Dissecting Cybersecurity Breaches

Jeremiah School – Impact Networking / DOT Security

impact

Introduction

impact

DOT Security + impact

Agenda

- Understanding a Breach
- Insights Into Breach Response
- Real World Stories
- Best Ways to Reduce Breach Risk
- Q&A

impact

Incident

An event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.

Breach

A cybersecurity breach is any unauthorized access to data, applications, devices, or networks. Typically, they're done with the intent to steal data or shut down key systems.

impact

Understanding Breaches

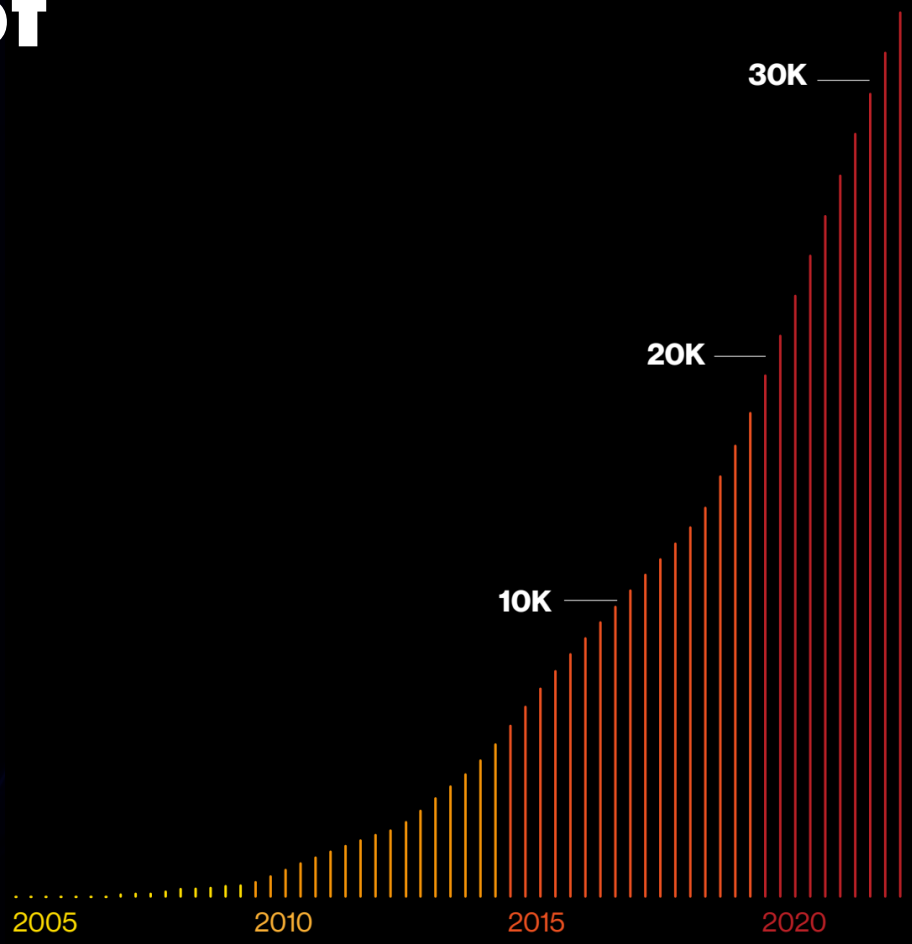
impact

Incident Severity

LEVEL 5 *Emergency*	**EMERGENCY SITUATION: ACTIVE CYBERATTACK** e.g. Evidence of an attacker operating from an escalated account (i.e. admin), malware or attack behavior on a high-value host (i.e. Domain Controller), multiple machines displaying attack behavior, data exfiltration.
LEVEL 4 *Severe*	**SEVERE, IMMEDIATE FUNCTIONAL IMPACT** e.g. Successful unauthorized logins, manual malicious commands being run on a host, alarms signifying an active persistent threat, multiple machines displaying similar attack evidence.
LEVEL 3 *High*	**HIGH POSSIBILITY OF FUNCTIONAL IMPACT** e.g. Credential loss due to phishing, verified malware execution on one or more hosts, detection of unauthorized program tasks or user activities.
LEVEL 2 *Medium*	**MODERATE POSSIBILITY OF FUNCTIONAL IMPACT** e.g. Malware quarantined or blocked, suspicious email(s) quarantined, suspicious inbound/outbound connections blocked, evidence of suspicious sign-in attempts/failures.
LEVEL 1 *Low*	**SLIGHT POSSIBILITY OF FUNCTIONAL IMPACT** e.g. Vulnerability scan or risk assessment of environment reveals vulnerable services, security holes, or other cyber risk.

