Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

CYBER FRIDAY:

Culture of Security

April 28, 2023 @ 11:00 am - Noon

Presented by Matt Frost, WPI

Wisconsin Procurement Institute

AN APEX ACCELERATOR

Cyber Friday

Webinar Etiquette

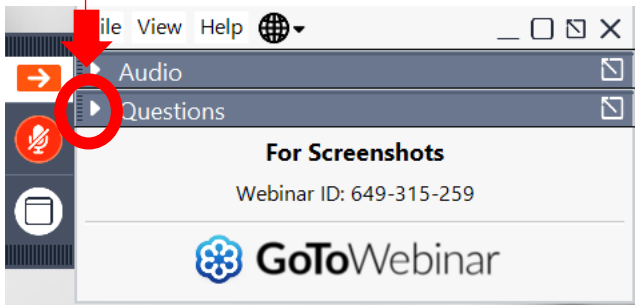
PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

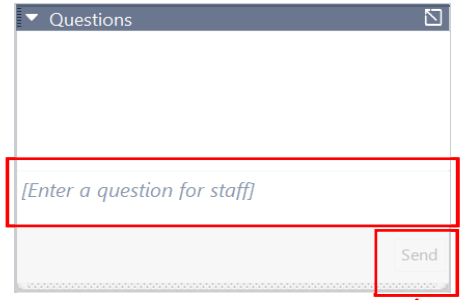
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

WPI is Wisconsin's APEX ACCELERATOR

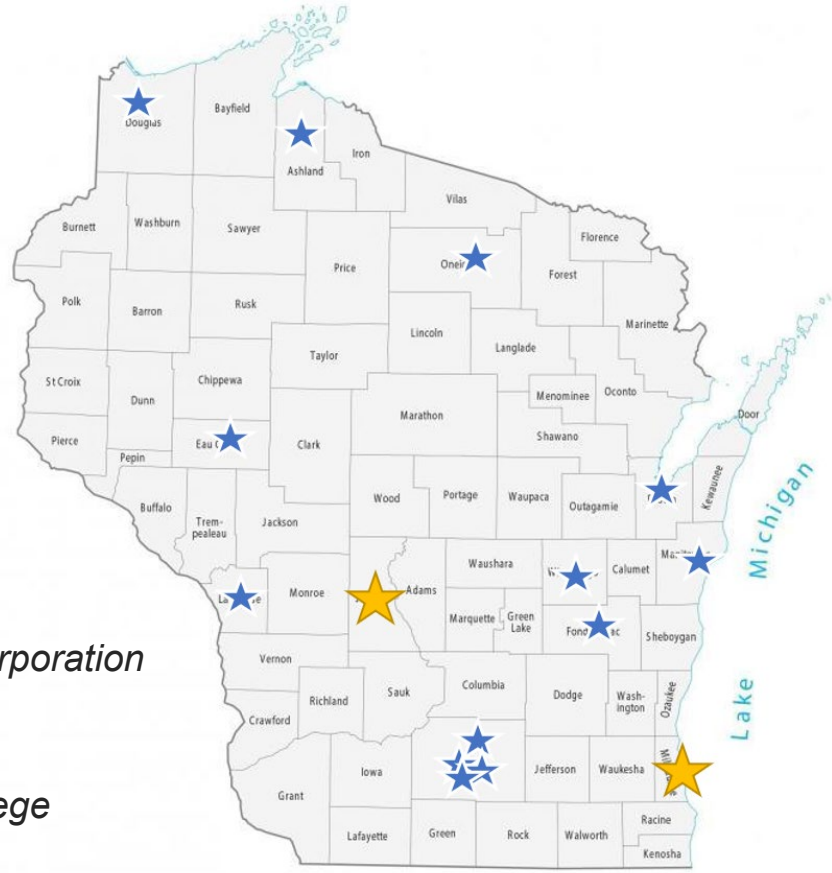
The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides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

