

A Comprehensive GRC Response To Ransomwares

Davindernain Singh Sehgal

CY6200 Final Paper

August 11, 2022

Introduction

Malware is a general term for any type of malicious software designed to damage or exploit a programmable device, service, or network. Cybercriminals commonly use it to extract data, which they can then use on their victims for financial gain. This data can range from financial data to medical records, personal emails and passwords. There are endless possibilities for different types of information to be compromised from. One of the most profitable and therefore popular types of malware among cybercriminals is ransomware. This malware installs itself on the victim's computer, encrypts files, and then demands a ransom (usually Bitcoin) to return the data to the user.

Businesses are effected by this type of malware very frequently, usually because of the scale of their organisation. When malicious actors perform a ransomware attack on a business by encrypting these files and demanding payment of a ransom for the decryption key, cyber attackers are putting companies in the position that paying the ransom is the easiest and cheapest way to regain access to their files. Some variants add additional features such as data theft to give ransomware victims another incentive to pay the ransom.

GRC (Governance Risk and Compliance) becomes very important in such scenarios as having an efficient threat response plan can prove very beneficial for both the organisation as well as the clients who might be effected by the attack. This paper will go over how a ransomware attack takes place in an organisation and also look at a ransomware attack in recent times to look at it through a GRC prespective and figure out a systematic response to ransomwares.

How A Ransomware Attack Works

To understand and create a systematic GRC threat response to this attack, it is crucial that we know how a Ransomware attack takes place. A ransomware attack can be broken down into three steps to make it simple and more understandable.

Step 1: An attacker generates a key pair and puts the corresponding public key into the malware. Malware is released. This is usually carried out using a trojan (a type of virus), entering the victim's system. This can be done by a malicious attachment, embedded link in a Phishing email, or a vulnerability in a network service.

Step 2: The malware then generates a random symmetric key and encrypts the victim's data with it. After successfully doing that, the malicious program typically would display a message to their victim. This "ransom note" simply informs the user that their files and data has been locked from them and also provides instructions on how to make the ransom payment to restore access. The victim usually has no other option to pay the ransom and get back access to their files.¹

Step 3: The attacker receives the payment, decrypts the asymmetric ciphertext using the attacker's private key, and sends the symmetric key to the victim. Then the victim decrypts the encrypted data again using the required symmetric key to complete the ransomware attack.

1. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, E. Kirda In USENIX Security Symposium Austin, TX US, Aug 2016

Cases Of Ransomware Attacks

Scenario 1: In recent times, there have been a lot of ransomware attacks on hospitals which not only puts the hospitals operations at risk but directly affects the patients and their lives. In this case particularly,

80 percent of HSE IT environments were encrypted by ransomware, severely disrupting healthcare services across the country. Encryption in key systems prevented access to diagnostics and medical records, revealing personal information about thousands of people who received the COVID-19 vaccine. The attackers were able to exfiltrate about 700 gigabytes of data included Protected Health Information(PHI) of a lot patients. HHS determined that at the time of the attack, HSE did not have a single responsible cybersecurity owner or senior cybersecurity officer. Also, there was no dedicated committee to guide or oversee cybersecurity and the activities necessary to reduce the cybersecurity risk of the organization.²

Scenario 2: hypothetical example of a similar attack scenario can be stated like:

A project manager for ABC Inc., a billion-dollar manufacturer with offices in 30 countries, steps out of an elevator at headquarters. She's back in the office after her lunch break and looking forward to returning to work on a major order from a major client next week. But something is wrong. As she sits at her desk, she looks like her computer isn't working. Instead of the usual desktop image of her on your monitor, you'll see a lock and a disturbing message.

"File is encrypted. If you do not transfer \$5 million in Bitcoin within 3 days, your files will be lost forever."

Concerned, she called her IT manager at her ABC across the floor, but the IT manager and his staff were too busy to answer. Other employees around the world report inability to access procurement and shipping software. The company's factories in China, India and elsewhere have shut down assembly lines. And the same message appears on every office computer in the company. The company is a victim of ransomware — an attack that is growing increasingly more frequent, severe, and sophisticated.³

2. Case Study: Ransomware locks up to 80 percent of 54 hospital health systems - <https://www.meditologyservices.com/case-study-ransomware-locks-up-80-of-54-hospital-health-system/>

3. Surviving a ransomware attack - <https://www.marsh.com/us/services/cyber-risk/insights/surviving-a-ransomware-attack.html>

In the first scenario, including the hospitals, we can see that HSE didn't have a single cyber security officer, and their cyber security risks were never calculated as there was no established GRC component that would watch over the policies and make sure that they were all followed correctly. Having no cyber security department that could be prepared for such a threat not only cost the company a lot of money but also resulted in compromising the health of a lot of patients. In the second scenario, we see that the project manager tried to call her IT manager, which could mean they have a CISO (Chief Information Security Officer) or a cybersecurity threat management head in their organization. However, we see how she tried to reach out to them but was still unable to reach them because of the lack of reach to the authorities who could have stopped the attack from spreading. Maybe in this organization, the IT department was also dealing with Cybersecurity risks, and they probably do not get equipped to deal with such cyber risks. That's why they chose to be "too busy to answer" for a threat that would eventually cost the company millions in ransom.

