

Ransomware 4.0

2024 Threat Response - a Legal Perspective

► Presented by: **John Pilch**

Woods Rogers

August 15, 2024





Agenda

1. Introduction
 2. Ransomware Evolution
 3. Incident Response Models
 4. Ransomware Walk–Through
 5. Questions
- 

Ransomware Evolution



Ransomware 1.0

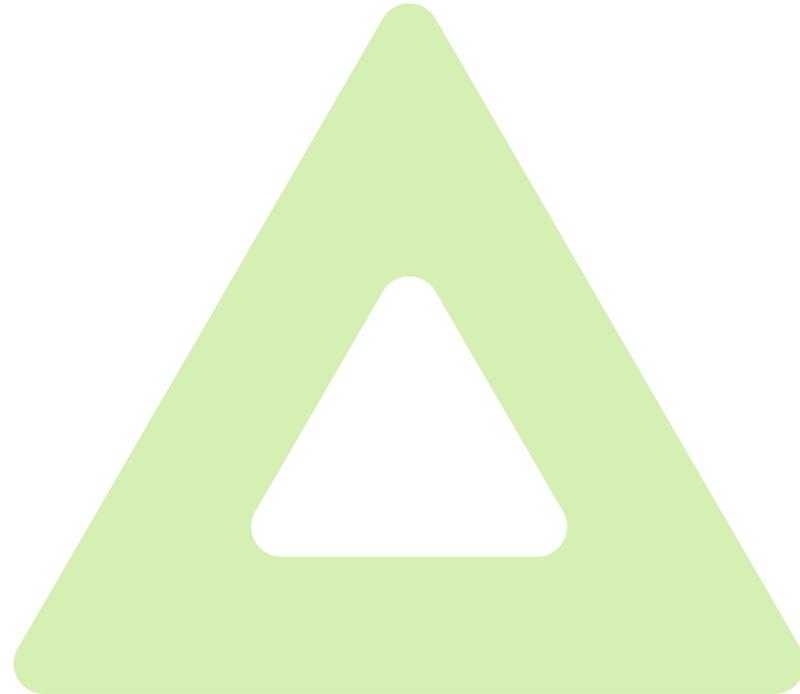
- Encryption
- Extortion - \$ for decryption key
- Countermeasures
 - Backups - hardware, software, data
 - Network segmentation

Ransomware 2.0

- Encryption + Data Theft
- Extortion - \$ or we publish the data
- Countermeasures
 - Notification
 - Data Inventory
 - Knowledge of Connections
 - Logs