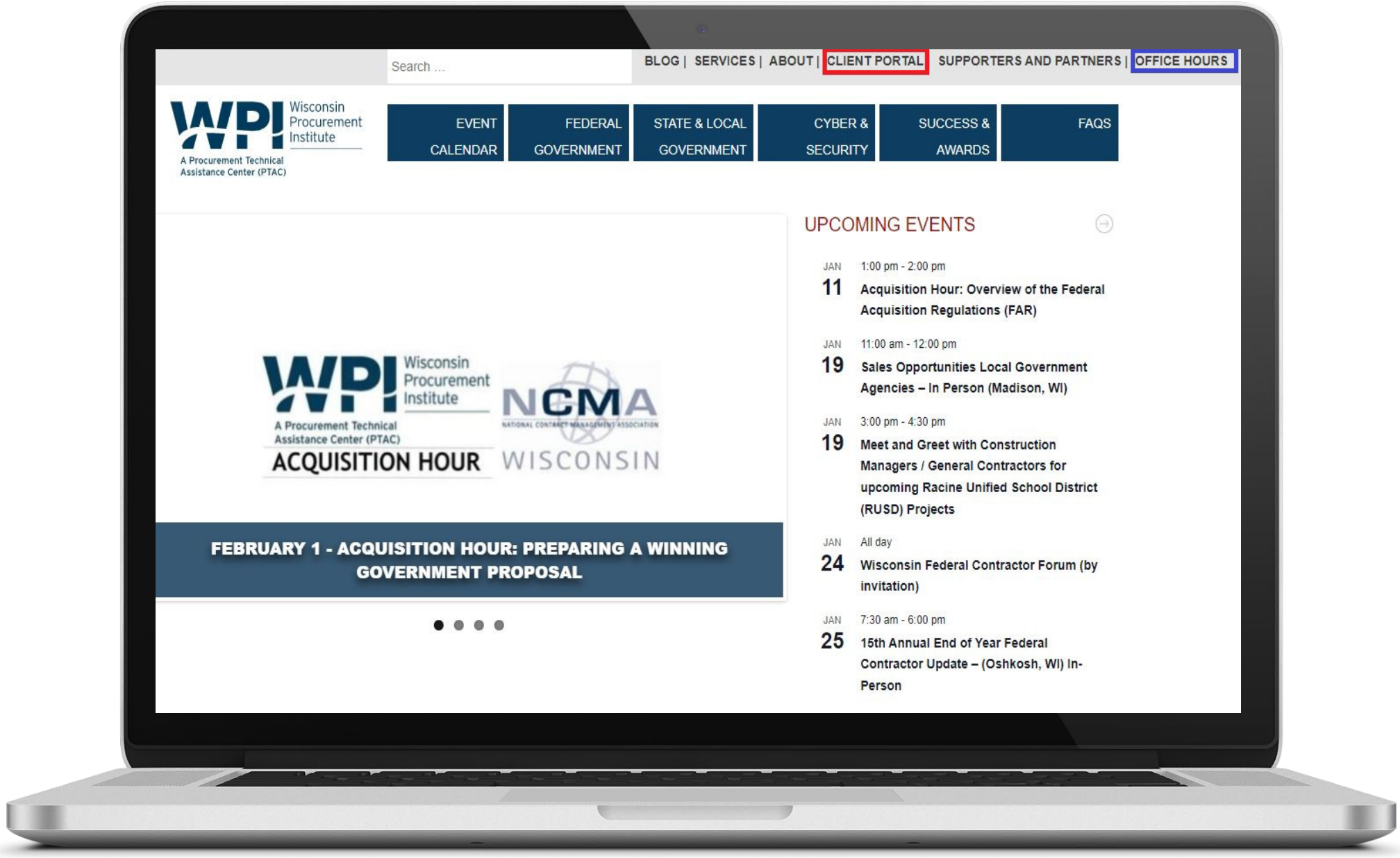
More about WPI

- WPI provides services to all of Wisconsin's 72 counties
  - Individual counseling at our offices, client's facility or virtually
  - Small group training – webinars and workshops
  - Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……
- Last year WPI sponsored or participated in over 80 events
- Last year WPI provided technical assistance to over 1300 companies
- The APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense
- WPI is also funded by the Wisconsin Economic Development Corporation (WEDC), contributions and in-kind

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **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*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

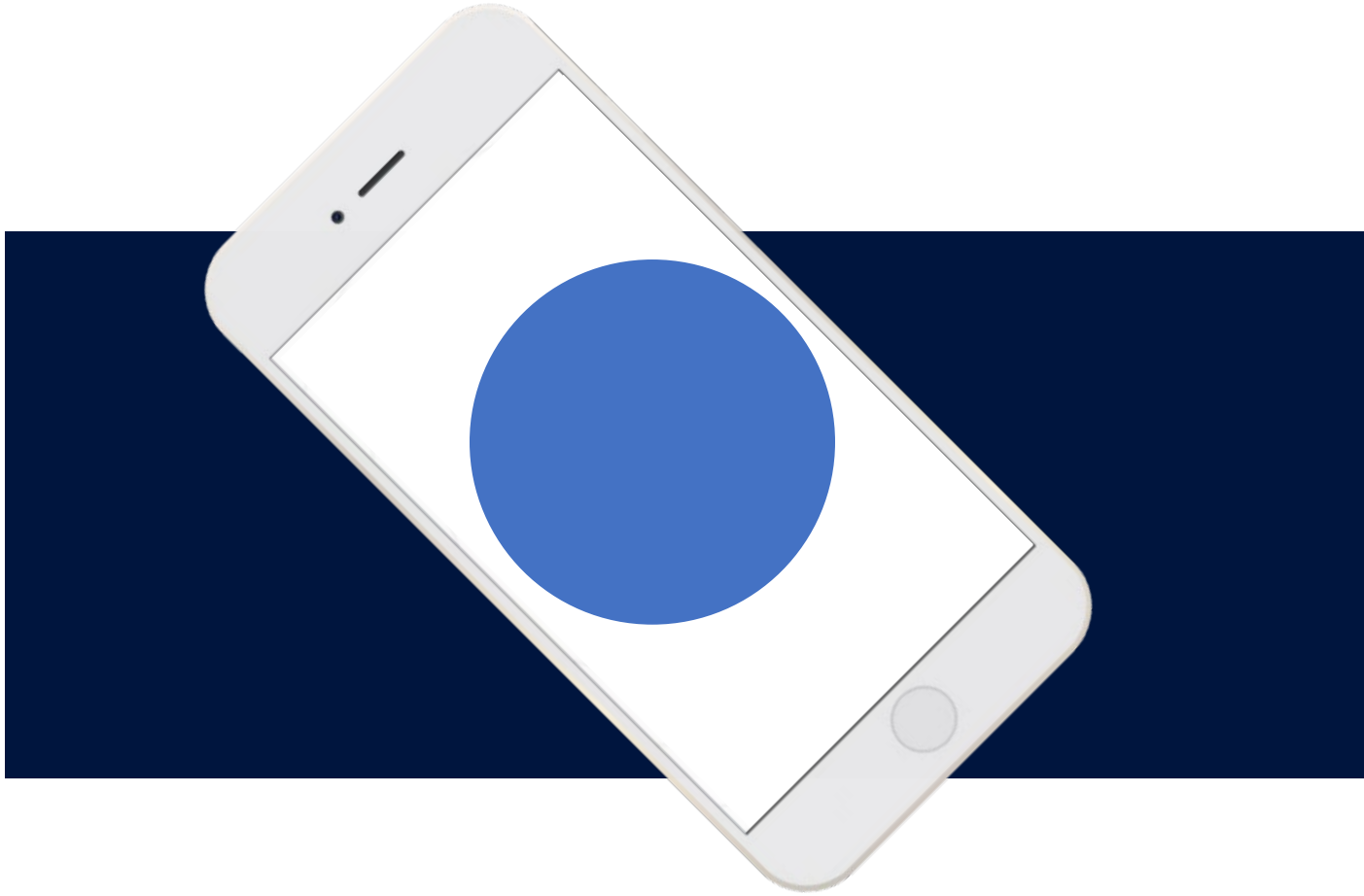



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR
NCMA
WISCONSIN
FEBRUARY 1 - ACQUISITION HOUR: PREPARING A WINNING GOVERNMENT PROPOSAL
UPCOMING EVENTS
JAN 11 1:00 pm - 2:00 pm Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)
JAN 19 11:00 am - 12:00 pm Sales Opportunities Local Government Agencies – In Person (Madison, WI)
JAN 19 3:00 pm - 4:30 pm Meet and Greet with Construction Managers / General Contractors for upcoming Racine Unified School District (RUSD) Projects
JAN 24 All day Wisconsin Federal Contractor Forum (by invitation)
JAN 25 7:30 am - 6:00 pm 15th Annual End of Year Federal Contractor Update – (Oshkosh, WI) In-Person

