Acquisition Hour:

The Basics of Cybersecurity for Any Small Business

January 21 | Noon – 1:00 pm

Presented by:
Matt Frost, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

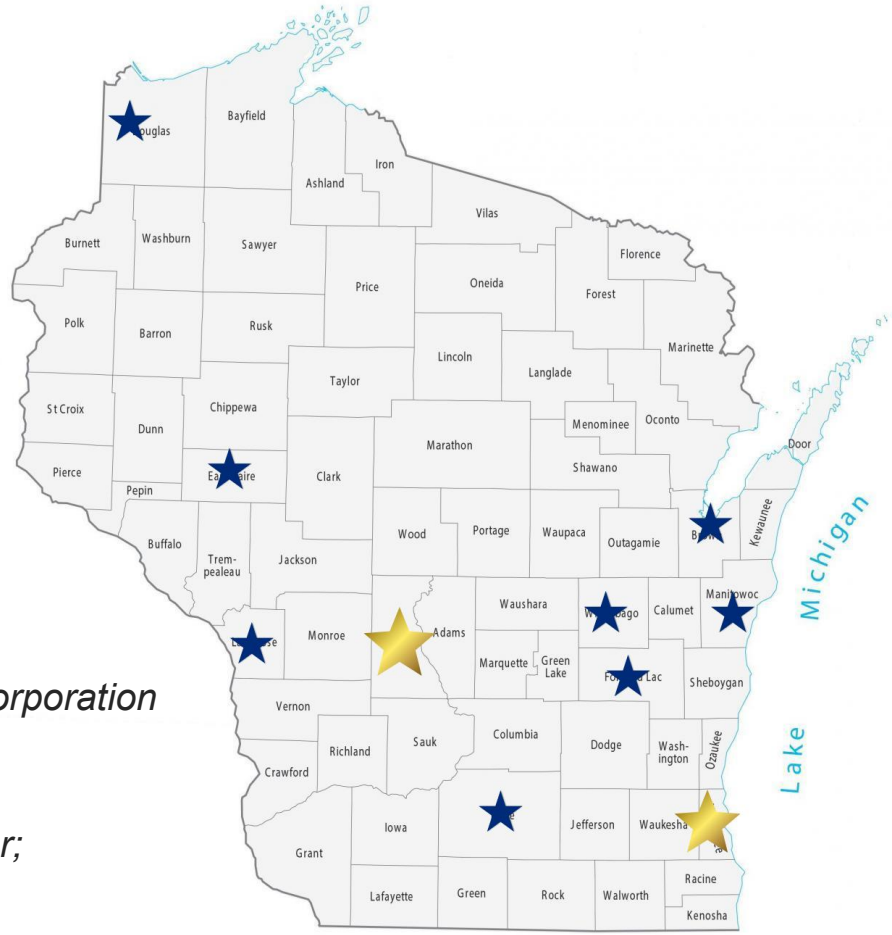
WPI provides services and training to all of Wisconsin's 72 counties

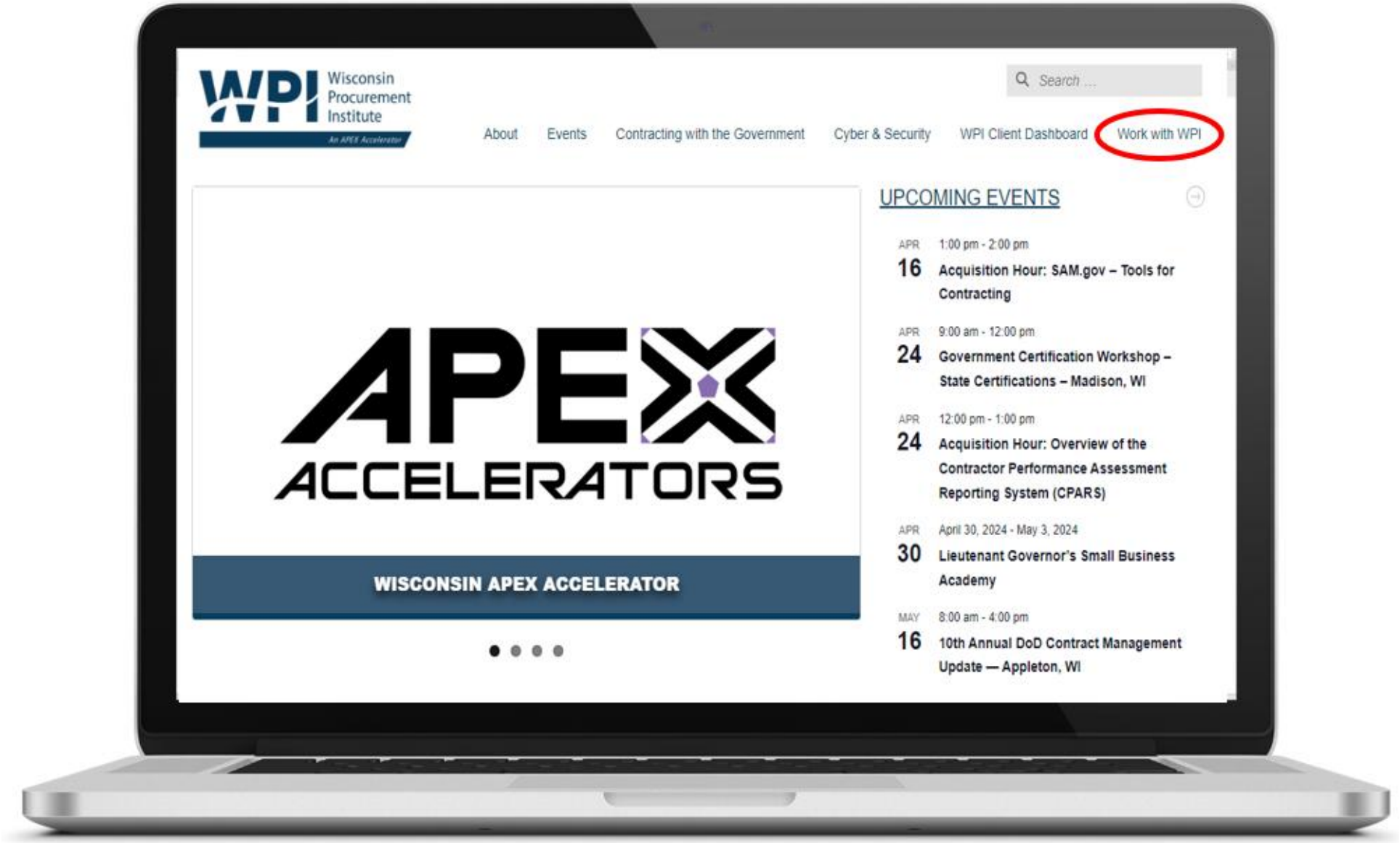
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