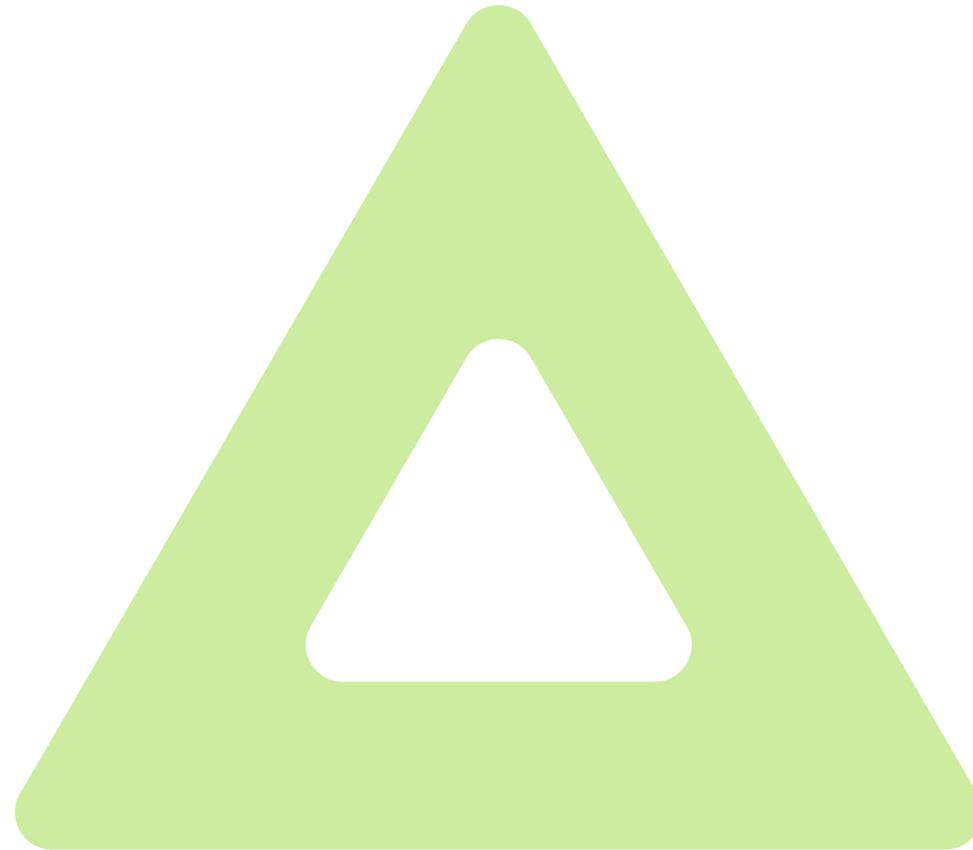
▶ Ransomware 3.0

- Encryption + Data Theft + Data Subject Contact

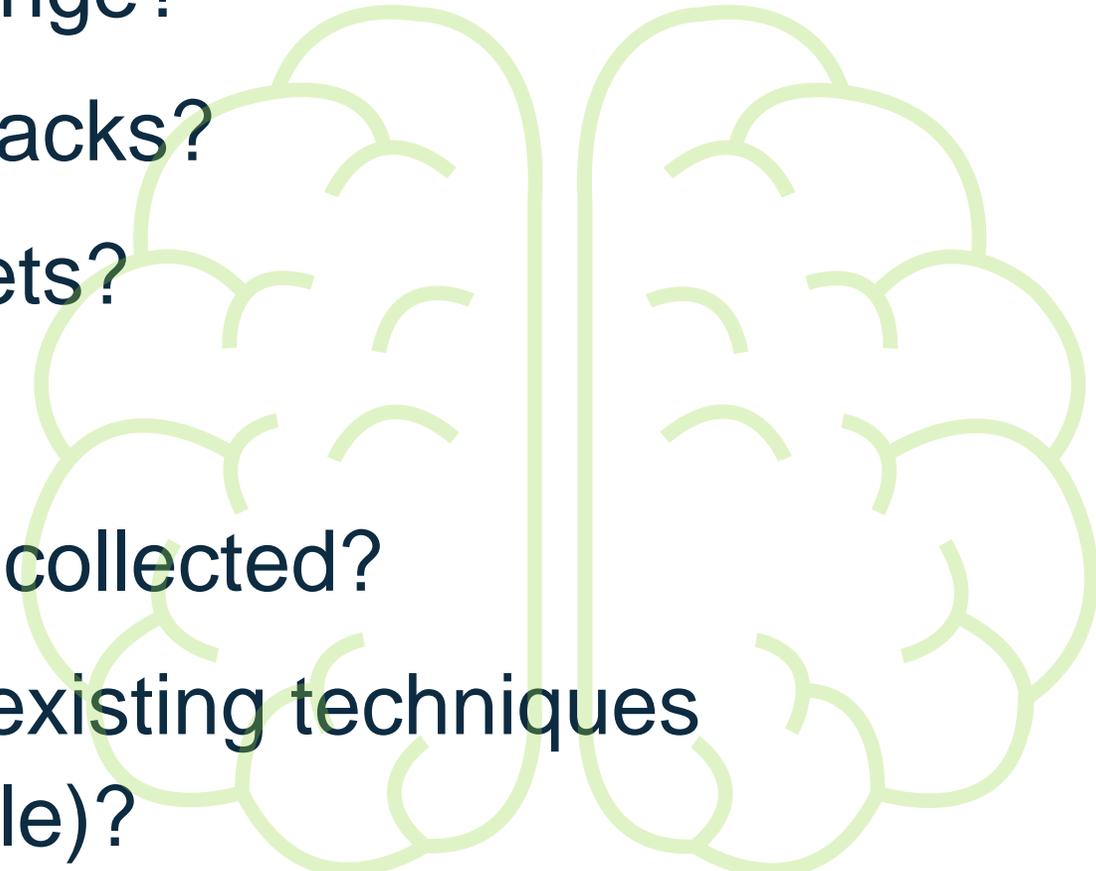


▶ Ransomware 4.0

- Encryption + Data Theft + Contact Supply Chain



Ransomware – AI?

- How would extortion model change?
 - Improve ability to conduct attacks?
 - Improve ability to select targets?
