2018 NSBA CYBER RISK REPORT:

School Board Communication at Risk

About This Report

Today every business and organization faces risks from cyber-attacks. Schools hold a special appeal for hackers as a school database often contains highly sensitive information on students which fetch high prices on the black market as identify theft from children is far less likely to be discovered, sometimes for many years. Unfortunately, school board communications can be used by cyber criminals as a gateway to access the sensitive information held by our schools. To assess the current state of cyber security among America's school districts, in July 2017 the National School Boards Association (NSBA) conducted a nationwide survey; there were 482 respondents with a representative distribution both geographically and among district size.

The findings clearly demonstrate that school boards must take additional steps to protect their board communications from cyber-attack. And, while there are no fool proof methods to stop cybercrime, there are a number of easy to implement practices that can significantly reduce risk. This report summarizes the key findings from the survey, provides observations on the significance of the findings and includes some suggested action steps for school boards to improve communication practices.

Introduction

Should Cybersecurity be a Concern for School Boards?

The term "cybercrime" might conjure up images of a shadowy group of 'hacktivists' attacking those in power, both to showcase their hacking prowess as well as making a political statement. But cybercrime these days tends to be far more mundane: focusing on easy targets whose cybersecurity defenses are the weakest, and who are the most likely to pay ransom in BitCoin, the value of which has exploded in recent years.

The survey suggests school officials are less prepared for cyberattack than private-sector companies, though both face formidable threats. The NSBA survey parallels a report called "The Price of Convenience," a survey of 381 directors of U.S. companies, completed in early 2017 by **NYSE Governance Services and Diligent**, which showed private company boards to be similarly underprepared. The threat, however, extends beyond the private sector. According to Dottie Schindlinger, vice president and Governance Technology Evangelist, who collaborated on the "Price of Convenience" report, "At the end of the day, organizations with leaders that don't have at least a good foundational understanding of cybersecurity are the most at risk. An easy way to gage a school's preparedness to handle a cyberattack is to look at their board minutes to see if the topic has come up — if it's never on the board's agenda, it likely indicates cybersecurity isn't a high priority for the school, and they are at greater risk."

Cybercrime is big business, with **ransomware alone generating over $5 billion in damages last year**, according to CSO Online — the leading magazine covering cybersecurity issues. It's true that many criminals target high-level executives of big companies, such as former US Secretary of State and Salesforce board member, Colin Powell, whose personal email account was hacked and a document containing the company's M&A strategy was leaked to the **Wall Street Journal**, negatively impacting share price. Yet, many hacking attempts are far more random — according to **Symantec's 2017 Internet Security Threat Report**, one in every 131 emails is malicious, and masses of ransomware-laden emails are blanketing organizations and individuals with the least cybersecurity prowess. The ransom demand is often a relatively small amount **averaging about $1,000** (CSO Online), and smaller organizations are more likely to pay to make the nuisance go away. But paying the ransom only makes the victim more vulnerable to future attacks — partly because once their systems are infected, they are likely to remain so until they are professionally scrubbed or replaced entirely. With cybercrime damages on pace to hit $6 trillion annually by 2021 (CSO Online), clearly this problem isn't going away anytime soon.

Are Schools Really at Risk of Cybercrime?

In October, the **US Department of Education** warned that cybercriminals were extorting schools for ransom to avoid making stolen student records public. In the foreseeable future, such attacks could cost not only the ransom payers or the victims of identity theft, but also the district's leaders themselves — including school board members. Recent EU legislation (General Data Protection Regulation, or GDPR) holds financially and legally responsible any entity that compromises the privacy of EU citizen data with fines of €20 million, or 4% of annual revenue — whichever is greater. This includes potential direct legal action against directors and officers of these entities. GDPR is considered a high-water mark for data protection legislation, and is actively being considered for replication in the US. Similar rules now exist in a few US jurisdictions, including recent rulings in **New York State by the Department of Financial Services (NYDFS)** holding financial service directors (and the vendors who provide services to them) liable for cybersecurity breaches. Meanwhile, rules taking effect in other states including Virginia and Georgia now include mandatory breach notification in as little as one week after an event is first discovered. Considering the severity and frequency of the hacks that took place in 2017, additional legislation targeting organizational leadership is expected.