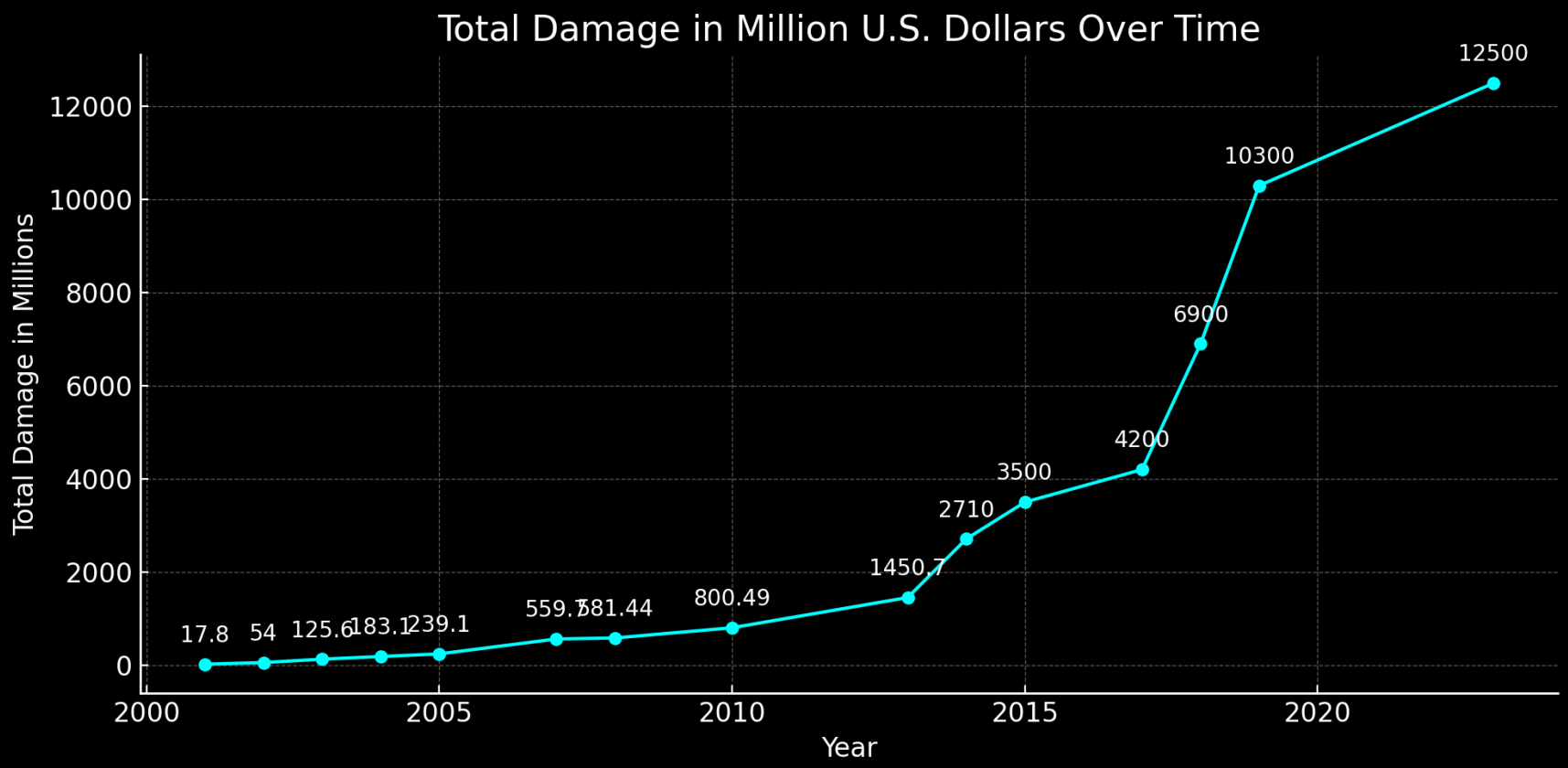
impact

Number of Breaches Over Time



Source: Verizon Data Breach Investigation Report 2023

impact



Source: FBI's 2023 IC3 Report

impact

Organizations Penetrated By Threat Actors

85%

< 1,000 Employees

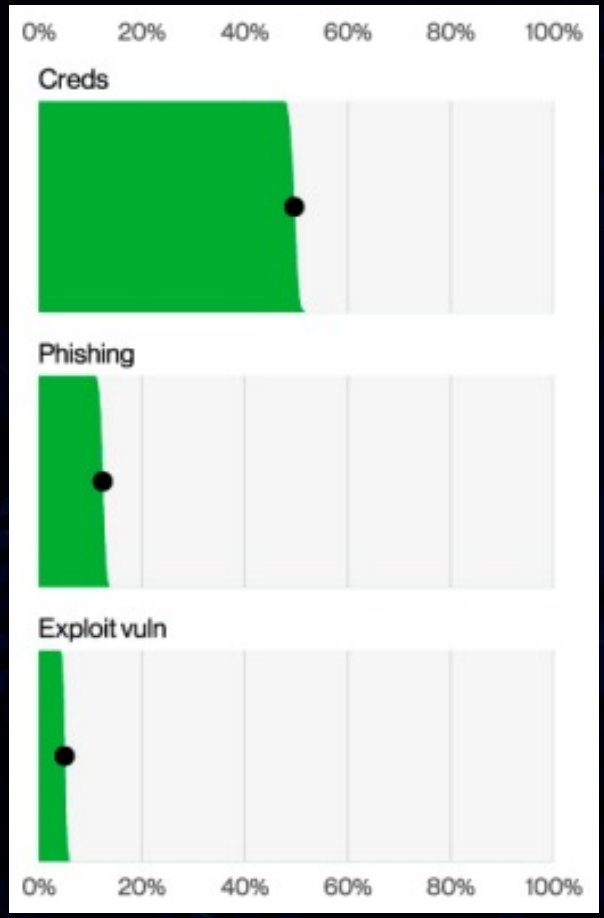
60%

> 1,000 Employees

Duke University/CFO Magazine Global Business Outlook Survey

impact

Top 3 Ways Attackers Access an Organization

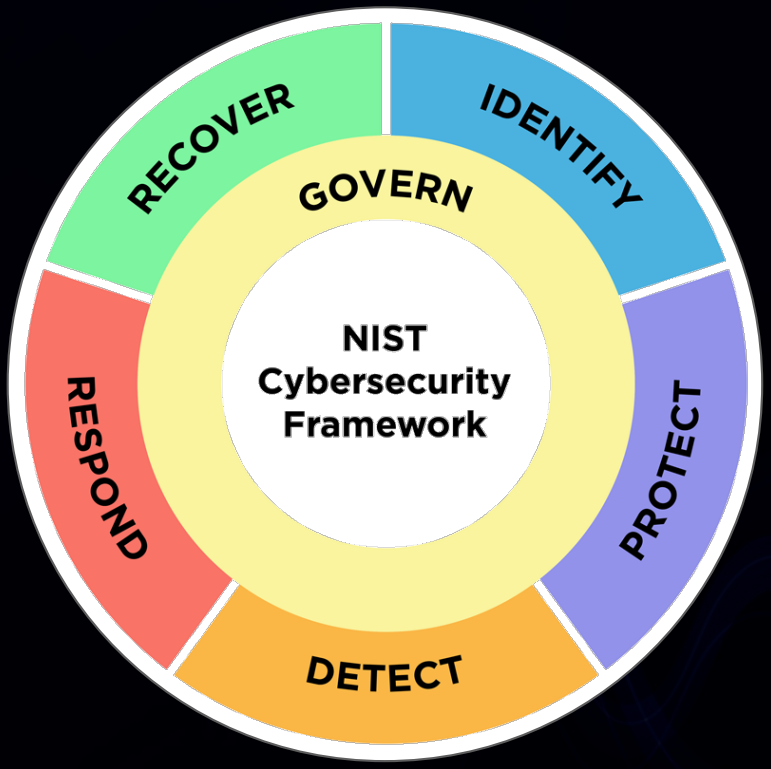


Source: Verizon Data Breach Investigation Report 2023

impact

Breach Response Insights

Response within Frameworks



CIS Control Groups

CONTROL 01 Inventory and Control of Enterprise Assets — 5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5	CONTROL 02 Inventory and Control of Software Assets — 7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7	CONTROL 03 Data Protection — 14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software — 12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12	CONTROL 05 Account Management — 6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6	CONTROL 06 Access Control Management — 8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8
CONTROL 07 Continuous Vulnerability Management — 7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7	CONTROL 08 Audit Log Management — 12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12	CONTROL 09 Email and Web Browser Protections — 7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7
CONTROL 10 Malware Defenses — 7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7	CONTROL 11 Data Recovery — 5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5	CONTROL 12 Network Infrastructure Management — 8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8
CONTROL 13 Network Monitoring and Defense — 11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11	CONTROL 14 Security Awareness and Skills Training — 9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9	CONTROL 15 Service Provider Management — 7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7
CONTROL 16 Applications Software Security — 14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14	CONTROL 17 Incident Response Management — 9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9	CONTROL 18 Penetration Testing — 5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

