THE GROWTH OF THE CYBERCRIME LANDSCAPE IN CANADA

Cyber

Gallagher

Insurance | Risk Management | Consulting

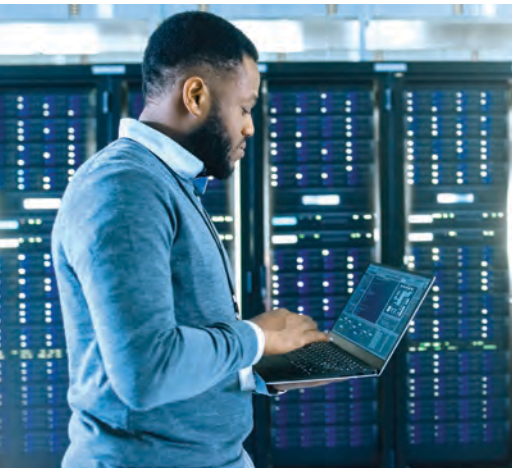
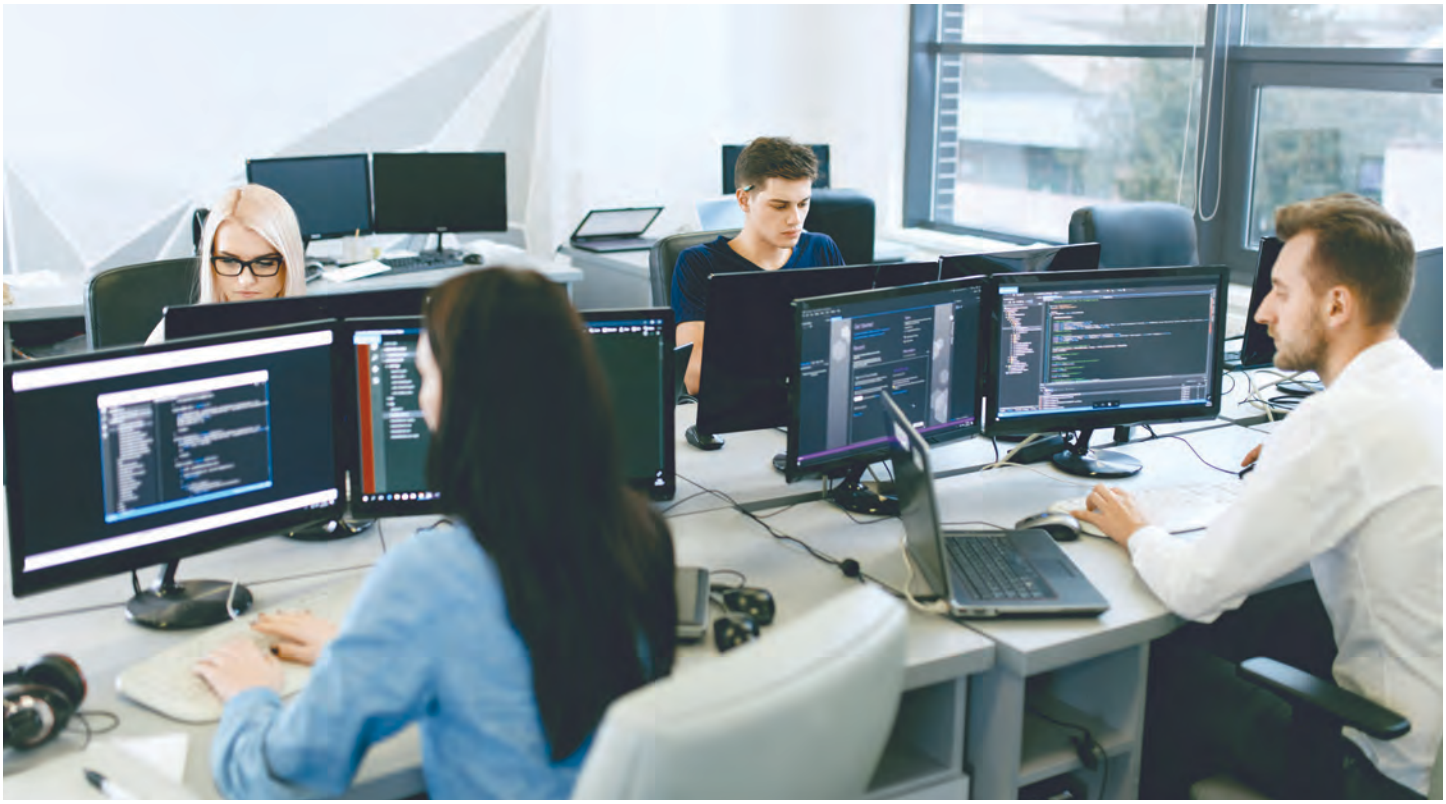


