CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Cybersecurity From the Inside Out

CYBERSECURITY FROM THE TRENCHES (BECAUSE SECURITY INCIDENTS ARE THE "NEW NORMAL")

By Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC

Overview

Based on news headlines, it may seem as though data breaches are an inevitable part of modern life. It comes as a surprise to many individuals and organizations that all damaging security incidents are preventable. While some are more difficult to anticipate, most cybersecurity incidents tend to follow a finite set of scenarios.

The case presented here is inspired by real events. The company, Fincharge Inc., is fictional. This case illustrates how incidents manifest themselves and the degree to which taking the right approach (even if it is a reactive approach) can make all the difference in defusing the attack and rapidly returning the company to normal operations.

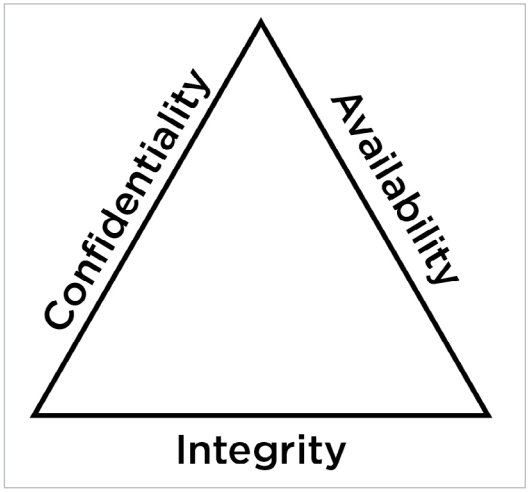
Cybersecurity is not easy but, as we will see here, it's not impossible, either. It just requires competent leadership and high-quality professionals. Do you think you have what it takes? What about your teams? How would you handle this type of event?

MANAGEMENT ACCOUNTING GUIDELINE | CASE STUDY

Case Study

It is *always* about the impact

In any cyberattack scenario, there's an element of trench warfare. Fincharge had identified cybersecurity and privacy as key objectives early in the past decade but largely failed to invest in security processes and tools to make data protection effective. This lack of preparedness meant that, in the event of an attack, the company would have to scramble and adapt to counter the advances of the adversary.



In the span of nine months, the company survived three cyber incidents that happened to fall directly into the three categories of the "CIA triad." Well-known by those in the information security field, the CIA triad's three components are data confidentiality, integrity and availability. In this case study, the company sustained attacks that impacted all three objectives of information security:

- Confidentiality: Sensitive information was permanently exposed
- Integrity: Information at rest was threatened by malicious software
- Availability: During the pandemic, systems were unusable for an extended period of time

How did it all get so real?

Confidentiality impact: Unbeknownst to Fincharge, its service provider, EnterTrust, suffered a cyber breach that exposed all customer records belonging to Fincharge. An internal employee accessed client data and made copies with the hope of profiting from sales of customer information. The incident was only reported to Fincharge seven weeks later, through EnterTrust's lawyer. That delay in reporting set an ominous tone for the relationship with this supplier, forcing the company to immediately notify impacted individuals and adapt to manage the influx of queries from concerned customers.

What really happened?

As soon as Fincharge learned of the data breach, the company's privacy officer and cybersecurity advisor reported the incident to the Office of the Privacy Commissioner of Canada (OPC), the agency in charge of privacy compliance, who issued the following recommendations:

1. Establish a phone line to enable Fincharge customers to call and ask questions about the breach and be referred to EnterTrust's own support line.

2. Take out cyber liability insurance to prevent the potential future exploitation of the compromised records from becoming a serious liability issue for Fincharge.
3. Notify customers and inform them of the severity of the impact and offer additional support, resources and guidance as needed.

