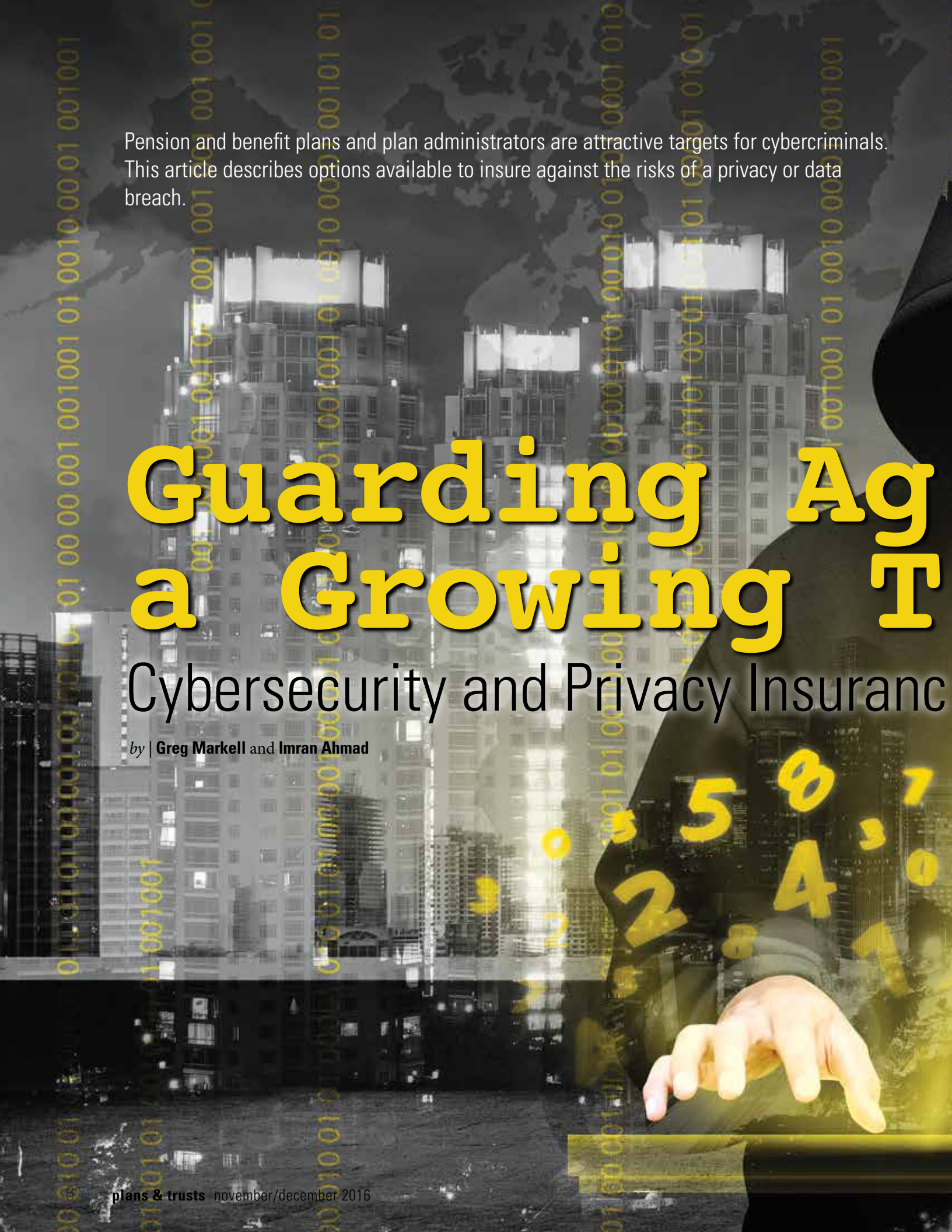
