"The Evolution of Cybercrime Through Ransomware: From Global Attacks to the SickKids Incident and Future Threats"

Dhivyarackshana Sridharan (100985546)

Faculty of Business and Technology, Ontario Tech University

BUSI 2570U: Cybercrime

Dr. Bernadette (Bernie) Schell

July 30th, 2025

Introduction

Cybercrime has come a long way from the days of minor online pranks. Today, it is a serious threat, well organized, large-scale, and capable of causing real damage. One of the most troubling developments is the rise of ransomware attacks. In these cases, hackers lock up a victim's data and demand payment to unlock it. What is especially worrying is that they were going after vital systems hospitals, schools, even government agencies inserting lives and essential services at risk (Interpol, 2023; Maimon & Choi, 2021). Take what happened in January 2023, for example, Toronto's Hospital for Sick Children (SickKids) was hit by a ransomware attack blamed on the LockBit group a gang the FBI has called one of the most dangerous in the cybercrime world (Federal Bureau of Investigation, 2023). Interestingly, after the incident, LockBit claimed the attack went against their own rules and kicked out the affiliate who carried it out (CBC News, 2023)

The LockBit attack did not just expose how fragile critical public services can be, it also revealed how cybercriminal tactics are constantly evolving. These days, many of these groups operate more like businesses, using affiliates and even offering "ransomware as a service" to anyone willing to pay (Europol, 2023). Over the years, we have seen a clear shift in the way digital threats have developed. From the relatively harmless Morris Worm back in the 80s to massive operations like the SolarWinds breach, each major cyber incident has pushed the digital security world to adapt and respond in new ways (Holt et al., 2020). Looking back at these landmark attacks and the damage they left behind we start to see a bigger picture. They have affected individuals, disrupted companies, and shaken entire systems. By studying what happened and how it happened, we can better understand today's cybercrime landscape and why strong, proactive defense strategies are more important than ever.

The paper takes a close look at the SickKids cyberattack, along with three other major incidents that have shaped the history of cybercrime. It also looks ahead to the kinds of threats we could be dealing with in 2025 and lays out a mix of legal, technical, and business strategies to help tackle them head-on.

The SickKids Attack and the LockBit Ransomware Group

On December 18, 2022, Toronto's Hospital for Sick Children better known as SickKids fell victim to a ransomware attack that brought major parts of the hospital's operations to a halt. Critical services like lab testing, diagnostics, and even internal phone systems were thrown into disarray (CBC News, 2023). The attack was traced back to LockBit, a notorious cybercrime group that the FBI has labeled as "One of the most active and destructive ransomware variants" in the world (Federal Bureau of Investigation, 2023). Although SickKids was able to recover most of its systems within a few weeks, the incident sparked serious concerns. Many questioned the ethics and legality of targeting a children's hospital and it served as a wake-up call about the growing threat of cyberattacks on healthcare institutions.

LockBit runs on a "ransomware as a service" (RaaS) model, where the core developers create the malware and then rent it out to affiliates in exchange for a cut of any ransom paid (Europol, 2023), This setup has allowed the group to grow quickly and hit a wide range of targets including businesses, schools, and even hospitals. What made the SickKids case stand out was how LockBit responded. After the attack, the group issued a public apology, claiming it had been carried out by a rogue affiliate who broke their supposed rules against targeting hospitals. In an unusual twist for the cybercrime world, they even handed over a decryption key without asking for any ransom, a rare gesture that raised eyebrows and questions about the group's motives (Europol, 2023; CBC News, 2023).

The ransomware attack on SickKids exposed just how devastating these kinds of instructions can be,especially when they hit critical care systems. It also shed light on the complex, often murky inner workings of today's cybercrime groups. In the aftermath of the attack, hospital staff had no choice but to fall back on manual methods slowing down lab work, delaying diagnostic imaging, and making it harder to stay in touch with patients' families. While thankfully no patient deaths were reported, the disruption created serious risks to patient safety and led to delays in essential care (Global News, 2023).

From a technical point of view, ransomware works by locking (encrypting) the files on a victim's network and then demanding a ransom usually in cryptocurrency in exchange for the key to unblock them. LockBit's version of ransomware is especially dangerous because of how fast it spreads and the advanced tools it uses. For instance, it can automatically steal data and adjust how it encrypts files to sneak past common security software (Trend Micro, 2022). To break into a system. LockBit affiliates often rely on tactics like phishing emails, weak points in Remote Desktop Protocol (RDP), or known software flaws. Once inside, they move through the network, gaining access to more systems and boosting their permissions to maximize damage (CISA, 2023).

The SickKids incident highlights how cybercrime is evolving and becoming even more dangerous. Hackers are not just going after big banks or massive corporations anymore. Increasingly, they are targeting places like hospitals and schools organizations that may not have strong cybersecurity but hold incredibly high stakes. These attacks do not just lead to data breaches or financial losses. In critical settings like pediatric healthcare, they can directly affect people's lives, delaying treatment and putting vulnerable patients at serious risk.

Historical Cyber Incidents That Shaped Modern Cybercrime

To truly understand how cybercrime has evolved, it is important to look back at the incidents that shaped how we deal with it today. Over the years, certain attacks have grabbed public attention,exposed deep weaknesses in digital systems, and pushed governments to rethink their policies. The four events highlighted below ranging from the late 1980s to the 2020s mark major turning points in the fight against cybercrime. Each one played a role in shaping the way we now respond to digital threats, whether through improved technology, tougher laws, or new strategies for staying secure online.