impact

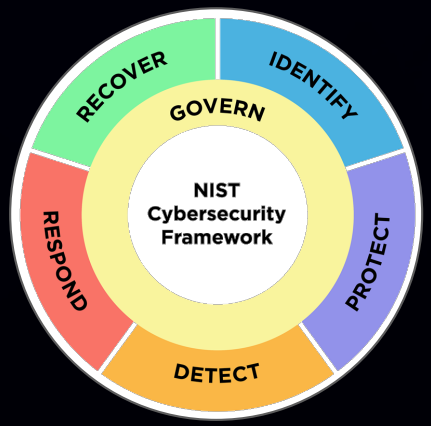
Response within Frameworks

CIS Control Groups

CONTROL 01 Inventory and Control of Enterprise Assets — 5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5	CONTROL 02 Inventory and Control of Software Assets — 7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7	CONTROL 03 Data Protection — 14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software — 12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12	CONTROL 05 Account Management — 6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6	CONTROL 06 Access Control Management — 8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8
CONTROL 07 Continuous Vulnerability Management — 7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7	CONTROL 08 Audit Log Management — 12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12	CONTROL 09 Email and Web Browser Protections — 7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7
CONTROL 10 Malware Defenses — 7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7	CONTROL 11 Data Recovery — 5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5	CONTROL 12 Network Infrastructure Management — 8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8
CONTROL 13 Network Monitoring and Defense — 11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11	CONTROL 14 Security Awareness and Skills Training — 9 Safeguards — IG1 8/9 — IG2 9/9 — IG3	CONTROL 15 Service Provider Management — 7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7
CONTROL 16 Applications Software Security — 14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14	CONTROL 17 Incident Response Management — 9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9	CONTROL 18 Penetration Testing — 5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

impact

Response within Frameworks



	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPLICATIONS					
DATA					
USERS					
DEGREE OF DEPENDENCY	TECHNOLOGY				PEOPLE
	PROCESS & GOVERNANCE				