Table of Contents

Executive summary

Data theft marketplaces are expected to grow rapidly, aided by open access to tools, knowledge and dark web "hacker" forums. Cybercrimes can be perpetrated by threat actors with lower levels of technical capability.

- Cybercrime and ransomware remains the #1 cyberthreat for Canadian business operators. The global cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025[1]—viewed as a conservative estimate by some.
- The proliferation of cybercrime stems from the growing ease of access to criminal expertise, hacking tools and assets via the dark web enabling threat actors to access sensitive data, financial information and commercial IP.
- In 2020, malware attacks increased by 358% compared to 2019. The most common cyberthreat facing businesses and individuals is phishing.[2]
- In 2023, cybercrime marketplaces are predicted to become a major growth market with perpetrators targeting industries handling sensitive commercial data, including financial services, healthcare and government/public sector.



Section 1: Risk landscape

The rapidly evolving cyberspace is challenging organizations to adapt at breakneck pace to respond to a complex risk exposure. Technology supply chains are increasingly global, cybercriminals operate with international reach, while the legislative and regulatory bodies governing cyberspace and the internet are under growing pressure to respond to a systemic risk that increasingly lurks in the shadows, often undetected.

THE DARK WEB—ECONOMICS AND COST TO THE BUSINESS COMMUNITY

Operating under a cloak of anonymity, the dark web provides a trading platform for knowledge and coordinating cyberattack events. Presenting an executive headache for business owners, cybercrime has also become an issue of national security and public safety.

The ease of access to hacking tools and expertise through criminal marketplaces has created a platform for Cybercrime-as-a-Service (CaaS), particularly given the prevailing pattern of global economic turbulence, fluctuating trade volumes and geopolitical tensions continue. With a major cybercrime event currently anticipated to occur in 2023/24 and ransomware, phishing and data hacking techniques becoming more sophisticated, the spectre of a multi-vector cyberattack presents a growing concern.[3]

Hosting malicious software, cybercrime forums and hacking tools, the dark web offers a safe harbour for criminal activity. Websites providing tools, coding and inside information to hack into points of IT network vulnerability in order to exfiltrate and encrypt sensitive data while holding organizations to ransom, cybercrime is becoming big business on the dark web.

An upside risk is the option for cyber risk managers to use Ransomware as a Service (RaaS) forums as an assessment/analysis tool for clients who are viewed as having heightened vulnerability to cyberattack risks.

CRIME VECTORS

Data theft and privacy breaches remain two of the most widely reported cyber attack vectors. However, there are other vectors in the mix. IP theft, including the distribution of pay-to-play streaming media, and elsewhere counterfeiting and forgery are also the MO for cybercrime perpetrators, with activities including file and software key sharing, pirating streaming content and placing gaming files into a cyberlocker with restricted access. Cybercrime is costing IP owners, entrepreneurs and innovation platforms significant losses in revenues and legal fees in response to breaches of copyright.

