Cybersecurity and Ransomware

February 18, 2021

International Association of Government Officials
Virtual Mid Winter Conference

iGO
INTERNATIONAL ASSOCIATION
OF GOVERNMENT OFFICIALS
Representing the finest clerks, recorders, election officials & treasurers

Introductions

Eugene Sisneros

M: 713-204-5734

in https://www.linkedin.com/in/eugene-sisneros-9419427/

Steve Russell

Chief Product Officer

in https://www.linkedin.com/in/steve-russell-07aa19/

Agenda

The State of Ransomware Today

Anatomy of a Ransomware Infection

Protecting from Ransomware - The Human Element

Protecting from Ransomware - Working with IT

Protecting from Ransomware - Working with your Vendors & Service Providers

Resources

State of Ransomware

The current scope and impact

Ransomware - A Brief Description

Ransomware is a type of malicious software. Once activated, it prevents users from accessing their *system* or *files* until the attacker is paid a ransom.

Ransomware: The Most Common Cybercrime

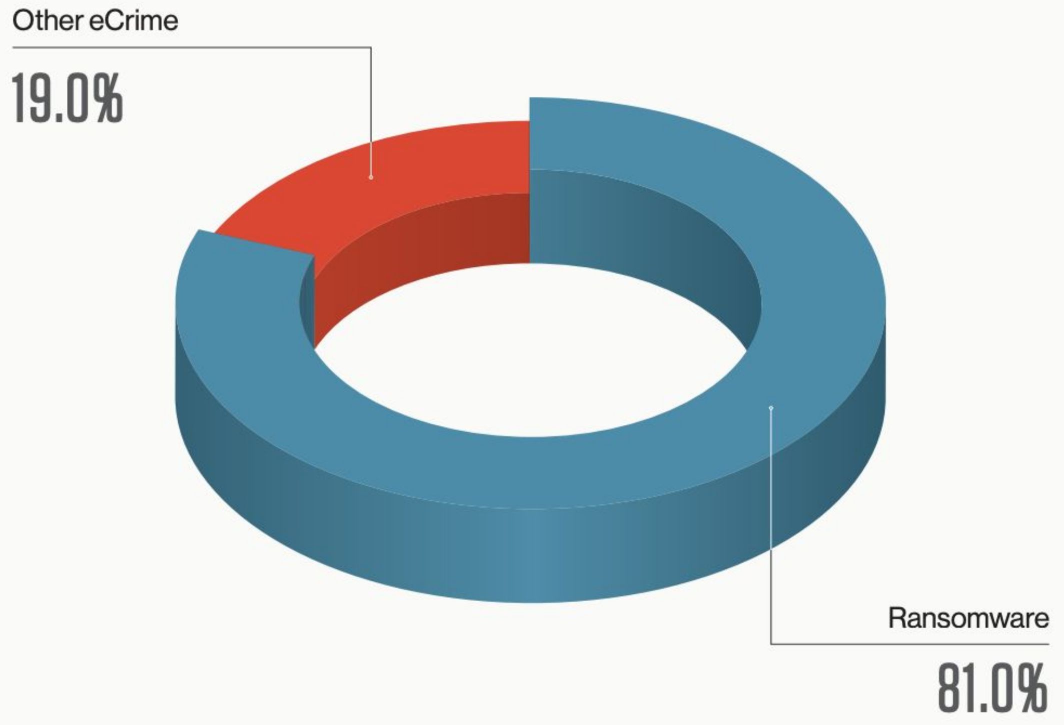
Ransomware has been around since 2013

It has mutated hundreds of times and there are currently hundreds of active variants

While early attacks focused on individuals, the trend is towards larger ransoms and on vulnerable networks and organizations

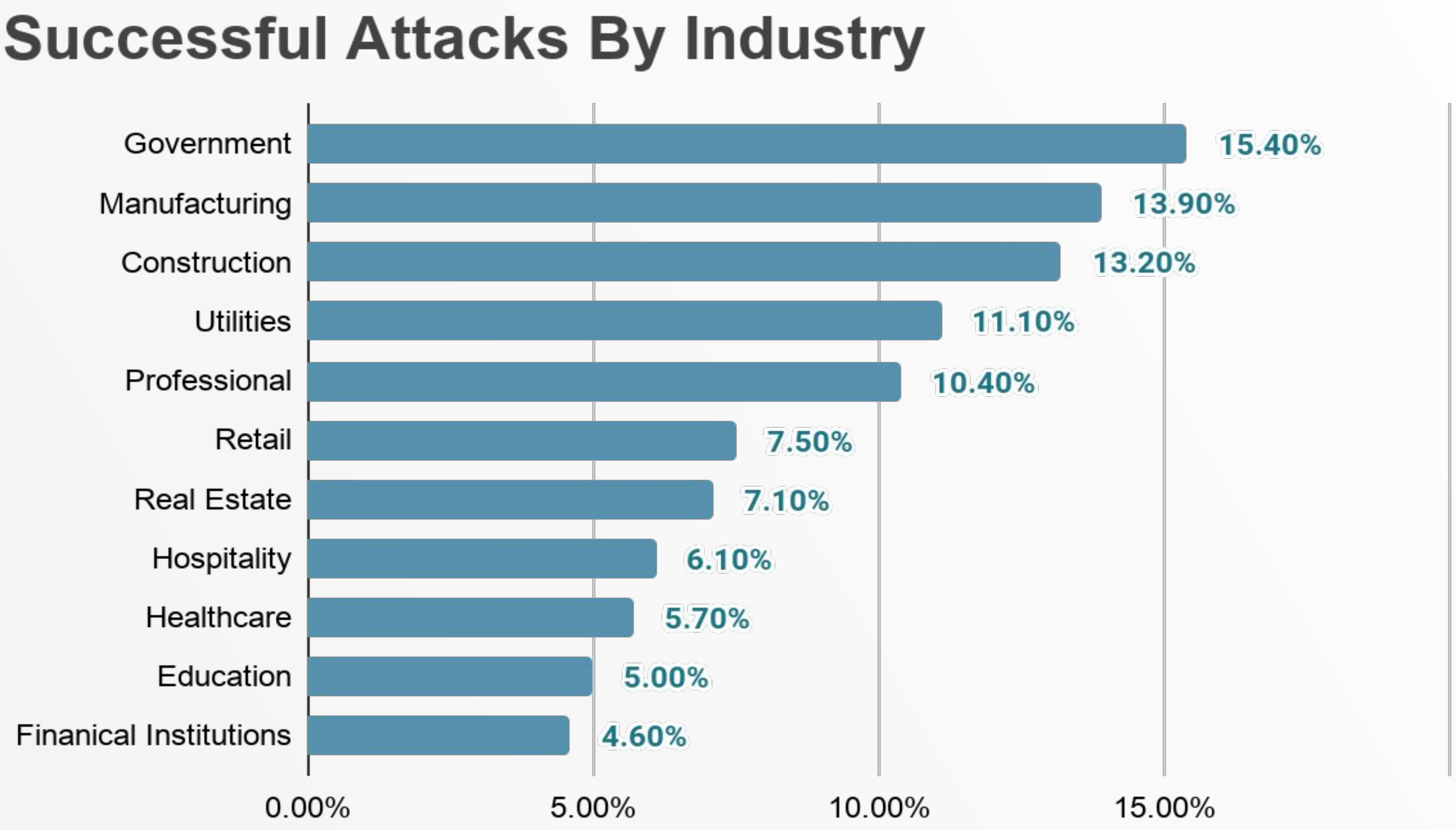
New “Ransomware-as-a-Service” makes it very easy to get into the ransomware business.

