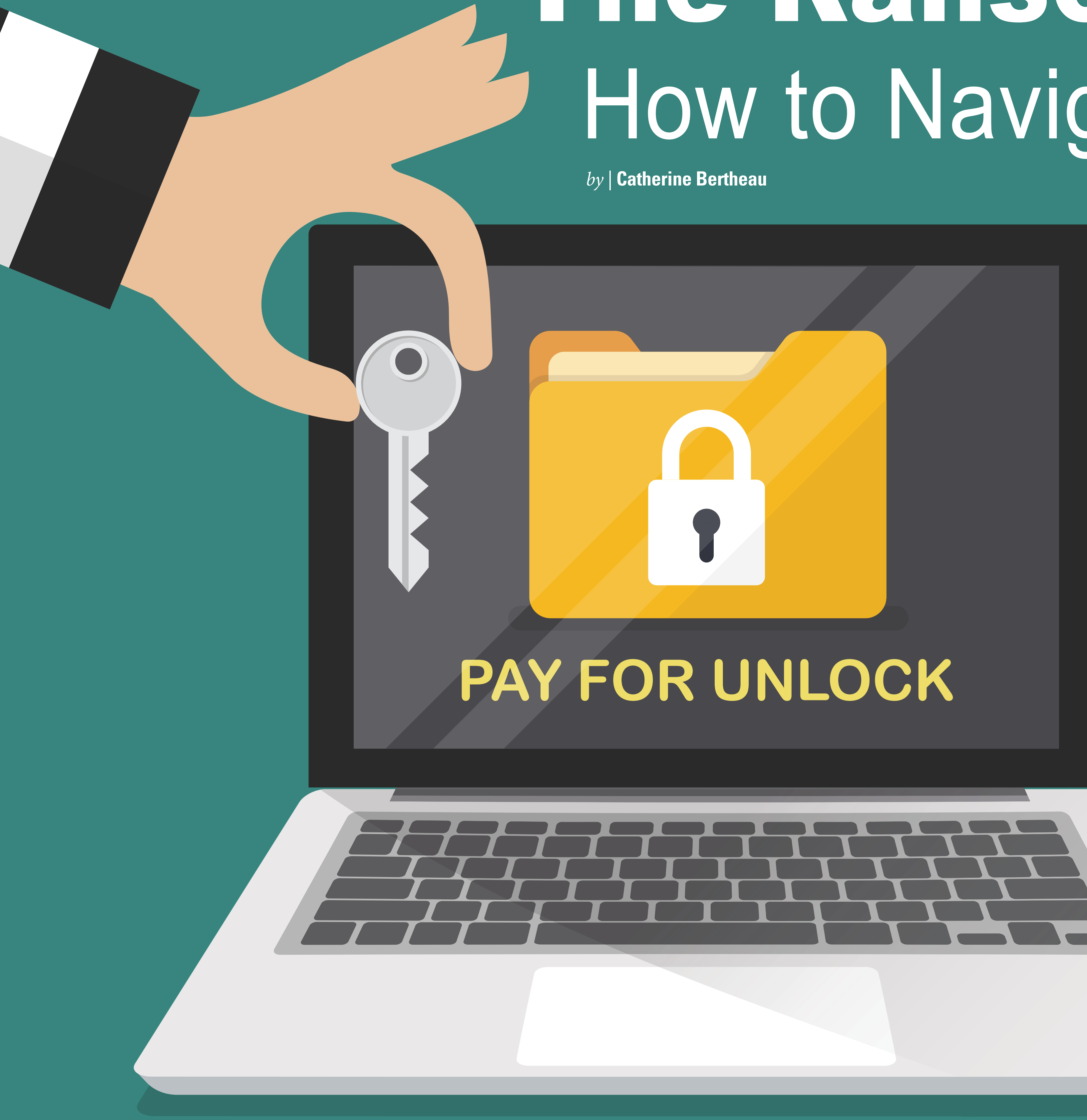
The Ranso

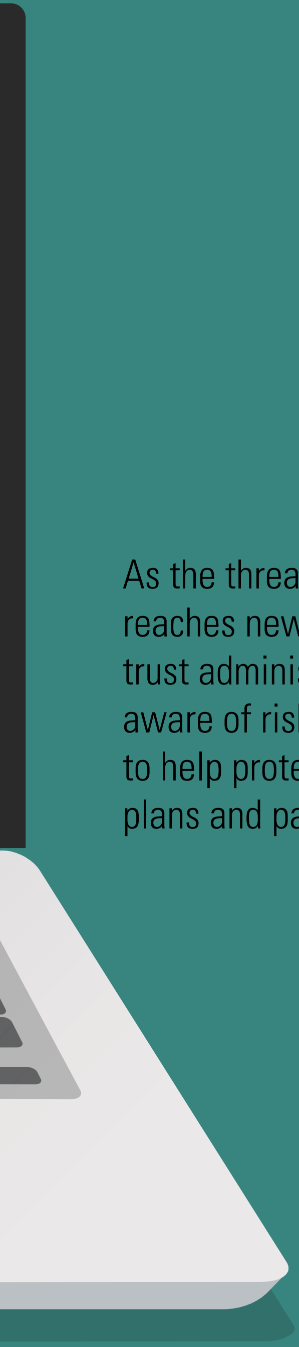
How to Navig

by | **Catherine Bertheau**



omware Deluge:

gate the Perfect Storm



As the threat of ransomware reaches new heights, plan and trust administrators need to be aware of risk mitigation strategies to help protect their organizations, plans and participants.

The digital world is undeniably moving fast and, with it, the threat landscape that the risk management industry is closely monitoring. It is vital for benefits professionals to understand its rapid mutations to help anticipate the perils related to cyber-risk and proactively respond to adverse cyberevents such as data breaches. Risk professionals have not seen such a dynamic and widespread menace to enterprise and personal well-being in a long time. Perhaps ever.

Just a few months ago, key concerns centered on phishing schemes, business email compromise, insider threats and fraudulent transfers. But ransomware has now claimed the front line of the elusive adversaries threatening everything and everyone.

This article will talk about the evolution of ransomware, explore the payment conundrum for organizations facing a ransom and provide five risk mitigation strategies for trust and plan administrators.

Then and Now

While this may seem like a new phenomenon, we can trace the first reported ransomware attack to 1989 and the health care industry. A Harvard-educated doctor and AIDS researcher distributed some 20,000 floppy disks in 90 countries, claiming that they contained breakthrough AIDS education software. Despite clear warnings of software disruption on the leaflets offered with the floppies, many recipients eagerly slid them into their machines, unknowingly installing a dormant malware that would activate upon the 90th reboot of the infected computer. What became known as the AIDS Trojan would then encrypt the computer's drive and file names and display a ransom note for a few hundred dollars to be sent to a Panamanian P.O. box.

Ransomware has greatly evolved from this floppy disk embarrassment, but its modus operandi remains to lock a computer user's content and then ask for a payment in exchange for a decryption key. What is shocking with modern-day malware variants is their sophisticated ability—among other capabilities—to spread using a combination of prebuilt and widely distributed infrastructure such as Trojans and obfuscate detection or reverse-engineering with