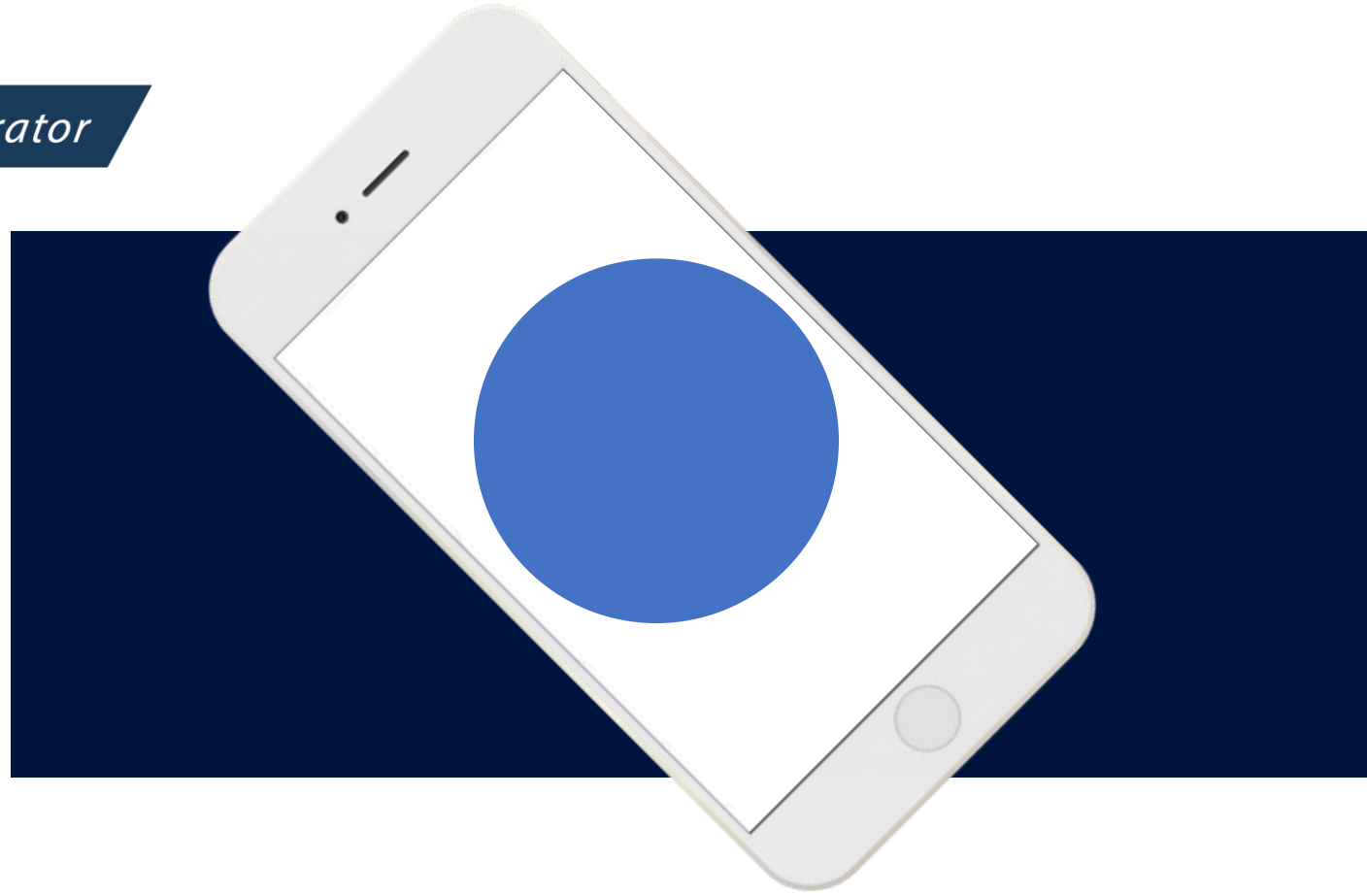



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Wisconsin Procurement Institute

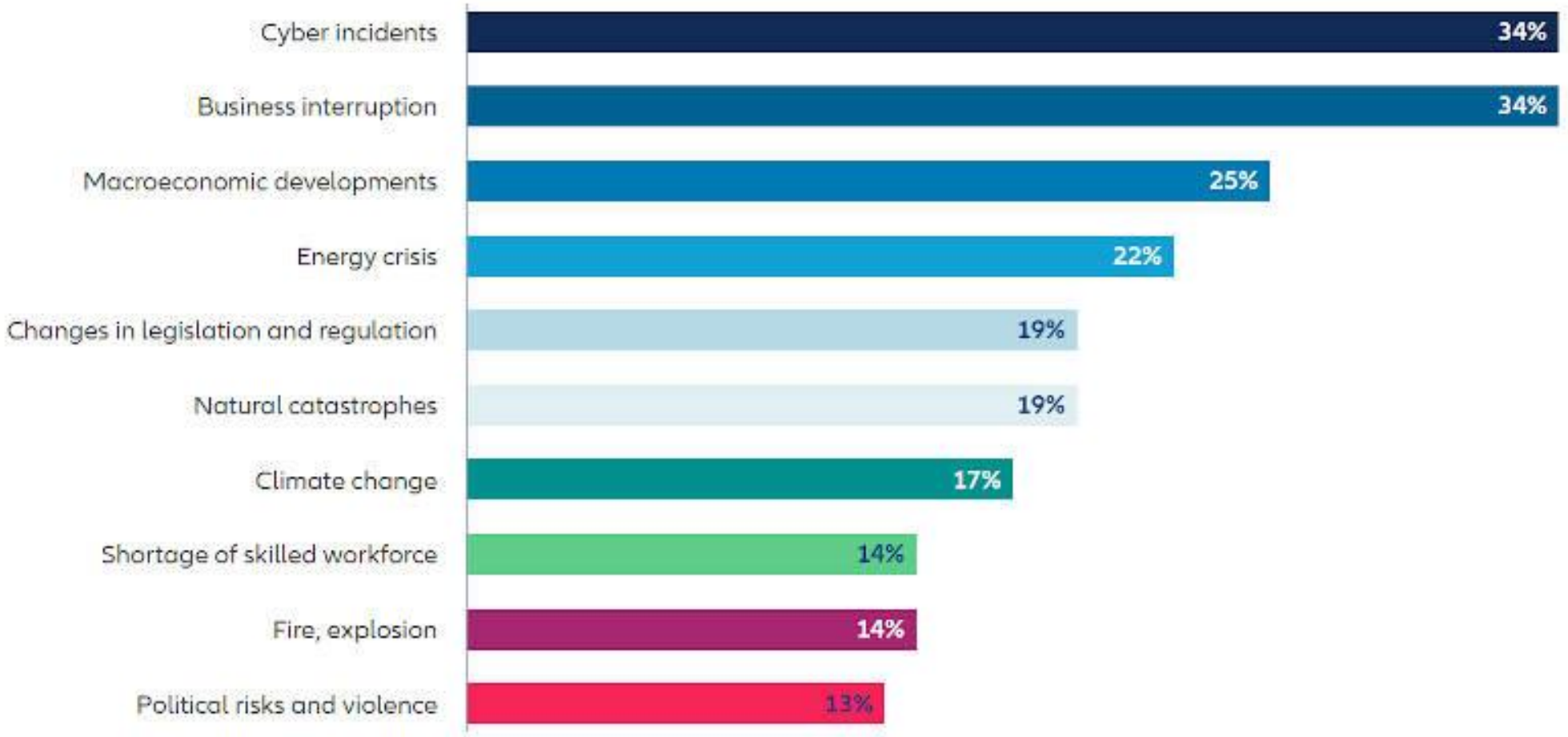
An APEX Accelerator

A Culture of Security



CYBER FRIDAY SESSIONS – January 21st, 2026

Why prepare?



Source: Allianz Risk Barometer 2023

The numbers represent the percentage of all participants who responded (2,712). The numbers do not add up to 100% because more than one risk could be selected.

Why prepare?

IN 2021

50% more attacks on corporate networks compared to 2020. *Checkpoint.com*

37% of malicious email attachments are .zip or .jar extensions. *Kaspersky*

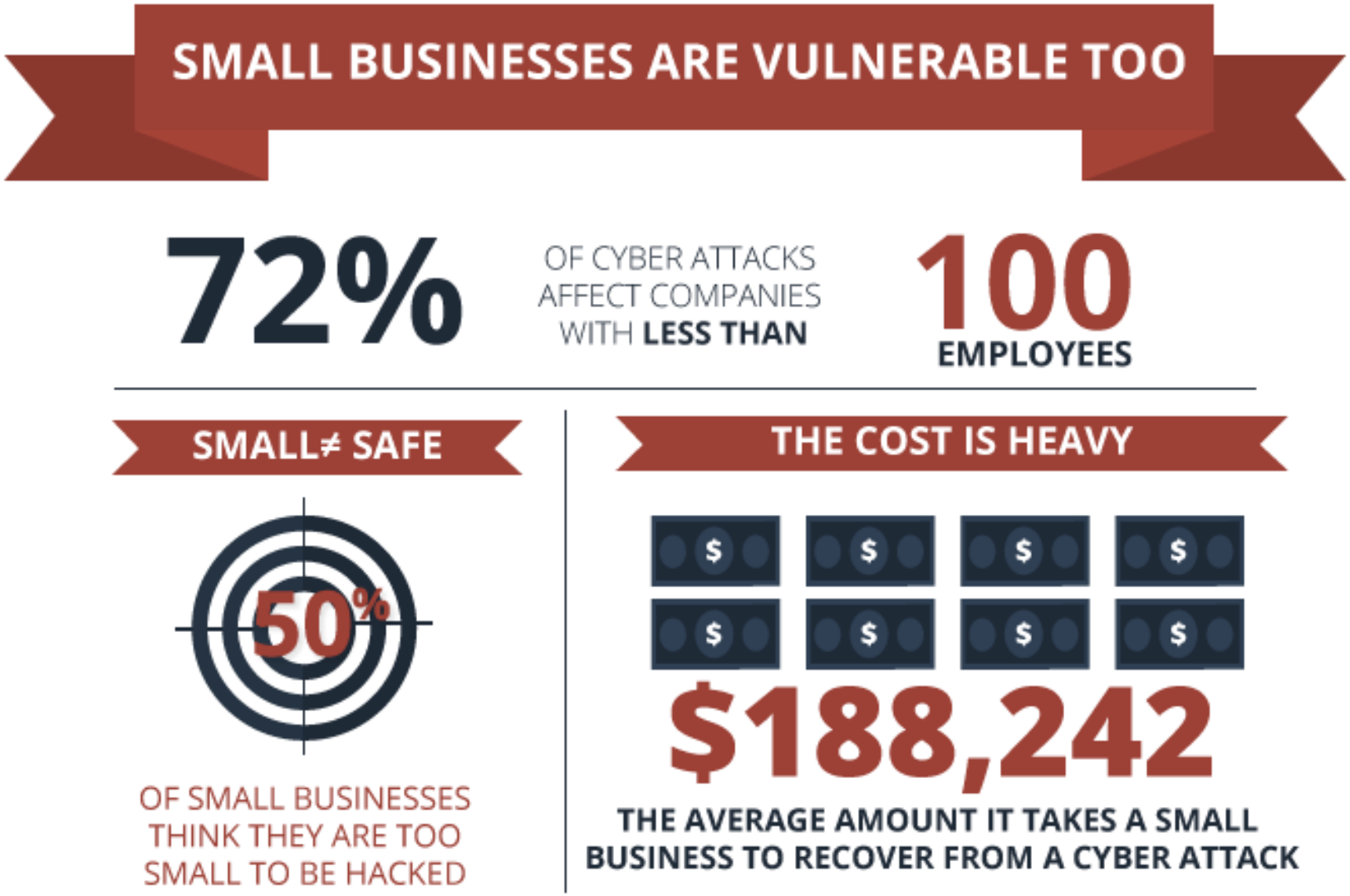
19.5% of malicious email attachments are .exe.

