Lessons from a Front Line Cyber Adjuster

Crawford®

Cyber attacks are common and pervasive. Controlling costs to manage loss ratios starts with using experts appropriately.

Loss adjusters manage risk through collaboration with specialists who apply technical knowledge and expertise, allowing adjusters to focus on details and guide the process.

The level of sophistication criminal outfits employ to target their victims, ranging from small to large enterprises, can be likened to regular business operations.

"Cyber attacks are becoming more frequent — so much so that criminals run it like a business," said Neal Jardine, Cyber Practice Leader at Crawford Canada.

"Attackers are developing software where they sell their crimes as a service."

Since 2017 Jardine and his team have handled over 200 cyber insurance claims.

His insights on how cyber criminals access and manipulate computer systems are strengthened by his background in computer science and information technology. Thus bringing a unique understanding of how systems are built and what goes into a cyber breach.

"I'm a computer expert who became an insurance adjuster," he said. *"I've worked with teams maintaining networks to keep hackers out and data safe by understanding how a network works and how computers interact."*

He said hackers operate today in the same manner as 15 years ago: *"they find a loophole, get in, escalate privileges, map the network, and launch the attack."*

Led by Jardine, Crawford's cyber practice is staffed with adjusters recruited within the company for their talent as adjusters paired with their intuitive computer skills. They are stationed in strategic provinces to best respond to client needs with round the clock support from the Global Cyber Team.

What is a Cyber Breach & How Can It Be Prevented?

Cyber criminals employ a range of tactics to infiltrate computer systems.

Common cyber attacks include:

- Phishing, a fraudulent entity masked as a trustworthy one attempts to obtain sensitive information such as usernames, passwords and credit card details;
- Social engineering, manipulating people through psychological means to perform actions or divulge confidential information;
- Ransomware and extortion, malicious software that threatens to publish victims' data or block access until ransom is paid;
- Data exfiltration, the unauthorized transfer of sensitive information from a target's network to a location controlled by the threat actor;
- Denial of service, an attack that makes a machine or network resource unavailable to its intended users by disrupting services of a host connected to the internet;
- Man-in-the-middle, where the attacker secretly relays and/or alters communication between two parties who believe they are communicating directly with each other.

In the past, ransom attacks were the most common cyber attack but now hackers are using phishing and psychological tactics to breach computer systems.

"Hackers used to be more disengaged and used a spray and prey approach with ransomware to extort their victim and commit crimes but now criminals are targeting employees in influential roles within a company to commit more complex attacks leading to higher payouts," Jardine said.

"Through phishing, threat actors can harvest login credentials. Once they have those credentials they can use them to socially engineer wire transfer fraud events on clients, employees and customers of the insured."

Examples like these are becoming more common, cyber attacks are growing in numbers and the average cost of cyber attacks is increasing.

In 2018 the average cost of an event ranged from $44,000 to $162,000, for medium-sized companies (50 to 249 employees) and large companies (250 to 999 employees) respectively. In 2019, that figure rose to the range of $184,000 to $715,000, for medium-sized and large companies respectively.

Business operations all have one thing in common — they are all at risk of a cyber breach.

"Businesses never think they will be the next victim," Jardine said.

"It doesn't matter that you don't store personal information. It's not about the data that you store: you are a business that makes money using data and that makes you a target. What people don't realize is that it's not the value of the data to the hackers that matters — it's the value of the data to you. What you would pay to get that data back."

In January 2021 The Canadian Anti-Fraud Centre, which collects and provides information on fraud and identity theft, warned about the prevalence of phishing attacks on businesses and organizations. It said that "spear phishing" (through email, text, phone, and fax) is the most common and dangerous attack method used on companies.

The centre said scammers who use phishing as a method of attack will use email to impose as business executives asking employees to send large wire transfers (sometimes exceeding $100,000) and that fraudsters will take their time to collect information to be able to send as convincing emails as possible.

Jardine said businesses are often unprepared for cyber breaches because of an underestimation of the risk.