Schools need cyber-protection every bit as much as their for-profit peers. Small budgets and an educational mission offer no protection. Rather, the schools that are the least prepared are the most likely to become prime targets precisely because of the ease of breaching their defenses.

The survey sought to determine school boards' level of preparedness and awareness to handle these challenges. Below, are the key findings along with observations on the significance of the data and suggested action items for school boards' consideration.

Key Findings

1. **A gap exists between school boards' concern for cyber risk and their approach to cybersecurity.**

More than 80% of respondents regularly use digital communication and 42% of respondents say that using digital technology for communications between the board and the administration has decreased security. The survey asked school board officials to share what they know about their present cybersecurity measures, with a special focus on board members' own communication practices. In the survey, board members often responded "don't know" when asked about the ways cybersecurity is managed. Though often entrusted with more sensitive information than most of the district's staff, tradition and culture lead many board members to assume the responsibility for cybersecurity begins and ends with the IT team. Not knowing has led to not acting, with boards not directly addressing the threat of cyberattack by ensuring they adhere to secure communication methods, policies, and increase their level of awareness, training, and preparedness.

ACTION ITEM

Consider creating specific procedures for board communication including digital files and storage, emails and texts; make this part of your new board member orientation. Members should specifically acknowledge receipt of the procedures and they should be reviewed and updated annually as digital communication evolves rapidly.

2. **School boards regularly transmit and store board documents through unsecured or minimally-secured methods.**

When asked about how they store board-related documents, 72% report keeping board documents in unsecured locations including school websites, "free" file-sharing websites, or personal hard drives.

of those surveyed keep board documents on file-hosting sites

What Is Ransomware, Anyway?

According to **CSO Online**, "Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising — not always truthfully — to restore access to the data upon payment."

"Free" Cloud Storage Sites Are Not "Risk Free"

Providers of "free" cloud storage sites offer convenient services attractive to groups collaborating on projects from remote locations. Although these providers typically offer basic password security and data back-ups, the free versions are frequently targeted by hackers and are not tightly secured. Meanwhile, the terms and conditions users must agree to in order to use these "free" services typically grant broad rights and access to user data to the providers, and absolve them from any damages in the event of a data breach.

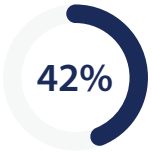
Additionally, cloud storage websites often automatically sync with each user's personal accounts. This can have the unintended consequence of creating multiple, redundant versions of files residing locally on board members' personal devices and drives without their awareness. These local copies are then outside the control of the board secretary and school district, and could quickly become outdated depending on the frequency of file syncing.

Email — Too Risky for Board Communication

School board members trust district-supplied email accounts more than personal email accounts — confidence in email is evident by the 79% of NSBA respondents who regularly conduct board business via email accounts linked to a district network.

store them on personal or external drives

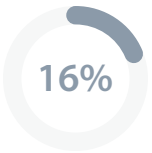
keep them on the school website



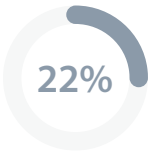
store digital board materials on a secure board portal

As most school board meetings are open to the public, meeting documents are frequently posted on school websites for public access. That said, the responses to our survey did not differentiate how public versions of school board documents might be handled differently from more confidential or sensitive data — such as unapproved drafts, or documents shared during closed meetings.

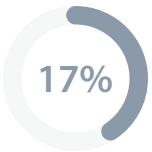
To this end, one-third of respondents trust personal/external hard drives, or free file-sharing websites such as iCloud, GoogleDocs and DropBox to store board documents.



of respondents believe such storage actually decreases risk



believe file-sharing systems have no effect on document security



have no idea how file-sharing sites affect risk

ACTION ITEM

Create a board policy on how digital board documents should be handled and stored, including which systems and devices are acceptable for board members to use. Implementing a centralized, secure cloud-based governance software solution — with "public" and "executive" content access options — can help reduce the need for multiple redundant file storage locations.

