KPMG

Fraudcast: stories of tricks & treachery

Episode 7: To pay or not to pay: the Ransomware question

Jazz Clemente

Hello everyone and welcome to the KPMG Fraudcast, where we unravel fraud cases in the news to uncover what happened and explore lessons learned. My name is Jazz Clemente.

Frédéric LeBlond

And I'm Frédéric LeBlond.

Jazz Clemente

We are both Senior Consultants within the KPMG in Canada's Forensic practice.

Frédéric LeBlond

The stories we will cover in this series are true events, but the names have been changed to aliases for the privacy of everyone involved. Although KPMG was not involved in these cases, we often work on cases similar to the ones of public knowledge we discuss.

Jazz Clemente

In this episode, we will be sharing stories detailing how events unfold when a group of skilled individuals hold sensitive company information hostage through the use of ransomware.

First, we will be discussing how a township in Ontario spent over $1.3 million to investigate and manage a cybersecurity incident, which saw files and servers encrypted in an attack involving the notorious ransomware, LockBit 3.0. On top of that expense, the town also paid a ransom of nearly $300,000 to obtain decryption keys, based on the recommendation of a third-party firm the town retained, to assist it through the incident.

Frédéric LeBlond

Wow so they actually paid the ransom. I didn't expect that.

Jazz Clemente

It must have been a hard decision to make.

The ransomware attack first came known to the town's IT staff as they were conducting a routine system backup. Upon discovery, staff quickly disconnected all servers which helped prevent further systems from being impacted. Because of quick actions of the IT team, the ransomware did not fully encrypt all the town's systems. None of the town's critical services were impacted. Two external firms were brought in. One serving as the town's technical lead and forensic auditor and the other acting as an incident response director. It was initially noted that the dark web portal for LockBit claimed that at least 67 gigabytes worth of data had been stolen from the town, including confidential data and financial documents. The town had until a week to pay a ransom, or the data would be published.

Frédéric LeBlond

So first they steal your data and make you pay to get it back, and you don't even know for sure that they'll honor that promise and then they blackmail you to get you again? That's too much.

Jazz Clemente

Agreed. This is a tactic known as double extortion. It's not clear how much had been originally sought by those involved in the attack. Ultimately, the town opted to retain a third-party negotiator to hash out a ransom payment in exchange for the decryptor keys to unlock the data. In the end, a ransom of $200,000 US dollars in Bitcoin or about $290,000 Canadian dollars was paid, the report says. According to the town's mayor, this was a hard decision to make, but it was the recommendation of the experts that were hired. He noted how there is no step-by-step guide as to how to deal with each circumstance because every circumstance is different.

Frédéric LeBlond

I think I understand this take. Looking at it from a different angle surely you have to ask yourself how much the data is worth to you as an organization. Perhaps $290,000 is a small cost compared to that of building everything back from scratch. I get it. I hope it was the right decision, in the end.

Jazz Clemente

The external firm hired undertook a design and rebuild of a new IT network for the town. The town has followed the guidelines and recommendations provided by the two firms and has engaged a third party to monitor the systems on an ongoing basis. It's not clear whether the town was targeted. Most ransomware attacks are done at random via malicious links and phishing emails, compromised credentials or unpatched vulnerabilities on internet-facing networks. Details about the attack itself remain under wraps, including how LockBit got into the town’s network, how many files were taken and whether any included sensitive personal data of staff or local residents were included.

Frédéric LeBlond

Jazz, I'm really curious, can you explain to us what LockBit actually is?

Jazz Clemente

Sure. LockBit is both a cyber-attack group and a malicious software used to carry out criminal attacks. LockBit, as a group, operates as a ransomware-as-a-service business, where teams develop malware that is licensed to affiliate networks, which then use it to carry out attacks, according to the director of innovation and policy at one of Canada's universities. Per the website of a well-known security software company, LockBit malware infiltrates its targets networks through unpatched vulnerabilities, insider access and zero-day exploits.

Frédéric LeBlond

What are zero-day exploits?

Jazz Clemente

They are flaws in the software discovered before the company which created it realizes the problem, giving them zero days to fix it. LockBit is then able to establish control of a victim’s system, collect network information, and steal or encrypt data. LockBit attacks typically use a double extortion tactic. First, they encourage victims to pay to regain access to their encrypted files. Then they ask the victims to pay again to prevent their stolen data from being posted publicly.

Frédéric LeBlond

This sounds pretty horrible. How prolific is LockBit actually?

Jazz Clemente

LockBit has made over $100 million in ransom demands and extracted tens of millions of dollars in payments from victims, according to a court document filed in one of the US states against a suspected LockBit member. LockBit emerged as early as January 2020, and members have since executed at least 1000 attacks against victims around the world.

Frédéric LeBlond

Do we know who is behind LockBit?

