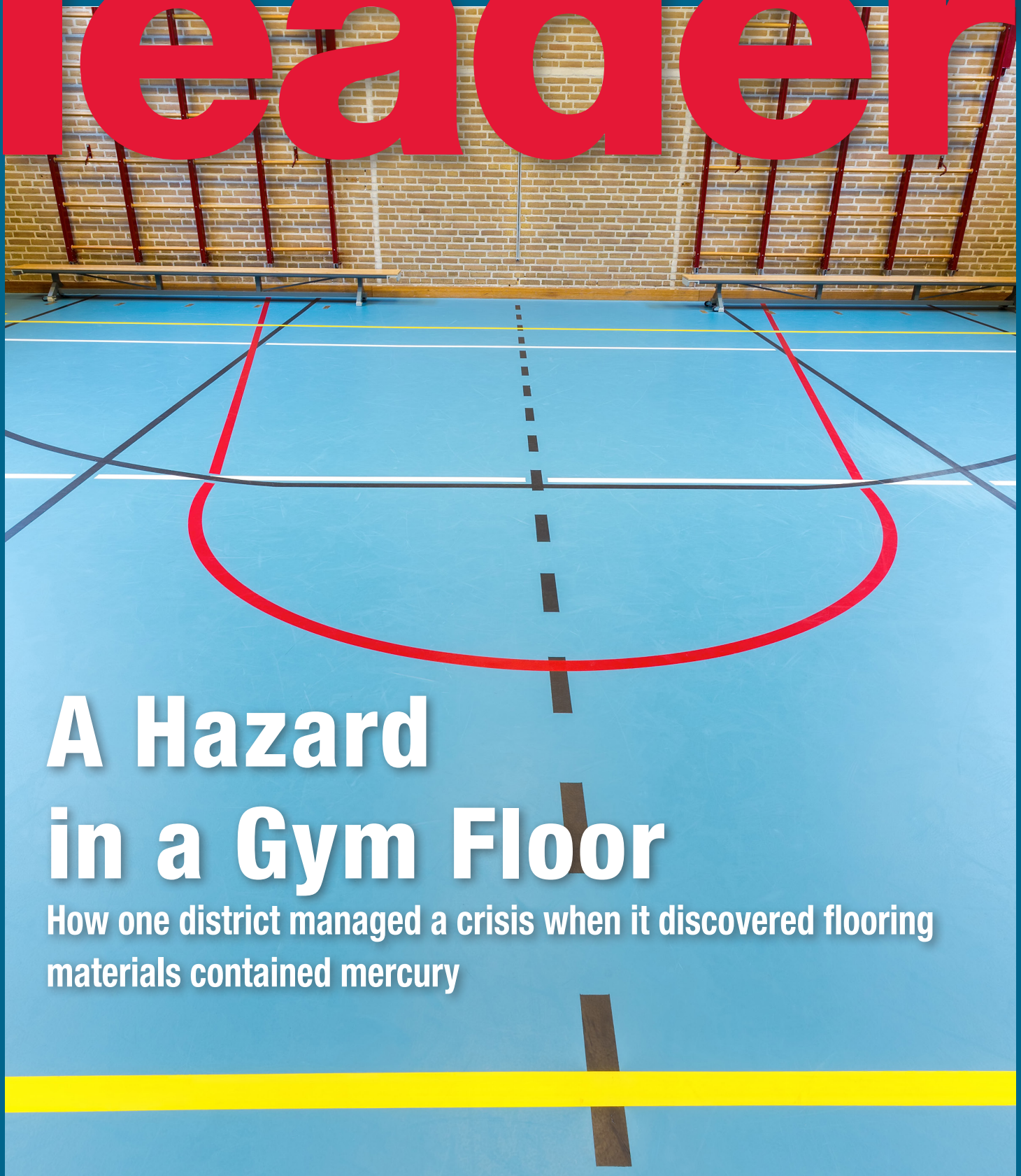
SCHOOL
leader



A Hazard in a Gym Floor

How one district managed a crisis when it discovered flooring materials contained mercury

Special Section on School Safety and Security

Tips on Conducting a Successful Community Survey

Policy on Uber Rides for Students

New Jersey School Boards Association

May/June 2017

of "school security drill" is expanded to include practice procedures for responding to bomb threats. The law goes into the effect at the beginning of the 2017-2018 school year.

Nonpublic Security Aid Approved in mid-2016, the "Secure Schools for All Children Act," (*P.L.2016*, c.49; A-2689/S-754) established a state aid program for security services, equipment or technology to ensure a safe and secure school environment for private and parochial school students. The FY2017 state budget allocated $7.5 million toward the program.

Financing School Security Improvements Another new law *(P.L.2016*, 100; A-2158/S-2241) will allow the use of emergency reserve funds or proceeds from bonds issued by the NJ Economic Development Authority to finance school security improvements. Such improvements would be limited to safety and security measures involving building monitoring and communication technology designed to address school crime and the safety of students, staff, and visitors to school facilities. This includes such items as: security cameras to monitor the school; an electronic notification system; an automatic door locking system; and a badge system for school employees.

