RANSOMWARE AND ITS SPAWNS

Posted on November 29, 2017

Categories: Insights, Publications

Introduction

The Risk - Cyber-attacks are considered one of the most serious risks your organisation faces and ransomware and its variants are a currently favoured variation (as evidenced by the recent "*WannaCry*" cyber-attack). Ransomware involves accessing your system, encrypting all or an important portion of your data and then offering to give you the encryption key for the payment of a modest amount, usually in the form of a crypto currency such as bitcoin. Spawns of ransomware like *NotPetya* disguised as ransomware are even more insidious as there is no way to recover the data back even if the ransom is paid. Both of these are discussed in this paper.

In addition to the risk of not receiving the key once the payment is made, your organisation faces the risk of others similarly exploring your system's vulnerabilities. Your officers and board should be concerned that a ransom attack may be like the canary in the coal mine; an early warning of dangers that might lie ahead. If a later more serious cyber-attack takes place, what kind of exposure might the officers and the board face if they just paid the ransom and did nothing more?

So far the authorities have not required that intrusions and ransoms be reported or held that payments of ransom constitute money laundering. If that changes, ransom attacks will take on a whole different level of risk.

WannaCry

In the recent "*WannaCry*" global attack, a ransomware variant compromised hundreds of thousands of computers in a matter of hours, resulting in the crippling of vast networks. The attack was likely introduced into the victims' networks via traditional malware vectors: phishing e-mails with infected attachments/links and/or exploiting vulnerabilities in outdated browser/plug-ins when visiting a compromised website and was not considered to be a targeted attack.[1] *WannaCry* spread so quickly that the perpetrators were not equipped to match the payments to the demands and subsequently many were left with scrambled data.

NotPetya

NotPetya is a spawn of the *Petya*[2] ransomware virus that was identified in 2016. While both show themselves

as ransomware targeting Microsoft Windows-based systems through the Server Message Block ("SMB") and are believed to trace their origins to EternalBlue allegedly developed by the US NSA, there are big differences between the two. *NotPetya*, does not contain code that allows it to unlock the encryption. Therefore, even if the demanded ransom is paid, the encrypted data cannot be recovered.

NotPetya first manifested in a global attack primarily targeting the Ukraine commencing on the eve of its Constitution Day. It affected Ukrainian targets including banks, ministries, metro systems and even the radiation monitoring system at the Chernobyl Nuclear Power Plant.

However, *NotPetya* spread worldwide affecting companies with no affiliation to the Ukraine including the British ad and market research company WPP; US pharmaceutical Merck; multinational law firm DLA Piper; German logistics DHL; India's largest container port JNPT and Cadbury's chocolate factory in Tasmania. Princeton Community Hospital in West Virginia will scrap and replace its entire computer system as a result of this attack.

Hardening/Bullet-proofing

How do you protect your organisation, your board and your executives from the risks of cyber ransom attacks?

Technical Hardening – There are six main technical considerations of ransomware and its spawn that create a technology "game changer" apart from the standard data breach exposures that have proliferated very publicly against many organisations over the last 10 years or so:

- *Data Value is no Longer Absolute* - With credit cards or Personal Health Information (PHI), there is a dark web market value attached to this kind of information, which provides the motivation to steal it. But in denying access to the data rather than stealing it, the bad actor doesn't need to find specifically valuable information, they only need to find information YOU might value.
- *No Exfiltration / Fencing Requirement* - Part of the bad actors' ROI on malicious cyber-crime typically involves finding a suitable dark market to sell the stolen information, knowing in such an environment they face getting ripped off themselves. The simple process of transferring stolen data out of the target victim network (exfiltration) is another point of risk where the bad actor can be detected by more sophisticated organisations. Ransomware requires no exfiltration, and no need to sell anything to derive value from the successful breach.
- *Attack Vectors are Typically Common Vulnerabilities / Social Engineering* – Every organisation has data. With such a wider range of targets for ransomware, each with their own self-defined valuable data, organisations previously that did not think of themselves as "targets" are now very exposed and in the crosshairs. Common vulnerabilities and simple email phishing schemes are being used successfully to breach unprepared organisations. What made the "*WannaCry*" attack so prevalent was its use of a

recently patched vulnerability in windows SMBv1[3] that allowed it to spread within a compromised network encrypting every vulnerable host and mapped network drive it could access.

