Alliance for Healthier Communities
Alliance pour des communautés en santé

Cybersecurity and Ransomware

Alliance member case studies

Table of Contents

"Ransomware is unique among cybercrime because, in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact"

– James Scott[1]

[1] Author of The CEO's Manual on Cyber Security

Introduction

Ransomware is a type of malware, or malicious software, which locks all known files through strong encryption and prevents users and administrators from accessing their networks, systems or data. Ransomware effectively denies access to organizational data by encrypting it and withholding decryption tools until a ransom is paid. Paying the ransom assumes the bad guys are ethical, but there is no guarantee that paying will get an organization the decryption key they need to access their data. The sole objective of ransomware is to make sure that people cannot access their electronic files.

Ransomware attacks

Ransomware attackers usually demand payment be sent via cryptocurrency (e.g. Bitcoins) since these payment methods are extremely hard to trace. There are several different ways ransomware can infect networks and computers. One of the most common methods is through malicious spam or unsolicited email that is used to deliver the malware. The email might include booby-trapped attachments, such as "official-looking" PDFs or Word documents. It might also contain innocuous and friendly looking links to malicious websites. These methods employ social engineering to trick people into opening attachments or clicking on links by presenting them as legitimate. Often emails appear to be from a trusted institution, colleague, or friend.

Another common method is a brute force attack[2]. A brute force attack is a trial-and-error method used to obtain a user password or PIN. Automated software is used to generate a large number of consecutive guesses of the desired password. These types of attacks are one of the reasons why you are often prompted when creating or entering an account password to "prove you are not a robot."

A focus on Healthcare

Healthcare institutions have become easy targets for hackers because of the necessity of, and reliance on, sensitive electronic medical records and corporate information. Also, these systems generally contain all the necessary data sets that allow hackers to steal identities, defraud insurance companies, encrypt for ransom, do cross-referencing for intelligence gathering, and steal intellectual property. Perhaps the most compelling reason for hackers to target healthcare institutions is the lack of adequate funding for IT-related systems and cybersecurity across the country[3].

Ransomware has grown in sophistication as the potential for criminal profits from the practice has grown. Today, such malware is stealthier, causing infection without notice, allow cyberattackers to steal data while also encrypting it locally. Even if you get a decryption key, if forensic IT analysis shows that the malware was capable of sending a copy of your data to another location off-site, the potential for recurring ransom attacks can grow as well as the potential for a breach of privacy and security laws.

The following case studies examine cyberattacks that occurred at four different member organizations and unpack exactly how the cyberattack was targeted at them.

[2] Read more about brute force attacks https://www.techopedia.com/definition/18091/brute-force-attack
[3] https://www.cbc.ca/news/canada/new-brunswick/david-shipley-medical-devices-cybersecurity-1.4236458

Case Study 1

Details of the Cyberattack

The attack happened on the weekend and all the computers that were either not shut down or in hibernation were infected. The centre was made aware of the attack on Monday morning when a staff member indicated they were unable to log into the system. There was an electronic ransomware message on the desktop and in every folder stating that the files were encrypted and stating the terms of the ransom.

The centre immediately disconnected from the Internet. Investigations indicated that access was gained through a decommissioned Windows 2003 terminal server that was supposed to be off (line) but was still on and connected to the network. Additionally, there was a firewall policy to enable a remote desktop protocol (RDP) connection on the server over the Internet without a virtual private network (VPN) connection. The remote desktop protocol is a network communications protocol designed for remote management and for remote access to virtual desktops, applications and an RDP terminal server.

> **"After years of not** suffering from migraines, I experienced a particularly brutal one a**fter this event"**
>
> - System Administrator

The cyberattacker(s) gained access to the entire network through the Windows 2003 server, sent themselves an administrator password and proceeded to encrypt all the servers. This then propagated to computers that were left on or in hibernation. Backups that were accessible on the network were also encrypted.

The centre was using the Nightingale on Demand electronic medical record (EMR) software, which was accessed securely over the Internet, therefore no client medical data was affected. Furthermore, the centre had moved to Office 365, a cloud-based application set, so no Office files (including emails) stored in the cloud were affected. Only local organizational and financial files were encrypted by the ransomware.

