AICPA

Private Companies Practice Section

What you need to know today

Cybersecurity FAQs

This tool was developed by PCPS in conjunction with:

LBMC MAKE A GOOD BUSINESS BETTER

Key elements of cybersecurity

Q: What is cybersecurity and should my organization be concerned?

A: Cybersecurity is the process of designing, implementing and operating controls to: (a) protect information and systems from security events that could compromise the achievement of the entity's objectives, and (b) detect, respond to, mitigate and recover from, on a timely basis, security events that are not prevented. In other words, an organization's cybersecurity program should identify and categorize potential security threats, implement controls designed to prevent the most significant threats whenever possible and detect when security breaches occur so the organization can respond properly.

In the current business landscape, all organizations have significant pieces of their operations consisting of, or relying on, various cyber functions. All organizations have an interest in protecting their confidential information from data breaches in which unauthorized persons can obtain private information, such as Social Security numbers, financial information, health records, credit card numbers, trade secrets, intellectual property or other protected data.

Q: What are common external cyberthreats to an organization and how should my organization address them?

A: Although the potential avenues of external attacks are numerous, there are some commonly exploited avenues that organizations can address to reduce susceptibility. The most common successful external exploits include social engineering attacks (typically via email phishing), password guessing, web-application attacks and access via system misconfiguration. To address these threats best practices, include the following:

- Use strong passwords that are long, complex and changed regularly, and change all "default" passwords
- Require multi-factor authentication such as a password plus a token for all remote access
- Ensure applications are written using secure coding principles
- Ensure all systems are "hardened" and frequently patched against known software and configuration vulnerabilities
- Establish a robust training and awareness program

Q: What are some common internal cyberthreats to an organization and how should my organization address them?

A: While many organizations focus on protection from external cyberthreats, the risk of compromise from internal threats often is underemphasized. Internal threats often include missing security patches, default system settings that leave systems vulnerable, easy-to-guess passwords and vulnerabilities introduced by third-party software running on a system. Organizations should consider the following to address internal threats:

- Use of strong passwords that are long, complex and changed regularly, and change all "default" passwords
- Identify the nature and types of sensitive data within the organization, and label systems containing sensitive data so they can be appropriately protected
- Apply access controls to computer systems and networks; ensure users have access only to systems and data needed for their job role
- Rigorously and regularly patch computers and third-party software to address known security weaknesses
- Regularly evaluate the security of the network via vulnerability scanning, and adjust when weaknesses are identified
- Implement security monitoring to identify and alert when security attacks are suspected. Management should research the security monitoring system that best protects their organization.

Q: What is "regulated data" and what are some examples?

A: Regulated data include types of data for which legal, regulatory and compliance obligations require the protection from unauthorized access and disclosure, typically by implementing specified security baseline controls. The prescribed protections must be applied to the regulated data types during storage, processing and transmission. The most common data types subject to regulations include personally identifiable information (PII), such as employee and customer Social Security numbers and tax return data, protected health information (PHI), such as medical records and treatment information, and cardholder data (CHD), such as credit card numbers.

Q: What is HIPAA and does it apply to my organization?

A: The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that applies to protected health information (PHI). PHI is information that can be used to identify an individual and an associated malady or treatment. The HIPAA guidelines include the Security Rule, which governs the handling of PHI in both physical and electronic (ePHI) formats, and requires the implementation and operation of a cybersecurity program.

Security Rule guidelines apply to covered entities, such as hospitals, clinics and doctors, as well as any business associates, including claims or billing service providers or other third parties who may encounter the covered entities' PHI data. Firms providing services to health care companies are likely to be requested to sign that client's business associate agreement. **If the firm elects to sign the agreement, the firm becomes a business associate and must comply with the HIPAA Security Rule.**

Q: What is PCI DSS and does it apply to my organization?

A: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to curb costly credit card data breaches affecting merchants and their service providers. The standard, divided into 12 requirements outlining aspects of security best practices, must be observed by any organization that stores, processes or transmits credit card data. Major credit card brands created PCI DSS, and it is not law, but is enforced via a process established by the card brands and the PCI Security Standards Council. **Organizations that accept credit cards as a form of payment may be subject to the PCI DSS requirements and compliance obligations.**

Q: What is the SOC Suite of Services and how do they apply to my organization's needs?

A: System and Organization Controls (SOC) is a suite of service offerings the AICPA created that CPAs may provide regarding system-level controls of a service organization or entity-level controls of other organizations. SOC for Service Organizations are internal control reports on the services provided by a service organization, which provides valuable information that users need to assess and address the risks associated with an outsourced service, including outsourced payroll providers. SOC for Cybersecurity is a reporting framework through which organizations can communicate relevant useful information about the effectiveness of their cybersecurity risk management program and CPAs can report on such information to meet the cybersecurity information needs of a broad range of stakeholders.

Q: How can I make my financial statement users and key stakeholders aware of my organization's cybersecurity risk management processes?

A: To address the market need of organizations to demonstrate they are managing cybersecurity threats, the AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. The framework is a key component of a new System and Organization Controls (SOC) for Cybersecurity engagement, through which a CPA reports on an organization's enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of an organization's efforts.

Q: What is a risk assessment?