crypters. Benefiting from footholds ranging from weeks to months into breached networks, according to numerous forensic investigations, cybercriminal activity evolved toward the end of 2019 to a tactic that we sometimes refer to as *double extortion*. To coerce users protected by adequate backups and fail-safe measures into paying ransoms, they started threatening the release of confidential information exfiltrated from their victims prior to executing the traditional ransomware encryption.

Many victim organizations then face the reputational and moral dilemma of refusing to comply with the ransom note instructions, only to risk sensitive documents belonging to their employees, clients or companies being leaked on public websites. In some instances, this meant still refusing to pay the ransom and offering credit and identity monitoring to the potentially affected individuals. In others, it meant contacting key stakeholders to kickstart a hasty public relations campaign to minimize the negative press around the event, accepting the risk of permanent data loss and business disruption. In far too many cases, however, this meant accepting that their backs were up against the wall and resigning to an all-or-nothing transfer of hundreds of thousands to millions of dollars in bitcoins to an untraceable crypto wallet.

Takeaways

- Ransomware attackers seek easy targets and return on investment. Organizations of every size, including small companies, can be within the realm of attractive targets.
- The first step in risk mitigation is to map your digital assets and sensitive information and evaluate your vendors in terms of breach management, notification protocols and overall cybersecurity. Review your contractual language with vendors.
- Educate and train employees on phishing and general cyberattacks to increase your security, and encourage staff to help detect and defend against ransomware attacks.
- Keep your systems up to date. Cybercriminals often use free tools to scan the internet and locate vulnerable systems to perpetrate ransomware attacks.
- Use multifactor authentication (e.g., providing a token, SMS code or phone call to a user) as an effective way to prevent criminals from stealing credentials and gaining access to a corporate network.
- Prepare an incident response plan and third-party response team before a ransomware attack occurs to lessen the potential negative impact to participants and the reputation of the organization.

