Creating a Ransomware-Resilient Business

Executive Summary: Understanding the Business Impacts of Malware and Ransomware

Malware and ransomware are two of the most pressing cyber security challenges facing businesses today. These types of attacks are designed to steal sensitive data and lock employees out of their devices. The attacker then demands that the business pay a ransom using cryptocurrency in order to restore system access or return the data.

For the amount of damage an attack can wreak, it often starts out simple. All it takes is for one employee to click the wrong link or download a malicious attachment for the malware or ransomware to encrypt devices and data across your network. These attacks can lead to significant business impacts, including:

- Business interruption due to compromised systems
- Significant remediation costs
- Loss of customer data or intellectual property
- Inability to execute payroll or pay suppliers
- Damaged brand reputation
- Fines, lawsuits, and increased regulatory scrutiny

In this white paper, we explore the business impact of malware and ransomware. By understanding the risks, you can set expectations for the rest of the company to help ensure compliance and set your IT team up for success.

RBC®

What Could Ransomware Cost You?

Costs associated with ransomware incidents in the US, Canada and Europe (USD)

$2,730,000	Average ransom demand[6]
$2,000,000	Average initial ransom demand[6]
$5,400,000	Average ransom demand for large enterprise
$70,000,000	Highest ransom demand[8]
$40,000,000	Highest ransom paid[12]
$1,850,000	Average ransom paid[13]
$207,875	Average cost of forensic engagement for large enterprise[15]
$40,719	Average cost of forensic engagement for small and midsize businesses[15]
$180	Per record cost of lost or stolen personally identifiable information[10]

Report cyber fraud to RBC.

If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

Welcome to Cyber Insecurity

No matter how big or small, every business relies on technology like their e-commerce website, email, cloud software and servers to connect, collaborate, and operate. All this technology increases efficiency, productivity, and innovation. However, it also significantly increases the risk of a cyber attack.

Every piece of internet-connected technology – from laptops, smartphones and tablets to servers, sensors, and printers – is a potential access point hackers can exploit to gain access to your network. In 2024, the average cost of a single lost or stolen customer record was $180. SMBs face an average data breach cost of roughly $3 million.[10] This makes cyber attacks one of the most pressing challenges facing your business today.

Organizational impacts of cyber attacks[1]

- Prevented employees from carrying out day-to-day work: **32%**
- Damage to reputation of organization **28%**
- Repair or recovery costs paid to suppliers **27%**
- Loss of revenue: **26%**
- Loss of customers: **26%**
- Discouraged us from carrying out future planned activity: **21%**
- Fines from regulators or authorities: **18%**
- Paid ransom payment: **17%**

Report cyber fraud to RBC. If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

The State of Cyber Attacks

Ransomware attacks increased by 44 percent globally in 2024 as attackers shifted to targeted attacks against businesses.[2] Not only are there more attacks, but they are growing more costly: losses from global cyber crime will reach $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.[3]

Here's a glimmer of good news: the proportion of Canadian businesses affected by cyber security incidents is on the decline - in 2023, about 16% of Canadian businesses were impacted, down from 18% in 2021 and 21% in 2019.[10] This decrease is likely the result of a boost in spending and training. In 2024, 55 percent of Canadian businesses made cyber security training mandatory for all employees, up from 32 percent in 2019. Further, three-quarters of Canadian organizations have increased their financial resources dedicated to IT systems management and cybersecurity and 76% have bolstered their human resources in these areas.[4]

Despite these declines this is not the time for businesses to sit back, as AI is making it easier for malicious actors to carry out attacks.

According to the 2024 CIRA Cybersecurity Survey, 7-in-10 (70 per cent) of respondents are worried about potential cyber threats from generative AI. And for good reason: the Financial Industry Regulatory Authority (FINRA) has highlighted the growing use of generative AI in creating personalized phishing emails and impersonating financial experts, a trend backed up by the FBI.[14] Further, AI-generated deepfakes - manipulated images, audio, or videos - are increasingly being used to deceive people and organizations.

