Cyber Security Essentials

For Heads and Other School Leaders

Today's Panelist

Jamie Britto
Chief Information Officer
Collegiate School
jbritto@collegiate-va.org

Sarah Hanawald
Executive Director
ATLIS
sarah@theatlis.org

Bob Olsen
Director
Navigant
robert.olsen@navigant.com

Today's Objectives

- Understand the ways in which you and other school leaders are targets for cyber crime
- Gain an executive understanding of how you can defend yourself and your school
- Learn how to form a cyber security team and ask them the right questions

Cyber Attacks on Independent Schools

- Head's email account is compromised; sensitive information is accessed, bank accounts are created
- Trustee's email account is compromised and used to transfer money
- Head's email is spoofed, money is erroneously sent

3 Ways to Protect Yourself

- Use multi factor authentication on your email accounts and other accounts when possible
- Use screen locks on computers, tablets, and phones
- Encrypt your hard drive so that you can
- “reasonably” protect sensitive information

3 Ways to Protect Your School

- Conduct a Cyber Security Audit
- Ask your tech department to send simulated phishing attacks
- Apply for Cyber Security Insurance

Form a Team

- Bring together risk management, technology, and sensitive data users
- Get to work on multi factor, screen locks, and disc encryption
- Review and respond to ATLIS recommendations

Cybersecurity Recommendations for Independent Schools

Independent schools are increasingly relying on technology and electronic data to manage every aspect of school operations, including many that involve protected information. Activities that involve protected or sensitive data include; making admission and financial aid decisions, guiding college searches, managing payroll, and reaching alumni. Independent school leaders **must** act to protect the school's resources and information. The risks of reputational harm and financial losses following a cybersecurity breach have been made clear in recent years. Further, independent school leaders must monitor developments in state laws requiring that school-collected data be safeguarded. The primary obligation for protecting data is assigned to the school, not to the company or organization the school selects for storing or managing data (e.g. a software company, data backup service, offsite storage, etc.).

Each school must take into consideration the security needs of the school community, the resources available, and the overall risk-management stance of the school. ATLIS recommends that heads of school and technology directors work together to form a cybersecurity team serving as a standing group that includes:

- Technology department leadership
- Risk management leadership from both the administration and the board
- Key employees who handle secure and/or privileged data

Responsibilities of the team:

1. Assess the school's current cybersecurity plans, resources, and measures.
2. Assess and update the knowledge level of the team members.
3. Conduct an annual review of the school's cybersecurity stance, policies and procedures, the threat landscape, training program, and insurance coverage.
4. Periodically, but at minimum every 3 years, oversee and respond to an external audit of the school's cybersecurity.

First Steps:
ATLIS recommends that the cybersecurity team review the school's needs and determine what level of security the school has currently, where the school needs to be in the short-term, and what the long-term goals are for the school. The levels below spell out guidelines to help schools prioritize. Many schools may choose to implement level one across the board and then add in selected higher-level recommendations based on the school's specific circumstances. The intent of the below document is to provide guidance in more accessible language that the school's IT staff will be able to use in discussions with colleagues and the campus cybersecurity team.

Links to sites with more technical information and term definitions can be found using the resources at the bottom of this chart.