A Culture of Security

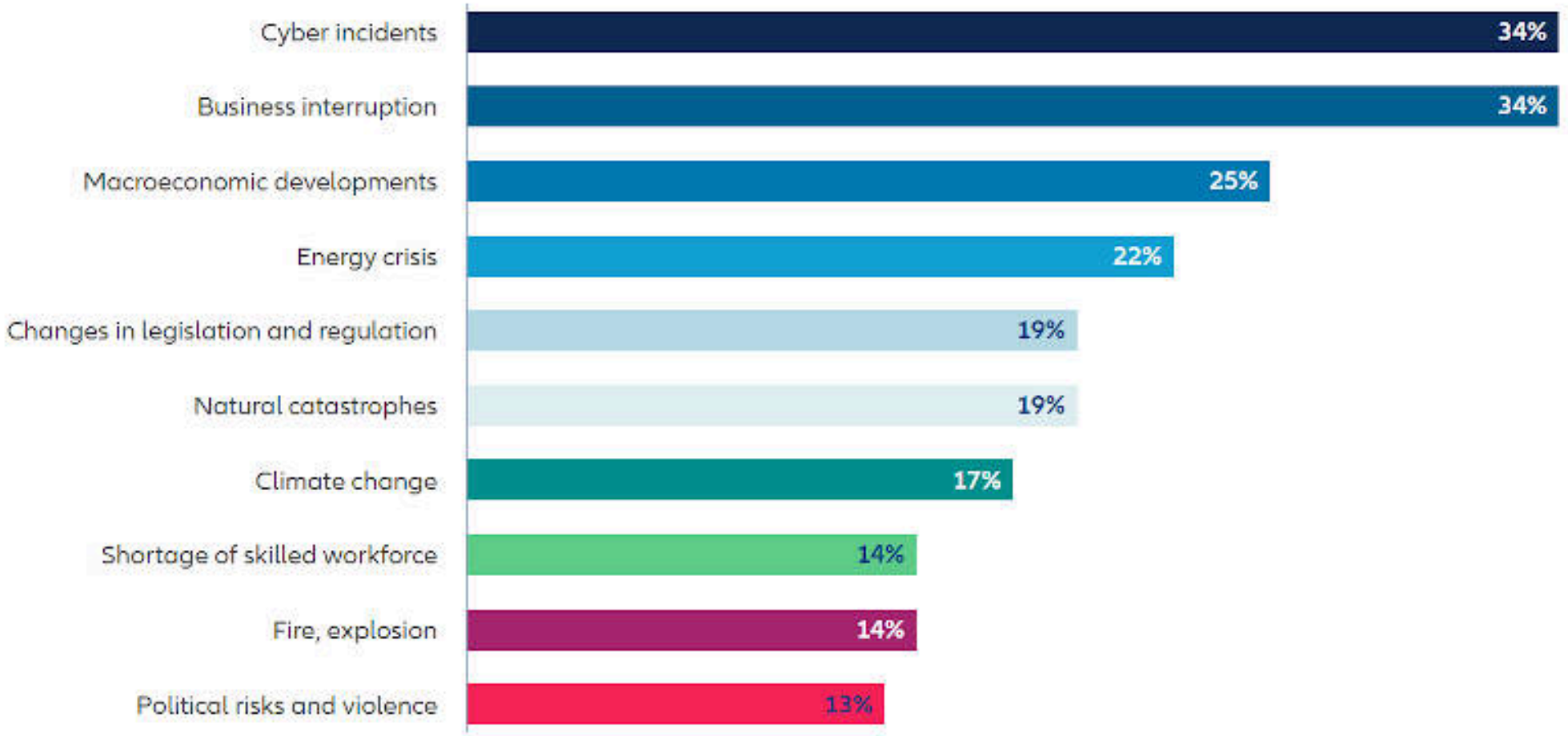
Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – April 28th, 2023

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.

IN 2020

<60% of data breaches were financially motivated.

Government Technology

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

Too small to see?