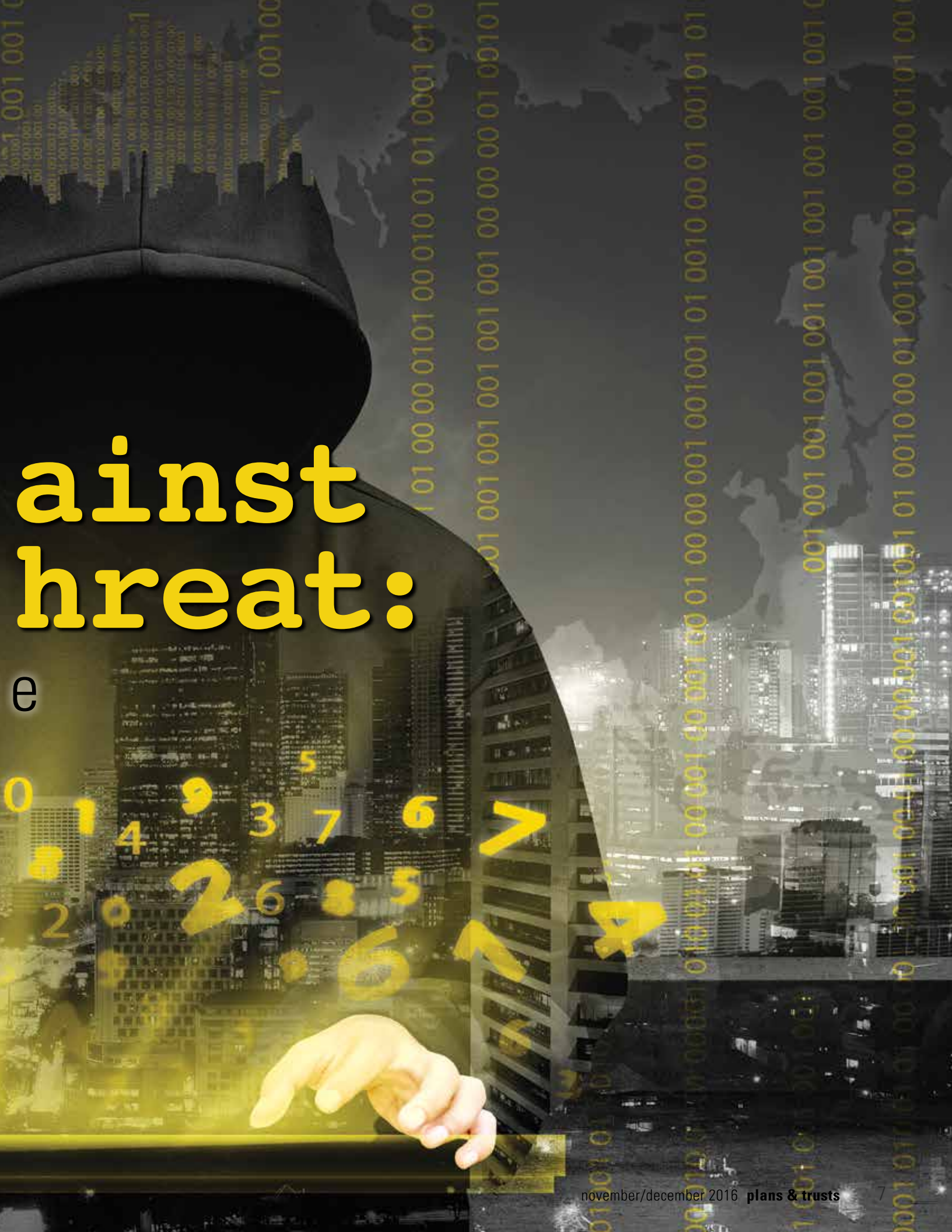


