2023 NJSBA Fall Conference

Lessons Learned from a Ransomware Incident

We hear about destructive ransomware in the news almost daily, with major organizations suffering from debilitating ransomware attacks. This program goes into an actual ransomware incidents and steps that were taken to recover from those incidents, both organizationally and technologically. The speakers will discuss what we can all learn that can help us protect against attacks, and what to do to recover when the worst happens.

Moderator/Speaker:
Karen Painter Randall, Esq.
Chair, Cybersecurity, Data Privacy and Incident Response Group
Connell Foley, LLP, Roseland

Speakers:
Chris Ballod
Managing Director, Cyber Risk
Kroll Associates, Inc.
Chadwick G. Shroy
Cybersecurity Advisor | Region 2: NY, NJ, PR and USVI Cybersecurity & Infrastructure Security Agency (CISA)
Don Wyper, COO
Digital Mint

CONNELL FOLEY

A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Lessons Learned from a Ransomware Attack

The NJSBA Fall Conference

November 20, 2023

Speakers:

Moderator

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Karen P. Randall

Chair, Cybersecurity, Data Privacy and Incident Response Group

Connell Foley LLP

Panelists

KROLL

Christopher Ballod

Managing Director, Cyber Risk

Kroll

Arch | Insurance

Rich Gatz

Vice President, Head of Cyber Claims

Arch Insurance Group, Inc.

digital mint

Angelo Martino

Managing Director, Cyber Incident Response

DigitalMint Cyber

CISA
CYBER+INFRASTRUCTURE

Chadwick G. Shroy

Cybersecurity Advisor | Region 2: NY, NJ, PR and USVI

Cybersecurity & Infrastructure Security Agency (CISA)

AGENDA

1. **2023 Cybersecurity Landscape**
2. **Ransomware Discussion**
    a. Evolving Ransomware Attacks
    b. Ransomware Statistics
3. **Responding to a Ransomware Attack**
    a. Initial Response
    b. To Pay or Not to Pay the Ransom
    c. Communications Strategy
    d. Lessons Learned
4. **Ransomware Tabletop Exercise**
5. **Best Practices**

Upfront with CISA

- Cybersecurity Infrastructure and Security Agency's expanding role
- Attacks Spurring Administration and Congress to Act
- Available CISA resources

CISA Resources

CYBERSECURITY RESOURCES

- CISA Ransomware Guide
- Telework Resources – Telework Guidance and Best Practices
- Cybersecurity Hub – Assessments, Prevention, and Response Resources
- Cyber Essentials – Cybersecurity Awareness and Best Practices Resources
- Cyber Essentials Toolkits – Action Items for IT and C-suite Leadership

SMALL BUSINESS RESOURCES

- FCC Cybersecurity Planning Gui
- DHS Cybersecurity Overview
- Social Media Guide
- Cybersecurity While Traveling
- Protect Your Workplace Material

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

SHIELDS UP

- Warnings issued addressing increased cyber risks arising out of the geopolitical conflict
- Guidance for Organizations
  - Reduce the likelihood of a damaging cyber intrusion
  - Take steps to quickly detect a potential intrusion
  - Ensure that the organization is prepared to respond if an intrusion occurs
  - Maximize the organization's resilience to a destructive cyber incident
- Guidance for C-Suite and Leadership
  - Empower Chief Information Security Officers (CISO)
  - Lower Reporting Thresholds
  - Participate in a Test of Response Plans
  - Focus on Continuity
  - Plan for the Worst

SHIELDS UP

- Recommendations for how to respond to a Ransomware Event
  - Determine which systems were impacted, and immediately isolate them.
  - Disconnect devices from the network or power them down to avoid further spread of the virus.
  - Triage impacted systems for restoration and recovery.
  - Consult with incident response team to develop and document an initial analysis of the event.
  - Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
  - Take a system image and memory capture of a sample of affected devices
  - Consult federal law enforcement regarding possible decryptors available

White House Guidance: Act Now to Protect Against Potential Cyberattacks

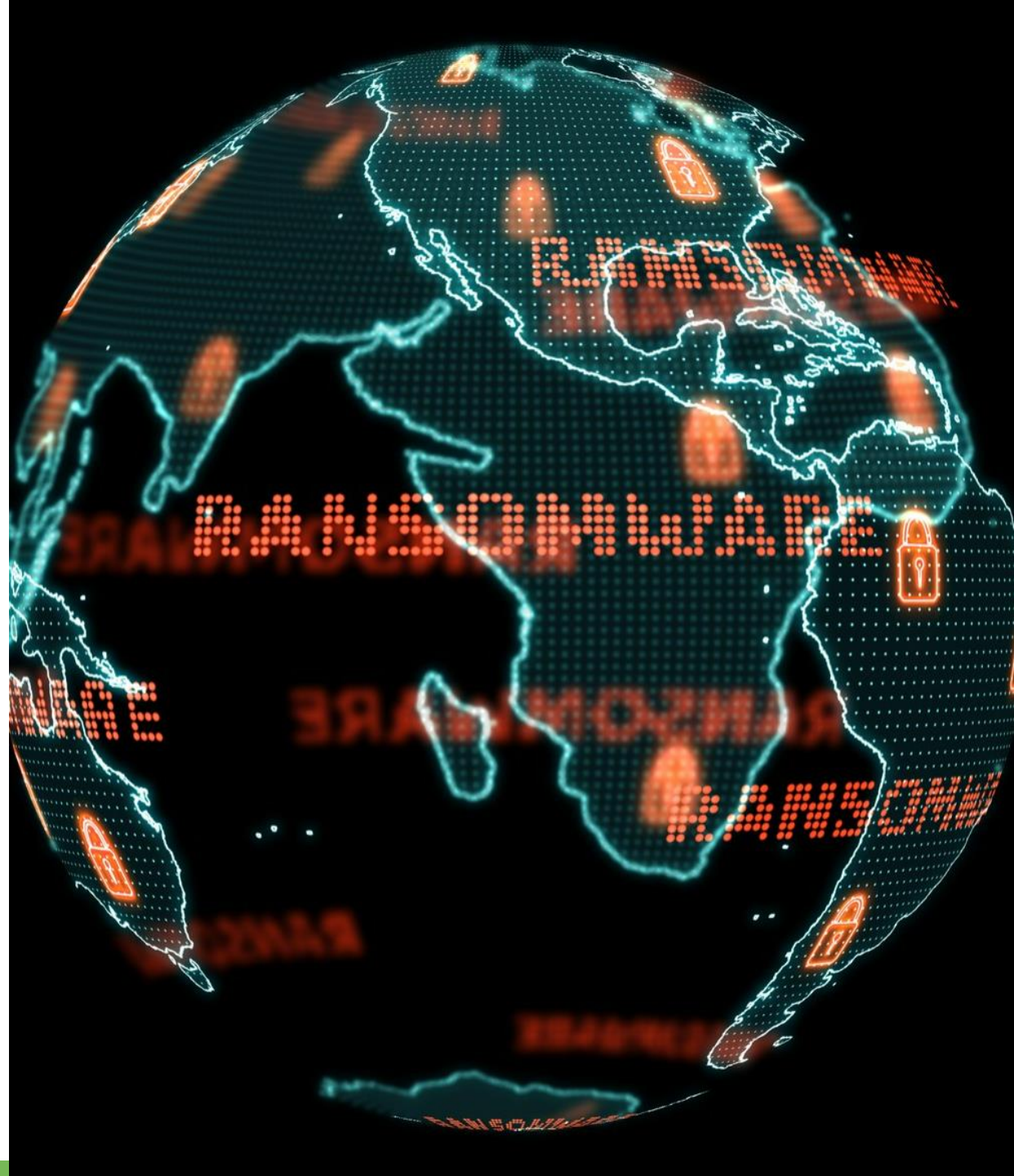
- Companies continue to be warned about potential cyberattacks and receive recommendations to adopt the following with urgency:

