



CSMFO Annual Conference

IT SECURITY ASSESSMENTS

What They Entail

Liana Bailey-Crimmins, CalPERS
Ric Jazaie, Macias Gini & O'Connell LLP

February 8, 2017

Speakers



Liana Bailey-Crimmins
Interim Deputy Executive Officer,
Benefit Programs Policy & Planning
and Chief Information Officer
CalPERS



Ric Jazaie
Director
Macias Gini & O'Connell LLP

Cybersecurity is the body
of technologies, processes,
and practices



AGENDA

- 🔒 Threat Landscape
- 🔒 Risk Intelligence
- 🔒 Best Practices
- 🔒 Assessments
- 🔒 Case Study

THREAT LANDSCAPE

cyber attack

JP Morgan learned the **hard** way





“The ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history.”

- General Keith Alexander
Former Director, National Security Agency

Los Angeles Times
L.A. County targeted in
phishing cyberattack; private
information of 750,000
people **compromised**.

-December 17, 2016

CNN.com
Election 2016: **Hackers**
Breach Election System

-CNN.com, August 30, 2016

Sutter County
Courthouse **data**
breach exposes
personal information

-Appeal Democrat, June 13, 2016

USA TODAY
Ransomware attack hit
San Francisco train system

-USA Today, November 28, 2016

USA TODAY
IRS Hack **Far Larger**
Than First Thought

-USA Today, August 17, 2015

The New York Times
Hackers' **\$81 Million Sneak**
Attack on World Banking

-The New York Times, April 30, 2016

The Boston Globe
Hackers extract \$300 ransom from
Town of Medfield after "locking"
town network

