ThinkOn™
Where Data Thrives

Ransomware & You

The Thinker's guide to comprehensive ransomware protection

Contents

Ransomware & You

It's a data world, after all

Our world runs on data.

The more we depend on complex digital infrastructures and platforms, the more vulnerable we become.

Today's cyber attacks are fast-evolving, sophisticated, specific, and often far more costly than the ransom itself. They represent one of the biggest challenges to global digital transformation.

In fact, in a recent survey, 300 global CEOs called a lack of cybersecurity "...the single greatest threat to the global economy over the ensuing decade".[1]

And every sector is at risk.

Making headlines for all the wrong reasons

The annual cost of cybercrime is expected to jump from $8.4 trillion in 2022 to more than $23 trillion in 2027.[2]

Post-pandemic, the APAC has emerged as global ground zero for this catastrophic increase in cybercrime. Rapid digital transformation, a increasingly hybrid workforce, and the overwhelming adoption of collaboration culture throughout the region has weakened security, expanding the threat surface.

The result? In the first week of 2023, the APAC experienced the highest year-over-year increase in weekly cybercrime attacks of any region in the world.

Size doesn't matter

And if you think you're too small, too insignificant, too under-the-radar to become the next statistic – think again. Attacks on large corporations or critical infrastructure are news-makers, but that doesn't mean small and medium-sized businesses (SMB) are not at risk.

Scary stuff, right?

But this story has a hero: You.

You have the power to make sure your business doesn't make the news for all the wrong reasons.

Be the hero your data deserves.

Battling the constant evolution of cybercrime is like playing a giant game of whack-a-mole—for every advance in security technology, hacker intelligence isn't far behind.[2] It's a game you won't win by pretending the threat doesn't exist, or by convincing yourself that you're too small to be hit[3], and especially not by throwing up your hands and bowing to the "inevitable."

A winning strategy is about protecting your data and bouncing back fast if and when disaster strikes. Because, let's face it, the best defense is a good offense—it pays to be prepared. Smart organizations create and maintain robust security protocols and business continuity planning with the help of a trusted partner who can provide comprehensive, industry-leading IT backup (BaaS) and disaster recovery (DRaaS) to anticipate, combat, and quickly recover from threats.

But before we take a closer look at solutions, let's first meet the enemy.

Size doesn't matter

Small and medium-sized enterprises are just as likely to be hit by ransomware attacks as large organizations.[4]

66% 2 out of 3 SMB have suffered a ransomware attack in the last 18 months

8% Only 8% of SMB recovered their data after paying the ransom

16.2 Ransomware attacks result in an average of 16.2 days downtime

40% 40% of SMB won't survive a disaster

75% 75% of SMB don't have a business continuity plan

Ransomware by the numbers

The number of bytes of data created every day [5]

2.5 quintillion

$1 billion

Estimated annual revenue of hacker groups [10]

The cost to purchase a RaaS kit on the dark web [6]

$40 RaaS Kit

16.2 days

The average number of downtime days caused by ransomware attacks [11]

The estimated frequency of ransomware attacks on businesses in 2022 [7]

40 seconds

$88k hour

The average cost of downtime ($1,467 / minute) [12]

63% businesses

The percentage of U.S. businesses unprepared to stop a ransomware attack [8]

$20 billion

The annual cost of ransomware globally [9]

82% breaches

The percentage of breaches caused by human error [13]

What's in a name?

Malware is a portmanteau of malicious and software. It's a piece of computer code used by threat actors to block user access to a computer system until a ransom is paid.

The enemy at the gate

Cyberattacks come in two basic flavors: profit and chaos. Also known as ransomware and hacktivism.

This is ransomware

There are many types of ransomware—from encryptors to leakware—and while the mechanics may differ, the basic principle is the same: A threat actor introduces malware (see sidebar) to a system. [14] This piece of code encrypts and/or steals data on that system, blocks user access to the system itself, and often installs a backdoor to allow for future access. The malware user then contacts the victim and threatens to either destroy the data, publish it, or keep it inaccessible unless a ransom is paid. Ransomware models can involve encrypting, non-encrypting, or data-wiping (a.k.a. wiper) malware. And with so much personal data on the table, hackers don't even need to bother encrypting the data anymore: The threat of making the information public is enough to have the victim scrambling to pay up.

