Readiness and Emergency Management for Schools (REMS)
Technical Assistance (TA) Center

CYBERSECURITY FOR SCHOOLS FACT SHEET

# Cybersecurity Considerations for K-12 Schools and School Districts

Schools (public and nonpublic) and school districts face a myriad of challenging hazards and threats.[1] In addition to natural hazards, technological hazards, and biological hazards, they now have to prepare for human-caused cyber threats. These incidents can be accidental or deliberate and disrupt education and critical operations; expose sensitive personally identifiable information (PII) of students, teachers, and staff; and lead to high recovery costs.

As an example of the impact of these types of threats, students' PII, such as Social Security numbers, was accidentally posted on a Florida school district Website; this resulted in students suing the school board.[2] The full scale of cybersecurity-related incidents such as this one is hard to gauge as most go unreported. Additionally, schools and school districts may be unaware that their IT systems have been compromised, and there is no one Federal department or agency that collects this type of data. However, a report from Privacy Rights Clearinghouse (PRC), a nonprofit consumer education and advocacy organization, provides some indication of the extent of the problem. The PRC reports 788 data breaches have occurred in K-12 schools and institutions of higher education that led to 14,871,122 compromised records since 2005. With the rise of technology use in schools, these figures are likely to only increase. Schools cannot ignore the need to plan for cyber threats in their emergency operations plans.

## CYBERSECURITY AND CYBER SAFETY

Cyber threats can impact either the human (students, teachers, and staff) or the physical or virtual (e.g., information technology [IT] networks and systems) elements of schools and school districts. While there may be some overlap in addressing human versus physical/virtual threats, preparing for each type can require input from different individuals with experience or expertise on that topic and unique actions before, during, and after an incident. Schools may therefore choose to plan for these threats separately, but still under a broader umbrella of cyber threats.

This fact sheet focuses on addressing threats to a **school's or school district's network and systems** also called ***cybersecurity*** considerations. Another fact sheet addressing threats to the human element, called cyber safety, can be found on the REMS TA Center's Website.

[1] *School* refers to all types, including private and public, and all grade levels for the purposes of this fact sheet.
[2] Students sue Miami-Dade school district after Social Security numbers posted online. http://www.miamiherald.com/news/local/education/article157361084.html#storylink=cpy

## Threats Facing School and School District Networks and Systems

According to the Federal Bureau of Investigation (FBI) and the Department of Defense's Defense Technical Information Center, some of the most common types of online threats are

- Data Breach. A data breach is a leak or spill of sensitive, protected, or confidential data from a secure to an insecure environment that are then copied, transmitted, viewed, stolen, or used in an unauthorized manner. Data breaches often occur with confidential information, such as students' records, that may be inappropriately viewed or used by an individual who should not have access to the information.
- Denial of Service. A Denial of Service attack, also known as a Distributed Denial of Service attack, occurs when a server is deliberately overloaded with requests such that the Website shuts down. Users are then unable to access the Website.
- Spoofing/Phishing. Both spoofing and phishing involve the use of fake electronic documents. Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (e.g., passwords, credit card numbers, or bank account information) after directing the user to visit a fake Website.
  - Spear phishing is a more targeted form of phishing and typically involves sending an email that appears to come from a colleague or acquaintance.
- Malware/Scareware. Malware is illicit software that damages or disables computers or computer systems. Similar to malware is scareware, which is malware that uses social engineering to cause fear or anxiety so that a user buys unwanted and unneeded software, such as antivirus software. Ways that computers can become infected include through users downloading a piece of malware or scareware disguised as legitimate software from peer-to-peer file sharing or email attachments or links. To help prevent becoming a victim from malware or scareware, users should keep their software up to date so that any critical software patches are received, and install antivirus software.
  - Ransomware is form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom—typically in virtual currency such as Bitcoin—for the users to regain access to their data. An example of ransomware is WannaCry, which infected computers across the globe in May 2017. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or images if the victim does not pay. The ransomware is frequently delivered through phishing/spoofing scams.

- Unpatched or Outdated Software Vulnerabilities. Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest software updates; thus, unauthorized users can gain access to information networks and systems.
- Removable Media. Media devices that can be connected to computers, such as thumb drives, CDs, DVDs, and external hard drives, also pose challenges to cybersecurity. First, these storage devices can be easily stolen. Second, corrupted devices can be intentionally or unwittingly connected to computers. Once opened, files from the device can then infect the computer with malware.

## Preparing for Threats

Schools and school districts can take a variety of actions to prevent, protect from, mitigate the effects of, respond to, and recover from cyber threats. These can be conducted before, during, and after an incident.

