MSBAIT Matters

Cybersecurity insurance marketplace remains volatile

By Marsh McLennan Agency

Comprehensive cyber insurance solutions may become even more challenging in 2022 for Minnesota public schools. Consequently, if your school district has not yet begun to embrace and implement more advanced cybersecurity controls, the time to do so is NOW!

While it's impossible for us to specifically know how the cybersecurity insurance marketplace will respond as we approach the significant July 1 insurance renewal date, we do anticipate that renewal pricing will likely go up (again) this year by double digit percentages for most school districts — and that it may be difficult to obtain new or renewal cybersecurity insurance policies at all for some (especially if they have either not enhanced their cybersecurity protocols at all or only done so minimally).

The number of cyberattacks (such as ransomware demands) — and the cost of providing recovery services after an attack — have been and are continuing to increase. As such, to help position your school district maintain or obtain a cybersecurity insurance policy this year, you must continue to secure your networks and data. And we are all recognizing that doing this will take more human (and technology) resources, as well as budget dollars. Although every school district is different (based on its size, access points, level of controls already in place, etc.), we anticipate a reasonable estimate of the additional costs may be between $25,000 and $250,000.

To illustrate what many cyber insurers have been and continue to be recommending and expecting as part of new and renewal cybersecurity insurance underwriting, **please review and assess** whether your school district has adopted — at a minimum — the following 12 security controls:

1. Multi-factor authentication (MFA) has been implemented for remote access, administration access, email, critical systems, vendor access, etc.

▪ There are 15 billion stolen credentials on the dark web — a 300% increase since 2018.* Multi-factor Authentication (MFA) prevents attackers from effectively using them without this additional factor. Remote working has put MFA at the forefront to secure access to critical systems & sensitive data.

* **Forbes.com: New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches**

2. Incident response plans are current and have been (frequently) tested.

▪ An up-to-date incident response plan with a trained team provides efficiency, speed, and quality in response to cyber incidents. When combined with backups and business continuity plans, it significantly helps to mitigate the impacts on operations and your organization's reputation, thereby limiting overall costs.

3. Endpoint detection and response (a/k/a/ "EDR") solutions are advanced and functioning.

▪ Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain their spread. Technology allows organizations to remotely respond to attacks and even prevent data leakage. The time when simple "anti-virus" was good enough is behind us.

4. Secured, encrypted, and tested backups

▪ Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully cripple and extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access), as well as regularly test backups and recovery plans.

5. Patch management and vulnerability management

▪ Unpatched vulnerabilities remain a leading cause of intrusions into systems. Hundreds of vulnerabilities are revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit their vulnerabilities.

6. Privileged Access Management (PAM)

▪ Privileged accounts are the keys of a network. When attackers compromise these accounts, the likelihood of causing significant harm is extremely high. Limiting the number of privileged accounts, using strong password security practices/vaults, MFA, and monitoring these accounts is critical to network security.

7. Email filtering and web security

▪ Malicious links and files are still the primary way to insert ransomware, steal passwords, and eventually access critical systems. Today's first line of defense includes indispensable

See CYBERSECURITY, Page 15

The MSBA Insurance Trust (MSBAIT) endorses the Marsh McLennan Agency as its insurance broker for property, casualty, and workers' compensation insurance and risk management products and services. Visit the Marsh McLennan website for more information.

CYBERSECURITY: One of the most difficult tasks for many organizations to tackle is proper patch and vulnerability management

(Continued from Page 14)

technologies to filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox" environment.

8. Cybersecurity awareness training and phishing testing

▪ Recently, attackers have taken advantage of COVID-19 — when people were stressed the most — as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Training and phishing campaigns help ensure people remain aware and vigilant.

9. Hardening techniques, including eliminating Remote Desktop Protocol (RDP)

▪ Attackers exploit default device settings or misconfigurations. Defining security baselines to harden devices, continuously managing secure configurations and change control processes is essential to preventing attackers from reaching their target.

10. Logging and monitoring/ network protections

▪ Logging and monitoring network activities allows organizations to identify something possibly harmful might be happening. Attackers actions can be detected and contained at an early stage. Automated technology combined with operators monitoring is needed to watch network events or anomalous behavior of users.

11. End-of-life systems replaced or protected

▪ One of the most difficult tasks for many organizations to tackle is proper patch and vulnerability management. Attackers commonly target these "legacy" systems as it is well known that patches and security issues are no longer being addressed. For mission-critical systems that are unable to be upgraded or migrated to newer systems, additional compensating controls should be enabled to allow for proper alerting on malicious behaviors as well as strict access management.

12. Vendor/digital supply chain risk management

▪ Supply chain and systemic risk now garner more focus

i. Aggregation exposure a concern for underwriters

ii. Systemic loss — possible cyber risks:

1. Common vulnerabilities — in hardware or software

2. Common dependencies – vendors (such as cloud providers) and software

▪ Cyber events are driving increased scrutiny (i.e. SolarWinds, Accellion, Microsoft Exchange, & Kaseya).

To learn more about cybersecurity insurance coverages and risk management plans — or to address more specific questions or concerns your school district may have — please contact **Amy Diedrich**, **Pat Truax**, **Casey Holland**, or other members of our Minnesota public schools team at the Marsh McLennan Agency.

Don't Forget Your Insurance and Risk Management Options!

It's almost never too early (or untimely) to review your insurance and risk management options and solutions! MSBAIT encourages school districts to actively review and consider their insurance and risk management options throughout the school year. So, consider, for example:

▪ Some school districts who don't currently participate in the **MSBAIT Risk Protection Program** to address their property/casualty insurance and risk management needs may be expected to provide **six-month notice requirements** to make a change!

▪ Because premiums and underwriting conditions appear to be rapidly accelerating upward for many cyber/data security insurance policies, the time for school districts to further assess and evaluate their information technology infrastructure needs and budgets is **now**!

Whatever insurance and risk management issues and concerns "pop up" in your school district, remember, too, that the MSBAIT endorses **Marsh McLennan**. Contact **Amy Diedrich** (**amy.diedrich@marshmma.com** at 763-746-8000) or **Patrick Truax** (**patrick.truax@marshmma.com** at 763-746-8000) to help you address your property-casualty and workers' compensation insurance and risk management needs. Contact **National Insurance Services**' **Steve Smith** (**ssmith@nisbenfits.com** or 800-627-3660) or **Rob Keller** (**rkeller@nisbenefits.com** or 800-627-3660) to help you address your group term life/disability insurance and risk management needs. For help, contact MSBA/MSBAIT staff members **Tiffany Gustin** (**tgustin@mnmsba.org** or 507-934-2450 or **Gary Lee** (**glee@mnmsba.org** or 507-934-2450)!