More to Come? It is clear from the activity we have witnessed at the statehouse in the last few years that that Legislature and governor have made school security a major policy priority. It is the hope of all stakeholders that these initiatives will reap tangible benefits for school districts and the children we all have a responsibility to protect. This issue is not one that is going away.

Jonathan Pushman is a legislative advocate with the NJSBA. He may be reached at jpushman@njsbsa.org.

School Security in the Time of Cyberthreats

BY JOHN G. GEPPERT AND KURT M. WATKINS

School districts face a unique challenge in terms of cyber risk. Not only do they possess a wealth of sensitive information, such as health records of students and staff; academic records; governmental records; financial records and more, they also have two types of "insider threats" – employees and students.

The 1983 movie "War Games," in which a student hacks into a school computer system to change his grades, was perhaps one of the first times the idea of a school's being hacked entered widespread public consciousness. Since that time, technology has progressed, and so have the means to hack into it. Just this spring, a high school sophomore in Texas was caught changing grades for an undisclosed fee.

These examples – separated by 25 years, the world wide web, and the smartphone – demonstrate the two unique issues with school cybersecurity. The well-prepared school must appropriately balance its access to technology with the protection of its data. This need and challenge are similar to providing physical school security, because just as a school can only be 100 percent secure if no one is ever allowed on the premises, data can only be made 100 percent secure if no one is ever allowed to interact with it.

The growth of technology As technology winds more and more into our lives, education, and work, cyberthreats to schools are likely to only increase in pervasiveness, subtlety, and impact. Unfortunately, this means complete cybersecurity does not exist. Rather, the goal of cybersecurity is to reduce as much

risk as possible without compromising a user's ability to use the system. This tradeoff should always be evaluated, and then reevaluated, as technology and the inevitable threats change.

In other words, any successful cyber risk management preparation is fundamentally an ongoing balance between protection and authorized access.

Cyber risk management The basic tenants of any successful school cyber risk management plan must include the following: 1) A commitment by the superintendent, head administrators, and board members to a comprehensive plan for the protection of teachers' and students' data as well as the school's network generally; 2) Personnel dedicated to effectuating that plan; and 3) Employees, teachers, and students who understand the plan.

Student actions and needs As will not surprise the readership, students can be crafty and prone to disrespect authority. However, at the same time, their education and well-being are the goals of any school system. In 2013, the Los Angeles School District encountered this tension as the district issued iPads to its students to make education more accessible. The iPads had various controls on them so that the students could not use them for recreation. Aside from the problem of students not attending to their studies, that was wise because having that many devices linked to the network, without strict controls, invites the danger of a student inadvertently visiting a malicious website and infecting the whole system.

However, in less than a week of deploying the iPads, students discovered a way to bypass these controls and were selling this service to other students, in addition to other problems with the plan.

More promisingly, In New Jersey many school districts have begun adopting a "1:1 Chromebook Initiative," to supply each student in certain grades a Chromebook. These policies have been largely successful in various school districts. However, maintaining those devices and ensuring none become compromised is inherently challenging. As Chromebooks become more popular, so too will developing ways to hack them. By compromising one Chromebook, a determined attacker could compromise them all, as well as the school's internal network.

One alternative to the Chromebook approach is to implement a "Bring Your Own Device" (BYOD) policy. When speaking to businesses, many practitioners in cybersecurity refer to this as "Bring Your Own Liability," or "Bring Your Own Disaster." The reason is simple: who knows where that device has been? This approach is both less expensive and provides the students great flexibility in their learning options. In the 2016 May/June School Leader, an effective implementation of this strategy was described. However, any BYOD policy requires constant monitoring and layers of security to prevent potentially-infected devices from infecting the school's systems. Indeed, if a BYOD policy is established and left unattended, it can become a large liability.

In the Cloud Another solution is to move school districts' cyber needs as much as possible to the "cloud" so that all users must interface with school data and programs through the cloud. The advantage is that the cloud provider updates, maintains, and deploys the system and the security. A cloud provider is better equipped than a school to do these tasks, and generally will have the latest hardware and cyber protections.

However, this is not an ideal solution either, because such a service is expensive; there will still be a need for internal systems; passwords can still be compromised; and it places total trust in the cloud provider. If the cloud provider gets hacked, goes down, or stops functioning, even if it were possible to shift all legal responsibly to the provider, parents of a school district are unlikely to accept "it was the cloud provider's fault" as an acceptable answer.

So, for a school to provide interactive technology for its students (WiFi, electronic lessons or homework, electronic grade reporting, etc.), there is no easy answer. The only effective answer requires constant diligence and a mixed strategy of cybersecurity tools, so students and faculty will both want to use technology, while keeping the school secure.

Regulated Data As an interesting note, cyberthreats have not truly increased because of technology per se. The risk of most cyberthreats has been around since the early 1990s, if not before. The real problem is that society is becoming much more dependent on technology, and trusts it with much more information. When cyberattacks occur, they are more devastating.

Think of all the data kept by a school. Schools are data-rich, containing personnel records, student records, medical information, evaluations, testing results, vendor contracts, bids, and more. Moreover, much of this data is protected by law.

