Cyber Insight Day Webinar Q&A
Categorized by Hamilton Best Practice

As background, the National Institute for Standards and Technology (NIST) publishes voluntary standards that address information security and controls to help owners and operators of critical infrastructure to identify, assess, and manage cyber risks. To make it easier to implement these NIST standards, the Center for Internet Security (CIS) (a non-profit organization) has broken down the information into the top 18 controls. Hamilton's 12 best practices are based on the top 18 CIS controls, and answers are consistent with CIS recommendations.

As a sidenote, if a question includes the name of a specific product, we have tried to answer the question posed, but that is not an endorsement of a specific vendor or product. Thank you for your patience while we gathered answers to the questions submitted.

1. Modern Firewall and Antivirus

No questions were submitted for this requirement.

2. Anti-virus Scanning

a. Does a next-gen anti-virus like CrowdStrike Falcon meet the anti-virus requirement, despite not doing scheduled daily scans? If not, would supplementing with Windows Defender scans cover it?

Answer: Yes. A next-gen anti-virus like CrowdStrike Falcon meets the requirement. Supplementing with a program like Defender is a good idea if Defender is configured properly. CrowdStrike can also be used to spot behavior-based activity and malware under a zero-trust based configuration, which in conjunction with Defender, can provide strong security benefits

3. Ransomware Prevention

There were no questions submitted for their requirement.

4. Operating System Patches

a. Do you have a recommendation for patch management software? We run into many issues allowing the automatic MS updates and prefer to not have patches deployed until tested.

Answer: Decisions about a particular type of patch management software should be made in consultation with your IT department or an external provider. It is important to consider a solution that allows you to maximize control, especially with network access. The benefits and costs of the software is a factor that must be weighed.

b. What if the security patch causes incompatibility with another software used for operation-critical solution like finance systems/state testing? Third-party systems might take more than 30 days to deploy compatible updates. Will that impact the requirement?

Answer: No, this will not impact the requirement. If legacy software compatibility becomes an issue, we recommend deciding whether there is another software platform that fulfills your needs while providing up-to-date security. If not, you should consider how to isolate the systems that use this software from your main network as well as how to ensure they are not accessible from the outside. Unpatched systems are a leading root cause of commercial network hacks and must be carefully managed.

c. At times installing the latest patches may cause unintended problems. What's the best practice in terms of attaining a balance between quick patching and preserving functionality?

Answer: Patches should be run in a select group of non-critical systems first during an overnight installation. As an alternative, a virtualized sand box style testing environment can be used. This will allow patches to be run immediately and allow the systems to be tested for proper post-patch functionality.

d. "Do you test the patches before deployment?" What does that mean and how would we turn this into a 'yes'?

Answer: Please refer to answer 4. c

5. Critical Patches

There were no questions submitted for this that were not answered above.

6. Employee Cyber Security Awareness Training

a. Do you have any recommendations for other training materials about internet/computer security in general? Something designed more for general staff to review best practices about identifying phishing attempts, spoofed emails etc. If you can suggest any education material for employees, that would be very helpful.

Answer: Members have access to Keenan SafeSchools and Keenan SafeColleges. The course list includes online courses on Browser Security Basics, Cybersecurity, Email and Messaging Safety, Password Security Basics and Protection Against Malware. See the course lists on the webinar page for additional information. Please contact your Keenan Account Manager for assistance.

b. Is there any state advocacy to mandate this training? With local CBAs it can be difficult to mandate unless there is some legislation.

Answer: There is no legislation mandating cyber security awareness training we are aware of.

c. Do you have a recommendation for interactive cybersecurity training like KnowBe4? We need more than just watching a video from time to time.

Answer: Members have access to Keenan SafeSchools and Keenan SafeColleges. The course list includes online courses on Browser Security Basics, Cybersecurity, Email and Messaging Safety, Password Security Basics and Protection Against Malware. See the course lists on the webinar page for additional information. Please contact your Keenan Account Manager for assistance.

d. Does Keenan have a video that districts can use to train staff during on-boarding and throughout the year as a reminder?

Answer: Yes. Members have access to Keenan SafeSchools and Keenan SafeColleges. The course list includes online courses on Browser Security Basics, Cybersecurity, Email and Messaging Safety, Password Security Basics and Protection Against Malware. See the course lists on the webinar page for additional information. Please contact your Keenan Account Manager for assistance.

7. Network Segregation and Segmentation

a. Can you further define "domain"? Do you mean Windows Active Directory domain or internet domain name? Or some other domain type?

Answer: The term "domain" used during the presentation was used in the context of Windows Domain, as in the local network environment. The requirement is to confirm there is segregation between networks in place, i.e., a firewall to stop malware from passing through.

b. The survey asked if separate domains are used, presumably for student and teacher email access. Can you give an example of what is best practice?