<60% IN 2020 of data breaches were financially motivated.

Government Technology

95% of cyber security breaches are caused by human error. *IBM*

Too small to see?



Owning Your Security

1 THREAT ENVIRONMENT

2 CASE STUDIES

3 PRACTICES

Types of Bad Actors

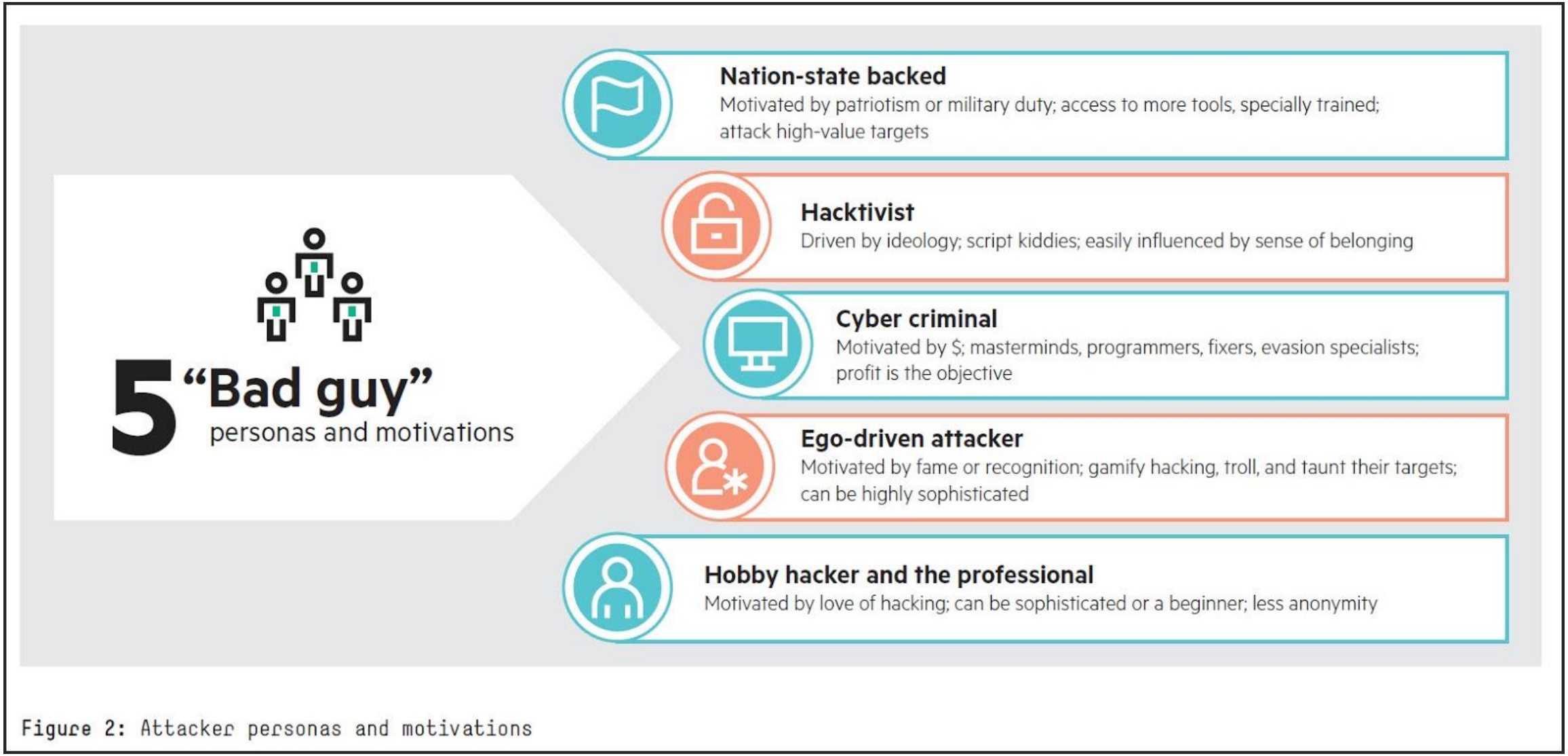
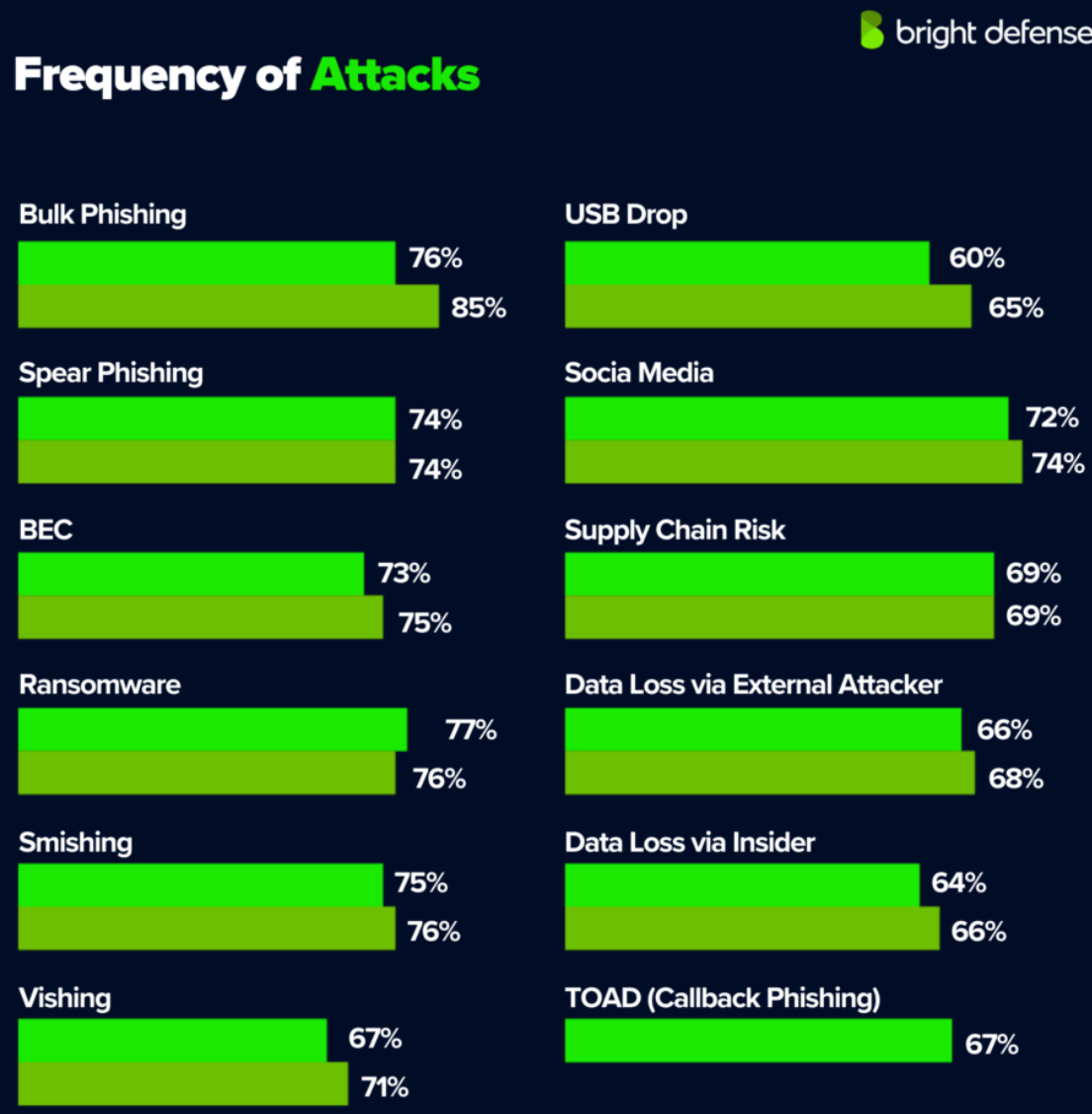