Jazz Clemente

It's a difficult task to find out who is behind LockBit as they operate in such secrecy. LockBit members could be located anywhere in the world. Two of the largest victims of LockBit in Canada would be a hospital and a bookstore, which would lead us to our next stories.

A hospital says it did not use the free decryptor offered by LockBit and has not paid ransom after a ransomware attack by the group.

Frédéric LeBlond

What a power move!

Jazz Clemente

The cyber-attack delayed lab and imaging results knocked out phone lines and shut down the staff payroll system of the hospital. They operated under a code gray, hospital code for system failure, in response to the cyber-attack. At the time of this report, the hospital says that about 80% of its priority systems are back after a ransomware attack affected its operations. According to their President and CEO, the cyber-attack was dealt with relatively quickly, with minimal disruptions to patients and families. LockBit, one of the world's most active and destructive ransomware groups, issued a brief apology and offered the hospital a free decryptor to unlock its data. This move, according to cybersecurity experts, is rare if not unprecedented for the infamous group. In the group statement, LockBit claimed to have blocked a partner responsible for the attack and offered the hospital a free decryptor to unlock its data.

Even if the hospital decided to use a LockBit decryptor, experts say the hospital still faces a number of hurdles. Ransomware groups are good at scrambling files, but not at unscrambling them, according to a research scientist of a cybersecurity firm. Healthcare organizations who use a ransomware groups decryptor recover on average about two thirds of their files per a survey of hundreds of organizations. The complex work of decryption is also left to the organization itself. For the hospital, there's also the issue of LockBit's partner. The LockBit statement says the partner who hit the hospital is no longer part of its program, but it's unclear whether the partner still holds any files that may have been stolen. The hospital says there is no evidence to date that personal information was compromised. LockBit's apology appears to be a way of managing its image as some partners might see the attack on a hospital as a step too far.

Frédéric LeBlond

Okay. I know this whole idea of a cybercriminal issuing an apology kind of sounds a little bit weird, but I do have a theory on this though as to why they even care about their image in the first place. I mean, I could be wrong, but I feel like LockBit might be one of those groups that believe they operate from a moral high ground, perhaps targeting groups they find flaws in, but I think they realize that indirectly harming our most vulnerable is definitely crossing a line and no one like cyber criminals. But I can imagine how much more involved people might get and stopping them should they keep crossing these lines. It's not about making sure they look good; it's about minimizing backlash. Nice to see they have some sense of ethics.

Jazz Clemente

Next, we have the story of how a Canadian bookstore was affected by an attack involving LockBit. The said Canadian bookstore would not agree to payment demands from an online group claiming affiliation with ransomware site LockBit because of the risk of terrorist financing.

Frédéric LeBlond

Again, what a power move. It definitely shows what their values are. On top of that, the risk of terrorist financing is very real here. Like you mentioned previously Jazz, LockBit is a ransomware as a service. That means they have customers. I don't know about you, but terrorist organizations are definitely top of my list as to who I think would request those services to fill their pockets. There's also the possibility that they're just claiming that affiliation for clout. It's not something we haven't seen before. It could help LockBit appear more threatening than they truly are.

Jazz Clemente

The hacker group threatened to post all stolen information publicly and posted a countdown timer on multiple versions of the LockBit dark web forum. After the deadline passed, the LockBit forum said that data had been released. However, both the news and an independent security analyst could not find actual data available to access. According to a privacy advocate and cybersecurity analyst, this does not mean that there's any less risk for Canadians affected by the data breach. It definitely doesn't mean the data won't be released in the future. Some employee data was stolen in the ransomware attack, the bookstore now says. Multiple current and former workers are worried about what happens if information such as their emails, home addresses, social insurance numbers and bank account details are made public. The bookstore has offered some current and former employees a credit protection service for two years. They said they will continue to address any concerns that may arise.

The bookstore has previously said that it didn't know the identity of the group behind the attack that stole the information. When the bookstore was hit by the cyber-attack, its website went offline entirely, and the chain's physical stores were also unable to process credit, debit or gift card transactions. Physical stores were back up after the following weekend. The website was back to taking some purchases shortly after. Being affected by a ransomware attack is truly a devastating situation to be in. Each scenario is unique and there is truly no all-encompassing guidebook to address the attacks. Having prevention measures would be key along with fast detection and response, if needed.

Jazz Clemente

Joining us for this episode as a guest is Paul Sammut, Partner with over 22 years of experience in IT and information security, providing security consultancy and assurance for clients across a range of sectors including technology, financial services, telecoms, consumer markets and non-profit organizations. Paul leads the KPMG Regions East cybersecurity team in Canada and has been in Ottawa since 2018 after seven years with KPMG in the UK. Paul is also a global lead on ISO 27001, the international standard for information security management.