In both the above cases, we can see situations where there were brief periods in which the attack could have been avoided, or at least its impact could have been reduced significantly. This is where GRC comes in, and this is why GRC has become such a big part of cyber security because you may not be equipped to deal with cyber threats and not know where to start from or you can have the right resources to deal with a cyber threat but not know how to manage them efficiently. GRC in cybersecurity has become a big requirement because it not only helps keep in check an organization's ability to calculate its cyber risks but is also very useful when it comes to managing the response to those threats.

How To Prevent And Limit The Impact Of Ransomwares

Cyber threats can never be completely prevented but their impacts can be reduced significantly. Following are some defenses against ransomware attacks:

Defense 1: Adding Multi-Factor Authentication(MFA): Traditional single-factor authentication systems require users to provide only one verification factor. H. Passwords to access systems or applications. Hackers can easily steal these passwords and break them into corporate systems. MFA systems require two or more factors to verify a user's identity and grant access to their account. MFA provides strong assurance that authorized users are whom they say they are and minimizes the possibility of unauthorized access. For these reasons, MFA protects systems much more effectively than passwords. This defense is the most underrated defense against ransomware attacks. If you have MFA enabled for your important servers and files and logins, it wouldn't matter if the attack has access to your password files because it would take more than a single password to access those entities.

Defense 2: Taking Frequent Offline Backups: MS-ISAC recommends that backing up important data is the most effective way to recover from ransomware infection. However, there are some things to consider. Backup files should be properly protected and stored offline or out-of-band to prevent attacks from attackers. Many cloud services keep previous versions of files so you can rely on unencrypted versions, which helps mitigate ransomware infections. Ensure that the validity of backups is tested regularly. In the event of an attack, make sure the backup is clean before rolling back.⁴

4. Steps to help prevent and limit the impact of ransomware:
<https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware>

Defense 3: Intrusion Detection Systems: An IDS looks for malicious activity by comparing intrusion detection system "IDS" network traffic logs against signatures that detect known malicious activity. A robust IDS updates signatures frequently and quickly alerts your organization when it detects potential malicious activity. IDS provides early detection and helps nip the infection in the bud. Early detection can greatly benefit organizations targeted by ransomware. This usually saves you downtime, replacement/upgrade costs and ultimately ransom payment. Secure, regularly maintained backups are essential to recovering your business when hit by ransomware.⁵

How To Respond To A Ransomware Attack Efficiently

Although there are many ways to prevent and limit the impact of ransomware attacks, sometimes, an incident is inevitable. Instead of organizations panicking at those moments, it is vital to take the right steps in "**Detecting, Analyzing, Containing and Eradicating**" the ransomware.

Detection:

The threat response team must identify affected systems and isolate them immediately. At the same time the threat response team must communicate the status with the authority in real time so that the management can inform other departments of the same risk in the entire company. If multiple systems or subnets appear to be affected, take the network offline at the switch level. Individual systems may not be disconnected during an incident. If taking the network temporarily offline is not immediately possible, locate the

5. Disrupting Ransomware with Security practices: <https://statescoop.com/disrupting-ransomware-security-best-practices-sc/>

network cable (e.g., Ethernet) and disconnect the affected device from the network or remove it from Wi-Fi to contain the infection increase. After the initial compromise, malicious actors can monitor your organization's activity or communications to understand whether their actions have been detected. Isolate systems in a coordinated manner and avoid using out-of-band communication methods, such as telephone calls or other means, to alert actors that an attacker has been detected and mitigation actions are being taken. Otherwise, actors may stray and gain access (an already common tactic) or spread ransomware before the network goes offline.⁶

Analysis:

Continue to identify the who, what, when, where, why and how of the incident at the best possible level. Use local operating system and application logs, and network device logs to find as much information about the attack as possible. Identify and prioritize critical systems needed for recovery and see what kind of data is stored on affected systems. Prioritize recovery and recovery based on a predefined critical resource list that includes information systems critical to health and safety, revenue generation, or other critical services and systems on which they depend. Track systems and devices known to be unaffected so they can be recovered and deprioritized. This allows businesses to resume business more efficiently. GRC comes into the picture by managing that analysis of these components is done thoroughly and that mistakes aren't made, this can be achieved by introducing a proper chain of command

6. A transportation company's response to ransomware attack:
<https://www.marsh.com/us/industries/transportation/insights/responding-to-ransomware-attack-transportation-company-journey.html>

between how the threat response team interacts with the general departments and the CISO who will be looking over these operations.