Answer: Best practice would involve a separate network with segregated and separate subnets where all student activities and interaction with the network exist. There would be another separate network for staff. There should be firewalls and if feasible demilitarized zones (DMZs) in place between network segments. Proper authentication must be required for all users, including administrators, to access the staff network or for any user who has access to both.

c. Can you point us to a document that describes or gives examples of the best configuration for segmentation and segregation?

Answer: The Hamilton 12 Best Practices are based on the CIS safeguards, which are a prioritized set of controls to mitigate the most prevalent cyber-attacks against systems and networks. Their information can be accessed here: https://www.cisecurity.org/controls/v8/

The National Institute of Standards and Technology (NIST) has a good guidance document on zero-trust architecture and can be accessed at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

In addition, K12 SIX is non-profit organization that provides school-specific cybersecurity resources and they have a good document called Guide to the NIST Cybersecurity Framework: A K-12 Perspective

d. Can you define and explain more about "software-defined access technology"?

Answer: Software-defined access technology refers to software used to monitor and manage access to systems such as VPN (Virtual Private Network), RDP (Remote Desktop Protocol), gateways, etc., allowing a process to limit access to only those who need it. Most members have already implemented some type of access management. For example: human resources employees have access to the information needed for their position, but do not have access to the business department and accounting information and vice versa.

e. As far as schools go, who has "software-defined access technology for segmentation by grouping and tagging network traffic"? Our IT folks didn't think anyone does this.

Answer: Software-defined access technology is one way to achieve segmentation but is not a requirement. Segmentation of the network is the requirement. There are many technologies or configuration of your current technology that can help you achieve this. You may already have it in place. For example, if your business department does not have access to your human resources department's information, you have segmentation.

Hamilton requires confirmation that access is restricted and the networks have segmentation. Using software-defined access technology is one way to monitor and manage access.

We do not know if this is heavily adopted to date by districts, but cyber security experts strongly recommend it be implemented.

f. Is LAPS recommended?

Answer: LAPS is a useful tool and can be implemented. However, do not place sole reliance on this solution. Ensuring local admins have strong passwords is critical. Additionally, restricting the number of admins, and what data certain admins can access is also critical. Always look to filter decisions especially when it comes to access to data though the "filters" of the need-to-know principles and within the principles of system and networks segmentation. These principles will help guide you to better security.

8. Privilege Access Management

The questions pertinent to privilege access management are about two-factor authentication. They are answered below.

9. Two Factor Authentication (also referred to as Multi Factor Authentication or MFA)

a. Does MFA for "administrators" mean for tech department administrators or also for non-tech administrators? Does it include senior leadership who are non-technical?

b. Who is required to have passwords and MFA enabled? Do we have to enable it for students and/or faculty? Or just those we deem as the biggest risk?

c. Is there a list of devices/accounts that must have 2FA to be considered "covered"? Work email for 2FA seems inappropriate if the purpose is to validate "out of band." Our staff will not use personal devices for codes so we would need to purchase RSA devices.

Answer: Any type of administrator or employee that has privileged access should be required to use MFA. If the administrator or employee has access to technical or sensitive information like business, human resources, PII or PHI of students, MFA should be implemented. The best-case scenario is for all staff to use it when accessing privileged information. If all staff isn't feasible, then all IT/tech admins and other school administrators who access sensitive information should have it. Yes, it includes senior leadership who are non-technical.

If the employees are on premises and using the member's equipment, MFA may not be needed for those employees. Any employee working with highly sensitive data or privileged access should have MFA. **Any employee connecting to the members' system off premises across the internet should have MFA. This includes remote access to work emails.**

The information on not using employee personal devices is included in answers f and g below.

d. How do you feel about Authy?

Answer: We are not commenting on the validity, reliability or effectiveness of any vendor programs.

e. What are your suggestions for student passwords? It was huge hump getting students up to 8 characters. 2FA becomes a larger issue with students as they do not have email accounts. Do we need to be as concerned if students do not have 2FA?

Answer: No, you do not need to be concerned if students do not have 2FA. The requirement from Hamilton applies only to employees. No students should have access to the network containing privileged information. With network segmentation and isolation of sensitive data from student systems, the risks of student accounts being compromised decreases. Students should not have computer access to any of the members' operations.

If you do want to implement a password with more than 8 characters, have the students use a phrase and some numbers. It is easier for them to remember and much harder for hackers to crack their password.

f. What is the average cost to implement a 2FA system?

Answer: Costs vary drastically, depending on the environment and product selected.

g. Does 2FA also include parental access to their Student System Portal?

Answer: Hamilton's requirement does not apply to Student Information Systems (SIS), as long as sensitive information such as student PHI or PII is not stored there. If those items are accessible through the SIS then a 2FA or MFA would be required.