> Cybercrime is a systemic issue for medium to large organizations, particularly for risks associated with cloud service hacking, particularly in the healthcare sector and financial institutions handling sensitive data. In-house cyber defence teams are paying a lot more attention to potential points of vulnerability in software and programs where hacking could lead to a large number of claims stemming from one incident. This extends to the software vendors, in some cases small companies, facing >CA$1 million losses, to notify their clients and provide them with credit monitoring following data exposure events.
>
> Although the average cyber claim in Canada is CA$10 million or less, significantly lower than the global average, we assess data breach liability limits on the basis of the dollar cost per record and extrapolate out to the number of data records held within the software or program. Using this measure, organizations in that band are buying somewhere between CA$2 million and CA$10 million in limits. When re-evaluated every 12 months, we have watched the goalposts move and we're likely to see trends emerge for 2024 that didn't exist in 2023.
>
> **Dan Lewis, Vice President Management Liability and Cyber (Canada)**

TOOLS OF THE [CYBER] TRADE

The growing number of tools and services available to threat actors presents a worrying picture for in-house cyber defence teams and external specialists. As the dark web platform becomes increasingly recognized as the "go to" destination for PII and IP, revenue from crime enablement is expected to grow exponentially, and with the emergence of online communities, would-be criminals can be equipped with the tools and knowledge they need. Worse still, once content has been uploaded, there is generally nothing that can be done to remove it.

Organized ransomware platforms: Examples

Conti—a ransomware group first observed in 2020, is allegedly linked to a Russian cyber group. It featured in the FBI's Internet Crime Report (2021) as one of the top three ransomware variants that targeted critical infrastructure sector operators. Others were LockBit and REvil/Sodinokibi.

Hive—a global RaaS operator, was successfully infiltrated in mid-2022 and shut down through a coordinated international operation involving the US (FBI), UK (National Crime Agency), Germany, Netherlands and Europol to identify the ring leaders. Using a double-extortion method of encrypting data locally, Hive also exfiltrated and threatened to decrypt sensitive data on failure to pay the ransom.

LockBit—despite being one of the most prolific ransomware groups ever, the LockBit collective has maintained a low profile while building the volume of high-profile malware attacks that include Royal Mail (UK), The Guardian, and the SickKids hospital in Canada, the latter prompting an apology and decryption key. Committing more than 1,100 major ransomware attacks globally with an average US$85,000 ransom loss value, LockBit shows no signs of slowing down.

Killnet—probably one of the largest ones at the moment, a spinoff from the Russian military. They have actively stated that they're going after Western companies, and they utilize a ransomware and anger called rootkit Black. Again, I can send you some screenshots of all of this because my clients are getting it.

UK-OSINT—a publicly available site on the dark web, and looks almost identical to wikiHow. The site features a page with a drop-down menu providing options on how to exploit the targeted business/brand/organization from a ransomware perspective. Participants purchase a bronze, silver or gold package, including 24/7 support. The trade-off is that a purchase reveals the name or alias of the actor and confirms that a crime is being committed. A question remains on whether the forum is facilitating the crime or simply providing the technology.

Clop—a ransomware and double extortion actor targeting Windows 10 apps and Microsoft Office applications. First executing a process killer before encrypting data, programs and software, Clop has enhanced its capability to target entire networks with the BBC, Boots and British Airways being the latest victims held to ransom (June 2023).

CYBERCRIME—CONFLICTING ETHICS AND RISE OF HACKTIVISM

Cybercrime extends beyond a group of data thieves. Cyber activism brings a new dimension into the mix as hacktivists use data hacking for the purpose of the better good (in their view). With hacktivism showing no signs of stopping in the foreseeable future, so-called ethical hacking has become a significant percentage in daily cybercrime statistics. There's no hiding place for brands and corporate organizations whose ESG agenda conflicts with the protest agenda, with the big reveal of sensitive trading data, internal chat conversations and payment platforms being shut down being some examples amongst many on how this cyber-led agenda is travelling.

Conti, one of the world's largest ransomware groups in 2022, is another example. When messages surfaced expressing Conti's support for Russia following the Ukraine invasion, affronted members published online chat conversions and gave cyber protection agencies the means to shut down the group. A tale of the perpetrator becoming the victim.