Integrity impact: Two months later, Fincharge experienced a direct, email-borne cyberattack that installed malicious software and threatened to encrypt and delete the data on Fincharge's servers. As many types of modern malware do, this cyber attack's approach was to send custom emails to a dozen Fincharge customers from what looked like their own co-workers, asking them to urgently open an attachment. When opened, the attachment proceeded to scan the local computer and surrounding network, looking for vulnerabilities and a way to "call home" for more malware. Fincharge IT scrambled to rapidly evolve in an attempt to get ahead of the invisible threat.

What really happened?

The objective of the malware was to locate and steal Fincharge's sensitive data and to interrupt operations long enough to extract a ransom payment. This incident was successfully defused by a rapid and appropriate series of activities carried out by Fincharge's IT team. This was possible because of the IT team's work responding to the initial data breach.

Successfully preventing a potential breach before it reached the extortion phase was a joint effort between Fincharge's IT team and its CPA, who was trained in cybersecurity incident response. Reporting to the CIO and CFO, the CPA's advisory function was able to bridge barriers and rapidly translate technical threat language into real business impact. These decisive approaches allowed the company to rapidly scan and isolate network computers, shut down unnecessary devices and individually investigate all assets that had come into contact with the original infected systems. This approach to "digital contact tracing" is different in each scenario, but the outcome is the same: effectively containing a data breach as soon as possible with limited IT resources.

Availability impact: At the outset of the COVID-19 pandemic, Fincharge made the decision to shut down its servers to reduce its exposure to threats.

Unfortunately, this decision also had the effect of preventing legitimate users from accessing their work resources. As a result, the company had to scramble to issue laptops and untested VPN tokens to employees. Work that used to take place inside the secure network perimeter now had to be done from home, essentially making every employee their own system administrator. The difficulty of providing IT support to diverse, remote home offices compounded by the productivity impact of the business interruption illustrated just how disruptive such malicious events can be.

The bumpy transition to this inefficient "pandemic" model illustrated the urgent need for planning, rehearsing, training and having access to reliable resources in a pinch.

What really happened?

In Q1 of 2020, the global COVID-19 pandemic forced Fincharge to interrupt normal operations and close its doors to the public.

From the beginning of this disruptive situation, Fincharge IT took key steps to prioritize user support, ensuring that staff had secure access to work resources, secure connectivity, and guidance for scenarios that required exceptions, additional research and rapid execution. Within any SME, this work would be a full-time job. The capabilities of Fincharge's IT team were taxed to the limit.

Aftermath and lessons learned

These three situations were independent of one another and separated by at least two months, giving the Fincharge IT department some breathing room as each situation was individually addressed.

The company concluded that the common denominator in all three situations was its longstanding false sense of security. To inform its approach to data protection, the organization had been relying on a templated privacy policy with little relevance to current operations. The company's already weak monitoring and detection capabilities hinted at inadequate preventative controls. However, the success of corrective actions was made possible by the heroic efforts of the IT team.

A risk assessment revealed that the organization was not, as expected, in the top tier of risk-aware organizations. In fact, Fincharge was rated just below 2.0 on a scale from 1 to 5.

Maturity model [1 to 5]	Risk preparedness
1. Heroic, unstructured, reactive efforts	Ad-hoc, reactive security practices
2. Task and project-specific actions	Some technical control enforcement
3. Proactively-defined and standardized response	Documented processes and policies
4. Measured, controlled and managed program	Systematic metrics and evidence
5. Continuous optimized improvement	Innovative, optimized risk solutions

This approach – measuring performance from process to security preparedness – is based on the capability maturity model, a standard industry metric. It is a qualitative process that any small or mid-size business can follow as part of a self-assessment. While not a precise science, this approach offers a valuable look into the company's degree of preparedness. Where available, CPA and IT staff can leverage security testing tools to approximate how their results can fit along a 1-to-5 scale. Armed with this information, SMEs and non-profits

can plan their security investments and prioritize risk-management activities with greater confidence and clarity.