Security	Configuration/Technical	Personnel Procedures	General Policies
First Steps	A plan for making and securing data backups (offsite) at determined levels of frequency to enable disaster recovery and provide options in the event of a cyber attack. Antivirus and malware protection software provided campus-wide.	In-person training for all privileged data users.	Develop baseline business continuity and disaster recovery plans.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level One	Multi-factor authentication for campus users with access to secure or sensitive data Total drive encryption on laptops for employees with access to privileged data such as admission, advancement, finance, medical, etc. A firewall providing dynamic packet filtering The security configuration of all devices on campus are deliberately set, implemented, and actively managed to meet campus security needs.	Background checks upon hire. Baseline simulated phishing attack. Administrative privilege/access managed and limited. Password policies (regarding complexity and scheduled changes) communicated and enforced. General awareness training periodically (annually at minimum) provided to entire faculty and staff in groups. Offboarding procedures designed to remove access to all school technology resources upon departure. Internal privacy and confidentiality policies that are published, enforced, and updated that focus on handling of secure data.	Cyber insurance or similar coverage and services. Determine, communicate, and enforce controls about what devices and software programs are permitted to connect to the campus network. Analyze the school's need for PCI compliance; review and implement accordingly. Review data security policies for all software purchases that involve protected data. Policy on third party remote access to systems, e.g. HVAC, POS, security. Ensure technology department leader undergoes annual cybersecurity professional development. Physical controls for data center and network closets with locked, secured areas for key network resources.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level Two	Network segmentation separates mission-critical network from other areas. Baseline network scans with reviews of the results performed semi-annually (at minimum) to determine vulnerabilities Create logs of network activity that can be analyzed to detect, prevent, or recover from an attack. Whole disk encryption for all employee laptops. Firewall: minimum level plus intrusion prevention Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers	Specific employee designated as responsible for cybersecurity. Cybersecurity training included as part of employee onboarding. Additional offboarding procedures identified with the departure of technology employees. Students digital citizenship curriculum includes cybersecurity training at an age-appropriate level. Regular training and ongoing briefings for key data stewards. Testing of employee responses in simulated cybersecurity scenarios. Follow-up training for those identified as needing it through the testing. Password vaults for admin users to protect key systems.	Annual review of cloud based security agreements Third party audit of cybersecurity stance Business continuity and disaster recovery plans fully developed in writing. Incident response plan developed and shared in writing. Review data security policies for all software purchases. Access logs maintained for key physical network resources. Remote working policies determining who can work remotely and when VPN encryption is needed.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level Three	Periodic internal and external network security scans. Whole disk encryption for all employee laptops and desktops. Firewall: Next generation firewall with configuration evaluation and review taking place semi-annually (at minimum).	Regular and varied training activities and drills to refresh skills for all users. Formal certification for individual charged with overseeing cybersecurity within the technology department.	Business continuity plans tested in a drill. Single tunnel VPN required when users work remotely. Meet and/or address top 20 controls defined by the Center for Internet Security,

Further resources:

ATLIS: Sample policies, templates, how-to webinars

Center for Internet Security: Comprehensive site including certification processes for cybersecurity professionals

US Computer Emergency Readiness Team offers mailing lists and feeds for a variety of products, including the National Cyber Awareness System and Current Activity updates.

National Initiative for Cybersecurity Careers and Studies: glossary of cybersecurity technical terms and definitions

ATLIS Cyber Threat Assessment
February 2018

The ATLIS Cybersecurity Advisory Panel, comprised of ATLIS members and cybersecurity professionals, has identified and prioritized the top nine threats currently facing independent schools. To compile the list, the panel reviewed the 2017 *Verizon Data Breach Investigation Report*, ATLIS member surveys and data, the experiences of Compass Cyber Security's clients, and RSM, LLC's 2017 *Cybersecurity Outlook and Key Considerations for Nonprofits.*

1. **Email Inboxes**
   Email is the source of over 80% of successful cyber attacks. The attacks tend to take the form of Ransomware, Phishing Attacks, and Business Email Compromise.
   The most effective defense against these attacks is employee training, particularly
   - simulated phishing attacks;
   - email filtering;
   - enabling multi-factor authentication.

2. **Employee Mistakes**
   Employees at schools have accidentally disclosed sensitive information to third-party vendors, have broken policies by storing sensitive data in unauthorized locations, and have been duped into sending money and protected data to criminals.
   Protect against employee mistakes by
   - regularly reviewing school policies;
   - discussing policies with users of sensitive or protected data;
   - providing ongoing professional development around cyber threats.

3. **Out-of-Date Software**
   The Wanna Cry Ransomware attacks of May 2017 highlighted the issue that out-of-date and unpatched operating systems make schools vulnerable to a variety of attacks. The exposure of National Security Agency hacking tools increases the importance of keeping school systems up-to-the-minute current.