 - Improve auction outcomes?
 - How would training data set be collected?
 - How would results compare to existing techniques (regression analysis, for example)?
 - Stay tuned
- 

Incident Response Models



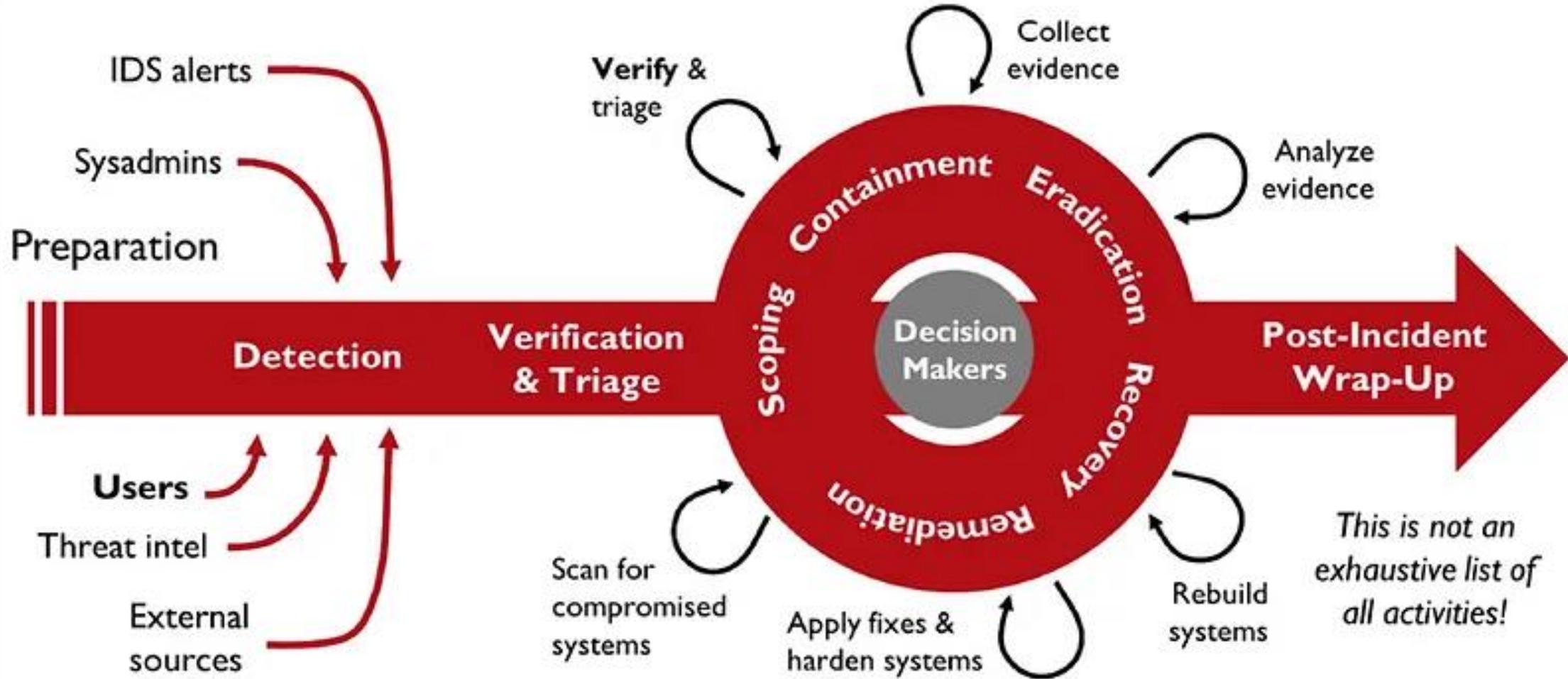
Classic Model - PICERL



NIST Model



Dynamic Approach to Incident Response (DAIR)