By contrast, only 30%regularly use personal email accounts. With most free email providers (e.g., Gmail, Yahoo! Mail!, AOL) having been breached in the past three years, users should assume these channels are unsecured and easily hacked. But, does using district-linked email accounts eliminate cyber risk? Unfortunately, no.

The danger inherent in board members' email communication can be severe. The 79% of districts that supply board members with district-linked email also list those addresses on their public websites so the community can connect with directors. But doing this provides hackers with information they can easily exploit to launch highly successful phishing attacks. According to research by cybersecurity firm PhishMe, 91% of cyberattacks begin with a phishing email, allowing hackers access to all the information stored on the network. In the case of school districts, this means student records, birthdates, health records, payroll information, Social Security numbers, and more. Using malware or ransomware, hackers can decide whether they want to sell these records on the Dark Web, shut down the district's network entirely, or threaten the district with releasing the records publicly until a ransom is paid in Bitcoin.

When It Comes to Cyber Risk, Not Knowing and Not Acting Could Constitute Negligence

The low rates of board cybersecurity training, the casual use of unsecured email and lack of oversight to ensure secure board communication practices are out of alignment with the level of board culpability in the event of a data breach. Boards that abdicate responsibility for data security to the IT department may not be fulfilling their "duty of care," part of their fiduciary obligation to stakeholders. Several states have recently enacted laws assigning responsibility for cybersecurity to board

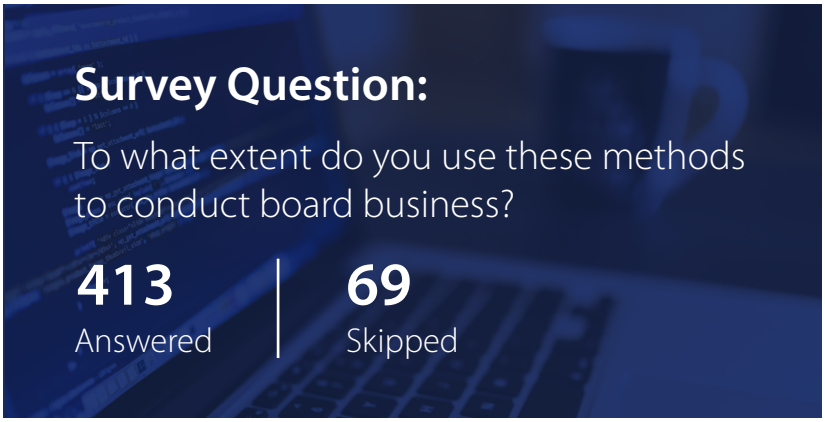
3. School boards discuss board matters using a variety of unsecured or minimally-secured communication channels.

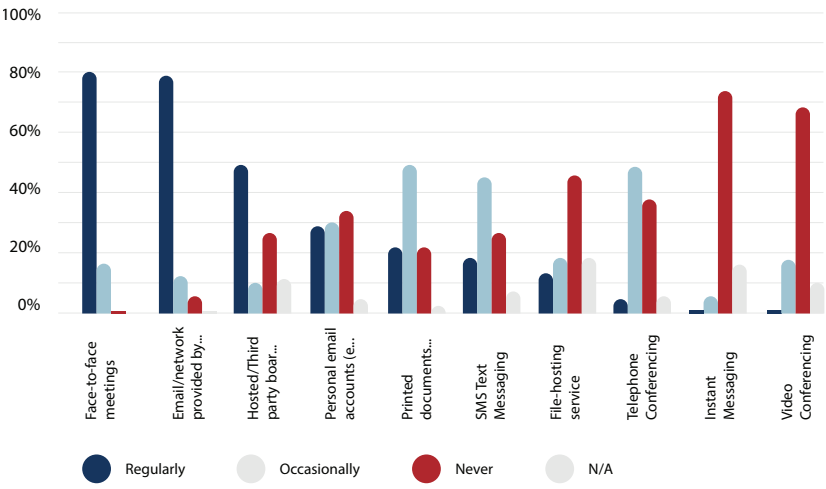
School boards are using a wide variety of communication methods, but outside of face-to-face meetings, email is their preferred communication channel:

