERSECURITY ATTACKS

The following cybersecurity attacks are frequently experienced by organizations and identifying them can help businesses proactively respond to the threats.

DATA BREACH

Data breach is the most common cybercrime among businesses. There's been a transformation in how data has been stored in organizations - from hardware to cloud storage. Data breach often involves the theft of hardware and access to data. Recently, however, cloud storage has become increasingly popular, and these types of storage require a different form of security. Back up data, virtual machines, security keys, and factor authentications are examples of ways to protect information in the cloud. The best way to protect yourself from a data breach of information stored in the cloud is to choose a proper cloud provider and add any form of data protection possible.

Data breaches can also happen at the hands of third-party providers. The recent surge of privacy policy updates is linked to third-party providers. These providers often have access to your data without you knowing it. While this can be for various reasons, privacy policies are often compromised.

POOR PASSWORD PROTECTION

With blockchain and One Time Passwords (OTPs) on the rise, single-use passwords are becoming out of date. Even personal email accounts and apps are protected with OTPs instead of single- use passwords. That's because passwords offer poor cyber-protection. They are easily hacked and shared among cybercriminals. Remarkably, a lot of businesses still use them. This results in poor protection and unauthorized access.

MALWARE

Aside from predators lurking in professional social media platforms, malware is often bundled in downloaded apps and programs that can hurt business by harming business devices, tracking employee operations, downloading sensitive information, recording videos through webcams, and making computers inaccessible, to name a few. With the increase of P2P services like torrent downloading, malware has become more common in the past few years. While anti-malware programs like Malwarebytes are free, professional organized cybercrime find ways to bypass basic malware protection. Businesses need professional assessment and protection.

APPLICATION PROGRAMMING INTERFACES (APIs)

Most businesses use APIs because of the ease of operations and accessibility. However, some APIs are insecure, compromising any business who uses them. Lack of security from authentication to encryption makes APIs vulnerable to attacks. Stringent cybersecurity procedures must be followed to avoid business compromise in API interactions.

Keep in mind that there are many forms of cybersecurity attacks aside from the ones listed here. While cybercrime cannot be fully controlled, there are many ways to prevent it and reduce/mitigate the risk to your business.

THE SOLUTION

HOW TO REDUCE/ MIGITATE RISK?

One of the most important solutions any business should implement is cybersecurity awareness training. Business owners, operators, and managers have the responsibility to know and assess the importance of data and safe cyber protection measures. Software protection, risk management programs, compliance, agreements and training should be provided by the business to all parties concerned, including employees and third-party agents.

Wilson Consulting Group provides these essential cybersecurity measures and more to protect your business and affiliated entities. Data breaches and other cybersecurity attacks can cause devastating financial losses and affect an organization's reputation for years. We work to minimize the risk of attack by providing high-quality assurance for your business. Questions? Please contact us at +1-866-780-1655 or sales@wilsoncgrp.com. We are here for your cybersecurity needs.

Thank you for downloading this free e-book!

Sources:

1. Cybint. (2019, May 16). 5 of the Biggest Cyber Security Risks for Businesses. Retrieved March 5, 2020, from https://www.cybintsolutions.com/5-of-the-biggest-cyber-security-risks-for-businesses/
2. Kingori, D. (2019, January 17). Top 10 Cybersecurity Risks For 2019. Retrieved March 5, 2020, from https://www.uscybersecurity.net/risks-2019/
3. Wilson Consulting Group Inc. (n.d.). IT Governance: What it is, the benefits, and solutions: Retrieved March 5, 2020, from https://blog.wilsoncgrp.com/it-governance-what-it-is-the-benefits-and-solutions/
4. Wilson Consulting Group, Inc. (n.d.). Ahead of the Curb: Security measures to take before potential IoT boom: Retrieved March 5, 2020, from https://blog.wilsoncgrp.com/ahead-of-the-curb-security-measures-to-take-befoe-potential-iot-boom