### Before an Incident

To protect their networks and systems as part of an overall preparedness program, schools and school districts can do the following:

- Develop and promote policies on responsible use. Before students, teachers, or staff access the school's or school district's networks and systems, they should be aware of any policies, rules, or laws regarding their use. The whole school community can be required to accept a Responsible Use Policy (see the REMS TA Center's "Cyber Safety Considerations for K-12 Schools and School Districts" fact sheet for more information). IT staff should also be aware of local, state, and Federal regulations about information security, privacy, and storage of PII.
- Store data securely to ensure that the whole school community's data are kept private and to comply with the Family Educational Rights and Privacy Act (FERPA). Ease of access to and use of cloud-based software makes this issue especially important, as this technology allows teachers and staff members to easily store and share students' personal information. Schools and school districts also need to regularly back up their data in case of accidental or deliberate corruption or destruction of data.
- Create firewalls and an approved list of individuals who have access to the school's or school district's networks and systems. The list should be regularly reviewed to ensure that only those individuals who have permission to access the systems can do so.
- Monitor networks continually to assess the risk from cyber threats. Schools and school districts can get support from the U.S. Department of Homeland Security (DHS; see below for more information) or data security firms.

Schools and school districts may also want to consider purchasing cyber insurance for themselves and require any contractors to purchase it as well, as commercial general liability and property insurance policies do not typically cover cyber risks. Cyber insurance policies can help pay for legal fees, credit monitoring for those impacted by a data breach, financial losses, and other services.

## During an Incident

Members of the school community need to know to whom they should report a cybersecurity incident, such as a data breach. In most cases, the first point of contact will likely be the school's or school district's IT manager or team. School and school district technical and leadership teams should then work to limit the damage and preserve sensitive information. Decisions may also need to be made about whether to request external assistance and from whom, such as from the school district; a local, state, or Federal government computer incident response team; or private vendor.

Law enforcement should be notified after an incident, as well as any individuals whose personal information may have been compromised. A report can be made to the

- FBI, via a Field Office Cyber Task Force;
- Internet Crime Complaint Center;
- National Cyber Investigative Joint Task Force (cywatch@ic.fbi.gov);
- National Cybersecurity and Communications Integration Center (NCCIC@hq.dhs.gov); or
- U.S. Computer Emergency Readiness Team (US-CERT).

## After an Incident

Once the incident has been contained, recovery may be needed for people, policies, and technology—all of which are interconnected. The response team will need to identify what *people* were impacted by the incident or caused the incident; in some cases, a cyber incident may have been caused by a user who conducted malicious activity. *Policies* may need to be revised, or new ones implemented, to prevent future cyber incidents from occurring. Finally, the school or school district needs to identify how *technology* was impacted and address any issues. For example, does malicious software need to be uninstalled?

Response teams should also conduct an After-Action Review or lessons learned meeting after an actual event or exercise to capture and document information from the event and make appropriate revisions to plans.

## Relation to Emergency Operation Plan (EOP) Development and Planning

The *Guide for Developing High-Quality School Emergency Operations Plans (School Guide)* was developed in partnership with six Federal departments and agencies, including the U.S. Department of Education (ED), with roles and responsibilities in emergency preparedness. The *School Guide* provides a recommended six-step planning process that is cyclical and ongoing to help schools develop a high-quality EOP and lists several threats and hazards that schools may want to include in the plan, including cyber incidents. This type of threat can be addressed in a Cyber Annex to the EOP, which can address both cybersecurity (i.e., IT systems and networks) and cyber safety (i.e., the human element).

When developing activities to address cyber threats before, during, and after an event occurs, a planning team can progress through the six steps as follows.

**Step 1: Form a collaborative planning team.** The planning team will likely comprise a core planning team, school personnel, community partners, and a school district representative. To address cyber threats, the planning team can seek the input of additional individuals such as IT staff; local, state, and Federal law enforcement; and emergency management, among others.

**Step 2: Understand the situation.** Here, the planning teams identifies threats—such as cyber threats—and hazards to the school and surrounding community using a variety of assessment tools, assesses those risks, and prioritizes them for inclusion in the EOP. Some assessments, such as scanning of school and school district networks and systems, may be ongoing. Others, such as identifying what threats or hazards the school or school district faces, can occur less frequently, such as annually.

### SIX-STEP PLANNING PROCESS

- **Step 1**: Form a collaborative planning team.
- **Step 2**: Understand the situation.
- **Step 3**: Determine goals and objectives.
- **Step 4**: Plan development (identify courses of action).
- **Step 5**: Plan preparation, review, and approval.
- **Step 6**: Plan implementation and maintenance.

**Step 3: Determine goals and objectives** and **Step 4: Plan development (identify courses of action).** In these steps, the planning team develops goals, objectives, and courses of action for before, during, and after each type of prioritized threat or hazard identified in Step 2.

Schools and school districts have several free resources that can aid in the creation of goals, objectives, and courses of action to address cyber threats to the school's IT infrastructure. First, the planning team may want to consider the activities described in *Framework for Improving Critical Infrastructure Cybersecurity*, which was released by the National Institute of Standards and Technology (NIST) to help reduce cyber risks (see the Key Resources section below for more information). The Framework comprises the five core functions of Identify, Protect, Detect, Respond, and Recover, which provide the overall framework for cybersecurity activities.

The National Cybersecurity Assessments and Technical Services team, which is a division of the DHS National Cybersecurity and Communications Integration Center, can be especially helpful with supporting the core functions of Identify, Protect, and Detect through its Cyber Hygiene (CyHy), Phishing Campaign Assessment (PCA), and Risk and Vulnerability Assessments (RVA):

1. CyHy comprises vulnerability scans with weekly reports, which are mostly automated after being established.
2. PCA measures the likelihood that the school community will click on email phishing lures.
3. As part of a RVA, schools can request assistance from DHS with phishing, wireless, and Web application assessments. Additional support includes network mapping, vulnerability scanning, penetration testing, operations systems security, and database security.