Evolution of an industry

Hackers monetized malware in the early 2000s with the spread of botnets. Since then, ransomware has only become more sophisticated. A successful ransomware attack depends on three things: access to the target system, and anonymous, untraceable means to both communicate with the victim and arrange payment. The technology needed for the first two has been available for decades, but it was the development of cryptocurrencies like Bitcoin, that made it possible for threat actors to receive payments anonymously from anywhere in the world and allowed the ransomware industry to really take off.

And make no mistake—it is an industry. A thriving one.

Hacker groups spent nearly thirty years developing more efficient ways to monetize malware, eventually moving away from the "spray-and-pray" email phishing model that targeted random individuals, to today's ransomware, which is well-organized and technologically sophisticated. In 2018, the number of reported ransomware attacks dropped by 20 percent, due largely to a "work smarter not harder" philosophy: Improved capabilities and greater sophistication of attacks and extortion methods allowed cybercriminals to focus on specific, high value targets—ones with deep pockets.

These increasingly complex and well-organized operations often employ other groups to provide services like asset hosting, access to victim infrastructure and even negotiations with the victim, creating a proven business model based on the SaaS model. [15]

Not the service you're looking for

Ransomware as a service (RaaS) is a business model in which "professional" hackers rent or sell malware kits. For as little as $40, criminals can purchase a bundle containing the necessary code, an encrypted communication system, and even the means to collect payments from the victim. This kind of business model allows the malware author to minimize their own risk while taking either a flat fee or earning a cut of the ransom.

Hacktivism: ransomware's radical younger sibling.

Powerful tool for change or dangerous brand of cyberterrorism? When it comes to hacktivism, it depends which side you're on.

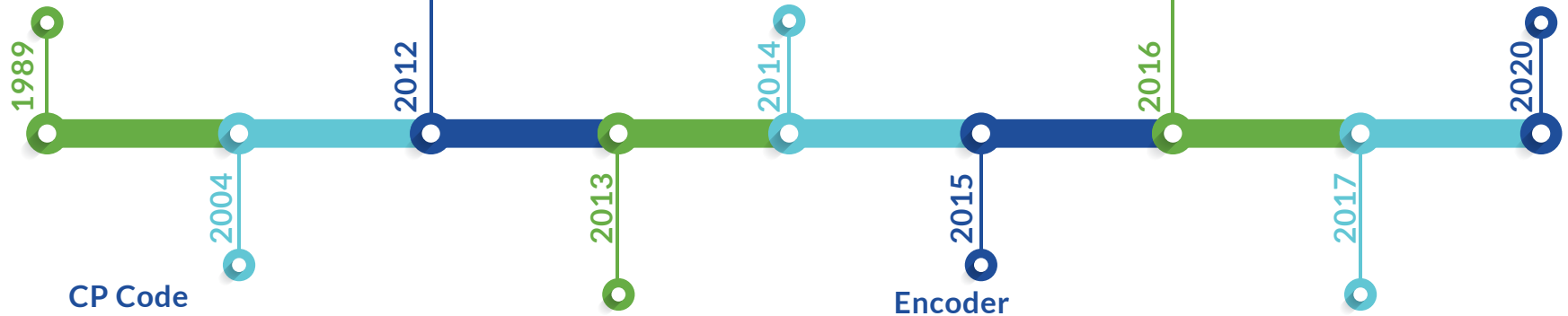
Originating from the words hack and activism, hacktivism is a kind of cyberattack directed at a government or corporate target that the attacker considers oppressive.[16] Hacktivist groups are highly organized, sophisticated operations; they may be state-sponsored or act independently, and individual groups often work together to achieve their objectives—through data theft, distributed denial of service (DDoS), website tampering, and/or social media manipulation.

As ransomware sophistication has evolved so has hacktivism, making headlines for its part in climate emergency activism, freedom of information movements, the Arab Spring, both sides of the Russia-Ukraine war, and the Black Lives Matter protests.

