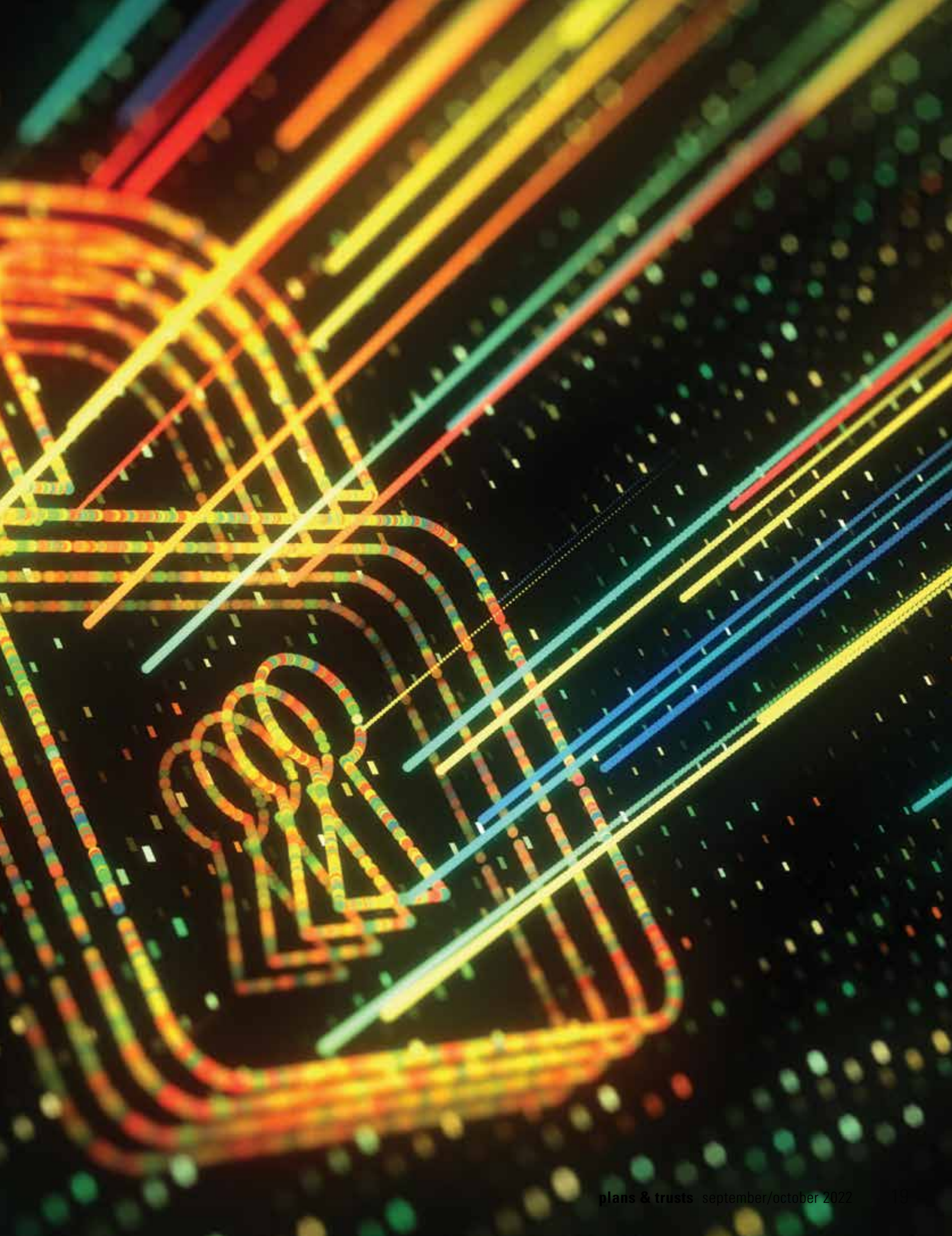
plans & trusts
education | research | information

The Cyberthreat Lights Are Flashing—

But Do Trustees Know How to Prevent Incidents?

by | **Rocco Galletto, David Veld** and **Chetan Sehgal**

Records of members' personal data and information are the new currency, and malicious cybercriminals are on the hunt for them. The authors discuss defense strategies to address the looming risks around trust funds and how they affect both trustees and trust fund members.