Fortunately, six years prior, the centre's outsourced Information Technology (IT) vendor had recommended the creation of a regular automatic backup. This was designed to run on a segregated virtual local area network or VLAN. A VLAN is a group of devices on one or more local area networks (LANs) that are configured to communicate as if they were attached to the same wire, when in fact they are not. This backup had been successfully running for the past six years and proved to be invaluable. After verifying that the files were intact, the centre used the backup copy to restore their systems.

Insurance

The centre did not reach out to their insurance company because they were able to do a full system restore. They did report the incident to the community police and informed their board of what data was lost, the overall costs, and suggestions for mitigation.

Cost

Costs were associated primarily with staff time including staff working directly on the restore and the tremendous amount of clean-up work that had to be done.

Timeline

Day 1	After work some staff left their computers on, others put them into hibernation and some shut down their computers.
Day 2	Unprotected Windows 2003 server was attacked and used to gain access to the rest of the network; all computers either in hibernation or that were left on were encrypted.
Day 3	
Day 4	Users found the network unavailable. Ransom note was found on computers. Work to investigate and restore began immediately; unfortunately, backups that were on network access storage (NAS) devices were encrypted. A backup process installed on a segregated virtual server was found to be untouched. Restoration and rebuilding activities began.
Day 5	Some users were given access to the EMR to continue serving clients
Day 6 – on	Back to full operational status.
CURRENT	Preventative measures to address the weakness in security exposed by the incident.

Case Study 2

Details of the Cyberattack

The cyberattack against this organization happened on a Thursday morning. Hackers used a brute force attack to get into the organization's servers through a vulnerable remote desktop protocol (RDP) server. Once they were in, hackers planted ransomware, effectively preventing anyone from accessing the system. The hackers were also able to access and delete onsite backups on two separate servers. There was also a cloud backup protocol in place. This was a full system backup in the cloud. Unfortunately, the centre discovered a significant problem with this backup. The database had grown so large that the cloud backup continued to fail without providing notification to the centre or any follow-up by the vendor. It was then discovered that the last full offsite backup of the system was a full six weeks prior to the incident. This was devastating news. This centre had a local instance of their EMR and this data was included in the backups. All other files were kept in the cloud via Office 365 and therefore remained accessible.

> "It took months of work to get our systems and processes back to where they were prior to the attack"
>
> - Executive Director

Fortunately, nine days prior, as part of its EMR transition activities, the centre was asked to transfer a full copy of their EMR to the transition vendor. Although this was much better than losing 40+ days of data, during the nine-day period the centre had been focused on a data cleanup exercise. All of that work was lost. The centre also incurred significant costs in having to reinstall, rebuild and restore the entire local EMR software environment.

Insurance

The centre did not reach out to their insurer having declined the additional cybersecurity insurance, offered to them a few weeks prior. They did, however, inform their board and clients of the attack.

Costs

The centre estimates that having a local instance of the EMR contributed greatly to the increase in restoration cost. It meant the reinstallation of the EMR could not be done without the EMR vendor and the IT vendor. Other costs were staff time and costs to inform clients. This included working directly on the restore and the tremendous amount of follow-up work that had to be done. The centre estimated a cost of approximately $60,000.

Timeline

Day 1	Brute-force attack granted access to the system followed by immediate ransomware infection. Centre discovers backups have been deleted and the online backup had fully failed six weeks prior without any notification by the vendor or error message by the system processes.
Day 2	Centre decided to use the last full system backup that was being used for data migration testing (only 9 days old)
Day 3	EMR reinstall, rebuild and restore begins
Day 4	
Day 5	
Day 6	Very limited access to EMR
Day 7 - on	Back to full operational status
CURRENT	Preventative measures to address the weakness in security exposed by the incident.

Case Study 3

Details of the Cyberattack

The centre was alerted to the possibility of an attack when a member of staff said they were having problems opening a document. Upon investigation, it was discovered that all documents on the network share had long names. Suspecting a cyberattack, the network was quickly disconnected from the Internet. It was then discovered that all files and folders on all network shares had been encrypted. There was a single text file in every folder acknowledging the presence of ransomware along with instructions on payment.