Pension and benefit plans and plan administrators are attractive targets for cybercriminals. This article describes options available to insure against the risks of a privacy or data breach.

Guarding Ag a Growing T

Cybersecurity and Privacy Insuranc

by | **Greg Markell** and **Imran Ahmad**



ainst hreat:

e

Companies around the world continue to dedicate significant resources to safeguard corporate and client information from cybercriminals, yet the bad guys continue to outpace those efforts.

Which information cybercriminals target is constantly evolving. When the value of stolen credit card information dipped, hackers adjusted their tactics and began hitting custodians of health care information. The theft of $81 million from the Bangladesh central bank earlier this year showed that hackers will not hesitate to go for a big payday, as opposed to hacking with the intent to resell information for profit.

Further, some groups are hacking simply to disrupt and incite fear in the hearts of average citizens. With *operational technology* (manufacturing lines, pipelines, etc.) and the *Internet of Things (IoT)* (wearable devices, smart homes, etc.) playing increasingly important roles in the day-to-day operations of organizations, cybersecurity issues for things like supply chain risk, product recall and potential down time due to hacking are all too real for many executives and boards of directors.

Pension and benefit plans and third-party administrators (TPAs) are not immune to these threats. In fact, they likely are attractive targets because of the sensitivity of client and plan member information under their care, custody and control. Access to large pools of money also would seem to put these organizations right in the cross hairs.

Cyberinsurance Solutions

Cybersecurity and privacy liability policies are a hot-button topic in the insurance industry. The proliferation of breaches, data corruption and ransomware is spurring business leaders to look at their options for (1) preventing this from happening to their organization and (2) lessening the impact of a cyberincident. Both of these points should be discussed by management and a board of directors and should be part of the overall risk management discussion.

There is no such thing as absolute cybersecurity, so having a plan for that "what if" scenario becomes increasingly critical. Insurers have recognized that these issues are keeping executives up at night and have responded with changes to cybersecurity/privacy insurance policies.

While cybersecurity risks may not be new, they have certainly evolved. So too must some of the common practices of organizations—and, for the purposes of this article, the evaluation of the insurance coverage they are purchasing. Traditional coverages now have exclusionary language as it relates to "data," which means organizations should be considering buying cyberliability policies to transfer risk off of their balance sheet.

Common Myths

Here is a breakdown of some commonly held myths about cyberattacks:

- **"My organization is not a target."** Unless an organization is completely analog and cash-based, there is likely a risk that someone can and will want to access its information. A cybercriminal may also try to cause a big enough inconvenience to be able to extort the business into paying to make the threat go away.
- **"We have all the latest technology to keep people out."** This is a great start but only one part of the "technology, people and processes" approach to cybersecurity. Plans and TPAs that invest in prevention do deflect many of the nuisance-related intrusions. However, there are still risks of information being compromised by employees, vendors with system access or even legacy paper files.
- **"What we do store isn't worth anything."** Not storing credit card or health care information does potentially reduce the cost per record in the event of a data breach. However, what about e-mails that someone didn't think anyone would ever see or inter-

Learn More

Education

Fraud Prevention Institute for Employee Benefit Plans
July 17-18, 2017, Chicago, Illinois
Visit *www.ifebp.org/fraudprevention* for details.

nal confidential reports about ongoing investigations? In addition, new federal legislation coming into effect within the next year (the Digital Privacy Act) will require mandatory reporting of a data breach to the Office of the Privacy Commissioner. This will add to costs as organizations will likely have to hire lawyers to help guide them through that process. They may also have to hire forensics experts to determine what happened, how it happened, when it happened and who saw anything, which can be extremely costly.

- **"We outsource all of our storage, processing, etc., so we've also outsourced all of our liability."** Plans and administrators should check the indemnification provisions in those contracts. The plan may not be liable if the vendor is clearly responsible for the data breach. But what happens if the organization is responsible or was a conduit through which the bad folks were able to get at the data? What if the organization didn't adhere to massive undertakings in terms of annual audit compliance or remediation procedures that give vendors wiggle room to get out of any issues?
- **"We're already covered under other policies."** Unlikely. There has been a delineation of traditional coverage away from intent to pick up cyberrelated losses. This often comes in the form of "absolute data exclusions" under property and casualty, as well as crime policies. At the very least, the U.S. courts have seen litigation as a result of ambiguous language, and most decisions have favoured the insurers.

The list goes on.

Types of Coverage

The good news for plans and administrators is that the current insurance market has evolved considerably. The application process for standalone coverage has moved away from a purely technical process and has become more of a governance-related exercise. As such, the speed of program implementation also has increased. Gone are the days of having to complete a 25-page, purely technical application that would require input from many different layers of the organization. Now, management and IT can generally complete the application process in 30 minutes.

The scope of available coverages also has increased. Below are some of the basic coverages available under a typical cyberliability and privacy policy that plans and TPAs should consider.

