The K-12 Cybersecurity Resource Center

NEW RESOURCE: "The K-12 Cybersecurity Self-Assessment"

K-12 Cybersecurity Self Assessment

Note: Please print or save your completed self-assessment report. It will not be saved.

K-12 Cybersecurity Self-Assessment Results

Based on the NIST Cybersecurity Framework (Version 1.1) available online at: https://www.nist.gov/cyberframework

==========

Completed: 08/17/2020 13:10

You scored 48 out of a possible 100 points on the K-12 Cybersecurity Self-Assessment.

Based on your answers, your cybersecurity risk exposure rating is HIGH. Improving cybersecurity controls should be an urgent priority for your school district.

==========

CRITICAL ISSUES:

URGENT: It is taking your school district more than 90 days to apply critical patches. This exposes your organization to signifant risk. To learn more, read 'How to Get a Handle on Patch Management:' **https://blog.opsecedu.com/how-to-get-a-handle-on-patch-management/** (-6 points, 'Protect' domain).

URGENT: Your school district does not enforce MFA ('multi-factor authentication') for staff logins to school district IT systems. To learn more, read 'Deploying MFA for staff in a K12 environment:' **https://blog.opsecedu.com/deploying-mfa-for-staff-in-a-k12-environment/** (-6 points, 'Protect' domain).

URGENT: In order to block ransomware and other potentially malicious software from infiltrating school district IT systems and devices, implement controls to block binaries or scripts running from documents (e.g., Microsoft Word macros) on end user devices. For more information, read 'Intel Insight: How to Disable Macros:' **https://www.cisecurity.org/white-papers/intel-insight-how-to-disable-macros/** (-5 points, 'Protect' domain).

SIGNIFICANT: Outbound/egress and DLP (Data Loss Prevention) cyber alerts must be reviewed and investigated promptly. If they are not acted upon, attackers' actions may remain hidden to you as they navigate your network and IT systems and extract your data (-4 points, 'Detect' domain).

Detailed Analysis by Topic Area:

IDENTIFY

You scored 4 out of a possible 11 points in the 'Identify' section of the self-assessment, defined as "developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities." Customized recommendations for your district include:

- **Needs Improvement:** Implement a configuration management database, including a complete inventory of all of your district's applications, clients, network equipment and servers (-2 points).
- **Needs Improvement**: Create/finish a complete list of all vendors that have access to your systems, including a process to keep it up to date (-1 point).
- **On Target:** Great job conducting regular vulnerability scans (at least every 6 months) and remediating issues.
- **Needs Improvement:** Generate and prioritize a list of your district's specific cyber risks, and then assign resources to address the identified threats and vulnerabilities (-2 points).
- **Needs Improvement:** Create an automated process that manages onboarding and offboarding of employees (-1 point).
- **Needs Improvement:** Create a process to automatically reset permissions when staff move from position to position and department to department (-1 point).
- **On Target:** Your school district has updated school board polices that address issues of data privacy, confidentiality and information security. Well done!

PROTECT

You scored 29 out of a possible 60 points in the 'Protect' section of the self-assessment, defined as "developing and implementing appropriate safeguards to ensure delivery of critical services." Customized recommendations for your district include:

- **Needs Improvement**: Record who logs into your network and applications. Credentials get compromised, and you'll need to be able to track the behavior of unauthorized users (-1 point).
- **Making Progress:** Finish implementing a solution to disable all accounts for a compromised user centrally. If centralized account management isn't available, it will be very difficult to isolate a compromised account or user (-1 point).
- **On Target:** Your school district is currently collecting and centralizing logs.
- **On Target:** Your school district's RFP templates include cybersecurity provisions. Be sure to review them regularly and update them as circumstances dictate.
- **Needs Improvement:** Complete formal data sharing agreements with all district vendors and partners that collect, generate, process, and/or store district data. Without agreements, district vendors may be free to share student or

employee PII ('personally identifiable information'), retain data indefinitely, and/or even potentially re-sell district data (-1 point).

- **Needs Improvement:** Encrypt your SIS ('student information system) database at rest and in transit during sessions (-2 points).
- **Needs Improvement:** Encrypt your human resources (HR)/payroll database systems at rest and in transit during sessions (-2 points).
- **On Target:** Your school district is testing and validating backups at least once a month.
- **Needs Improvement:** Properly delete or destroy old fax, copier, and/or printer storage when disposing of devices (-1 point).
- **On Target:** Your school district is actively preventing student and guest traffic from getting to critical staff-only systems like ERP and Grade Marking.
- **On Target:** Your school district has enabled and regularly tunes anti-malware and anti-phishing filtering solutions (for both email and web access).
- **Needs Improvement:** Regularly purge files that are no longer needed by the school district (-1 point).
- **Making Progress:** Your school district only partially prohibits server and global administrative accounts from logging into regular workstations and browsing the web (-1 point).
- **Needs Improvement:** Use tools (like Microsoft LAPS) to create unique administrative/root passwords for all devices (-1 point).
- **Needs Improvement:** Regularly train your users about good cyber hygiene practices, including developing and sharing written policies/guidelines they can reference (-2 points).
- **On Target:** Your school district auto-expires vendor accounts.
- **On Target:** Your school district routinely assesses vendors (including your cloud software vendors) for data privacy and security risks.
- **On Target:** Your school district protects remote access to grade marking tools with MFA ('multi-factor authentication') and/or VPN access (or does not expose grade marking tools to the internet).
- **On Target:** Your school district protects changes to payroll deposits with MFA ('multi-factor authentication') and/or VPN access and/or via other methods, including via an in-person control.
- **Needs Improvement:** Create a system to auto-disable accounts or systems flagged as compromised (-1 point).
- **On Track:** Your school district requires MFA ('Multi factor authentication') for remote desktop access to school district IT systems.
- **On Track:** Your school district encrypts your laptops/mobile devices to protect data against theft and accidental loss.