The centre had a two-level backup system in place. One was using an external hard drive to back up all documents in personal and network shares. The second was a magnetic tape system where the Exchange server and all emails were backed up. Unfortunately, it was determined that the external hard drive had failed over two months prior to the incident. This meant that the last known good backup was 60 days old. No alerts were issued to inform the centre of this failure. The tape backup was unaffected. Financial and EMR data was stored in the cloud and was unaffected.

> "You have to know your systems and architecture; every **single part of it"**
>
> - System Administrator

A decision was made to contact the cyberattacker(s). Within a matter of hours, they received a reply asking for more details (e.g. number of machines affected, size of the organization, server operating systems). Realizing that doing this alerted the cyberattacker of a potential victim (and could also potentially affect the size of the ransom that would be requested), they immediately blocked the email address and domain. Back to reassessing the damage, it was decided to delete all the encrypted files and folders and fall back to the last known good backup that was done two months earlier. This decision was made fairly quickly since the number of files generated by users in that time span was determined to be fairly small. Within a matter of a few hours after the attack, the centre was operational again.

During the root cause analysis, it was discovered that there was a Windows 2003 server setup for remote access with an Internet-facing external port. It appeared that this server was used by a past system administrator for off-site administration. The current administrator was unaware of this as there was no previous system infrastructure documentation. It was through this server that unauthorized network access was achieved.

Insurance

The centre did reach out to their insurer who indicated that since they were not negotiating with the cyberattackers, they would not intercede.

Costs

Costs were associated with staff time working directly on the restore for an entire day.

Timeline

Day 1	5:00 am – Attack begins and all files on the network shares are encrypted 8:00 am – Attack discovered and centre disconnected from the network 1:00 pm – Centre decides to delete encrypted files and use two-month-old backup
Day 2 – on	Back to full operational status minus any files that were created during the two month period
CURRENT	Preventative measures to address the weakness in security exposed by the incident.

Case Study 4

Details of the Cyberattack

Unlike the other centres among these four case studies, this centre had no IT personnel onsite who could understand and manage the attack. They had transitioned from a private IT vendor to a hospital-based IT vendor. The centre was also in the middle of the three-year IT implementation plan that was proposed by their current vendor. One of the items identified in this plan was to have the centre's systems, which were currently being backed up onsite, moved to an offsite backup location at the hospital. In the interim, the new IT vendor was relying on the onsite backup. However, this backup was not being done on a segregated server.

The cyberattack was initiated when a user clicked on a link containing the ransomware. Soon after, the centre determined that no one could access email.

> "When changing vendors, make sure there is a proper transition of **responsibility"**
>
> - Executive Director

An urgent call was made to the IT vendor, who discovered that the Exchange server had been compromised through a ransomware infection. They also found that the local backup had been encrypted. The Executive Director remembered that the previous vendor had created a disaster recovery backup on a segregated server and asked the current vendor to look into this. Unfortunately, this process took almost three days. After a lot of finger-pointing between vendors, the centre was able to restore their environment.

The Executive Director recommends that if anyone is planning to switch vendors, they should ensure that their new vendor is fully familiar with the organization's entire network infrastructure. It is also highly recommended that centres regularly test their Business Continuity Plan (BCP) and Disaster Recovery (DR).

Insurance

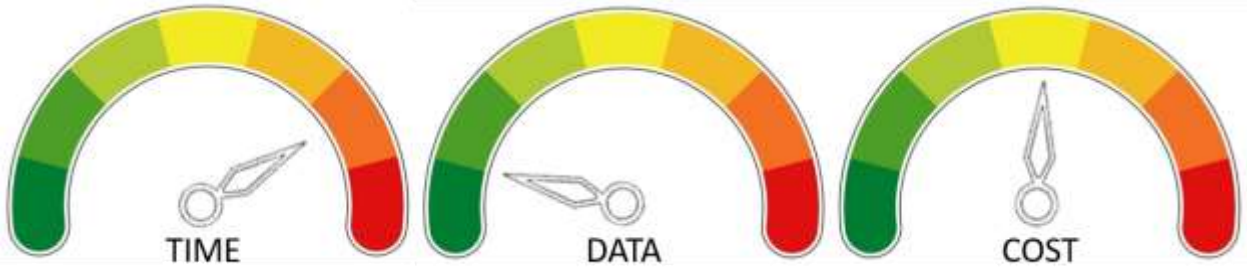
The centre did reach out to their insurer who indicated that since they were not negotiating with the cyberattackers, they would not intercede.