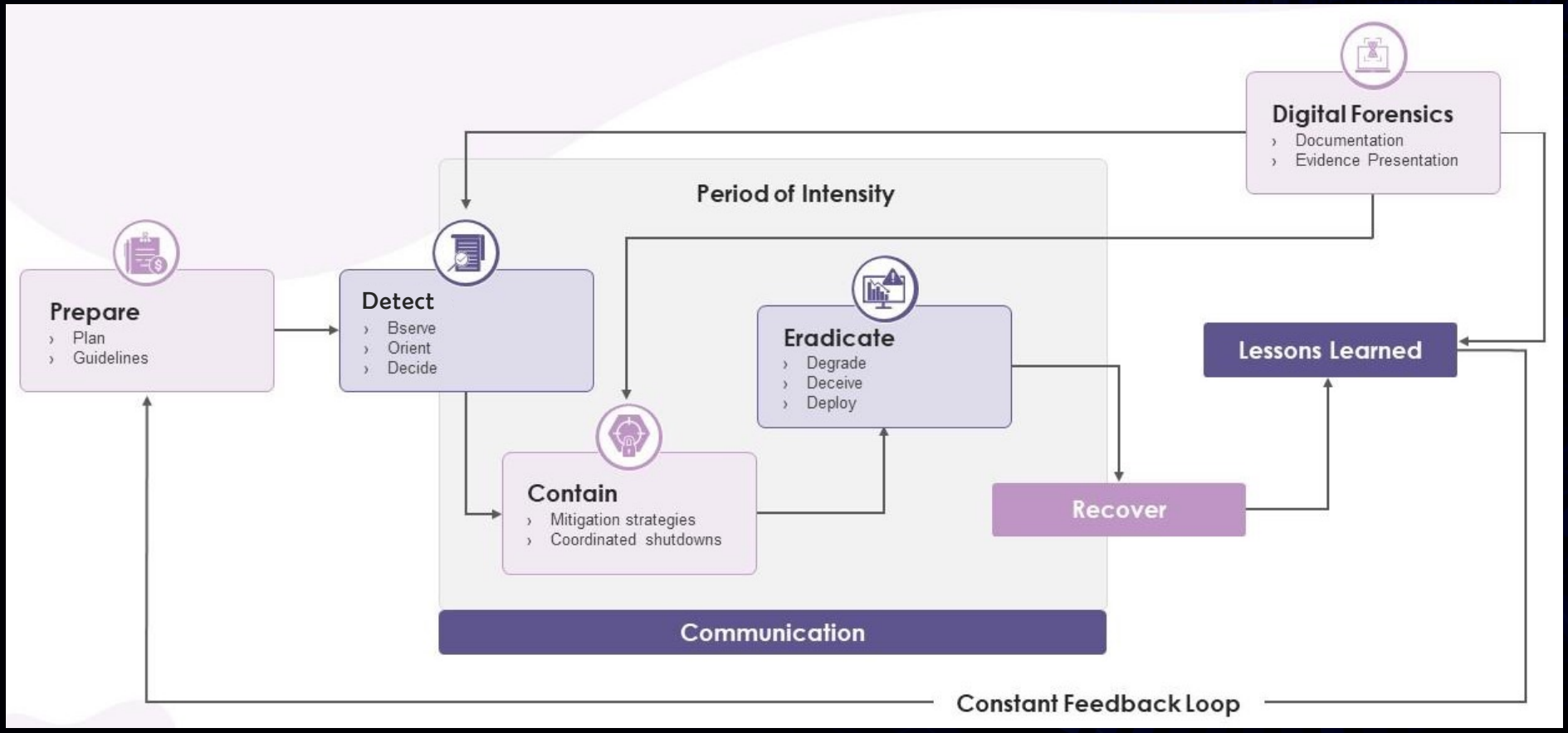
impact

IT vs Cyber Teams

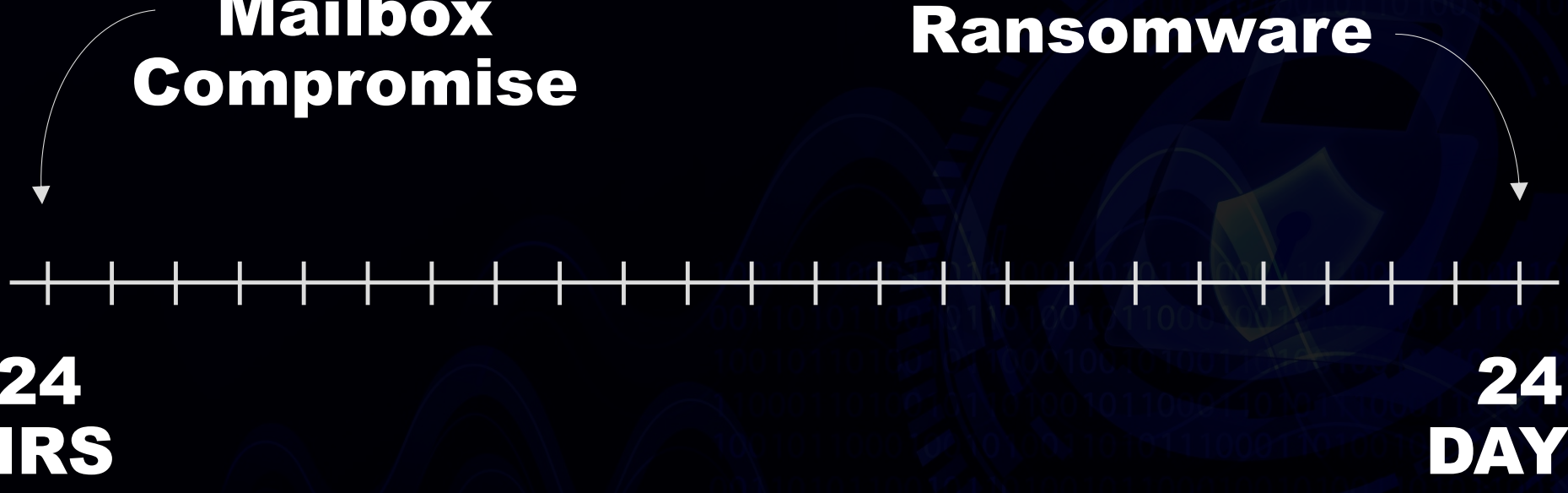
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPLICATIONS					
DATA					
USERS					
DEGREE OF DEPENDENCY	TECHNOLOGY / PEOPLE; PROCESS & GOVERNANCE				
	impact + DOT Security	impact	DOT Security	impact + DOT Security	

impact

Response Lifecycle



Average Recovery Times



impact

Real World Stories

impact

Business Email Compromise

Company Profile	Cold Storage Warehousing 50 Employees Internal IT Team DOT Security Cyber Team
Attack Profile	Stolen Credentials Used MFA Bombing
Organization Impact	User Mailbox Rules User Impacted for the Day
Preventative Measures	End User Education

impact

Ransomware

Company Profile	Oregon & Louisiana DMV State IT and Cyber Teams
Attack Profile	Software Vulnerability Attack 6mm and 3.5mm records stolen Drivers License, SSN & PII Data MoveIT Software Bug Data held for extorsion No ransome paid
Organization Impact	Most operations sustained File transfer capabilities impacted
Preventative Measures	Being prepared

impact

Ransomware

Company Profile	Electrical Contractor 250 Employees & 7 locations Part of holding company MSP IT Partner No Cybersecurity Partner
Attack Profile	Encryption of all endpoints $6.5mm ransom demanded

