Technological Advances Bring New Cyber Risks. Here's How to Mitigate Them.

Author: **Randy Sadler, *CIC Services***
Published: **February 28, 2022, *Entrepreneur***

See original here: **https://www.entrepreneur.com/article/413535**

Technology can be a wonderful thing. Properly utilized, advanced technology solutions allow us to better engage our customers, streamline ordering and invoicing processes, and increase the efficiency of our audit and internal communications. Just like with all emerging technologies, the advantages that these new solutions bring are also creating new risks and challenges for businesses to manage and overcome. Unlike in the past, the cyber risks faced by CFOs today are increasingly catastrophic and incredibly difficult to control.

Reliance upon technology is a requirement for businesses to remain agile and responsive, and the new opportunities presented by advancement are exciting and can be quite profitable. Unfortunately, risk management is behind the eight ball as it relates to cyber and technology threats. It is a monumental task to plan and protect against risks that heretofore simply did not exist. An awareness and understanding of some basic cyber threats and proactive methods of loss prevention can be a great start to protecting your organization's valuable IP, customer data and digital assets.

Hacking

Cybercrime is making a shift from a broad-based attack to more specific targeting. By targeting software vulnerabilities in specific servers, hackers can have a higher likelihood of successfully gaining unauthorized access to data or systems and can potentially avoid detection entirely.

Help protect against hacking-related losses by beefing up your info security protocols. Mandate password changes on a frequent basis. Require special characters, numbers, length and limit reuse, and enable double authentication. Ensure that patch and firmware updates are implemented at both the user device and server/enterprise level and consider implementing penetration testing and audits by an independent third party.

Ransomware

Unlike in popular movies of old, do not expect to receive a ransom notice via an anonymous letter comprised of cut-and-pasted type from random magazines. Ransomware often enters and compromises a system via malicious emails. Once intruders have access to valuable data, they will encrypt the data, block off access to authorized users and demand payment for release — often in some form of cryptocurrency.

The impact of a ransomware attack can be lessened significantly with the implementation of proper data backups. Consider implementing services that automate the backup of critical and sensitive data on a frequent basis. Help ensure integrity of your backups by keeping the redundant files segregated from standard networks and, if possible, offline completely.

Data leakage

The proliferation of technology significantly complicates the process of maintaining control of your digital assets. Cell phones, tablets and laptop computers are everywhere, and portable storage devices like USB drives, external SSDs, etc. are common methods of transporting data and information between parties. Unlike the other common methods of intrusion, these devices turn your digital information into physical form and are now subject to loss and theft by unrelated parties or disgruntled employees and contractors. The comingling of personal devices that have access to or retain company data provides opportunity for additional vulnerabilities.

The physical nature of leakage fortunately comes with more concrete risk-management methods. Consider disabling external-drive connections on user devices (i.e. turning off USB connection ports). Turn on GPS tracking of all applicable devices and ensure that devices can be locked and wiped remotely if lost or stolen.

Phishing

An exposure presented often by social or human engineering, phishing often attempts to disguise nefarious attempts to access information by posing as a source (website, individual, attachment, etc.) that is trusted to the specifically targeted individual. Perpetrators commonly use fake emails from supervisors to request transfer of funds and issue fraudulent invoices for products or services with wire info going to the criminal's account.

Because phishing intrusion is often individual or social in nature, you can work to combat this risk with effective awareness training. Provide employees with information and examples of fraudulent requests and consider implementing procedures that require in-person or telephonic confirmation of invoice changes or internal wire requests.

Effective management of a risk that comes from so many sources is no small task. Unknown assailants, multiple methods and developing regulatory framework (FISMA, GDPR, etc.) require 24/7 vigilance for a risk that never sleeps. Developing a comprehensive and flexible protection and response plan will help protect your digital assets, avoid the costs associated with a cyber loss and provide your organization a potentially significant competitive advantage.

RANDY SADLER started his career in risk management as an officer in the U.S. Army, where he was responsible for the training and safety of hundreds of soldiers and over 150 wheeled and tracked vehicles. He graduated from the U.S. Military Academy at West Point with a Bachelor of Science degree in International and Strategic History with a focus on U.S. – Chinese Relations in the 20th century. He has been a Principal with CIC Services, LLC for 7 years and consults directly with business owners, CEOs and CFOs in the formation of captive insurance programs for their respective businesses.

CIC Services, LLC manages over 100 captives.