For more information, email ncats_info@hq.dhs.gov

CoSN (Consortium for School Networking) also provides a toolkit that includes a self-assessment for school districts to measure their digital security, a planning rubric to assess readiness, and a planning template to prioritize improvements.

**Step 5: Plan preparation, review, and approval.** In this step, a draft of the EOP is written and circulated to obtain feedback from those responsible for implementing the document. Edits are made based on those comments, and approval is obtained from the appropriate leadership.

As the Cyber Annex will address both cybersecurity and cyber safety, this part of the document will include goals, objectives, and courses of action for keeping both the school's IT systems and networks and the students safe. Additional goals, objectives, and courses of action may also be included in functional annexes, which describe cross-cutting activities before, during, and after threats and hazards. For those relating to IT infrastructure, these functional annexes could include a Continuity of Operations annex—which describes how the learning environment will continue after a major incident for up to 30 days—and a Recovery Annex, which addresses academics; physical and structural concerns; business functions; and social, emotional, and behavioral recovery.

**Step 6: Plan implementation and maintenance.** In this final step, schools and school districts implement the activities described in the EOP, including conducting training or professional development for those who have a role or responsibilities in an emergency. Exercises are also conducted to test the school's or school district's ability to respond to a threat or hazard, and the plan is reviewed at least annually. As new cyber threats are constantly emerging, planning teams may decide to review the Cyber Annex more frequently.

## Summary

The Internet has brought obvious benefits to the K-12 community, such as the ability to provide online instruction and communicate with teachers and other individuals anywhere in the world. However, with these benefits come challenges, such as cyber threats to school and school district IT systems and networks, such as data breaches and Denial of Service attacks. Preparedness activities to address such threats include developing and promoting policies on responsible use, storing data securely, and creating firewalls. Planning teams should also consider what actions should be taken before, during, and after an incident occurs when creating a Cyber Annex to the EOP, taking into consideration privacy and confidentiality of the school community.

## Key Resources

Several Federal and national publications and organizations support schools and school districts with cybersecurity. These include the following:

- *Framework for Improving Critical Infrastructure Cybersecurity*, NIST. The voluntary Framework was developed as collaborative effort among government agencies and departments, academia, and the private sector to help organizations manage their cybersecurity risk. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- Critical Infrastructure Cyber Community ($C^3$) Voluntary Program, US-CERT. To help organizations that want to use the *Framework for Improving Critical Infrastructure Cybersecurity* to strengthen their IT networks and systems, DHS launched the $C^3$ program. The program connects organizations to Federal departments and agencies and the private sector with expertise in managing cyber risks and provides cyber-related resources. https://www.us-cert.gov/ccubedvp
- Integrating Cybersecurity with Emergency Operations Plans (EOPs) for K-12 Schools Webinar, REMS TA Center. In this archived Webinar, presenters provide an overview of the landscape of cyber threats facing K-12 schools. Also shared were resources, programs, and tools to help schools maintain secure networks and prevent cyber attacks. http://rems.ed.gov/IntegratingCybersecurityForK12.aspx

- Office of Educational Technology (OET) Web page, U.S. Department of Education (ED). The OET develops national educational technology strategy and policy for how technology can be used by K-12, higher education, and adult education leaners. https://tech.ed.gov/

### Privacy and Confidentiality Regulations and Laws

To help protect against cyber threats and ensure students' privacy, confidentiality of information, and safety online, schools and school districts need to be aware of several Federal regulations and laws that may apply to them or third-party vendors they use:

- Family Educational Rights and Privacy Act (FERPA). FERPA gives parents and eligible students rights to inspect and review the student's education records maintained by the student's school, request that the school amend those records, consent in writing to the disclosure of PII, and file a complaint about a violation under FERPA with the Family Policy Compliance Office.

*Learn more about information sharing in the school setting by visiting this REMS TA Center Information Sharing Web page.*

*Get details on state Data Security Laws from the National Conference of State Legislatures.*

- Children's Internet Protection Act (CIPA). CIPA aims to protect children from obscene or harmful content on the Internet. CIPA states that schools or libraries that are eligible to receive discounts for telecommunications, Internet access, or internal connections through the E-rate program (Universal Service Program for Schools and Libraries) must certify they have an Internet safety policy that blocks or filters access to pictures that are obscene, child pornography, or harmful to minors.
- Protection of Pupil Rights Amendment (PPRA). PPRA applies to schools and contractors that receive funding from ED and seeks to ensure that parents can look at instructional materials that will be used in connection with an ED-funded survey, analysis, or evaluation in which their children will participate. Schools and contractors must also obtain written approval before students who are minors participate in any ED-funded survey, analysis, or evaluation that reveals certain information.

These laws do not describe every possible legal consideration, so schools and school districts should work with their Office of General Counsel to consider application of other relevant Federal, state, and local laws.