Preparation

- Backups, Network Segmentation, Data Inventory, Logging
- Identifying the IR team
- Cyberinsurance and external support
- Testing, Training, Exercising

Ransomware Walk-Through



The Beginning

Inc. Ransomware

We have hacked you and downloaded all confidential data of your company and its clients. It can be spread out to people and media. Your reputation will be ruined. Do not hesitate and save your business.

Please, contact us via:

[REDACTED] n/

Your personal ID:

[REDACTED]

We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come of it.

Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:

[REDACTED]

You should be informed, in our business reputation - is a basic condition of the success.

Inc provides a deal. After successful negotiations you will be provided:

1. Decryption assistance;
2. Initial access;
3. How to secure your network;
4. Evidence of deletion of internal documents.

Saturday	
1:48AM	Encryption event occurs.
6:30AM	CIO is notified of the incident and incident response plan engaged.
6:49AM	CIO calls outside cybersecurity counsel Beth Waller on personal cell, waking her up.
6:52AM	While on call with client, Waller Signal messages Mandiant leads requesting forensic support.
7:00AM	Waller also emails Mandiant inbounds mailbox. Convenes internal IR team.
7:16AM	Mandiant's IR team covering early operations in Belgium responded directly via phone call to Waller and began triaging the incident from Europe until East Coast team goes online at 9AM.
7:44AM	Call with insurance broker notifying broker of incident and requesting direct contact for insurance carrier.
8:41AM	Initial claim email sent reporting claim, notifying insurance carrier of event and requesting approval of engagement of vendors.
9:00AM	Forensic meeting with counsel and Mandiant. Begin implementing second EDR tool in environment. Continued technical syncs run in parallel throughout the day.
10:20AM	FBI (RVA Cyber) notified directly about the incident, with a request for threat intelligence regarding Royal.
10:41AM	Threat actor negotiation firm engaged officially.
12:48PM	Engaged FTI Consulting's Cyber Crisis Publication Relations team.
1:15PM	FBI (RVA Cyber) provides initial threat indicators for Royal from FBI Field Office in charge of Royal investigations.
2:00PM	Initial meeting with Crisis PR and client.
2:30PM	Initial meeting with Threat Negotiation Firm to discuss response strategy.
3:00PM	All hands meeting. Call simultaneously with Chubb for clearance on approvals for formal engagements.
4:00PM	Executive leadership meeting / discussion of strategy and scope of incident. Board notified.
6:00PM	CEO authorizes engagement of additional remediation team to increase boots on the ground, flights booked for that evening for remediation specialists to arrive in multiple time zones simultaneously.
9:00PM	Executive leadership call regarding materiality.

Privilege Considerations



Attorney Client Privilege

Communication made in confidence for the predominant purpose of obtaining legal advice from a lawyer.



Work Product Doctrine

Information prepared in anticipation of litigation, at the direction of an attorney.

Privilege

WAIVER

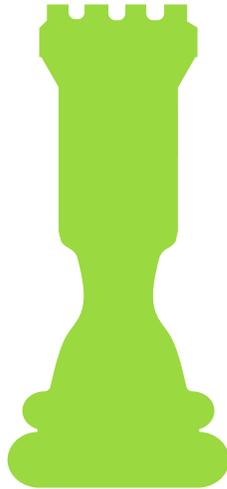
Be attuned to forwarding communications outside of the "Circle of Trust"



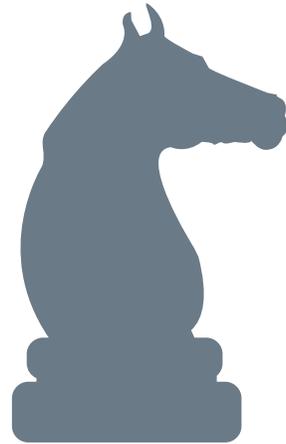
MAINTAIN PRIVILEGE

Keep communications with counsel.

