Data Security: The First Step to Protect Student Privacy

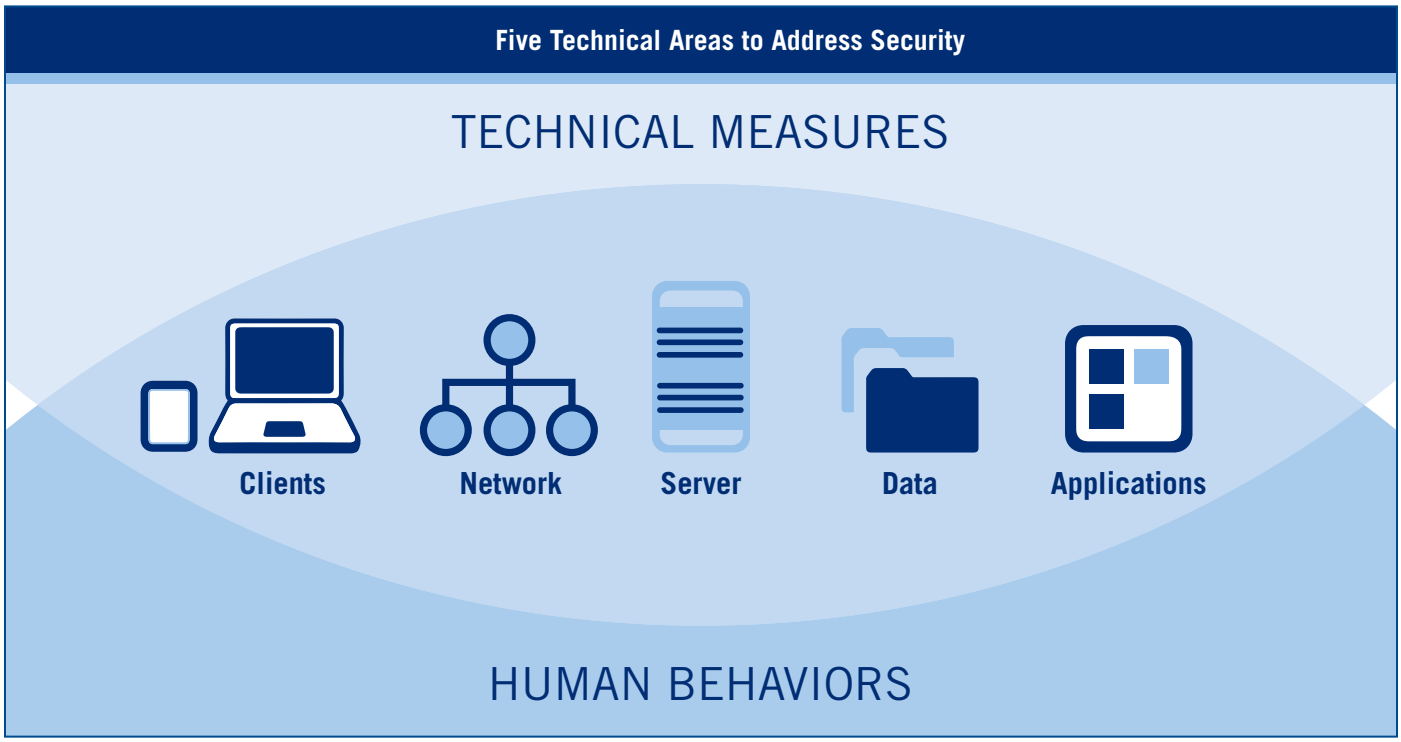
BY BOB MOORE
RJM Strategies, LLC

Data Security – While the term "security" may not be as provocative as "privacy," security breaches almost always become privacy crises. Recently, when it was reported that 1.2 billion passwords had been stolen from some 420,000 web sites, thoughts immediately turned to loss of privacy. When a large retailer suffered a data security breach of its credit card system, the headlines talked about breaches of consumer privacy. A breach of a school's student information system raises massive privacy concerns, but it starts as a security breach. Ensuring security of data does not ensure privacy, but without effective security measures, there can be no expectation of privacy.

