Ransomware Calculator

How Much Could It Cost You?

When done strategically, ransomware security doesn't have to be expensive. However, getting the green light from business leaders can be a challenge, as not all can appreciate the very real risks to the organization. Building a successful business case requires accurate data that makes an impact.

Use the guided questions below to get started with your risk assessment by calculating how much a ransomware breach could cost your organization.

Assessing the Threat

First you need to assess the likelihood that your organization will experience a ransomware attack. The grim news? If you've managed to avoid one so far, consider yourself extremely lucky. According to a recent Statista report, **68.5%** of companies experienced a ransomware attack in 2021, and Canadian officials expect them to continue to drastically increase.

There's no surefire way to predict an attack, but from historical trends, we know there are certain risk factors to be cautious of.

Industry risk factors:

Public sector (healthcare, municipalities, education, energy, manufacturing)	5 pts
Professional Services	3 pts
Supply vendor for one of the above	3 pts

Behavioural risk factors:

Hybrid or remote users	5 pts
Untrained end-users (Cyber Security Awareness Training)	5 pts

Technology risk factors:

Out of date patch management	5 pts
RDP vulnerabilities	5 pts
Use of web applications	5 pts
Use of cloud file shares	3pts

Geographic risk factors:

International organization	5 pts
Canadian organization	3 pts

Canada often ranks among the top countries affected by ransomware, with public sector organizations hit the hardest and making up half of all victims. Professional services such as finance and legal firms, are suffering attacks at an alarming rate.

A ransomware criminal's ideal target has weak security measures, remote users and a willingness to promptly pay up.

Calculate your risk review score:

15 or above	High
11-14	Moderate
3-10	Some

Calculating Potential Loss

Loss of productivity due to system downtime is a significant consequence of ransomware that often slips under the radar.

Downtime is typically tied to two things – the organization's preparedness and whether they choose to engage with the cyber criminal. A solid backup infrastructure enables the IT team to move straight to remediation and recovery, whereas negotiations and ransom payment will delay the resumption of business-critical operations.

On average, statistics show that organizations experience 22 days of downtime from a ransomware breach. However, Ricoh has observed that 7 days (40 business hours) is a more typical timeframe for small to mid-size businesses.

Productivity Loss

How many employees would be materially impacted by a network shutdown?	
What is the average cost for one employee's hour of work?	

Calculate:
1. Multiply the average cost of one hour of work by the number of employees materially impacted by network downtime.
2. Multiply your results by 40 business hours of total downtime.

Example: 50 employees at $25/hr with a downtime of 40 business hours = $50,000
Example: 200 employees at $25/hr with a downtime of 40 business hours = $200,000

Your potential productivity loss:	

Ransom Payment

Many factors go into deciding whether it's in an organization's best interest to pay the ransom:
- How much damage would be incurred if data were released (legal, reputational and client impact)
- Whether the data can be restored from backups
- Whether the organization can continue operations without it

Would your organization pay? The average ransom in Canada in 2021 was $200,000 CAD, which has stabilized as cyber criminals become better at tailoring their demands to their victims.

If your organization is likely to pay, add $200,000 to your total loss.

Your potential productivity loss:	

Remediation & Recovery

In 2021, the average cost of recovery from a Canadian ransomware incident was $2.3M CAD, which has doubled since 2020.

This figure includes ransom payment, which works out to $2.1M CAD for remediation and recovery, likely skewed by large-scale costly attacks like that against the city of Saint John. A more reliable way to calculate your organization is to use IBM's average $206 per record.

Total number of encrypted records	

Further Considerations

Forensics and Reports

Depending on the type of data affected by the ransomware breach, your organization may be obligated to run forensics and submit a report to authorities or a regulator. Costs vary greatly but are largely dependent on the number of records affected and reporting requirements of the regulator.
The cost of retaining specialized forensics averages at approximately $93,000 CAD.

Liability and fines

According to a 2021 IBM report, highly regulated organizations with compliance failures (resulting in fines, penalties and lawsuits) averaged a cost of 5.65M USD ($7.05M CAD) per breach, a **51.1% higher cost than less regulated industries**.

Highly regulated industries were defined as energy, healthcare, consumer goods, financial, technology, pharmaceuticals, communication, public sector and education.

Insurance coverage

Cyber risk insurance policies are designed to mitigate financial loss from cyber attacks such as ransomware. Businesses are well-advised to maintain comprehensive cyber insurance, however they must be aware it isn't a universal remedy. Cyber security insurance is a relatively new but rapidly growing product in Canada and not all types of risk are covered.

It also means insured parties must comply with strict security standards to meet the minimal requirements of coverage. Additionally, policies should be priced to the full, potential cost of a breach. Organizations with a higher risk profile may find insurers unwilling to provide comprehensive coverage.

How much would ransomware cost you?

It's time to tally up your total:

Risk level:	
Total $$ loss:	$

The case for ransomware prevention and mitigation

The best defence is a proactive one, with end-to-end security coverage. Consider completing a full risk profile and security assessment to identify gaps in your organization's security posture.

Implementing intelligent breach protections at every endpoint is especially important if you have remote and hybrid employees accessing systems from outside the secure office zone.

Prevention is critical but even so, new strains of ransomware are becoming smarter, faster and stealthier. Their ability to breach through endpoint protections and even bypass them altogether to directly target file shares continue to rapidly evolve.

Consider evolving your security strategy by adding ransomware mitigation alongside prevention. Solutions such as automated ransomware containment function as a second line of defence, stopping active infection in its tracks and preventing further damage with little to no disruption.

Ricoh can help. From comprehensive risk assessments to proactive security management and innovative ransomware containment solutions, we've got you covered at all times.

Contact us to discuss ransomware protection today

RICOH
imagine. change.