- *Automation Implies Indiscriminate Targeting* - With common vulnerabilities and simple phishing techniques being so successful, bad actors have been able to automate the reconnaissance and infiltration processes. This allows bad actors to attack wide swaths of organisations quite indiscriminately without bias. No organisation can be considered safe.
- *Quality Encryption Works Well for Bad Actors Too* - The types of encryption now available to the public, when implemented correctly, are virtually impossible to break. For both asynchronous (RSA 2048) and synchronous (AES 256) methods typically used, it would take more time than there has existed in the universe to brute-force crack with millions of CPUs/GPUs.
- *Ransomware in Disguise (Wolf in Sheep's Clothing)* - Just as in the case of a biological virus that can morph into more lethal forms, ransomware can be modified to wreak greater havoc. As *NotPetya* shows, destructive attacks disguised as ransomware can spread to victims well beyond the initial targets.

When ransomware hits, it is very often too late to do anything technically to mitigate it. Due to the prevalence of the "*WannaCry*" malware, Microsoft took the unusual step of releasing a patch for EOL versions of windows such as Windows XPiii.[4] However, a patch cannot protect against possible mutations and copycat variations. *NotPetya* is but one example.

Most of the traditional security defenses (firewalls, anti-virus, etc.) do virtually nothing to prevent or protect against ransomware. To harden defenses against ransomware, you need to abandon the breach detection mentality that these products emphasise in favor of the more proactive managing of risk to break the bad actor automation cycle, and do so at reasonable costs.

Managing risk means attacking risk holistically across these following four main risk dimensions:

- *Core IT Infrastructure Risk* - The core IT infrastructure (networks, platforms, systems) need to be constantly scanned for vulnerabilities; these vulnerabilities then need to be prioritized and mitigated. This is usually accomplished through patching and configuration error detection. Many ransomware packages continue to exploit old and well-known vulnerabilities.
- *Data & Application Risk* - The most critical applications are often HTTP-based, designed to transmit through the firewall to a mobile app through an API. Bad actors can attack these systems directly, or though a phishing attack gain entry to the network and pivot to critical internal applications. It is critical that key data is therefore prioritized for more frequent and thorough "snapshots" for backup and restore capabilities. Often the only recovery possible after a well-crafted and successful ransomware attack is restoring data made possible through a proactive data risk management program.

- *Process Risk* - Processes help target the most critical assets disproportionately against real world vulnerability exploitability. Whether it's a deliberate "red team" penetration team exercise, or the application of multi-factor authentication on the most critically exposed and/or valuable resources, applying process risk means regularly and proactively applying selected processes designed to probe for real exploitability against IT security policies. Since ransomware relies to some extent on automation, so too must an organisation's defenses rely on process and automation.
- *People Risk* - People risk addresses one of the weakest links that are exploited by most ransomware tool kits, namely fooling employees into inadvertently supplying information or being fooled into the allowing of arbitrary execution of code. Applying social engineering penetration tests, anti-phishing campaigns, and security awareness training are all components of a successful people risk management program.

It is only through a proactive risk management strategy combined across these four risk dimensions can you hope to harden your organisation and prevent the potentially damaging effects of ransomware.

Legal bullet-proofing – Even with the benefit of hindsight, courts do not look for perfection. In assessing whether directors and officers fulfilled their governance duties, courts look at the governance processes and procedures of the organisation. Were they reasonable? Were they followed? If the answer to both is yes, courts will be unlikely to second guess. How do you get there?

The first task is to have a credible assessment of the risk. In the case of cyber-breach and ransomware, the chance of it happening is high; the consequences if it does is more difficult to assess.

Some initial questions that are worth considering are:

- As ransomware involves the unauthorised encryption of data,
    - Is there data that is more sensitive (customer personal info; intellectual property) that should, therefore, receive more attention and protection?
    - Where is your data stored? What due diligence/oversight is in place to protect your data that is in the hands of suppliers and outsourced entities? What contractual indemnities and limitations are in place for your data in the hands of third parties?
- What backup protocols are in place? Are they robust? Secure?
- Does your organisation have a written protocol for protecting or restoring data? Is it robust enough? Is it being followed?
- Does your organisation have the expertise internally to fashion a data protection plan and to monitor adherence to it?

Because the threat of cyber breach and ransomware is so high and so well publicised, not having a procedure

in place that addresses it needlessly exposes the board and the officers of the organisation to liability if the organisation suffers a major loss. Having a procedure in place that is not followed is even more dangerous.

