Cyber Security – Best Practices

1. Introduction – What is cyber security and why is it important?

Computers and the Internet have become commonplace in current day society. Every day these systems store, manipulate and exchange business and personal information. Cyber security is the steps taken to protect this information by preventing, detecting and responding to attempts to vandalize, steal or corrupt data.

Organizations need to address cyber security for several reasons. Individuals and employees who have provided personal information to an organization have the expectation that it will be respected and appropriately protected. Organizational data also needs to be protected. Entities that partner or provide services to your organization will want assurance that their information and systems will not be put at risk when electronic transactions occur. Finally, many types of information must be safeguarded due to regulatory requirements. If your organization provides employee health benefits, operates a school or receives credit card payments then security standards such as the Health Insurance Portability & Accountability Act (HIPAA), Family Educational Rights and Privacy (FERPA), and Payment Card Industry Data Security Standards (PCI DSS) apply.

It is not possible for an organization to develop a perfect cyber security plan. Rather, organizations should implement and continuously evaluate cyber security practices that protect sensitive data, while making their computers and networks a difficult target for malicious intent. The following section outlines basic best practices for cyber security in your organization.

General Questions to ask school/district staff:

- What is the most confidential information you have in your department?
- How secure is it on a scale of 1-10?
- Do we need to keep it?
- What would be some recommendations for reducing the risk?

2. Best practices for cyber security.

a. Establish policies/guidelines and educate staff in cyber security principles.

Educate staff on the proper use of computers and other technology devices in your organization. Define what sensitive data is and the types of sensitive data stored on your system. Clearly identify what data needs to be secured and how that protection is accomplished. Create and implement policies/guidelines describing how to handle and protect sensitive information and data. Create a culture of cyber security by establishing basic security practices for all staff, including volunteers. Promote security awareness and education in your organization.

General Discussion Questions:

- Do we have any Information Security policies/guidelines?
- Is our staff aware of these policies and guidelines?
- Do we have security awareness training for existing and new staff?

b. Protect information, computers and networks from cyber-attacks.

Install anti-virus and anti-malware software to keep computers and other technology devices free from viruses, spyware and other malicious programs. Having the latest security software, web browsers, and operating systems also help to defend against these threats. Whenever possible, anti-virus and anti-malware software should updated automatically and run in "real-time" mode to continuously monitor for and mitigate threats should they occur. In addition to real time protection, a complete anti-virus/anti-malware scan of each computer should be performed on a weekly basis.

General Discussion Questions:

- Do we have full 'endpoint protection' which includes anti-virus and anti-malware on all school owned devices?
- Are we monitoring the Endpoint protection system software to identify when a device has been compromised?
- Do we regularly run reports on infected devices? If so, how many devices are infected per month.
- Do we allow staff and students to bring in personal devices and connect to our private network? If so, how are we guaranteeing that these personal devices are not infecting our network?

c. Keep computer operating systems and application software up to date.

Vendors that manufacture computer operating systems and application software are continuously introducing new versions of their product and/or provide patches and bug fixes when a vulnerability is identified. It's important to keep computers and other technology devices up to date as new versions or updates are made available. Many vendors –such as Microsoft and Apple- regularly schedule release updates, but may publish a patch at any time to address a particularly serious threat. Most computer operating systems can be configured to automatically update themselves or provide notification when an update is available. Regardless of the type of operating system or application software used, new versions, patches and fixes should be updated regularly.

General Discussion Questions:

- Do we have any devices (end user or servers) which have unsupported operating systems that are not getting new security updates?
- Is there a plan in place to update devices that are nearing 'end of support'?

- How are we updating the operating systems on our devices? Is it automated?

d. Provide firewall security for your Internet connection.

It is commonplace for most organizations to have an Internet connection that is "always on" exposing computers to external threats 24 hours a day. Firewalls are critical as they help protect Internet-connected computers from these threats. Firewalls may be integrated into a router or wireless access point, provided as a service from your Internet Service Provider, or purchased separately from a firewall manufacturer. Regardless of the type, product updates should be regularly applied and administrative passwords changed when first deployed and regularly over time. Many computer operating systems have an integrated software firewall feature that should be enabled wherever possible. If staff work from home, verify that their home computer system(s) are protected by a firewall and are subject to your organization's cyber security policies and procedures.

