Cyber Terms 101

Patti Tobin, Producer, Financial Practices Division
Community BancInsurance Services, A Gallagher Company
Springfield, IL

There are many types of cybercrime that can impact your business, community bank or organization. Building a better vocabulary around cyber security can give you a stronger foundation to help mitigate its many risks. The more you know, the better equipped you'll be to protect your data, employees, customers and bottom line. Here's a list of key terms to help you brush up on your cyber vocabulary.

BOTNET is a collection of compromised computers, sometimes numbering in the thousands or even millions, that are under the control of a single entry. Botnets are typically used to steal data, such as online banking credentials, or to facilitate other types of cybercrime, like spamming or DDoS attacks.

CLOUD-BASED AUTHENTICATION can allow a company to consolidate and simplify its sign-on procedures but is not generally used to identify gaps in a company's security. Risk assessments, however, are widely recommended by cyber security professionals because risk assessments can provide a company with an overall evaluation of its security strategy and potential gaps. Penetration testing ("pen testing") is also important in helping a company evaluate its cyber security, by testing the company's security against a hypothetical attacker.

CRISIS COMMUNICATIONS PLAN Data breaches are unique in that they can involve confidential customer information and are subject to time-sensitive state and federal notification requirements. Having a specialized communications plan can help protect your reputation and bottom line.

CYBER INCIDENT RESPONSE PLAN (CIRP) Many plans, policies and strategies contribute to your organization's overall preparedness, but an incident response plan is specifically designed to minimize or contain damage associated with a data breach or network intrusion.

DARK WEB is an anonymous part of the Internet where criminals can buy and sell information stolen from businesses or other entities. It is a marketplace where private, protected and proprietary information, as well as the tools that cyber criminals use to hack into computers – such as viruses, exploit kits and other malware – are readily available for purchase and use.

DATA BREACH COACH is an outside legal counsel experienced in providing guidance throughout the incident response effort, particularly on issues relating to privacy, notification requirements, regulatory compliance, retaining forensic professionals and managing crisis communications.

DENIAL-OF-SERVICE, or DoS, occurs when a network is flooded with spurious traffic to prevent legitimate users from accessing the network. Many experts believe that DoS attacks are likely to worsen as criminals begin to exploit vulnerabilities in the "Internet of Things," such as networked appliances or smartphones, to carry out the attacks.

DIGITAL FORENSICS EXPERT After a breach, use of an outside digital forensics expert may be necessary to analyze malware or examine detailed logs of network traffic, particularly if the incident might give rise to litigation.

ENCRYPTION is a method of encoding data so that only authorized parties who possess a decryption key can access the data. Encryption should be considered to protect any sensitive data that is being stored ("data at rest") as well as data that is being moved ("data in motion").

HONEYPOT is a closely-monitored system that is deliberately configured to invite attacks. They are often used to attract and trap cyber criminals but can also be used by businesses to determine when a network has been compromised.

HOT SITE is a redundant data center that would be immediately available to support a company's operations if a primary data center were to fail. In contrast, a "cold site" is a backup data center that could be brought online in the event of an emergency, although with some time and effort.

INCIDENT RESPONSE PLAN Many plans, policies and strategies contribute to your organization's overall preparedness, but an incident response plan is specifically designed to minimize or contain damage associated with a data breach or network intrusion.

INTRUSION DETECTION SYSTEM (IDS) is a device or software application designed to monitor networks for malicious activity or policy violations. They typically use signature-based detection to recognize bad patterns, like malware, or anomaly-based detection to identify deviations from normal network activity.

MULTI-FACTOR AUTHENTICATION (MFA) is an authentication tool that combines "something you know" (such as a password), "something you have" (such as a text message), and "something you are" (such as a fingerprint scan) to create a stronger access control than only requiring a password. MFA can prevent intruders from spreading across a network from a single compromised computer.

PATCH MANAGEMENT systems are used by companies to obtain, prioritize, validate and install the various "patches" or code changes that are made available from the vendors of various

applications and systems. Exploiting an unpatched vulnerability is one of the easiest and most common methods criminals use to compromise a computer system or network.

PHISHING is a scheme to acquire private, personal or financial information using fraudulent email messages. These types of attacks are declining, though more targeted attacks against one or a small number of individuals, known as "spear phishing," have become more common.

RANSOMWARE is a type of malicious software that prevents users from accessing their data or systems until a ransom is paid. Cyber criminals are known to have deleted backup files, so maintaining off-site backups is a sound practice.

TABLETOP EXERCISE is a discussion-based simulation involving the full incident response team. Conducted annually, it's designed to expose, report and fix any vulnerabilities in your incident response plan before an attack occurs and can help ensure post-incident recovery efforts run smoothly.

VIRTUAL PRIVATE NETWORK (VPN) is a secured communication channel that typically uses encryption and is built atop another network, such as the Internet. Businesses that use a VPN to secure remote access to a corporate network are less vulnerable to certain threats, including those associated with using public Wi-Fi hotspots.

For questions on this subject, please contact Community BancInsurance Services, a division of Arthur J. Gallagher & Co., the exclusively-endorsed insurance representative of CBAI/CBSC. Ask for Patti Tobin, CIC, Insurance Advisor, Area Financial Institutions Director 217.414.4485 or patti_tobin@ajg.com.