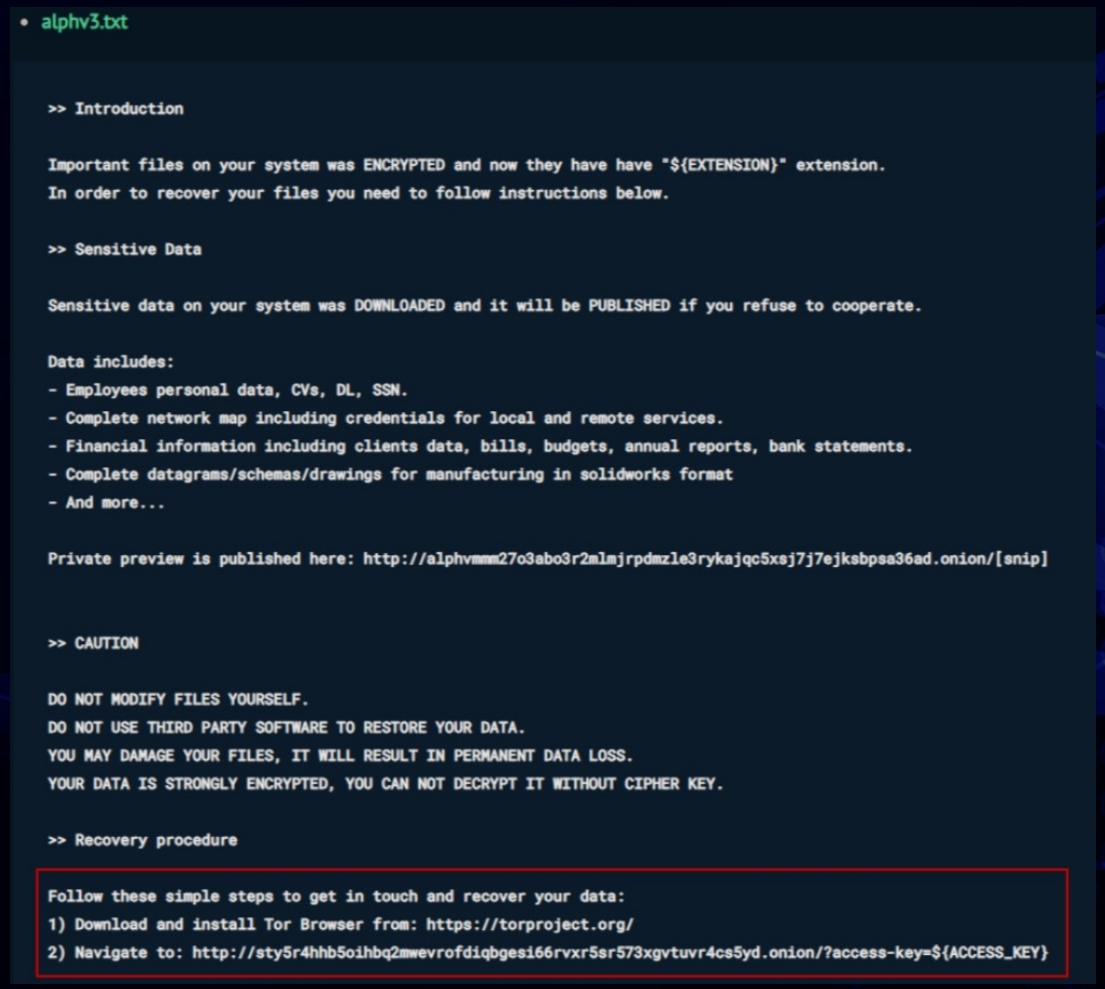
Organization Impact	Loss of operations for 30 days C Level Panic Reputational Loss
Preventative Measures	Improved IT Practices Basic Cybersecurity Services Incident Response Plan