Containment:

The containment phase is primarily aimed at limiting damage, preventing further damage, and retaining data for possible use in further investigations or legal proceedings. For ransomware, a short period of containment is usually accompanied by identification of the attack. If not already done, the threat response team must physically or logically disconnect the infected or suspect device from the network. The ideal situation is to leave the device powered on and disconnected. In some cases, the ransomware unlock key remains in memory and can be used to easily restore the device. A forensic image of the affected device may be required to understand the root cause of the attack. Ideally, these images are collected before mitigation actions are performed on the system. However, this is not always possible. Therefore, please try to collect items in their original form (untouched) as much as possible. GRC comes in the scenario in case the company does not have their own digital forensics investigators and are depending on a third party forensics company, the cybersecurity department will have to communicate and analyze the report. It is up to them if they want to submit the same report to the board of directors or other important entities of the organisation or come up with a simpler report that can be written in layman terms.⁷

7. University of Toronto: Information Security and Enterprise Architecture : <https://isea.utoronto.ca/policies-procedures/guidelines-2/short-incident-response-playbook-for-ransomware/>

Eradication :

The eradication step actually removes malware or other methods used or established by attackers on affected systems. Recovery of the system and finalization of the detailed schedule and scope of the incident are also made here. If the scope and severity of the incident are justified, hire an outside forensics firm to conduct a more thorough review of the affected systems(Which will again be looked by the manager responsible of handling cybersecurity proceedings). This is typically done at the direction of the CSIRT, using one of the pre-identified services that have already been evaluated and contracted to provide these services across the university. Ransomware attacks are known to occur repeatedly, so it is important to identify the root cause of the infection to limit the likelihood of such occurrences. Complete a formal incident timeline with as much detail as possible, including the following questions: 1. Who accessed the system and what accounts were modified, accessed or created. 2. What changes did the attacker make to the system? What malicious or other code did the attacker install or use? What data was affected, accessed, or stolen by the attacker? What is?

Recovery :

The cybersecurity department will now interact with all the departments in the organisation for the recovery of their systems and making sure an incident like this does not occur again. Recovery is the safe redeployment of the affected system into production. The quickest and easiest way to recover from the ransomware attack is to restore from a known good backup. However, you should address the root cause of the attack and simply replace the corrupted file. This makes the chances of being compromised again as low as possi-

ble and eliminates the chances of the same attack vector succeeding. All deployed systems should be fully patched before redeployment. Simply patching the software that caused the breach is not enough. All software on the system must be patched. If software cannot be patched, compensating controls must be applied to protect the software, and patching dates must be fixed. Systems should be hardened according to industry standards to minimize the initial attack surface and limit the likelihood of weak or default configurations being introduced into production. This is where the Compliance part of GRC comes into the scenario and helps the organization maintain an industry standard after its recovery from an attack. The Center for Internet Security Benchmarks offers free hardening standards that provide excellent baseline security validated by multiple organizations.

if the above response steps were taken by the above two example scenarios, their impact could have been reduced significantly and would have not cost those organisation millions of dollars in ransom.

Conclusions

Governance, Risk, and Compliance (GRC) existed primarily within large enterprise organizations. However, ransomware risks affect organizations of all shapes and sizes, so basic GRC practices can be an effective part of a defense strategy, even for small businesses. By implementing a GRC strategy, organizations can identify and raise awareness of security risks, including ransomware. Organizations can also take appropriate protective measures to mitigate these risks. After reading the above examples, it is evident that by following

the right GRC response steps to ransomware attacks, the organisations could have handled the situation more systematically. All types of security risks must be addressed and When deciding which solution to implement, organisations should not make the mistake that many organizations make and focus on just one line of business. It is important for organizations to understand that GRC solutions benefit the entire organization, not just those most at risk.

GRC goes hand in hand with the overall operations of an organization and Cyber-Security. Having good Governance in your organization to manage full-scale operations is as important as identifying the risk and factor in ways to protect against those risks (like Ransomware) which in turn is as important as Complying with industry-standard to not only be a more secure organization but to also maintain trust with your clients/customers.

This paper explained how ransomware attacks work, shared two examples of those scenarios in an organization and also stated key points in how to defend against such malware and how to respond to them systematically using the GRC threat response approach while also showing how GRC goes hand in hand with cybersecurity and why it is vital to any organization that deals with any kind of data.