Paul Sammut

Hi Jazz. Thanks for the intro and it's great to be here.

Jazz Clemente

For our first question, what should be the initial response once you discovered that your company has fallen victim to a ransomware attack?

Paul Sammut

Well, I think often the most immediate reaction we see at organizations is one of kind of shock, panic and disbelief that their own organization has been targeted. Those early hours of discovery are often the most critical time when a ransomware attack does happen. For people listening to this podcast now, and those that haven't been hit by ransomware, then there's some steps that people can take to make them better prepared.

Firstly, having an incident response retainer in place, which means that you have experts on call 24/7 who can respond within an hour, will make a huge difference. If you think of your organization being hit by ransomware, being able to pick up the phone to somebody who's dealt with these kind of situations before, regularly, and they're able to come in, access your systems and verify whether the attacker is actually still on your systems, they can help you through the whole process and that makes such a big difference in these times of panic and extreme scenario.

They can also help liaise with a breach coach, so that's a lawyer who has experience in ransom negotiations. Secondly, if you go into this situation, having practiced your response through something like a tabletop exercise, or TTX as we call them, this would mean that people on your crisis management team know their roles and you've already understood how long it takes to recover your backups and things like how you'll deal with your internal communications, but also how you would deal with external communications if your company appears in the media, for example. Having this kind of exercise very much like you would do with a fire drill, it just puts you in a much better position to be able to deal with such an event and actually help mitigate and reduce the potential impact of such an event like a ransomware attack.

Jazz Clemente

Are there any sectors or types of companies more likely to be targeted or susceptible to a ransomware attack?

Paul Sammut

What we we're seeing is that attackers are targeting less mature organizations, ones that have made less of an investment in cybersecurity and in their technology just because purely they're easier targets. Microsoft actually brought out their digital defense report last month, in October 2023, and one of the statistics in there was that 70% of organizations that encountered human operated ransomware had fewer than 500 employees. These were obviously generally small to medium size organizations and if you think about it, it's much easier for an attacker to target an organization of that size that maybe has one or two people doing security in it as opposed to a bank which may have 100 or 200 employees helping to protect the organization.

I think certainly within the last year where I work in Ontario, the two of the most targeted sectors we've seen have been manufacturing. Typically, these are smaller organizations, and they only have a few people responsible for IT security, and they're also reliant on those systems to be able to continue their manufacturing processes. Something like a ransomware attack can have a devastating impact and result in lost weeks of production and cause major disruption. That's definitely one of the sectors we've seen being hit, partly because they're generally less mature in their technology. Unfortunately, the second is care and hospitals and Jazz, you mentioned some examples earlier, we've seen a number of high-profile examples of a ransomware attack, which can have devastating effects on a hospital, which can result in emergency departments being closed, surgery appointments being canceled, and wards being closed due to the ransomware attack. A number of hospitals have been hit and it makes the media because of the amount of disruption and the importance of these services that they're providing, being impacted in such a way can impact people's daily lives very severely.

Jazz Clemente

Is it a good idea to pay the attackers the ransom, in order to access your systems or decrypt data and files if you're attacked with ransomware?

Paul Sammut

Well, this is the million-dollar question or sometimes multimillion dollar question and when I present at conferences and seminars, it's often one of the first questions we get asked, whether you should pay the ransom. But there's a number of ethical questions around that too, and considerations. Generally, if you're paying the ransom, you are perpetuating the ransomware business model. If no one ever paid a ransom as a result of a ransomware attack, then the attackers would quickly stop doing it, but you also don't know where the money is going. It may be used to fund further organized crime, further ransomware attacks, things such as human trafficking or terrorism. So that's a real consideration if you're going to pay half a million dollars or a million dollars to cyber criminals. However, it may come down to a business decision cost versus risk versus benefit.

If you think in the case of a hospital, it's a potential life and death scenario of keeping services and operations running. What it's important to do now is to discuss it in advance as an organization, with your executive management team and board and really capture and understand who's going to be responsible for authorizing a decision to pay a ransom, what internal approvals would you need and do you have a general policy in terms of like a no pay policy, for example. But also, other considerations are in terms of whether paying the ransom and getting the decryption keys to get your data back, whether that actually works. Generally, there's a belief that you get your data back, otherwise why would anyone pay the ransom? However, we have seen some worst-case scenarios where organizations have paid the ransom and still not gotten their data back and then had to do a full rebuild of their environment and that's really a situation you don't want to risk being in.

Jazz Clemente

What can companies do to avoid being a victim to a ransomware attack?

