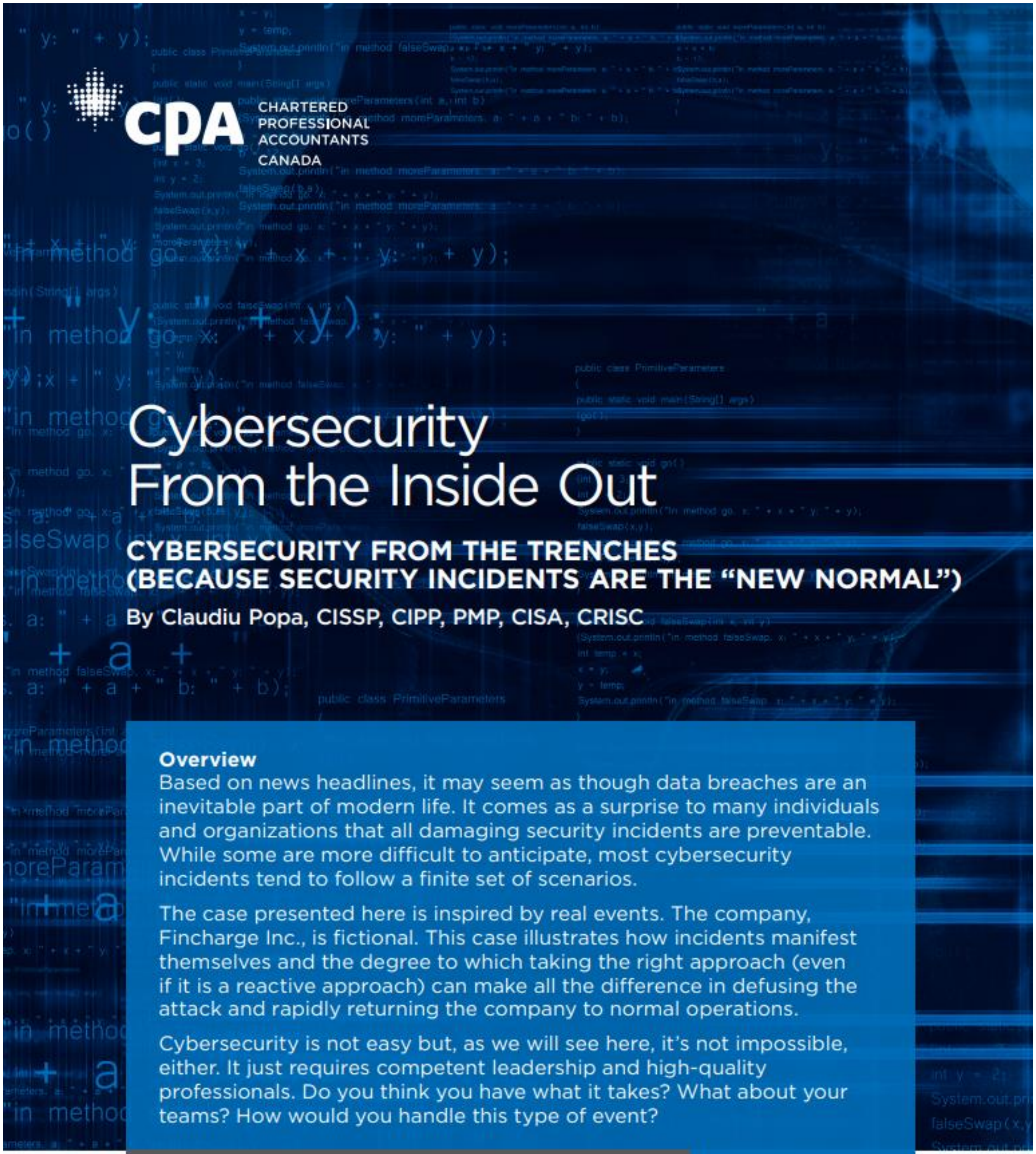


CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

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

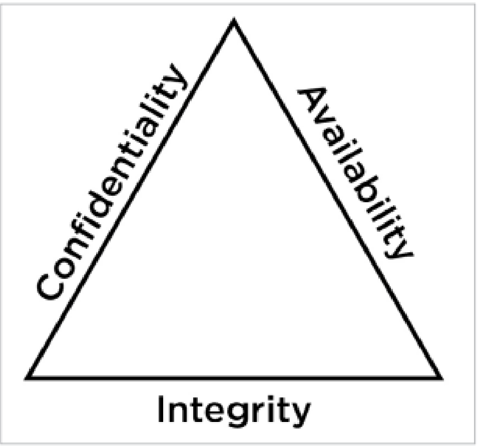
CASE STUDY

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:



How did it all get so real?

IMPACT 1 : 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.

IMPACT 2 : 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.

IMPACT 3 : 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.