Risky Business: Protecting Your Organization From Cyber Threats

By **Courtney Kiss** and **Joy Merten**

Greg Daniel, CISA, CRMA is a Senior Manager on Johnson Lambert LLP's Business Advisory Services team. He is an IT expert with over a decade of experience and holds a Master of Professional Accountancy from Bryant University.

Cyber security may not be a top concern for associations, but any organization that holds the personal data of its customers, or members, should take proactive steps to ensure that the data is protected. Small associations may think that they are not a target for cyber-attacks due to their size and scope, but that line of thinking is misguided. As with most disruptions, the time to think about cybersecurity is before a breach occurs—not after.

FORUM spoke with Greg Daniel, CISA, CRMA, about how associations, even those with limited budgets, can mitigate threats, prepare for the possibility of an attack and protect the data of the organizations and its members.

FORUM: What are some of the biggest cyber threats to the association community?

Life in the 21st century is tied to the internet. We are connected constantly, both at work and at home. With this reliance, many members of the association community expect certain safety measures to be followed by the online services they use without actual confirmation. As a result, these members become more vulnerable to cybersecurity threats and attacks. The biggest cyber threats impacting our community today are:

- **Malware.** Short for "malicious software," these computer programs are designed to infiltrate and damage computers without the users' consent.
- **Ransomware.** A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. Also known as "crypto-malware."
- **Pharming.** Malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without a user's knowledge or consent.
- **Phishing.** A form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity.

Cyber attackers are gaining more sophisticated hacking programs/tools to exploit security vulnerabilities to access sensitive personal data (i.e., Personally-Identifiable Information (PII), for example Name, DOB, Mother's Maiden Name, etc.) or Nonpublic Information (NPI), for example Driver's License Number, SSN, Bank Account Number, etc.). These attackers can even restrict access to an entire system from the very individuals that own it!

Associations should ensure they consider data at rest (i.e. data stored on hard-drives, laptops, mobile devices and databases) and data in transit across the internet via email, text message or transfer to a cloud storage device when assessing the risks of cybersecurity threats and attacks.

FORUM: Are certain systems or applications more susceptible to cyber-attacks than others?

The simple answer: we are all exposed. Nearly all systems produced in the last 20 years have an Intel CPU chip. Recently, two serious computer processor unit (CPU) security bugs were found from vulnerabilities in these chips. Both bugs, nicknamed "Meltdown" and "Spectre," take advantage of a CPU flaw intended to increase computer performance. This CPU feature is used to increase the performance speed of computers by "guessing" what actions the user will take and then storing the needed files or data behind the scenes for quick retrieval if those actions are taken. Though exploitation of this vulnerability requires adept technical knowledge, a hacker could potentially use the Meltdown bug to read a computer's memory and

Greg Daniel, CISA, CRMA, *Senior Manager*, Johnson Lambert LLP

steal passwords, photos, and/or other sensitive content residing on the system. The Spectre vulnerability also affects chips from Intel, AMD and ARM that could potentially allow hackers to trick otherwise error-free applications into giving up secret information.

Intel and other technology companies are currently working on updates to protect against these recently disclosed security vulnerabilities. Apple Inc. has released software patches to mitigate both these weaknesses. However, since Meltdown and Spectre are hardware level vulnerabilities, software patches will not immediately solve all issues. Therefore, associations and their members should be vigilant in monitoring for remediation activities from these companies to address security flaws for all systems they use.

FORUM: We frequently hear that organizations should be planning for WHEN they are a victim of a cyber-attack, not IF. However, associations may not have the budgets like some for-profit counterparts to prepare for such events. What can associations—large and small—do now to help protect themselves and their members?

Establishment of an enterprise-wide cybersecurity risk management program is essential for associations to protect themselves and their members against cybersecurity attacks. Adapting a security strategy that uses a preventive and proactive mindset can save the association resources both before and after cyber events occur.