Paul Sammut

That's a great question. Often it comes down to what we say are good cyber hygiene practices, which can at least reduce the likelihood of being hit by a ransomware attack, but then if you do get hit, it can mitigate the impacts. One of the most basic things is patching your systems. Keeping your computer systems servers up to date. Anything that isn't up to date is potentially exploitable by an attacker to gain further access. We've seen cases where organizations have the vast majority of their systems up to date, but there's one server they forgot to patch, or it was delayed in being patched and that's the one way in for an attacker to gain access to their network and unleash their ransomware.

Secondly, invest in active monitoring. Whether that's through your own IT team or using a service provider who can monitor your systems for suspicious activity, potential signs of compromise because what we typically see in ransomware attacks is that the attacker gains access to the environment and then does reconnaissance, learns about the network, the way the business operates and actually sits and waits for the best time to deploy the ransomware to cause maximum disruption and panic. If your organization is proactively monitoring for suspicious behavior, then you have the best chance of detecting the attacker and potentially even detect them before they have the chance to deploy the ransomware, which would be the ideal scenario.

Three more to consider. Regular penetration testing of systems, letting an external service provider to test your systems, look for ways that your systems could be exploited or compromised, especially your external facing ones, VPN service for example are often ways that an attacker can gain access to your network and environment, it's important to test these. Carry out phishing testing, often the way an attacker gains access is a very targeted, specific phishing email to one of your employees, making them click on the link and provide their credentials, for example. By carrying out kind of actual testing on your employees, ideally on a monthly basis, they become more practiced in looking out for phishing because they don't want to fall foul of your own testing that you're doing. This makes them more generally aware to look out for potential phishing emails when they do come in and it really improves awareness.

Finally, run a tabletop exercise. As I mentioned earlier, this can really reduce the impact of an attack and make your people much better prepared. We all run fire drills in case a fire happens, but you could argue that being hit by a ransomware attack is actually more likely nowadays than experiencing a fire. This is something that organizations really should be preparing for because it could have a devastating impact on your business.

Jazz Clemente

For my last question, given the threat of ransomware attacks and thinking of privacy requirements and regulations, is there anything organizations should be aware of right now?

Paul Sammut

Certainly, within Canada, the big thing to be aware of is Act 25, which has come out of Quebec and effectively came into law in the last kind of month or so. This has a general principle of transparency in relation to the way an organization looks after their customer's information, so their personal information. If anybody's heard of GDPR, which was the EU general data protection regulation, it very much aligns to that. It provides much more protection for us as consumers, but it's important for businesses to then ensure they comply with the Act, and they are protecting their customer's data in the same way that that complies with the legislation. One of the key principles is if a person consents to share their personal information with you as an organization, they may consent to a specific purpose and it's down to you as an organization to ensure that consent is managed in terms of how that data will be used and communicated and possibly shared with third parties.

Organizations need to be very careful about the consumer data that they hold, obviously for people within Quebec, what they use it for and what consent was given. They also need to be aware that that consent can be withdrawn by consumers who no longer want you as an organization to hold their personal data. Having defined practices in place is really key. With Act 25, we expect to see potentially very large fines on organizations that don't comply with this and are found to be misusing their customer's data. This is really not something you want to ignore and it's really important to be proactive now that it is the law within Quebec, we expect to see other provinces in Canada follow suit as well. It's really important to be taking proactive action.

Jazz Clemente

Thank you so much for your time and for all that valuable information, Paul.

Paul Sammut

Thanks Jazz, it was great to be here.

Frédéric LeBlond

Each episode we'd like to leave you with a little something to help increase fraud awareness. Here's Jazz with our fraud scheme of the week - Ransomware.

Jazz Clemente

Ransomware continues to make headlines and is seen on the news more these days. It's definitely scary and stressful to have all of your files and data locked up until you make a payment. Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. It would typically be classified as a different form of malware than a virus. The earliest variance of ransomware demanded payments to be sent via snail mail. Today, ransomware authors demand that payments be sent by a cryptocurrency or credit cards. Attackers target individuals, businesses and organizations of all kinds. Some ransomware authors even sell the service to other criminals, which is known as ransomware as a service.

Frédéric LeBlond

How can we best manage this?

Jazz Clemente

The best way to avoid being exposed to ransomware or malware in general, as a computer user is to be cautious. Always be careful about what you download and click on. Other tips to protect yourself include keeping operating systems, software and applications current and up to date, making sure antivirus and anti-malware solutions are set up to update automatically and scan regularly, backing up data regularly and double checking that those backups were completed. Securing your backups and creating a continuity plan in case your business or organization is the victim of a ransomware attack.

Frédéric LeBlond

KPMG Forensic professionals transform how clients identify, mitigate and respond to risk, saving time and money. We help individuals and organizations stay on top of fraud and we would love to help you too. On behalf of the whole KPMG in Canada Forensic team, thank you very much for tuning into this episode of the KPMG Fraudcast.

Jazz Clemente

And we hope you join us again next time.