Figure 2: Attacker personas and motivations

Wow. That escalated quickly! (From Checkpoint)



The Incident Response Plan

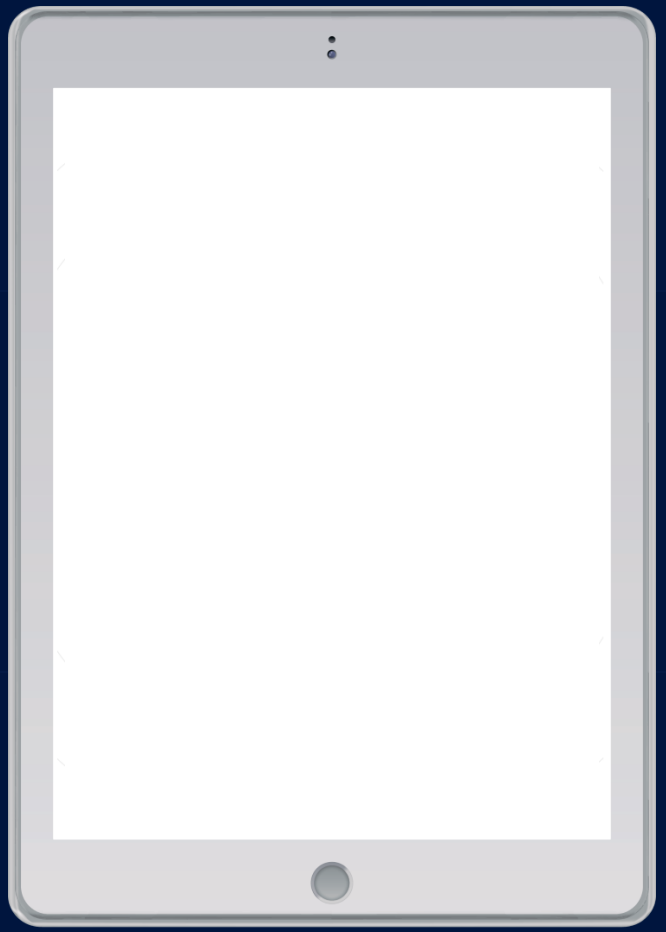
NIST SP 800-61

1 THREAT ENVIRONMENT

2 CASE STUDIES

3 PRACTICES

1 RANSOMEWARE



REFRIGERATED CONSUMABLES

Annual Revenue: 30 Million

Date of Attack: December 2017

FAILURE TO REPORT

Employee recognized they had encountered a suspicious event but failed to report it.

EVENT LASTED NEARLY 16 DAYS

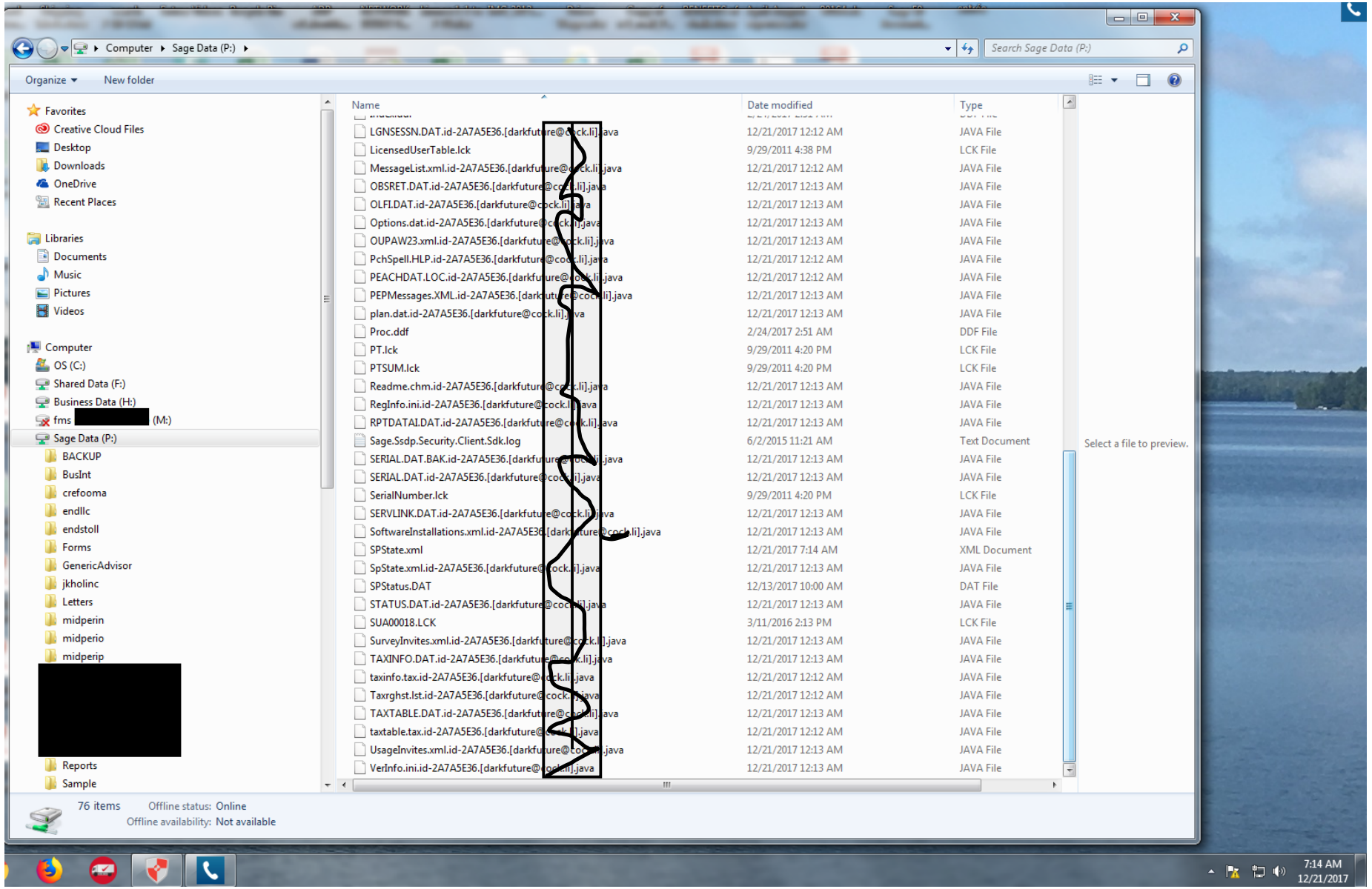
Initial Infection (1 Week Prior to Report)

Malware Propagation (5 Days Prior to Report)

Ransomware Activation Friday 7:00pm CST

Notification Monday, 6:45AM CST

Full Functionality Restored 9 Days Later


Computer ▸ Sage Data (P:) ▸
Search Sage Data (P:)
Organize
New folder
Favorites
Creative Cloud Files
Desktop
Downloads
OneDrive
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
OS (C:)
Shared Data (F:)
Business Data (H:)
fms [redacted] (M:)
Sage Data (P:)
BACKUP
BusInt
crefooma
endllc
endstoll
Forms
GenericAdvisor
jkholinc
Letters
midperin
midperio
midperip
[redacted]
Reports
Sample
Name
Date modified
Type
LGNSESSN.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
LicensedUserTable.lck 9/29/2011 4:38 PM LCK File
MessageList.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
OBSRET.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
OLFI.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
Options.dat.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
OUPAW23.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
PchSpell.HLP.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
PEACHDAT.LOC.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
PEPMessages.XML.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
plan.dat.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
Proc.ddf 2/24/2017 2:51 AM DDF File
PT.lck 9/29/2011 4:20 PM LCK File
PTSUM.lck 9/29/2011 4:20 PM LCK File
Readme.chm.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
RegInfo.ini.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
RPTDATAI.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
Sage.Ssdp.Security.Client.Sdk.log 6/2/2015 11:21 AM Text Document
SERIAL.DAT.BAK.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SERIAL.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SerialNumber.lck 9/29/2011 4:20 PM LCK File
SERVLINK.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SoftwareInstallations.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SPState.xml 12/21/2017 7:14 AM XML Document
SpState.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SPStatus.DAT 12/13/2017 10:00 AM DAT File
STATUS.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
SUA00018.LCK 3/11/2016 2:13 PM LCK File
SurveyInvites.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
TAXINFO.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
taxinfo.tax.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
Taxrghst.lst.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
TAXTABLE.DAT.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
taxtable.tax.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:12 AM JAVA File
UsageInvites.xml.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
VerInfo.ini.id-2A7A5E36.[darkfuture@cock.li].java 12/21/2017 12:13 AM JAVA File
Select a file to preview.
76 items
Offline status: Online
Offline availability: Not available
7:14 AM
12/21/2017

Employee Responses

59

Paid Ransom

Fear Loss of Reputation
Fear Loss of Pride
Believe They Are Personally Targetted

73

Are Millenials

Younger employees are in a less-secure position professionally, tend to feel they are competing for recognition and reputation, have a deep distrust of management support.