Most modern Canadian corporate statutes recognise that commercial activity carries risks and that the directors cannot be expected to have all the answers to address the risks. Most statutes, therefore, provide a safe harbour for directors who in good faith rely on the advice of experts. In the case of the *Canada Business Corporations Act*, the relevant provision is:

A director … has complied with his or her duties under subsection 122(2) [the duty of care, diligence and skill]., if the director exercised the care, diligence and skill that a reasonably prudent person would have exercised in comparable circumstances, **including reliance in good faith on … a report of a person whose profession lends credibility to a statement made by the professional person.**

A director has complied with his or her duties under subsection 122(1) [fiduciary duty] if the director relied in good faith on .. a report of a person whose profession lends credibility to a statement made by the professional person.[5] *[emphasis added]*
In the area of cybersecurity, one possible way in which a board and in some cases the officers can protect themselves is to have a suitably qualified professional draft or critique the security procedures and then ensure that they are followed.

Risk Transfer – Depending on how and where the cyber-attack originated, it might be that another person can be held liable for the damages. For example, if the vulnerability was the result of a failure on the part of person to which tasks were outsourced, the outsourcing agreement might transfer the liabilities to that person via covenants and/or indemnities. The problems associated with relying only on this are limitations, difficulties of enforcement and the creditworthiness of the person.

Insurance – Inevitably, no matter how robust the cybersecurity processes and procedures are, there will always remain some residual risk. Even if your organisation has a “bullet-proof” set of systems and processes protecting it from third party attacks, it is likely that you won’t be able to fully account for human error and/or the possible naivety, selfishness or political whims of employees.

The value of a cybersecurity insurance policy to mitigate and protect your organisation from this residual risk cannot be overstated. However, cybersecurity insurance is still in its infancy and is constantly evolving. While underwriters continue to struggle with the predictive accuracy of how a cyber breach can impact the business, reputation, property, etc. of organisations of different sizes and complexities across various different sectors, cybersecurity policy coverages, exclusions, deductibles and premiums also continue to change.

Although most claims are currently being made from the health sector where the protection of PHI reigns

paramount, the number of claims being made throughout all sectors continues to rise.[6]

Given the relative complexity and interoperability between insurance policies governing cyber, business interruption, property, etc. it is incumbent to work directly with your broker and/or legal counsel to ensure that every breach scenario is contemplated such that the policies in place will cover and adequately respond to a cyber breach (which may or may not have cascading effects).

One area of interest specifically related to ransomware is the balance between paying a ransom (which is often below the deductible, at least for a mid to large size organisation) or going ahead with a claim under your policy. Unfortunately, bad actors have honed in on this limitation and are using it to their advantage. Indeed, most ransomware attackers ask for a relatively small amount of money (typically below $10,000) such that organisations are more willing to pay the ransom and be done with it. In the area of ransomware, it's really not how big the fish is, but rather how often it bites. However, in the case of attacks like those perpetrated by *NotPetya* insurance may be an important financial lifeline for the organization.

Conclusion

Cybersecurity, ransomware and malware are risks that all organisations must be cognizant of and develop procedures to guard against. Every organisation of every size in every country is a target for ransomware. The "*WannaCry*" malware certainly was not the last to indiscriminately threaten an organizations' critical IT and data assets. *NotPetya* took the attacks to a significantly higher and more dangerous level.

There are a number of technical, educational, legal and risk transfer factors that should be considered. Since the solutions are interdisciplinary, your organisation's IT, risk management and legal advisers should be involved. They can not only reduce the risk of a successful attack, they can help mitigate the legal exposure if you are attacked.

This article was authored in collaboration with Steve McGeown, Senior Vice President of Product and Marketing at *RootCellar Technologies*, a hybrid IT Consulting and IT Security firm.

by Frank Palmay and Darcy Ammerman of McMillan and Steve McGeown, SVP, Product & Marketing of RootCellar Technologies

[1] RootCellar Technologies, *Frequently Asked Questions: "WannaCry" and Ransomware* (May 15, 2017).
[2] Named after the satellites carrying the "Goldeneye" atomic bombs in the 1995 James Bond movie with that title.
[3] https://technet.microsoft.com/library/security/MS17-010.

[4] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

[5] CBCA s. 123 Similar provisions are contained in a number of jurisdictions including: (1) *Business Corporations Act* of Ontario s. 135; (2) *Business Corporations Act of Alberta s. 123*; (3) *Business Corporations Act* of British Columbia s. 157; (4) *The Corporations Act* of Manitoba s. 118; (5) *Business Corporations Act* of Quebec s.121; (6) *Bank Act* s.211; and (7) *Insurance Companies Act* s. 220.

[6] See, for instance, The Canadian Chamber of Commerce, *Cyber Security in Canada: Practical Solutions to a Growing Problem* (April, 2017).

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.