General Discussion Questions:

- What is the replacement lifecycle of our firewall?
- Is our current firewall sufficient for our needs? Does it provide an adequate level of protection for our network?
- Is the firewall updated regularly to ensure protection? Are updates postponed for any reason?

e. Create a mobile device action plan.

Mobile devices including smartphones, pads, tablets, USB/memory sticks and mobile hard disk drives create significant data security concerns especially if they contain confidential information or can access computers or data in your internal network. Limit their use wherever possible and require users to encrypt stored data, enable password protection, and install security applications to prevent the theft of information while the device is operating, especially over a public network. Be sure to implement reporting procedures for staff to follow when mobile devices are lost or stolen.

General Discussion Questions:

- Do we have any monitoring or management solution for district owned mobile devices?
- What would happen if my smartphone or tablet was stolen? How would we handle that incident?
- Do we have any guidelines or requirements for what data is available on mobile devices? Do we enforce any passcode to lock devices?

f. Make backup copies of important business data and information.

Regularly backup the data on all computers. Critical data includes –but is not limited to- word processing documents, spreadsheets, databases, human resources files, and financial information including accounts receivable/payable files. Whenever possible, backup data automatically throughout the day and execute a complete backup every night. At the minimum, perform a weekly backup of systems. Store the backup copies either offsite or in the Cloud. Data stored offsite containing personal, financial or health information must be encrypted. Regardless of the frequency in which data is backed up or where copies are kept, establish and test the process for restoring data back to the system.

General Discussion Questions:

- How do our backup systems work? How frequent are the backups?
- If this building were to go down tomorrow what data would be lost?
- Do we have a list of data which we store electronically and has it been identified as to criticality (non-critical, essential, critical, highly critical).

g. Control physical access to your computers and create user accounts for each staff member.

Prevent access or use of business computers by unauthorized individuals. In situations where computer monitors display sensitive data and may be inadvertently viewed, the use of a privacy screen or re-positioning the monitor is suggested. Enable screen savers wherever possible and require a password to unlock the computer. Laptops can be particularly easy targets for theft or can be lost, so physically secure them when unattended. Make sure a separate user account is created for each staff member and require the use of strong passwords. Administrative-level access should be restricted to key personnel only.

General Discussion Questions:

- Does each staff member have their own usernames and passwords?
- Do guests use staff devices? If so, are they monitored when doing so?
- What type of sensitive content have you seen on individual monitors because they didn't close a window or software application when you approached?
- What departments could use a privacy screen?
- Do staff lock their workstations when leaving their office environment?

h. Secure wireless networks.

If you have a Wi-Fi network in your workplace, make sure transmissions are secure and encrypted using the most up-to-date standards. Ensure that administrative access to the router is protected with a strong password. If your organization

provides guest Wi-Fi services, ensure that the guest Wi-Fi network is completely isolated from your workplace Wi-Fi network.

General Discussion Questions:

- What is our current setup with regard to guest wireless access and student/staff wireless access? What access do devices on the guest network have?
- What security measures do we have in place to ensure that our network is protected from unwanted wireless users?
- What is our replacement cycle for wireless? Does this timeframe allow us to have the most secure wireless options?

i. Limit access to data and information; authority to install software.

Limit –wherever possible- the circumstances that provide any one employee access to all data systems. Rather, determine the requirements for each staff person's' specific job function and limit their access to specific systems based on those requirements. Staff should not be able to install any software without permission. Consider the use of content monitoring and filtering systems for those computers that access the Internet.

General Discussion Questions:

- What type of access does a teacher have to their workstation? Can they install software?
- What is the guideline IT uses for creating user permissions?
- Is there anyone person who has access to all data systems including HR/Payroll?
- Do we have updated documentation that lists who has access to sensitive information?

j. Passwords and authentication.

Require staff to use unique passwords and change passwords minimally every three months. Minimally a 6 to 8 digit mix of upper and lower case letters, numbers and special characters is best. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your business partners that handle sensitive data -especially financial institutions- to see if they offer multi-factor authentication for your account.

General Discussion Questions:

- Does staff each have their own passwords?

- Does IT keep a list of everyone's passwords (this is a 'no no')?
- Do we force the changing of passwords? If so, how frequently?
- Is there a minimum character limit on passwords?
- Do staff share passwords or user credentials with each other ('no no')?

k. Don't forget embedded systems and other often missed data sources.