A Prolific Industry

Ransomware has become a self-sustaining and highly lucrative industry where success breeds success. The professionalism and white-glove service of certain criminal groups is a comically perplexing reminder of the fact that this *is* a business after all. Discounts offered to recognize timely ransom payment, chat windows to hold the victims' hands in decrypting files and systems, customer satisfaction surveys to rate the overall service level: No expense is spared to streamline operations and maximize profits.

Still today, most reports infer that ransomware perpetrators rarely face retaliation or extradition in their home countries. They are either outside the reach of local laws, too sophisticated to be categorically prosecuted or downright protected by their respective governments that reap the benefits of stolen files and intellectual property. More so, the absence of a requirement for entities to notify law enforcement if victimized by ransomware or in connection with payment of a ransom as part of a ransomware event keeps a significant pool of victims unaccounted for.

The Payment Conundrum

To this day, law enforcement has remained mostly neutral on the issue of ransom payments. The most interesting story line last year emerged from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) Specifically Designated Nationals (SDN) list. OFAC is the agency that enforces economic sanctions and prohibits U.S. persons from conducting business or engaging in financial transactions with any person appearing on the SDN list. This could lead to parties involved in ransomware payments or their reimbursement to be found in violation of OFAC regulations and subject to civil fines and penalties. Russian-based Evil Corp made an appearance on the list alongside other sophisticated cyberthreat actors. While OFAC SDN had little traction imposing sanctions due to the difficulty of tying crypto wallets to specific individuals or groups, it was believed by many in the threat intelligence community that Evil Corp was the singular owner of a specific malware variant labelled WastedLocker. This unique credit could allow government officials to diligently intervene by concluding that whenever WastedLocker was used, the ransom recipient was, in fact, a blocked person or entity.

Another growing consideration in the payment conundrum has emerged from a year of skyrocketing ransomware losses indemnified by insurance companies. Historically, detractors have condemned insurance companies for facilitating and reimbursing ransomware payments sent to criminals on behalf of attacked policyholders. Some reports even pointed to cybercriminals referencing the amount of cyber-extortion coverage afforded by a victim's insurance policy in their ransom negotiations. Many were calling for reform and consultations within the industry to stop incentivizing cybercriminals. It is, however, the disproportionate losses incurred on a global scale that pushed insurers to increasingly underwrite to, sublimit or, in newer policies, impose a coinsurance penalty on ransomware losses. Some are referring to a pivotal moment for the cyberinsurance market, and we may very well see more insurers taking a hard stance on ransomware payments and an elevated focus on loss prevention.

One thing has become very clear, and it is that organizations and individuals must adapt and adopt adequate cyber-hygiene measures and make cyber-risk management a priority. This is key to their resilience while facing adverse events and a changing risk landscape. It is unsurprisingly becoming a *sine qua non* to maintaining (affordable) insurability and respecting current and future moral, contractual and legal obligations.

Learn More

Education

Fraud Prevention Institute for Employee Benefit Plans

July 19-20, Nashville, Tennessee

Visit *www.ifebp.org/fraudprevention* for more information.

From the Bookstore

Employee Benefits in Canada, Fourth Edition

Mark Zigler, D. Cameron Hunter, Murray Gold,
Michael Mazzuca and Roberto Tomassini.

International Foundation of Employee Benefit Plans. 2015.

Visit *www.ifebp.org/employeebenefitsincanada* for more information.

Risk Mitigation Strategies for Trust and Plan Administrators

Threat actors are criminally motivated and vested in long-term profiling of victim organizations. They seek easy targets and returns on investment, which can be sizable even when targeting small organizations that misleadingly feel outside the realm of attractive targets. At a very high level—without getting into technical solutions such as advanced hunting and threat detection systems and next-generation antivirus software—there are several strategies that are relatively easy to implement and will readily improve an administrator's cyber posture.