The landscape of ransomware attacks has also evolved, with cybercriminals shifting from traditional data encryption methods to direct extortion tactics. In these scenarios, attackers infiltrate systems, steal sensitive data and then threaten to publicly release or sell the information unless a ransom is paid. This approach eliminates the need for encrypting data, which enables criminals to exert pressure through the threat of exposure alone.

Report cyber fraud to RBC.

If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

Understanding Malware and Ransomware

Two of the most common and damaging types of cyber attacks that businesses face are malware and ransomware:

Malware is any type of malicious program that is designed to attack and exploit a device. There are many different types of malware, such as spyware that tracks device activity, bots that use your devices to carry out attacks, and rootkits that allow a hacker to control a device. Once malware compromises a device, hackers can use it to steal data, access your financial accounts, disrupt your operations, or as a jumping-off point for attacking other parts of your network.

One specific type of malware that is often in the news is **ransomware**. This is an attack that locks access to your data and devices through encryption until you pay a ransom in exchange for the encryption key.

How Ransomware Works

STEP 1

The ransomware is downloaded onto a device by an employee clicking a malicious link or attachment. One of the most common ways ransomware is delivered is through a 'phishing' email, which pretends to be from someone a user can trust, such as a colleague or customer.

STEP 2

The ransomware program spreads throughout the device or network to look for data.

STEP 3

The ransomware program encrypts the data, making it inaccessible.

STEP 4

The program provides instructions for how to pay the ransom, usually through the use of **untraceable cryptocurrency**.

STEP 5

Once the ransom is paid, the program is supposed to provide a **decryption key to restore access**.

Report cyber fraud to RBC.

If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

The High Costs of Ransomware

Most cyber criminals are financially motivated, making ransomware an increasingly popular method of attack. After all, it's far more efficient to demand money than it is to steal data and sell it on the dark web. Victims paid roughly $1.1 billion USD in ransom in 2023, nearly doubling the $567 million paid in 2022.[5] Not only that, but the average payment increased to $2 million USD in 2023, which is a 500% increase compared to 2022.[6]

The cost of malware and ransomware extends far beyond the money lost from a hacker emptying your bank account or paying a ransom. Stolen customer data can expose you to angry customers, lost brand value, and significant fines.

Even an attack that results in no data or financial loss can still disrupt normal business operations, distract staff, and cost significant time and money dealing with investigations and remediation. In fact, it's not uncommon for the total cost of recovery to far exceed the cost of the actual breach. For example, in June 2024, a provider of IT and digital marketing solutions to the automotive industry, experienced a ransomware attack that disrupted services for thousands of car dealerships across the U.S. and Canada. While company paid a $25 million ransom, affected dealerships reported combined financial losses of approximately $944 million due to operational disruptions within the first three weeks alone.[7]

What about cyber insurance? While it can help mitigate some of the financial loss of a ransomware attack, it won't help you make up for the loss of other things such as lost intellectual property or reputational harm. In addition, it generally will not cover things like lost potential revenue or the cost to upgrade your system in the wake of an attack.

One question you'll face during a ransomware attack: to pay or not to pay? Law enforcement experts such as the FBI recommend that you don't pay the ransom, as there's no guarantee that the hacker will actually release your data.[11] Hackers are even "double extorting" victims by threatening to leak stolen data after they've been paid to give access back. If you do pay, you may be targeted for additional attacks since they know you're likely to pay up again in the future. In addition, governments increasingly sanction businesses that pay ransoms with civil and criminal penalties in order to discourage payments that will fund additional attacks.

Report cyber fraud to RBC. If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

How to Prepare for and Prevent Cyber Attacks

While the IT team works to prevent, detect and respond to attacks, business leaders and employees across the organization all have a role to play in keeping the organization safe. Here are a few best practices you can implement immediately to help prevent malware or ransomware from making it into your network in the first place.

Create regular off-site backups.

Create a process for backing up all data at a secure, off-site facility, and regularly refresh the backup with new versions of the data. This will help you quickly restore your systems should your data get trapped by a ransomware attack while avoiding paying the ransom.

Prioritize patching.