Whether the goal is to stir conflict or promote positive social change, one thing is certain, groups like WikiLeaks, Anonymous, and LulzSec have become headline makers—and they are here to stay.[17]

When the COVID-19 pandemic forced businesses and public sector organizations to move employees and services online, there was an immediate surge in ransomware attacks. By June 2020, the U.S. Federal Bureau of Investigation had seen a 75 percent spike in cybercrimes, and one year into the pandemic the U.K. reported that more than 34.5 million had been lost to coronavirus scams targeting the National Health Service, vaccine producers, and supply chains. Recent threats against health care infrastructure, food production and distribution, and retail sectors highlight our data-dependent vulnerability to ransomware attacks and the urgent need for mitigation.[18]

A ransomware timeline



AIDS Trojan

- Spread via Floppy disk
- Used Symmetric Cryptography
- Monitored Boot Time count

CP Code

- Spread via Phishing Emails
- Used Asymmetric Cryptography
- Encrypted 'My Documents' Directory

Reveton

- Spread via outdated plugins
- Used Symmetric Cryptography
- Used an unstoppable DLL

Cryptolocker

- Spread via Phishing Emails
- Used Asymmetric Cryptography
- Encrypted 'My Documents' Directory

Sypeng

- Spread via Email attachments
- Used Asymmetric Cryptography
- Payloads added themselves to the registry entries via bypassing.

Encoder

- Spread via a backdoor in Magento CMS
- Used Symmetric Cryptography
- Payload replicated itself in every directory with SUID permissions.

KeRanger

- Spread via a flaw in BitTorrent
- Used Asymmetric Cryptography
- Bypassed Gatekeeper to infect the system with .RTF

WannaCry

- Spread via a flaw in SMB server
- Used Asymmetric Cryptography
- Used a backdoor called DoublePulsar to lock registry

Netwalker

- Spread via COVID-19 advisory emails.
- Used Asymmetric Cryptography
- Used a VB script for UAC bypassing.

The cost of ransomware

As we've already seen, the global cost of cybercrime is expected to grow to an almost unimaginable $23 trillion by 2027. [19]

And while every sector is at risk, it's the ones we depend on the most – retail, health care, manufacturing, supply chains and infrastructure – that make the juiciest targets for threat actors. Let's meet a few of the biggest hits to make the news in recent years.

Food for thought

If pandemic-related empty shelves at the grocery store have taught us anything, it's the vulnerability of our food supply chains – from field to table and all points in between. And threat actors understand this only too well.

In 2021, threat actors hit Australia-based JBS Foods, the world's largest meat processor, and demanded an $11M ransom, resulting in a five-day shutdown of the company's entire operation.

For a critical operation of this size, shutting down operations and suspending shipments, even for a relatively short time, has follow-on effects that are devastating to the consumer and costly to both the company and the economy.

Commenting after the attack, Lani Refiti, Regional Director for cybersecurity specialists, Claroty, warned that future attacks on the food supply chain are inevitable. "It's not a matter of 'if' a major attack will happen [...] it's a matter of 'when'". [20]

Shopping trip

Retail stores depend on data for in-store and online shopping, and their systems are bursting with personal customer and employee details – information that can be sold on by hackers for use in targeted phishing or business email attacks.

"Retailers are not immune to cyber attacks, which have increased in many industry sectors [...] internationally. This issue is a top priority for everyone," said Michelle Wasylyshen, spokesperson for the Retail Council of Canada.

Bruce Winder, retail analyst and author, adds, "While the public has empathy for the retailer, if the problem doesn't get fixed quickly, public sentiment can start to sour. They'll start to ask why the company didn't prepare for something like this." [21,22]

Beyond the ransom

Ransomware costs go far beyond the ransom itself – from downtime and system repair to legal fees, insurance, and damage to brand reputation.

The answer?

Invest in a plan that both protects and allows for a fast recovery.

Health care ... hacked

When cyber criminals target the health care sector, it can be difficult to spot an incursion – harder still to determine what data was compromised – and the impact to patient care and privacy can be devastating. According to Australia's cyber security agency, the ACSC, cyber attacks on that country's health care sector increased by more than 84% between 2019 and 2020.[23]

And the hits keep coming, from the 2022 attack on Medlab, one of the country's largest diagnostic labs, that exposed the personal data of more than 223,000 patients[24], to the 2023 attack on St. Vincent's Health, Australia's largest not-for-profit health and aged care provider – who subsequently came under fire for their silence about the breach.[25]

Patients and employees in the health care sector trust their service providers to keep their sensitive personal data safe. When that doesn't happen, the fallout can be widespread and severe.

All is not well

On October 13, 2022, a group of hackers, allegedly linked to the Russian ransomware group REvil, accessed the Medibank network[26], putting Australia's largest private health care insurance provider in the centre of one of the worst cyberattacks in the country's history.

