Data Security: Top Threats to Data Protection

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://ed.gov/ptac.

Purpose

Advancements in information technology (IT) have raised concerns about the risks to data associated with weak IT security, including vulnerability to viruses, malware, attacks and compromise of network systems and services. Inadequate IT security may result in compromised confidentiality, integrity, and availability of the data due to unauthorized access. To ensure that individual privacy remains carefully protected, local and state education agencies should implement state-of-the-art information security practices.

Staying ahead of the ever-evolving threat of a data breach requires diligence on the part of the education community in understanding and anticipating the risks. This short paper outlines critical threats to educational data and information systems. Threats are divided into two categories: technical and non-technical. A brief description of each threat is followed by a suggestion of appropriate risk mitigation measures. As a rule, an organization can greatly reduce its vulnerability to security threats by implementing a comprehensive privacy and data security plan. PTAC's Data Security Checklist provides additional guidance on protecting information systems.

Technical Data Security Threats to Information Systems

- **Non-existent Security Architecture.** Some organizations do not have an established security architecture in place, leaving their networks vulnerable to exploitation and the loss of personally identifiable information (PII). At times, due to a lack of resources or qualified IT staff, organizations' networks are connected to the internet directly, or are connected using out-of-the-box network appliances with default configurations attached, with no additional layer of protection. It is important to note that having a firewall alone is not sufficient to ensure the safety of a network. Inadequate network protection results in increased vulnerability of the data, hardware, and software, including susceptibility to malicious software

(malware), viruses, and hacking. If the network contains sensitive information or PII, such as students' social security numbers, it is critical that even in a very limited resource environment, minimal user, network and perimeter security protection mechanisms (such as anti-virus) are implemented, including making sure that anti-virus software is properly configured. Robust security architecture is essential and provides a roadmap to implementing necessary data protection measures.

Mitigation: If an organization does not have the appropriate personnel to design a security architecture, it is recommended that a third party be brought in to consult with the IT team.

- **Un-patched Client Side Software and Applications.** Computers run a variety of software applications, including older versions of that may sometimes contain vulnerabilities that can be exploited by malicious actors. Keeping up with software updates and upgrades, in addition to applying manufacturer-recommended patches, minimizes many of the vulnerabilities.

  Mitigation: To reduce the ability of malicious actors to compromise or destroy an organization's security system, implement a robust patch management program that identifies vulnerable software applications and regularly updates the software security to ensure ongoing protection from known threats.

- **"Phishing" and Targeted Attacks ("Spear Phishing").** One way malicious individuals or criminals (e.g., hackers) target individuals and organizations to gain access to personal information is through emails containing malicious code—this is referred to as phishing. Once infected emails are opened, the user's machine can be compromised.

  Mitigation: To reduce vulnerability to phishing and other e-mail security scams, organizations should install professional enterprise-level e-mail security software. It is recommended that this software check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised. In addition, organizations should provide regular internet security training to staff to ensure user-awareness about e-mail scams.

- **Internet Web sites**. Malicious code can be transferred to a computer through browsing webpages that have not undergone security updates. Therefore, simply browsing the internet and visiting compromised or unsecured websites could result in malicious software being downloaded to an organization's computers and network.

  Mitigation: To prevent threats from compromised websites, employ firewalls and antivirus software to help identify and block potentially risky web pages.

- **Poor Configuration Management.** Any computer connected to the network, whether at work or at home, that does not follow configuration management policy, is vulnerable to an attack. Weak data security protection measures that do not restrict which machines can connect to the organization's network make it vulnerable to this type of threat.

  Mitigation: Establish a configuration management policy for connecting any hardware to the

network. The policy should specify security mechanisms and procedures for various types of hardware, including computers, printers, and networking devices. It is also recommended to implement a Network Access Control solution to enforce configuration policy requirements (e.g., by automatically preventing network access to the devices that do not comply with the network security policies).

- **Mobile Devices.** Use of mobile devices, such as laptops or handheld devices, including smartphones, is exploding; however, the ability to secure them is lagging behind. The situation is complicated by the fact that these devices are often used to conduct work outside the organization's regular network security boundaries. Data breaches can occur in a number of ways: devices can be lost, stolen, or their security can be compromised by malicious code invading the operating system and applications.

  Mitigation: To promote data security in case a device is lost or stolen, encrypt data on all mobile devices storing sensitive information (i.e., data that carry the risk for harm[1] from an unauthorized or inadvertent disclosure). Until more data encryption, user authentication, and anti-malware solutions become available for mobile devices, the best protection strategy is to implement a strict mobile device usage policy and monitor the network for malicious activity.