1. Mandate the use of multi-factor authentication
2. Deploy modern security tools on your computers and devices
3. Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks
4. Back up your data and ensure you have offline backups beyond the reach of malicious actors
5. Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack
6. Encrypt your data so it cannot be used if it is stolen
7. Educate your employees to common tactics that attackers will use over email or through websites
8. Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents

Evolving Ransomware Attacks

What Is Ransomware?

- Form of malware
- Encrypts victim's data and/or system
- Demands payment for decryption
- Numerous iterations
- One infected user can ***SHUT DOWN*** an entire organization
- Uses social engineering by sending employees suspicious emails with invoices or business documents most will likely open



The Ransom Note

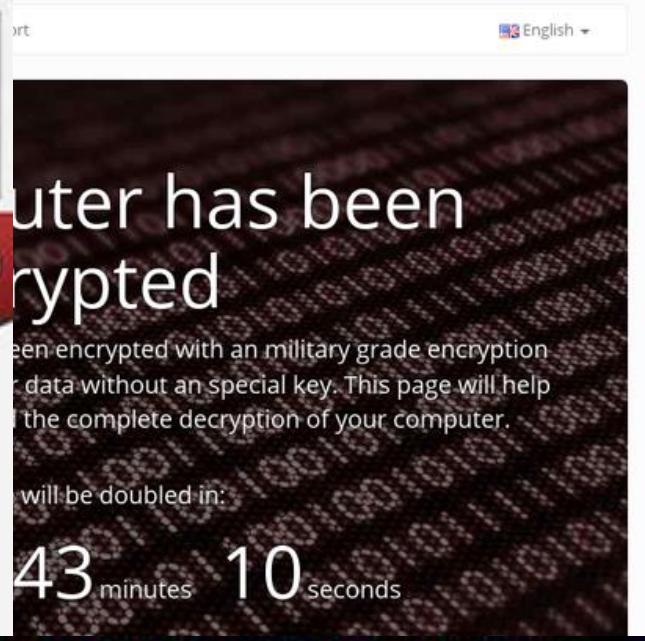
- Once deployed, the ransomware generates a “Ransom Note” on the infected system providing:
  - Information about victim’s computer
  - Cost to decrypt
  - Deadlines
  - Instructions for payment
  - Identification of threat actor group
  - Contact information
- Ransom Note “Themes”
  - Movies and TV Shows
  - Federal Agencies (FBI, CIA)

A Ransom Note inspired by the TV Show “Breaking Bad”

Source: KnowBe4, “Heads-up: 'Breaking Bad' Ransomware Beta Tested Down Under”


Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/8/2013
5:52 PM
Time left
56 : 16 : 12


United States
THIS COMPUTER HAS BEEN BLOCKED
HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.
Article 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)
Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)
computer you are obliged to pay a fine of $300.
must pay the fine through MoneyPak.
Pay Mon
Pick up a MoneyPak and purchase it with cash at the register


English
uter has been
rypted
een encrypted with an military grade encryption
data without an special key. This page will help
the complete decryption of your computer.
will be doubled in:
43 minutes
10 seconds


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
OK
MoneyPak
Where I can buy MoneyPak?
Walmart
Walgreens
RITE AID
CVS pharmacy
kmart


Your personal files are encrypted by CTB-Locker.
Your personal files are encrypted by CTB-Locker.
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.
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' for the next page.
View
95 59 22
Next >>

Why Are Threat Actors Using Ransomware?

- High success rate and visibility
- Simple
- Ransom is paid
- Payment is typically made with Cryptocurrency or Bitcoin
- Commoditization of malware
- Do-it-yourself ransomware kits
- Publicity

What are the Crown Jewels?