Armed with a stolen Medibank username and password from a third-party IT service provider, the hackers took advantage of a misconfigured firewall, stealing the medical records of 9.7 million Medibank customers and threatening to release those records to the dark web unless the company paid a $9.7M ransom[27].

But Medibank refused to pay, citing concerns – shared by IT experts and the Australian government – that there was only a slim chance the data would actually be returned, and that paying the ransom would encourage the criminals to directly extort customers[28].

A bleak prognosis

The aftermath was not pretty. The alleged culprit was eventually caught, but not before the entire 5GB dataset was dumped onto the dark web. Medibank is now potentially facing several class-action lawsuits brought by the affected customers.

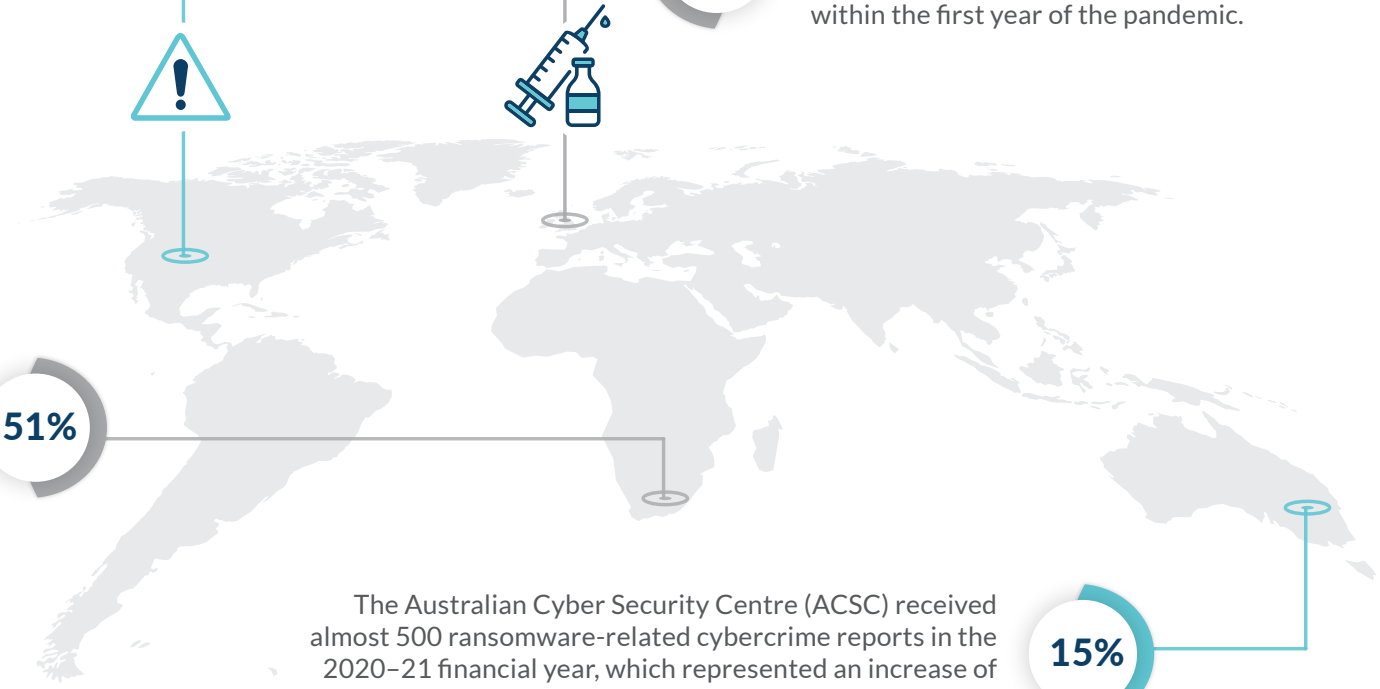
A pandemic of opportunity

Between March and June 2020, the FBI reported a 75% uptick in cybercrime in the U.S.

75%

34.5 MILLION

Meanwhile, in the U.K., it's estimated that $34.5 million was lost to coronavirus scams targeting the National Health Service, vaccine producers, and supply chains within the first year of the pandemic.



51% of South African organizations were hit with ransomware in 2021.

51%

The Australian Cyber Security Centre (ACSC) received almost 500 ransomware-related cybercrime reports in the 2020–21 financial year, which represented an increase of nearly 15% over the previous financial year.