- **Cloud Computing.** Delegating the bulk of data protection services to a third party shifts enterprise security architecture. In cloud computing, for example, large amounts of customer data are stored in shared resources, which raises a variety of data encryption and availability issues. Further, the cloud provider faces the same data security responsibilities and challenges as the organization that owns the data, including patching and managing their applications against malicious code.

  Mitigation: Conduct an assessment to compare benefits from adopting cloud computing, including cost savings and increased efficiency, against associated security risks. It is critical to ensure that solutions offered by the cloud provider effectively comply with the organization's information system security requirements, including operational and risk management policies. As cloud solutions and security requirements continue to evolve, periodically review the cost-benefit assessment. Also review applicable requirements of the Family Educational Rights and Privacy Act, in addition to the state, local, and organization's policies and regulations.

- **Removable media.** The use of removable media (e.g., flash drives, CDs, and external hard drives) on an organization's network poses a significant security threat. Without proper protection, these types of media provide a pathway for malware to move between networks or hosts. Following proper security measures when using removable media devices is necessary to decrease the risk of infecting organization's machines or the entire network.

  Mitigation: To minimize the security risks, apply simple preventative steps. These include disabling the "auto run" feature of the operating system on the organization's machines and training users to scan removable media for viruses before opening the files.

[1] Here, harm refers to any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, p. 3-1, 2). Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging).

- **Botnets.** Botnets are networks of compromised computers used by hackers for malicious purposes, usually criminal in nature. If it is discovered that an organization's network has been infected, it is organization's responsibility to notify stakeholders about a potential compromise of all data residing on the network, regardless of whether the data themselves were the target. Clean up efforts resulting from botnet infestation may be costly and damaging to an organization's reputation.

  Mitigation: Since there are many ways computers can become compromised, having a strong security architecture is critical to defending against a malicious botnet attack. Implement a holistic approach to data security and use preventative measures to ensure that the network is secure. Strategies for botnet detection involve analyzing patterns of data sent over the network, and monitoring computer resources usage and external connections.

- **Zero-day Attacks.** A zero-day attack is a threat aimed at exploiting a software application vulnerability before the application vendor becomes aware of it and before the vulnerability becomes widely known to the internet security community. These attacks are among the hardest to mitigate and leave computers and networks extremely vulnerable.

  Mitigation: Unless an organization has access to IT analysts who are highly experienced in technical vulnerability assessment, a frequently recommended approach to mitigation is to wait for the vendor to release a patch that fixes the vulnerability. The organization should keep abreast of the latest software patches and deploy the fix as soon as it is distributed by the developer.

Non-technical Cyber Security Threats to Information Systems

- **Insider.** An insider is defined as someone with legitimate access to the network. Because information accessed by insiders can be easily stolen, copied, deleted, misfiled, or changed, insider threats can be some of the most damaging, regardless of whether they occur due to user carelessness or malicious attempts.

  Mitigation: To mitigate this type of threat, establish and enforce a well-defined privilege rights management system, restricting users' access to certain information and allowing them to only perform specific functions. Audit programs are useful in enforcing access controls and monitoring suspicious activity. In addition, it is recommended that organizations conduct annual training and awareness programs to educate users about insider threats.

- **Poor Passwords.** Implementing a policy on strong user passwords is critical to data protection. It is especially important for users with access to the most sensitive information. Modern password-cracking programs can easily break weak passwords, such as those containing common words or word groups found in a dictionary. For this reason, user-selected passwords are generally considered to be weaker than randomly-generated passwords. User-generated

passwords often follow a predictable pattern or association to something in the user's life (city, family, or pet names for example) and are therefore more vulnerable to password-cracking programs. While randomly-generated passwords may be harder to remember, they are relatively more secure.

Mitigation: Use a professional password-generating program as an enterprise-level solution. A variety of highly-rated programs are available on the market. In addition to implementing procedures for generating strong passwords, train users on how to maintain the security of their passwords, which includes not keeping written passwords in the vicinity of the computer. For enhanced security, consider implementing more advanced authentication capabilities, such as multi-factor authentication.

- **Physical Security.** Physical security is essential to preventing unauthorized access to sensitive data as well as protecting an organization's personnel and resources. An effective physical security system is an integral part of a comprehensive security program. Physical safety measures include securing access to dedicated computers, server rooms, routers, printers, and any areas that process or store sensitive data.