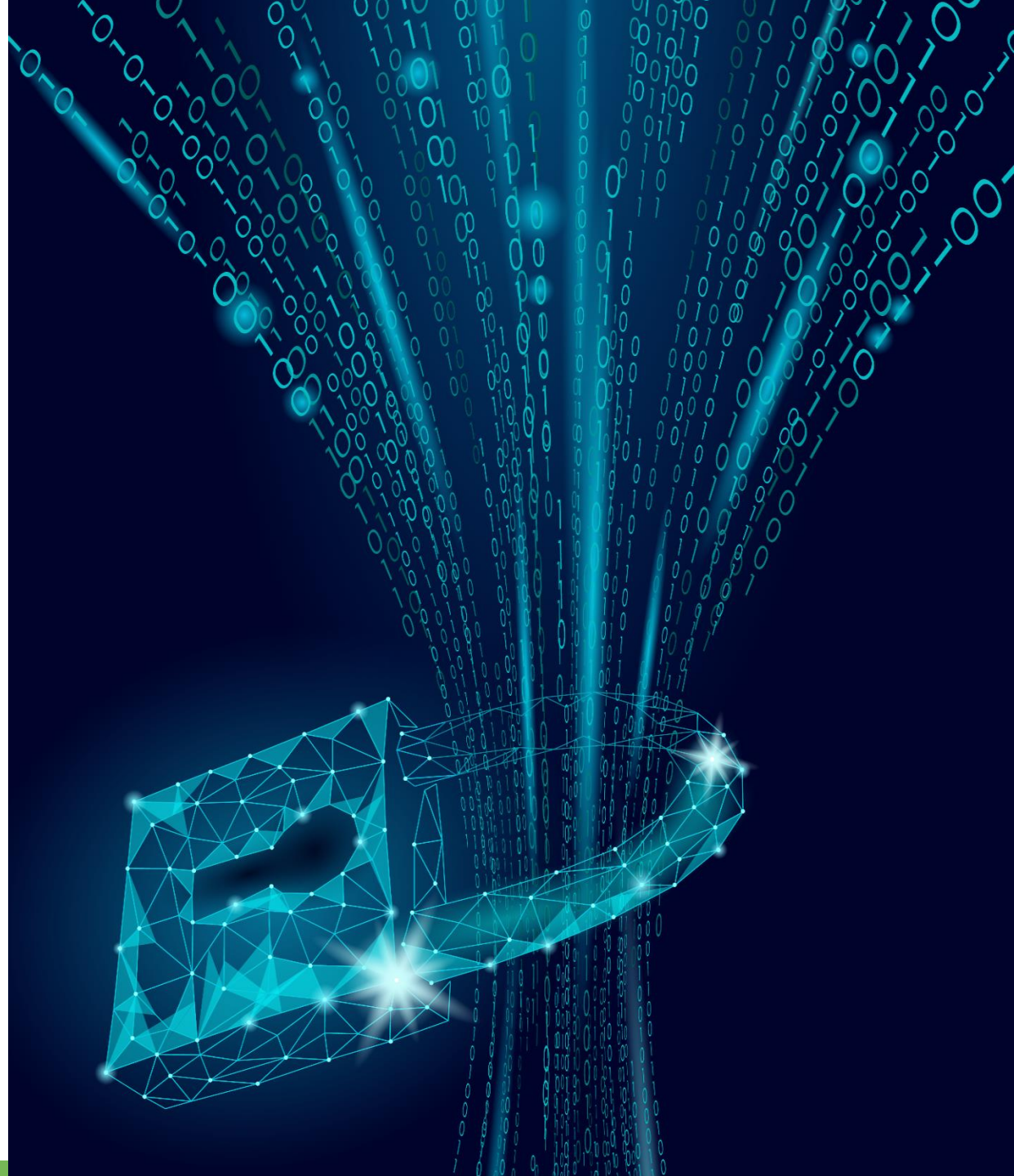
- Personally Identifiable Information, or PII varies from state to state, but may include:
  - Social Security Number
  - Date of Birth
  - Bank Account/Financial Account/
    - Credit Card Number (PCI)
  - Email Address
  - Biometric Data
  - Employee Identification Number
- Personal Health Information, or PHI
  - Demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care

Crown Jewels Model

- **Old Model**: Cybercriminal hacks into an organization's network and takes its crown jewels—data that had some measure of value on the cyber black market, i.e., the DarkNet.
  - The bad guy then monetizes this crime by selling the data on the DarkNet to someone who would use it for fraudulent purposes to also make money.
  - The profit was in stealing data and so data has to be worth something to make it profitable for the bad guy.
- **Myth**: If enterprise does not have crown jewels…it will not be a target for hackers.

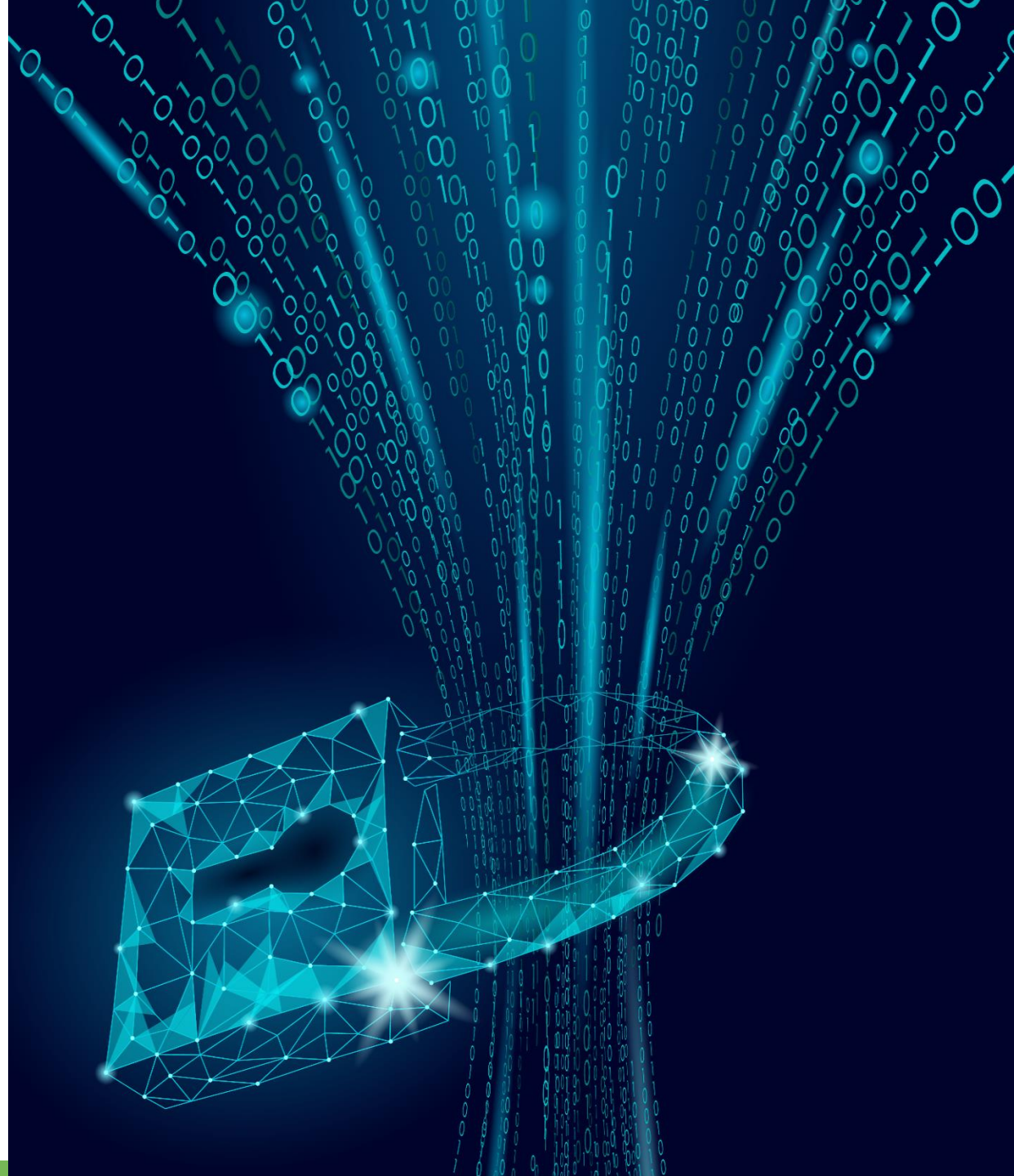
Double Extortion Model

- Hackers are now targeting the organization's back-up systems first in order to cripple the ability to retrieve critical data and remediate the system without paying the ransom.
- Cybercriminals are threatening to post sensitive and embarrassing exfiltrated information on leak sites if they do not receive the ransom payment and may even auction off the data.
- Ex: The Grubman Law Firm