In *Making Sense of Student Data Privacy* (http://www.k12blueprint.com/privacy), released in May 2014, I wrote briefly about data security and included it as one of the critical steps that every district should take to ensure privacy. The intent of this analyst report is to present the practical steps that every school technology leader should be taking to ensure security of data, with protecting privacy as the end in mind.

The idea of robust data security in an academic setting may be off-putting to some as it may imply restrictions on technology use that could be roadblocks to innovation in the classroom. While strong security protocols are not necessarily in conflict with academic freedom, the reality is that it is very difficult to provide an "anything goes" technology environment, while at the same time protect privacy in a way that meets parent, student, and staff expectations.

Think of data security in terms of overlapping layers of protection. The various layers include the client device, network, server (both in-district and cloud), data, and applications. Within each of these layers there are technical considerations, as well as human behavioral considerations. For IT security experts this may seem like an over-simplification, but security can get very technical, and with that it can overwhelm even the most technically savvy IT professional. The purpose here is not to delve into the technical issues, rather to present some practical steps every school technology leader can take, regardless of the technical expertise of their staff. Before describing those steps, let's consider the layers.



Client Device – Some devices are inherently more secure than others. Those designed for institutional use, rather than simple consumer use, tend to have more security features built in. Device security features may include things such as data encryption enabled by the device OS, as in Windows 8.1, but that is only one part of device security. Device security depends largely on the ability to keep the OS of the device up-to-date. Security patches are released frequently and devices such as tablets designed for consumer use are typically much more cumbersome to update, whereas devices built for organization use are easily and efficiently managed.

Network – This refers to the networks inside the district, whether LAN or WAN, wired or wireless. Network security technology and protocols are plentiful and mature. There are established best practices for network security. Open, freely available wireless networks are a security breach waiting to happen. Take advantage of the security features that are built into your network switches, routers and access points.

Servers – In this case, the term "servers" is a catch-all term referring to a wide range of devices, physical and virtual, housed both in-district, as well as cloud-based managed by service providers. Change management processes and lack of documentation can be a challenge for even the most disciplined IT team that is rushing to meet the needs of very demanding end users. ITIL (Information Technology Infrastructure Library) offers a set of widely adopted IT service management practices that can be very helpful. Find out more at http://www.itil-officialsite.com. The ISO/IEC (International Standards Organization/International Electrotechnical Commission) publishes joint security standards for cloud services. Learn more at http://www.iso27001security.com/html/27017.html.

Data – Securing data is much more complex than preventing unauthorized access to data using something like a password. Encrypting data on client devices can also be a useful practice. You also have to give significant thought to who has access to certain data. In addition, the erasure, or destruction of data is critical. The NIST (National Institute of Standards and Technology) is the go-to source to understand the current requirements for data destruction best practices. NIST has many IT security resources at http://www.nist.gov/information-technology-portal.cfm.

Applications – Applications can refer to software installed on a computer, run from a server in your data center or from a cloud based service, as well as apps installed on a tablet or smart-phone. While applications can create significant security risks, you often have little or no control over how the application is coded and, thus, no control of the security. You should ask security questions of an online service provider and can have security provisions written into a contract. You can also have mission critical applications tested for security as suggested in step nine below.