1,400

Average Payout

Typically are re-ransomed within 6 weeks.

20

Data Not Recovered

And in nearly every case this employee was often not the only employee affected.

GENERAL CONTRACTORS

Annual Revenue: 10 Million

Date of Attack: March 2018

FAILURE TO RECOGNIZE

Employee did not recognize they had been phished – bank did not recognize anomaly

EVENT LASTED ONLY 3 HOURS

Employee Phished

Wire Transfer Request to Bank for $40,000

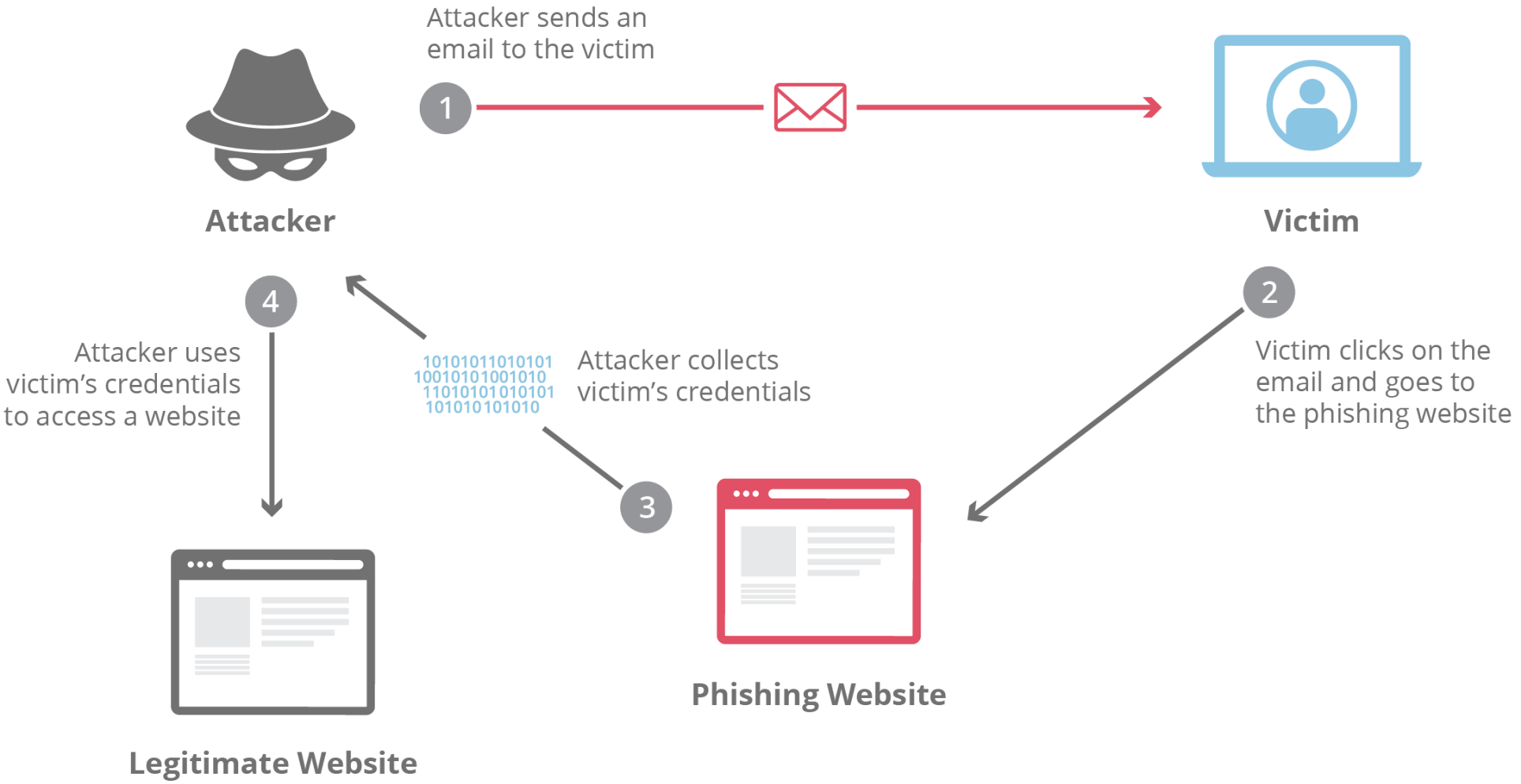
Payroll Company Issues Check in Excess of $16,000

Suspicious Email Reported 11:00 AM CST

Bank Calls Company to Verify Wire Transfer of $96,000

1 Spear Phish

Anatomy of a Phish



Increasingly Sophisticated

But common threads exist...

6 ways to spot a phishing email

LAN SUPPORT
Managed IT Services

1 Spelling mistakes

This is the most common sign that the email isn't legit. Some are harder to spot, make sure you check in close detail.

2 The email was unexpected

An immediate red flag - if you get an email about something that hasn't happened.

3 A suspicious sense of urgency

Phishing emails try to trick you into acting immediately in case something bad has happened.

4 Uses generic salutations

Legit companies often directly refer to you by your name, rather than 'Dear customer' etc.

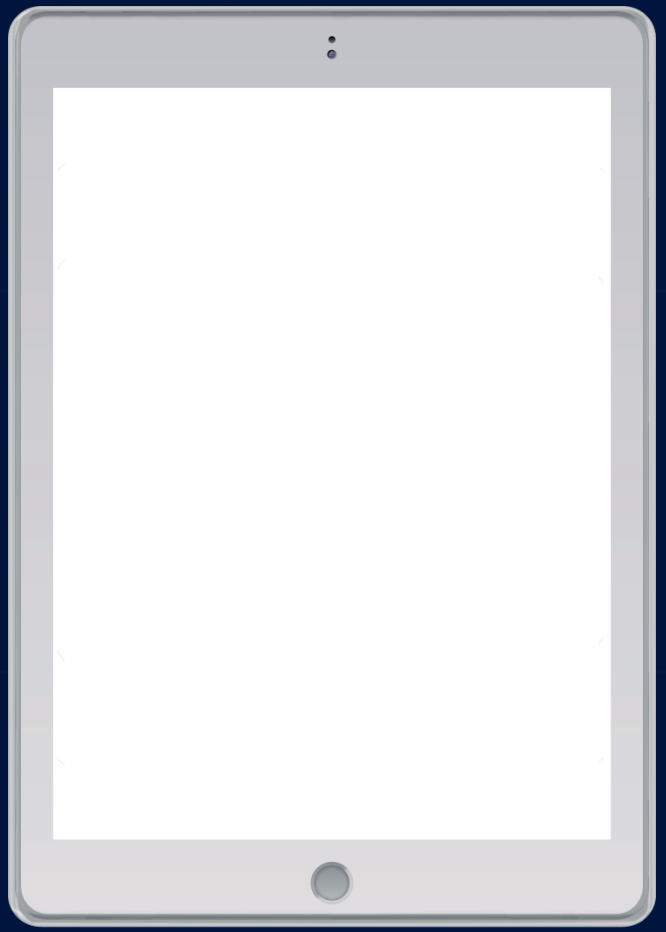
5 Includes an unusual attachment

Almost all emails with attachments should be treated as suspicious, especially if they have file extensions such as .zip, .rar, .scr etc.

6 Requesting personal information

Never give out personal information via email. Reputable companies will never ask for this, so it is likely to be a phishing email.

1 Comprehensive Breach



CUSTOM ROBOTICS MANUFACTURER

Annual Revenue: 100 Million

Date of Attack: January 2014

MASSIVE FTP INFO EXTRACTION

Bandwidth so entirely consumed that email and other functional traffic was more or less halted.