of respondents to the NSBA survey regularly or occasionally use personal email accounts to communicate about board business

of school board members use district-supplied email addresses

While these numbers are lower than what was observed in the corporate sector, where 92% of directors reported using personal email to communicate on board-related business, the reliance on email is inviting unnecessary levels of risk for school districts (see sidebar).



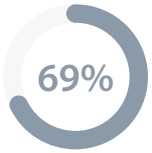


members and top executives; depending on your school's jurisdiction, school board officers might already face legal issues if a data breach is discovered and not reported to all those effected within a few days. Most analysts expect many more of these types of laws to come on the books over the course of the next year in direct response to the severity of recent data breaches such as those at Equifax (145 million customers hacked), Verizon (all 3 billion Yahoo! accounts breached), and the attacks on US public schools (800 schools hacked with an ISIS-initiated insertion virus, and a Montana school district extorted by hacker group Dark Overlord).

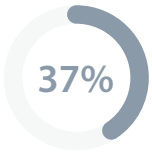
ACTION ITEM: Secure all board communications.

Move away from email and unsecured text messaging in favor of secured, cloud-hosted board communication software. Some providers offer a way for board information to be shared with the public along with a way to gather public comments and share those back with board members. Using such a system helps separate any attempted attacks from the rest of the district's most sensitive records, and gives the district the added malware protection offered by the board software provider.

4. School board members are downloading, storing and transmitting board documents on a wide variety of systems, with little or no oversight from IT/security teams.



said they regularly download board documents onto personal devices



reported doing this at least half the time

It's interesting to note that the actual number of downloads is probably higher than board members might realize. The 79% using district email to communicate about board business are likely downloading offline copies of all messages and attachments onto every device they use to read the emails – including smartphones, tablets, and computers. Unless the district restricts the devices board members use to those that have been vetted by their IT security teams, it's possible that these devices have no encryption or password protection enabled – making every document and message stored on these devices easier to breach.

Meanwhile, the lack of consistent policy around where board members can download and store documents means that it will be exceedingly difficult to track down copies of these files in the event of a lawsuit and discovery requests.

ACTION ITEM: Create a Secure Board Communications Policy and give oversight authority to the district's data security team.

The policy should mandate the methods, storage options, and devices board members can use for board business. Ideally, the board will rely primarily on a single, secured board portal system that is purpose-built for public governing bodies. From there, it is possible to minimize further proliferation three ways:

1. *Create policies around which documents may be downloaded, vs. which may only be "viewed" online.*
2. *Ask the data security team to conduct an annual audit of board communications to ensure the policy is effective.*
3. *Provide annual reviews of the Secure Board Communication Policy in open session, helping ensure that the board understands and will abide by it.*

5. School boards are largely unaware of their role in overseeing cybersecurity, nor do they receive adequate training and support to oversee cyber risk management.

To illuminate the issues, the survey inquired about a number of practices boards may engage in to ensure they are aware of their organization's level of cyber risk and preparedness to handle a cyber event. The survey looked to determine to what extent board members themselves are asked to participate in these efforts, as part of their fiduciary obligation to ensure risk mitigation and management.

When asked whether a security audit of the school board's communication practices had ever been conducted.

More than half

said, "I don't know"

Nearly a third

responded, "No"

Additionally, we asked if districts are providing school board members with any cybersecurity training. The results were:

More than two-thirds (67%) of districts do not provide board members with any cybersecurity training

said they "don't know" if their board requires such training

Of the small minority (12%) that receive mandatory cybersecurity training:

40% receive it only once in their tenure with the board

60% The remainder (60%) receive training annually

Of all the findings in this report, these in particular should raise concerns for school districts. Cybersecurity is not a low-stakes business, and board members are at high risk precisely because of their public profiles and minimal level of data security oversight. While it's true that board members need not become data security experts, the risk of district data and operations is too great for them to receive such little preparation. Cyber risk has become the number one source of enterprise risk for every kind of enterprise — schools included.