Triple Extortion Model

- Some threat actor groups hire affiliates to call the organization victimized by the attack to encourage them to make payment for decryption tool or to prevent publication.
- DoppelPaymer ransomware victims were called by hackers, post-infection.
  - In one instance, the attacker used a spoofed US-based telephone number while claiming to be located in North Korea, threatened to leak or sell data from an identified business if the business did not pay the ransom.
- Re-attacks - DDoS

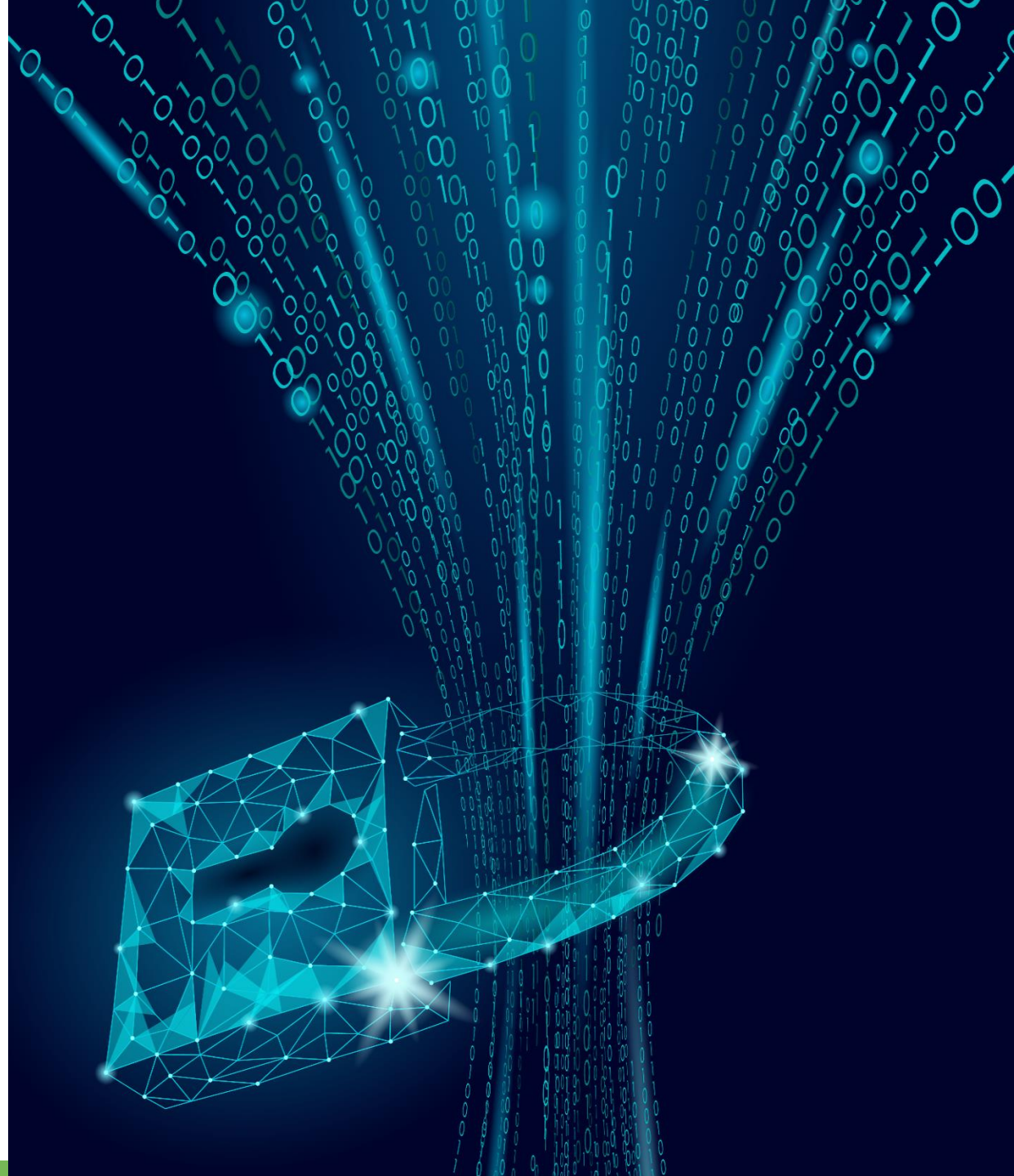


Quadruple Extortion Model

- Increasingly aggressive tactics
- Encryption, Data theft, DDoS and Harassment involving employees, business customers/clients and calls media to inform them of hack.
- Re-attacks – DDoS to shut down public websites