10 Data Security Steps Every School District Should Take Today

1. **Designate a Security Lead for IT –** IT departments can be organized in any number of different ways. Regardless of what your organizational chart looks like, there needs to be a senior technical staff member designated as the security lead. They need to have the technical knowledge necessary to understand security issues in all facets of IT operations. Specialists in each area will still have security responsibilities, but one person needs to see how all of the pieces fit and where there are gaps.
2. **Communicate to Stakeholders –** All stakeholders need to understand why certain security measures are undertaken. For example, rather than simply notifying staff of a new password policy that requires longer/more complex passwords or more frequent changes, discuss the proposed change with other district administrative leadership and teacher leaders. Seek input on proposed changes and help others to understand why the changes are important. IT leaders who approach security issues in a dictatorial manner often experience significant backlash and lack of support for the most reasonable security practices.
3. **Seek Legal Counsel –** Breaches of data security can have legal implications, particularly if those breaches result in privacy issues. Your state may have legal requirements regarding public notification should a data breach occur. Make sure your district's legal counsel is familiar with data security-related issues. Once a breach has occurred you'll need to act quickly and knowing who to turn to is critical.
4. **Know Best Practices –** Technology leaders in all industries have been dealing with security issues for many years and, as such, there are well-established smart practices regarding data security. It would be easy to get lost in the "alphabet soup" of technical organizations publishing security standards for cloud computing and data transmission, among other issues. To make matters worse, security threats evolve just as technology continues to change. Stay current on security threats and how to deal with them. Active membership in professional associations, subscribing to blogs and reading IT/security-related publications are just some of the ways to stay current.
5. **Implement Workable Practices –** It is important to note that what works for one industry, banking for example, may be too restrictive for education. The term "best practice" is relative. This is where industry-specific guidance can be helpful. For example, CoSN (Consortium for School Network) has done quite a bit of work on security, and resources such as the free Security Planning Rubric can be obtained at www.cosn.org/cybersecurity.
6. **Partner with Vendors –** Use your technology providers as important resources in helping you to deal with security issues. Technology providers know their technology better than anyone, so they are naturally a good source for security information. They typically have highly-trained engineers that can assist you with technical issues. Request that you be granted NDA (Non-Disclosure Agreement) status, so you can be privy to information that may not be available to the general public.
7. **Leverage Procurement –** Make sure to build security requirements into the contract when contracting for any online services that will collect, manage, or store student and/or employee data. Once agreed to in contract, they are legally enforceable. See the free CoSN toolkit *Protecting Privacy in Connected Learning*, available at www.cosn.org/privacy for a detailed set of security questions to ask an online service provider, as well as suggested terms of contract.
8. **Provide Training –** Any staff working to manage district technology systems need ongoing training to ensure that they are up-to-date on current security procedures, as well as the various IT security tools being used. For certain key positions, such as database administrators, network engineers and others, security training and relevant certifications should be considered job requirements.
9. **Test Your Security –** The ideal situation is to have a company that specializes in IT security perform regular tests and audits on at least an annual basis. A thorough audit will not only include tests of the technical security measures, but determine how well end users follow good security practices. It may be cliché, but the sticky note with password attached to the computer display still happens far too often. Many security breaches are the result of carelessness or other human errors, rather than technical problems.
10. **Review & Adjust –** As with any set of policies and procedures, you'll need to review your security measures on a regular basis. New laws may have been passed that require new security measures. By reviewing your work regularly you can better ensure that you are striking a reasonable balance between good security and the freedom that students and teachers need.

Good data security practices are perhaps the most important step you can take to better ensure privacy of student and staff data. Make sure to address both technical issues, as well as human behavioral issues. Practicing good security does not mean loss of freedom to explore and innovate for teachers and students; but meeting the understandably high expectations for privacy, let alone legal requirements, does mean that the "anything goes" approach when it comes to technology use is not reasonable. By taking the steps described above, school technology leaders will take significant strides in securing data and protecting privacy in their digital learning environments.

BOB MOORE

With more than 25 years in education technology, Bob Moore works with schools, education organizations, nonprofit associations, and business clients as a strategist, advisor, and subject matter expert. Bob started RJM Strategies, LLC following several years as lead strategist for a large global technology company and a career of two decades as a CIO in K-12 schools.

E-mail: BobMoore@RJMStrategies.com

Twitter: @BobMEdTech

LinkedIn: http://www.linkedin.com/pub/bob-moore/0/ba4/675/

Printed in USA 0314/SL/HBD/PDF ♻ Please Recycle