ACTION ITEM: Create a "Cyber Risk Taskforce," charged with ensuring board members receive adequate training, oversight, and preparation for cyber events.

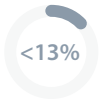
Impress upon school board members the gravity of their responsibility to mitigate risk, and that they should assume a data breach will happen, and may already have happened. The taskforce can spearhead efforts to create a strategic relationship between the district's IT/data security team and the board. Include cyber threat landscape and district preparedness reports at every board meeting. Engage outside experts as needed to coach the board and key staff through the kinds of questions leaders should be asking. Ensure board members receive cybersecurity training (which can be handled easily through online tools) at least once a year, and conduct an annual security audit to ensure the training is effective. Conduct an annual "tabletop exercise" where the board has to respond to a cyber event. Taking these steps will help ensure the board will be ready when the next cyber event happens.

6. Most districts have a non-cybersecurity professional leading or facilitating the security of board communications.

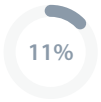
The survey asked who in the district is responsible for overseeing the communication methods the board may use, and who facilitates the board's communications.

The Superintendent was the most common response — **32%** oversee and **28%** facilitate board communication methods.

Few schools grant oversight of board communication methods to district personnel most normally associated with managing risk:



IT/IS/Data Security Team

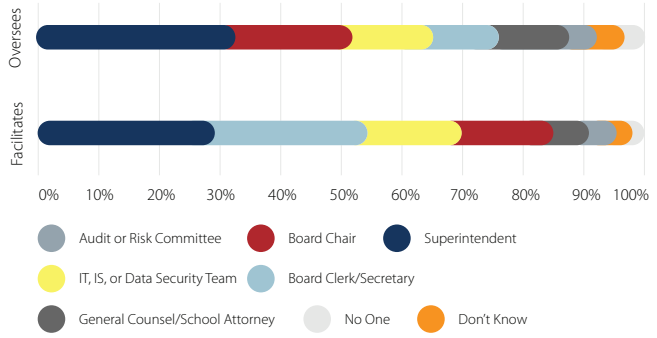


General Counsel/ School Attorney

Audit/Risk Committee

ask the Board Chair to provide this oversight — regardless of the chair's level of cybersecurity knowledge

Question: Who is responsible for overseeing the communication methods the board may use? Who facilitates the board's communications?



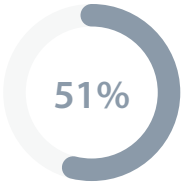
Here, schools do little better than the corporate sector. The NYSE/Diligent survey found that only eight percent of corporate boards have IT/data security provide oversight, consistent with a survey by ISACA (the largest organization of data security professionals) which found that only 29% of private-sector organizational leaders continuously assess their risk from technology use, only 21% are briefed on cybersecurity issues at every board meeting, and 69% say they need to align business goals with IT spending.

ACTION ITEM: Appoint a Data Protection Officer (DPO) who oversees data security programs and reports regularly on cyber risk to the board and senior leadership.

The concept of a DPO comes from the EU's GDPR rules, and serves as a practice that could be adopted by school districts to help increase their cybersecurity posture. If a district does not have a CISO (Chief Information Security Officer), it could hire outside IT consultants to audit board communications, oversee changes, train board members, and report regularly to board meetings. That consultant can work with the district to identify an individual to serve as the DPO, and help perform regular external audits of the district's cybersecurity preparedness.

7. In most districts, board members lack awareness of the steps that need to be taken after a data breach or cyber event — including the roles and responsibilities of board, staff, insurers, legal counsel, and law enforcement.

