asaefoundation
Advancing Association and Nonprofit Leadership

Research Brief

December 2016

Association Data Breach Preparedness

Summary of Qualitative Findings on Status and Needs

by Colleen Ryan Leonard

Most organizations, from the federal government to small online boutiques to associations of all sizes, use some form of online transactions and maintain networked data. Online business continues to grow despite the fact that threats of data breaches, viruses, and ransomware are increasingly part of the nature of doing such business. In response to these threats, the ASAE Foundation worked with SCIPP International, a nonprofit educational organization that focuses on information security awareness, to explore how associations are preparing for cyberattacks, and to describe the processes and actions that can help them improve their defenses.

A series of focus groups were convened that built on, and indeed confirmed, the findings of SCIPP International's 2015 survey study. The latter study suggested that many associations do not have sufficient security in place, and may not have a plan to effectively manage a future breach. According to the current research, most CEOs and CIOs expect they eventually will be confronted with a cyberattack. Faced with this inevitability, association leaders agreed that cybersecurity is important, but they also agreed that it often only becomes urgent—and therefore a priority—after a breach.

Cyberattacks and preventative measures must also be figured into an association's budget. Most associations expect they will have to cover the

financial costs of a breach from their general fund—including those who have cyber risk insurance. In general, cost is a major barrier to proactivity related to cybersecurity.

Association leaders also find several of the key processes related to improving their security—like obtaining insurance and conducting a risk assessment—to be daunting, preventing them from actively taking these steps. Most alarmingly, association leaders are often dissuaded against proactive measures by the feeling of cyberattack inevitability—the mindset becomes, "why spend money when an attack will happen anyway?"

Ultimately, the focus group discussions revealed much about the current state of association cybersecurity and highlighted a number of opportunities for associations moving forward. This report summarizes the findings from those conversations.

PERCEIVED RISK

CEOs and CIOs consider an attack virtually inevitable. Every participant was worried about data breaches and other cyberattacks. Several executives had experienced a breach through ransomware or an attempted breach through emails from someone posing as the membership director requesting the member list. Overall, these associations are taking steps toward greater security and "hoping for the best" given that intrusion attempts are inevitable. Their efforts range widely from minor steps to full-blown security risk assessment and "friendly" hacking to test security. The perceived inevitability made some CEOs and CIOs "just want to pull the covers over their heads."

In the face of an inevitable attack, all of the focus group participants agreed that security efforts are not only about actual prevention, but also:

1. Recovering quickly, and
2. Saving the association's reputation by demonstrating you did all that you could to prevent it.

> *"So I think it's inevitable. I worry about it all the time. It's the reaction part of it. What do we have in place to deal with this when it happens? At what magnitude can we protect it in layers? 'Okay, you got into system A but you couldn't get to system B'. So I think creating that sort of defense is important. But, yes, I worry about it all the time. But I think I'm realistic that it will likely happen."* —CIO

CIOs are concerned about human vulnerability to organizational threats. By far, CIOs' top security worry was staff members' missteps that would give bad actors access (e.g., opening a dangerous email attachment or being tricked into sending out payroll data). CEOs also recognized the risks that humans pose, but they did not emphasize this issue as much as CIOs did. A few other risk factors were mentioned but these did not dominate concern in the way social engineering and trickery did. These other factors included the risk of staff being able to access private information—such as members' passwords or credit card numbers—and concern that vendors or staff who access networks from home or mobile devices might create a vulnerability.

Attacks in the news do make it easy to discuss preparedness. CIOs and CEOs admit that they regularly use these examples to show that breaches can happen to anyone and with huge consequences.

Associations collect a wide range of sensitive data. CEOs and CIOs were asked, "What is the most sensitive data you collect?" They said:

- Member data (addresses, phone numbers, email addresses)/"Any" PII (personally identifiable information)
- Credit card numbers
- Member passwords
- Financial information
- Sensitive survey data submitted by member institutions
- Social security numbers (association runs background checks)
- Healthcare/Medical information (just one participant's association stores this type of information)

Many focus group participants noted that they outsource credit card payment functions specifically to avoid risk. Virtually all of the participants were familiar with Payment Card Industry (PCI) Security Standards Council, and those who store credit card numbers say they are careful to comply with their standards.

> *I will say that it is a priority for IT, and I just need to sell it to make it a priority for our management.—CIO*

HOW PREPAREDNESS FITS AMONG PRIORITIES

By far, the biggest challenge is the "tyranny of the urgent over the important." Cybersecurity is important to associations, but it often becomes urgent only after a breach occurs. This theme was very strong throughout the conversations, and the phrase "urgent versus important" was used in several groups.

Industry affects prioritizing preparedness. CEOs and CIOs who work in sectors like banking and healthcare with more stringent regulations and requirements had greater protections in place than those working in other sectors.

> *If cybersecurity is getting any attention in my organization, it's because it's on fire. There are a dozen priorities ahead of it. That's not to say that it's not important to the folks. But, they're dealing...with a dozen priorities ahead of that. I'm sitting here thinking, "Oh my gosh, this is not the thing I want to be in the paper. I don't want to have my name associated with [a breach], much less my organization's name." But, we have lots of priorities.*—CIO

For these focus group participants, association leaders (specifically, CEOs and boards of directors) are not perceived as a major barrier to making cybersecurity a priority. They might not be its champions, but they see it as important and do not obstruct efforts to improve security systems. The responsibility typically falls to the CIO to bring up cybersecurity concerns and effectively argue for resources. Indeed, like every association function, cybersecurity is vying for budget. However, association leaders generally seem to accept the importance of security. The few focus group participants who saw a CEO or board members as barriers reported several contributing factors: the CEO is hoping the association is somewhat protected by its small size and relative anonymity, older board members do not view security as a priority, or C-

level staff ask for exceptions such as never having to change passwords.

BUDGETING AND INSURANCE

For most participants, cybersecurity is in the information technology (IT) budget and is not standalone. Most participants said that, in the event of a breach, their association would use reserve or general fund money as opposed to having a designated breach fund. This is a strong finding. It was true among those with and without cyber risk insurance, as even the insured assumed that they would incur costs.

Many have cyber risk insurance and those without it were very interested. In fact, having such insurance was termed a "best practice" by participants. For some associations, auditors had suggested it. A few—both CIOs and CEOs—who did not yet have insurance said they were looking into it or had their interest in it sparked by the group discussion. Association leaders understand it is a liability issue. Even if boards and CEOs do not understand the technology issues, they understand the need for risk management.

No participant thought having insurance meant liberation from worry about cybersecurity. Insurance was seen as helpful both financially and for demonstrating that the association did all it could to be prepared for disaster. Although insurance was reassuring from a financial perspective, CEOs and CIOs still had two concerns—first, that insurance would not cover the costs because the insurer would find a loophole to deny coverage, and second that insurance would help little or not at all in restoring non-monetary losses such as reputation damage.

The process of obtaining cyber insurance was considered very daunting and time consuming. There was a strong consensus around this finding among the focus groups, and it points to a potentially significant barrier to obtaining this insurance. An insurance broker who participated in the conversations suggested a second challenge: CIOs resist the applying for cyber insurance because that process delves into current security practices and makes them feel defensive. Importantly, those participants who had been through the insurance application process really valued it in the end because it forced discussion, assessment, and action around cybersecurity.

> *If [a breach]… hit the front page of the paper, [having insurance] would help you tell the story that, "These are the things that we've done to protect ourselves and we have this insurance in place to protect our members." I think it's just part of the warm, fuzzy feeling. But, no, just having it doesn't give me a full night's sleep.*—CIO

STAFFING

"IT" is typically responsible for cybersecurity. Associations in these focus groups were split between those that had CEOs and boards actively involved or those where leaders "just want IT to take care of it." A few CIOs said that, day-to-day, the feel like "doomsayers" about security practices. One deals with that by telling staff, "The auditors say we have to do this."

> *The [goal] is to try and reduce that risk as much as possible, transfer it to somebody [external] who is in a much better position to be responsible for securing that data because it's their business. It's not my business. My business is to teach people how to be better [at a specific profession], and that's what I focus on.*—CEO

Vendors and consultants seem to have a major role in the association industry's management of cybersecurity risk. Among vendors, those that store and protect information—especially credit card data—remove a key burden from the association. Using such a vendor was a common strategy for mitigating cyber risk even though vendors cost money. Consultants were used somewhat less commonly, although a couple of CIOs and CEOs reported using consultants to analyze their security, train staff, and attempt breaches (e.g., Wombat and KnowB4). Training videos are also valued for relieving CIOs of the burden of writing general training content. The perceived primary strength of consultants in cybersecurity is that they think of nothing else, thereby keeping up with changes that IT staff at an association cannot follow because their work is broader in scope.

PREPAREDNESS TRAINING AND DOCUMENTS

All who participated in this research offer their staff some form of cybersecurity training. Most use consultants or supplement their in-house training with external material so that they do not need to write all their own material. Online modules are a cornerstone of training.

Both CEOs and CIOs mentioned that they do talk about cybersecurity in-house, whether in staff meetings or in blogs or newsletters. They provide reminders to staff about things like not sending files via personal email. In one case, a CEO wrote a blog post to warn readers about phishing and explicitly said, "I will never ask you for sensitive data like payroll or membership lists via email." The ideal, said one participant is to infuse security into corporate culture. One association currently involved in a risk assessment process intends to further share lessons learned with members as part of an effort to extend that security-focused culture to members.

> *We have a meeting every week with senior leadership and I always talk about breaches. It's always put in our consciousness. IT professionals should be putting that into their corporate consciousness.*—CIO

When it comes to creating written planning documents—specifically a data breach readiness plan and a security risk assessment—the biggest barrier remains elevating cybersecurity to "urgent" status. Most of these qualitative research participants do not have a data breach readiness plan. However, they are not entirely unprepared. Some specified that their data breach response is covered by their disaster response plan. In other words, a data breach would—like a fire or other disaster—prompt them to follow their disaster plan. Roughly one-quarter to one-third of the participants said that they do have a *specific* data breach readiness plan.

CEOs and CIOS were very in-tune with the notion that breach response is not just about re-securing the data. It is also about restoring the business-flow, repairing their reputation, re-establishing their members' faith, and possibly setting things right by providing ID care coverage or taking other steps. However, only a handful of CEOs and CIOs said they had conducted a security risk assessment. Most saw conducting such an assessment as something that would need to be done by an external organization. Such external assessments were seen as costly, which is a barrier.

> *A security risk assessment is over our heads. Maybe a mega-association like AARP could do this [in-house], but not us].*— CIO

Associations have to balance cost with the need to prepare. In deciding that they would proactively address cybersecurity issues, association leaders frequently cited protecting against the breach itself and mitigating reputation damage by making some visible effort as the two key motivators for conducting a security risk assessment despite the cost. One association was prompted to conduct an assessment only after an experience with ransomware. Another organization chose a "rapid assessment" (at a price of $20,000) over a full assessment (with a price in the "low six figures") for cost reasons. Staff decided that even a rapid assessment would enable them to show they had done all they could. Moreover, spending over $100,000 knowing that breach could still happen despite their best efforts helped dissuade them.

WHAT ASSOCIATIONS CAN DO NOW

Communication is key. Internal communication with staff, the flow of information to members, sharing ideas with other associations, reaching out to experts—all of these are fundamental to preparing for potential online threats. First, prioritize conversations about and planning for cybersecurity threats. When threats rely on misinformation or missing information, the presence of clear policies and procedures is important to combatting those threats. Regular messaging to stakeholders, staff training, and planning documentation are relatively easy routes to raise awareness and keep everyone on the same page regarding organizational policies. If you are not sure what you don't know, don't hesitate to reach out to someone you do trust for information, advice, or a connection to a consultant or other expert who can provide further information.

Cost can be mitigated by collective action. One idea from the focus groups was to create small groups of similar associations that committed work together on a task using a single consultant, lawyer, or other expect. For example, a group could share costs for a single consultant to guide them through the process of obtaining cyber risk insurance or preparing a data breach readiness plan.

Models and samples are much in demand. A number of association leaders expressed a desire for examples of what associations are doing in this area. Information found on the internet is often not the most relevant to association operations or concerns. However, there is a complication to compiling models and samples—CEOs and CIOs noted that their own lawyers would not let *them* share samples from their own efforts.

ACKNOWLEDGEMENTS

The ASAE Foundation would like to thank Marjorie Valin of ITPG and SCIPP International. Established in 2006, SCIPP International offers online security awareness courses for the workplace, including a more technical course for web application developers who use, build, administer, or have access to web applications.

ABOUT THE AUTHOR

COLLEEN RYAN LEONARD is a professional meeting facilitator and qualitative researcher. She has worked with public sector and nonprofit clients for over 20 years--aiding their efforts to define needs, understand their audiences, and solve challenges. Before she began her consulting practice, Ms. Leonard was a Vice President in the Social Marketing Practice Group at Porter Novelli.

asae foundation
Advancing Association and Nonprofit Leadership

ASAE FOUNDATION PROVIDES future-oriented research for the benefit of ASAE members and the association management profession. The Foundation seeks to identify critical trends and effective practices by conducting cutting-edge research no single organization can undertake on its own, while delivering the highest degrees of credibility and impact. The Foundation partners with other organizations in the non-profit arena, as well as leading research and consulting firms, and top colleges and universities to provide the most significant and relevant information on the association industry.

CONTACT US

1575 I Street, NW, Washington, DC 20005
Phone: 202.626.2893
E-mail: evaluations@asaefoundation.org

asaefoundation.org