RESEARCH BY

CIO ASSOCIATION OF CANADA

CIOCAN-CISO Division

Blueprint: The Engine Behind Ransomware

SUPPORTED BY

CALIAN®

Confidence. Engineered.

Foreward

As CIO of a global organization, I am acutely aware of how quickly the threat landscape is evolving. Today, anyone can buy ransomware-as-a-service for less than $100 a month. Artificial intelligence tools, such as ChatGPT, make it easy to create convincing emails that can expose an organization to breaches and will make it easier for bad actors to code and create new ransomware. It's also more profitable than ever with broader use of cryptocurrencies, which make ransomware payments harder to trace. This white paper, based on discussions among a prominent group of Canadian CIOs, myself included, outlines some of the most effective ways to combat ransomware.

Preparation is Key

Many organizations simply aren't prepared—from a people, process, or technology perspective. Preparation involves everything from having the right technology in place to having the right processes so that when an incident happens you already have well-rehearsed playbooks in place.

You don't want to be figuring out how to leave a building for the first time when it's on fire. Similarly, with cyber events it's incredibly important to be prepared by building plans ahead of time. If part of your infrastructure is impacted by ransomware, what's your next step to recover?

People and Processes

Minimizing the attack surface is one important way to reduce risk by limiting the ways for cyber criminals to enter your enterprise. Often, threat actors are breaching networks remotely, from somewhere across the globe. So, a big part of prevention is reducing your attack surface by minimizing what you need to access remotely.

But no matter what technology and processes you have in place, people will always be your biggest vulnerability. Most attacks exploit employees because they already have access to the network. Phishing emails are a common tool used by attackers, because people often aren't trained to know what to look for. They click a safe-looking link, and quickly become the point of intrusion.

The rising threat of ransomware underscores the need for companies to prepare as if they are already under attack (because whether they know it, they likely are). I invite you to read this white paper to learn more about how to protect your organization.

The Right Technology

There are lots of technology solutions that can help protect your organization. Part of the reason that cyber criminals target smaller businesses, or sometimes even hospitals, is because they know that these organizations traditionally haven't invested enough in keeping up with global trends.

And while most organizations have some form of backups, threat actors are becoming increasingly sophisticated and finding ways to even encrypt backups that aren't air-gapped (physically or digitally isolated). Staying up to date means not just keeping up with software patching, but also having robust endpoint detection and response (EDR) software. Some businesses think that they can't afford to keep up with cyber trends. In reality, they can't afford not to if they want to stay in business. Cyber insurance—if you can afford it and get it—can be a stopgap, but you wouldn't leave your car unlocked just because you have car insurance, would you?

Lacking cyber expertise in your company? Not only does Calian invest heavily into its own cyber programs but we also deliver those services externally for companies worldwide. Our customers trust us when they can't fail!

Calian is pleased to support the production of this white paper with the CIO Association of Canada. We hope you will find useful.

Michael Muldner
CIO, Calian

Introduction

A national retailer's ability to sell via e-commerce is brought to a halt, and its customers are unable to have their loyalty program points updated. A copper mining company must shut down one of its mills. A municipal police force discovers a local business's IT systems may have been compromised by a foreign entity.

These are just three examples of ransomware attacks that have been publicly reported in Canada within the past six months at the time this report was written. According to research published last year, there were more than 140 Canadian organizations that suffered a ransomware attack in 2021. The Canadian Centre for Cyber Security, meanwhile, has found that about half of ransomware attacks between January and June of 2021 were targeting critical infrastructure providers.

While chief information security officers (CISOs) have been monitoring and mitigating ransomware threats for many years, the increased volume and sophistication of the attacks requires a deeper analysis. It also calls for cross-industry collaboration among executive peers who can share knowledge and help support one another in their efforts to safeguard their organizations, data, and people.