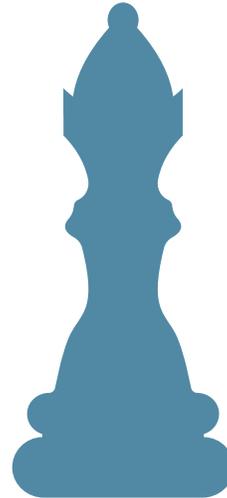
The Incident Response Chessboard



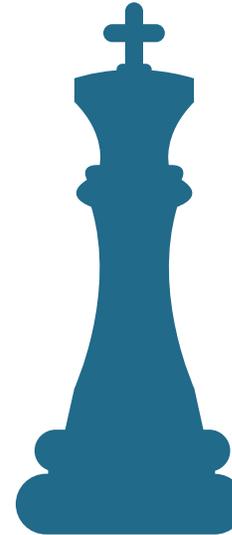
**OUTMANUEVER
THREAT ACTOR/
SHAM ENGAGEMENT
TO SHUT DOWN
FOOTHOLD**



**CRISIS
COMMUNICATIONS**



**WORK WITH
LAW ENFORCEMENT
(INCLUDING
MANDATORY REPORTS) +
DECISION ON EMERGENCY
PROCLAMATION**

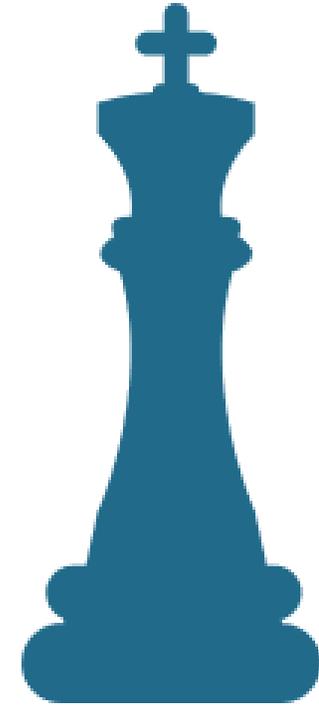


**REBUILD / RESTORE
YOUR
ENVIRONMENT**



**NOTIFY IMPACTED
CONSTITUENTS**

- Contain and eradicate malware
- Use EDR to monitor environment 24/7
- Restore services and data



**REBUILD / RESTORE
YOUR
ENVIRONMENT**

- Collect logs, images, and other artifacts
- Forensics team investigates
- What happened?
- What data was affected?



**NOTIFY IMPACTED
CONSTITUENTS**

Virginia's General Breach Statute

§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.



Notification

- Usually by mail
 - Required contents
 - Who to notify?
 - Forensic evidence
 - Communication with Threat Actor
 - Published data
- 

Negotiation Logs

[REDACTED]

We are looking to contact the people who left us the note

Hello [REDACTED]! As you know, in addition encrypting the data, I have also downloaded 1.6Tb of your data from local network. Our price is \$5,000,000. After payment, we will clean up all your data on our server and send you the deletion log, a decryption program and manual. If you do not pay, then your data will be published in our blog and Twitter. The brief analyse of you information: 1. Financial documents - consolidated balance sheets, bank statements, dividends, accounts payable and receivables, budget, various payment statements, various tax returns, audit reports, forms W2,w9,KPI, calculation of profits, transfers information, investment plans. There is all the information on finance and accounting NASDAQ. 2. Employees - lists of employees with the date of birth, SSN, ID numbers, addresses of residence, phone numbers, salary information and bonuses, information about taxes, contracts, tax forms, i9, medical forms, SCAN PASSPORTS and many others. 3. Clients, partners - NDA forms, contracts, customer and partners, base of personal data address, mail, phone and others, projects, information about each order and customer, including [REDACTED]. 4. Many working documentation - information about new developments, laboratory tests, patentsmarketing research, projects, various correspondence with state bodies, orders, information department and much more. 5. Postal correspondence. 6. SQL databases. I think you clearly understand that the publication of your data will lead to big problems. Therefore, in your interests to close the deal. You have 10 days (you can see the timer) to make an agreement.