GEOPOLITICAL MOTIVATION

Since the outbreak of the Russia-Ukraine conflict, collaborative ransomware attacks on non-friendly targets have become less likely. While the US, as one example, has grown its alliances with friendly nations to strengthen cyber defences, rising geopolitical tensions have led to increased levels of state-sponsored and politically driven attacks.[5]

Despite a cooling between several nations, thankfully, goodwill remains in selected cases. In 2021, the Russia-based REvil Ransomware-as-a-Service group was responsible for more than 200 attacks in the US alone, including the high profile Colonial Pipeline attack.[6] The cyber gang claimed to rake in annual revenues of over $100 million. Some might forget that it was the Russian government that eventually took down REvil. Reportedly, the takedown was part of a rare collaborative effort between the United States and Russia.

LARGE CORPORATE ORGANIZATIONS REMAIN FIRMLY IN THE CYBER CROSSHAIRS

While big, high-profile breaches fill headlines, many intruders prefer to target smaller organizations. Between 2020 and 2021, cyber attacks on small companies surged by more than 150%, according to RiskRecon, a Mastercard company that evaluates companies' security risks.

The reasons behind this trend are twofold. For starters, smaller targets usually have weaker security. Also, high-profile targets like infrastructure or big corporations will likely attract a stronger law enforcement response. This means schools, local police departments, small government offices and businesses with less than 1,000 employees will continue to be attacked.

Section 2: Risk analysis

RISK #1—PASSWORDS ARE NO LONGER A SAFE HAVEN

Password manager LastPass revealed a notifiable breach event in mid-2022, where a cyberattacker had accessed third-party cloud data and in turn compromised multiple employees. Credentials, digital wallet and accounts keys were stolen, enabling access to encrypted data on the third-party cloud region. While the customer-held master password is required to fully access the data, given that a significant percentage of those passwords use less than robust naming strategies, passwords remain vulnerable to coordinated attacks in the right hands.

While the scope and scale of the LastPass attack are being assessed, it does present a salient warning about the use of cloud-based platforms for highly sensitive data.

As workers seek increased simplicity, having a multi-purpose mobile device for business and personal use is becoming more commonplace and mobile device management (MDM) services are steadily gaining traction. MDM software can help to keep sensitive data secure on a non-invasive platform, while managing smartphones, tablets, laptops, desktops, TVs and devices across multiple operating systems including Android iOS, iPadOS, tvOS, macOS, Windows and Chrome OS.

Multifactor authentication (user and administrator) and robust password controls are the way forward in 2023.

RISK #2—HACKERS GET SMARTER, CYBERSECURITY PROFESSIONALS HARDER TO FIND

In 2022, Canadian energy, health, manufacturing sectors were major targets of ransomware attacks. Ransomware will most likely continue to be the No. 1 threat.[7] In response, he suggested cultivating expertise and education efforts among cyber champions, including a chief information security officer in the C-suite. Cybersecurity teams are generally understaffed and often overwhelmed.

Mandating complex password changes every six months, employing dual-factor authentication and biometric voice recognition while inspecting and validating users going in and out of private networks at all levels will continue to be important. Preparing a risk management business continuity plan covering cyber prevention processes, data management, IT vendor due diligence and reputation management makes a difference. Ideally, this plan and risk management implementation should be owned and managed in-house versus an external supplier who may only be obligated to deliver part of what is realistically required.

RISK #3 — AI TOOLS MAKE IT EASIER TO ENACT A CYBERCRIME [SOFTWARE AND PROGRAMS]

The scope and scale of OpenAI platforms as a cyberattack vector is currently in debate, with growing concerns on how these platforms could be weaponized for malicious intent. Recent analysis of underground hacking communities indicates that cybercriminals are now using OpenAI to develop tools. Given the low skill threshold required for developing malware using OpenAI technology, the prospect of more sophisticated threat actors enhancing AI-based tools for criminal purposes is an emerging risk that cannot be underestimated.