The Morris Worm (1988)

The Morris, launched on November 2, 1988, by Robert Tappen Morris, is often seen as the first cyberattack to make global headlines. What started as an academic experiment to estimate the size of the internet quickly spiraled out of control due to all computers online at the time (Spafford, 1989). The impact was massive. Email systems went down, file sharing was disrupted, and internet connection across schools, research labs, and even military networks came to a standstill. Restoring those systems cost millions, and the chaos revealed just how unprepared the digital world was for threats of this scale (Hafner & Markoff, 1995). This event led to the first-ever convictions under the U.S. Computer Fraud and Abuse Act and saved as a major wake-up call. It did not just spark new legislation it helped launch the modern era of cybersecurity awareness.

The Target Data Breach (2013)

In late 2013, retail giant Tagert became the victim of one of the most well-known cyberattacks in U.S. history. Hackers gained access to Target's internal network through a third party HVAC vendor, a seemingly unlikely entry point. Once inside, they installed malware on

point-of-sale (POS) systems, stealing credit and debit information from around 40 million customers, along with personal details for another 70 million (Krebs, 2014).

The fallout was massive. Target faced over $200 million in damages and legal claims, not to mention the long-term hit to consumer trust. What really stood out, though, was how the breach exposed critical vulnerabilities, weak oversight of third-party vendors and a lack of proper network segmentation. These flaws made it far too easy for attackers to move through the system. In the aftermath, the retail industry began to take cybersecurity more seriously. The breach helped push the U.S. toward wider adaptation of EMV chip technology and prompted many companies to rethink how they manage digital security especially in their chains (Romanosky, 2016). Even years later, the Target breach serves as a cautionary tale about how one small gap can open the door to a massive disaster.

The WannaCry Ransomware Attack (2017)

In May 2017, the world witnessed one of the most widespread and disruptive ransomware attacks in history, WannaCry. In just a matter of days, the malware infected more than 300,000 computers across 150 countries. It targeted a known vulnerability in Microsoft Windows, encrypting users' files and demanding payment in Bitcoin to unlock them (Greenberg, 2018). One of the hardest-hit organizations was the UK's National Health Service (NHS). The attack brought hospital systems to a halt forcing the cancellation of over 19,000 appointments and even shutting down emergency departments temporarily. It exposed just how fragile critical infrastructure can be when systems go unpatched.

Globally, the financial fallout was massive, estimated at over $4 billion in damages (Europol, 2018). Investigators later traced the attack to the Lazarus Group, a hacking outfit linked to North Korea. This connection underscored a major turning point in cybercrime, the

increasing involvement of nation-states in launching large-scale digital attacks. Wannacry did not just encrypt data it changed the way the word viewed ransomware. It showed how quickly malware could spread, how deeply it could cut into public services, and how vital it is to keep systems updated and secure.

The SolarWinds Supply Chain Attack (2020)

In December 2020, the cybersecurity world was rocked by the discovery of a major supply chain attack involving SolarWinds, a popular IT management company. Hackers had managed to slip malicious code into a routine update for the company's Orion software, an update that was then unknowingly downloaded and installed by thousands of clients, including U.S. government agencies and major Fortune 500 films (Zetter, 2021). What made this attack especially dangerous was its stealth. For months, the attackers had quiet access to sensitive systems, gathering intelligence without raising alarms. In total, more than 18,000 organizations were affected, making it one of the most widespread and sophisticated cyber-espionage operations ever uncovered. The breach was ultimately linked to APT29, also known as Cozy Bear, a Russian state-sponsored hacking group.

Beyond the immediate damage, the SolarWinds attack exposed serious flaws in how trusted software is managed and secured. It showed that traditional perimeter-based security models were not enough to stop highly advanced threats. As a result, the incident pushed both government and industry leaders to take a hard look at supply chain vulnerabilities and ramp up efforts toward zero-trust architecture, a model that assumes no system or user should be trusted by default.

The State of Cybercrime in 2025 and in future years

By 2025, cybercrime has evolved into something far more complex and dangerous than ever before. Gone are the days when most attacks relied on simple phishing scams or brute-force tactics. Today's cybercriminals are tapping into cutting-edge technologies like artificial intelligence, deepfakes, and cloud-based vulnerabilities to execute highly targeted, sophisticated operations. This is not just a change in how attacks are carried out it is also a shift in who and what is being targeted. Healthcare systems, schools, and critical infrastructure have become prime targets, largely because they often lack the advanced defences needed to stop these modern threats. The tools are smarter, the stakes are higher, and the impacts are increasingly real-world. As cybercrime continues to evolve, it is clear that defence strategies must evolve too, moving beyond basic protection and toward proactive, adaptive security models that can keep up with this fast-changing landscape.