It's no secret that companies, government agencies and organizations across the spectrum are becoming increasingly vigilant and unwilling to accept the risks of the evolving cyberthreat space.

As cybersecurity threats grow in scale, complexity and sophistication, today's businesses are faced with complicated risks carrying inevitable aftermath. What used to be a "what if" scenario planned abstractedly for a potential possibility has evolved into a business priority requiring a "when it happens" defense strategy.

Trust funds are no different than any other organization—except they hold one of today's most valuable assets: personal information. Records of members' personal data and information—including real names, email addresses, wage details and health information as well as unique identifiers like social insurance numbers and other information—are the new currency, and malicious cybercriminals are on the hunt for them.

The proliferation in threat actor activities has resulted in compromising this business-critical asset. In fact, recent statistics show that nearly 80% of Canadian businesses have experienced a cyberincident,[1] and an annual loss of $3.12 billion was reportedly attributed to cybercrimes in Canada alone.[2] Billions of customer records have been breached by cybercriminals, and the advent of ransomware and other forms of advanced malware has exposed additional threats to trust funds.

Takeaways

- The prevalence of cyberthreats continues to rise, and no business is immune—especially pension and benefit plan trustees who handle today's modern form of currency: personal data.
- Holistic cybersecurity strategies are the foundational base to secure today's most critical assets; a proactive approach needs to be in place to detect threats early on before it's too late.
- It is the responsibility of trustees to protect client data, or else face monetary, reputational and legal consequences.
- Trustees can proactively safeguard the data at hand by following five key strategies to stay ahead of cyberthreat actors: enhanced account protection, detection mechanism, cyberthreat intelligence, member training and trustee technical control.

Cybersecurity: Trustees' New Frontier

Cybersecurity, now a necessity not to compromise, should be addressed in unconventional ways for organizations to thrive. Trustees need to consider an all-encompassing approach to cyberdefense to safeguard their businesses from all types of threats. This piece sheds light on the risks and threats surrounding trust funds and what steps can be taken to combat cybercrime.

The Bigger Picture: The Role of Trustees

To better understand the looming risks around trust funds and how they affect both trustees and trust fund members, this article focuses on what trust funds hold in their possession and how they make an attractive target for cyberthreats.

Regardless of the type of trust fund, trustees are accountable for the proper management of all property and other assets under their fiduciary responsibility, with the main goal of the trust fund providing benefits to its membership and dependents. Their duties differ according to the type of trust involved and they may employ the services of a third-party administrator to execute functions but, generally, their oversight roles and responsibilities include the following:

- Appoint professional advisers
- Maintain financial and member records
- Ensure registration with regulatory bodies
- Ensure annual filings are completed
- Document records of trustee meetings, decisions and transactions.
- Oversee the financial reporting process of the trust fund
- Ensure there are internal controls over the financial reporting process and trust fund's operations, including the provision of benefits
- Make investment decisions and appoint investment advisers
- Provide information to members and beneficiaries.

The crux of the matter is that all their duties entail holding access to members' personal data, which is where the risk lies.

The Frailty: Accessibility to Personal Data

Trust funds are vulnerable to threats involving sensitive information held by their administrators. Pension and benefit plan trustees have the fiduciary responsibility—and thus the duty—to take measures to ensure they protect the trust funds they oversee.

Personal information, the modern form of currency, is an attractive target for threat actors seeking to monetize their efforts by stealing or compromising records. In fact, the theft and sale of personal information has become a thriving black-market industry.

To better comprehend the assets at stake vs. the threat angle, let's break down the cyberthreat cast against trustees:

Who Is After Your Clients' Data?