EVENT LASTED NEARLY 10 MONTHS

Initial Infection (20 Weeks Prior to Report)

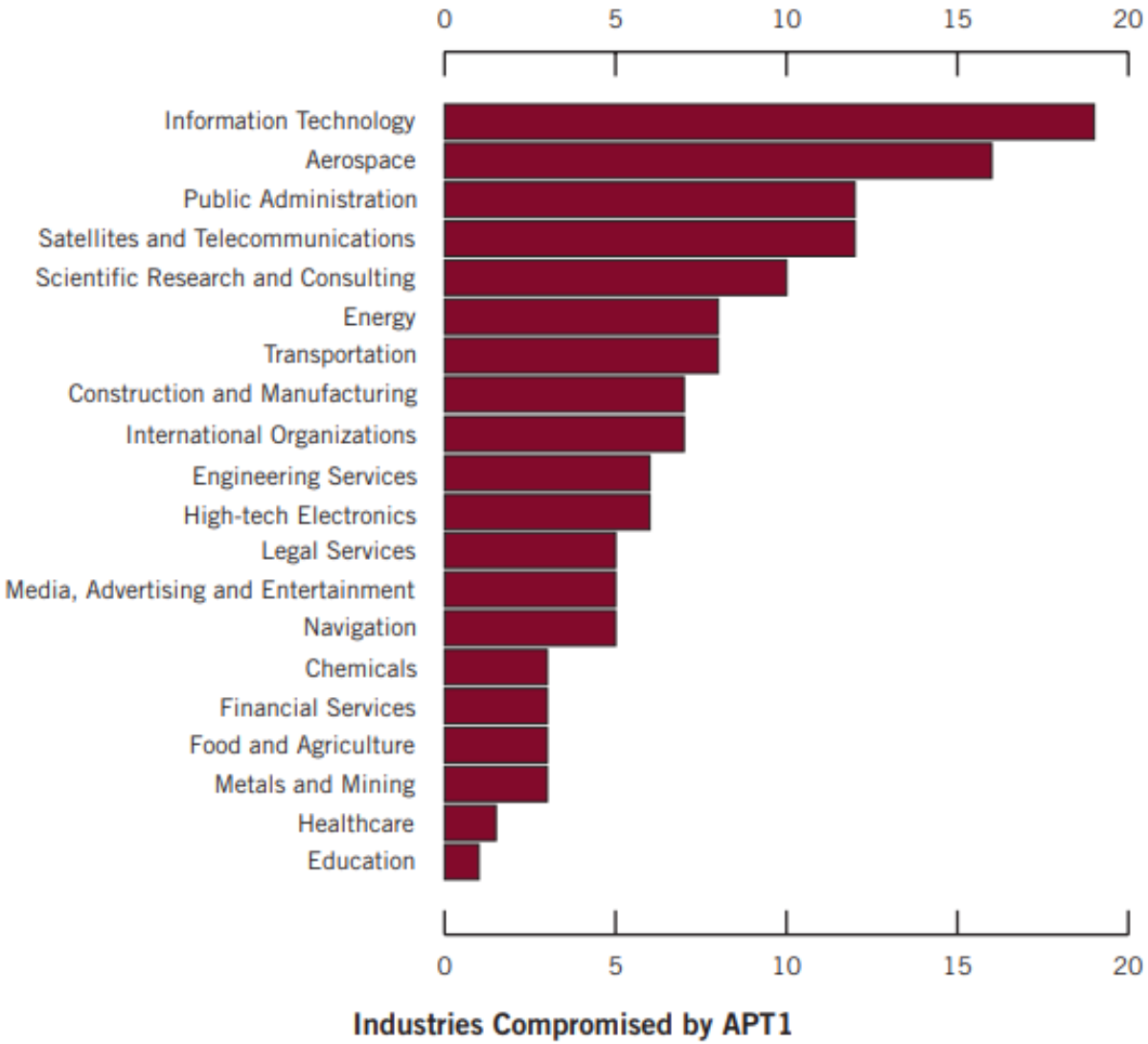
Scouting and Recon

CISO Notified While Playing Golf on the weekend

Size of Breach Discovered

Disclosure to Buyers and General Public

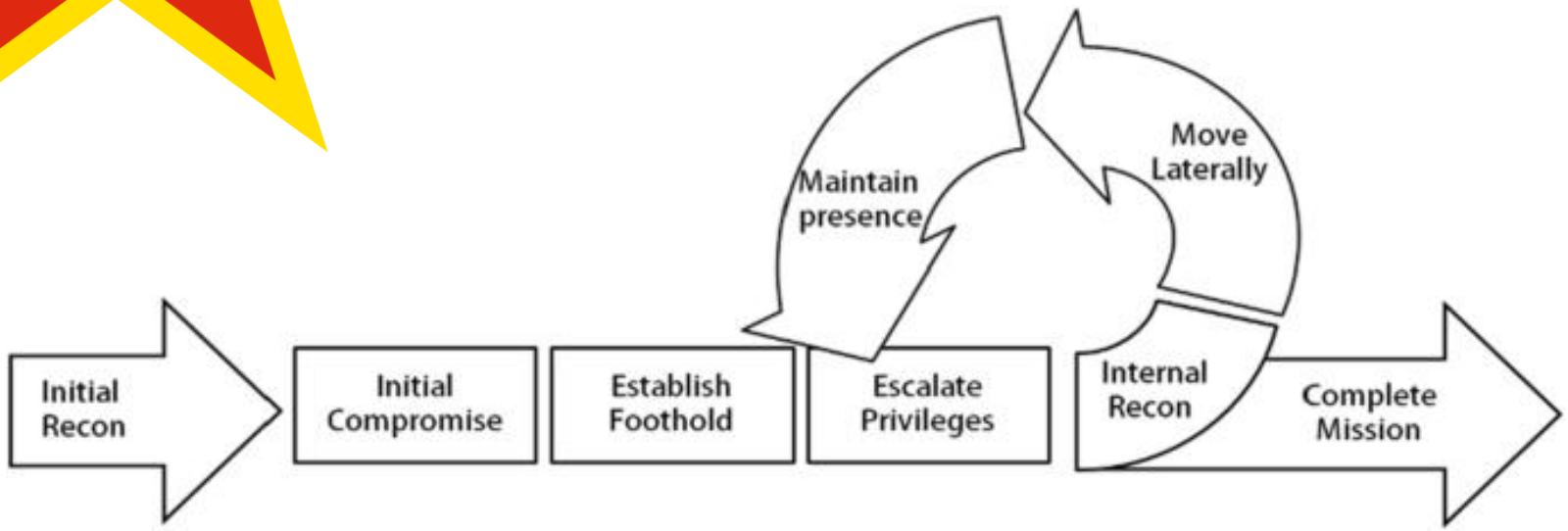
A World at War



Industries Compromised by APT1

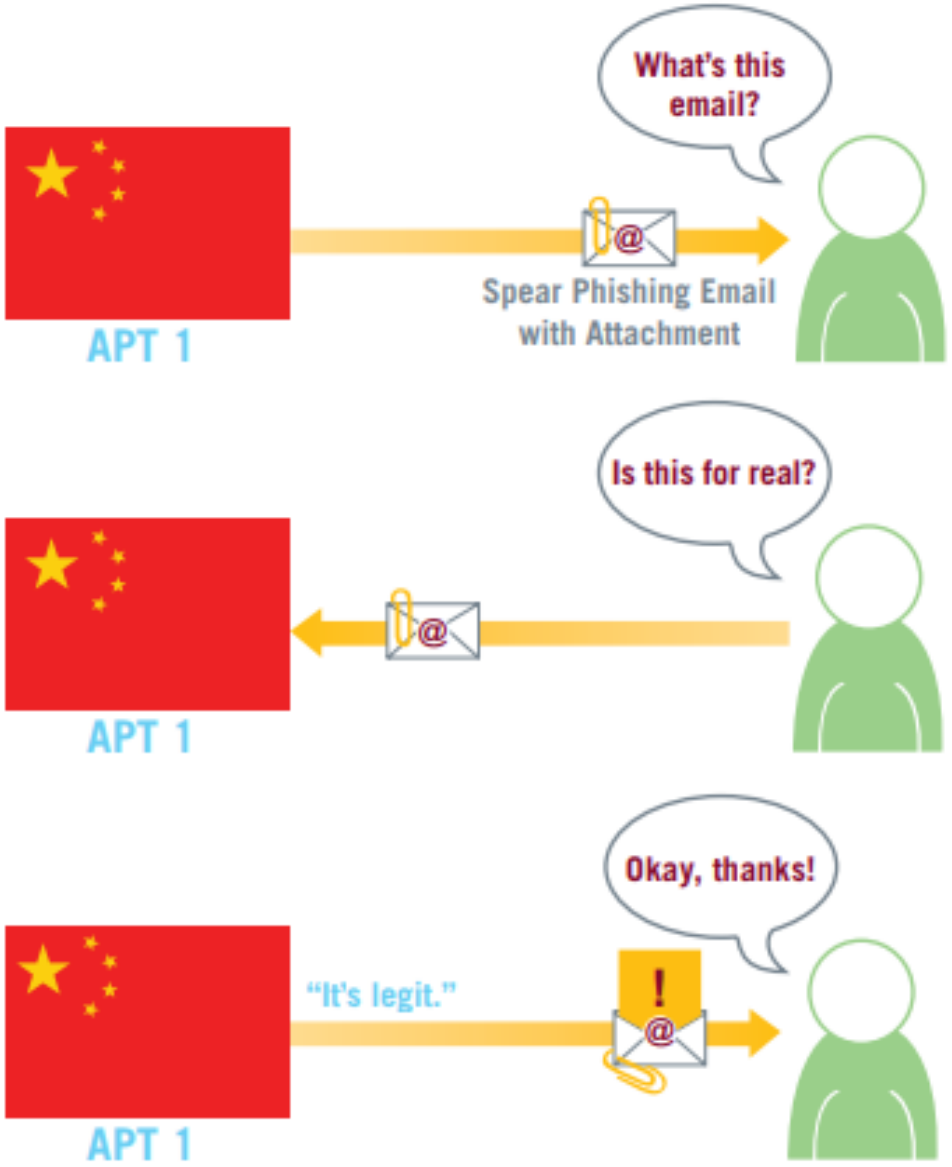
On Multiple Fronts