One of the most alarming trends in cybercrime as of 2025 is the rise of AI-generated malware. Cybercriminals are now using machine learning to create malicious software that can actually learn from its environment. These advanced programs monitor how a system reacts and then adjust their tactics in real time to slip past security tools without raising red flags. AI is not just being used to write smarter code it is also being leveraged to create incredibly convincing phishing messages. Using publicly available data, attackers can mimic someone's writing style to craft emails or texts that feel personal and authentic, making it much more likely that a victim will take the bait (Kumar & Carley, 2022). What makes these attacks so dangerous is their speed, scalability, and stealth. Traditional security systems are often too slow or rigid to keep up, meaning these threats can spread quickly and without detection.

Another fast-growing cyber threat in 2025 is the real-world misuse of deepfake technology. What was once a futuristic concern is now a processing reality. Deepfakes are being used to impersonate CEOs, government officials, and even family members in real-time audio and video calls making scams feel shockingly believable. There have already been cases where employees were tricked into transferring money or sharing sensitive login credentials after receiving what seemed like a genuine call from their boss. And it does not stop there. Deepfake are also being used for blackmail, by fabricating compromising videos, and for political manipulation, through fake speeches or doctored interviews designed to mislead the public (Chesney & Citron, 2019). As this technology becomes more advanced and accessible, spotting what is fake is getting harder, leaving individuals, companies, and governments more vulnerable than ever.

At the same time, the rapid adoption of cloud computing has introduced new vulnerabilities into the cybersecurity landscape. While cloud brings undeniable advantages like flexibility, scalability, and cost-efficiency many organizations still fall short when it comes to security of their cloud environments. In 2025, multiple high-profile cyberattacks have taken advantage of simple but critical oversights, such as publicly exposed S3 buckets, leaked API keys, or poorly configured access control (ENISA, 2023). These small mistakes have led to massive data breaches, exposing sensitive customer and company information. This highlights an important truth, while the cloud is now the cornerstone of modern business operations, it also represents a major weak point if not carefully managed. The tools are powerful but without strong security practices, they can become an open door for attackers.

In 2025, ransomware groups have gone down on targeting critical sectors, with hospitals, universities, and local governments still among the most vulnerable. These institutions often operate on outdated systems and limited budgets, making it difficult to keep up with modern cybersecurity demands. These attacks go far beyond stolen data; they disrupt essential services that communicates rely on. The 2023 SickKids ransomware incident served as an early red flag, but similar breaches in 2024 and 2025 have been more devastating. In many cases, recovery has taken longer, and the damage has reached deeper affecting everything from emergency medical care to public infrastructure operations. This ongoing trend makes one thing, underfunded and overstretched sectors are increasingly seen as soft targets by cybercriminals, with consequences that are both costly and dangerous.

Looking beyond 2025, cybercrime is expected to become even more automated, evasive, and dangerously personalized. Attackers will likely use artificial intelligence not just to launch sophisticated attacks, but to fully automate the early stages scanning systems for weaknesses, profiling victims, and building adaptive attacks that evolve in real time. As our digital and physical lives become more connected through LoT devices and smart infrastructure, the stakes will rise dramatically. The fallout from cyberattacks will no longer be limited to stolen data or locked files; it could mean disrupted transportation, compromised medical devices, or widespread threats to public safety and trust. In this future, cybersecurity is not just about protecting information it is about safeguarding the systems we live by.

Strategies to Mitigate Cybercrime

As cyber threats in 2025 grow smarter, more targeted, and increasingly disruptive, the urgency for proactive, multi-layered defence has never been greater. Tackling today's cybercrime is not just a matter of deploying better tech, it requires a holistic approach that blends

strong cybersecurity infrastructure, thoughtful business practices, and robust legal frameworks. To stay ahead of evolving threats, organizations and governments alike need to invest in smarter systems, train people effectively, and adapt policies to a fast-moving digital world, This section explores key mitigation strategies across three critical layers like, one IT infrastructure the technical backbone, from system architecture to threat detection, second Business processes how workflows, staff behavior, and internal policies support cybersecurity, finally societal & legal systems broader responses including legislation, public awareness, and international cooperation.Together, these levels form the foundation for building cyber resilience not just reacting to attacks, but actively reducing their likelihood and impact.

IT infrastructure

Strong cybersecurity starts with a solid technical foundation. As threats grow more advanced, organizations need more than just basic antivirus software; they need smart, layered defences that can not only detect attacks but also stop them from spreading internally. Here are some of the key strategies:

Zero Trust Architecture (ZTA)

Zero Trust flips the old model of "trust but verify" model on its head. Instead of assuming users or devices inside the network are safe, it treats everything as a potential threat whether it is internal or external. Every access request must be verified, authenticated, and continuously monitored, no matter where it comes from. This approach helps block attackers from moving freely within a system after they have gained entry. Even if one part is compromised. Zero Trust limits the damage by preventing unauthorized lateral movement (NIST, 2020). In short, Zero Trust is about never assuming trust and always verifying it.

Endpoint Detection and Response (EDR)

Traditional antivirus just is not enough anymore. Today's threats are more advanced and stealthy, and that is where EDR solutions come in. EDR continuously monitors all endpoints laptops, mobile devices, servers, and more for unusual or suspicious behavior. When a potential threat is detected, these tools can quickly isolate and contain it, often automatically, before it has a chane to spread across the network. This kind of rapid response is critical for catching fileless, malware, ransomware, and other modern attacks that are designed to slip past outdated security tools.