15%

Don’t pay the ransom

You’ve been hit by a ransomware attack.
The easiest option is to pay up, right?

Not so much.

Companies meet ransom demands because they think it’s cheaper and easier than any alternative scenario, but recent studies show that paying the ransom only makes the problem worse.[29]

In fact, the National Cyber Security Centre in the U.K. and both the Federal Bureau of Investigation and the Department of Homeland Security in the U.S. recommend not paying the ransom because,

- paying the ransom increases overall cost of the attack,
- there’s no guarantee you’ll get your data back even if you pay the ransom,
- ransoms funds 6–10 new attacks, and
- by paying, you make yourself a bigger target for future attacks.

And there are wider considerations, too. In the recent attack on Canadian bookseller Indigo (see page 10), the company, in consultation with Canadian and U.S. law enforcement, refused to pay the ransom, citing concerns that the money would “… end up in the hands of terrorists or others on sanctions lists.”

Prevention and cure

The true cost of a cyberattack goes far beyond the ransom alone and can be difficult to tally. The estimated global annual cost of reported ransomware attacks is $20 billion. But hacker revenue is only $1 billion.

You can guess where the difference lies.

The immediate cost to repair systems and restore data is only the tip of a very expensive iceberg. In the aftermath of an attack, companies face costs related to downtime, stop-gaps, public relations to repair brand reputation and customer confidence, insurance deductibles, lawyers’ fees, impact mitigation for lost/compromised information…. Not to mention that loss of corporate records may trigger regulatory or reputational issues that can lead to bankruptcy.

Why add ransom to that list?

Studies estimate that ransom demands can be as much as a whopping 67 percent of the total cost of a ransomware attack. Instead of paying out, companies are better off investing in cybersecurity and data backup actions that can reduce the risk of a successful attack, and—in case an attack happens—crisis response and incident leadership.

“Houston, we have a problem…”

Actually, we have several.

Cyberattacks are becoming more sophisticated and larger in scope. Attackers are more innovative, organized, and well-resourced.

Companies tend to either put their heads in the sand and hope they won’t be hit, or they cross their fingers that “good enough is good enough. Companies must take it seriously at all levels of the organisation—from cybersecurity awareness training for staff, to installing multilayered defence, DNS hardened firewalls, multifactor authentication, and access control.

Not enough focus or money is being put into systems and technologies to keep up with the volume of attacks—and not enough allocated specifically to cybersecurity. According to Byron Holland, chief executive officer of the Canadian Internet Registration Authority, “In the digital world, people don’t see the impact, so there is little support for more resources.”

Legacy software and hardware prevents/impedes adoption of new technologies.

Critical infrastructure like power generation and industrial plants use air-gapping (see sidebar) to protect their systems, but the introduction of portable data devices can create vulnerabilities. Hackers can gain physical access through third-party service vendors, contract services, and staff agencies.