FERPA, the Family Educational Rights and Privacy Act, requires that student information be protected. HIPAA, the Health Insurance Portability and Accountability Act, governs all electronically-stored medical information. PPRA, the Protection of Pupil Rights Amendment, governs certain marketing with student personal information, and can be implicated when students use online educational services. Further, New Jersey has corollary regulations to protect student and employee data.

Failure to comply with any one of

these laws could result in serious penalties for the district and some, like HIPAA, can result in personal liability. Most importantly, if anything were to happen to a school's network, a torrent of concerned and vocal parents would flood the school board's meetings. In short, there is no shortage of laws protecting and regulating school data, and no doubt that parents will demand compliance, if not even greater safeguards.

Types of Cyber Threats At a macrolevel, there are two types of cyberthreats: mass and targeted. Targeted attacks are less likely, as they require an attacker to specifically target a school district. Mass threats are the more likely ones for any organization. These take the form of generic malware; the most pervasive form is ransomware.

As one example, malware infected the Swedesboro-Woolwich Elementary School District a few years ago, according to published reports. While ransomware is the most likely mass attack, it does not actually take or access school data; it just locks it. When this occurs, the school has the choice of paying the attacker to unlock the data (a risky proposition to trust a criminal once paid) or restore the system from back-ups. To their credit, the Swedesboro-Woolwich school district chose the latter option. However, the process was time-intensive and required the school to have back-ups, and the school still lost the data between the time of the attack and its last back-up.

Bogus Word documents or "phishing" emails (like the one that compromised John Podesta's email) can breach the security of a system to access, copy, or edit its data. No attack like this is known to have occurred on a wide scale in New Jersey. Nonetheless, it may be only a matter of time.

Sony, Home Depot, Target, Anthem Health Insurance, eBay, Heartland Payments, the DNC and others have experienced incalculable damage to each of their organizations and the people connected to them. The worst and most difficult aspect of cybersecurity is that these were caused by mass threats, not even targeting the specific organization.

Cyber Policy By far the largest factor determining whether a school or a district will have effective policy is a commitment by its leadership. Mitigating cyber risk inherently requires an outlay of resources and coherent procedure across the organization. Because there are so many facets to good policy, no one, except superintendents, administrators, and board members, will see how they all interact and can make effective changes. Briefly speaking, there are nine distinct areas to address. They are as follows:

- The risk management assessment determines how large the system is, where its weak points are, and how it can be monitored.
- The cybersecurity policy is the developed plan for the whole system.
- Implementing personnel training is essential for all users in the system to know how it works, how to safely interact with it, and how to detect and report suspicious activity.
- Establishing clear operations for the use and troubleshooting of the network ensures that problems do not occur or are addressed competently.
- Protecting the physical hardware prevents an attacker from short-circuiting all the software security.
- Managing third-party risk means requiring that any vendors or service providers who have access to the system are themselves secure.
- Having secure protocols for users to communicate with the system prevents unwanted intrusion.
- Updating and patching software ensures that all known attack vectors on the software do not occur or that you are aware of them.
- Finally, maintaining a well-designed cyber insurance policy for when all else fails will provide some of the means and resources for addressing an attack when it occurs.

In sum, just as other organizations are realizing, schools can no longer deal with cyberthreats by ignoring them. But the standard rubric for protecting a private company does not match exactly what a school district needs to implement. As a unique organization, a school requires unique solutions to provide the best cyber risk management. While the concern is always how to prevent an attack because the downside is so terrible, it is important to bear in mind the upside of effective cyber policy.

A school well-prepared for this modern-day adversity can provide its students a truly interactive, dynamic, and tailored education, while providing its faculty and administrators greater efficiency, clear guidelines, and peace of mind. Because school districts are unique in their functions and in their legal exposure to cyberthreats, consulting a board attorney throughout the process of adopting a cyber risk management plan is essential.

John G. Geppert is a partner and chair of the education law group with Scarinci Hollenbeck. He is also chair of the New Jersey State Bar Association School Law Committee. He may be reached at jgeppert@sh-law.com. **Kurt M. Watkins** is an associate with Scarinci Hollenbeck. He may be reached at kwatkins@sh-law.com.

Vision | Strategy | Teamwork

Cyber Security

Stay in Control of Your Data

Protect Your Students, Protect Your Teachers

Areas Of Service

- **CYBER SECURITY**
- **CYBER HYGIENE TRAINING**
- **CYBER RISK MANAGEMENT**
- **DATA PROTECTION**
- GENERAL EDUCATION
- BOARD GOVERNANCE
- COLLECTIVE BARGAINING
- LEAD CONTAMINATION
- PUBLIC CONTRACTING
- CONTRACTS
- TENURE
- LITIGATION
- LABOR
- REAL ESTATE
- ENVIRONMENTAL
- PLANNING

SCARINCI | HOLLENBECK
ATTORNEYS AT LAW

WWW.SH-LAW.COM ▶ LYNDHURST | RED BANK | JERSEY CITY ◀ 201-896-4100