"IT departments' defences are not at the same level of sophistication as criminals' offences," he said. *"And unfortunately criminals' sophistication level is much higher than what businesses perceive it to be."*

If a company thinks they will not be victim to a cyber breach, it will not take the problem seriously enough to implement robust security measures. The bottleneck on putting appropriate security measures into place can be compared to the time when seatbelts in cars were first introduced.

"People found seatbelts restrictive, it was an extra and bothersome step for drivers but now it is considered a normal part of driving," Jardine said.

"In cyber security, people describe the two-factor authentication — an extra security step when logging into a computer system — the same way: restrictive and bothersome."

Same as drivers and passengers overcame the perceived restrictive quality of the seatbelt, a shift in perception about the restrictiveness of added cyber security measures is imperative.

"Getting over the restrictiveness of security can help reduce claim frequency and costs," Jardine said.

"After a cyber event, an adjuster can sit down with clients to go over what went wrong and prevent it from happening again."

Company Culture and Hiring the Right Expert

Assessing cyber risk goes beyond looking at the price tag of a security breach. If a breach happens, the aftershock will permeate the whole business.

"That is why there has to be a culture of security built into a company's risk management foundation," Jardine said.

"The risk has to be treated seriously at the board room-level and throughout the organization because when a breach happens it will have a ripple effect throughout the company."

He said companies' risk managers have to understand the intricacies of their cyber insurance policy. And the cyber insurance landscape is in flux as coverage continues to evolve.

"There are more insurers in the market offering cyber coverage," Jardine said.

"Historically cyber coverage was built out of the need for business interruption during the 'dot-com' era. Now we are seeing coverages expand to include supply chain interruption and the new attack vectors of threat actors. Eventually we are likely to see coverage turn to an all-risk product subject to exclusion —but the industry is not quite there yet."

He said while product availability is increasing and becoming more sophisticated, where the product is really changing is, increasingly, insurers are placing the onus on insureds to take steps to prevent cyber breaches and handle them in a specific manner when they occur.

He said businesses may slowly start to realize how enticing their data and operations are to cyber criminals but it can't be overstated how large a number 200 cyber claims in three years is — given how young the cyber insurance market is.

The prevalence and sophistication of cyber breaches requires loss adjusters' expertise to handle claims appropriately and control costs. The role of adjusters has always been to investigate the event, manage the process, assign experts and control the costs.

"Crawford's Global Cyber team acts as the first notice of loss for many insurers globally. Adjusters are there to answer the call when the insurance client needs them the most. The team of cyber adjusters quickly assess the type of event and assign the most effective experts for a specific task or role, be it a ransom negotiation or analyzing a forensic report to determine any regulatory compliance requirements", Jardine said.

Breach Coaches may be needed to help the insured understand the legal compliance requirement when personal information is exposed to threat actors.

However Jardine advises *"Breach Coaches can often get pulled into dealing with business interruption, public relations or ransom negotiations."*

This can dramatically increase claims adjusting costs given the justifiably high rates that many of the expert and legally trained Breach Coaches charge.

There are intricacies to handling an insurance claim that can be cost effectively handled by expert cyber adjusters who will control claim loss costs, gather the facts, focus on the details of insurance coverage and engage the necessary experts to provide the best action plan post cyber event for the insurance client to protect their insured and uninsured assets.

Adjusters with a broad range of cyber experiences can explain to a client how the insurance policy will respond, what is not covered and what their requirements are under the various privacy laws in Canada.

With cyber loss ratios rising, controlling claims costs starts with using experts appropriately.

Contact our Expert

Neal Jardine BSc, CSM, CRM, CIP, CFEI
Senior General Adjuster | Cyber Practice Leader Canada
P: (416) 957-5040
M: (416) 458-7476
E: Neal.Jardine@crawco.ca

About Crawford & Company®

For over 75 years, Crawford has solved the world's claims handling challenges and helped businesses keep their focus where it belongs – on people.

Loss Adjusting

Third Party Administration

Managed Repair

Medical Management

On-Demand Services

Catastrophe Response

9,000 employees | **50,000** field resources | **70** countries | **$18B+** claims managed annually

Crawford®

CRAW-0221

Learn more at
www.crawco.ca