SMALL BUSINESSES ARE VULNERABLE TOO

72% OF CYBER ATTACKS AFFECT COMPANIES WITH **LESS THAN** **100** **EMPLOYEES**

SMALL≠ SAFE

OF SMALL BUSINESSES THINK THEY ARE TOO SMALL TO BE HACKED

THE COST IS HEAVY

$188,242

THE AVERAGE AMOUNT IT TAKES A SMALL BUSINESS TO RECOVER FROM A CYBER ATTACK

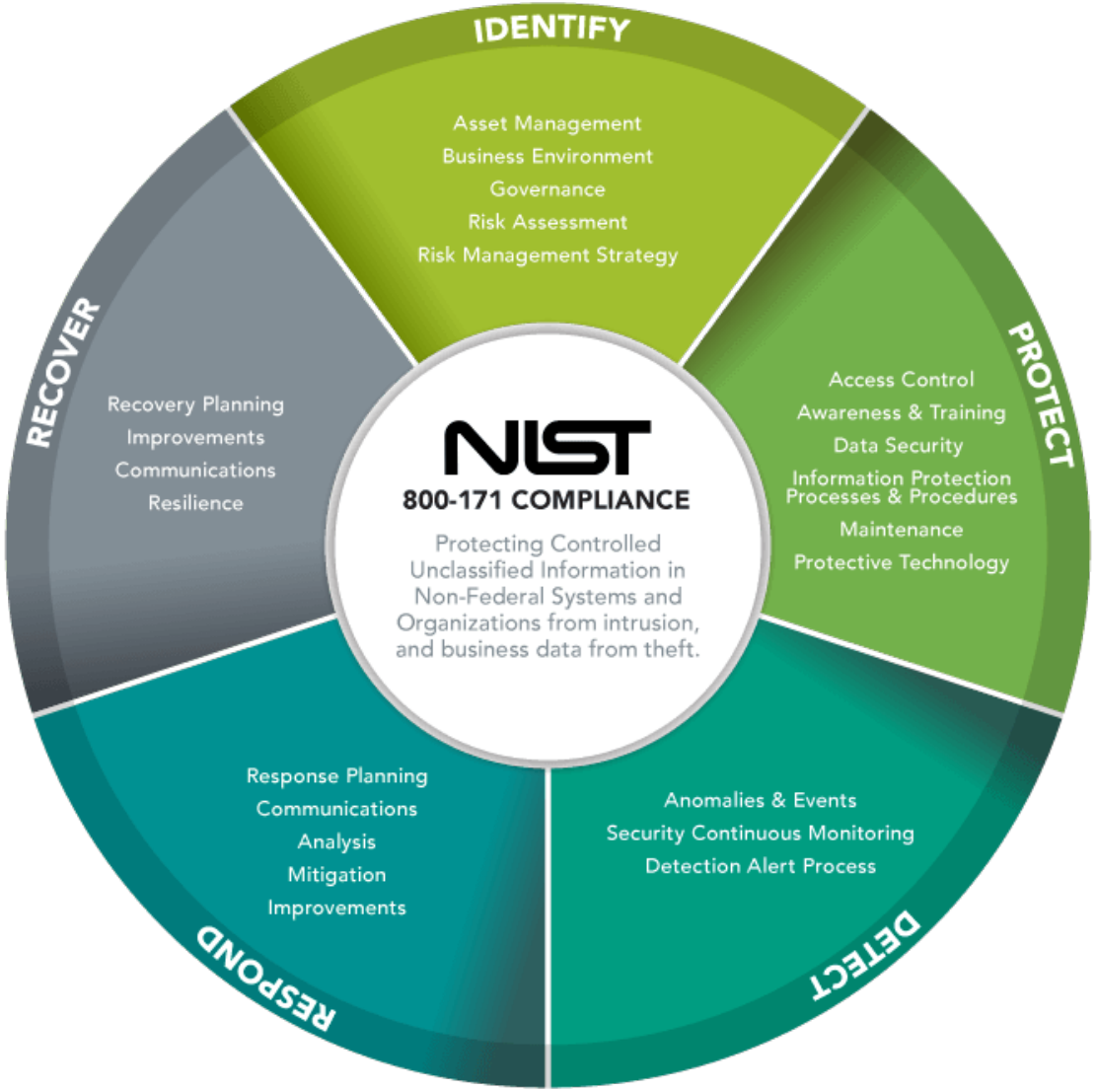
DFARS 252.204-7012

National Institute of Standards and Technology

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

3.2.2
Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract… the Contractor shall rapidly report cyber incidents to DoD.



1 NIST

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

2 CISA

Department of Homeland Security's Cybersecurity & Infrastructure Security Agency

3 NIST SP 800-171 R2

NIST Special Publication 800-171 R2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Owning Your Security

1 THREAT ENVIRONMENT

2 CASE STUDIES

3 PRACTICES

Types of Bad Actors

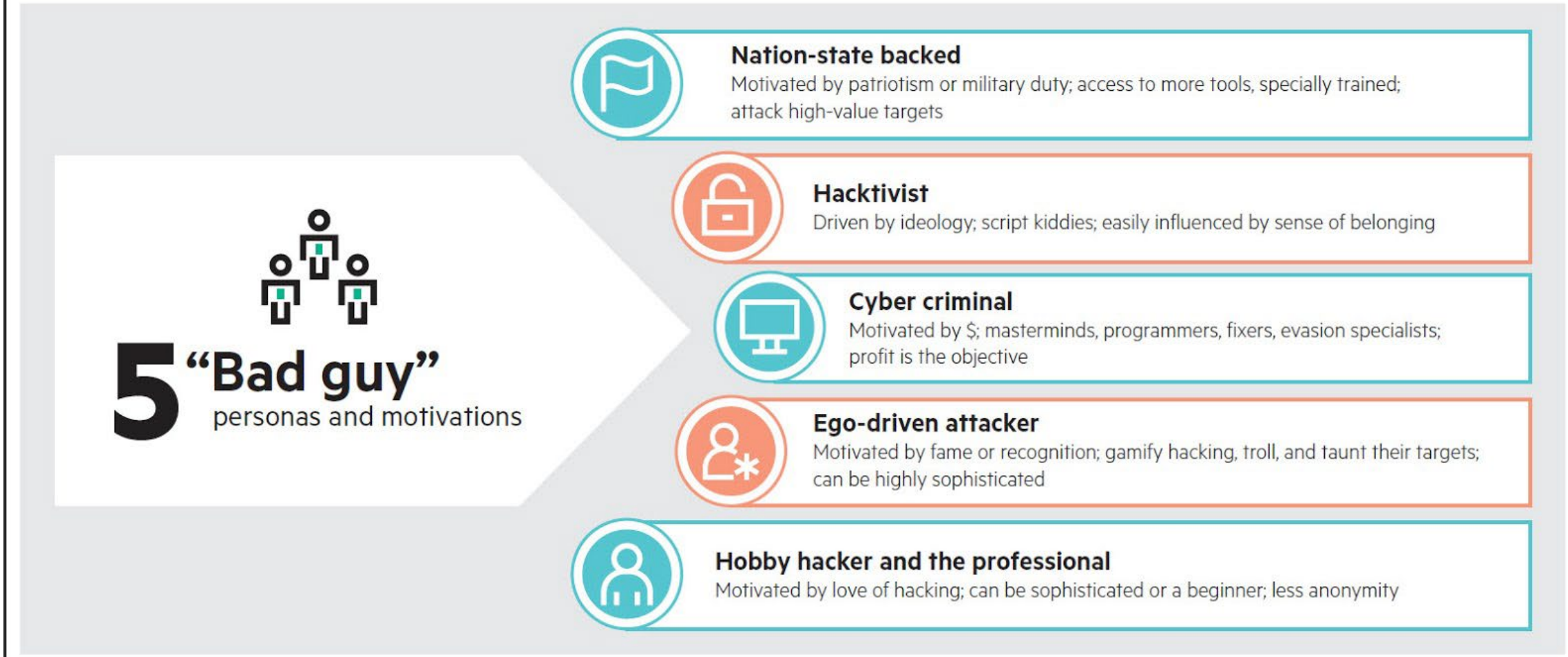


Figure 2: Attacker personas and motivations

The Incident Response Plan

NIST SP 800-61

1 — THREAT ENVIRONMENT

2 — CASE STUDIES

3 — PRACTICES

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)