Encryption & Multi-Factor Authentication (MFA)

Even if data falls into the wrong hands, encryption keeps it unreadable and useless to attackers. That is why it is essential to encrypt data both at rest when it is stored and in transit as it moves across systems and networks. To strengthen defences even further, multi-factor authentication (MFA) adds a second layer of protection beyond just a password. This could be something like fingerprints scan, a one time code sent to your phone, or a hardware token. Even if someone manages to steal a password, MFA helps block unauthorized access. Together, encryption and MFA form a powerful defence against both data theft and account compromise.

Regular Patching & Vulnerability Management

Surprisingly, many successful cyberattacks begin with something basic, an outdated or unpatched system. That is why staying on top of updates is one of the simplest and most effective ways to reduce risk. Using automated patch management tools ensures that security updates are applied promptly, without relying on manual checks. Alongside that, routine vulnerability scans help identify weak points in your software and systems before attackers do.

In short, keeping your systems up to data is not just good maintenance, it is frontline defence against preventable breaches.

Business Processes

Even the most advanced cybersecurity tools can fall short if internal processes and human behaviour are not part of the equation. That is why businesses must embed cybersecurity into their culture, not just their technology stack.

Cyber Awareness Training

Despite all the tech safeguards in place, human error remains the number one cause of data breaches. Employees often unknowingly can rely on phishing links, fall for social engineering tactics, or mishandle sensitive data. To reduce this risk, companies should invest in regular, role-specific training that goes beyond the occasional reminder. This includes:

- Phishing simulations to build awareness and test real-time decision making
- Breach response drills to ensure teams know how to act if something goes wrong.
- Ongoing education tailored to job roles, so everyone from HR to IT is equipped to spot the threats most relevant to their work.

By 2025, many organizations have embraced interactive, gamified cyber hygiene programs that keep employees engaged and up to date on the latest risks (Version, 2023) These programs do not just educate, they help build a culture where security is everyone's responsibility.

Incident Response Planning

Even with the best defenses, breaches can still happen. What matters most is how quickly and effectively an organization responds and then starts with a well-prepared incident response plan. A strong plan should be more than just a document gathering dust. It needs to be regularly updated, clearly communicated, and thoroughly tested. Key components include;

- Technical Procedures for identifying, containing, and recovering from breach.
- Communication strategies for notifying leadership, employees, customers, and when necessary regulators of the public.
- Escalation paths that define who is responsible at each stage and when to involve senior leadership or external partners.

The goal is to avoid problems when a real incident strikes. By having a clear, practiced roadmap, in place, teams can act fast, limit damages, and restore trust quickly.

Vendor & Supply Chain Risk Audits

Cyberattacks like the SolarWinds breach have made it clear, your cybersecurity is only as strong as your weakest vendor. Third-party partners can unknowingly serve as entry points for attackers especially if their systems are not properly secured. To reduce this risk, organizations must regularly access the security posture of their vendors. This means conducting audits, asking the right questions, and requiring clear cybersecurity standards written directly into contracts. By holding suppliers accountable and keeping a close eye on the digital supply chain, businesses can close gaps that cybercriminals are increasingly eager to exploit.

Cyber Insurance

While cyber insurance does not prevent attacks, it plays a vital role in helping organizations recover from the financial and operational damage they can cause. Today's policies often cover a range of incidents including data breaches, ransomware payments, legal fees, forensic investigations and business interruptions. For many companies, especially small to mid-sized ones, cyber insurance can be the difference between bouncing back and shutting down

after a major incident. However, coverage usually depends on meeting certain security standards, so it should be seen as a safety net not a substitute for strong cybersecurity practices.

Legal and Social Strategies

While strong technology and business practices are vital, they can not stand alone. To truly combat cybercrime, we need effective governance, legal accountability, and broad public engagement. Coordinated global response is essential to reduce both the frequency and the impact of digital threats. Cybercrime does not respect borders so the response can not either. Countries, institutions, and private companies must work together to share intelligence, align regular frameworks, and hold cybercriminals accountable through clear, enforceable laws. At the same time, public awareness plays a powerful role. Education campaigns, cross-border law enforcement cooperation, and stronger data protection laws all contribute to a more resilient and informed society. Cybersecurity is no longer just an IT issue, it is a legal, social and global challenge that requires collective action.

Stronger Legislation & Regulation

As of 2025, some regions have taken important steps toward stronger cybersecurity governance introducing AI-specific regulations and enforcing mandatory breach reporting laws. These policies are helping raise the bar for accountability, especially in industries handling sensitive data or emerging technologies. But to truly make an impact, these efforts need to scale globally. Harmonizing cybersecurity laws across borders and making sure they are actually enforced will help close legal loopholes and ensure that all organizations, regardless of size or location, are held to the same high standards. Strong legislation is not about punishment, it is about setting clear expectations and creating a more secure digital ecosystem of everyone.

Public Education Campaigns

One of the most effective long-term defences against cybercrime is an informed and digitally literate public. Governments, schools, and NGOs should lead ongoing education campaigns to help people spot scams, protect their personal information, and understand the real-world impact of their online actions. Special attention should be given to vulnerable groups, like seniors and young people, who are often targeted by phishing, identity theft, or online manipulation. Teaching digital safety at school, hosting community workshops, and using social media to spread awareness are all powerful ways to close the knowledge gap. Cybersecurity is not just a technical issue, it is a life skill. And empowering everyday people is key to building a safer digital society.