Cyberthreat actors. From cybercriminals to hackers or fraudsters, a threat actor exhibits a wide range of capabilities and sophistication, with some being more capable than others. Cyberthreat actors may operate in silos or as part of a larger organization.

What Are Threat Actors After?

Personal information. Threat actors will target personal identification data like names and addresses or financial data like investment amounts and account credentials. Access to identity and personal data is the goal.

Why Are They After the Data?

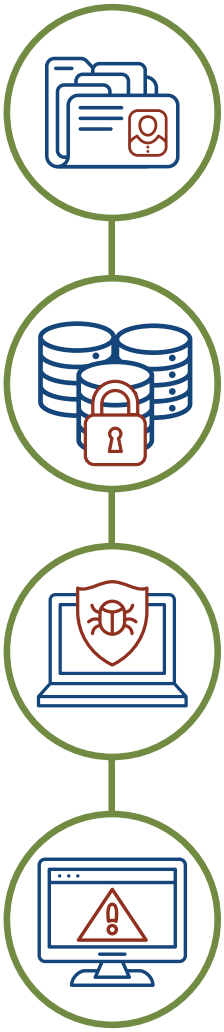
Monetary gain. Threat actors seek personal information to take over accounts and impersonate victims for financial gain or identity theft. In fact, a significant surge in fraudulent activities following the pandemic has been reported on a global scale. According to Statista, global e-commerce fraud grew to $20 billion worldwide in 2021.

What Do They Do With the Data?

Targeted or untargeted attacks. The data is either sold on the dark web, enabling an underground fraud ring, or impersonated to create new accounts and credit card applications. It can also be leveraged to launch more targeted—potentially ransom-based—attacks on individuals.

FIGURE

The Threat Lifecycle



Stage 1
Trust funds collect and hold the personally identifiable information of plan members. This data is sensitive because it contains names, addresses, phone numbers and financial/wage information.

Stage 2
Access to member accounts is often provided using a form of an online portal. The backend database houses and segments all plan member data where a massive repository is held in many storage locations.

Stage 3
This is where an incident may strike. Cyberthreats creep in from fraudulent activities to ransomware or malware. Without end-to-end security measures in place, the data trustees oversee is in grave danger.

Stage 4
When an incident happens, trustees can encounter losses in confidential, personal and financial data. They are also likely to experience operational issues resulting from network/system services interruption, reputational harm and financial harm—from software restoration costs to regulatory penalties and legal fees.

The Threat Lifecycle

Cyberthreats can cause enormous harm to an organization's reputation and finances as well as exposure to legal ramifications. To address the consequences of an incident, it's important to understand the threat that emerges around the data that trustees are handling and how it can end up in the wrong hands.

The figure above outlines the sensitive data that trustees work with and illustrates where and how threat actors strike.

The Solution: Combating Threats Proactively

A fulsome cybersecurity strategy is now considered the baseline require-

ment for all organizations. Trustees, given the wealth of personal information they hold, can rely on insurance to cover financial loss, assuming the organization has fully complied with the policy. But this is only a response to an issue when the damage has already been done, rather than a prevention strategy. Proactive measures should be taken to stop threat actors from succeeding, as a complement to mere reactive mechanisms, when protecting clients' data.

Another consideration is the trustees' existing cyber-footprint—that is, where they hold their database and what measures should be in place to protect the information. It's important to look at the entire security ecosystem, which includes more than just database and server protection.

Stopping cyberattacks at an early stage often achieves the greatest success in defending against complex threats. To help prevent and secure members' data, consider the following five strategies.

Enhanced Account Protection

The general public continues to reuse the same passwords across their multiple web logins, making it easy for a threat actor to compromise their accounts. Consider implementing two-factor authentication (2FA) for added security layers. This helps prevent unauthorized activities and threat actors from gaining access to existing accounts. A combination of a password and a text with a code sent to a smartphone or other means of identification can safeguard potential entry points.

