ATLIS Cyber Threat Assessment August 2017

The ATLIS Cybersecurity Advisory Panel, comprised of ATLIS members and cybersecurity professionals, has identified and prioritized the top seven 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.*

The threats are:

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, such as password protecting sensitive files and not sharing the passwords in email,**
   - **providing ongoing professional development around cyber threats.**

3. **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 having to account for and report any data as potentially released.

4. **Out-of-Date Software**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.**

5. **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 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.**

6. **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.**

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 measures.

   In these scenarios, the panel recommends subscribing to threat intelligence feeds from the

Department of Homeland Security and other federal agencies that can provide an early warning system. Parent organization networks may also prove valuable in assessing risks.

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