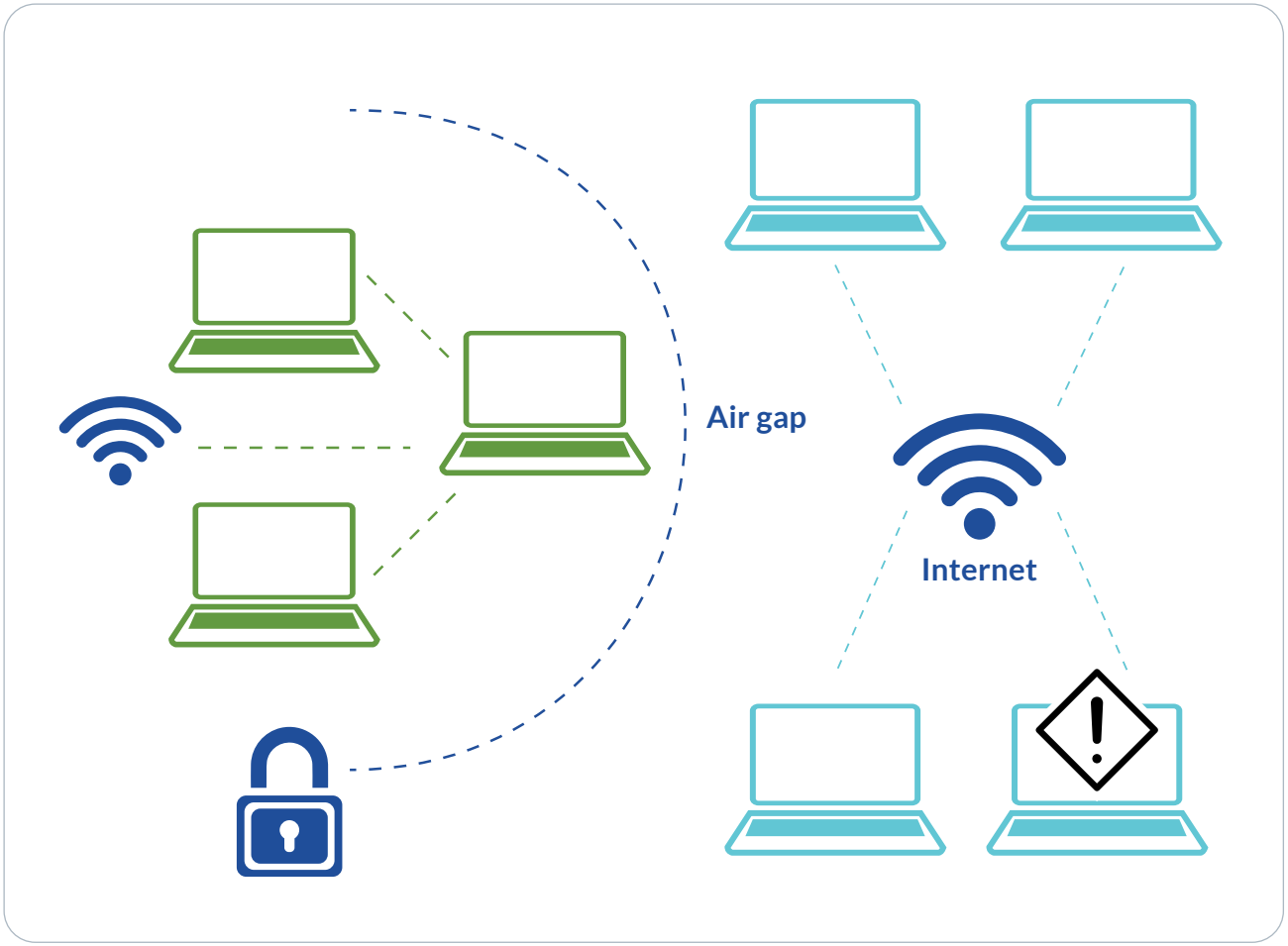
Experts recommend a proactive, head-on approach.

“This is the new normal and will continue to happen,” says Charles Finlay, executive director of Rogers Cybersecure Catalyst at Toronto Metropolitan University. “There’s an increase in the severity of the attacks which is why it’s so important we all take the steps we can to prevent [them]. And when they do happen, we must be prepared to handle them.”

Retail industry analyst Lisa Hutcheson agrees: “Every company needs a cybersecurity plan. It’s not a matter of if, it’s a matter of when.”

Air gapped network :

If they can't get at your data, they can't hold it hostage



Air gapping is the best way to ensure your backup data is protected.

Yes, data immutability is great, but it also means your data is "read only," and THAT means your data might be read and exfiltrated as part of a ransomware attack.

With air-gapped solutions, your data is completely inaccessible to external threats.

Top 5 ransomware defense strategies

1 Have a plan

When it comes to cybersecurity, too many organizations either put their heads in the sand and hope they don't get hit or take the "good-enough-is-good-enough" approach. With this kind of thinking, they'd have to be pretty lucky to avoid being hit by some kind of cyber threat. Smart businesses don't rely on luck. Instead, they build a comprehensive cybersecurity and disaster plan and make sure that every level of the organization is involved.

2 Invest at every level

Invest in the most up-to-date advice, technology, and training that you can afford—at every level of your organization.

Practice good IT hygiene—train employees to recognize and isolate risks and hazards. Phishing emails are the vector for 66 percent of ransomware infections and in 33 percent of infection cases, the cause was insufficient user security training.

Use multifactor authentication and strong, unique login credentials. Use security software that takes a multilayered approach.

3 Stay Current

Keep your systems up to date. Practice good patch management and keep operating systems current.