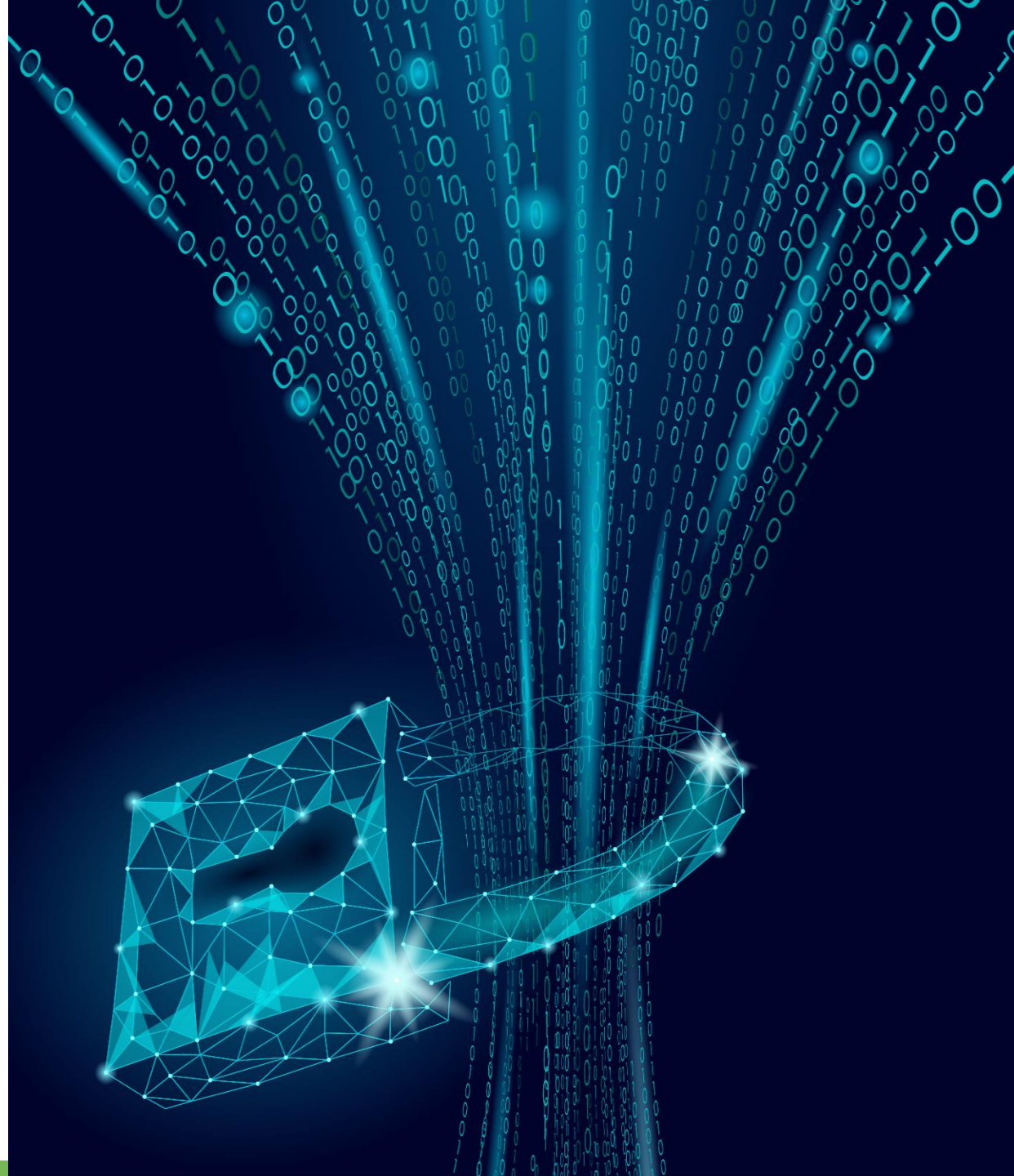
Examples:

- Grief Gang (REvil affiliate) and the Ragnar Locker ransomware group issuing memos notifying victims to keep the negotiation between them “or else”



Quintuple Extortion Model

- Conti has changed its business model…less work…greater return.
- No encryption
- Rather than doxing exfiltrated information, it is offering it to interested buyers – so even if the ransom isn't paid, the criminals still make a profit.



REWARD

OF UP TO

$10,000,000.00 USD

FOR INFORMATION LEADING TO THE LOCATION, ARREST, AND/OR CONVICTION OF OWNERS/OPERATORS/AFFILIATES OF THE

Conti

Ransomware Group

SUBMIT TIPS VIA TELEPHONE OR WEBPAGE:

Follow-on contacts to be established through WhatsApp, Telegram, Signal, or other platform of reporting party's choosing

1-800-CALL FBI (1-800-225-5324) **https://tips.fbi.gov**

Increase in Ransomware Damage Costs

The collateral costs of a ransomware attack include:

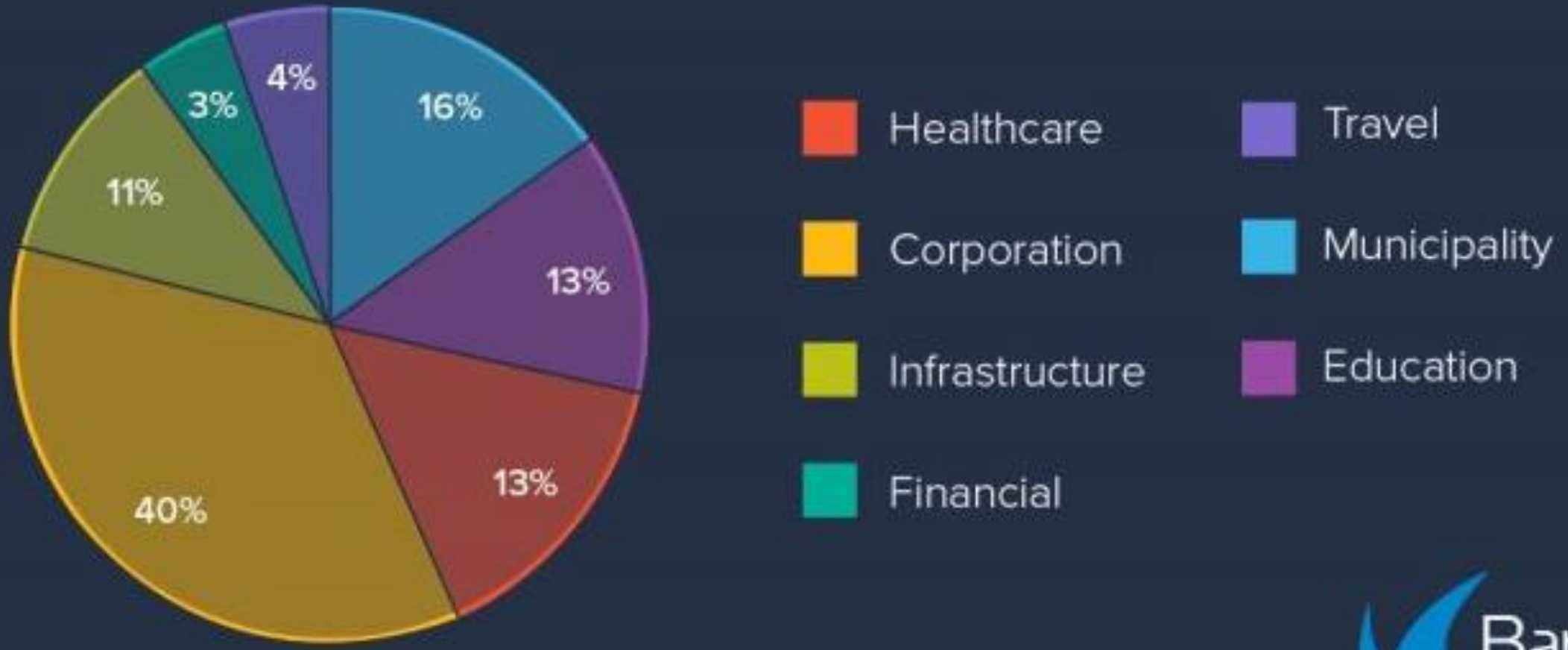
- Damage and destruction (or loss) of data
- Downtime
- Lost productivity
- Post-attack disruption to business
- Forensic investigation
- Restoration and deletion of hostage data and systems
- Reputational harm
- Employee training in direct response to attack
- Global spending on security awareness training for employees predicted to be $10 billion in 2027

Ransomware Statistics

Ransomware attacks by country

Source: Barracuda

Ransomware attacks by industry



Barracuda.
Your journey, secured.