When asked if their school/district has a crisis communication plan in place in the event of a cybersecurity event or data breach:



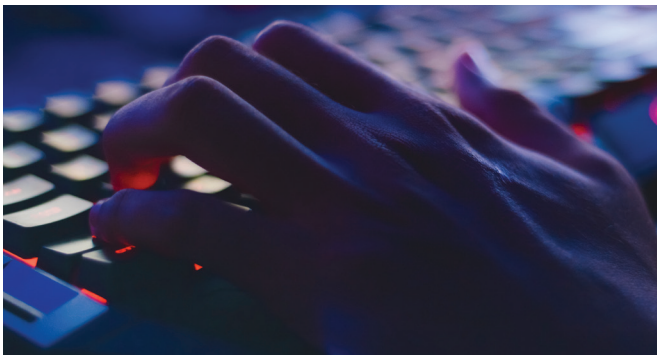
reported that they "don't know"

know that their school or district has such a plan, but only **9%** of those communication plans give partial or full involvement to the board, who are ultimately responsible

This knowledge gap could turn a data breach into an even bigger catastrophe than it already is. After The Islamic State hijacked 800 school computers, only 312 of the schools had a plan to handle communications with police, IT, parents, teachers, students, the media, lawyers and community members. Even when such plans exist, they don't always include the board.

ACTION ITEM: Create a specific Disaster Recovery/ Business Continuity (DRBC) plan for cyber events, including the board's role — and then practice it annually in a data breach simulation.

Every district's emergency preparedness team should collaborate with cybersecurity staff to establish a clear response plan in the event of a successful cyberattack. The plan should include details on insurance coverages, contact information for law enforcement, legal counsel, and a plan to alert staff and parents in case email and other systems are taken offline. Store the plan in a secure, cloud-hosted board portal or similar location that remains separate from the district's network — so that it can be accessed by leaders even if the district's network is compromised. The board should know the plan inside and out, and simulate enacting it at least once a year.



Conclusion:

There is no software or insurance provider that can fully protect a district from cyberattacks and there are numerous examples of hackers penetrating the most sophisticated of systems. However, it is clear that the less a district prepares to prevent an attack, the greater the odds one will happen. The action items listed in this report are just some of the practices can help shelter a district's hardware from kidnappers, protect students and staff from identity theft, and insulate board members from legal and financial liability in a cyber breach.

Meanwhile, we believe it's time for our nation's school boards to acknowledge the seriousness of cyber risk, and approach oversight with the same vigor they would oversee financial decisions. When it comes to the district's finances, board members are fully aware and take most seriously their stewardship responsibility. The staff or external consultants may provide the board with technical support on the nuances of financial decisions, but the board does not regard the technical nature of finance as a barrier and carries out its obligation for financial oversight.

The same must hold true for school boards when it comes to overseeing the district's cybersecurity. District staff or external consultants can provide the board with technical support on the nuances of cyber risk decisions, but the responsibility for ensuring the safety of the district's data and systems resides with the board.

With this in mind, we hope that the findings and suggested action items in this report will galvanize our nation's school boards to take action to increase their level of preparedness and oversight of cyber risk. The safety of our students, faculty, administration, and board members is at stake.

This report was made possible through funding provided by:

BoardDocs
Your Paperless Governance Solution

BoardDocs has helped thousands of organizations dramatically lower costs, increase transparency and reduce time-of-staff by up to 75%. Because our solutions are so easy to use, your organization will operate more effectively from day one. BoardDocs' next-generation, cloud-based services allow organizations to significantly improve the way they create and manage board packets, access information and conduct meetings.

Questions? Ask about their products, implementation or anything else.

Website: BoardDocs.com

Phone: (800) 407-0141

Request a demo at Boarddocs.com

"I would encourage anyone to switch to a full electronic board management solution, particularly BoardDocs. It's extremely user-friendly, and the time and cost savings alone are worth the upgrade."

— Ann Naylor, Assistant to Superintendent
Dr. Cheryl A. Potteiger

1680 Duke Street, 2nd Floor, Alexandria, Virginia 22314-3493
www.nsba.org