Parental access to any student system portal is not specifically outlined for 2FA or MFA by Hamilton. If there is PII or PHI, then the 2FA or MFA would be required. Does the parent get their own password? If not, it is recommended they have their own password and not utilize the student's password.

h. Google does not offer token-based authentication as a 2FA option, so I don't think there's one silver bullet 2FA device that isn't a cell phone that works for everything. By token, I mean time-based token.

Answer: Correct. Google does not offer token-based authentication as a 2FA option. There are third-party fobs, e.g. YUBI Key, that can be implemented to meet this purpose if employees will not use their cell phones. Whether or not it is a time-based token would be the requirement of the vendor you select and their ability to integrate with Google.

i. For 2FA, is TOTP (Time-based One Time Password) acceptable as a second factor?

Answer: Yes, but it may be difficult to use. It is a great option for password recovery.

TOTP may be an acceptable second factor assuming the absence of an authenticator app and assuming you can secure the transmission of the password and control over the system issuing the codes.

j. Has Hamilton implemented 2FA within a school district? If so, how did they address union concerns and how long did it take?

Answer: No, but intelligence sharing cyber hubs for school districts provide a good option for learning how others have implemented controls such as MFA. K12 SIX is one non-profit organization that provides the opportunity to learn from each other and recently produced a webinar: Dispelling Myths About Multi-Factor Authentication in K12 that provides this level of insight in the K-12 school environment.

k. Is Keenan going to start requiring an MFA solution? If so, can you please provide detailed requirements on this?

Answer: This is a requirement from Hamilton, the insurance company providing cyber coverage for SAFER. They have outlined the 12 best practices needed to offer the same deductible as last year. If the 12 best practices are not met, the district's deductible doubles in the event of a cyber loss.

l. Who can I contact to ask more about MFA?

Answer: Please contact your respective IT vendors. You may already have access to these services.

m. When it comes to enforcing MFA for employees with PII or financial data, do you have any suggestions about CBAs and bargaining units?

Answer: If an employee already has access to PII or financial data, it seems like the confidentiality of this data would already be addressed in their job description. 2FA and MFA are an extension of protecting this data.

n. Does 2FA/MFA lower our liability or policy costs?

Answer: Meeting the 12 Best Practices, as required by Hamilton, will allow members to avoid a doubling of the district's cyber policy deductible. Adherence to these Best Practices will also aide in the prevention and mitigation of cyber related losses.

o. With MFA, could a user log in once a day for all-day access or would you require frequent logins?

Answer: It is possible to allow a user to log in once per day for all access, but it would depend on refresh, the application in question, and the configuration of the applications.

p. MFA requires the end user to have a third-party device (personal phone). How do you deal with the pushback from users that don't want to use their own devices? In considering our bargaining contracts with certificated and classified employees, do we need to think about providing these devices to our staff or paying stipends for use of their personal device? A lot of schools won't be able to force staff to use their personal cell phones for MFA and we worry that unions will push for schools to pay for their phones if that is required.

q. Best Practice 9 says MFA "can be rolled out quickly without busting your budget." Can you give some examples of simple and inexpensive MFA systems?

Answer: If the employees will not use their personal device to receive a code for the MFA or the District is not issuing cell phones, the district will need to issue fobs to meet this requirement. K12 SIX has strategies when faced with union issues. You may want to start with an analysis of who has privileged access before implementing MFA for every employee.

If you are a small district and there are other districts in your area that also need to implement MFA, consider a group purchase of the MFA fobs to reduce the cost.

r. What are considered "high risk actions"?

Answer: High risk actions are considered access to sensitive systems, privileged access to data especially from an off-premises connection.

10. Password Policy

a. Do you recommend prohibiting or allowing browsers to store passwords?

Answer: Yes, it should be prohibited to allow browsers to store passwords.

b. Microsoft's best policy is "Don't require mandatory periodic password resets for user accounts." Is this acceptable?

Answer: Yes, this policy is acceptable and recommended by the NIST. Here is the link to the NIST recommendations: https://pages.nist.gov/800-63-3/

c. Instead of recommending "complex passwords" in the way of adding capital letters, symbols, and numbers, will a random passphrase made of 3-4 random words without the other complexities meet the requirement?

Answer: Yes. This meets the requirement.

d. What do you recommend for keeping track of passwords for all my programs and sites without writing them down? Would a password manager, such as Lastpass, be a good option?

Answer: Yes. Password management tools such as Lastpass are good options.

e. We are a public K-12 school district with accounts for students as young as 5 years old. It's not realistic for us to set a complex password policy for those students. Do we need to have a separate policy for them?

Answer: This Best Practice is specific to employees and does not pertain to student records. FERPA requires student PII and other information be kept private.