2020 eCrime Attacks



Source: Crowdstrike, 2021

State and Local Governments are Prime Targets



Ransomware Attack Success Indicators

1. Ease of attack and entry

   Unsophisticated network and workstation defenses, primarily due to IT investment relative to risk

2. Perceived cost to recover

   Data or systems that are difficult to restore, particularly if the backup window is insufficient

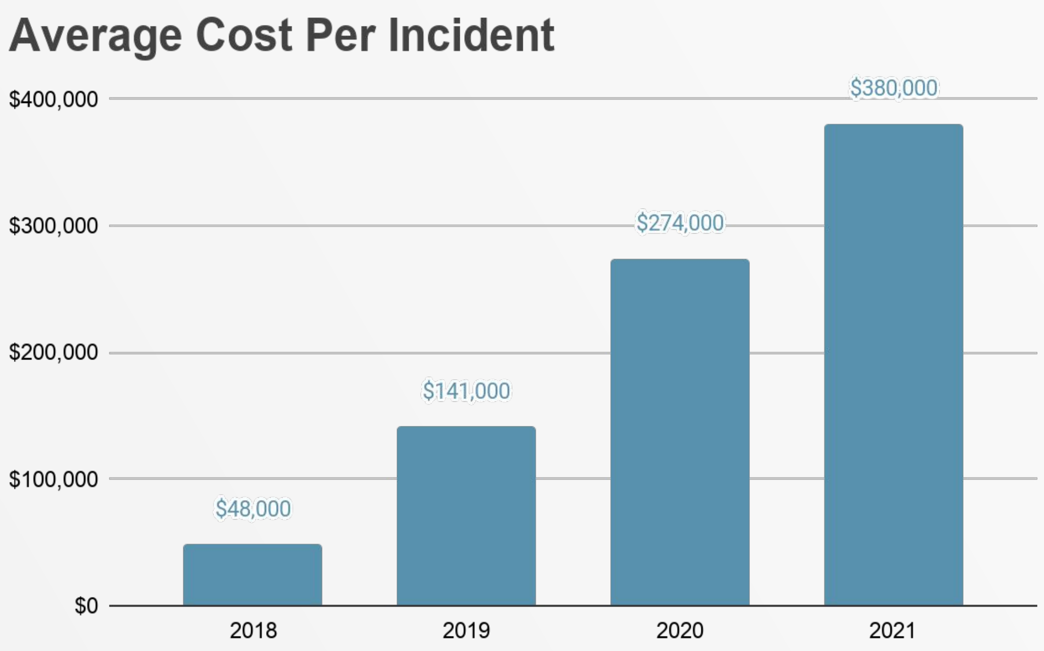
3. Motivation to Recover

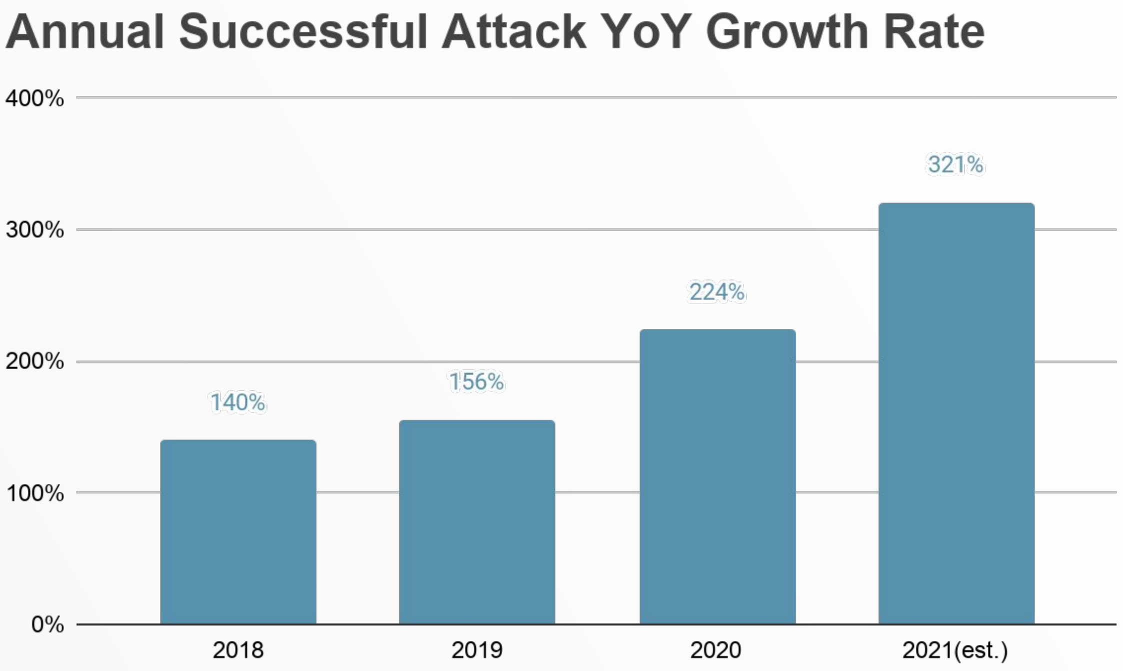
   Highly motivated victim who wants to "just make the problem go away"

4. Critical systems or data

   Cost to have data or system unavailable is very high for the victim

Accelerating Growth in Attacks and Costs





Attack trend is a shift from individuals to institutions as the primary target set

The question: "Why, after 7 years of attacks is this still a problem?"

Ransomware Preparation – The Myth

Question: “We run the latest virus scanning software and our systems are backed up regularly, so we should be safe, right?”

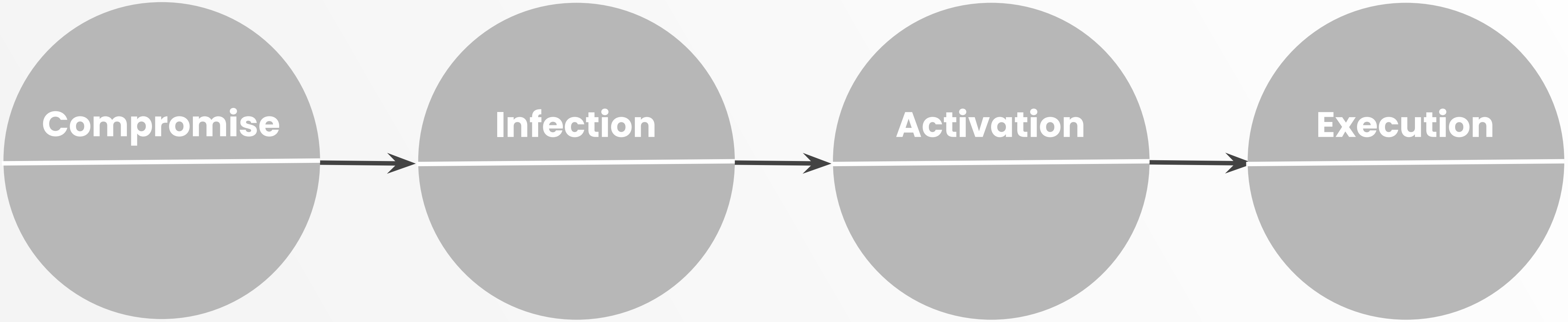
Answer: “I wouldn’t count on it”

Next question: “Well why not, and what can we do?”