Incident analysis

The problems uncovered during the malware attack incident can be summarized as the convergence of several factors:

1. **Prevention: inadequate controls to prevent the attack from reaching users**
   Organizations that have suffered data breaches commonly discover that their security tools were inadequately configured and maintained. A false sense of security can hamper efforts to contain a breach. In Fincharge's case, attempts at structuring a legacy security program were not prioritized. Had such activities taken place, IT could have helped to increase the organization's risk maturity.

2. **Detection: inconsistent action during the cyberattack**
   Several employees noticed the unusual email communications but did not initially report it, while others felt uncomfortable about escalating the issue. A consistent approach based on a simple incident response reporting form will serve to record incidents as soon as they occur and empower employees with situational awareness.

   A role-based system that is specific to the types of situations experienced by employees in different departments must help employees consistently monitor, detect and identify potential incidents. An asset inventory and risk register are tools companies should use to document which assets require active security monitoring.

3. **Reaction: lack of prepared communications and clear guidance for employees**
   Fincharge had to rapidly assign functional roles to IT team members, create company-wide communications and make decisions to contain the breach. Such reactive measures should be prepared ahead of time, with team members ready to complete a sequence of tasks and employees sensitized to the possibility of receiving approved communications asking them to take specific actions on their workstations.

The data breach experienced by Fincharge's third-party service provider, EnterTrust, can be presented in similar terms:

1. **Prevention: Service-level management agreements should include the use of security controls**
   Every service provider with access to Fincharge data, particularly personal information, must agree to conform to secure data transfer and storage practices. The information should be encrypted during transfer to specific individuals, and Fincharge should carry out an annual review of its security procedures.

2. **Detection: Controls should be in place to detect breaches as they occur**
   The ability to detect and identify security incidents experienced by third parties depends in large part on the effectiveness of their security monitoring and the enforcement of any requirements to disclose such information to Fincharge. Detective and compensating

controls (i.e., proprietary database entries and recurring inventory activities) should be adopted to ensure that if such practices are not followed, Fincharge will be made aware.

3. **Reaction: Response and reporting should immediately follow detection**
   Having an incident response team ready to report the data breach to the proper authorities as soon as it is detected should be the goal of the reaction phase. This helps mitigate the risk of a potential backlash by data subjects related to risky delays, anticipated impact, potential liability and violations of compliance.

These above events resulted in a number of cybersecurity improvements including the creation of a subset of the IT team focused specifically on defensive cybersecurity. This group is responsible for managing preventative activities related to the protection of data, systems and applications, such as patch management and event monitoring. This protection is a fundamental ingredient in Fincharge's information risk management capabilities.

The events of the past year demonstrated Fincharge's need for proactive security testing. Such exercises include penetration testing to uncover unknown weaknesses, scanning for vulnerabilities, risk reviews, threat-risk assessments (TRA), and data protection and compliance reviews called privacy impact assessments (PIA).

Remediation steps taken

Some of the key activities that took place at Fincharge during and immediately following these events included:

- raising user awareness about proper incident reporting
- employees participating in and supporting IT security measures to reduce the negative impact of the incidents
- learning about the overall cybersecurity posture of Fincharge, identifying which ad-hoc measures work, what documentation is in place and which team skills can be focused on defensive versus investigative incident response activities

Fincharge can improve its cybersecurity posture by completing an inventory of its sensitive information including all its storage locations. Not knowing where the data is and how much information is stored presents a significant risk for the organization due to the inconsistent allocation of controls and standardized metrics to determine the effectiveness of security measures.