Many malware and ransomware variants exploit known vulnerabilities that software companies have already provided patches to fix. Make sure you have a process for regularly issuing and installing updates on every device on your network to eliminate known exploits.

Implement formal security policies.

Establish and enforce formal security policies across your organization so employees don't have to guess about security. Ensure employees use strong, unique passwords when logging into your system, utilize multi-factor authentication when available, and limit employee access to only the data they need to do their jobs to ensure a hacker isn't able to use their credentials to gain control.

Educate employees.

All it takes is one employee downloading a malicious file to cost your company millions. Train employees about common attack tactics so they can learn how to avoid downloading unsafe files. In addition, make sure they know who to call in IT if their computer experiences an attack. The faster IT can quarantine the device, the less likely the attack will spread across your network.

Prioritize cyber security technology investments.

There are thousands of different cyber security products available that can reduce the risk of malware and ransomware. Work with your IT team to identify weak points in your attack surface so you can strategically invest your time, money, and resources in securing the company and reducing its risk.

Who Should You Call in Case of an Incident?

For many businesses, the natural inclination is to keep an attack quiet in order to avoid negative press. In fact, only 9.6 percent of businesses report incidents to the police.[9] However, this can prevent you from getting the support you need to effectively respond while allowing the criminals to remain free to exploit the next unaware victim.

In the planning and preparation section of your incident response plan, you should include the contact information for everyone you should consider informing in the case of an incident. There are two organizations you should contact immediately in the event of an attack:

Law enforcement

Local or federal law enforcement have trained specialists who can help provide a rapid response. They can also help coordinate your efforts and share information with other governmental agencies and departments for additional assistance. Finally, they will be crucial in collecting evidence and conducting a criminal investigation so that the attackers can be brought to justice.

Financial partners

Once an attack takes place, it can be difficult to know where it's going or where it will stop. If you see unusual activity or have identified an attack, call your bank and other financial partners immediately so they can watch your accounts for fraudulent activity. RBC clients should visit the Report Fraud to RBC web page for contact information and call us immediately in the event of an attack or account compromise.

The Canadian Centre for Cyber Security

The Cyber Centre works with law enforcement, businesses and the public sector to lead the government's response to cyber security events.

Email: contact@cyber.gc.ca
Toll Free: 1.833.CYBER.88
(1.833.292.3788)

Keep in mind that not every business and every incident requires contacting all the same people. A minor attack on a small business might only warrant a call to the police and their bank, while a major attack on a healthcare facility or critical business may also require resources like federal investigators, elected leaders, and cyber security specialists.

While it may feel daunting, malware and ransomware are just one more business challenge that you'll need to manage. By working with your team and having the right plan in place, you'll be able to reduce your risk and get back to business faster in case of an attack.

RBC is here to help your business stay safe and secure. Visit rbc.com/cyber/business for more tips on how to protect your business.

SOURCES

1. CIRA, Perceptions and Attitudes of Canadian Organizations Toward Cybersecurity, August 2024.
2. Check Point Software Technologies, The State of Global Security 2025.
3. Cybersecurity Ventures, Cybercrime to Cost the World $10.5 Trillion Annually by 2025.
4. Get Cyber Safe, How Canadian Organizations are Navigating Cyber Security in 2024.
5. Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline.
6. Sophos, State of Ransomware 2024.
7. Anderson Economic Group, Dealer Losses Due to CDK Cyberattack to Reach $944 Million in First Three Weeks.
8. NetApp, Measuring the True Cost of a Ransomware Attack.
9. Public Safety Canada, Profile of Canadian Businesses Who Report Cybercrime to Police.
10. Statistics Canada.
11. FinCEN Guidance, FIN-2020-A00X, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," October 1, 2020
12. Business Insider, One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack.
13. Astra, 100+ Ransomware Attack Statistics 2025: Trends & Cost.
14. The Wall Street Journal, GenAI Increasingly Powering Scams, Wall Street Watchdog Warns.
15. 2021 Palo Alto Networks, Ransomware Threat Report.

Report cyber fraud to RBC.

If you believe you are the victim of a malware attack or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.