4 Comprehensive approach

Take a comprehensive approach to backup and recovery with BaaS + DRaaS. "If companies have backed up their data, they are less vulnerable to the pressure to pay a ransom," according to Michelle Wasylyshen, spokesperson for Retail Council of Canada.[31] And while data backup is critical, it's only part of the story. Companies need to be able to bounce back as quickly and as accurately as possible. Companies that integrate Backup as a Service (BaaS) with Disaster Recovery as a Service (DRaaS) stand the best chance of making a full recovery.

5 Ask the experts

Because, let's face it, when it comes to the evolving and fast paced world of IT, sometimes you just don't know what you don't know. And that's okay! Partner with an industry expert and free up your time to focus on doing what you do best: running your business.

Dynamic Duo—BaaS and DRaaS

Once upon a time, when it came to data you just backed everything up. Archived project data? Back it up. That rush order that just came in? Back it up.

But today's IT innovation gives you the power to go beyond the old one-size-fits-all solution and create a business continuity plan tailored to fit your business and your data.

How?

Know your data

Different types of data can be protected in different ways. Understanding how your business uses data and knowing your tolerance for data loss and recovery time (RPO/RTO) helps you optimize the economic and strategic benefits of a comprehensive recovery plan.

Understand the options

When it comes to mission critical applications—e-commerce, system state, security—DRaaS offerings keep data geographically isolated and constantly up to date, providing fast recovery with minimal data and infrastructure loss. All that power can come with a higher price tag, so it's best used for critical data.

But what about the rest of your data? The long-term storage and low-risk infrastructure with RPO/RTO of days or weeks instead of minutes or seconds?

That's where BaaS shines, with lower-cost offerings that focus on long-term storage for non-mission critical or archival data.

Individually, BaaS and DRaaS offerings each focus on minimizing data loss, but a "one-size-fits-all" never actually fits anyone that well. Together, BaaS and DRaaS optimize every aspect of your recovery.

It's a bird! It's a plane! It's…ThinkOn?!

ThinkOn is your trusted partner for ransomware protection—the superhero your data deserves.

From critical and high change rate workloads to protected offsite backup and remote restore, when it comes to preventing data loss and meeting compliance and regulatory requirements, ThinkOn does it all—at whatever speed you need.

Our team of ThinkOn Thinkers are data experts, supported by the latest in cutting-edge solutions and features to meet all your data protection and compliance needs.

- Industry leading DRaaS with Veeam and Data Protect with Veeam (BaaS) and RansomGuard, and Compass Data Protect for M365—simple and secure data protection and recovery solutions powered by Veeam
- We're backup software agnostic. We use Veeam and other industry leading disaster recovery solutions. With our solutions, you don't have to change of pick just one.
- Fully S3-compatible Object Storage in all regions, with the latest security features, including Object Lock (immutability) and legal hold, that is up to 50 percent less expensive than the hyperscalers' comparable solution
- With ThinkOn's global data center locations, you choose where to replicate your data
- No-nonsense billing with no fine print, no escalating cloud allocation use charges, and no hidden fees

Learn more at https://thinkon.com/draas-baas/

When disaster strikes

According to the U.S. Federal Emergency Management Agency (FEMA)[32]

40% 40% of businesses that experience a major disaster never return to the marketplace

70% 70% fail within 3 years

90% 90% of smaller companies fail within one year of a disaster if they can't resume operations within 5 days[33]

The big picture

Backup and disaster recovery solutions protect your data—and your business—from more than ransomware. Physical disaster or human error can mean application failure, hardware failure, infrastructure damage, and systems outages.

No matter the disaster, having a comprehensive business continuity plan that includes data backup and disaster recovery will save the day—and your business—helping you to get your business back up and running as quickly as possible. [34]

Spoiler alert!

So, what's next?

There are no advanced movie screenings when it comes to knowing what the next cyberthreat will be, but experts are constantly assessing both the IT and ransomware industries to better understand potential security gaps in evolving technologies.

The Internet of Things

The Internet of Things (IoT) is the network of physical objects equipped with sensors that "talk" to each other. From smart home and personal devices—think fitness trackers and smart thermostats—to industrial applications like location tracking and predictive maintenance.

It is one of the most significant technologies of the 21st century, made possible by low-cost computing, the cloud, big data, analytics, and mobile technologies. But many IoT devices present vulnerabilities that are easily overlooked. They're often poorly configured, with default settings and weak passwords, leaving security gaps that threat actors can walk right through.