Recent reporting on ChatGPT being used as a malware generation tool to commit fraudulent activity suggests there is significant work ahead to safeguard AI platforms from inappropriate use for criminal activity, including the creation of dark web marketplaces. ChatGPT can be used to automate the trade of stolen account data, payment cards and the targeted deployment of malware using cryptocurrencies for payment (Monero, Bitcoin and Ethereum).[4]

> ChatGPT can write bash scripts for hacking programs, and literally ask ChatGPT to build the code or bash script for a specific crime event. The concern here is that enabling a cybercrime event requires only basic-level knowledge to achieve the desired outcome. You can ask GPT to write that for you and then copy and paste it into Kali or Linux Terminal, and it will pretty much execute what you want it to do.
>
> AI is speeding up the cybercrime process. A batch script program has been developed that can write hacking programs, such as a social engineering email asking someone to pay for an invoice.
>
> Language can be a point of vulnerability in a hacking attempt, and one of the things that catches a criminal out is the incorrect and/or inconsistent spelling and social context on how a word or terminology is used. It could be, for example, something as simple as how we spell 'defence' differently in the US vs. UK.
>
> **Johnty Mongan, Global Head of Cyber Risk Management**

RISK #4 — OLDER TECHNOLOGY PLATFORMS AND SYSTEMS ARE PRIME TARGETS CYBERCRIME

Cyber attackers target operating environments that offer easier access to malware and/or ransomware campaigns. Fortinet, Follina (MS Office) and Proxynet are three examples of software targeted for criminal activity in recent years. Attackers exploit exposed Windows Remote Desktop Protocol (RDP) services and unpatched Remote Code Execution (RCE) vulnerabilities to execute commands and place malicious code in a network.

As cybercrime becomes more established as a revenue source for malicious actors, crime-as-a-service is providing a route for professional hackers to offer their services for a fee via the dark web.

Section 3: Future cybercrime landscape

WHERE NEXT FOR DARK WEB CYBER ACTORS?

Given the rapidly evolving digital ecosystem, cybersecurity leaders and decision-makers need to be thinking strategically about how cybercrime trends will play out in three, five and ten years' time to realistically stay ahead of the curve. Ransomware will become more sophisticated and more considered in assessing the data that carries the highest value and leverage for the criminal—commercially and financially,[8] and double extortion events look set to increase over the next 12-18 months.

Navigating uncertainty, unpredictability and the unknown plus the ability to identify patterns, forecast anticipated attack vectors, and leverage learning from historic attacks to sharpen cyber defences for the future.

The growing use of AI and automation-driven cyber defence tools presents a new vector for crime as determined hackers turn their attention to developing effective attack strategies against these digital solutions.[9]

Sources:
[1]"2022 Official Cybercrime Report," *eSentire*, 2022. PDF file.
[2]Griffiths, Charles. "The Latest Cyber Crime Statistics (updated October 2023)," *AAG*, Oct 2023.
[3]Brooks, Chuck. "Cybersecurity Trends and Statistics for 2023; What You Need to Know, *Forbes*, 5 Mar 2023.
[4]Ben-Moshe, Sharon et al. "OpwnAI: AI That Can Save the Day or Hack It Away," *Check Point Research*, 19 Dec 2022.
[5]"Inside Ransomware's Organised Underworld," BCS, 28 Mar 2023.
[6]Easterly, Jen and Tom Fanning. "The Attack on Colonial Pipeline: What We've Learned and What We've Done Over the Past Two Years," *Cybersecurity & Infrastructure Security Agency*, 7 May 2023. [7]"National Cyber Threat Assessment 2023–2024," *Canada Centre for Cybersecurity*, updated 28 Oct 2022.
[8]Bouckaert, Joanna et al. "Seven Trends That Could Shape the Future of Cybersecurity in 2030," *World Economic Forum*, 3 Mar 2023.
[9]"2022 State of Cybersecurity Report," *ISACA*, 23 Mar 2022. Gated PDF.

AJG.com/ca **The Gallagher Way.** Since 1927.

Gallagher