Anatomy of an attack

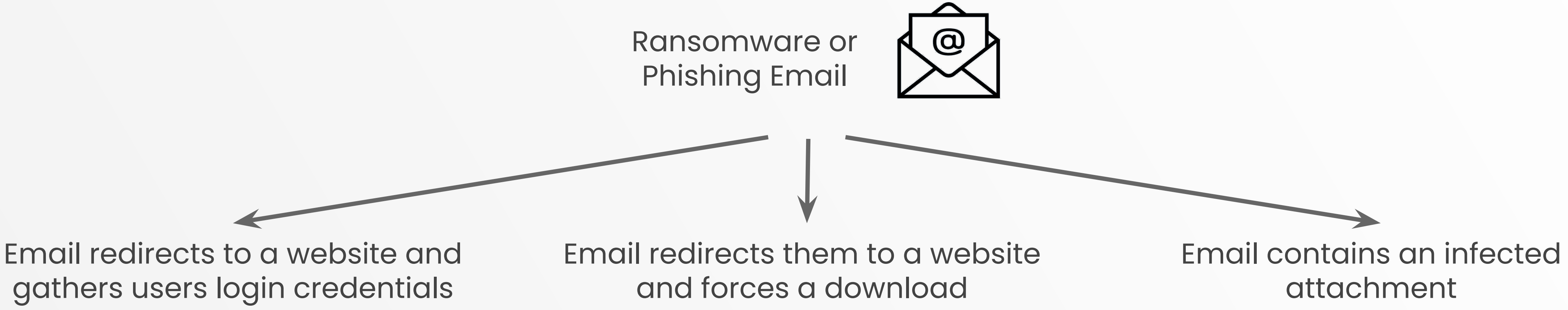
Vulnerabilities, Infection and Recovery

Anatomy of an Attack – The Four Phases



Compromise – The Human Element

Over 90% of all infections involve a human exploitation, typically due to lax controls or unwitting employees



Ransomware or Phishing Email

Email redirects to a website and gathers users login credentials

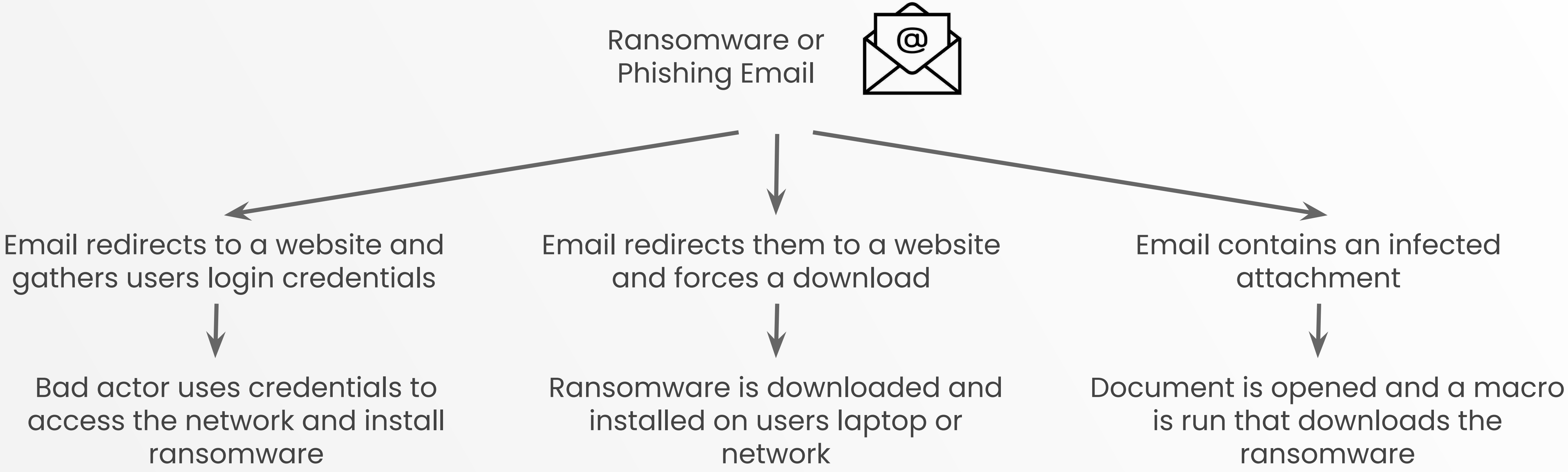
Email redirects them to a website and forces a download

Email contains an infected attachment

Other compromise vectors typically exploit system vulnerabilities that are shared within the Ransomware community (e.g. out-of-date software)

Infection

An infection occurs when the ransomware is installed on the target network or workstation. This “opens the door”.



Ransomware or Phishing Email

Email redirects to a website and gathers users login credentials

Bad actor uses credentials to access the network and install ransomware

Email redirects them to a website and forces a download

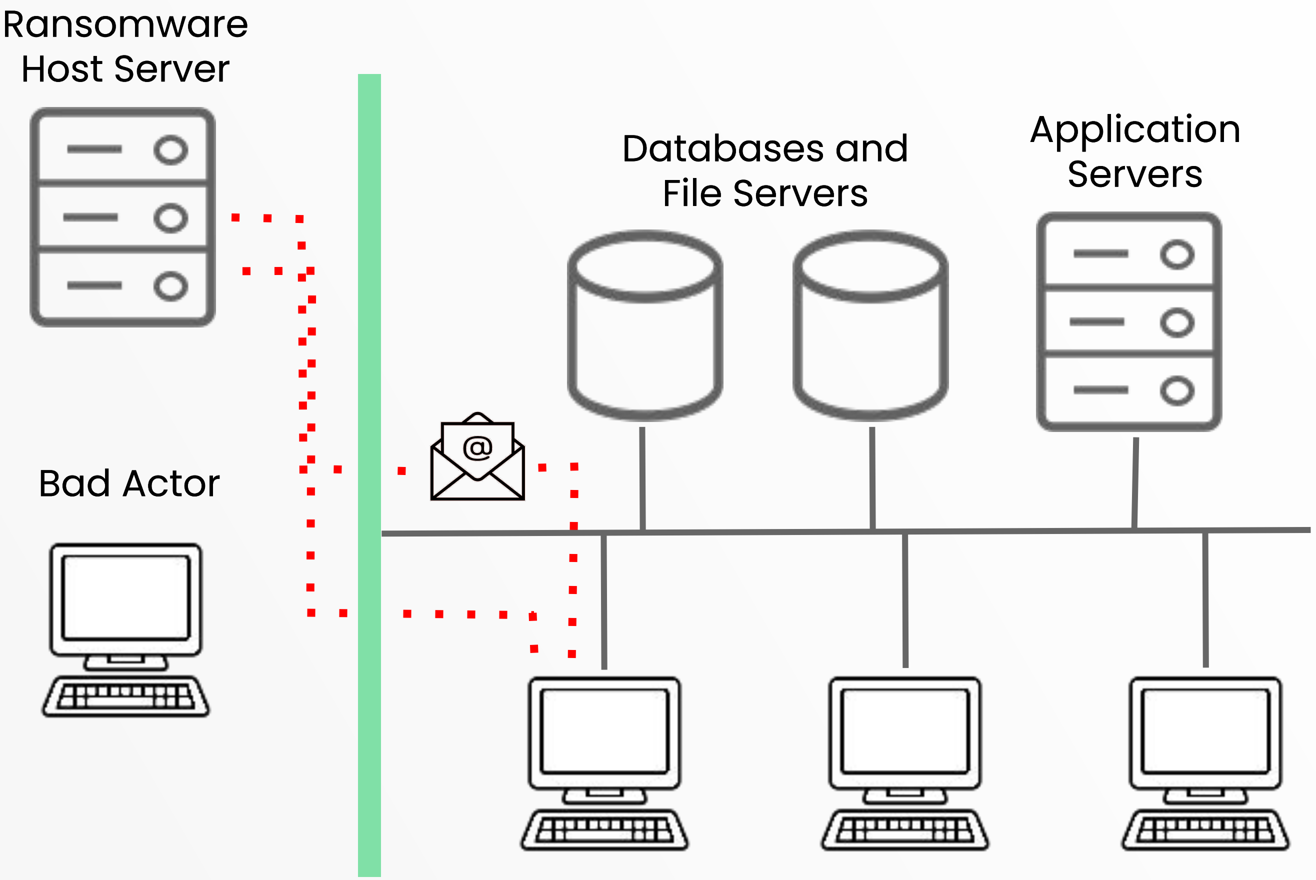
Ransomware is downloaded and installed on users laptop or network