Many organizations have dedicated computers that are used to monitor and control on premise systems such as heating and cooling, lighting, security and telephones. These computers can operate autonomously or by personnel at a remote location and are usually connected via the Internet. Wherever possible, these systems should be completely isolated from other computers in your organization, and, if available, using a separate Internet connection. If it's not possible to completely isolate these devices, they should then be electronically quarantined from other computers and devices to prevent access to secure data or the introduction of viruses or malware. Devices such as copiers, printers, scanners and fax machines are sometimes equipped with internal memory or hard disk drives. Ensure that any internal storage is adequately erased when retiring these devices from active service.

General Discussion Questions:

- What contractors have remote access to our environment? Is the documentation on this updated regularly?
- Do we have Service Level or Confidentiality Agreements with them?
- Have we isolated facilities software and systems from the rest of our network?
- Do we know what happens to our copiers/printers/scanners/fax machines when they are retired and removed from our premises?
- Do those devices have internal storage and is that storage adequately erased?
-

l. Payment Cards

Organizations that accept credit card payments must keep customer data safe. Wherever possible use a third party institution to capture and process credit card data. If credit cards are processed internally, keep only the information absolutely needed, securely disposing of the rest. Carefully control employee access to payment systems and electrically isolate computers that process payments from other organizational computers. Computers that process credit card payment should be restricted from surfing the Internet.

General Discussion Questions:

- What are we using to process credit card information?
- Is it handled internally or by a third party service?
- Do we store credit card information within the district?

- If so, is it physical or electronic?
- Do we have any policies or training on the proper handling of payment cards?

Adapted from the FCC document "Cyber Security for Small Business" and the NIST IR7621 publication "Small Business Information Security: The Fundamentals"

Resource links for additional cyber security information:

- Federal Trade Commission – Identity Theft Information - Website
- FCC Small Business Cyber Planner - Website
- FCC Smartphone Security Checker - Website
- National Initiative for Cyber Security Education – Website
- National Cyber Security Alliance – NCSA – Website
- Security for Small Businesses - Microsoft – PDF
- Stay Sharp on Internet Safety at Work – Website Video
- Microsoft Safety and Cyber Security Center - Website
- Information Security for Churches & Non-Profit Organizations – PDF (dated)
- Visa Data Security – Tips and Tools for Small Merchant Businesses - PDF

Cyber Security – Best Practices

Glossary of terms:

A

Adware
Software that displays advertising content on your computer. Like its cousin spyware, some adware runs with your full knowledge and consent, some doesn't. More often an annoyance than a security risk, adware may also monitor browsing activities and relay that information to someone else over the Internet.

Anti-Virus Software
Anti-virus software is a program or collection of programs that will protect a computer from viruses that try to infect a system. As new viruses are introduced daily, anti-virus software should be updated on a regular basis.

Asymmetric encryption
An encryption method using a widely published public key to encrypt messages, and a corresponding private key to decrypt them.

Attachment
An electronic file (document, image, video clip, program, etc.) that can be attached and sent via email or instant messaging program. Attachments can contain viruses and spyware and should be only opened when received from a reputable source.

B

Backup
An extra copy of computer files, usually kept physically separate from the originals. Essential for recovery when original files are damaged or lost.

Bot or Web bot
Derived from "robot." An automated program, such as a Web crawler, that performs or simulates human actions on the Internet. Used for legitimate purposes by search engines, instant message (IM) programs, and other Internet services. Web bot can also be used to take control of computers, launch attacks, and compromise data; may act as part of a blended threat. See also, *botnet*.

Botnet or zombie armies
A group of computers that have been compromised and brought under the control of an individual. The individual uses malware installed on the compromised computers to launch denial-of-service attacks, send spam, or perpetrate other malicious acts.

BYOD
Acronym for **B**ring **Y**our **O**wn **D**evice. A operational policy adopted by some organizations allowing employees to use personal mobile devices or smartphones to gain access to organizational information.

C

Certificate authority
In public key cryptography, a trusted third party who authenticates entities and their public keys. To do so, certificate authorities issue digital certificates, which validate that a public key belongs to the person whose digital signature is listed on the certificate.

Cookie
A small text file placed on your computer when you visit a Web page. Used to remember you or your preferences when you revisit that page or to track your browsing activities, cookies facilitate virtual shopping carts, page customization, and targeted advertising. They are not programs and cannot read your hard drive or cause damage to your computer.

D

Digital certificate
Also called *public key certificate* or *identity certificate*. In public key cryptography, validates that a public key is owned by the entity sending encrypted or digitally signed data with that key. Digital certificates are issued by a certificate authority and contain the sender's public key plus a digital signature verifying that the certificate is authentic and that the key belongs to the sender.