PLA Unit 61398



Pudong, Shanghai

Big Things Start Small



1

THREAT ENVIRONMENT

2

CASE STUDIES

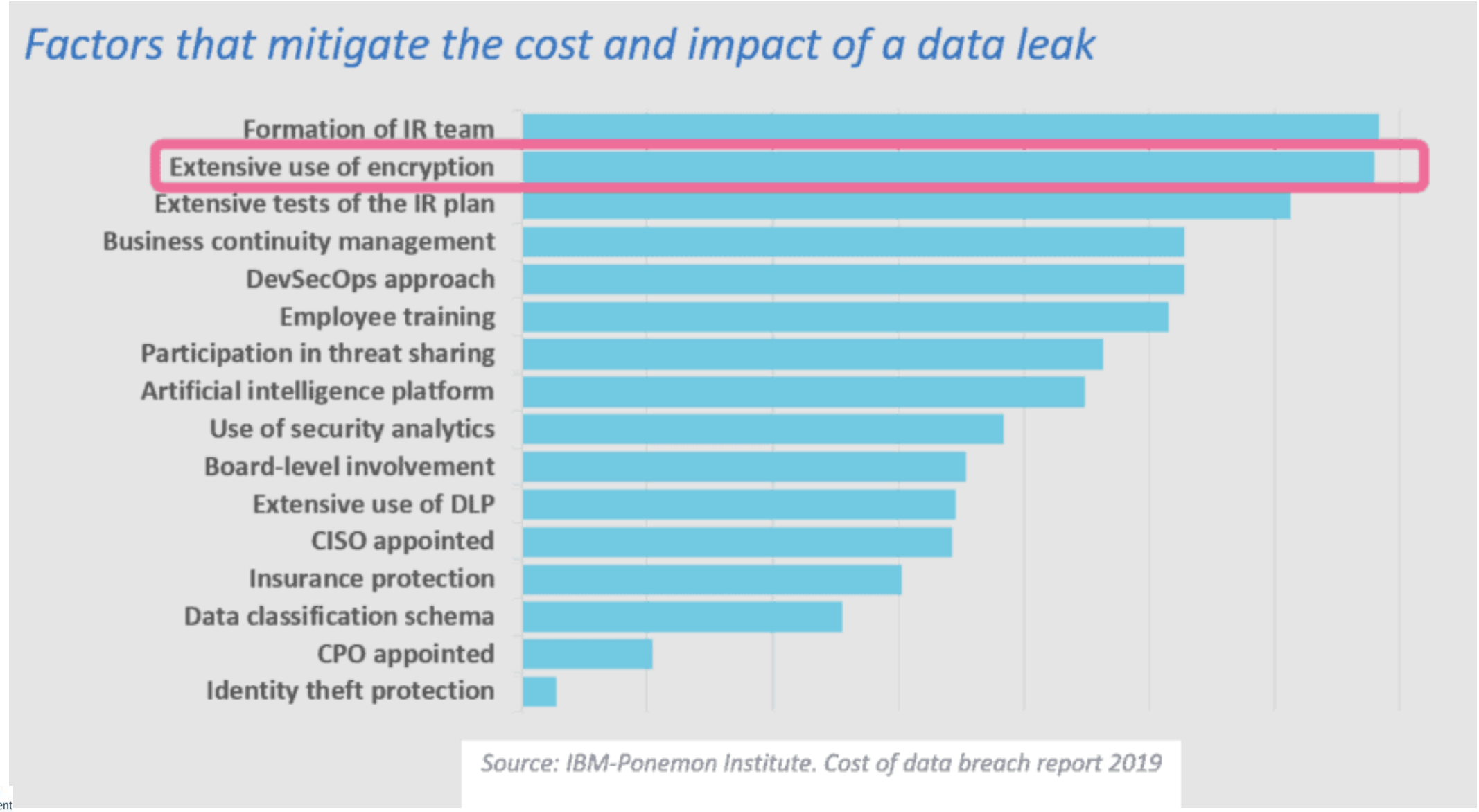
3

PRACTICES

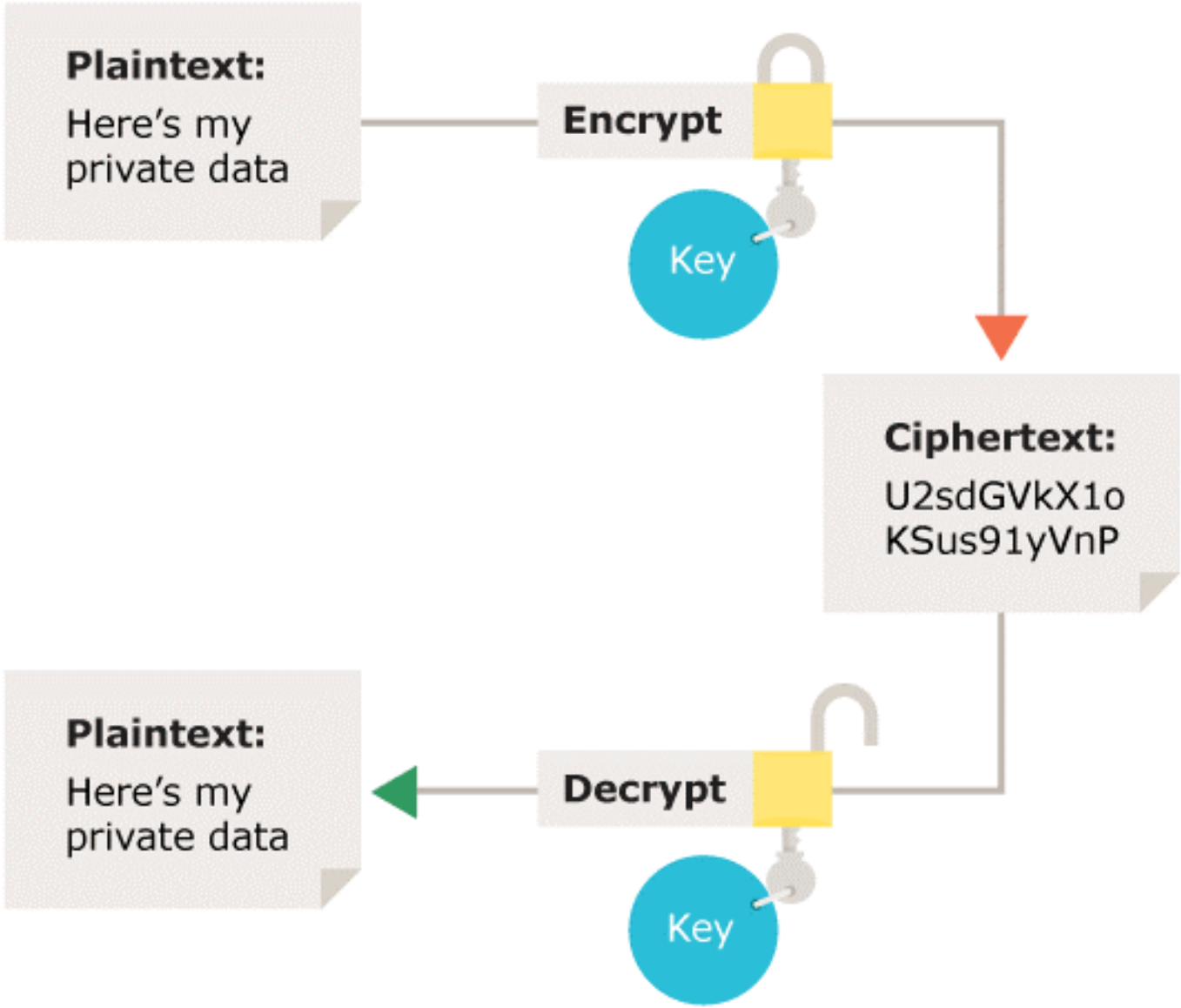
THINGS TO DO

- ✓ TRAIN – If you see something, say something!
- ✓ Take IT Concerns Seriously
- ✓ Create a Supportive Environment
- ✓ Do Not Tolerate Complacency
- ✓ Prepare for the Inevitable

Why encrypt?