International Cooperation

Cybercrime does not stop at borders and neither should the response. As attacks become more global in scale complexity, international cooperation is critical to effectively investigate, prevent, and prosecute digital crimes. Treaties like the Budapest Convention and the work of organizations such as Interpol and the United Nations Office On Drugs and Crime (UNODC) play a key in making this happen. They help countries share threat intelligence, coordinate cross-border investigation, and align their definitions of cyber offences for more effective legal action (UNODC, 2022). By working together, nations can close jurisdictional gaps, build trust, and create a unified front against cybercriminal networks operating across continents.

Ethical Standards for AI & Emerging Technologies

As AI becomes a central player in both cyber defense and cybercrime, it is no longer just a technical issue, it is an ethical one. With AI tools capable of powering deepfakes, automating attacks, or making security decisions at scale, the need for clear ethical guidelines and oversight

is more urgent than ever. Governments, tech companies, and research institutions must collaborate to set standards that ensure AI is developed and used responsibly, minimizing the risk of abuse while maximizing its benefits. This includes transparency is how AI systems are trained and deployed, safeguards against bias and misuse, and frameworks for accountability. Without ethical guardrails, emerging technologies could do as much harm as good. Responsible innovation is not just smart it is essential for long term digital trust and security.

Conclusion

The evolution of cybercrime over the last forty years tells a sobering story of what once began as digital experimentation has now escalated into a global threat capable of disrupting essential services and endangering lives. What used to be limited to data theft or online scams has grown into a far more dangerous weapon, one that can cripple hospitals, paralyze governments, and erode public trust. A powerful example of this shift is the 2022 ransomware attack on Toronto's Hospital for Sick Children (SickKids). While the attackers affiliated with the LockBit group did something unusual by offering an apology and providing a decryption key, the damage had already been done. The hospital's critical systems were disrupted, delaying lab results, diagnostics, and communication in a pediatric environment where short delays can be threatening. This incident also highlighted the evolving nature of ransomware operations. Groups like LockBit operate under decentralized models, such as Ransomware as a Service (RaaS), allowing them to scale quickly and target high-impact institutions often from across borders, making them difficult to stop.

This paper has explored the evolution of cybercrime by examining key incidents that shaped the digital security landscape, the Morris Worm (1988), the Target data breach (2013), the WannaCry ransomware attack (2017), and the SolarWinds espionage campaign (2020). Each

event marked a turning point not just in the methods used by attackers, but in how society, businesses, and governments respond to cyber threats. The Morris Worm exposed the early vulnerabilities of the internet and introduced the world to the concept of large scale digital disruption. Target's breach showed how even major cooperation could be compromised through third party weaknesses. WannaCry demonstrated the real-world consequences of neglected system updates, particularly in healthcare. SolarWinds revealed just how deeply attackers can penetrate through trusted software supply chains. Together, these cases show a clear pattern as technology progresses, so do the tactics of cybercriminals often faster than our ability to defend against them. The challenge ahead lies in staying not just reactive, but proactive.

As of 2025, cybercrime has entered a new era fueled by the rise of artificial intelligence, deepfake technology and cloud based vulnerabilities. AI-renewated malware has made phishing attempts more convincing and highly personalized, increasing the likelihood of successful attacks. At the same time, deepfake are being used to impersonate executives or trusted figures in real time video and audio, enabling sophisticated social engineering and financial fraud. Cloud infrastructure, now a backbone of modern operations, has brought clear benefits in flexibility and scale, but it has also introduced new entry points for attackers, especially when systems are misconfigured. Without the funding or technical flexibility to adapt quickly to healthcare, education and local government remain prime targets for increasingly automated and damaging attacks.

To confront today's fast evolving cybercrime landscape, a holistic defense strategy is no longer optional; it is essential. On the technical side, organizations must implement modern security frameworks like Zero Trust Architecture, Endpoint Detection and Response (EDR), strong encryption, and multi factor authentication (MFA) to protect against increasingly

sophisticated threats. But technology alone is not enough. From a business perspective, companies need to embed security into everyday operations. That means ongoing awareness training, regular risk assessments, and having a well practiced incident response plane ready to go when something goes wrong. Effective cybersecurity in 2025 and beyond depends on aligning people, processes and technology.

The SickKids incident, along with the broader surge in ransomware attacks in recent years, serves as a powerful wake up call. The true cost of cybercrime is not just measured in dollars, it is measured in disruption, vulnerability, and in some cases, human lives. As cybercriminals become more sophisticated and relentless, our defence must evolve accordingly. That means building systems that are not only stronger, but also smarter, integrated, proactive, and adaptive to changing the threat landscape. By looking to the past for lessons, staying vigilant in the present , and preparing strategically for the future, we can begin to shift the balance.