Detection Mechanism

The sophistication of today's cyberthreats requires organizations to shift their focus onto detecting cyberthreats at any phase of their life cycle to mitigate the risks as quickly as possible before any damage is done. Threat actors continue to find ways to evade purpose-built cyberdefenses, and the need for a deliberate, 24/7, year-round, human-led and intelligence-informed cyberdetection and response program to monitor systems for nefarious behavior is critical in modern security operations.

Security controls in the form of technology are a must in the defense against cyberthreats, but these tool sets must be augmented by strong human defenders to act quickly and contain the threat before it achieves its objectives.

Managed detection and response capabilities can further protect trustees' infrastructure and attack surface. They provide a broader coverage by facilitating active monitoring, threat intelligence, threat hunting and vulnerability management.

BIOS

Rocco Galletto is a partner at BDO Canada and leads the firm's cybersecurity practice. He has more than 20 years of experience providing IT and cybersecurity services to companies in various industries, including retail, financial services and the public sector. Galletto helps clients develop effective cyberstrategies and build strong cybersecurity defenses by managing their cyber-risk through business and technology transformation programs.

David Veld is a partner and national pension and benefits leader at BDO Canada. With over 20 years of experience providing assurance, accounting and advisory services to clients in multiple sectors, he specializes in pensions and other employee benefit funds. Veld is also a regular speaker at pension and benefit industry conferences and has authored numerous publications for this industry sector. He is also a member of the accounting standards board Pension Plan Working Group.

Chetan Sehgal is a BDO Canada partner focused on forensic disputes and investigations, including insurance loss claim preparation services. As a seasoned expert with over 20 years of professional accounting and advisory services, he works with companies of varying sizes from all industries in Canada and around the globe. Sehgal has served as an adjunct professor and is a regular speaker, providing his thought leadership in forensic accounting.

Cyberthreat Intelligence (CTI)

Intelligence is a critical component of a modern cybersecurity program. Observations from effective intelligence collection lead to important actions otherwise impossible with traditional security tools.

End-to-end CTI comprises a collection of information covering context, mechanisms, indications and implications regarding targeted or untargeted threats to your organization, informing defensive response and improving your security status. This is an outside-in view, leveraging signals from external sources, monitoring your environment for vulnerabilities and discovering underground campaigns that may target your organization.

Member Training

One of the layers of cyberdefense should include promoting security awareness and training among employees, stakeholders and beneficiaries to ensure they recognize and respond to cyberthreats.

This should be an integral, sustainable part of the efforts to protect the privacy of the data at hand, as both threats and security measures evolve by the day.

Trustee Technical Control

The need for technical controls for trustees is greater now than ever. Any safeguard used to avoid, detect, counteract or minimize security risks to members' personal data and information is considered a security control. Trustees themselves may not have the technical background to design and implement technical controls; however, it is critical that they are satisfied that these controls operate effectively. In many cases, trustees can achieve this by undertaking an independent cybersecurity review of the trust fund's operations.

Technical controls can be tremendously helpful as a significant defense in the event of threat detection prior to a cyberincident. On another note, organizations that can also establish contemporaneous documentation that they used reasonable security safeguards may well succeed in defending against liability and/or mitigating damages and loss exposure. As technology continues to fuel business, technology risk must be managed and, in this continued evolution, security controls must continue to be assessed to ensure coverage is well maintained.

The Silver Lining

Even as cyberthreat actors continue their relentless pursuit to attack organizations, one of the most important defenses against them is preparation. Those with oversight responsibility of the organization must be ready and armed to anticipate and prevent their attacks.

One of the key recommendations is to continue monitoring existing cybersecurity vulnerabilities and sustain strategy enhancements, including training, frameworks and standards, risk assessment, governance, security operations, security engineering and incident response.

Endnotes

1. Canada cybersecurity and cybercrime statistics (2020-2022), Comparitech, Jan 30, 2022, https://www.comparitech.com/blog/information-security/canada-cyber-crime-statistics/.
2. Canadian Cyberfacts, Canadian Cyberthreat Exchange, https://cctx.ca/cyber-facts/.

pdf/922