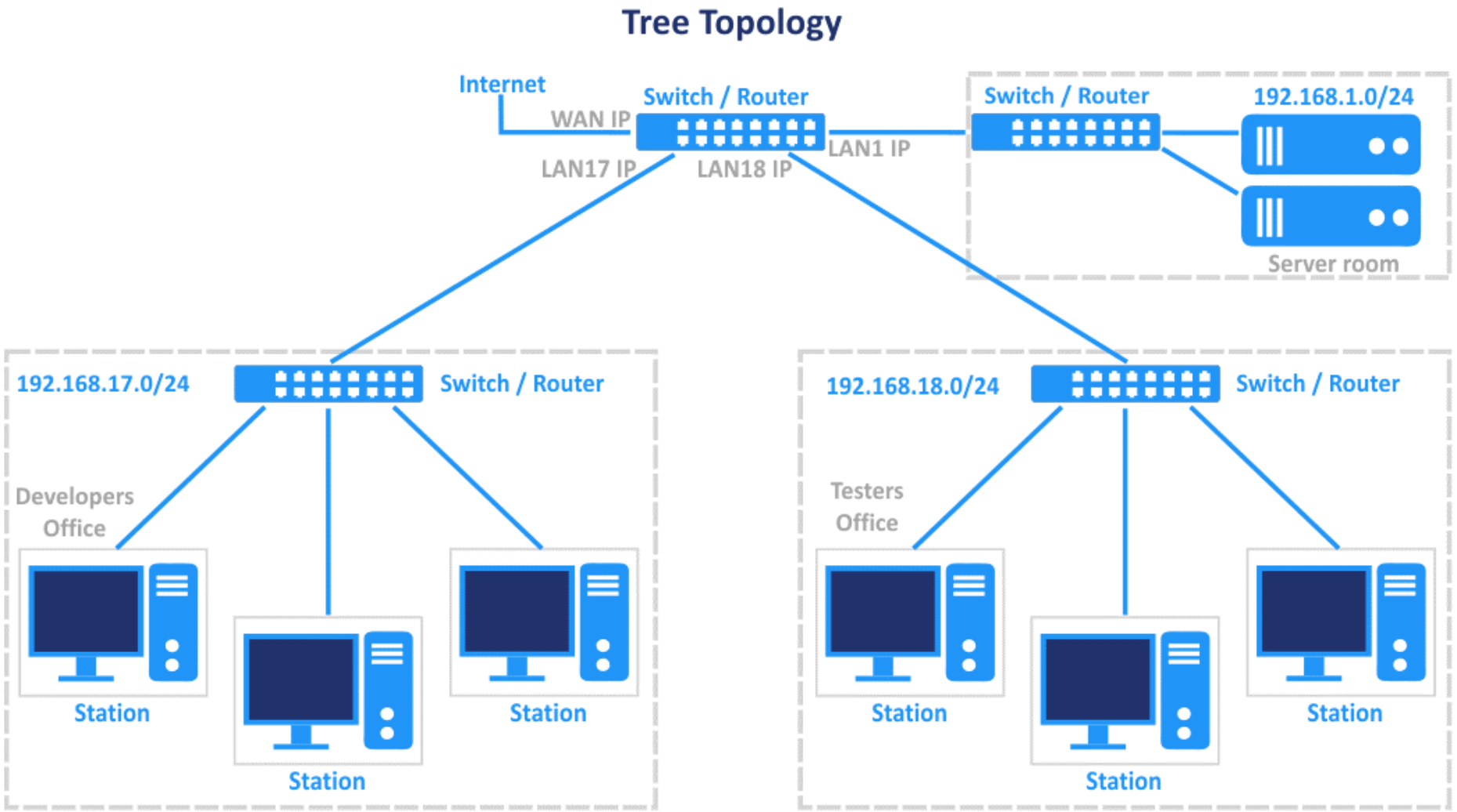

Factors that mitigate the cost and impact of a data leak
Formation of IR team
Extensive use of encryption
Extensive tests of the IR plan
Business continuity management
DevSecOps approach
Employee training
Participation in threat sharing
Artificial intelligence platform
Use of security analytics
Board-level involvement
Extensive use of DLP
CISO appointed
Insurance protection
Data classification schema
CPO appointed
Identity theft protection
Source: IBM-Ponemon Institute. Cost of data breach report 2019

Symmetric vs Asymmetric




At Rest
In Transit

The Visual


Tree Topology
Internet
WAN IP
Switch / Router
LAN17 IP
LAN18 IP
LAN1 IP
Switch / Router
192.168.1.0/24
Server room
192.168.17.0/24
Switch / Router
Developers
Office
Station
Station
Station
192.168.18.0/24
Switch / Router
Testers
Office
Station
Station
Station

4 Pillars of Next-Generation Endpoint Security

01

AI-Powered Threat Intelligence

02

Automated Malware Quarantine

03

Comprehensive Data Loss Prevention

04

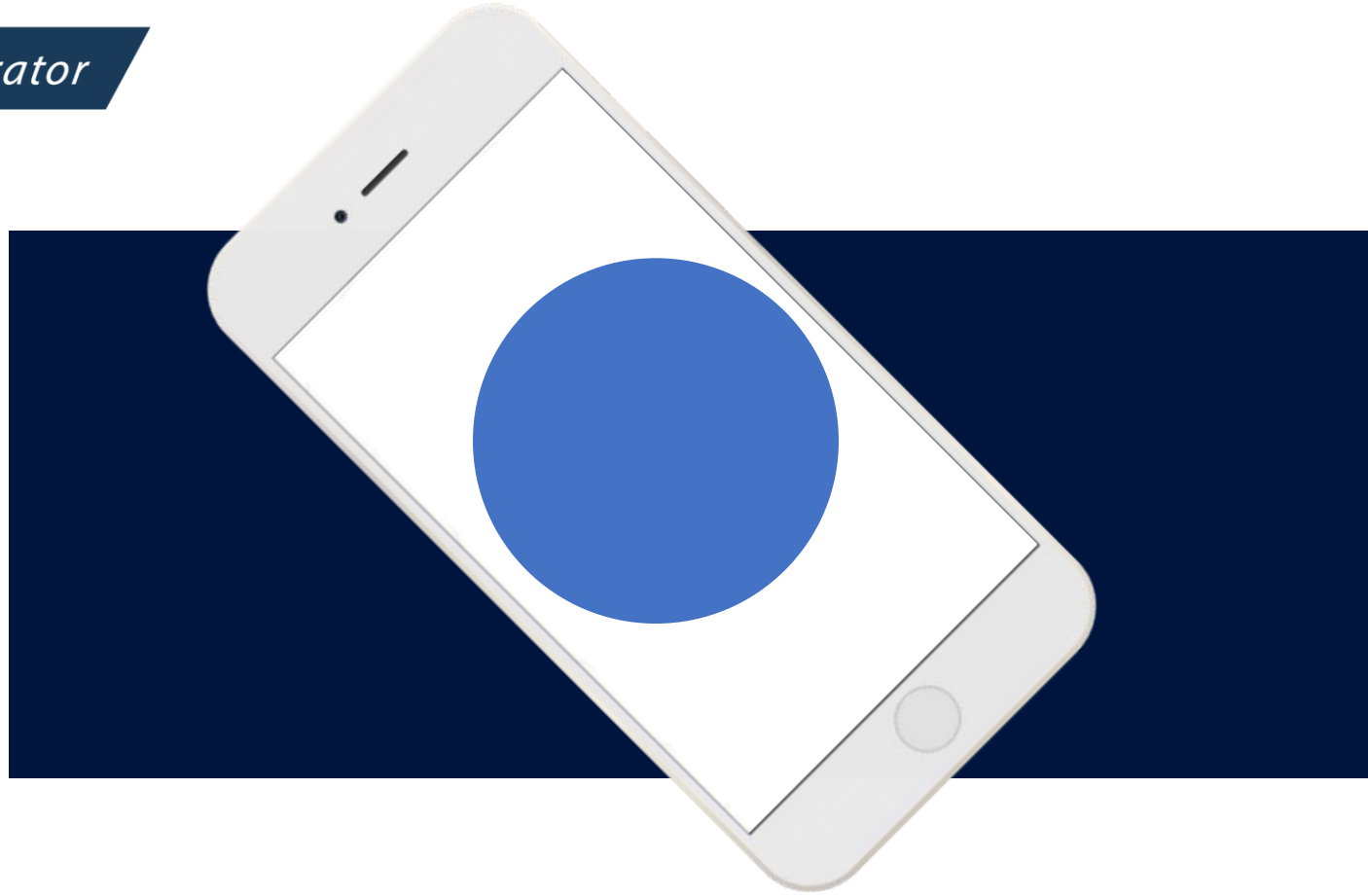
Proactive Vulnerability Management

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org



APEX ACCELERATORS

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **January 21**– The Basics of Cybersecurity for Any Small Business
- **February 11** – Is the GSA Schedule Right for Your Business?
- **February 18** – Overview of the Contractor Performance Assessment Reporting System (CPARS)

…More information and registrations at wispro.org/events

Cyber Thursday

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **January 22** – CMMC: Correctly Scoping Your Environment
- **February 26** – CMMC: Control Set Series: 3.1 Access Control
- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

January 21 2026

This webinar is eligible for

1 CPE credit

To receive a certificate of completion, contact apexaccelerator@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226
414-270-3600