To present a clearer picture of proper information risk management, we have illustrated Fincharge's overall approach across six categories (or pillars) of risk:

1. Asset management: Complete an inventory and classification of Fincharge's information assets

2. Operational security: Improve protection against data loss and data leaks
3. Vulnerability management: Introduce systematic vulnerability scanning (and rate the relative risk of identified threats)
4. Administrative security: Present departmental cybersecurity training to all staff (with a focus on incident management and situational awareness)
5. Privacy management: Complete preliminary privacy impact analysis (PPIA) on processes, systems and applications that contain sensitive information
6. Risk management: Select and test an appropriate cyber liability insurance policy for Fincharge

Although Fincharge does not currently possess detailed documentation of its practices and configurations, the IT Security Team's ability to carry out the following critical tasks was pivotal the company's defence against the cyberattacks it faced:

- rapidly inventorying systems suspected of infection
- tracking the root cause of the infection (i.e., determining the original "patient zero" within the company)
- removing suspected infected machines from the network
- inoculating and temporarily monitoring suspect workstations
- updating email filtering technology to block email-borne attacks
- updating firewall filtering to block the malware's home servers
- performing multiple layers of antivirus scanning to avoid false negative detections
- deploying new anti-malware on servers
- testing ransomware to determine whether systems can detect and contain it
- implementing measures to shut down machines during evenings and weekends to reduce risk

This approach was correctly sequenced to ensure the best use of time and resources at a time of high urgency, however it continues to lack systematic controls for proactive network scanning, behavioural analysis and data leak prevention – all elements that would result in a significantly more mature operational security posture.

A note on frequent security testing

Beyond the implementation and identification of such layered controls (often called "defence in depth") it is important to provide assurance of control effectiveness to stakeholders by carrying out standardized testing. One of the key benefits of a disciplined testing methodology is its ability to derive a clear picture of the organization's asset inventory, which is necessary for numerous operational, strategic and compliance activities including data classification, workforce cybersecurity education, budgeting for IT investments and qualifying for cyber liability insurance.

Summary

This case study serves as a reminder to accounting practitioners, professionals and other trusted advisors about the fact that organizations can compensate for a lack of controls with a corresponding level of employee awareness and vigilance.

The need for compliance and enforcement is predicated by the actions taken to empower and educate employees. This is most effectively done using relevant statistics, role-based examples and structured opportunities for learning and information exchange.

With the combination of frictionless safeguards, responsible leadership and an unwavering focus on the interests of stakeholders, organizations stand to benefit from the most valuable return on investment: the earned trust of customers, partners and employees.

Resources

Also by Claudiu Popa:

- *The Canadian Privacy and Data Security Toolkit for SME* (1st and 2nd ed. CPA Canada, 2015)
- *Managing Personal Information for Privacy-Savvy Organizations* (Carswell, 2012)
- *The Canadian Cyberfraud Handbook* (Thomson Reuters, 2017)
- *Technology Spotlight: Cybersecurity and Data Protection* (CPA Canada, 2019)
- *Technology Spotlight: Securing Your Brand and Reputation on Social Media* (CPA Canada, 2019)

Additional references

- CPA Canada, *Management Accounting Guideline (MAG) – From Data to Decisions: A Five-Step Approach to Data-Driven Decision-Making* (2020)
- AICPA, Controls Mapping Documents (2017)
- Industry Canada, The CyberSecure Canada Control Framework (2021)
- NIST, Cybersecurity Framework (2020)
- The Canadian Centre for Cyber Security, The Path to Enterprise Security (2020)

About the author

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC, is a certified information security and privacy professional and media contributor on enterprise risk management, IT security and data protection. With over 25 years of global experience in security auditing, international standards and board-level risk consulting, Claudiu is a trusted management advisor to Canadian enterprises and their stakeholders, supporting critical security strategy and decision support for privacy and security compliance, data protection and cybercrime prevention.

He is the author of four published books, numerous articles and multiple academic papers on information protection, compliance and risk governance based on primary cybersecurity research. As a certified professional, Claudiu remains an ardent champion of information security and a trusted corporate coach to Canadian organizations that are passionate about improving their security and protecting their customers.

DISCLAIMER

This paper was prepared by CPA Canada as non-authoritative guidance.

CPA Canada and the author do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use or application of or reliance on this material.