Digital signature
Used in public key cryptography to validate the integrity of encrypted data and to confirm both the identity of a digital certificate holder and the authenticity of the certificate itself.

Domain spoofing or Domain hijacking
Manipulation of the domain name system to associate a legitimate Web address with an imposter or otherwise malicious website. Used to perpetrate phishing and other types of attack, the user is sent to the imposter website with little or no warning.

DoS
Denial-of-Service. An attack on a computer or network in which bandwidth is flooded or resources are overloaded to the point where the computer or network's services are unavailable to clients. Can also be carried out by malicious code that simply shuts down resources.

Download
The transfer of any type of data between computers. Like attachments above, malicious programs and viruses can accompany files being downloaded.

E

Encryption
A security method that makes information unreadable to anyone who doesn't have a key to decipher it; commonly used to secure online purchases and other transactions. When a website indicates it's "secure," that usually means the data you send and receive is encrypted. See also, *public key cryptography*.

F

Firewall (network)
A hardware or software device, or both, that controls network access and communications between a network and the Internet, or between one part of a network and another.

Firewall (personal)
Software that controls access and communications between a computer and the Internet or a local network. Blocks hackers and other unauthorized traffic, while allowing authorized traffic through.

FTP
File Transfer Protocol. A conventional set of communication rules for transferring files between computers on the

Internet. While most Web browsers can transfer files using FTP, you can also use a dedicated FTP program, which usually provides better security features.

H

Hacker
Commonly, a person who uses programming skills and technical knowledge to gain unauthorized access to computer systems for malicious or criminal purposes. The programming community, however, prefers to use the term "cracker" for such persons; they reserve "hacker" for any well-respected, highly skilled programmer.

HTML
Hypertext Markup Language. The principal language used to create and format Web pages. Controls the layout, design, and display of text, hyperlinks, images, and other media on most Web pages.

HTML tags
The standard set of HTML code elements used to create and format Web pages.

HTTP
Hypertext Transfer Protocol. A conventional set of communication rules for controlling how Web browsers and servers pass information back and forth over the Internet.

HTTPS
HTTP conventions for passing information to a server that's secured using encryption and/or authentication measures. The URLs of websites offering secure HTTP connections begin with "https:".

Hyperlink
A clickable word, phrase, or image that takes you from one Web page to another Web page, or another resource on the Internet. Hyperlinks are created using HTML tags, and when displayed in a browser, they're typically underlined or set apart by a different color.

I

IM
Instant Message. A program that allows two or more people to communicate with one another over the Internet in real time. While most IM communications occur as text, some IM programs also offer streaming audio-visual conferencing and file exchange services. IM can also refer to messages sent by instant messaging, or to the act of sending an instant message.

Internet or the Net
A public, worldwide network of computers and computer networks. The World Wide Web, email, instant messaging, chat rooms, and many other online services and data transmissions are facilitated by the Internet.

IP address
Internet Protocol address. A unique identifier for each computer or other device on a network, including the Internet. Conceptually similar to a phone number, IP addresses are a string of numbers that allow computers, routers, printers, and other devices to recognize [identify] one another and communicate.

K

Keylogger
Software that monitors and captures everything a user types into a computer keyboard. Used for technical support

and surveillance purposes. Can also be integrated into malware and used to gather passwords, user names, and other private information.

M

Malware
Derived from "malicious software." Software designed to do harm by causing damage to systems or data, invading privacy, stealing information, or infiltrating computers without permission. Includes viruses, worms, Trojan horses, some keyloggers, spyware, adware, and bots.

N

Network or computer network
A group of two or more computers connected by cables or wireless signals or both, which can communicate with one another using network protocols. Networks can also include other devices, including printers, routers, and network hubs.

Network hub
A hardware device that connects computers to one another on a local network.

P

Personal Information
Any information that can identify an individual such as their name, address, phone number, Social Security Number, bank account numbers, credit card numbers, etc.

Phishing
An attempt to mislead people into divulging confidential information, such as Social Security numbers and passwords. Phishing typically uses legitimate-looking email or IMs in combination with imposter websites to make fraudulent requests for information (e.g., to go "fishing" for data). See also, *social engineering*.

Pharming
An attempt to defraud Internet surfers by hijacking a website's domain name, or URL, and redirecting users to an imposter website where fraudulent requests for information are made. See also, *URL spoofing*.