1. **Identify your crown jewels and their life cycle.** Administrators have a fiduciary duty with respect to the management of the plan, which includes the duty to care for personally identifiable information (PII) and protected health information (PHI). Nowadays, most plan sponsors and service organizations use proprietary or cloud-based platforms to store and update participant records, conduct financial transactions for the plan and interact with participants. The use of multiple outside providers, including actuaries, auditors, recordkeepers and many others, lengthens the chain of custody and greatly increases the attack surface for the PII and PHI of the participants. Visibility into how this sensitive information is secured through its life cycle and with multiple partners is often murky at best. The first steps for an organization would be to map its digital assets and sensitive information *(crown jewels)* and evaluate/mitigate vendor risk with clear contractual language—especially as it relates to breach management and notification—as well as perform due diligence on the vendor's cyber-risk posture.
2. **Educate your employees.** Many ransomware attacks spread through phishing emails that are socially engineered to lure victims to click on a link or open an attachment. Training users on phishing indicators and general cyber-awareness is a simple yet effective practice to promote a culture where all feel encouraged to participate in the detection of and defence against ransomware attacks. There is a multitude of affordable and entertaining online-based training modules complete with fake phishing campaigns to measure the propensity of employees to interact with potentially harmful content. While the focus here is on ransomware egress, the benefits of awareness around general items such as the importance of hiding information from computer cameras, locking video conferences, turning off personal assistants—especially around workspaces—and changing default passwords on home devices such as a router are also crucial with growing work-from-home arrangements.
3. **Keep your systems up to date.** One of the most prolific activities for savvy cybercriminals is to use free tools to scan the internet and locate vulnerable systems to perpetrate ransomware attacks. With the deployment of remote workforces and the continued adoption of new systems, applications and vendors that are natural to business growth, the schedule of patches and update releases is surprisingly easy to overlook. Attackers focus on vulnerabilities in personal computers, software and operating systems (such as unsupported Windows 7 and Windows Server 2008), and weaknesses in legacy or unpatched systems on the corporate network as well as those that may be found on the infrastructure of service providers.
4. **Employ multifactor authentication.** In addition to practicing good *password hygiene*, which is the use of unique, lengthy and complex passwords, multifactor (or *two-factor*) authentication has been recognized as an effective measure to prevent the exploitation of stolen credentials to gain access to a corporate network. When properly configured across all forms of log-in and access to email, remote desktops, and external-facing or cloud-based systems and networks, this second factor (such as a token, SMS code, phone call or something else owned only by the user at the time of connecting) is an additional deterrent to capable attackers. While it does not mitigate the need for user training or deeper lines of defence, it should be used by organizations whenever possible.
5. **Prepare for the "when" rather than the "if."** Plan management should prepare an incident response plan and prearrange a third-party response team to lessen the potential impact of a ransomware incident on their reputation and goodwill as well as the residual impact to the participants. The incident response plan should, at a minimum, consider the administrator's current contractual, legal and regulatory obligations, especially as they relate to breach notification. To assist under duress, prevetted individuals/provid-

ers across the disciplines of forensic incident response, legal counsel, crisis communications, ransom negotiation and payment—as well as their contact information—should be clearly laid out in an accessible offline format. With indemnification for breach notification expenses, financial loss, fees and expenses associated with the ransom and incident response, and access to a team of expert vendors, cyber-insurance remains a worthy investment to lessen the burden of an incident on a plan administrator and its participants.

Conclusion

Ransomware is and will continue to be a key concern for all types of organizations, irrespective of size and industry, because of the simple fact that it works. It is a crime in its simplest form: It is easily and highly replicable, it is clean and leverages a currency that is hard to trace, and its payouts are increasing not only in size but also in frequency. With a growing dependence on technology and connectivity and a worldwide pandemic that will by most accounts permanently alter how we conduct business and live, we are undeniably facing a perfect storm.

BIO

Catherine Bertheau is vice president, cyber solutions business development lead, Eastern Canada for Aon Risk Solutions in Montreal, Quebec. She leads the business development activities for Aon's Cyber Solutions, which include assessment and quantification of cyber-risk, protection of critical assets, incident response and the recovery of financial loss associated with an attack. Bertheau is a frequent keynote speaker and cyber-risk panelist at high-profile conferences across the country. Connected to a global network of security, legal and insurance providers, she facilitates cyber-resilience discussions with public and private sector clients across all industry segments to help optimize investment decisions and design more fit-for-purpose risk financing and transfer arrangements.