11. Offsite Back Up

a. Even if you have sufficient data backups, is it worthwhile to contact the insurance company before attempting to restore any data or hardware loss?

Answer: Yes. Filing a claim can and should be done in conjunction with evidence preservation and containment activities during an incident. The initial contact is free and the coach may be able to help you prevent filing a claim depending on the nature of the situation. There are many issues that need to be considered when connecting data to a network that has been previously compromised. The coach should be consulted before reimaging servers and workstations or repairing any hardware loss/damage due to an attack.

b. Is tape still being used extensively to get the offsite component? And is cloud being considered different media?

Answer: Yes to both questions. Tape is still used, and cloud is considered a different media. It should be noted that cloud should and can be used, but not as the sole form of back-up. There have been cases where cloud back-ups become compromised. If you choose to use cloud, it is advised to still maintain some form of off-site backup.

c. We store our backups in a fireproof safe in a physically separate building across the parking lot from our data center. Is that considered "offsite" enough?

Answer: Yes, this form of offsite storage is considered adequate.

d. If a school has three sites in different physical locations, can an off-site backup count as having a backup on all 3 sites? If something happened to one physical location, the other site across town would have a backup. Or should it be stored in a cloud service?

Answer: This method does count as cold storage/offsite backups with emphasis that the building it is stored in is not the building where the servers are located. The best scenario is to have up-to-date backups in all buildings for all three locations.

e. Regarding backup, how are you backing up Azure / SharePoint / OneDrive / AWS / Google, etc., both from a team level and individual level?

Answer: Cloud storage in conjunction with offsite backup is the preferred best practice.

12. Spam Filters

a. If using Google for email, are third-party products required to meet the spam filtering requirements? I know it filters inbound emails, but I'm not sure about the ability and extent to filter outbound emails and what is required.

Answer: We can't speak to Google's ability to handle spam filtering. Inbound email is the biggest risk to mitigate due to the chance of creating an incident, but encrypting outgoing packets is important as well. We recommend you check with your IT vendor or Google.

13. Other Questions

a. Does double retention apply when/if there is a claim? Or if all elements are not in place does the double retention apply up front for the policy cost/retention.

Answer: Yes. The doubling of the retention applies for losses on or after 9/30/21 if there is a loss and the member has not met the 12 Best Practices required by Hamilton.

b. Does the provided incident response integrate with something like CISA/CIS's incident response?

Answer: No, it does not integrate with a CISA/CIS's incident response. Working within your incident response plan, notify any personnel you're required to. As stated in the webinar, please immediately contact Cipriani & Werner. They will advise what you are legally required to do.

c. Is there a grace period or a time frame to allow implementation of these 12 Best Practices? We only received this notice in May or June.

Answer: The grace period is July 1, 2021 through September 28, 2021. The survey Keenan has sent out is due August 31, 2021. If members are able to meet the 12 Best Practices after 9/28/21, notify your account executive or account manager and Keenan will ask Hamilton for re-consideration of the district(s)' deductible.

d. Do we need to take action when an employee is tricked into transferring personal funds to a bad actor?

Answer: Yes. Immediately upon knowledge of any possible cyber incident, report it to Cipriani & Werner (see SAFER Cyber Claim Reporting Procedure).

e. In the event of a breach, is there a list of providers that the District must use for asset restoration and other types of mitigation in order to be reimbursed? Where can the list be found?

Answer: Immediately upon knowledge of any possible cyber incident, report it to Cipriani & Werner (see SAFER Cyber Claim Reporting Procedure) who will assess the situation and determine the best next steps.

f. We are considering purchasing an annual incident response service retainer with a cyber security vendor. The service would include a cyber security reaction team that would handle all aspects of a security incident. Is this level of service included in your policy?

Answer: Yes. Immediately upon knowledge of any possible cyber incident, report it to Cipriani & Werner (see SAFER Cyber Claim Reporting Procedure). They will assess the situation and determine the best next steps. This includes determining appropriate third-party vendors to contain the incident and support the member in recovery of their business activities.

g. Can we try to contain the damage before calling CyberScout or while waiting for you to answer the phone? What's the process to get in contact with Security Breach Response team if needed?

Answer: Immediately upon knowledge of any possible cyber incident, report it to Cipriani & Werner (see SAFER Cyber Claim Reporting Procedure).

h. What are the specific cybersecurity requirements to be implemented for the 2021-2022 school year to avoid a price escalation? What is the deadline to implement?

Answer: The 12 Best Practices, as required by Hamilton, must be met by 9/28/21 to avoid the increase in member retention. Keenan has sent out a survey due by 8/31/21 inquiring about the districts' status on the 12 Best Practices. If the Best Practices are met after 9/28/21, contact your Keenan representative who will facilitate a review and consideration of reducing the retention.