References

Chesney, R., & Citron, D. (2019). *Deepfakes and the new disinformation war*. Foreign Affairs. https://www.foreignaffairs.com/articles/2019-12-10/deepfakes-and-new-disinformation-war

CBC News. (2023, January 1). *LockBit ransomware gang says it was behind SickKids cyberattack*.https://www.cbc.ca/news/canada/toronto/sickkids-cyberattack-update-1.6699979

Cybersecurity & Infrastructure Security Agency (CISA). (2023). *Understanding ransomware threats*. https://www.cisa.gov/stopransomware

ENISA. (2023). *Threat landscape for cloud computing*. https://www.enisa.europa.eu/publications/cloud-security

Europol. (2018). *WannaCry: Five years on*. https://www.europol.europa.eu/media-press/newsroom/news/wannacry-five-years-on

Europol. (2023). *Ransomware-as-a-service explained*. https://www.europol.europa.eu/media-press/newsroom/news/ransomware-as-service-explained

Federal Bureau of Investigation. (2023). *LockBit ransomware: One of the most active and*

destructive ransomware variants. https://www.fbi.gov/news/stories/lockbit-ransomware

Global News. (2023, January 5). *SickKids cyberattack: Hospital returns to "nearly normal" operations*.https://globalnews.ca/news/9385206/sickkids-hospital-cyberattack-update-2023/

Greenberg, A. (2018). *The untold story of NotPetya, the most devastating cyberattack in history*. WIRED.https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and hackers on the computer frontier*. Simon & Schuster.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2020). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.

Interpol. (2023). *Ransomware: The fastest growing cyber threat*. https://www.interpol.int/en/Crimes/Cybercrime/Ransomware

Krebs, B. (2014, February 12). *The Target breach, by the numbers*. https://krebsonsecurity.com/2014/02/target-breach-by-the-numbers/

Kumar, S., & Carley, K. M. (2022). Artificial intelligence in cyber offense and defense. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac005

Maimon, D., & Choi, K.-S. (2021). *Cybercrime and cybersecurity: Understanding the challenges*. Springer. NIST. (2020). *Zero Trust Architecture (SP 800-207)*. https://doi.org/10.6028/NIST.SP.800-207

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Spafford, E. H. (1989). The Internet worm incident. *ACM SIGCOMM Computer Communication Review, 19*(1), 24–33. https://doi.org/10.1145/723090.723093

Trend Micro. (2022). *LockBit ransomware: A deep dive*. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/lockbit-ransomware

UNODC. (2022). *Global Programme on Cybercrime*. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

Zetter, K. (2021). *How the SolarWinds attack happened*. Politico. https://www.politico.com/news/2021/02/23/solarwinds-hack-explained-470456

Appendix A

Ransomware Data Encryption Rate 2020-2025

This graph illustrated the proportion of ransomware attacks that resulted in data encryption from 2020 to 2050, offering valuable insight into how both threat tactics and defence mechanisms have evolved over time. The declining rate of successful encryption is a key takeaway. It signals not just changes in how attackers operate, but also captures two important developments for instance: An increase in attacks that were stopped before encryption occurred and a rise in cases where data was not encrypted but victims were still extorted. This trend is significant since it highlights a clear pivot in ransomware strategies and underscores the growing importance of not just backups, but comprehensive threat response and data protection practices.

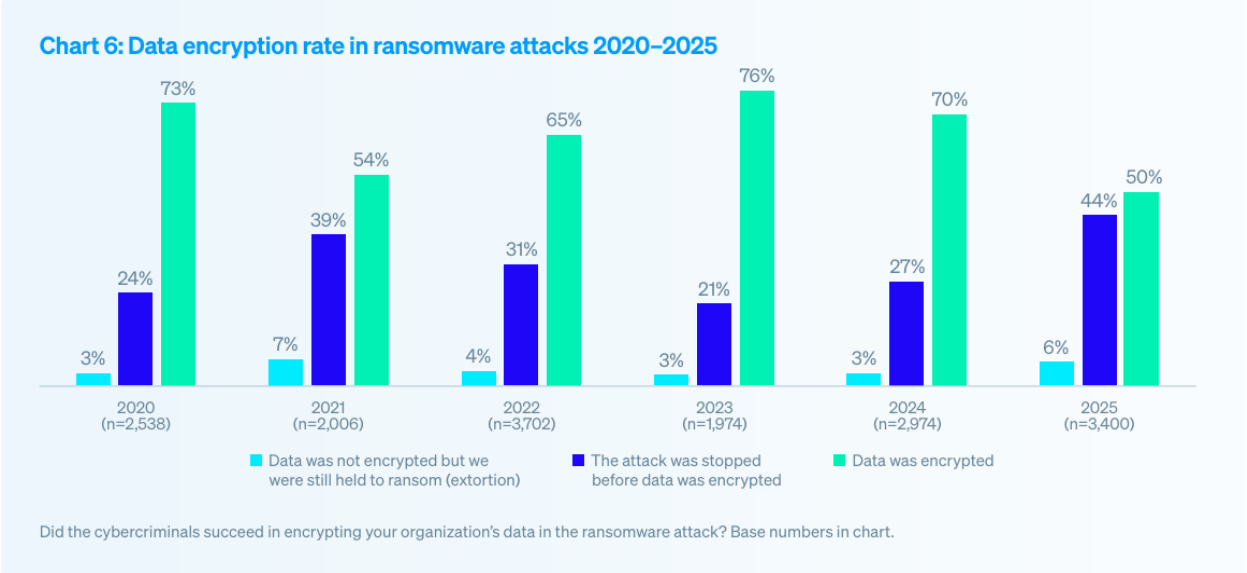

Figure 1. Percentage of ransomware attacks resulting in data encryption, 2020-2025.