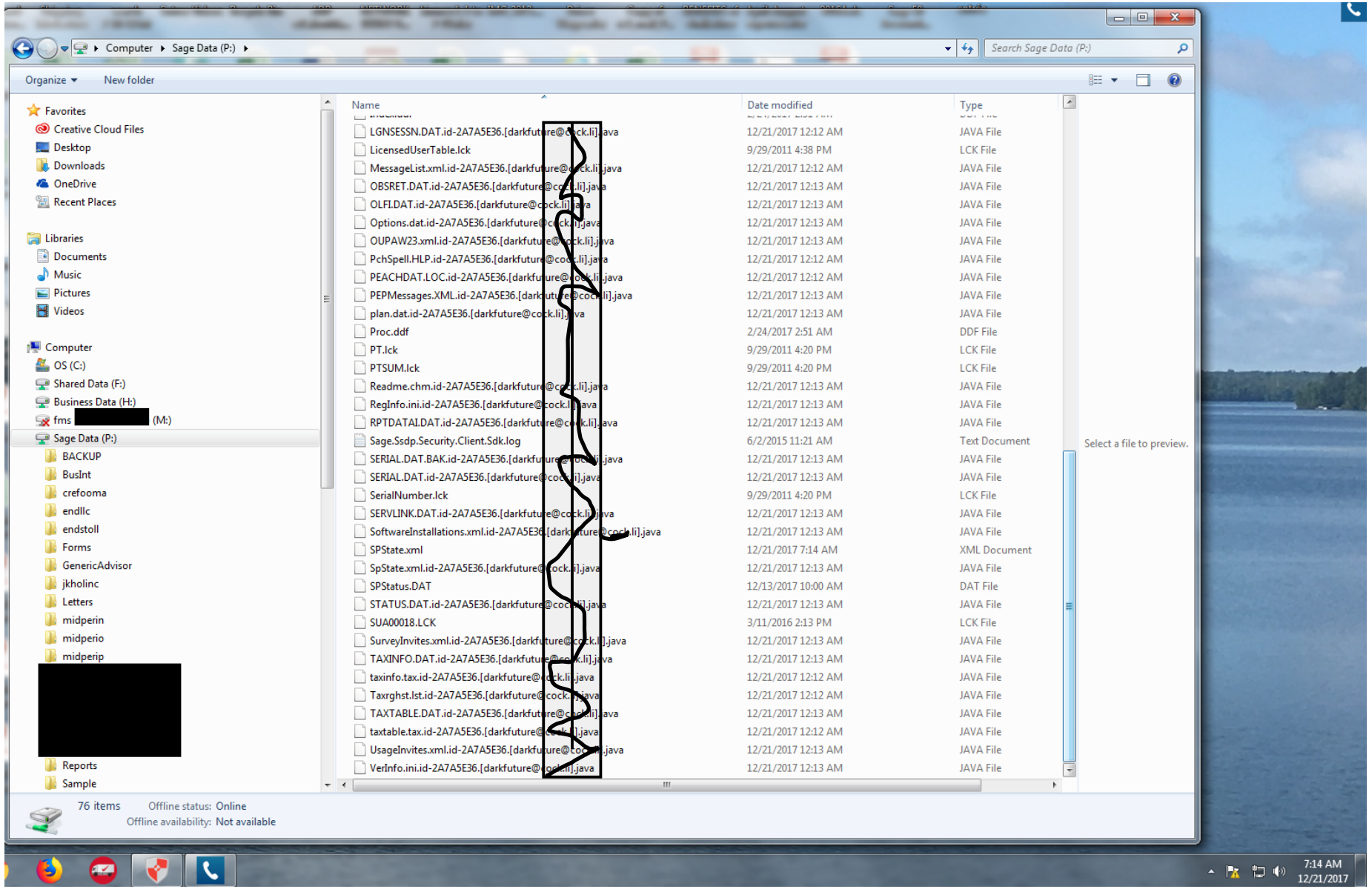
Ransomware Activation Friday 7:00pm CST

Notification Monday, 6:45AM CST

Full Functionality Restored 9 Days Later

1 RANSOMEWARE

NIST 800-171 3.3 Components



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

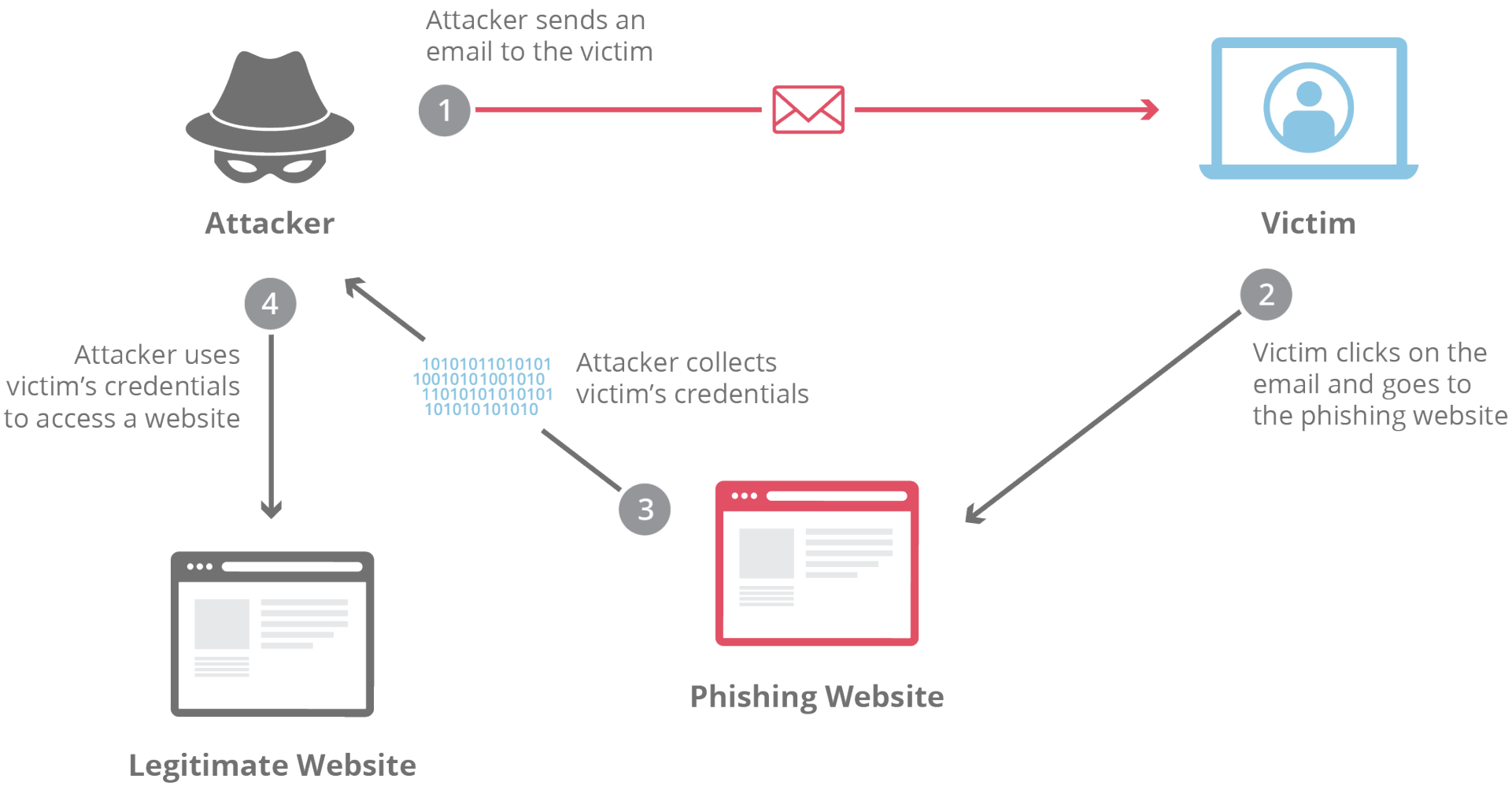
Payroll Company Issues Check in Excess of $16,000