Source: Barracuda

Ransom Payment Increases in Q3 2023

AVERAGE RANSOM PAYMENT

$850,700

+15% from Q2 2023

INREASE OF VICTIMS WHO PAY

34% in Q2 to 41% in Q3

Source: *Coveware*, *"Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting"*

ATTACK VECTORS
TOP 3 RANSOMWARE TYPES

1. RDP Compromise
2. Email Phishing
3. Software Vulnerability

MOST COMMON RANSOMWARE VARIANTS IN Q3

1. AKIRA
2. BLACKCAT
3. RHYSIDA
4. LOCKBIT 3.0
5. CLOP

Source: *Coveware*, "*Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting*"

Responding to a Ransomware Attack

The First 72 Hours May Be the Most Crucial!

- Containing an intrusion before it reaches systems PII or PHI may stop a data breach from ever occurring
- Limit the economic/reputational harm
- Limit legal liability and ethics complaints
- Maintain employee morale
- Forestall regulatory scrutiny
- Placing broker/carrier on notice

The First Four Steps

- **Step 1:** Don’t Panic, Assemble the Incident Response Team
- **Step 2:** Containment and Eradication
- **Step 3:** Determine Scope of Compromise/Encryption
- **Step 4:** Determine Strain of Ransomware

Step 5: Evolving Response Options

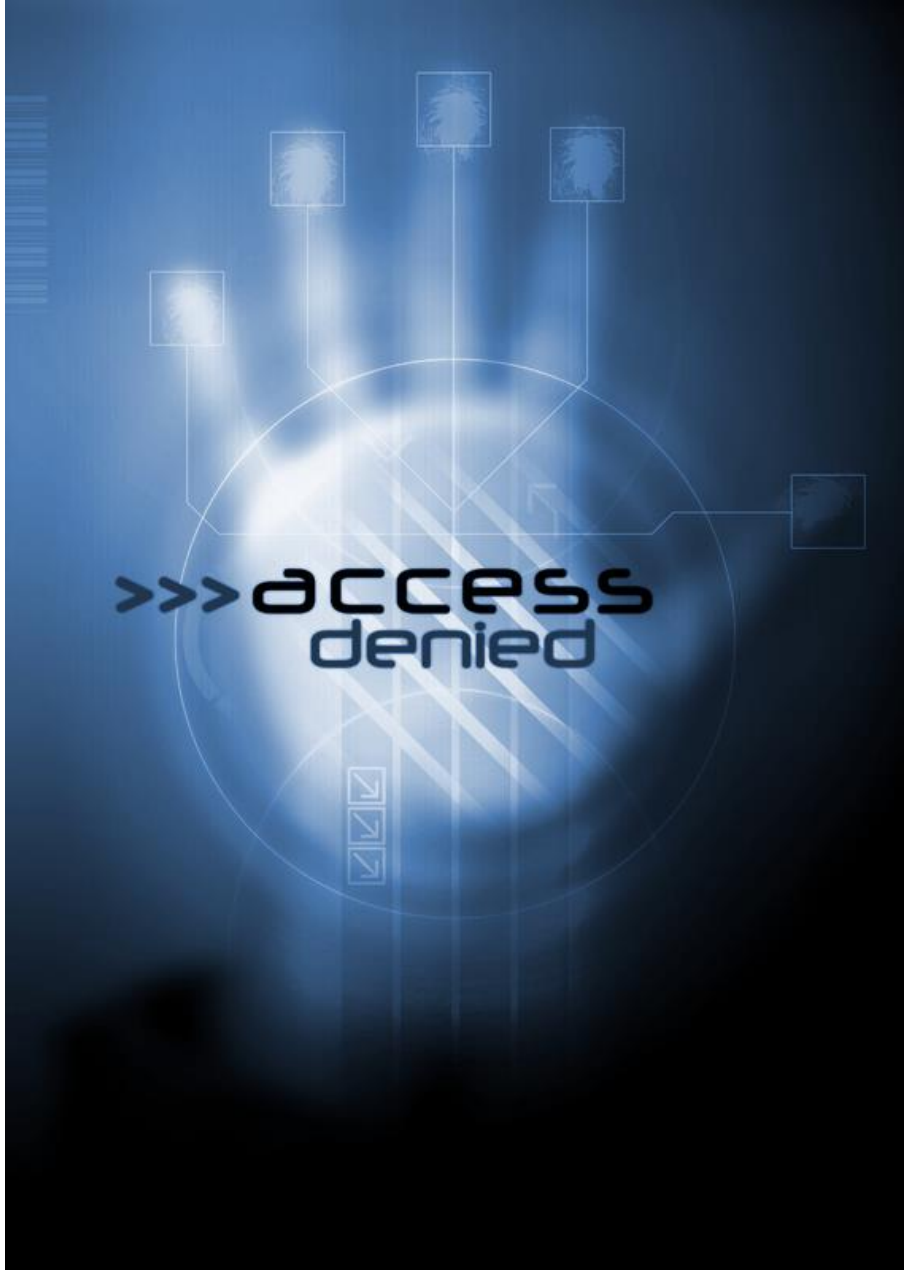
After identifying scope and strain, the following are four basic responses to a ransomware attack

- **Option 1:** Restore Files from a Backup
- **Option 2:** Try to Decrypt
- **Option 3:** Do Nothing and Lose Data
- **Option 4:** Negotiate and/or Pay the Ransom


To Pay or Not to Pay

To Pay or Not to Pay

- Is the decision becoming more difficult and why?
- Does making a decision during the incident response effort impact negotiations and decision to pay a ransom?
- What is client advice when considering paying?
- Are attackers willing to still negotiate?
- Hospitals and Patient Safety Considerations



Factors to Consider Before Paying a Ransom

- Both the FBI and U.S. Conference of Mayors recommend against making a payment.
- Legal due diligence is mandatory
- Reporting requirements
- U.S. Treasury Department / Office of Foreign Asset Control
- Should you engage in negotiations if you have no intention of paying the ransom?