First of all, since the greatest amount of attacks use social engineering (e.g., malware and phishing) training of employees on common security threats is crucial. In this risk management program, associations should leverage a risk framework to document systems, the flow of data throughout these systems, and identify any assets that would significantly impact the operations of the association or require them to report to their clients. By doing this, associations will have a solid understanding of what sensitive information is at risk and the level of risk for each data asset and/or system.

Associations can then focus their resources on the highest priority risks identified. Other security practices such as intrusion detection systems, penetration tests, etc. can be implemented once higher risks are alleviated.

FORUM: What would be additional steps, projects, or programs that associations may want to consider budgeting for in the future?

As associations and their members continue to focus on activities to strengthen their cybersecurity posture, a key piece after developing a cybersecurity program is establishing a continuous monitoring process. An assessment should be performed to identify potential security vulnerabilities and determine the association's cybersecurity preparedness. The sophistication and the volume of cyber threats will continue to increase, and assessment results need to be evaluated. Corrective actions should be prioritized and tools need to be updated to adapt to the environmental changes that can negatively impact your association.

FORUM: Education is often cited as one of the best ways to protect from cyber-attacks. Do you have any recommendations how associations can help educate their staffs and members?

Human error is indeed the weakest link in organizations reaching their cybersecurity and data protection goals. Therefore, regular cybersecurity training should be held to ensure associations and members are aware of current threats and risky conduct. For example, associations should teach their staff what phishing attacks look like and randomly send fake phishing emails to test the readiness of employees.

If there are budget constraints, associations can have specific members attend the training and have those attendees train the remaining members. In addition, training institutes have lately begun offering some training sessions that can be leveraged by associations and their members at no cost.

FORUM: What conversations might management want to have with the board to ensure appropriate attention is given to cybersecurity concerns?

The accountability of an effective enterprise-wide cybersecurity risk management program relies on the direction of executive management and board. Cybersecurity program leadership must be knowledgeable, and at an appropriate level within the organization to design, implement, oversee, and enforce program requirements. As such, management should have conversations with the board to explain where the association is most vulnerable based on results from an internal or external assessment of the program's effectiveness. In addition, provide detail on what steps are being taken to mitigate those vulnerabilities. Then, objectively assess and report on the program.

FORUM: If an organization experiences a cyber-attack, what should it do?

As part of the enterprise-wide cybersecurity risk management program, an organization should have incident procedures in place. An incident response team should be assembled to effectively assess the situation when a cyber-attack occurs. This team should consist of:

- Data protection experts,
- A tech team that will identify the breach
- Intellectual property experts who will help minimize the damage and recover every piece of stolen information
- Employee representatives who will deal with incidents that affect employees
- Legal representatives who will provide advice on all the legal implications of a cyber-attack.

Once the scope of the threat has been identified, the organization should secure systems and contain the breach. The communication plan should be executed to officials and to impacted stakeholders. Without an effective communication plan, an organization's reputation will be negatively impacted and may be subject to legal sanctions.

> "There is a lot at stake – working to avoid and knowing how to quickly respond to these threats is critical for all organizations."

FORUM: As someone who knows the reality of the cyber threats every organization, and even individual, faces, what keeps you up at night?

What keeps me up at night is the reality that these cyber-attacks are taking lives. And I do not mean ruining people's lives by stealing their identity. I mean literally taking human lives. We are on the verge of a perfect storm fueled by more sophisticated cyber attackers and the anonymity of cryptocurrency. My fear is there will be more attacks like the Wanna Decryptor (also known as WannaCry) ransomware attacks that occurred in 2017.

With the vulnerabilities from the "Meltdown" and "Spectre" bugs, attackers can now potentially impact airlines and more hospitals and remain untraceable. For example, the compromise of these organizations' key systems could cause deaths to customers and/or patients, if systems are not unlocked in time to avoid crashes or continue operations to patients. There is much at stake—working to avoid and knowing how to quickly respond is critical for all organizations.

Courtney Kiss is the Marketing Director at Johnson Lambert, LLP. She can be reached at **ckiss@johnsonlambert.com. Joy Merten** is a Marketing Coordinator at Sentergroup, Inc. She can be reached at **jmerten@thesentergroup.com.**