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)

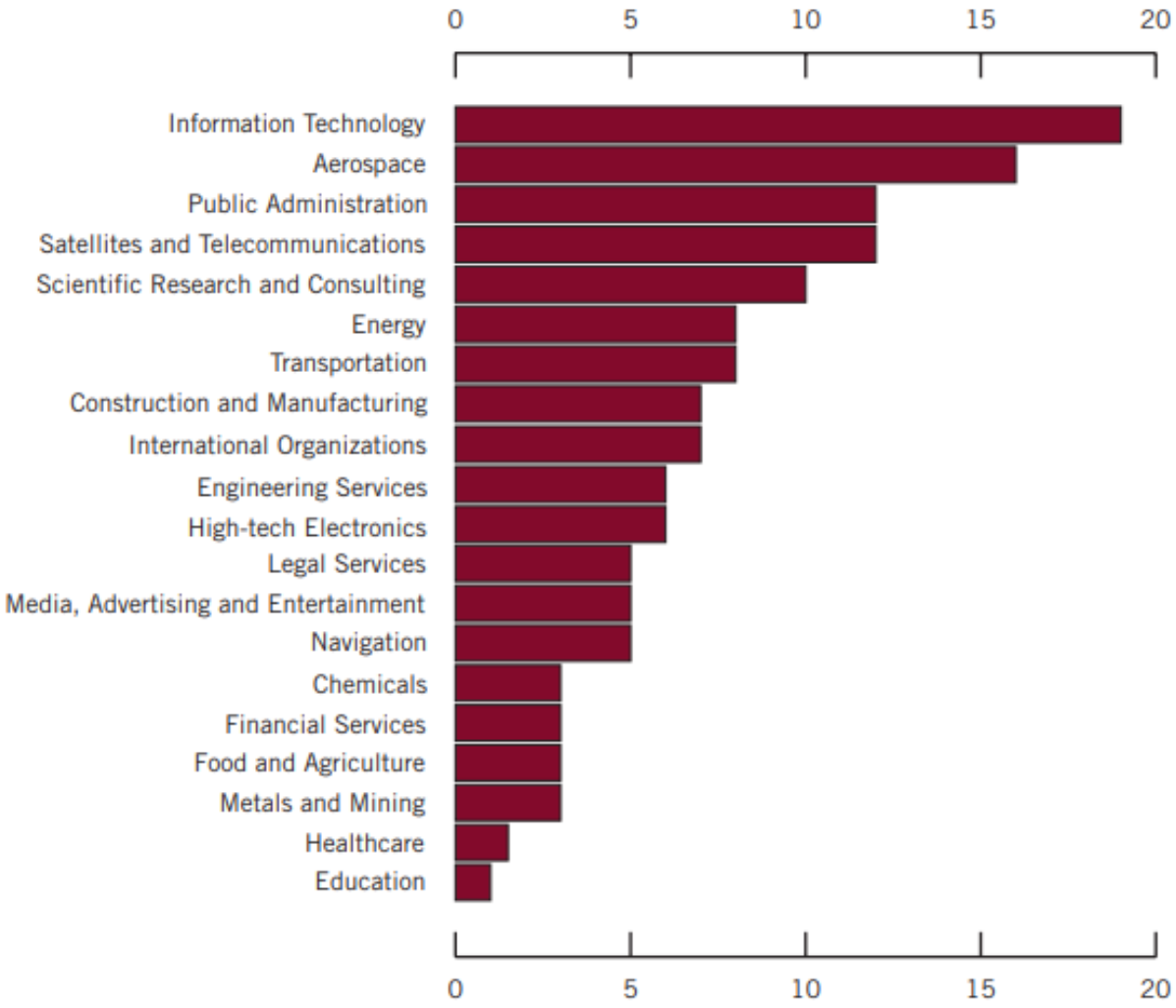
Scouting and Recon

CISO Notified While Playing Golf on the weekend

Size of Breach Discovered

Disclosure to Buyers and General Public

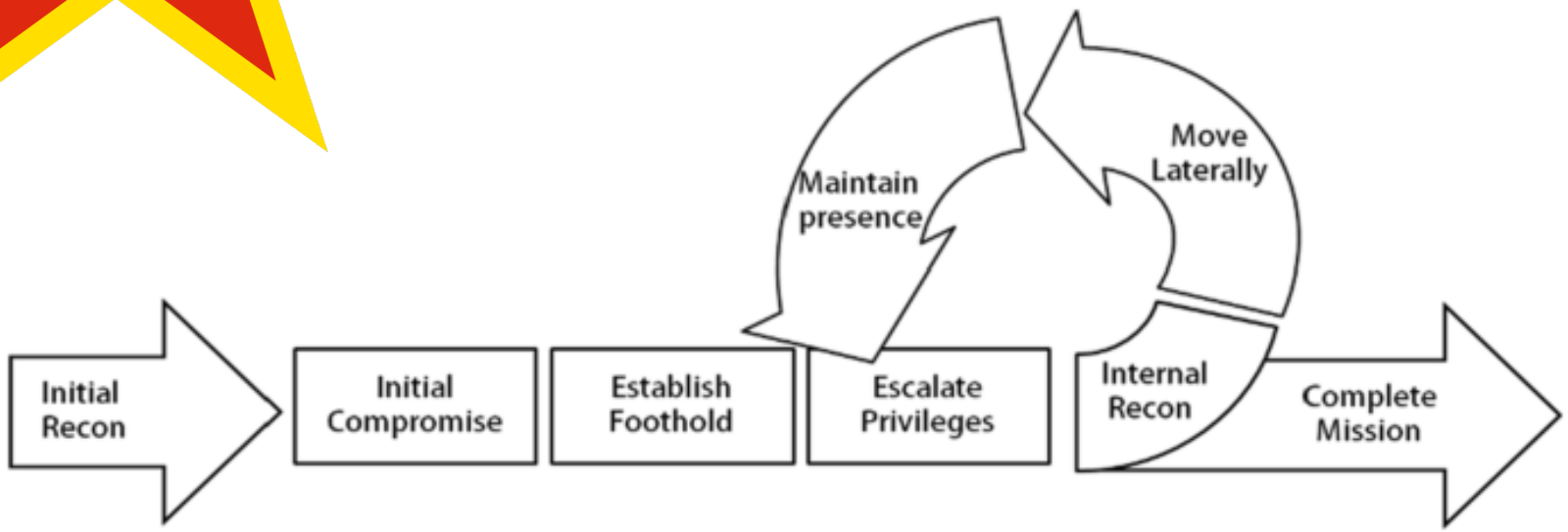
A World at War



Industries Compromised by APT1

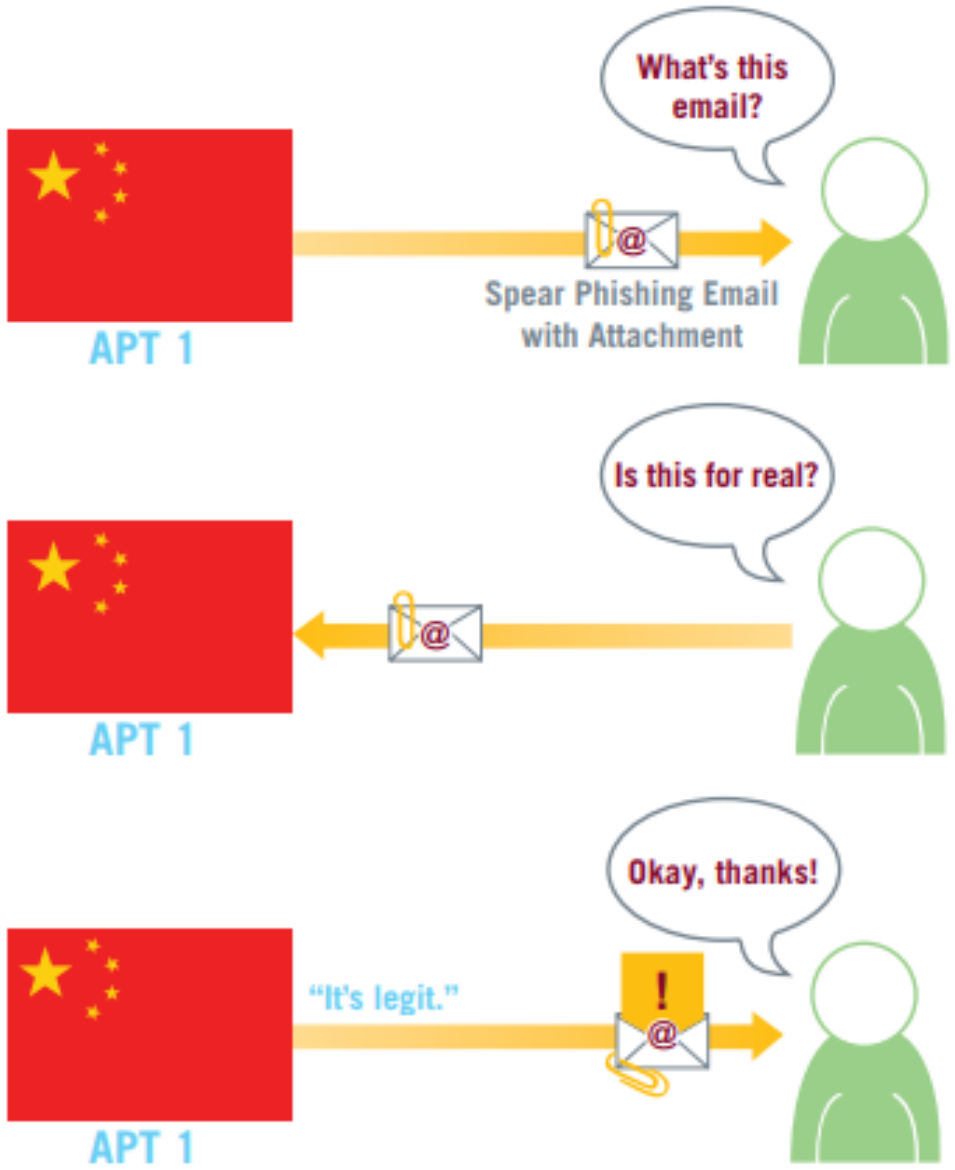
On Multiple Fronts

PLA Unit 61398



Pudong, Shanghai

Big Things Start Small



1

THREAT ENVIRONMENT

2

CASE STUDIES

3

PRACTICES

THINGS TO DO

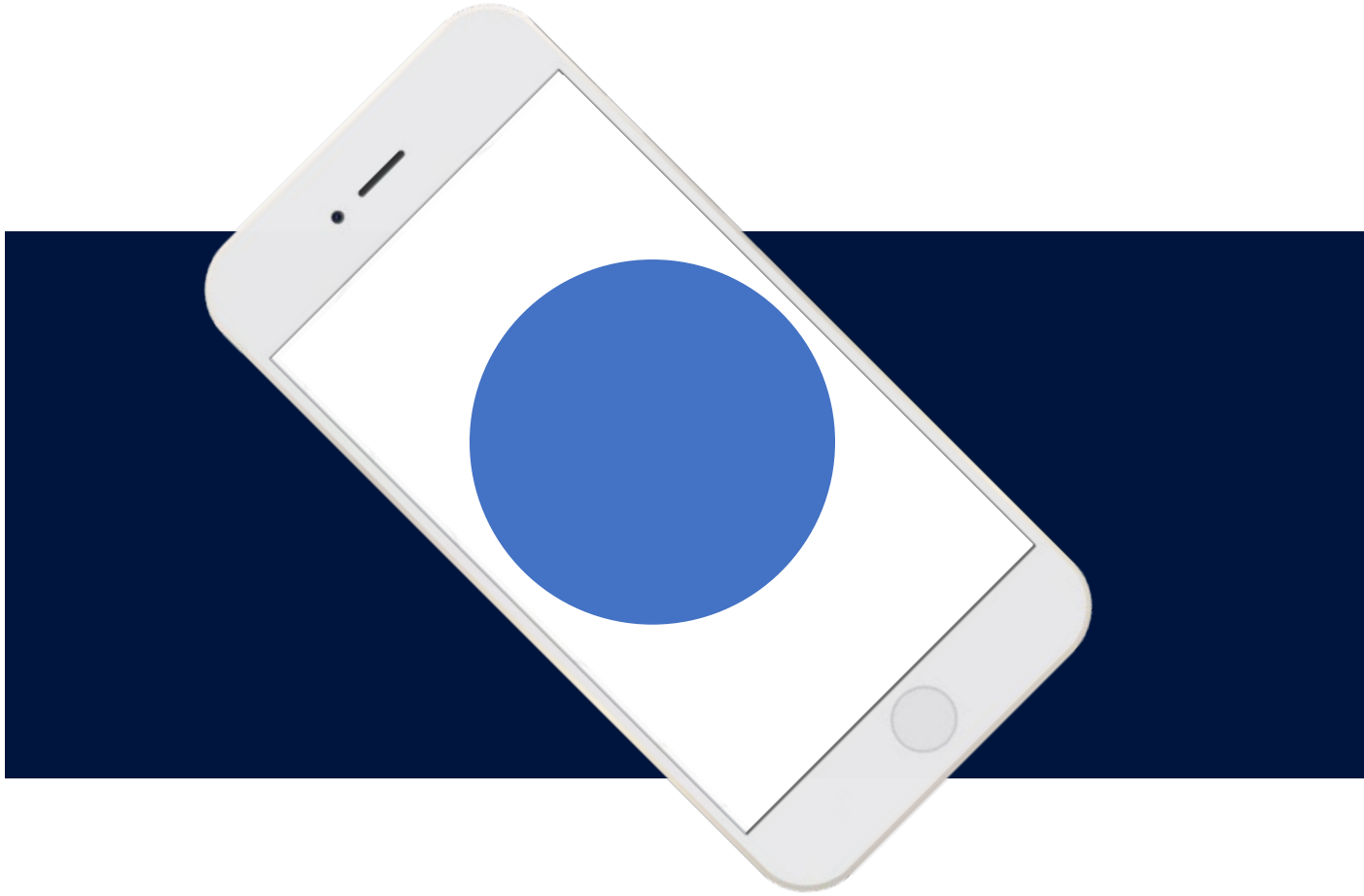
- ✓ TRAIN – If you see something, say something!
- ✓ Take IT Concerns Seriously
- ✓ Create a Supportive Environment