Costs

Costs were associated with staff time including staff working directly on the restore and the tremendous amount of follow-up work that had to be done. The centre had to resort to faxing and phones as there was no access to emails during this time.

Timeline

Day 1	Staff member clicks on a link that begins to infect the system. Although the physical connection to the network was removed quickly, it was not fast enough to prevent a lockdown of the Exchange Server. IT vendor contacted
Day 2	No response from IT vendor
Day 3	
Day 4	
Day 5	Current IT vendor begins working on system restoration but indicates that the backup system was not set up correctly
Day 6	Current and previous IT vendors work on system restoration
Day 7	
Day 8 –on	Back to full operational status
CURRENT	Preventative measures to address the weakness in security exposed by the incident.



Conclusion and Lessons Learned

In all our cases studies, cyberattackers were interested in encrypting information rather than simply stealing data outright. There was no activity suggesting data was transferred out of local networks. However, this is an increasing trend. Attackers are encrypting or deleting data after copying it. They then either attempt to ransom it to the owner or sell it to other interested parties. Centres who use a cloud-based Electronic Medical Record (EMR) and who had migrated to cloud-based Office systems e.g. Office 365, were safeguarded against an encryption attack on these systems.

Cyberattackers can gain access by being right just once, but your centre's defences need to be right all the time. Protecting against such attacks and hardening your organization's cyber-resiliency can only be accomplished through a systematic multi-layered approach. Here are nine of the main lessons to take away:

- The first level of mitigation is to promptly apply software patches and use anti-malware technologies to block or at least detect malware infections. Disable all redundant services and enable firewalls.

- Limit the kinds of tasks the system administrator performs on the backup server that might place it at risk. System administrators should never browse the web directly from the backup machine, and especially not from a privileged account on that machine.

- Be familiar with your network infrastructure – overlooked or unknown and vulnerable servers were attacked in two of the case studies. Since many attacks also come via the Remote Desktop Protocol (RDP), disabling external access to RDP is always a good idea. If your organization uses RDP as part of your operation, consider putting it behind an internal firewall. For example, limit RDP access to only those who have authenticated themselves and utilize a VPN for access.

- Educate your users. In all four case studies, ransomware attacks either started at an unprotected Windows-based server and crawled through the network, or were initiated by the inadvertent actions of a user on the network. Develop "acceptable use" computer policies and educate users on the importance of safe online activity but also on staying vigilant when working with technology.

- Ensure that senior management and your organization's Board are aware of any potential technological risks, mitigation and associated costs. This is especially true of smaller centres with limited resources. However, as there is a heightened awareness of information as a commodity, this type of communication would be essential for all organizations. The oversight of the Board and the establishment of senior management accountability policies are critical foundational components that engender the development of a culture of cyber-risk awareness and management.

- Backups are the last and most crucial line of defence. Make sure that it is one of the first systems to receive security patches. Segregate the backup systems as much as

possible. This means not using an Active Directory authentication to log into the backup server. Use a separate account that is used only on the backup system. It is also important to put the backup system on a separate network or VLAN. This will potentially minimize the risk of malware that crawls through the network looking for other systems to compromise.

- Consider the benefits/costs of a cyber-insurance policy, also referred to as cyber-risk insurance or cyber-liability insurance coverage. These policies are designed to help an organization mitigate risk exposure, by offsetting costs involved with recovery, after a cyber-related security breach or similar event. Ensure that you are familiar with your cyber-insurance policy and coverage limitations. A cyber-insurance policy may include monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage. Policies may also cover legal expenses associated with the release of confidential information and intellectual property, legal settlements, regulatory fines and the costs of cyber-extortion, such as from ransomware[4].

- Paying ransom is discouraged by provincial/territorial authorities and the Canadian Centre for Cyber Security[5] as it does not guarantee the decryption keys will work or the organization will not be vulnerable to further attacks or extortion. It only encourages and guarantees criminals can benefit from these activities.