This is a list of your stolen files so that you can evaluate the scale of the tragedy.

```
██████████ - Notepad
File Edit Format View Help
Volume in drive D is New Volume
Volume Serial Number is ██████████

Directory of D:\██████████

01/25/2023 02:27 PM <DIR> ██████████ \Administrators .
01/25/2023 02:27 PM <DIR> ██████████ SECURITY\SYSTEM ..
01/02/2023 04:59 AM <DIR> ██████████ \Administrators ██████████
12/29/2022 09:00 AM <DIR> ██████████ \Administrators ██████████
12/26/2022 11:58 AM <DIR> ██████████ \Administrators ██████████
12/26/2022 11:58 AM <DIR> ██████████ \Administrators ██████████
12/29/2022 09:01 AM <DIR> ██████████ \Administrators ██████████
12/26/2022 11:58 AM <DIR> ██████████ \Administrators ██████████
12/26/2022 12:01 PM <DIR> ██████████ \Administrators ██████████
12/29/2022 09:04 AM <DIR> ██████████ \Administrators ██████████
01/27/2023 04:54 PM <DIR> ██████████ \Administrators 2
12/26/2022 09:10 AM <DIR> ██████████ \Administrators A-Team
12/25/2022 09:20 AM <DIR> ██████████ \Administrators ACCT
01/25/2023 12:13 PM <DIR> ██████████ \Administrators Board
12/25/2022 09:53 AM <DIR> ██████████ \Administrators Contracts
12/25/2022 09:54 AM <DIR> ██████████ \Administrators ██████████
12/25/2022 08:45 AM <DIR> ██████████ \Administrators ██████████
12/30/2022 03:28 PM <DIR> ██████████ \Administrators HomeFolder
10/11/2022 09:08 AM <DIR> ██████████ \Administrators HR
12/25/2022 08:45 AM <DIR> ██████████ \Administrators IP
12/25/2022 08:46 AM <DIR> ██████████ \Administrators KPI
12/25/2022 08:53 AM <DIR> ██████████ \Administrators Legal
01/03/2023 04:13 AM <DIR> ██████████ \Administrators LT-Manufacturing
12/26/2022 09:11 AM <DIR> ██████████ \Administrators ██████████
01/09/2023 05:20 AM <DIR> ██████████ \Administrators New folder
12/26/2022 09:57 AM <DIR> ██████████ \Administrators OSG
06/30/2022 11:42 AM <DIR> ██████████ \Administrators Payroll
12/25/2022 08:53 AM <DIR> ██████████ \Administrators Proposals
12/22/2022 10:19 PM <DIR> ██████████ \Administrators Purchasing
12/22/2022 10:19 PM <DIR> ██████████ \Administrators QUEST_LOGS
12/26/2022 09:07 AM <DIR> ██████████ \Administrators RECYCLER
12/26/2022 09:11 AM <DIR> ██████████ \Administrators Research
```

Day 1 of negotiations – TA provided a .txt file with over 70K file names in an unusable format.



▶ Taking Care of the Team

- Physical demands – sleep, food
- Mental demands – downtime
- Health
- Sense of failure



■ “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.”

■ —Gene Spafford



Final Discussions and Lessons Learned

- Final status meeting with external legal and tech teams
- Internal discussions

Questions?



John Pilch

► Cybersecurity and Data Privacy Analyst

John.pilch@woodsrogers.com

This material is provided for informational purposes only. It is not intended to constitute legal advice nor does it create a lawyer/client relationship. The information provided may not be applicable in all situations and readers should speak with an attorney about their specific concerns. This material may be considered attorney advertising in some jurisdictions.

