Know Your CyberSpeak: A Cyber Risk Glossary

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Navigating the world of cyber risk often feels a lot like learning a foreign language. Terms and concepts can be confusing and unfamiliar. This Cyber Risk Glossary will help nonprofit leaders as they examine cyber liability insurance policies and develop the necessary technology-related security protocols to protect their missions.

Cloud – The term "Cloud" refers to a product created and hosted by a third party and accessible via the internet. Cloud products range from data storage solutions such as OneDrive and Dropbox, to communications tools such as Gmail, and software and productivity products such as Microsoft Office or Google Docs. Cloud products can generally be customized, adapted, and arguably 'managed' in house by an end user or a nonprofit's IT team. Many organizations view cloud-based products as a key to business continuity; if servers and systems at a nonprofit are damaged or otherwise inaccessible, systems and data stored 'in the cloud' should still be accessible by a user with an Internet connection and an authorized login.

Cloud Risks: It's risky to assume that the cloud solves all your storage and redundancy problems! Peruse "Cloud Computing – BCP Boon or Boobytrap?" to review how to manage the risk of getting lost in a technology fog.

Cyber Resilience – Nonprofits that practice cyber resilience work to prevent cyber-attacks while accepting that not every attack is avoidable. Resilient organizations implement strategies that provide rapid recovery and response methods and manage downside events and outcomes to mitigate losses and ensure continuity of operations.

Cybersecurity – Cybersecurity is a collection of technology, processes, and practices that focus on protecting electronically stored information from theft or damage. The NIST Cybersecurity Framework, released in 2014, is one of the best-known cybersecurity frameworks and is structured as a series of stages: prevention, detection, and response. Cybersecurity's focus is broader than its counterpart, data security. Nonprofits should use this framework to protect networks and infrastructure from attacks, disruption, misdirection, and bad actors.

Data Security – Data security is the narrower arm of cybersecurity. In this discipline, nonprofit information technology specialists focus on protecting the data stored by organizations, for example, keeping names, social security numbers, and payment information secure. Data security policies and procedures center on keeping unauthorized individuals from acquiring personal information—either from a data breach or even a lost laptop.

Encryption key – An encryption key is a random string created by an automated security algorithm to secure and protect information. Encryption keys can be used to secure data that needs to be sent to other parties. The key is used to scramble data and unscramble data when the authorized party has received it and is ready to view it. Computer-generated algorithms ensure the key is randomly generated and unique, making it more difficult for hackers to crack.

Internet of Things (IoT) – Internet of Things (IoT) is the general term used to capture the growing number of devices able to connect to the internet and provide "use" data. In recent years, the IoT has expanded beyond computers and cell phones to include "smart" appliances and speakers, health care equipment, security cameras, thermostats, and many other devices. These devices capture many different types of data, some more sensitive than others. Because they don't rely on human intervention to function, they can fall victim to

being set up and forgotten about. Each IoT device provides another potential access point for bad actors to access the network and/or the data it connects to.

IoT Risks: IoT allows nonprofits to harness "big data" and automate areas that previously required valuable staff time. The risk of a data breach can be more significant if proper measures aren't established to protect data and automated sensors. Learn more about cyber threats and security protocols for the IoT from Deloitte's article "Cyber Risk in an Internet of Things World."

Malware – A catchall term for any piece of software that changes the behavior of a computer, website, application, or other device which causes harm. Examples of malware include viruses, keyloggers, ransomware, and other malicious programs. Often malware is used to collect sensitive information such as credit card or social security numbers, or to disrupt the everyday use of a network by shutting down servers or making web pages unusable.

Phishing – Phishing scam emails are composed and sent to trick the receiver into revealing sensitive information such as employee IDs, usernames, and passwords. Scammers often encourage the receiver to click on a link that leads to a website controlled by a hacker; these false websites may look convincingly like the sites they are mimicking.

Ransomware – Ransomware is a specific type of malware that infects a system and then encrypts all of the user's information. The user is then instructed to pay for the encryption key to avoid losing their data or access, often through a cryptocurrency such as bitcoin.

Social Engineering – Social engineering is the act of manipulating a person into providing confidential information. Many phishing attempts use social engineering to encourage the receiver to trust the email's author and provide the requested information. Pretexting is another method of social engineering, but generally involves a malicious actor attempting to trick, cajole, or threaten someone into revealing sensitive information over the phone.

Two-Factor Authentication (2FA) – An extra layer of security where access to a user is only granted once they have provided a secondary form of identification after providing their initial username and password. Two-Factor Authentication usually requires a user to prove that they are the owner of an email account, cellphone, or other device where one-time access codes are sent or generated and then provided as proof that they have the permissions to access the protected application or device. Multi-factor authentication (MFA) requires two or more independent credentials. An easy way to remember what MFA means is that it requires 1) something you "know,' such as a password, 2) something you 'are,' such as a form of biometric recognition, and 3) something you 'have', such as a security token.

2FA Risks: Two-Factor Authentication does provide an added layer of security for access to sites storing sensitive data. However, nonprofits should be vigilant when selecting and updating access devices as staff leave their roles at the nonprofit. Critical access could be denied if the access device (a cell phone or alternate email address) is no longer available.

Virtual Private Network (VPN) – An encrypted pathway through the internet that allows a user to access a primary network from a remote location. VPNs are commonly used to enable employees to access office systems from home, and often require two-factor authentication or other layers of security before a secure connection is established.

VPN Risks: Virtual Private Networks are excellent avenues to connect staff with essential software and data. However, the COVID-19 pandemic has exposed additional risks nonprofits should consider when utilizing VPNs for work-from-home staff members. Often home networks are insecure, making VPNs more vulnerable to hackers and bad actors.