- ✓ Do Not Tolerate Complacency
- ✓ Prepare for the Inevitable

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

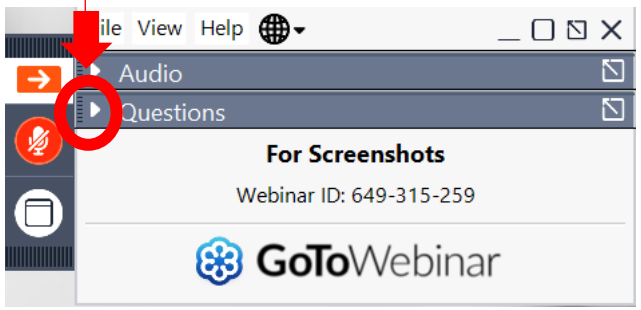
AN APEX ACCELERATOR



QUESTIONS?

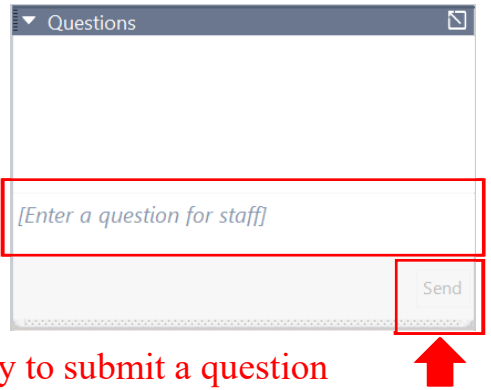
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

- ~~March 24~~
  ~~Protecting the Data~~

- ~~April 14~~
  ~~The Forensic Record~~

- April 28
  Culture of Security

PRESENTED BY

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
Cyber Friday

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association WISCONSIN

APEX ACCELERATORS

The Contracting Academy

Developing and Growing Government Contractors

Presents:

9th Annual DOD Contract Management Update

–VIRTUAL–

May 2-3, 2023

Visit WIContractingAcademy.org

WPI Wisconsin Procurement Institute
A DOD APEX ACCELERATOR

NDIA Great Lakes

NCMA National Contract Management Association WISCONSIN

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

April 28, 2023

SURVEY

Wisconsin Procurement Institute
AN APEX ACCELERATOR

April 28, 2023

APEX ACCELERATORS

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Jack Laufenberg
jackl@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Matthew Frost
Wisconsin Procurement Institute
mattf@wispro.org | 608.293.0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226