In that spirit, the CIO Association of Canada's CISO Community Division held a private virtual gathering in February 2023. Their facilitated discussion provided an opportunity to reflect on the evolving nature of ransomware attacks, the biggest areas of potential risk and, perhaps most importantly, the ways in which organizations can respond and defend themselves.

While the comments in this white paper will remain anonymous, they represent the insights of highly experienced cybersecurity leaders and are offered in a spirit of education and professional development.

The economics of ransomware: A brief history (and where it's heading)

Where the effort required to develop and deploy a ransomware attack would once have required considerable expertise, CISO Community members noted that advancements in technology have lowered the barrier considerably. This includes the emergence of ransomware-as-a-service offerings that can be leveraged for less than $100/month, in some cases.

Many governments are still struggling to keep pace with the threat, which means there is plenty of financial incentive for cybercriminals to target their victims.

One CISO Community member in our conversation also noted how ransomware attacks have expanded in terms of the degree in which victims are extorted.

Initially, for instance, cybercriminals would use ransomware to gain a foothold in a network, and then encrypt an organization's sensitive data so it would be unavailable until the ransom was paid.

Next came double extortion, where bad actors would not only steal the data but threaten to leak it on the Internet. This, of course, could further damage an organization's reputation and even threaten the personal safety of employees and customers.

Triple extortion may be worst of all, where data compromised via ransomware could be used to disrupt an organization's business partners and the wider supply chain. Using compromised data, for example, cybercriminals could tamper with the routes used to transport goods or prevent the ability to process payments with suppliers. The economics of ransomware therefore goes beyond the impact on an organization but threatens an entire ecosystem.

"It's given rise to a whole new workforce," one CISO Community member said. "Look at ransomware negotiators. That role and title didn't exist a few years ago. Now we have specialists in that domain, so I don't see the threat of ransomware slowing down anytime soon."

CISO Community members also noted how ransomware attacks are not only being targeted at organizations with strong defences and resources, but those that may be underfunded or less prepared to safeguard their systems. This includes healthcare or medical organizations, where the impact of a ransomware attack can have truly life-or-death consequences.

"It's given rise to a whole new workforce," one CISO Community member said. "Look at ransomware negotiators. That role and title didn't exist a few years ago. Now we have specialists in that domain, so I don't see the threat of ransomware slowing down anytime soon."

Where ransomware sits on the spectrum of malware profitability

Cybercriminals may not always perform a formal return-on-investment (ROI) calculation when they're planning an attack, but the risk of being caught and brought to justice requires that the ends justify their means. In other words, compared with more traditional malware such as adware, bots, trojans and worms, is ransomware really worth it?

One CISO Community member likened ransomware attacks to car thefts. Just as it's relatively easy to break open a window and hot-wire your way to starting the ignition, ransomware attacks can be carried out with relative ease.

On the other hand, the escalation of ransomware demands could also indicate a desperation to maximize the financial payout of an attack, another member suggested. After all, awareness of ransomware is increasing, attack surfaces are getting smaller and (at least in some cases), controls are getting better. This could lead to a "tightening market" for ransomware attackers.

"Why are they taking on more risk to get to these higher levels of extortion? It's likely because profitability is decreasing," the CISO Community member said. "They're having to find new ways to leverage that single foothold when they gain access to your systems and to monetize them."

"Why are they taking on more risk to get to these higher levels of extortion? It's likely because profitability is decreasing,"

The financial motivation behind ransomware, and new underground business models

The catalysts for a ransomware attack aren't limited to greed. In some cases, activists might want to disrupt the operations of an organization or a group of organizations to make a point. Others might deploy ransomware for political purposes. For a number of those in our CISO Community discussion, however, ransomware appears to be a tool purpose-built to support the objectives of organized crime.

Rather than running casinos behind the scenes or selling drugs, for example, ransomware could be a relatively easier way to generate revenue for those operating an underground business model.