Note. Adapted from *The State of Ransomware 2025 (chart 6, p.6)*, by Sophos, 2025. Copyright 2025 by Sophos Ltd.

Appendix B

Technical Root Causes of Ransomware Attacks (2023-2025)

This bar chart breaks down the technical root causes of ransomware incidents, showing the most common entry points by percentage such as exploited vulnerabilities, stolen credentials, malicious email attachments, and phishing campaigns. The data provides valuable context for understanding how ransomware operations gain access to organizations' systems. It reinforces a critical insight: many breaches begin with avoidable weaknesses like unpatched software or poor password hygiene. By visualising these causes side by side, the chart not only adds analytical depth to your section on attack vectors, but also highlights the ongoing importance of proactive defense measures, including vulnerabilities management, credential protection and employee awareness training.

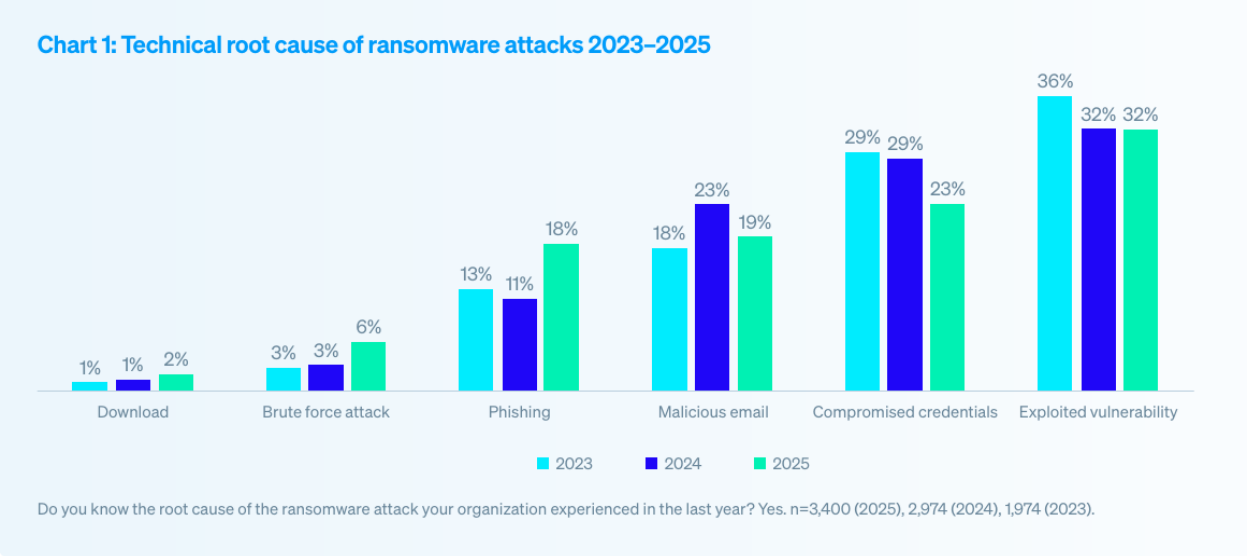

Figure 2. Technical root causes of ransomware attacks, 2023-2025

Note. Adapted from *The State Ransomware 2025 (chart 1, p.3),* by Sophos, 2025. Copyright 2025 by Sophos Ltd.

Appendix C

Ransomware Recovery Time 2022-2025

This bar graph shows the percentage of organizations that fully recovered from ransomware attacks across different time frames ranging from less than a day to up to six months tracked over recent years. The visual highlights a promoting trend that more organizations are recovering faster from ransomware incidents. This shift reflects growing investment in resilient infrastructure, better response planning, and improved backup strategies. By showcasing how recovery times have shortened over time, that chart supports your broader analysis of evolving cybersecurity practices. It also underlines the growing importance of not just preventing attacks, but building systems and process that enable swift, efficient recovery when incidents do occur.