Email contains an infected attachment

Document is opened and a macro is run that downloads the ransomware

Infection Flow

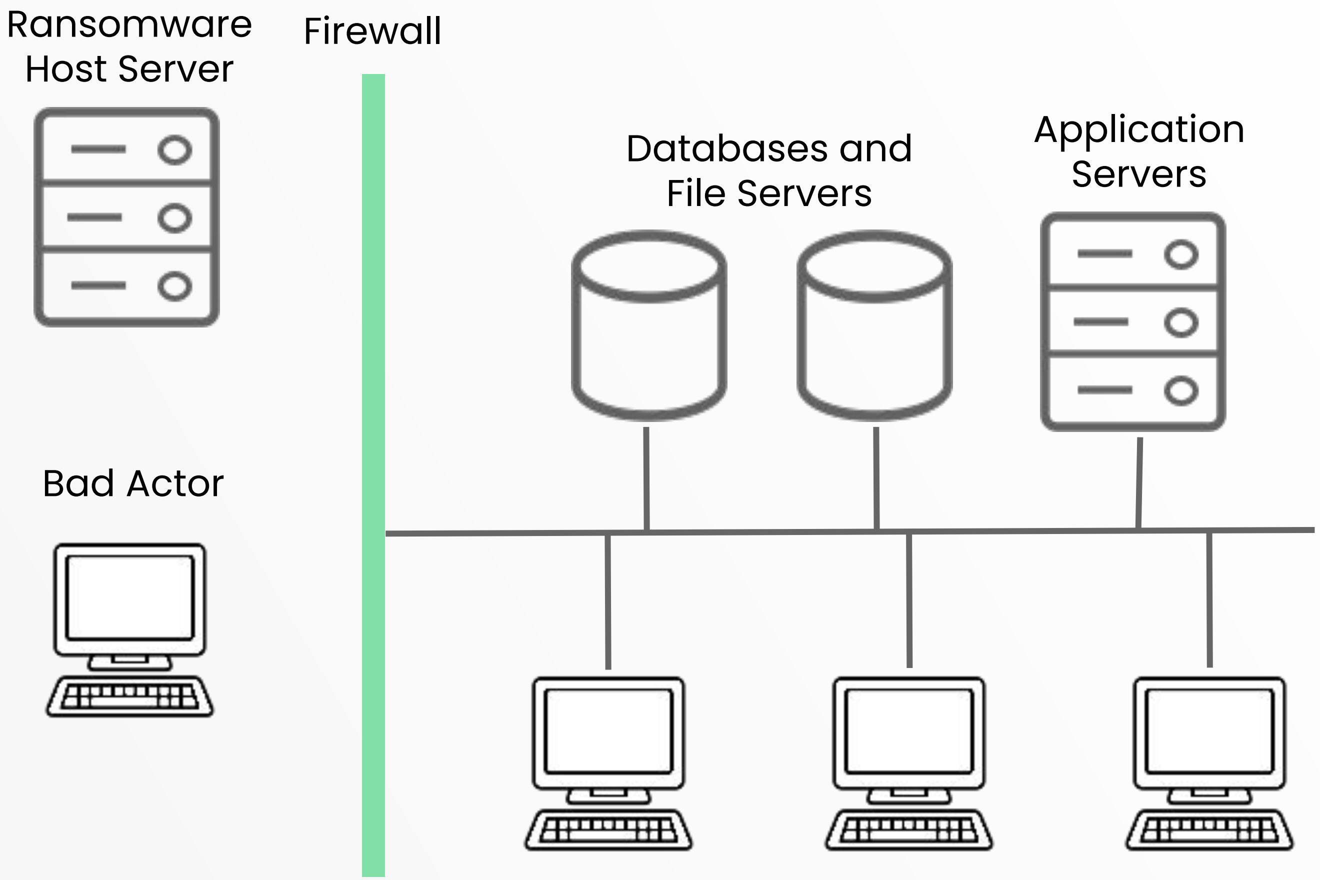
1. Bot sends spam email with attachment(e.g. MS Word doc)
2. User receives the email and opens the attachment
3. A macro in the Word doc runs which goes back out to the ransomware host and downloads the ransomware
4. It is now installed and the network or workstation is now infected



Virus Scanning and Web Filtering

1. **Spam filter** should stop the email
2. **Email virus scan** should flag the attachment and quarantine
3. **Workstation and server virus scanning** should flag the attachment file once saved
4. **Web filter** should block the Ransomware download

75% of organizations infected by ransomware were running up-to-date virus Protection



The Systems Security Cycle

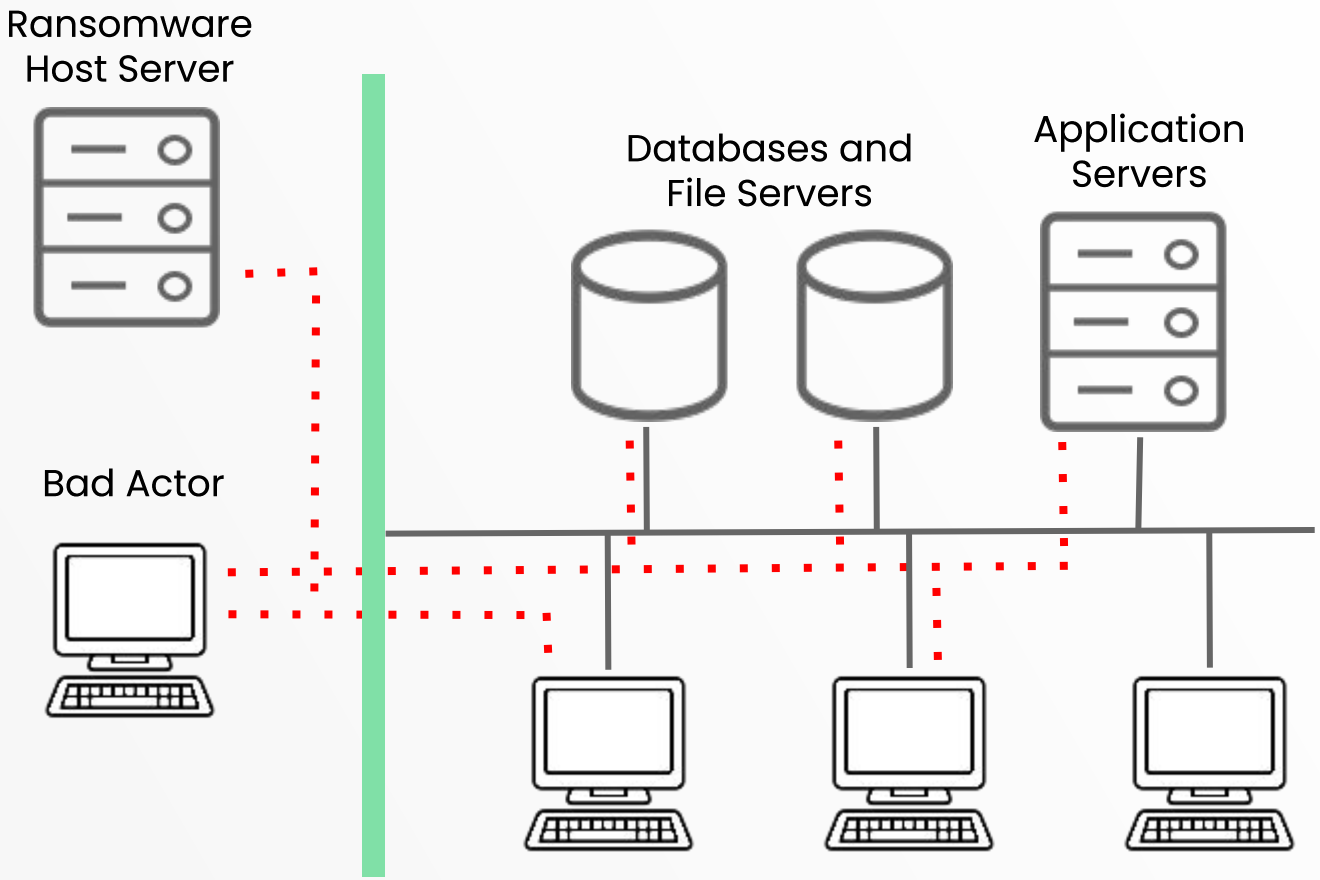
1. Virus, Systems, or Application vendor identifies a new variant or security risk
2. Vendor analyzes and develops a way to identify and block, or patch risk
3. Vendor packages, tests and distributes the update
4. IT patches or updates infrastructure
5. Bad actor realizes attacks are are no longer working
6. Bad actor creates a new variant or adapts the process
7. Return to step 1