Rather than running casinos behind the scenes or selling drugs, for example, ransomware could be a relatively easier way to generate revenue for those operating an underground business model.

Regardless of who is behind ransomware attacks, the financial motivation may has become stronger in part due to the way technology is transforming the kinds of currencies we use, and the payment systems that manage digital transactions.

"The rise of cryptocurrencies like Bitcoin make a lot of these transactions untraceable," said one CISO community member. "That has become a primary motivator for attacks because it means the money that changes hands can be hidden. Nobody can detect where it's going."

This could be a short-term advantage, another member argued. As crypto exchanges strive for legitimacy and overcome negative perceptions among certain segments of the public, it will behoove them to make sure they aren't primarily thought about as a mechanism to support ransomware.

"At some point, if you want to convert it into cash, that ransom money is very much traceable," they said. "I think we're going to start seeing more and more cases where the platforms that are used to convert crypto participate with authorities to crack down on this kind of thing, because ultimately, that's the only real way to stop it."

In the meantime, though, CISO Community members pointed out that the financial motivation may also be fuelled by the current state of software within many organizations. Major vulnerabilities continue to crop up in some of the most popular applications and operating systems on a regular basis. Cybercriminals are quick to exploit them.

IT departments have long struggled to maintain consistent patch management programs to stay ahead of bugs and vulnerabilities, particularly as more employees work remotely or with mobile computing devices. That leaves an open door for ransomware attackers who stay on the alert. The risk is even be worse among Canada's many small and medium-sized businesses that lack sufficient IT resources.

Added to this is the consequence of the increasing number of high-profile cybersecurity incidents where loose ends were not properly tied up, another member said.

"Everyone knows or realizes that all you need is to collect a list of usernames and passwords that have been lifted from other breaches and you start targeting them," they said.

Finally, it's important to recognize that the data compromised in a ransomware attack may have more intrinsic value than personally identifiable information or credit card numbers, another member said. Rogue actors may be planning some of their attacks with this in mind.

A good example would be getting information about the financial performance of a publicly traded company before its quarterly results are announced. These types of secrets could be highly lucrative and spawn another underground business model based on insider trading.

"It may be worth more than the ransom itself to sell it to different organizations," the CISO Community member said.

To pay or not to pay: Calculating the cost of a ransomware response

If you believe in the old business adage that time is money, a prolonged ransomware attack must be terrifying. The longer you wait to try and get your lost data back, the more time that gives customers to take their business elsewhere, and for financial repercussions to outstrip any ability to recover.

CISO Community members agreed that the decision on whether to pay and when, will vary from one organization to another. A key best practice, however, is to determine your response plan prior to facing an attack.

"My number one consideration is, 'how long can we afford to be down?'" one said. "Some businesses can manage to be down for an hour. Others could be fine for two weeks. Everybody's got their own thresholds, but those conversations about what's acceptable really must happen in advance."

"The rise of cryptocurrencies like Bitcoin make a lot of these transactions untraceable," said one CISO community member. "That has become a primary motivator for attacks because it means the money that changes hands can be hidden.

For other kinds of organizations – such as those in the public sector – paying ransom is a non-starter. Instead, the costs that equate to the ransom might be allocated to doing whatever it takes to get data back and services up and running again. This could make such organizations less attractive to ransomware, another member argued, given that rogue actors will realize such tactics will get them nowhere.

Blanket policies aside, CISOs also need to consider individual users and how they might respond in an emergency. One community member referenced a ransomware attack at a postsecondary institution. While the university had chosen not to pay the ransom, a doctoral fellow who feared losing valuable research data made the Bitcoin payment himself.

This speaks to the need for a deeper investment in education and training around an organization's ransomware policy, the member continued. "The ransomware demands went up on screens all across the campus," they said. "It's pretty hard to control that."

Part of the cost calculations may not be related to the short-term operational damage to an organization, but whether the data in question was truly critical and whether it was properly backed up elsewhere. This is often not the case among small and medium-sized businesses, whose data would likely be impossible to restore if the ransom goes unpaid.