Private key
In asymmetric encryption, an unpublished key used to decrypt messages encrypted using a corresponding public key.

Public key
In asymmetric encryption, a key made available to anyone who wants to send an encrypted message to the owner of the key. The owner of the public key uses his or her private key to decrypt messages.

Public key cryptography
An encryption technique using public keys to encrypt messages, digital signatures to validate the integrity of messages, and digital certificates to authenticate the identity of public key owners.

Public key infrastructure (PKI)
A set of standards and services designed to support public key cryptography. Uses digital certificates issued by certificate authorities to authenticate public keys and the entities who own them.

R

Recovery
The process of using backups to restore original data files that have been damaged or are no longer accessible.

Router
A hardware device that connects two networks and directs traffic from one network to the appropriate destination on the other. Often used to connect a network to the Internet, some routers have network firewalls and other features built into them.

S

Symmetric encryption
An encryption method using the same secret key to encrypt and decrypt messages.

SMTP
Simple Mail Transfer Protocol. A conventional set of communication rules for sending email messages over the Internet.

Social engineering
A method of deceiving users into divulging private information, social engineering takes advantage of our natural tendency to trust one another rather than rely solely on technological means to steal information. Often associated with phishing, pharming, spam, and other Internet-based scams.

Spam
Unsolicited email, usually sent in bulk to a large number of random accounts; often contains ads for products or services. Also used in phishing scams and other online fraud. Can be minimized using email filtering software.

Spoofing
Forging an email or instant message to appear as if it came from someone or somewhere other than its true source.

Spyware
Software that collects information about your computer and how you use it and relays that information to someone else over the Internet. Spyware ordinarily runs in the background, and in some cases installs itself on your computer without your knowledge or permission.

T

Trojan horse
A malicious program disguised as legitimate software; often gives someone else the power to take remote control of your computer; may also attack data or systems. Unlike viruses and worms, Trojan horses cannot replicate or propagate themselves and therefore must rely on other methods of distribution.

U

URL
Uniform Resource Locator. A website or Web page's address (e.g., www.symantec.com or www.symantec.com/home_homeoffice/index.html). Browsers use URLs to identify and download Web pages from the Web servers where they're located.

URL spoofing
Attempting to masquerade or closely mimic the URL displayed in a Web browser's address bar. Used in phishing attacks and other online scams to make an imposter website appear legitimate, the attacker obscures the actual URL by overlaying a legitimate looking address or by using a similarly spelled URL.

V

Virus
A program that can self-replicate and infect files, programs, and computer systems. Some viruses simply replicate and spread themselves, while others can also damage your computer system and data.

VoIP
Voice over Internet Protocol. A digital telephone service that facilitates voice transmissions over the Internet or other IP networks.

W

Web page
A file, usually in HTML format, available for retrieval by a browser on the Web. Web pages can contain text, images, and multimedia resources. They usually include hyperlinks to other Web pages or files, and some contain forms through which you can send information to the page host.

Web server
A computer that makes Web pages and other resources available for sharing over the Internet. Using HTTP, Web browsers request pages from Web servers, which then send or download those pages to the requester. Also refers to a program that facilitates a Web server's functions.

WEP
Wired Equivalent Privacy. Part of the 802.11 IEEE standards, WEP is a security protocol for encrypting information and preventing unauthorized access to wireless networks. Designed to provide as much security as hard-wired networks, WEP has serious flaws and has been replaced by WPA and WPA2 as the preferred wireless security protocols.

Wi-Fi
Wireless Fidelity. A play on the term "hi-fidelity." A descriptive term used to refer to 802.11 wireless networks, devices, or anything associated with 802.11 wireless technology (e.g., Wi-Fi hotspot).

Wi-Fi hotspot
A physical area where you can use a Wi-Fi-enabled device to connect to the Internet over a public wireless network. Some hotspots have no security measures in place, while others use WEP or WPA to secure transmissions.

Worm
An often malicious program that can copy and propagate itself over the Internet using email programs or other transport tools. May also compromise the security of an infected computer or cause system and data damage.

WPA
Wi-Fi Protected Access. Part of the 802.11 wireless standards, WPA is an extension and improvement of the WEP security protocol, offering better encryption and user authentication measures.

WPA2

Part of the 802.11 wireless standards, WPA2 enhances the WPA security protocol. WEP, WPA, and WPA2 are all still in use, but WPA and WPA2 offer better protection.