VRSA

Virginia Risk Sharing Association

Double the Trouble: Increasing the pressure to pay cyber extortion

Presented by:

Shawn Talmadge
Cary Scardina
Marcus Hensel
Thomas Bullock
Darius Davenport

This presentation is for educational purposes only. It is not legal advice for any particular situation. Laws change all the time. Always verify that information is accurate and up to date before you rely on it.

DISCLAIMER

Cybersecurity Is Not Just an IT Issue…

Headlines

Hit with ransomware attack, Howard University forced to cancel classes

Warren County recovering from March computer infiltration

Virginia Tech Says It Was Targeted in Two Recent Cyberattacks

Smyth County Schools' computers targeted by ransomware

Fairfax County Public Schools hit by Maze ransomware

Ransomware attack leads to shutdown of major U.S. pipeline system

After cyberattack, stolen Chatham County data and sensitive documents posted online

Water Plant Cyberattack Is Wake Up Call, 20 Years in the Making

New Kent County Public Schools victim of ransomware attack

$600,000 payment for turf football field stolen from Spotsylvania

Why does this matter?

- Local governments hold significant amounts of sensitive data
  - Legal
  - Health
  - Financial
- Older, more vulnerable computer systems
- Valuable data
- Disruption
- Virginia Public Procurement Act
- Freedom of Information Act

Ransomware

Ransomware

- Ransomware is a **form of malicious software (“malware”)** designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data

WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link

or http://maktubuyatq4rfyo.torstorm.org

or http://maktubuyatq4rfyo.tor2web.org

Double Extortion Ransomware

- Double extortion is a tactic wherein a crypto-malware strain steals information stored on a victim's machine before encrypting the remaining files.
- The malicious actor demands payment in exchange for decryption
- The malicious actor also demands payment in exchange for not publicizing the stolen data on the dark web.

Show of Hands

- Would your organization pay a demand?

Hypothetical Scenario

Hypothetical 1: Ransomware

- An employee in your department calls the help desk stating that her computer rebooted and is now displaying a message that says her personal files are now encrypted and that she has 1 day, 23 hours and 20 minutes to pay a ransom of 2 bitcoin in order to obtain the decryption key. Three other staff members also report to your IT director that they can no longer access files in the shared department folder. They are all receiving the same ransomware message.

Questions & Answers

- **Once you hear about this incident from employees?**
  - Activate your incident response team
  - Call your Data Counsel

- **Who makes up the Incident Response team (IRT) and what is their role?**
  - Your ITR should be made up of your leadership team, IT, HR, Data Counsel and external data forensics professionals. Their job is to stop the incident, investigate, restore data, and make any necessary notifications.
  - Your internal IT staff likely is not equipped to respond to a sophisticated attack alone no matter what they say.

Questions & Answers

- **Do you call your insurance carrier?**
- Call them immediately!

- **Why should you call your carrier?**
- Your insurance carrier may have resources (legal, data forensics, call centers, etc.) that can assist in the containment, remediation, recovery and notification process.
- Not notifying your carrier could result in policy exclusions.
- Incident response requires immediate action and the application of external resources.

Questions & Answers

- **What do you tell your CIO to immediately do?**
  - Disconnect from network
  - Take screenshots of ransom note
  - Capture BTC addresses, email addresses, file extensions for FBI
  - Conduct memory capture before shutting down
  - Don’t start wiping hard-drives
  - Power down infected servers
  - Cooperate with outside vendors
  - Cooperate with outside counsel

Hypothetical 1: Ransomware

- You receive a call on your cell phone from the Director of Public Safety who notifies you that ransomware notices are appearing on the city's public safety computer systems. Computer systems in the police, and fire departments are now displaying the ransomware message informing users that their files are being encrypted. You attempt to call the Chief of Police at his desk, but the phone call does not go through.

Questions & Answers

- **Do you pay the ransom?**
  - The FBI will never advocate for paying ransoms
  - This is an organizational decision
  - You may have to reevaluate this decision based on the severity of the attack
  - There are potential serious implications for paying a ransom
  - Paying the ransom does not guarantee (1) you will be able to decrypt or (2) that you will not be extorted again

Hypothetical 1: Ransomware

- As computer and communication systems across the city begin to slow and fail, employees begin to call and email each other speculating that the city may be experiencing a data breach. A handful of employees begin to report that they received an email from the hacker stating that they have taken files from the City's servers and that the hackers will dump those files into a dark web marketplace if the ransom is not paid.