Evaluating your backup and recovery processes could therefore be another step following the development of ransomware policies. The consequences of a payment decision undoubtedly have ripple effects that go well beyond the organization targeted, though.

"We know that people pay," another member said. "Maybe we've gone too far, where too many people just pay the ransom, which is now going to make it harder for those that actually need to deal with a one-off situation."

There are also real questions around whether some organizations can realistically afford to pay ransoms that vary widely in terms of the amounts demanded. If a payment is made, the same bad actors might target the organization a second time, seeing it as low-hanging fruit. Further incidents could also come from other attackers who conclude the organization's defences are weak.

As another CISO community member added, payment also doesn't guarantee you'll get your data back. If you do, there may be spillover effects from an attack that don't become evident until much later.

"Even though you're paying for the key to decrypt your data, you still don't know if your data has actually left your premises," they said. "You don't know if the data has been replicated. You don't know how that's going to affect your business down the road."

Theoretically, this is where the concept of cyber-insurance could play a helpful role, but many of those in the CISO Community virtual discussion cited challenges and frustrations with getting the assistance or coverage they need.

"I've actually heard a couple of high-profile cases where a company got hit with ransomware, they put in a claim to their insurance company and the insurance company failed to pay," a member said. "In one case they ended up having to sue the insurance provider."

Some insurance providers are eschewing the responsibility for ransomware entirely, another member said.

"Our latest cyber insurance quote actually excluded ransomware. They won't cover it," they said. "It's at the point now where they're seeing it as too high of a risk."

Part of the problem could be that some ransomware attacks aren't linked to organized crime but foreign entities that are acting out of geopolitical considerations. This could make the full scope of risk difficult to evaluate.

"My number one consideration is, 'how long can we afford to be down?'"

"Maybe we've gone too far, where too many people just pay the ransom, which is now going to make it harder for those that actually need to deal with a one-off situation."

"We just renewed our insurance and they do ask a lot more detailed questions in terms of the cybersecurity controls that we've got in place," another CISO Community member said. "They've told me that they're not going to pay for any nation state-based attacks."

All this means that the number of hoops CISOs must jump through to get insurance may have them questioning whether it's worth it.

"They're either jacking up the premiums to a point where people go 'This isn't worth it,' or they start asking the house insurance equivalent of 'So how many smoke detectors do you have?'" a member said. "And if you make a claim, the first thing they're going to ask is what is your evidence that you were doing periodic backups?"

All this seemed to underscore to the CISO Community members that it was up to them to help their organizations be in the best position to come back from a ransomware attack – or better yet, to avoid one altogether.

The impact of emerging technologies on the ransomware economy

Innovation is the lifeblood of progress in business, and organizations continue to count on breakthrough technologies to help them achieve their most ambitious goals. The trouble is that cybercriminals are often well aware of emerging innovations too, and just as eager to harness them to improve the way they penetrate network defences to compromise applications and data.

The CISO Community members explored two of these technologies in detail to consider how they might be used in ransomware attacks. The first was quantum computing, where work is being done to use subatomic particles to overtake the capabilities of classical PCs and servers by an order of magnitude. While quantum computing could be highly beneficial in areas such as drug discovery and financial modelling, IT security leaders are concerned about where it might be misused.

"Everything that we know from an encryption standpoint is going to get blown out of the water," one member said.

Not only might quantum computing make encryption even tougher to break following a ransomware attack, members added, but it could be used first by nation state actors who have closer ties to the researchers working on the technology. Another CISO Community member wondered if quantum encryption could make ransomware more "competitive" by shifting the power of to attack to a limited few with the ability to leverage it.

The full development of quantum computers is still years away, but other technologies, like generative artificial intelligence (AI) are maturing at a rapid pace. This includes the recent interest in Open AI's ChatGPT, which uses language learning models to offer users a simple way to ask questions and get highly detailed answers in seconds.