-Boston Globe, February 2, 2016



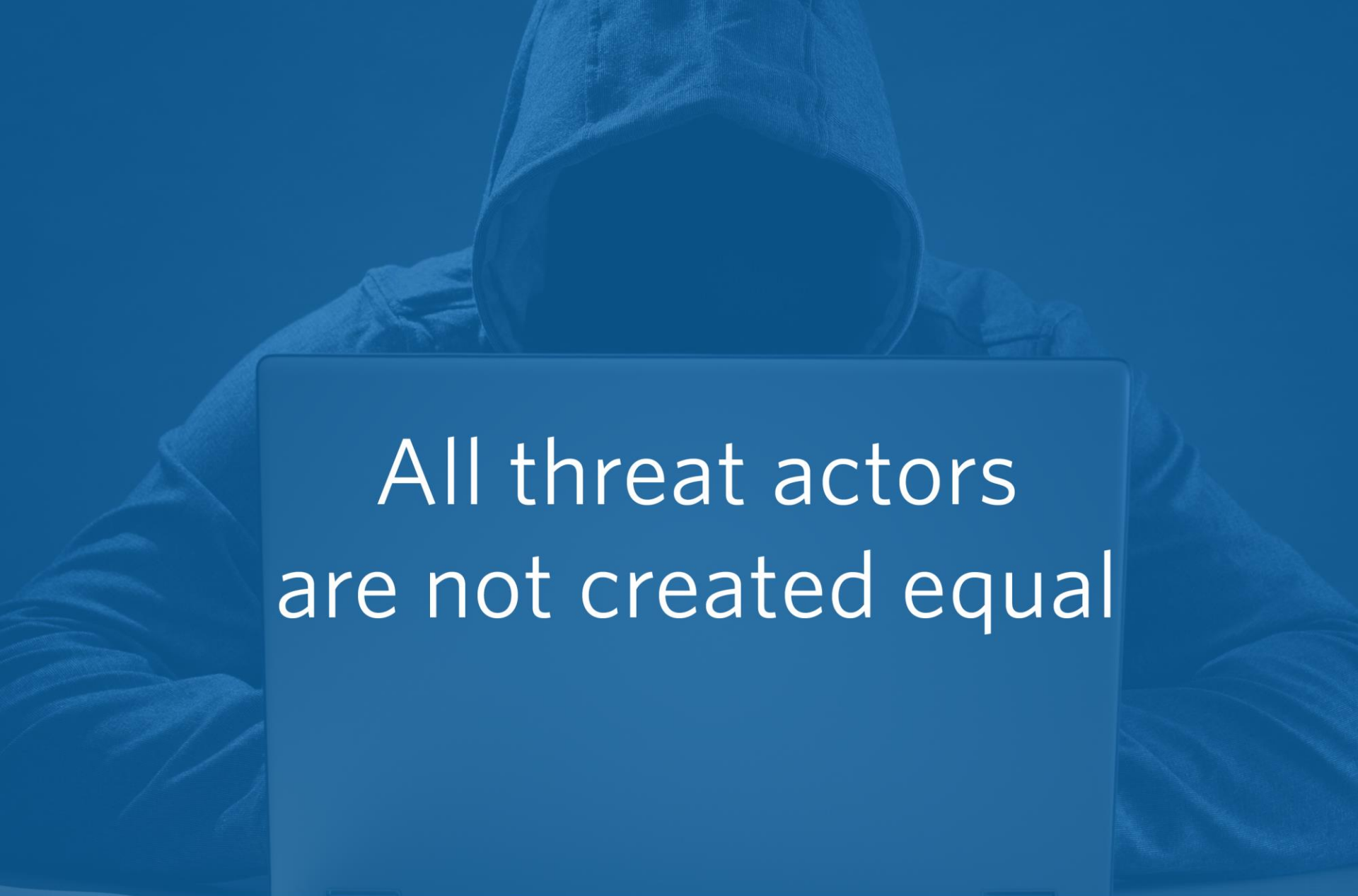
TRENDS

Impersonation & Identity Theft





Ransomware



All threat actors
are not created equal

Who are the **threat actors**?

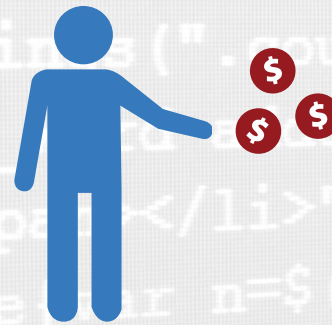
	 State Sponsored	 Cyber Crime	 Network Attack	 Insiders (Intentional & Unintentional)	 Hacktivism	 Nuisance
Objective	Economic, Political Advantage	Financial Gain	Escalation, Destruction	Revenge, Monetary Gain	Defamation, Press & Policy	Access & Propagation
Example	Intellectual Property Theft, PH/PHI	Credit Card Theft PH/PHI	Destroy Critical Infrastructure, DDOS	Destruction, Theft	Website Defacements	Botnets & Spam