DETECT

You scored 1 out of a possible 9 points in the 'Detect' section of the self-assessment, defined as "developing and implementing appropriate activities to identify the occurrence of a cybersecurity event." Customized recommendations for your district include:

- **Needs Improvement:** Prohibit your users (via published policy or tech) from putting district files on personal cloud file shares like iCloud and Dropbox (-1 point).

- **Needs Improvement:** Create a snapshot of what "normal" looks like on your school district's authentication and network tools (-1 point).
- **Needs Improvement:** Deploy a SIEM ('security information and event management') solution or similar tool to identify and escalate potentially critical cyber events (-2 points).
- **On Target:** Your school district has audited your users and groups for unexpected permissions within the last 6 months. Keep it up!

RESPOND

You scored 11 out of a possible 16 points in the 'Respond' section of the self-assessment, defined as "developing and implementing appropriate activities to take action regarding a detected cybersecurity incident." Customized recommendations for your district include:

- **On Target:** Your school district has an incident response plan that covers cybersecurity incidents and has tested it.
- **On Track:** Your school district has offsite and offline backups with copies of your installers and keys.
- **Making Progress:** Your school district should ensure its emergency contact list is up-to-date and includes cyber insurance information (-1 point).
- **Needs Improvement:** Ensure that IT staff are cognizant of to whom a cyber incident must be reported and under what timeframe (-1 point).
- **Needs Improvement:** Develop procedures for live memory and disk capture in cases of potentially compromised devices (-1 point).
- **On Track:** Your school district has reviewed and updated its disaster recovery plan within the last six months.
- **Needs Improvement:** Create a press communications plan that can be activated during incident response (-1 point).
- **On Track:** Your district has a relationship with an incident response vendor who can assist in the event of a major cyber event.
- **Needs Improvement:** Implement an event logging protocol to record cyber incident event details, including actions taken to research and remediate incidents (-1 point).

RECOVER

You scored 3 out of a possible 4 points in the 'Recover' section of the self-assessment, defined as "developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident." Customized recommendations for your district include:

- **On Track:** Your school district has identified the priority order/criticality and dependencies of the IT systems you would need to restore in the event of a cyber incident.
- **On Target:** Your school district has cyber response runbooks for commonly experienced issues.
- **On Target:** Thank you for sharing your lessons learned with other peer cybersecurity groups, so that we can all learn from one another and be safer together.
- **Needs Improvement:** Define who has the authority to invoke your school district's incident response and disaster recovery plans (-1 point).

Frequently Asked Questions (FAQs)

- **Why was this self-assessment created?** K-12 leaders need a functional assessment that is *vendor-neutral, free, quick, useful, private, and anonymous*. For more background, read 'Introducing the K-12 Cybersecurity Self-Assessment' by April Mardock.
- **Is this self-assessment truly anonymous?** While skepticism is warranted, the application does not log or collect information that could be used to identify a school district, the individual completing the questionnaire, IT systems used by a school district, or individuals associated with a district (including students or staff). Neither your individual responses nor your resulting report will be shared with any third party or permanently retained. No account is required to take the self-assessment, and the self-assessment must be completed in one browser session.
- **For items that ask about the presence of cybersecurity controls, when should I select the 'partial' response option?** The 'partial' response option exists for situations when a control is either in process of being implemented or is only partially implemented (e.g., on some, but not all IT systems, or for a subset of a user group). In short, you should select this option when you cannot answer 100% yes to all of an items's components, but have nonetheless made some progress. As a self-assessment, you alone are the best judge of when this may apply.
- **Why does this self-assessment give me different feedback than others my district has taken?** This self-assessment is based on the NIST CSF, which is only one cybersecurity risk management framework. Other frameworks exist, each with different pros and cons for the K-12 use case. Moreover, this self-assessment is designed primarily to offer practical and actionable steps that school district IT leaders can take to reduce the cybersecurity risks they may be facing. It is not designed as a substitute for any other (potentially required) compliance testing and reporting with which your school district may have experience. Rather, it should be viewed as additive and any recommendations should be considered in light of your district's specific context, needs, resources, and future plans.
- **How can I provide feedback or ask a question about this self-assessment?** Feedback provided using this contact form will be directed to the appropriate parties.

Breaking News: Cybersecurity Vulnerabilities and Threats

US-CERT Current Activity | US-CERT Alerts | CERT Vulnerability Notes | Dark Reading | Naked Security | Threatpost | OpsecEdu

Malicious Cyber Actors Continue to Target SBA with Fraudulent Schemes

Apache Releases Security Advisory for Struts 2

Joint NSA and FBI Cybersecurity Advisory Discloses Russian Malware Drovorub

SAP Releases August 2020 Security Updates

Microsoft Addresses RCE and Spoofing Vulnerabilities Under Active Exploitation