ChatGPT is already raising questions about how organizations might create content for marketing and sales purposes, but CISO Community members recognized it as a possible new weapon in cybercriminals' arsenals.

Early on, for instance, one member said it was possible to use a prompt like "Write me a spear phishing e-mail," and ChatGPT could easily oblige. The technology has since been improved to guard against those kinds of actions, the member added, but bad actors could still probably find workarounds. It could be as simple as asking ChatGPT to assist with writing an email about a lost password that will look authentic and genuine.

"What actually scares me is how good spear phishing could become in the future," another member said. "I still rely on the fact that those messages are not quite crafted the right way compared to a legitimate e-mail that comes in. I think things like ChatGPT

"Everything that we know from an encryption standpoint is going to get blown out of the water," one member said.

Early on, for instance, one member said it was possible to use a prompt like "Write me a spear phishing e-mail," and ChatGPT could easily oblige.

are going to make them a lot harder to detect, and I don't want to build a team of people who sit there and have to ask themselves, 'Is this a phishing email or not?'"

It's possible, of course, that IT security teams will benefit from emerging technologies like quantum computing and generative AI to strengthen their own data encryption models, or to detect bogus e-mails. This, however, will require organizational support to prevent them from playing catchup with cybercriminals.

"It's almost like a cat and mouse game," one member said. "Unfortunately, I think it's those on the offensive side who might leverage some of these technologies sooner."

Conclusion

Ransomware is an IT security issue that can't possibly be solved during a single discussion, even with the most experienced cybersecurity professionals available. The CIOCAN CISO Community session was proof, however, that there is value in having peers provide their current perspectives and identify some ways forward.

To summarize key takeaways, a few of the best practices to combat ransomware include:

- Assess the degree of organizational vulnerability to ransomware based on the rise in attacks, the ease in launching attacks, and your organization's current safeguards, controls, and access privileges.
- Augment any existing incident response plans to determine how your organization should act immediately following the discovery of ransomware. This should include whether the organization would ever consider payment, and who has authority to make that decision.
- Confirm the availability of coverage for ransomware from insurance providers and evaluate what kind of preparedness or security best practices you'll need to demonstrate to obtain it.
- Calculate the true cost of a ransomware attack – the financial fallout from being offline for a prolonged period, the resources needed to get data back and what it will take to recover lost revenue, customer trust and more.
- Take a critical look at emerging technologies like quantum computing and generative AI that goes beyond business benefits. Consider the advantages they might offer to ransomware attackers. Bolster your organizational defences accordingly.

Ransomware is a challenging cyber threat, but there is strength in working together as professionals. Learn more about CIOCAN's CISO Community.

"What actually scares me is how good spear phishing could become in the future,"

Thank you

Our thanks to the panel of experts who contributed their knowledge and expertise to this paper. The panel included the following:

Ashroff Khan, Vice President, Information Technology, NORR
Bill Dunnion, Senior Director, Physical & Cyber Security, Calian Group
Dianna Pieper, Director of IT, Independent
Doug Howell, Vice President, Technology, PRIMED Medical Products Inc.
Edward Pereira, CEO & vCISO Practice Leader, Carmel Info-Risk Consulting Group
Jasbir Kooner, Director, IT - BRM and Cybersecurity, Englobe Corp
Karl Galbraith, CISO, Galbraith & Associates Inc.
Martin Kyle, Chief Information Security Officer, Payments Canada
Matti Pearce, VP, Information Security, Risk, and Compliance, Absolute Software Corporation
Michael Muldner, CIO, Calian Group
Omid Hamed, vCISO, Retired
Rob Milman, Manager, Infrastructure and Security, UPEI
Sonny Sarai, Director, Information Security, Pattison Food Group
Taylor Mammel, CISO, BC Liquor Distribution Branch