Third-party software

Businesses generally assume thatthe third-party software they're running—from accounting to logistics management—is secure. After all, you'd think that someone else in the digital supply chain would have checked, right? Unfortunately, that's not always the case and threat actors know it, exploiting weaknesses to create devastating outcomes.

Operational systems

The Colonial pipeline attack highlights the vulnerability of operational systems. An attacker enters an unsegmented network through an innocuous back door in a piece of accounting software or an unsecured IoT monitoring device and the next thing the company knows, their entire operational network is in jeopardy.

No matter what comes next for technology, when it comes to ransomware, the best approach is a proactive one. Businesses must understand the risks and plan for them, building a cybersecurity culture at every level of their organization.

Post-credits scene

Can there be a "happily ever after" when it comes to ransomware?

Absolutely.

Make the right kind of headlines.

Stay ahead of ransomware's evolving threats with the help of a team of trusted experts who understand your business and your data protection needs.

Visit the ThinkOn website today and find out how our team of data-obsessed experts can help your organization build and implement a comprehensive cybersecurity strategy.

Be the action movie superstar your data deserves.

We're here to help! Reach out to our team of Thinkers and let's ransomware-proof your future—today!

ThinkOn™
Where Data Thrives

ThinkOn, Inc. is a cloud solution provider with a global data center footprint—consider us your dedicated department of data-obsessed experts who will protect your data like it's our own, making it more resilient, secure, actionable, and searchable.

North America 884 888 4465
U.K. +44 2039 667963

sales@thinkon.com

www.ThinkOn.com

Resources

[1] TechTarget. Colonial Pipeline hack explained: Everything you need to know.
[2] https://www.researchgate.net/figure/Evolution-of-Ransomware-70_fig7_341719300
[3] Government Technology. Small Businesses Are a Vital Part of Community Resiliency but Often Overlook Vulnerabilities.
[4] Comparitech. 14 Shocking data loss and disaster recovery statistics.
[5] Rivery. Big Data Statistics: How Much Data Is There in the World?
[6] Crowdstrike. Ransomware as a Service (RAAS) Explained. How it Works & Examples.
[7] Comparitech. 14 Shocking data loss and disaster recovery statistics.
[8, 9, 10] Cloudwards. Ransomware Statistics, Trends and Facts for 2023 and Beyond.
[11, 12, 13] Comparitech. 14 Shocking data loss and disaster recovery statistics.
[14] Malwarebytes. All about ransomware attacks.
[15] Fortinet. Key Findings from the 2H2022 FortiGuard Labs Threat Report.
[16] Check Point Research. The New Era of Hacktivism—State-Mobilized Hacktivism Proliferates to the West and Beyond.
[17] Cyber Talk. 5 hacktivism examples: Most famous and devastating cases.
[18] Cointelegraph. Cybercrime Up 75% During COVID-19, Congressional Hearing Details.
[19] IT World Canada. "Management, lack of money blamed for poor cybersecurity at Canadian hospitals."
[20] MSN Tech Radar. Fruit shortages could be on the way following Dole ransomware attack.
[21] Toronto Star. "Indigo website still down and company likely losing 'millions' after cybersecurity attack last week."
[22] Sophos. The State of Ransomware in Retail 2021.
[23] Toronto Star. "Indigo website still down and company likely losing 'millions' after cybersecurity attack last week."
[24] Newswire. Indigo Reports FY22 Full Year Results - Indigo delivers $1.06 billion in sales and returns to profitability
[25] Financial Post. "What's next for Indigo one month after cyberattack?"
[26] Toronto Star. "Indigo website still down and company likely losing 'millions' after cybersecurity attack last week."
[27] Financial Post. "'Inappropriate': Indigo refuses to pay ransom in cyberattack possibly linked to Russians."
[28] IT World Canada. "Updated: Indigo admits cyberattack was ransomware, employee data accessed."
[29] IT Pro. Paying ransomware gangs could fund up to ten additional attacks.
[30] National Institute of Standards and Technology Computer Security Resource Center.
[31] Toronto Star. "Indigo website still down and company likely losing 'millions' after cybersecurity attack last week."
[32] www.fema.gov
[33] Forbes. "Why Disaster Recovery Is No Longer Optional For Today's Businesses"
[34] InvenioIT. What's the difference between disaster recovery plan and business continuity plan?

ThinkOn™
Where Data Thrives

North America 884 888 4465
U.K. +44 2039 667963
sales@thinkon.com

www.ThinkOn.com