This cycle is the window of opportunity for the bad actors

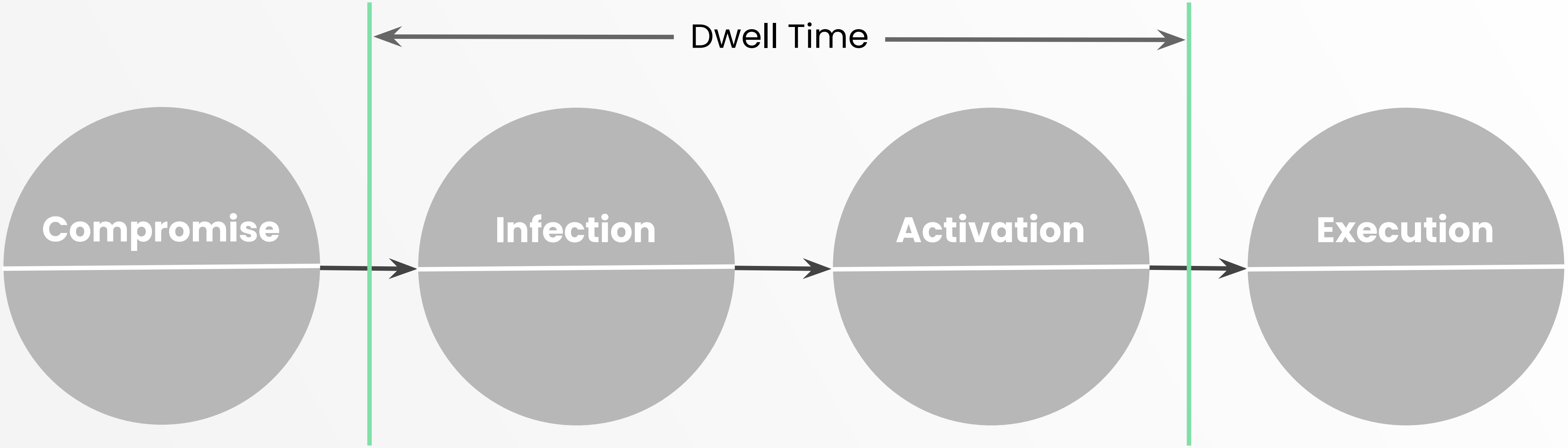
This cycle can’t be eliminated so the focus is on making it shorter

Activation

1. Ransomware is installed during the Infection stage
2. The ransomware grants the bad actor remote access to the network (Activation)
3. Bad actor can then analyze data and backup procedures, install rogue software, etc. and plan the execution
4. Will install ransomware in as many data stores and systems as possible



Activation And Dwell Time



Dwell Time is the amount of time a bad actor remains undetected inside your network

The average Dwell Time during reported successful ransomware attacks in 2020 was **43 days**

Backing Up and Restoring Data

Plan: What is going to be backed up and why

Schedule: How often will backups be made

Store: Where will backups be kept and how quickly can they be restored

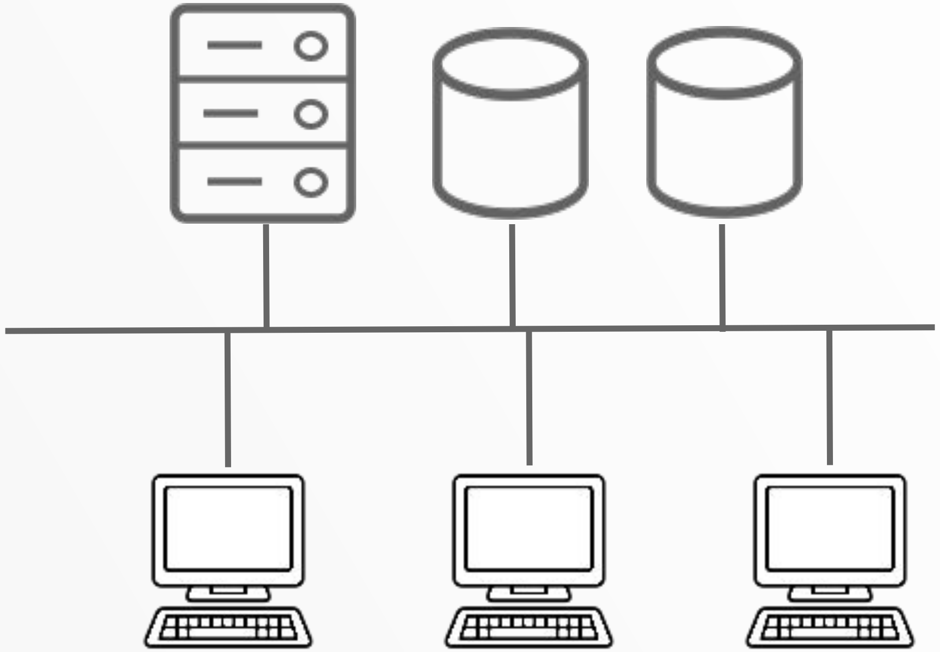
Copy: How many copies and in what locations

Retain: How long are backups kept

Test: Test restoring from backups including recovery window

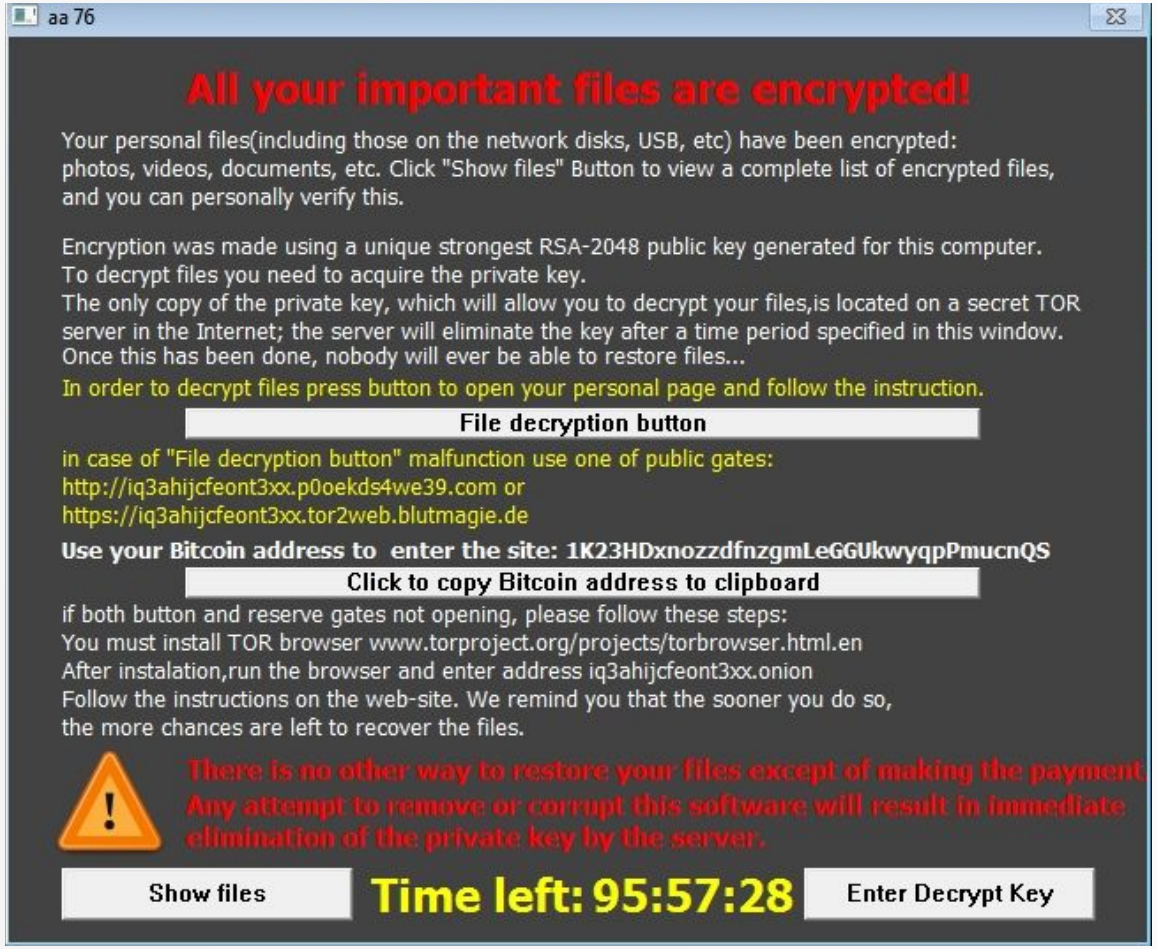
Recovery Window: Time between outage and last backup