Questions & Answers

- **Do you communicate with the hacker?**
  - Wait as long as possible to communicate with the hacker
  - Data security firm/professional negotiator (crypto-wallet)

- **Do you contact law enforcement?**
  - Yes – you are a victim
  - Law enforcement and data forensics firms are great resources because they have a wealth of knowledge regarding malware variants and hacker modes of operation

Questions & Answers

- **Is it time to give in and pay the ransom?**
  - FBI will not advocate paying a ransom
  - Make the hacker provide a sample of data to prove they actually have acquired data

- **Are there other law enforcement resources?**
  - Virginia Fusion Center
  - Virginia National Guard

Hypothetical 1: Ransomware

- You look at your watch and realize you have one hour left on the hacker's encryption countdown. You check your cellphone and learn that news that your city has been the victim of the THANOS ransomware attack is trending on social media. Moments later your deputy city manager is contacted by a local news station to confirm these reports. Your cellphone rings and the hacker tells you that you should not have called the FBI and that they are doubling the ransom, posting emails from the mayor's email account and going to add some fluoride to the water system.

Questions & Answers

- **What do you tell the media?**
  - Confirm your facts before making any statements
  - Its ok to say that the city has deployed resources, is investigating, and will provide additional information as soon as it is available.
  - Consider crisis communications professionals
  - There is a big difference b/w a data incident and breach
- **What do you tell employees?**
  - Same as media
  - Encourage them to report suspicious activity
  - Use discretion when discussing the matter

Questions & Answers

- **What's the best way to communicate with staff during a serious data incident?**
- Develop an out of band communication system
  - Cell phones
  - Non-municipal email accounts
- Good when standard communications are potentially being monitored
- Good when standard communications are not available

Questions & Answers

- **How can you prevent this from happening?**
- Develop an IRP (Know your key players)
- Tabletop Exercises
- Train employees
- Develop cyber specific policies
- Encrypt your data while it is not in use
- Phish your employees – make it fun, give out awards and/or make it a unit-vs-unit competition if possible; open-source statistics show email is the vector in about 95% of cybercrime.
- Contract for IT services such as vulnerability and penetration testing
- Use antivirus (signature-based) AND heuristic (non-signature-based) audit controls– this can help you determine which data was accessed or exfiltrated if an event occurs
- Use offline backups or other immutable storage methods

Questions & Answers

- **How can you prevent this from happening?**
- Defense in depth – use Firewalls on individual devices to prevent lateral movement within your own perimeter (multi-factor)
- Have an out-of-band call/email plan ready
- Monitor baseline traffic flow to backups – (depending on backup type) if ransomware cannot encrypt backups directly, it may try to overwrite backups with junk; one victim caught the malicious activity because it saw an unusual spike in backup activity.
- Employ 'zero-trust' network configuration where possible

Office of Foreign Asset Control

U.S. Department of Treasury, OFAC

- Many major hackers are on OFAC's list of Specially Designated Nationals, Blocked Persons, and those covered by embargos.
- Many major hackers are associated with organized crime, terrorist organizations, cyber intelligence agencies, and/or enemies of the US.
- Paying a ransom can equal support to one of the organizations above
- Paying a ransom can subject you to OFAC sanctions

U.S. Department of Treasury, OFAC

- Sanctions range from cautionary letters to civil penalties up to $311,562
- In determining sanctions, OFAC looks to factors such as:
  - Willful or reckless violation of law
  - Harm to OFAC's sanction program objectives
  - Circumstances and characteristics of violator
  - Adequacy of violator's OFAC compliance program
  - Remedial response

U.S. Department of Treasury, OFAC

- Recommendations
  - Get a Data Security Attorney if you experience a ransomware attack
  - Contact OFAC if a Banned Person or Entity is involved
  - Engage law enforcement
- OFAC considers full and timely cooperation with law enforcement as a significant mitigating factor when evaluating sanctions

Minimum prevention measures

User Education

Password Complexity

Firewalls

Back-up key systems and databases

Patching

Where does insurance fit?

- Cyber insurance must act like other lines of business even if the loss behavior is fundamentally different. In this case, bad actors are **intentionally and actively** trying to cause harm.

- An organization can invest in **better security** and look to keep a lower premium.

VRSA Incidents

- City: The payroll department received an email from a city employee to change their direct deposit banking information The payroll dept complied
- Water/Wastewater Authority: Member received fraudulent instructions to wire funds to a Bank of America account. The funds were inadvertently wired on that day.
- Town: Member released funds for employee pay based on fraudulent email communication.
- Town: Employees W2s were inadvertently sent to other current/former employees

VRSA Incidents

- Water/Wastewater Authority: Member received a request to update ACH information for a general contractor. Transfer took place on August 1st. It was discovered to have been to a fraudulent account on August 2nd.
- County: We received a fraudulent email from a vendor requesting that we change their payment information to an EFT. We issued payment this fraudulent account.
- Town: Email security breach. Payer was sent incorrect wiring instructions appearing that it came from my email. Funds were wired to fraudulent account.


ANY
QUESTIONS ?