Factors to Consider Before Paying a Ransom

- Is there backup (test restore)?
- Is time on your side?
- Is Incident Response Team deployed?
- Has cyber liability carrier been contacted?

Factors to Consider Before Paying a Ransom

Other considerations:

- Reputation of attacker to follow through on promise to return data and restore access. What is default rate? (Conti).
- Is ransom payment covered by insurance?
- $10,000 deductible versus hours of time, money, and resources to rebuild system.
- Will the decrypted files be corrupted?
- Has integrity of data been harmed?
- Will data be posted to a leak site?

OFAC – Sanctions Concerns

- On October 1, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issued an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments.
- Companies that engage with victims of ransomware attacks - cyber insurance, digital forensics and incident response as well as financial services providers that may be involved in processing ransom payments, must account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction…ex) Iran
- Civil penalties for sanctions violations based upon strict liability
- Cooperation with law enforcement and compliance are considered substantial mitigating factors.
- Companies must carefully consider all advantages and implications before paying a sanctioned entity and engaging with government authorities, including OFAC and DOJ.

OFAC – Sanctions Concerns

- How do you know if a ransomware threat actor group is on the OFAC Sanctions list?

https://sanctionssearch.ofac.treas.gov/

Sanctions List Search

This Sanctions List Search application ("Sanctions List Search") is designed to facilitate the use of the Specially Designated Nationals and Blocked Persons list ("SDN List") and other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions, the Non-SDN Palestinian Legislative Council List, the Non-SDN Menu-Based Sanctions List, and the Non-SDN Communist Chinese Military Companies List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. To aid users of the tool, Sanctions List Search contains a feature entitled "Minimum Name Score" that functions on a sliding scale, allowing for a user to set a threshold (i.e., a fuzziness rating) for the closeness of any potential match returned as a result of a user's search. This feature enables Sanctions List Search to detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

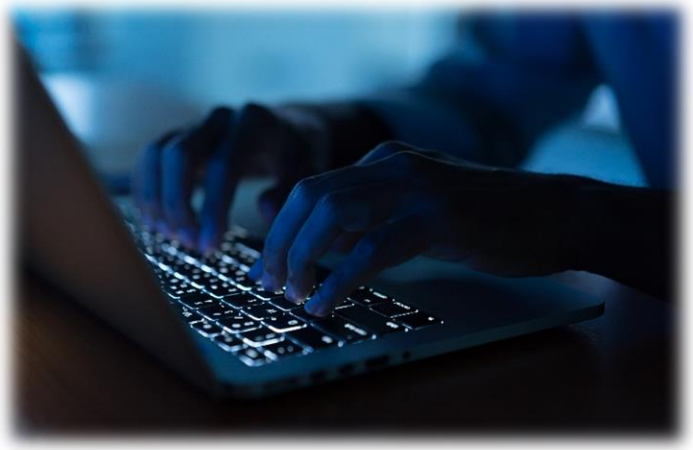
Download the Consolidated Non-SDN List | Program Code Key

Sample Negotiation with Threat Actor

- We are here to discuss our files on the website. What is price to reach an agreement?
- Price for you is 11btc. You need to pay this amount and we will give you decrypt tool for all your machines, security report on how you were hacked, file tree on what we have downloaded from your network and wiping log of that information. Take into consideration that we have downloaded a lot of data from your network that in case of not payment will be published on public news website and sold on the black-markets. Were move it after payment and wiping log is provided as well. To start a business we offer you to make payment in two stages. What amount you can pay today?
- Is there anyway that we can see what you stole from us? We are nervous about what may have been taken, so we would appreciate if you can show us.
- Part of it you could check here…the rest, more valuable part is preparing for selling.
- We would like to discuss a deal. Can you remove this post from the website while we are coming to an agreement?
- We told you the price. If you agree to pay it today, we will remove the data and stop selling process. The price will increase on Monday.

Escalating Negotiations With Threat Actor

- Time is enough for you. After this time we don't talk with you any more. We're busy. We'll send all information to parents' email and say you're children are in danger
- I told you if you emailed anybody, the deal was off…who did you email?
- We sent emails to 3 parents and 3 employees but it is not end, so we are asking you about payment so what? Pay or not?
- I told you if you emailed any body there would be no deal. Then you did it anyway. If you want to regain our trust, you need to send us more proof of files that you have from the network
- Ok. Wait for our counterattack.
- You have a strange way of trying to get us to pay. Attacking, emailing our people. None of this increases our belief that you can be trusted. Your choice i guess.



Ransomware's Impact on Cyber Insurance

- Ransomware attacks are affecting the cyber liability insurance factors on multiple levels

Rising Cost of Insurance

Co-Insurance

Sublimits

Business Interruption

Exclusions/ Endorsements

Impact of Cyber Insurance on Cyber Compliance

- Cyber insurance is driving improvements to cyber defenses: companies find that obtaining cyber insurance, and lowering the premium for their cyber coverage, requires taking proactive measures to improve their cybersecurity

- 64% have implemented new technologies or services
- 56% have increased staff training & education activities
- 52% have changed processes and behaviors

Source: Sophos: The State of Ransomware 2022

Notification and Lessons Learned

Notification & Lesson Learned

Post-Incident Activity

- **Notification** – to individuals, entities, state/federal agencies
  - The IR Team must determine (1) who is entitled to notification and (2) what are the notification deadlines
- **De-Brief and Lessons Learned**
  - Prevent Future Breaches and Data Security Incidents
  - Make necessary updates to the Incident Response Plan
  - “Repeat offenders” are more likely to be the subject of government investigations, and resulting penalties

Reporting Internet-Related Crime

Victims of ransomware should consider reporting the attack immediately to CISA at www.us-cert.gov/report, a local FBI Field Office, or Secret Service Field Office.

- FBI local office – fbi.gov/contact-us/field-offices/field-offices
- U.S. Secret Service - secretservice.gov/contact/field-offices
- Internet Crime Complaint Center - ic3.gov
- Department of Homeland Security's National Infrastructure Coordinating Center: (202) 282-9201 (report incidents relating to national security and infrastructure issues)
- U.S. Computer Emergency Readiness Team (U.S. CERT) (online reporting for technicians)

Ransomware Tabletop Exercise

RANSOMWARE ATTACK EXERCISE

CONNELL FOLEY

SCENARIO

Your law firm just won a multimillion dollar class action lawsuit. The press and new clients are contacting the firm nonstop, and your Managing Partner was even featured in a segment on Bloomberg News.