- Backup every night and every weekend.
- Copy the weekend backup and send offsite
- Keep one month’s worth of data



A clean backup is the only way to restore a system and avoid paying the ransom

Execution – Sign Of A Bad Day



All your important files are encrypted!

Your personal files(including those on the network disks, USB, etc) have been encrypted:
photos, videos, documents, etc. Click "Show files" Button to view a complete list of encrypted files,
and you can personally verify this.

Encryption was made using a unique strongest RSA-2048 public key generated for this computer.
To decrypt files you need to acquire the private key.
The only copy of the private key, which will allow you to decrypt your files,is located on a secret TOR
server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt files press button to open your personal page and follow the instruction.

in case of "File decryption button" malfunction use one of public gates:
http://iq3ahijcfeont3xx.p0oekds4we39.com or
https://iq3ahijcfeont3xx.tor2web.blutmagie.de

Use your Bitcoin address to enter the site: 1K23HDxnozzdfnzgmLeGGUkwyqpPmucnQS

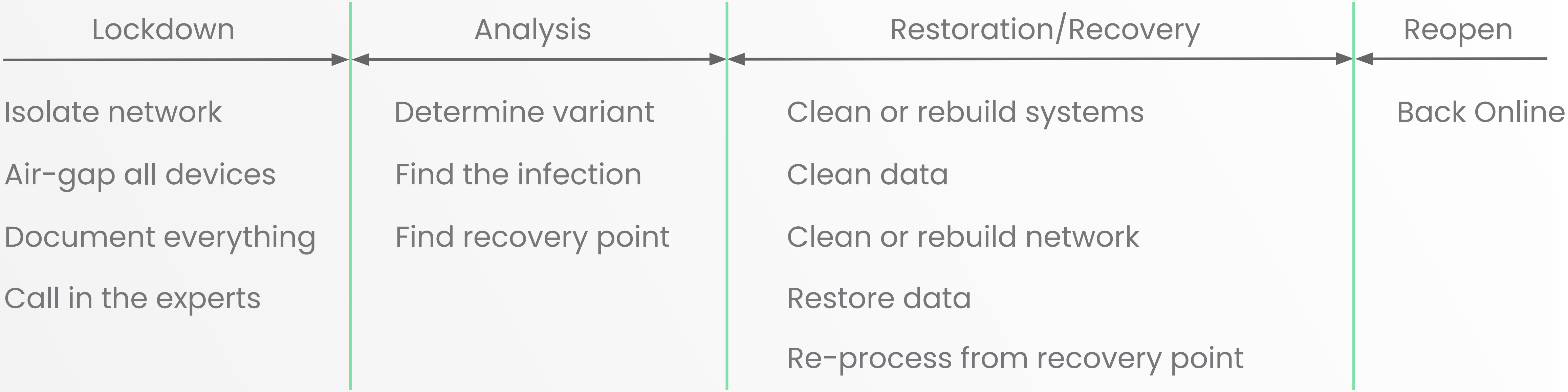
if both button and reserve gates not opening, please follow these steps:
You must install TOR browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address iq3ahijcfeont3xx.onion
Follow the instructions on the web-site. We remind you that the sooner you do so,
the more chances are left to recover the files.

There is no other way to restore your files except of making the payment
Any attempt to remove or corrupt this software will result in immediate
elimination of the private key by the server.

Time left: 95:57:28

Execution – This is where it gets painful

Costs $$ - The axiom “Time is Money” is very appropriate



Lockdown	Analysis	Restoration/Recovery	Reopen
Isolate network	Determine variant	Clean or rebuild systems	Back Online
Air-gap all devices	Find the infection	Clean data	
Document everything	Find recovery point	Clean or rebuild network	
Call in the experts		Restore data	
		Re-process from recovery point	

This process is the real cost, not the ransom

Even if the ransom is paid, the infection must be removed. Otherwise…round two?

Some Notable Incidents and Costs

City of Baltimore 2019- $18 million

City of Atlanta 2018 - $17 million

Over 23 Texas Municipalities in 2019 - $13 million

7 Florida Municipalities in 2019 - Over $9 million

City of New Orleans in 2019 - $3 million

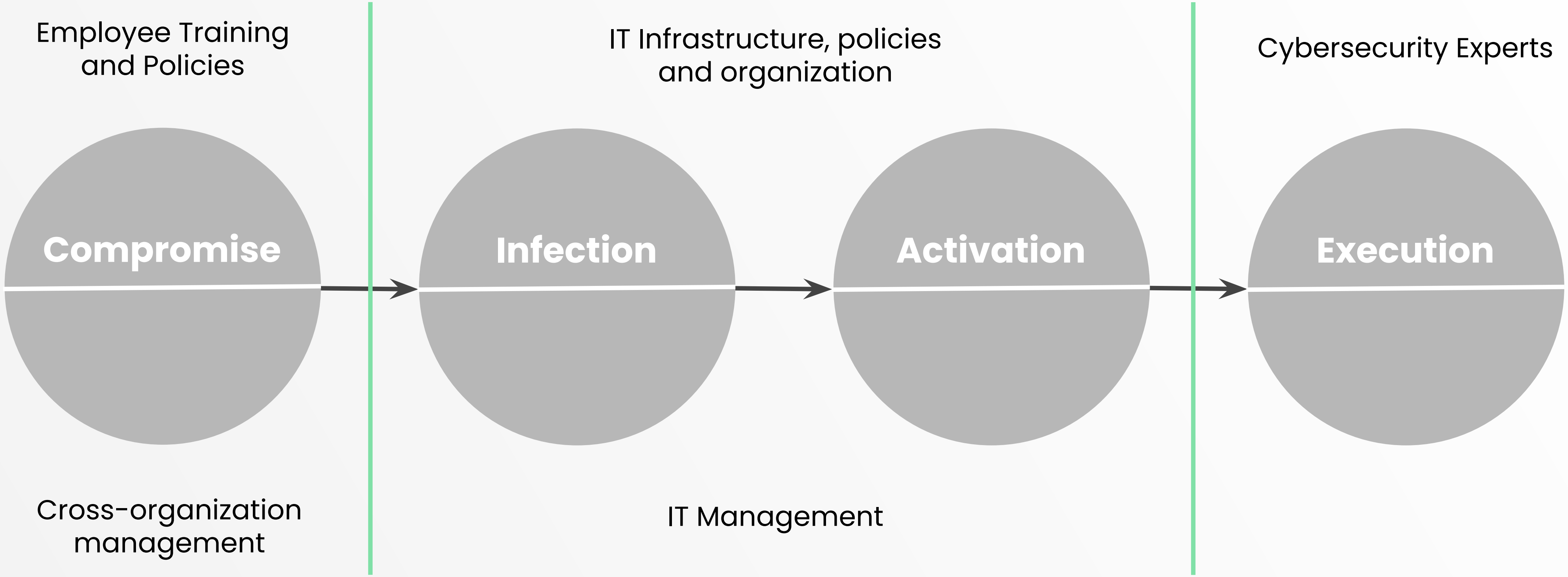
Summary Thus Far

1. The vast majority of attacks are the result of human exploitation
2. Bad actors target smaller organizations with limited IT resources (money and people)
3. Keeping infrastructure current (software versions, etc.) does not guarantee security
4. Bad actors exploit the **Systems Security Cycle** - it's a cat and mouse game
5. Data backups need to ensure data isolation and long recovery windows

What You Can Do

Strategies for minimizing risk and optimizing recovery

Anatomy of an Attack



Employee Training and Policies

IT Infrastructure, policies and organization

Cybersecurity Experts

Compromise

Infection

Activation

Execution

Cross-organization management

IT Management

Primary Points of Control and Impact

The Human Element - Employees, Contractors and Vendors

Systems and Network Security and keeping Systems Current

Data - Limiting Exposure and Ensuring Clean Data

1. An Employee Awareness & Testing Program

Build Employee Awareness - Security Training

Understanding vulnerabilities and how they are exploited

Security best practices (passwords, data access, etc.)