- Cybersecurity is not an information technology issue alone. It should be addressed as part of your organization's overall Business Continuity Program/Disaster Recovery (BCP/DR) integrated risk and recovery management program.

[4] Healthcare Insurance Reciprocal of Canada https://www.hiroc.com/
[5] https://www.cse-cst.gc.ca/en/backgrounder-fiche-information

Appendices

- The Alliance for Healthier Communities publishes monthly newsletters on Privacy and Security. Please visit our member portal for back issues at our Member Portal here https://aohc.site-ym.com/members/group_content_view.asp?group=141556&id=529385
- 9 things to think about when preparing against a cyber-attack
- Incident Response Plan
- Cyberattack Immediate Response Checklist
- Ransomware Prevention Checklist
- Glossary

9 things to think about when preparing against a cyberattack

ACTION	DESCRIPTION
Anti-virus and network privileges	Antivirus solutions don't suffice as a standalone solution anymore. Set up privileges so they perform tasks such as granting the appropriate network shares or user permissions. A privilege allows a user to perform an action.
Back up data	In the event of an attack, you can power down the affected system, reimage it, and reinstall from your recent backup. You may recover all your data – from your last successful backup. This, however, presupposes that the ransomware has not also affected and encrypted your backup. Speak with your IT experts on strategies you can use to secure your backups. It is also critically important to check that your automated backups are happening and even do test restores to ensure the integrity and validity of the data. Validating your backups is just as important as setting them up.
Educate users	The weakest links in any security chain are people. Helping users learn how to spot phishing and malware emails will empower them to help protect your network
Monitor network activity	Being able to see everything happening across your network can help you uncover attacks. Monitoring bandwidth usage, network speed and database activity can quickly raise red flags.
Patch systems	It is essential that software is regularly updated. Patching commonly exploited third-party software will foil many attacks. Users should not be allowed to postpone the application of patches as this is proven to further increase the risk of attacks.
Prevent effortless infiltration	Most ransomware infections occur through an email attachment or a malicious download. Diligently block malicious websites, emails, and attachments through a layered security approach.
Protect your network	Take a layered approach, with security infused in every layer.
Paying the ransom should be last resort	Contemplate paying the ransom as an absolute last resort. However, you should know that there's no guarantee you'll get your data back, and you're only fueling the cyber-criminals' appetite for more attacks. Involve your insurer in the process, should you decide to go for this option as they can help you in the process.
Segment your network	Limit the resources that an attacker can access. By dynamically controlling access at all times, you help ensure that your entire network is not compromised in a single attack.

Incident Response Plan

ITEM	ACTION	NOTES
Incident Response Team Management	Identify the members of your response team and their individual responsibilities	At minimum, the Response team should include: - Incident Response Lead - Member of senior management - Information system subject matter expert
Backup and Restore Testing	Validate your backup data	- Ensure daily backups of all critical systems are taken and maintained offline and offsite to protect them from a potential breach - Periodically test restoring the data from your backups to verify the integrity of the data and validate the backup process
Downtime policy	Validate and communicate your EMR downtime/unavailable policy	How does the workflow change if your centre has limited or no access to the Internet and the EMR?
Communications Plan	Initiate your communication plan	- Determine what happens if customary methods of communication are compromised e.g. email - Who gets informed and how? - Who speaks to the media? What are their key messages?
Legal	Determine your legal obligations	- Determine what regulatory bodies need to be informed if there is a data breach or loss of data - Determine communication that may have to be sent to clients - Determine if the privacy commissioner would need to be informed
Insurance	Determine if you have coverage and for what	Not all financial losses associated with cyber incidents are covered under general liability or property policies. Certain situations would need a separate cyber risk policy to provide coverage. Review your coverages and limits to ensure they are appropriate and adequate, and that you're meeting the requirements of your organization's policy

Cyberattack Immediate Response Checklist

Incident Management		
☐	Contact the Incident Response team	
☐	Initiate the Incident Communication plan	
☐	Engage with insurance provider if necessary	
☐	Communicate with regulatory bodies if required	
☐	Communicate with clients if necessary	
☐	Communicate with the privacy commissioner if necessary	