This victory has boosted your brand and reputation, but it has also alerted many cybercriminals to the firm's financial success. As a result, staff and attorneys alike have been targeted with phishing emails, some even generated by AI/CHATGPT. On one late Friday afternoon of a holiday weekend, the COO's assistant clicked on a phishing email in the COO's email account, introducing malware. Over the weekend, unbeknownst to the firm, the attack spread laterally.

On Tuesday, upon arriving at the office after a holiday weekend, the Managing Partner found all online systems locked down. IT and staff sat idly at their computers staring at a message from the threat actor. The hacker's message proffered that they had accessed and exfiltrated sensitive and confidential client data including internal attorney client strategic memos about the class action lawsuit and even the firm's Cyber/Tech E&O policy information. Workforce data was also at risk. The bad actor stated that if the $40 million ransom demand was not paid in three days the group would start a DDoS campaign against the company, harassment of employees via calls/text/email, and publicly post the highly sensitive and confidential information on the Dark Web. Moreover, the information will be publicly leaked to the media, clients, bar association and competitors.

How does your firm respond?

KAREN PAINTER RANDALL
Partner and Certified Civil Trial Attorney
Chair, Cybersecurity, Data Privacy and Incident Response
krandall@connellfoley.com I 973.840.2423

24/7 Data Breach Response Hotline
Phone: 973.840.2500
Email: breachresponse@connellfoley.com

Best Practices

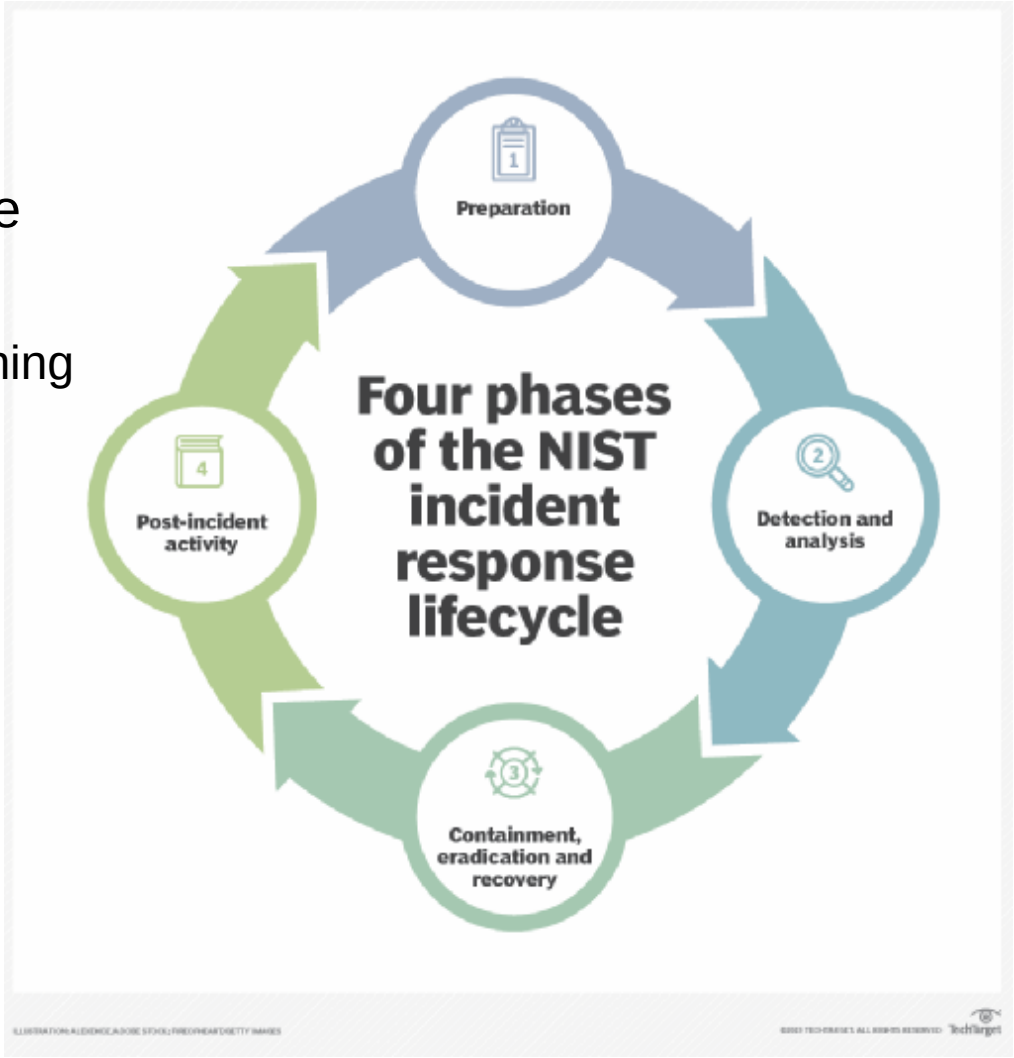
Best Practices

- Backup critical data and test restore from secure backup.
- Prepare and maintain inventory of hardware and software assets
- Implement security awareness training with simulated phishing attacks.
- Have strong access controls especially in remote environment.
- Use multifactor authentication.
- Smart passwords
- End-to-end encryption
- Patch management. (Follow Microsoft patch Tuesdays).
- Review all policies of insurance and procure a standalone cyber liability policy that best fits coverage needs, including ransomware and business interruption.
- EDR to protect against potential malicious endpoint activity.
- Incident Response Plan, Incident Response Team, Tabletop Exercises
- Vet and manage third-party vendors to transfer risk. Vendor Agreements are essential.

Follow a Ransomware Framework and Resources

National Institute of Standards and Technology (NIST)

- **Example:** NIST Computer Security Incident Handling Guide
  - Organize your Incident Response Capability
    1. Establish the need for an Incident Response Plan (obtaining "buy-in" from C-Suite, Board and other stakeholders)
    2. Define events v. incidents
    3. Designate the Incident Response Team
    4. Create a Comprehensive Incident Response Plan
  - Handling an Incident
    1. Preparation
    2. Detection and Analysis
    3. Containment, Eradication, and Recovery
    4. Post-Incident Activity



Follow a Ransomware Framework and Resources

CISA Resource:

- CISA has released its first CISA Insights products, which discusses the rapid emergence of ransomware across our Nation's networks.
- Helping organizations protect themselves from ransomware is a chief priority for CISA. Organizations are encouraged to review the following resources to help prevent, mitigate, and recover against ransomware:
- CISA Ransomware Guide - https://www.cisa.gov/stopransomware/ransomware-guide

Final Thoughts

“If you’re not doing scans and penetration tests, then just know that someone else is. And they don’t work for you.”

- George Grachis, Senior Consultant, Maxis360 - 2016