Plans and administrators can buy policies that cover direct expenses, also called *first-party costs*:

- **Notification costs.** These are associated with providing notification of a breach to those affected, including mailing campaigns, credit monitoring, call centres to handle questions and others.
- **Forensic investigative costs.** These are associated with hiring a professional third party to determine where, when and how the breach occurred. This is often one of the costliest areas of a breach, because even if the data was not compromised, there is still a cost for the investigation, and experts charge by the hour for their services.
- **Business interruption.** Lost income if a breach shuts down operations.
- **Crisis management expenses.** These are incurred in hiring a professional team to help prevent harm to a business's reputation. This could include a public relations team, a lawyer to draft a press release, etc.

Takeaways

- Pension and benefit plans and third-party administrators (TPAs) are likely attractive targets for cybercriminals because of the sensitivity of information in their custody and access to large amounts of money.
- Hackers have a variety of methods and motives. Some target information for reselling, while others have stolen large amounts of money or have extorted money from businesses.
- Cybersecurity and privacy insurance policies can cover direct costs of a security breach, including notification, investigation and business interruption costs.
- Policies also can be purchased to cover a firm's liability for damage caused to its clients.
- Buying the right cyberinsurance policy requires a firm to understand its risk profile and have a risk management strategy.

- **Data restoration costs.** These are incurred in restoring the network and data to their prebreach point and can include both hardware and software replacement.
- **Cyberextortion costs.** These are associated with a demand for compensation to stop an attack. This is the most common threat that small businesses face that an insurance policy can address.
- **Regulatory proceedings.** Coverage provides for costs associated with being called in front of a civil, administrative or regulatory proceeding. This portion of the policy will become more important with the Digital Privacy Act coming into effect. Some carriers place this insuring agreement under the third-party coverages.

These types of policies are available for third-party cost coverage (*liability coverages*) if lawsuits are filed against the plan:

- **Network security liability** covers damages and claims expenses associated with the unauthorized access to, degradation of or disruption to the insured's network through the use of malware, denial-of-service attacks, phishing, etc., causing loss.
- **Privacy liability** covers the unauthorized collection, disclosure, use, access, destruction or modification of personal protected information.
- **Internet media liability** covers liability resulting from allegations of infringement of privacy, defamation, disparagement, piracy, copyright infringement, etc., related to content displayed electronically, e.g., on a website, blog, chat forum, etc.

Conclusion

While these are the basic coverages, it is important to note that other concerns can be addressed with a cyberliability and privacy policy. Things like reputational harm and *social engineering fraud* (e-mail scams in which someone pretends to be a supplier/customer and requests money to be sent) can be addressed, subject to underwriting approval of the risk. This is why it is important for clients to talk to their advisors (lawyers and brokers) about what is right for the organization.

Each organization is unique, and much of its risk profile will depend on the type of information it holds, how it operates and how it engages with clients. Accordingly, the right cyberinsurance solution will depend in large part on the organization having a clear (and honest) understanding of its risk profile. Put simply, a "one-size-fits-all" strategy does not work in the new cyberworld.

Having a true risk management discussion (and associated strategy) is vitally important. While companies are buying these policies, it's important to ask: "What is right for our business?" Every organization has different risk-transfer needs, so dialogue to promote efficient insurance purchasing is an essential part of the procurement process.

BIOS

Greg Markell is president and chief executive office of Ridge Canada Cyber Solutions Inc., a Toronto cybersecurity and privacy insurance firm. He previously worked at HUB International, where he focused on privacy liability and cybersecurity/directors and officers insurance. Markell has a bachelor of commerce degree with a minor in economics from Queen's University.

Imran Ahmad is a partner at Miller Thomson LLP in Toronto and leads the cybersecurity and data protection law practice. He serves on the Canadian Advanced Technology Alliance's Cyber Security Council and is a member of the executive committee of the Ontario Bar Association's Privacy and Access to Information Law Section. Ahmad has an LL.M. degree in competition law from the University of Ottawa, an LL.B. degree in corporate law from the University of Montreal and a D.E.S.S. degree in common law from the University of Sherbrooke.