impact

Example Ransomware Screen

impact

Example Ransomware Screen

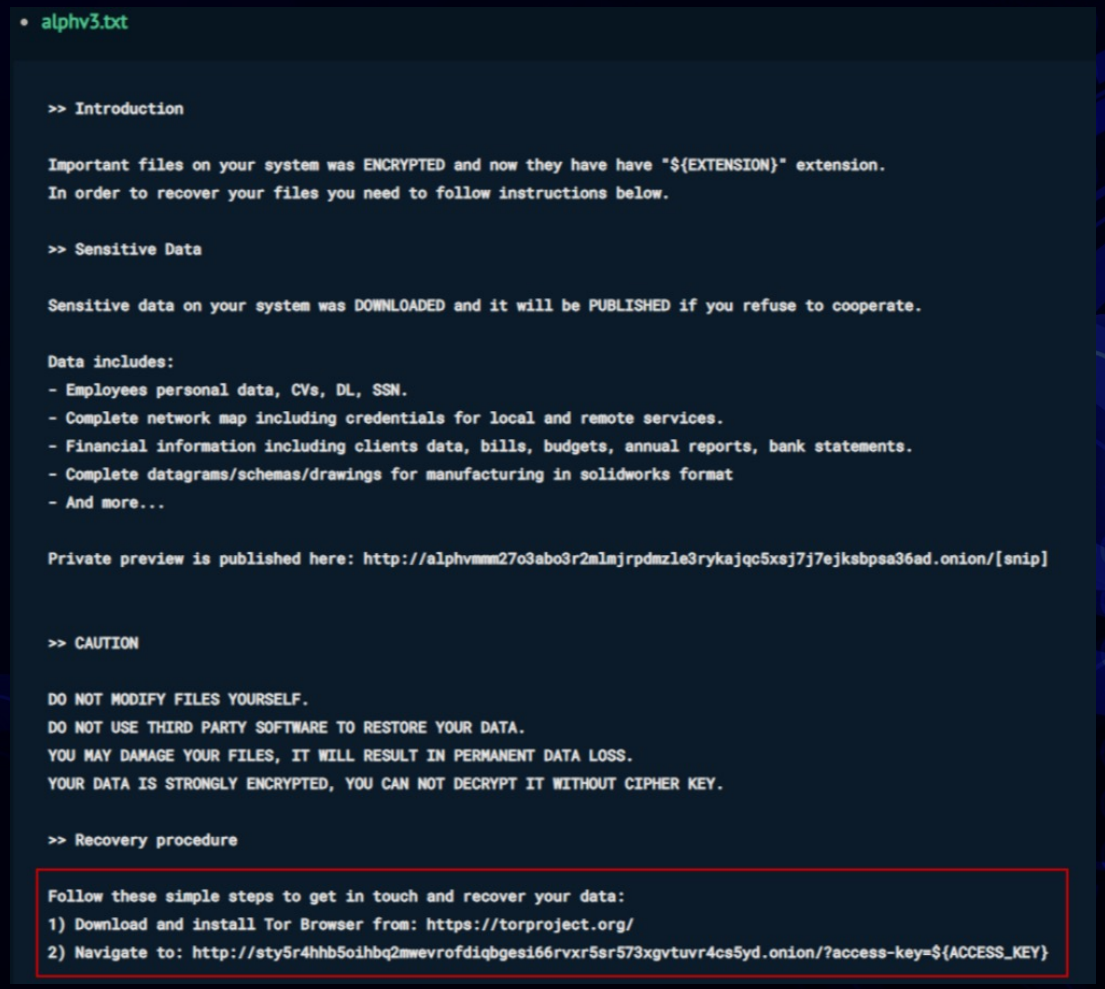


• alphv3.txt

```
>> Introduction

Important files on your system was ENCRYPTED and now they have have "${EXTENSION}" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

Private preview is published here: http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/[snip]


>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=${ACCESS_KEY}
```

impact

Example Ransomware Screen



• alphv3.txt

```
>> Introduction

Important files on your system was ENCRYPTED and now they have have "${EXTENSION}" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

Private preview is published here: http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/[snip]


>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=${ACCESS_KEY}
```

impact

Example Ransomware Chats

[redacted]: Help?

12/30/2020, 2:34:05 PM

Support: Hello

12/30/2020, 2:56:23 PM

Support: Are you ready to negotiate?

12/30/2020, 2:57:23 PM

Support: As you already know - your network and all of your data were encrypted by CONTI team. Besides the encryption process we've downloaded a large pack of your internal documents and files that will be published in case our negotiations fail. How it happens can be seen on our website https://continews.best/ (TOR mirror: http://fylszpcqfel7joif.onion). The recovery price is $8500000 (302.5 BTC). This initial offer is based on the details about your revenue and internal financial documents we currently have access to. If you want to make sure we can recover all of your data - you can send us the two files of your choice and we will decrypt them free of charge. If we reach mutual agreement your will be provided with decryption tool, none of your internal data will be published, all the backdoors will be removed from your network and you will be provided with security tips on how to avoid further breaches. We strongly recommend to review our offer in a timely manner to avoid additional expenses from your side on security software and on building the new network from scratch.

12/30/2020, 3:07:43 PM

[redacted]: That's a crazy price. How do we even know if this will work?

12/30/2020, 3:14:33 PM

Support: You can send 2 files for decrypt. Its free.

12/30/2020, 3:15:25 PM

Support: Are you ready to transfer money?

1/8/2021, 2:41:45 PM

[redacted]: Yes. I would like to fix the problem but I don't have this amount of money. Please tell me how we can resolve.

1/8/2021, 5:27:46 PM

Support: According to the public records your revenue is [more than 30],000,000$, so this price is reasonable. https://www.dnb.com/business-directory/company-profiles.[redacted].html Also you should remember that the price is much cheaper then you will pay lawsuits, that your clients will send you and government fines, because you have lost so much of their data.

1/8/2021, 5:37:26 PM

[redacted]: We would like to fix this problem but we have been out of service during Covid and do not have this amount of money. I am trying to fix and please let me know what we can do.

1/8/2021, 7:09:42 PM

Support: What is your best proposal?

1/8/2021, 7:12:28 PM

[redacted]: I have the ability to send 20,000 as soon as I can transfer money. I would like to get this fixed and please let me know if we can get this fixed.

1/8/2021, 7:40:16 PM

[redacted]: How can we test to see if this can be fixed?