A: An information security risk assessment is a process of identifying and cataloging the types of cybersecurity risks an organization faces, determining the risk of exposure to each threat, and reporting the results to the organization's leadership. Risk assessment results are used to facilitate decision-making regarding the allocation of resources to protect critical systems and data against real and perceived threats.

Q: What is a security vulnerability?

A: A security vulnerability is an inherent weakness in a computer system that a threat can exploit, resulting in an undesirable impact on the confidentiality, integrity or availability of the computer system and/or the data it contains.

Q: What is a penetration test?

A: A penetration test is a set of activities performed against computer systems, networks and applications to identify and exploit potential security vulnerabilities to gain unauthorized access to systems and/or data within the target environment. Testing may be performed from outside the network (external penetration) to simulate an outside attacker on the internet, or from inside the organization's network (internal penetration) to reveal the entity's susceptibility to insider threats. Testing may also be conducted against wireless networks, web applications or against the physical security controls of an organization's facilities.

Q: What is a vulnerability assessment and how does it differ from a penetration test?

A: A vulnerability assessment (sometimes called a vulnerability scan) is a set of activities performed on an IT system, network or website to identify and catalog the security vulnerabilities that are present in the target environment. A vulnerability assessment is intended to identify and assign a priority rating to potential security weaknesses in the environment, but, unlike a penetration test, it does not seek to exploit the weaknesses identified. Therefore, a vulnerability assessment provides the organization with a perspective on the technical security posture of the organization's IT systems, but does not provide any validation of the likelihood that the organization could be successfully compromised via one of the identified vulnerabilities. Vulnerability assessments are performed primarily using automated tools. While automated tools are available that can assist a penetration tester in identifying potential exploit vectors, most penetration tests involve both automated and manual techniques and require a high degree of skill for the assessor. While they are different testing activities, vulnerability scans and penetration tests are both important components of a comprehensive information security risk management program.

Q: What is an incident response plan?

A: In the event an organization suffers a security breach of any magnitude, it must be able to minimize the impact of the incident, restore the affected environment to full working order and communicate with affected parties, as necessary. An effective response plan allows the organization to communicate quickly and clearly with necessary parties if a security breach occurs, whether it's in the form of public relations or internal communication with employees and stakeholders. A successful plan is regularly rehearsed before it is executed in the heat of battle, so that all personnel are aware of their responsibilities.

Q: What is a business continuity plan?

A: While many organizations understand the need to be able to recover systems and data in the event of an outage or disaster, they are often not as well prepared to maintain regular business operations while the recovery is ongoing. Organizational functions, such as customer service, accounting, finance and HR must be able to meet obligations regardless of if the network is up and running. A business continuity plan considers all business operations to ensure the organization can operate effectively and serve its customers and clients when the unexpected occurs.

Q: What is malware and how do I protect my organization against it?

A: Malware is short for malicious software, and was previously known as computer viruses. The days of simply relying on antivirus software to address the threat of malware have long passed. Protecting against the numerous strains of malicious software requires a robust approach to user and system security. Antivirus/anti-malware software should still be leveraged, but can only identify known types of malware. The newest malware prevention software protects against malware threats by using "whitelisting," which is pre-defining the software that can run on a computer, and preventing all other software from running. Other innovative malware protections include analyzing each software program before it runs to identify malicious characteristics. Monitoring utilities, such as intrusion detection and prevention systems, file integrity monitoring and security information and event management (SIEM) systems, can be used to monitor for suspicious network activity that may indicate a compromise. A robust training and awareness campaign also is critical to educating users to be vigilant against phishing attacks, visiting malicious websites and other means attackers use to insert malware into an organization's network.

Q: What is ransomware?

A: Ransomware is a type of malware that denies access to an IT system or encrypts critical data until the system operator pays a sum of money or agrees to other demands. Organizations can protect themselves by educating users to identify and avoid falling victim to phishing emails, using whitelisting capabilities to define acceptable software and regularly backing up critical systems and data.

Q: What is a phishing attack?

A: Phishing is a form of computer fraud in which the attacker tries to trick users into disclosing sensitive information, such as login credentials or account information by masquerading as a reputable entity or person via email or other communication channels. Phishing is one form of a category of attacks called "social engineering."

Q: What is multi-factor authentication?

A: Multi-factor authentication is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to prove his/her identity to the computer system. Multi-factor authentication enhances the traditional method of authenticating user identity through only a name and password. By requiring at least two separate factors to authenticate a user's identity, an organization can reduce the likelihood of an attacker gaining unauthorized access to its systems and networks via stolen user credentials. Factors include *something you know*, such as a password or PIN, *something you have*, such as a smartphone or key fob token, and *something you are*, such as a fingerprint or retina scan. Examples include requiring a password and smartphone token for remote VPN access, or requiring a PIN and fingerprint for data center access.

Q: Do I need cybersecurity insurance?

A: A breach in even the most highly protected organization is possible, and organizations should consider their need for cybersecurity insurance. Researching current coverage to determine if additional cybersecurity insurance needs are necessary is an important first step. A separate policy or rider may need to be added to an existing commercial policy. It's important to consider both first- and third-party coverage to mitigate potential losses because of an organization's weakness as well as that of a third-party vendor. Having a basic cybersecurity program in place may assist in reducing premiums.

This tool was developed
by PCPS in conjunction with: