CYBER COVERAGE CREATIVITY IN A HARD MARKET

A Risk Program Administrators Publication

RPA
RISK PROGRAM ADMINISTRATORS

When it comes to cyber risk and public entities, the current state of affairs is challenging at best: every entity has exposures; potential claim fallout is enormous; tech infrastructure is probably dated; resources are finite; and coverage is hard to come by.
Cyber hackers know public entities are vulnerable and often target towns, cities, schools, etc., for ransom. When losses inevitably occur, cyber triage is critical—but necessary resources are expensive and in short supply. Furthermore, even if a public entity prioritizes and strongly promotes cyber hygiene among its employees, constituents, and business partners, the bad guys will always be one step ahead, and the market may be reluctant to cover risks.

In all of this, the realities of cyber risk today echo the insurance crisis of the 1980s, in which pooling has its roots. As in that earlier time, pools are uniquely positioned to help members solve this conundrum—both through coverage and member service and training programs. This brief white paper shares three specific approaches and highlights some commonalities between them for all pools to consider.

Cyber Coverage Q&A with the Trust

The Arizona School Risk Retention Trust (the Trust) provides property and liability coverage to more than 250 K–12 districts and community colleges across Arizona. It has offered cybersecurity coverage and services for nearly a decade.

INTERVIEW WITH RYAN COLE, TRUST ASSOCIATE EXECUTIVE DIRECTOR AND WES GATES, TRUST CYBERSECURITY DIRECTOR

When did the Trust begin offering cyber coverage?

The Trust first offered this coverage in 2013. According to Cole: "It was an emerging offering, and we could do it very inexpensively—$100,000 or so for the whole pool, originally." The coverage was initially provided to pool members for free. (Editor's note: Imagine!) Members were eager to take advantage because of a recent, large-scale, highly publicized security breach at a local educational institution.

When did you realize you might need to offer more than just coverage?

In 2015, Gates met with representatives of a large, Phoenix-area school district to get an overview of its IT landscape. At one point, the conversation turned to cybersecurity concerns. Gates recalled, "We started keeping a list, and the list kept growing and growing. Everyone kind of looked at each other like, 'Wow, this is a big deal.' That's when the light bulb went on and we realized we might need to provide additional services on top of the coverage."

What cyber services has the Trust offered over the years?

The first service that resulted from the 2015 meeting was a cyber risk assessment. It involved a simple, self-administered survey followed by a prioritized list of risks. Next was phishing education and training for pool members. Pool member employees would receive a realistic-looking simulated phishing email with directions to click on a link, download a file, or otherwise transmit sensitive information. Those who complied did no damage (the email was sent by a cybersecurity contractor, not an actual hacker) but received follow-up education and training on how to steer clear of trouble in the future.

The phishing initiative was followed by a series of additional products and services that were implemented over the years: model templates for pool cyber policies and cyber incident response; member consulting on network architecture, encryption, and access control; training and education on both general and specialized topics (e.g., cybersecurity awareness and disaster recovery); and vulnerability assessments involving a scan of member networks, a report of any identified vulnerabilities, and remediation guidance.

While member service has been the highest priority during this effort, there's also been a consistent message about member ownership of the security issue. As an example, when cybersecurity policies renew in 2022, members who wish to qualify for the lowest deductible must have adopted at least twice-yearly phishing education campaigns plus an air gap backup system for networked resources. ("Air gap backup" refers to a data backup process in which a copy of sensitive data exists that is physically disconnected from and inaccessible via the network.)

How have the Trust's reinsurers influenced the program?

According to Cole, "Markets are becoming skittish about public entity exposure because insurers think hackers are shooting fish in a barrel. So, we're seeing increasing rates, reduced limits, and more stringent underwriting standards. Just to give an illustration, our broker approached 93 markets for reinsurance, and we heard back from 2. It's a shame because our loss experience has actually been good."

The Trust's cyber liability coverage provides members with financial protection for expenses and damages related to a data breach or other cyber liability event. These expenses include:

- **notification costs;**
- **credit monitoring costs;**
- **damages that the member is legally obligated to pay; and**
- **attorney's fees, legal costs, and other expenses resulting from the investigation, adjustment, defense, and appeal of a cyber claim, or circumstances that might lead to a cyber claim.**

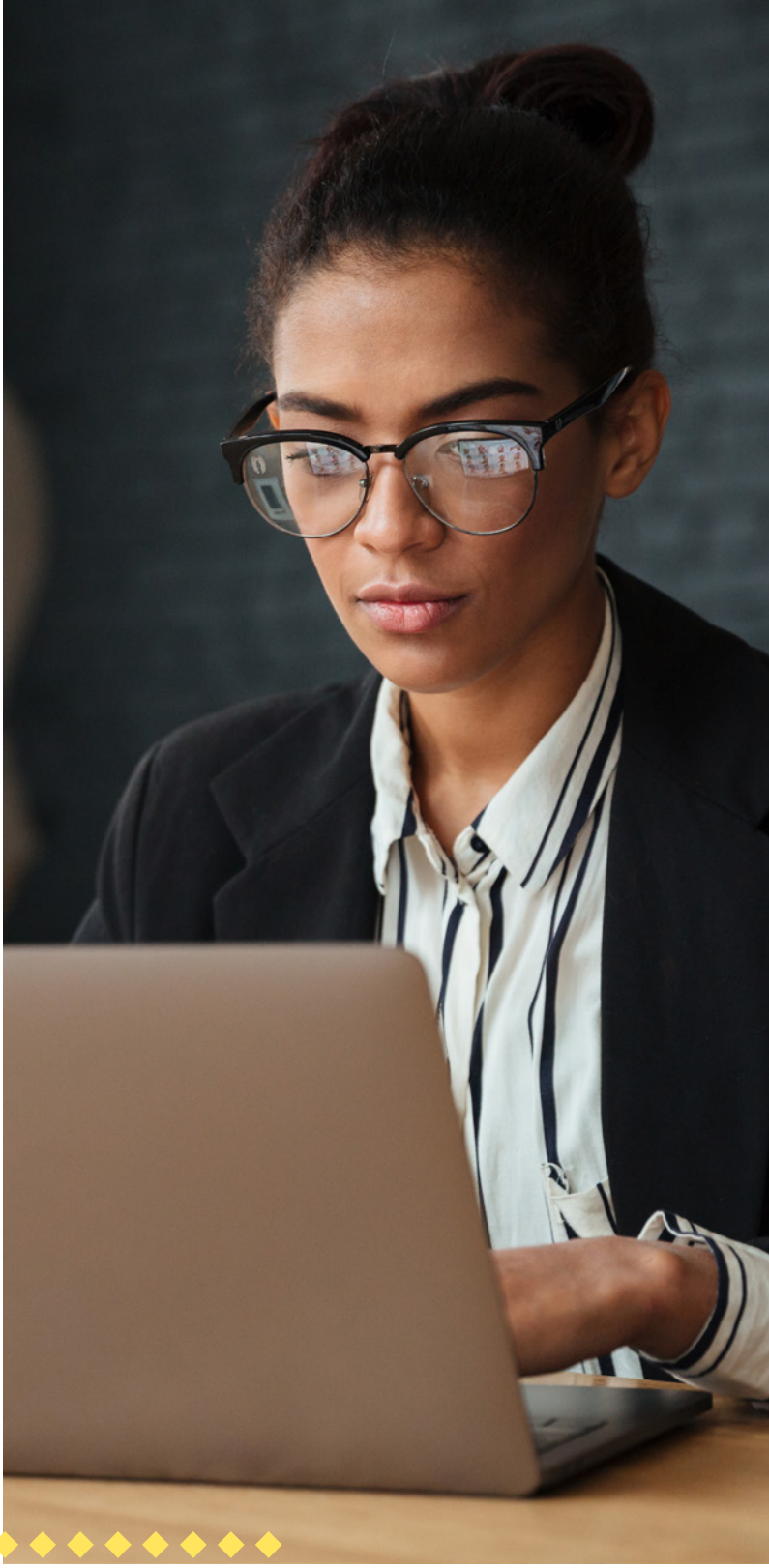
The net result of this has been gentle but continual pressure by the Trust for members to "raise their security game" to meet reinsurers' expectations. Per Gates: "One of the reasons cyber is different from other lines of coverage is that we're asking for a change in behavior from the insureds. These days, you need to do multifactor authentication, have air gap backup, and so on, before reinsurers will even talk to you."

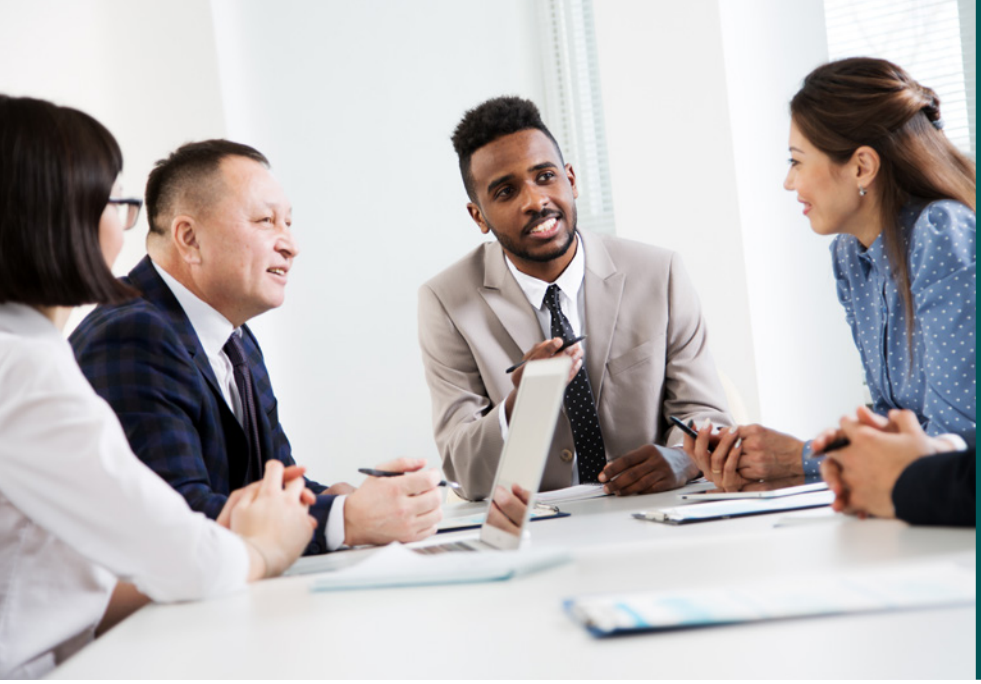
What is member engagement with the cyber program like?

Member willingness to participate in available services, even when they are provided for free, can be a challenge. Gates noted: "Member IT departments are often understaffed, and there are limits to what they can do. So, we would sometimes hear, 'If this isn't part of an audit or something that qualifies us for funds, I've got other fires I need to put out'." But Gates says he sees this changing—a result of an increase in cyber attacks, stricter coverage terms, and the possibility of bad publicity or an undesirable audit finding: "Cybersecurity has evolved quite a bit. What I'm starting to sense is not just a recognition that these things are desirable, but that you really have to do them. Members recognize the need more than they used to."

How do you envision the future of cybersecurity in the pooling space?

Gates sees a continued need for cybersecurity services from pool administrators because the threats are only increasing: "One analogy I'd use is leapfrog. Bad guys come up with a new attack vector, and then everybody moves to patch that. Then the bad guys jump ahead to the next thing. It's a very well-funded criminal enterprise...they're evolving quickly, and they're operating like sophisticated businesses. There's just a lot of momentum—for bad guys, it's a no-brainer as a business."





Creating Member-Specific Cybersecurity Programs: MEL and SPELL Case Studies

By: Scott Tennant, Senior Program Administrator

The Municipal Excess Liability Joint Insurance Fund (MEL) is an excess pool for three municipal Joint Insurance Funds (JIFs) in New Jersey. The School Pool for Excess Liability Limits Joint Insurance Fund (SPELL) is a similar program for three New Jersey school pools. Both programs provide resources to their owner pools, including insurance and member services. The pools, however, are not permitted to use prior years' surplus to fund operating services. Particularly in the case of SPELL, this has impacted the approach to cyber mitigation by limiting the funds available for this effort.

Like most pools, MEL and SPELL did not offer cyber coverage to members until the early 2000s. Then, options were plentiful, limits were high, and retentions were low. However, by the early 2010s, things had changed. The State of New Jersey began requiring public entities to maintain a website and utilize technology-based reporting. Additionally, municipalities were starting to receive credit cards, use direct deposit, and install computer system updates via the internet, while schools were collecting and storing significant personally identifiable information (PII) for employees and students (mostly minors). The pools knew a cyber breach could put New Jersey public entities and citizens at risk, halt normal business operations for days on end, and/or cause significant reputational damage. It was time to more thoroughly address cyber risk.

- MEL and SPELL took broadly similar cyber approaches, with some differences, too, based on available resources, the size of their operations, and their member profiles. These efforts illustrate some ways pools can address cyber risk at different resource levels and regardless of the nature of their membership.

MEL: ROBUST RESOURCE AVAILABILITY

MEL was able to invest significantly in its cyber program, both financially and with talent. In collaboration with a local state university, the pool created a task force comprised of representatives from all members to help understand the full extent of its members' cyber exposures. The taskforce eventually selected a single cyber vendor to evaluate the cybersecurity profiles of the more than 100 members that comprise MEL.

The selected vendor performed on-site evaluations of members over 18 months using a uniform set of evaluation criteria. The resulting information was used to develop cyber risk management programs for MEL members, which included:

- individual cyber hygiene training for employees;
- phishing exercises;
- external scanning of all public-facing IP addresses;
- cyber awareness marketing collateral to be used with members;
- policy and procedure guidance for members on data backup, password standards and maintenance, employee network access, cyber incident response, etc; and
- a cyber-incident hotline to report events (in collaboration with the reinsurer).

The MEL Cyber Risk Management Taskforce also developed a Cyber Risk Management Plan. The three-tiered plan outlines technology security guidelines that each member of a MEL-affiliated JIF is encouraged to adopt and implement. Most aspects of the plan were developed based on member audit findings, with additional input from MEL underwriting. Members are incentivized to adhere to the plan standards through a $25,000 per claim deductible reimbursement if the member is in compliance at the time of the incident.

Finally, MEL has invested in its cyber risk mitigation efforts by directly hiring a technology risk services director to assist members with individual technology audits and help upgrade member technology profiles over time. The program also has a designated dollar amount in the MEL annual budget to directly help members offset technology costs, including new hardware, software, and IT security.

SPELL: CREATIVITY WITH MINIMAL RESOURCES

Unlike MEL, SPELL did not have significant resources to devote to cyber risk management. However, the two pools' overall approach has some similarities, including utilizing a committee, evaluating members, and tiering coverage.

SPELL created an IT/cyber subcommittee comprised of 18 district IT leaders. The subcommittee was tasked with developing a risk management program to improve member awareness of cybersecurity issues and how to manage them. The subcommittee participants knew they needed member data, but they also knew they could not individually evaluate all SPELL members. Thus, they elected to conduct a thorough cyber risk evaluation of two members, with members competing for the opportunity to be evaluated. Lessons learned from the evaluation were extrapolated to create a list of 16 critical cyber risk elements pertinent to the entire SPELL membership.

For coverage, SPELL outlined a cyber application addressing the 16 elements, along with best practices for managing each risk. Member retentions for cyber coverage vary based on their response to the 16 application elements. Members who answer all 16 elements favorably have a retention of $50,000 per claim with 25% coinsurance. Members not in compliance with all 16 elements have a $100,000 retention per claim with 50% coinsurance.

Finally, SPELL also created a webinar series on cyber risk management. Four of the webinars were presented at various conferences, and several more are part of an on-demand, zero-cost webinar series for members.

Despite SPELL's best efforts, the pool has encountered some member resistance on policies impacting human behavior (e.g., password complexity, administrative password restriction, multifactor authentication, personal device registration and control, etc.). It has also found the cost of services and the sheer number of member employees and sites to be more than the pool can fund. For these reasons, the pool's cybersecurity efforts are ongoing but at a relatively low level.

Conclusion

Regardless of resources—financial, analytical, human, or otherwise—pools can and should help members address cyber risks. In the true spirit of pooling, helping often under-resourced members tackle cybersecurity can simply be the right thing to do. As an added bonus, these efforts can make the pool more attractive to reinsurance partners.

Here are some lessons learned and best practice approaches from the pools highlighted in this paper:

- Leverage your membership. However you choose to structure it—special committee, subcommittee, board members, member IT professionals, etc.—a dedicated group of member representatives can help you keep a pulse on member needs and tailor cyber risk management programs accordingly.
- Evaluate member capabilities. Cyber hygiene practices and technology resources will vary greatly among your members. Even if you can't evaluate each member individually, devise an idea of the most common resources and vulnerabilities, then target them with loss control efforts.
- Incentivize behavior. Using coverage tiers may inspire members to adopt good cyber hygiene practices.

Let's Connect

www.rpadmin.com

info@rpadmin.com

RPA
RISK PROGRAM ADMINISTRATORS