  Mitigation: Establish and enforce a physical security system. Strong physical security includes access control policies and procedures; physical barriers (e.g., fences, doors, locks, safes, etc.); surveillance and alarm systems; and security breach notification, response, and system recovery procedures.

- **Insufficient Backup and Recovery.** Lack of a robust data backup and recovery solution puts an organization's data at risk and undermines the effectiveness of its IT operations. Data and system recovery capabilities allow an organization to reduce the risk of damage associated with a data breach. It is essential to conduct routine backups of critical data and store backup media in a safe and secure manner.

  Mitigation: Establish an organizational policy and specify procedures for data backup, storage, and retrieval. Many advanced data and system backup and recovery tools are available on the market.

- **Improper Destruction**. Paper documents, such as reports and catalogs, may contain sensitive data. Unless these documents are destroyed properly (for example, by shredding or incinerating), they may be salvaged and misused. Discarded electronic devices, such as computers or portable drives, that have been used in processing and storing sensitive data, remain vulnerable unless the data are erased properly. A data breach can occur if recovery tools are used to extract improperly erased or overwritten data.

  Mitigation: Establish a policy for protecting or destroying no longer needed IT assets and media that may contain sensitive data. Several standards organizations offer guidelines that outline best practices for ensuring data are discarded properly, including recommendations published

by the National Institute of Standards and Technology (NIST) titled NIST SP 800-88, "Guidelines for Media Sanitization." (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

- **Social Media.** Using organization's devices and network resources to access social media websites poses a high data security threat. Social networking sites are often targeted by malware, receive a high degree of spam, and are frequently used to gain information for identity theft.

  Mitigation: Introduce and reinforce a policy forbidding access to some social media websites while using an organization's resources and equipment. Train users about the security threats generated by visiting these sites. Organizations that allow access to social media websites should deploy a strong anti-virus and spam filtering solution.

- **Social Engineering.** Breaking into a network does not require technical skills. Access to sensitive information can be gained by manipulating legitimate users after securing their trust. Caution should be advised when communicating any account or network information. This involves making sure the requester is well-known to the user and has a legitimate reason for this information. Socially engineered attacks are the means for some hackers to gain passwords, access codes, IP addresses, router or server names, and other information that can be exploited to break into a network.

  Mitigation: Train users to increase their awareness about social engineering threats and educate them on how to avoid being manipulated. For example, users should be instructed to use caution when someone inquires about their account information or technical information about the network, especially if this person claims to be a network administrator.

Summary

This paper briefly describes various threats to an organization's information system and highlights the importance of implementing a broad approach to data security protection, encompassing both technical and non-technical solutions. Understanding the vast array of threats is the first step in ensuring adequate protection of sensitive data. All networks are vulnerable to cybersecurity threats. A comprehensive data security program is essential for mitigating these threats and preventing a data breach. A holistic approach to data security begins with understanding the network, its architecture, user population, and mission requirements. For example, security risks for networks with large user populations and networks connected to the internet are particularly high. Once the risks have been assessed and organizational security policies specified, a security architecture should be designed and a security plan implemented. Consistent implementation of the security plan will reduce susceptibility to cyber threats and increase the overall security of an organization's data.

Glossary

Configuration management policy also referred to as Secure Configuration Management policy, is the management of security features through control of changes made to hardware, software, firmware, and security documentation throughout the life cycle of an information system.

Network security mechanisms are the security products, and policies used by network security personnel to prevent and monitor unauthorized access misuse, modification, or denial of the information system and network resources. For example, anti-virus and e-mail security software are network security mechanisms.

Perimeter security mechanisms are the specific security policies and products used at the network perimeter which is defined as the boundary between the private locally managed and operated side of the network and the public side of the network. For example a firewall and an intrusion detection system are perimeter security mechanisms.

Personally identifiable information (PII) refers to information, such student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, for more information.

Additional Resources

National Institute of Standards and Technology (NIST) titled NIST SP 800-88, "Guidelines for Media Sanitization."

Department of Homeland Security's Computer Emergency Response Team's (DHS US-CERT) website: www.us-cert.gov/index.html

Carnegie Mellon University Computer Emergency Response Team (CERT) website: http://www.cert.org/

System Administration, Networking, and Security (SANS) Institute website: http://www.sans.org/

PTAC's Data Security Checklist: http://www2.ed.gov/policy/gen/guid/ptac/pdf/ptac-data-security-checklist.pdf