Disconnect Everything		
☐	Unplug your computer from the network	
☐	Turn off any wireless functionality: Wi-Fi, Bluetooth, Near Field Communications	
☐	Reach out to your IT vendor or subject matter experts	
☐	Reach out to Alliance staff	

Scope of the Infection		
☐	Mapped or shared drives compromised	
☐	Mapped or shared folders from other computers compromised	
☐	Network storage devices of any kind	
☐	External Hard Drives	
☐	USB storage devices of any kind	
☐	Cloud-based storage: Dropbox, Google Drive, OneDrive etc.	
☐	Applications that may have been compromised	
☐	Ensure unaffected systems are protected	

Determine Ransomware Strain		
☐	What strain/type of ransomware? For example CryptoWall, Teslacrypt, Dharma, etc.	

Determine Response

Option 1 - Restore from unencrypted backup		
☐	Locate your backups	
☐	Verify integrity of backups	
☐	Check for any previous versions of files that may be stored on cloud storage	
☐	Remove the ransomware from your infected system	
☐	Restore your files from backups	
☐	Determine infection vector & protect against future attacks	

Option 2 - Decrypt solution		
☐	Determine strain and version of the ransomware, if possible	
☐	Look for a decryptor online, however, there may not be one for newer strains	
☐	If successful, attach any storage media that contains encrypted files (hard drives, USB sticks etc.)	
☐	Decrypt files	
☐	Determine the infection vector & handle	

Option 3 - Do Nothing (Lose Files)		
☐	Remove the ransomware	

Post-incident		
☐	Post-incident review and any necessary adjustments to the cyber security incident response plan based on first-hand experience and analysis of the event	
☐	Root cause analysis including the documentation of facts, findings, activities, outcomes and mitigating recommendations where applicable	
☐	Reporting on the incident and lessons learned	

Ransomware Prevention Checklist

Protecting Yourself in the Future		
☐	Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed	
☐	Conduct simulated phishing attacks to familiarize users against current threats	
☐	Ensure you have a functioning firewall and a secure configuration	
☐	Implement antispam and/or anti-phishing. This can be done with software or through dedicated hardware such as SonicWALL or Barracuda devices (or similar)	
☐	Ensure everyone in your organization is using up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking	
☐	Implement software restriction policies (including disabling USB ports, autorun capabilities, etc.) on your network to prevent unauthorized applications from running. (*optional*)	
☐	Implement a highly disciplined patch procedure that updates all applications	
☐	Implement a backup solution: Software-based, hardware-based, or combination	
☐	Ensure all possible data you need to access or save is backed up, including mobile/USB storage	
☐	Ensure your data is safe, redundant and easily accessible once backed up	
☐	Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups	

Glossary

WORD	MEANING
Brute force attack	A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).
Click-bait	Content whose main purpose is to attract attention and encourage visitors to click on a link to a particular web page
Encryption	The process of converting information or data into a code, especially to prevent (*unauthorized*) access
LAN	A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct area such as an office. Computers and other mobile devices use a LAN connection to share resources such as a printer or network storage.
Malware	Any software that is intended to damage or disable computers and computer systems
Network privilege	Network privilege is the concept of only allowing users to do certain things. For example, an ordinary user is typically prevented from changing operating system files, while a system administrator is typically permitted to do so because this is part of maintaining a computer system.
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers
Ransomware	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
RAS	A remote access server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet. Once connected with a RAS, a user can access his or her data, desktop, application, print and/or other supported services.
RDP	Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.
Scareware	Malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection
Screen lockers	Ransomware that may ask you to confirm something on a website, but causes your screen to seize and display a message from a lock screen ransomware. The ransomware generally demands payment. Your operating system is completely locked out by the ransomware.
Spear phishing	The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. Unlike a traditional phishing attack, a spear phishing attack will be highly targeted. The message will be sent only to one person or a few, carefully selected individuals. The overall goal of the attack will determine who gets selected as intended victims

WORD	MEANING
Spyware	Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive
TOR	Tor is free software for enabling anonymous communication
VLAN	A VLAN is a group of devices on one or more local area network configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different local area network segments
VPN	A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network