1/8/2021, 7:41:25 PM

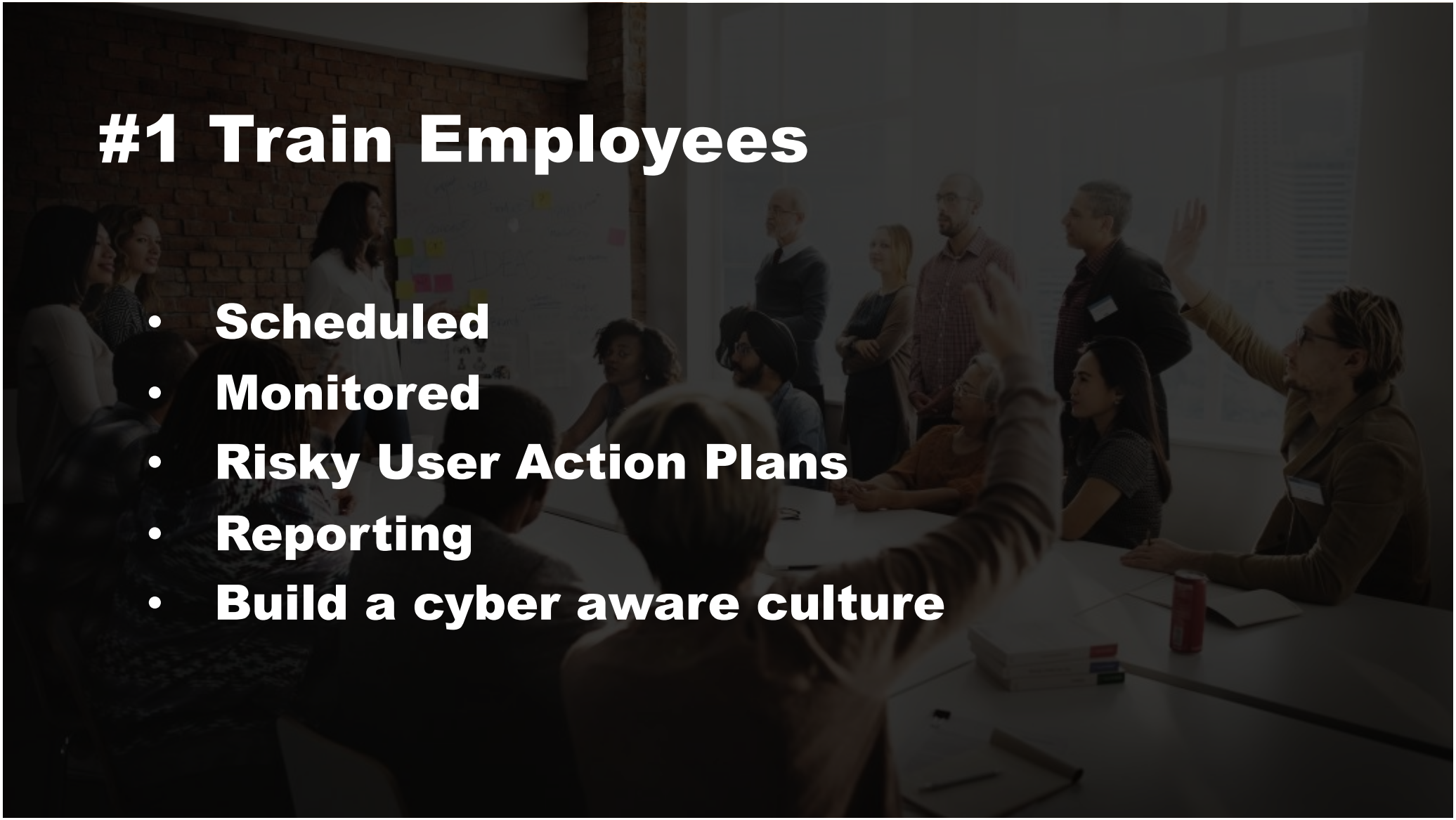
Support: We could not accept that offer, but we could reduce the price and give you the new one 800,000$. We could decrypt 1-2 files as samples.

1/8/2021, 8:04:33 PM

impact

Top 5 Cybersecurity Tips

impact



#1 Train Employees

- Scheduled
- Monitored
- Risky User Action Plans
- Reporting
- Build a cyber aware culture

#2 Unknown System Bugs

- Know what systems you have
- Patch hardware & software monthly – quarterly
- Apply critical patches ASAP
- Manage patch health

#3 Have a Cybersecurity Strategy

- Perform a Risk Audit
- Provide a Board Room Seat
- Cybersecurity Maturity Roadmap
- Tested Incident Response Plan

#4 Identify & Monitor Assets

- Clear reporting of users, licenses, subscriptions and devices
- Reporting of system health
- Properly managed Endpoint Detection & Response (EDR) software
- Property managed Security Information & Event Management (SIEM) Software

impact

#5 Replace Outdated Systems

- Do not use unsupported systems
- Segment outdated systems
- Wrap higher level security controls around higher risk systems

Top Personal Cybersecurity Tips

Top Personal Cybersecurity Tips

- Keep your technology updated
- Use a password manager
- Backup your data
- Trust but verify
- Freeze your credit

impact

Q&A

Thank You

Jeremiah School
920-750-2679
jschool@dotsecurity.com

impact