   To minimize risk, keep computers up-to-date by adopting these practices:
   - use patch management systems like Meraki or Windows Update Servers;
   - consider limiting end-users' administrative rights on issued computers;
   - maintain an application/program whitelist;
   - establish a new application vetting process;
   - conduct periodic vulnerability scanning to identify unpatched systems and provide prioritized remediation steps.

4. **Unencrypted Drives**
   When an unencrypted drive is lost or stolen, the school must consider its data to be “out in the open.”
   The panel recommends that schools encrypt drives containing school data. Drive encryption allows schools to reasonably conclude that no data was released into the open and saves the time, pain, and expense of forensically accounting for and reporting any data as potentially released

5. **Malicious Software**
   Malware is a general term that encompasses many types of online threats including spyware, viruses, worms, trojans, adware, ransomware, and more. These types of software range from nuisances to serious threats.
   To minimize individual computers becoming infected with malware:
   - install comprehensive antivirus software on every machine;
   - ensure that the protective software is updated regularly and automatically;
   - consider restricting end-users’ ability to download and install software.

6. **Unauthorized Network Access**
   Criminals and vandals want to access school networks to steal valuable data, damage school equipment, and erase or encrypt files.
   To reduce the likelihood of unauthorized access, address these essential practices:
   - use a firewall;
   - segment network traffic;
   - scan the network regularly;
   - review configurations, scans, and policies quarterly, (or at the very least annually), to assess the potential for unauthorized access, keeping in mind the ingenuity and skill of bad actors;
   - monitor logs and analyze critical assets (firewalls, routers, servers) for suspicious behavior.

7. **School Affiliations**
   If a school is affiliated with a national, religious, or cultural identity that is frequently a target of cyber attacks, or if the school enrolls children from high-profile families, the school may be at increased risk for the above threats as well as for denial of service attacks and other purely disruptive or destructive events.

   In these scenarios, the panel recommends subscribing to threat intelligence feeds from the Department of Homeland Security (see resource 3, below) and other federal agencies that can provide an early warning system. Parent organization networks may also prove valuable in assessing risks.

8. **Doxing**
   Criminals have recently demanded extortion payments from schools to prevent the publication of sensitive information stolen from compromised systems. One of most infamous examples involved an attack on Iowa's Johnston Community Schools District in October of 2017. While still a relatively small threat, doxing highlights increasingly sophisticated and creative ways hackers are finding to make money from targeted schools. Taking the steps listed above, particularly in 1,2,4, and 5, should help keep sensitive information out of the wrong hands.

9. **Acts of God**
   Storms, power outages, and fires can disrupt school data and IT services and make everyday operations difficult.
   To address this possibility, the panel recommends these practices to help schools get up and running as quickly as possible after a disruption:
   - equip the school with redundant systems, batteries, and generators;
   - procure secure off-campus storage for data and essential server configurations.

This document contains general information for the use of our members. It is not a substitute for professional advice or services. This document does not constitute legal, technical, or other professional advice and you should consult a qualified professional advisor before taking any action based on the information included. ATLIS, its affiliates, and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person or organization.

Resources

1. Verizon, "How long since you took a hard look at your cybersecurity?" Video; *2017 Data Breach Investigations Report: Executive Summary,* 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.
2. RSM, "Cybersecurity Outlook and Key Considerations for Nonprofits," 2017. http://rsmus.com/content/dam/mcgladrey/pdf_download/wc_cybersecurity_outlook_key_considerations_nonprofit.pdf.
3. US-CERT (Computer Emergency Readiness Team) offers mailing lists and feeds for a variety of products, including the National Cyber Awareness System and Current Activity updates. The National Cyber Awareness System was created to ensure that you have access to timely information about security topics and threats. https://www.us-cert.gov/mailing-lists-and-feeds
4. Linh Ta and Jason Clayworth, "'Dark Overlord' hackers posted stolen student info, Johnston officials say," *Des Moines Register,* Oct. 5, 2017. https://www.desmoinesregister.com/story/news/crime-and-courts/2017/10/05/dark-overlord-hacker-johnston-schools-threats/735950001/.

For more information, please contact Susan Davis, Prof. Development, ATLIS, sdavis@theatlis.org.