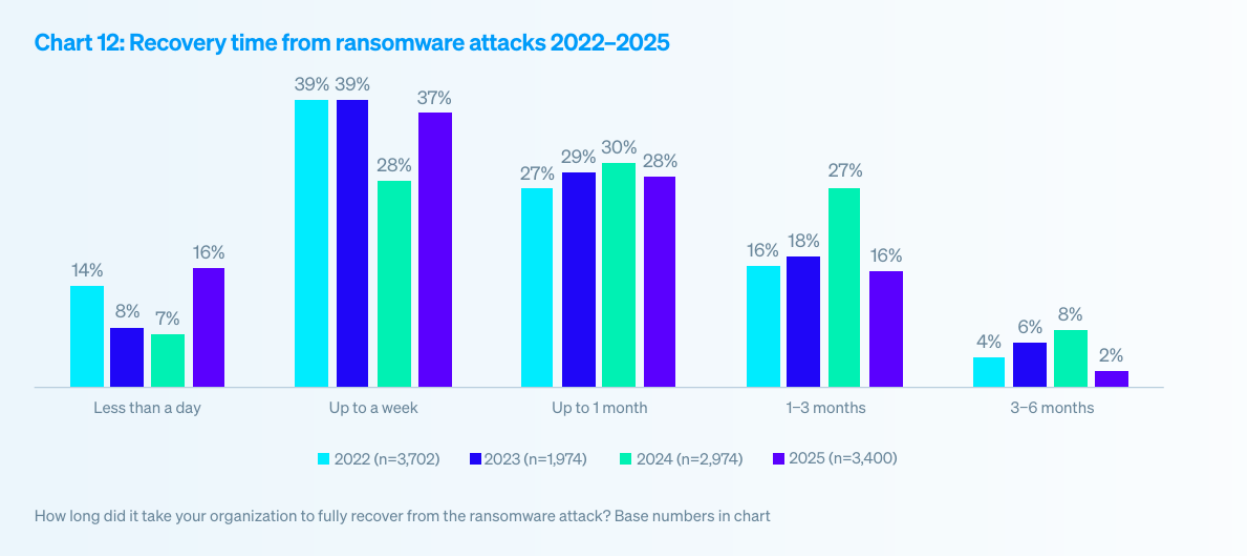

Figure 3. Recovery time following ransomware attacks, 2022-2025.

Note. Adapted from *The State of Ransomware 2025 (Chart 12, p.13)*, by Sophos, 2025, Copyright 2025 by Sophos Ltd.

Appendix D

Ransomware Infection prevalence by year 2020-2023

The figure illustrates the shifting dominance of major ransomware groups including LockBit, Conti, and REvil/Sodinokidi based on Sophos incident response cases from 2020 to 2023. The most striking insight is LockBit's clear lead in 2023, with more than double the number of cases compared to any other group. This trend signals a growing consolidation of attacks among a small number of highly organized ransomware operations. This figure supports the broader observation that ransomware ecosystems are becoming more centralized, with a few dominant players leveraging tolls like Ransomware as a Service (RaaS) to scale their reach and impact across industries.

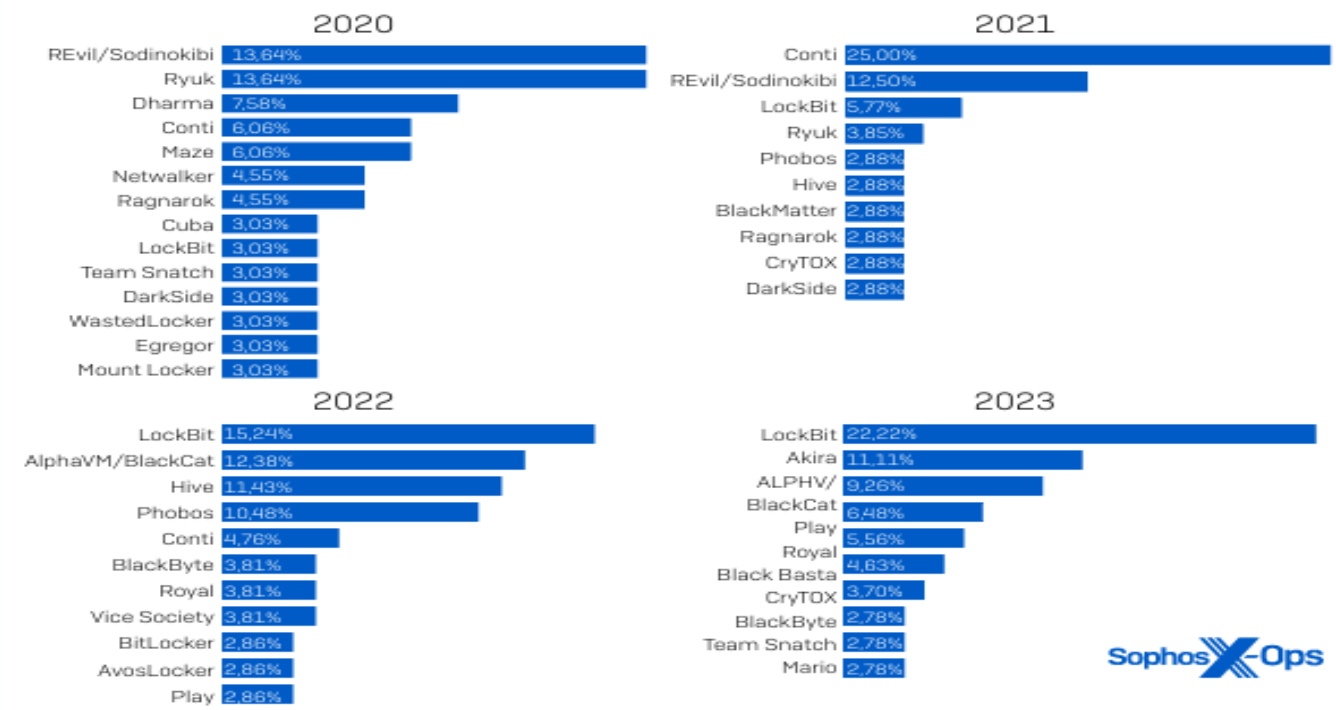

Figure 4. Ravalancensomware infection prevalence in Sophos X-Ops Incident Response cases by year, 2020-2023

Note. Adapted from Figure5, p.6, in *The Sophos Active Adversary Report for 1H 2024* by Sophos, 2024. Copyright 2024 by Sophos Ltd.