Common threats and bad actor patterns

Recognizing threats and suspicious activities

Device exposures (laptop, phones, etc.)

Test and Track Security Practices and Compliance

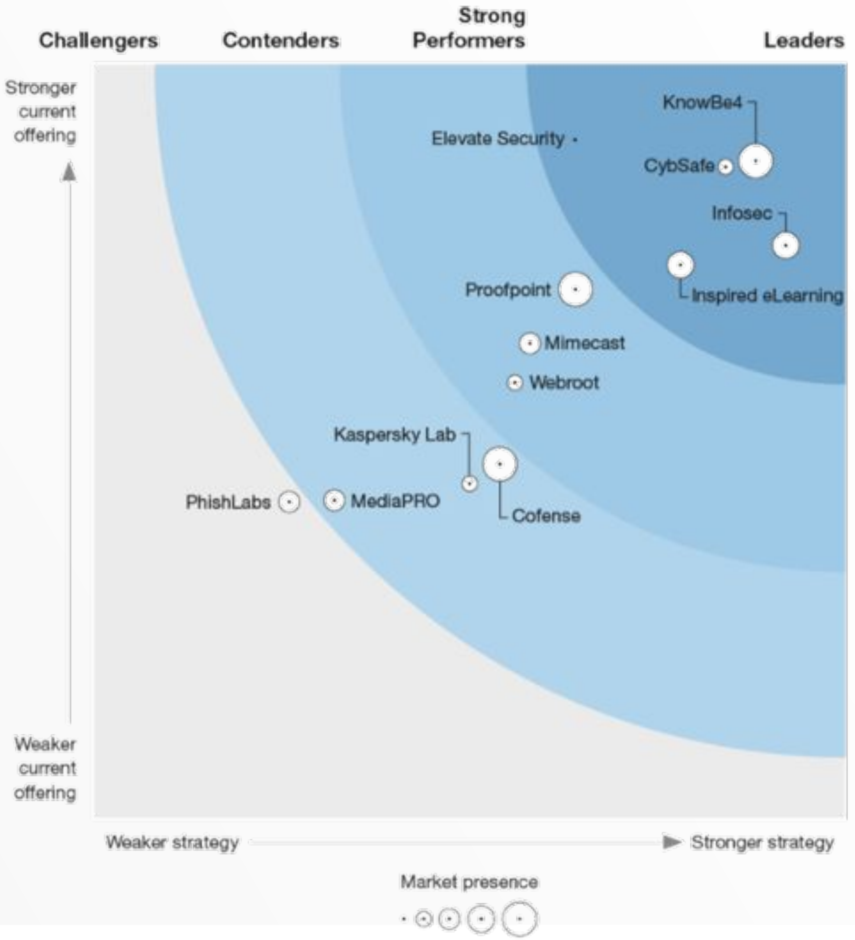
Formal compliance testing and adherence

Systems to ensure compliance (e.g. passwords)

Blind testing to track training effectiveness (test emails)

An Awareness Program is fast and efficient protection

Forrester - Security Awareness & Training



GovOS
A Kofile Company

2. Working with Internal IT – Data Backups

Questions - Data Management	Desired Answers
What data is being backed up?	All data that you have determined is necessary to run you operation.
How often are the backups run?	Snapshots at least every 15 minutes and full backups nightly.
How often are the backups isolated from the network?	At least weekly, preferably nightly.
What is our “Time To Recovery” (TTR)?	At least four hours.
How often do we verify and test our backup and restore procedures?	At least one a year, preferably twice a year and with different outage scenarios.
Do we have a copy of our critical data in a format that we can load or access in a different system?	Yes, we ensure that all critical data is exported, not just backed up. In case we need to quickly get that data available, there is a way to do so.

3. Working with Internal IT – Infrastructure

Questions - Virus Scanning and Infrastructure	Desired Answers
Are we using a virus scanner on our email system?	All incoming and outgoing emails are scanned for viruses or rouge URLs. All email is scanned prior to being placed in a user's inbox.
Are all of our workstations and servers scanned?	All endpoints are centrally managed which includes virus scanning.
How often are our virus scanning signatures updated?	All are updated automatically and implemented when the vendor makes a new signature file available.
Beyond virus scanning, what other threat protection software is installed?	We have web filtering through a Next Generation Firewall (NGFW) and an Intrusion Protection System (IPS).
Do we have tooling that prevents unauthorized applications from being launched?	Yes, we implement application whitelisting under our security management system, which controls what applications can be run and from where.
What process do we have to ensure our systems and applications are current, including security patches?	We monitor and escalate applying, testing and rolling out all new system updates that include security patches.
Do we have a cybersecurity insurance policy and if so, does it cover ransomware attacks?	Yes, we have insurance and it covers investigation costs, business losses, privacy notifications and extortion/ransomware

4. The Cloud – Leveraging Cloud Scale & Expertise

Not a Panacea! Not all clouds are created equal

Public Cloud	All services run in the cloud and leverage advanced cloud services (Microsoft, Amazon, Google)
Private Cloud	Service is private and provides limited services (software vendors hosting customer systems)
Hybrid Cloud	Solution runs in both on-premise and cloud (local application backed up to the cloud)

Public Cloud is the “gold standard” for security and infrastructure

As an example, Microsoft Azure spent $1 billion in 2020 on cyber security

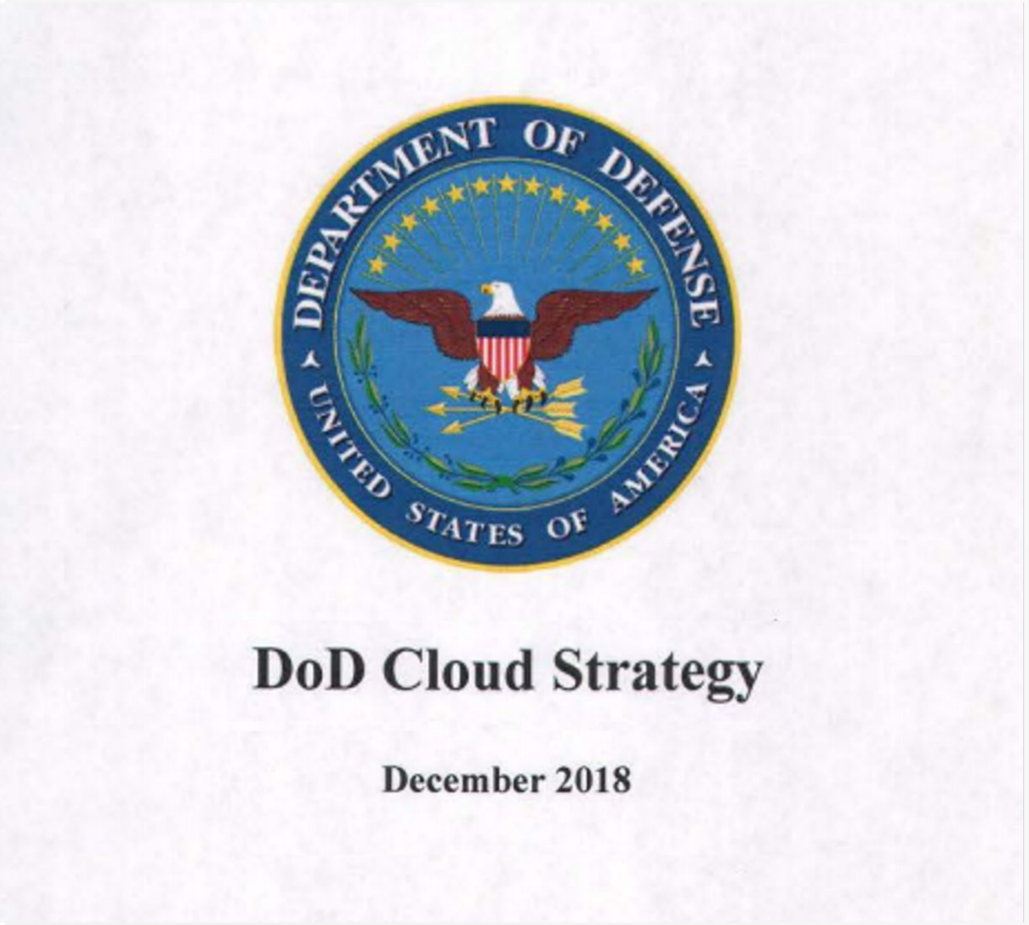
Public cloud vendors have the fastest cyber security remediation cycle in the industry

Highly proactive Artificial Intelligence based threat detection and analysis

Advanced storage and file management for immediate backup and long retention periods

Requires software designed to leverage the public cloud (just running there doesn’t count)

Systems and Data Security – Leverage The Cloud



DoD Cloud Strategy

December 2018

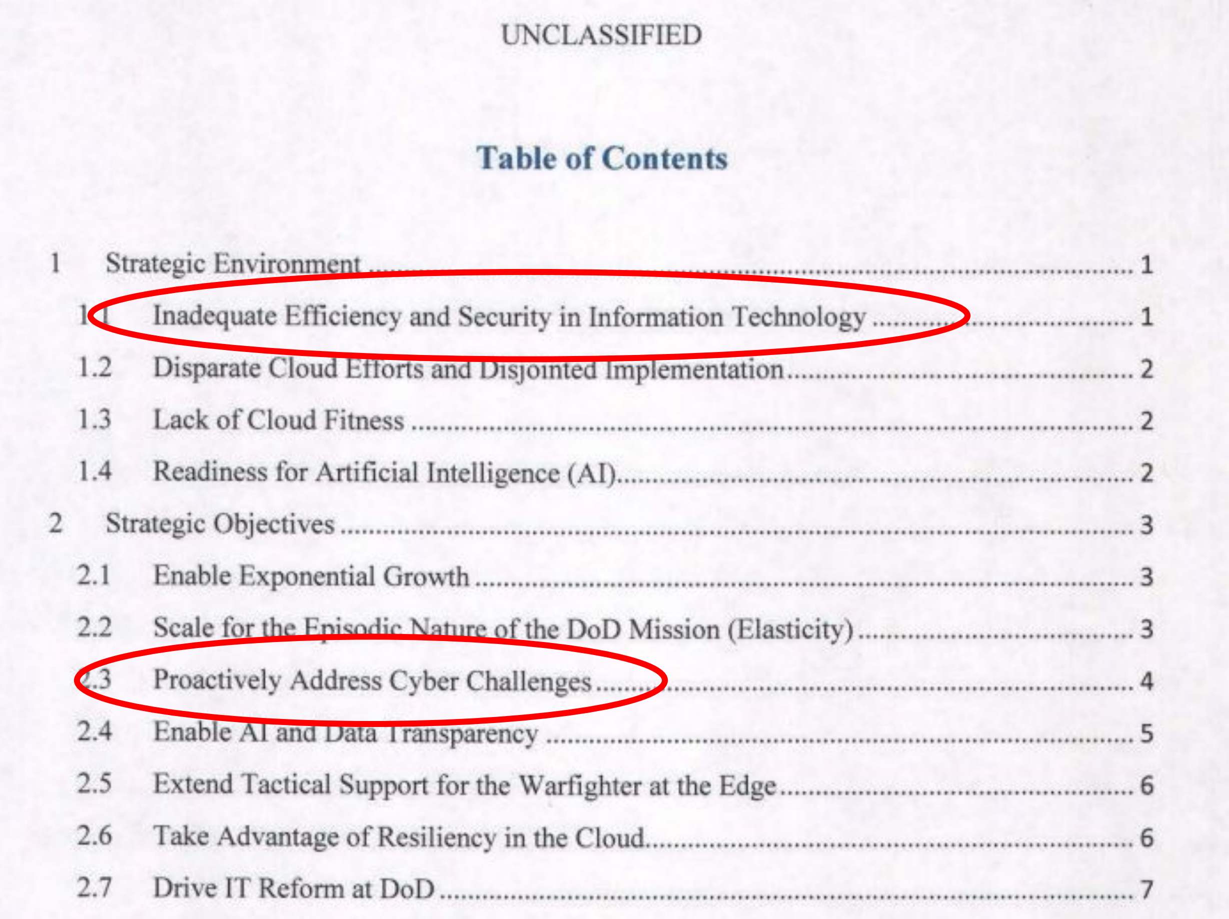

UNCLASSIFIED

Table of Contents

Department of Defense Cloud Strategy

Working with IT and Vendors – The Cloud

Questions - Cloud Deployed Systems	Desired Answers
Are we running in a public or private cloud and whose cloud?	We run in the Public cloud, Microsoft Azure (or Google or Amazon)
If not public, what certifications and standards are supported?	All Federal security and data protection standards (e.g. FedRamp, GDPR, etc.)
Is the application that we are running in the cloud, architected and leveraging the cloud infrastructure?	The application is multi-tenant, designed for the cloud and leverages cloud replication and data management.
How are backups being performed with our cloud application?	We use the Cloud Vendors backup and data replication strategy which gives us real-time backups, geo-replication and network isolation.
Do we have access to our data and do we have copies of it outside of the vendor’s cloud?	Yes, we export and download the data on a weekly basis.
Does the cloud application require us to have any data stored or managed by our on-premise network?	No, all data is managed and maintained in the cloud.
Does our vendor carry cyber insurance and does it cover our losses?	Yes, as a part of our contract with the vendor, they are obligated to carry cyber insurance and that policy covers any losses that we may incur.

Resources

Information from the Internet Crime Complaint Center (IC3)

Ransomware: What it is and what to do about it (pdf)

High Impact Ransomware Attacks Threaten U.S. Businesses and Organizations

Ransomware Victims Urged to Report Infections to Federal Law Enforcement

Related FBI News and Multimedia

The National Cyber Investigative Joint Task Force Releases Ransomware Fact Sheet

Protected Voices: Ransomware

Building a Digital Defense Against Ransomware Targeting Businesses

Security Vendor Websites

Crowdstrike

McAfee

Norton

Kaspersky

Summary

1. The vast majority of attacks are the result of human exploitation - This can be impacted
2. Keeping infrastructure current (SW versions, etc.) does not guarantee security
3. Bad actors exploit the **Systems Security Cycle** - reduce it where you can
4. Understand your data backup strategy to ensure isolation and long recovery windows
5. It isn’t enough to just run backups and virus scans. The depth of what is done is critical
6. Manage vendors very closely to ensure the above, particularly managed service providers for on-premise systems
7. Leverage the public cloud to reduce risk but review vendor/IT cloud model

Questions & Answers

Thank You

Eugene Sisneros

M: 713-204-5734

in https://www.linkedin.com/in/eugene-sisneros-9419427/

Steve Russell

Chief Product Officer

in https://www.linkedin.com/in/steve-russell-07aa19/

GovOS

A Kofile Company