Source Mandiant

Demystifying the Myths



All assets are not created equal



Can't throw money at it to make it go away



Compliance does not mean you are secure



The bad guy doesn't think about the budget cycle

Illusion of control







What's at stake? **Business Disruptions**

Possible **system outages**
resulting in the inability to
do business

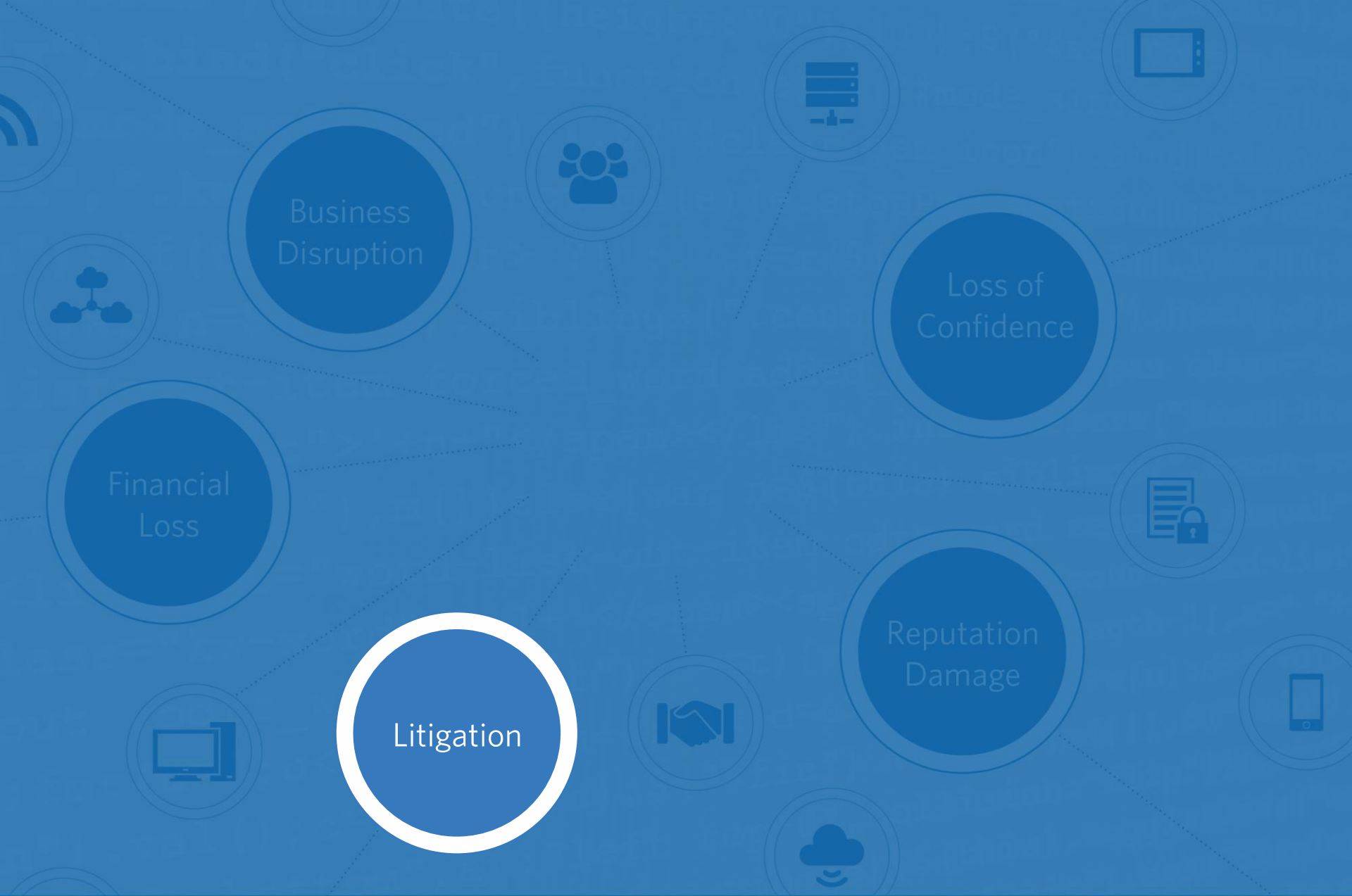
Financial
Loss

Business
Disruption

Loss of
Confidence

Reputation
Damage

Litigation



U.S. "cyber" law... a patchwork



Laws imposing civil
or criminal liability
for **hacking**



Laws requiring
implementation of
security measures



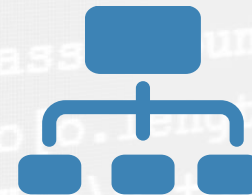
Laws requiring
notification of
security breaches



Contractual duties
re: security and/or
breach notification



Regulator enforcement
consent decrees and
related requirements



Regulator and industry
standards, guidelines,
and frameworks

BEST PRACTICES



Cybersecurity Framework

National Institute of Standards & Technology (NIST)

Identify cybersecurity risks and vulnerabilities

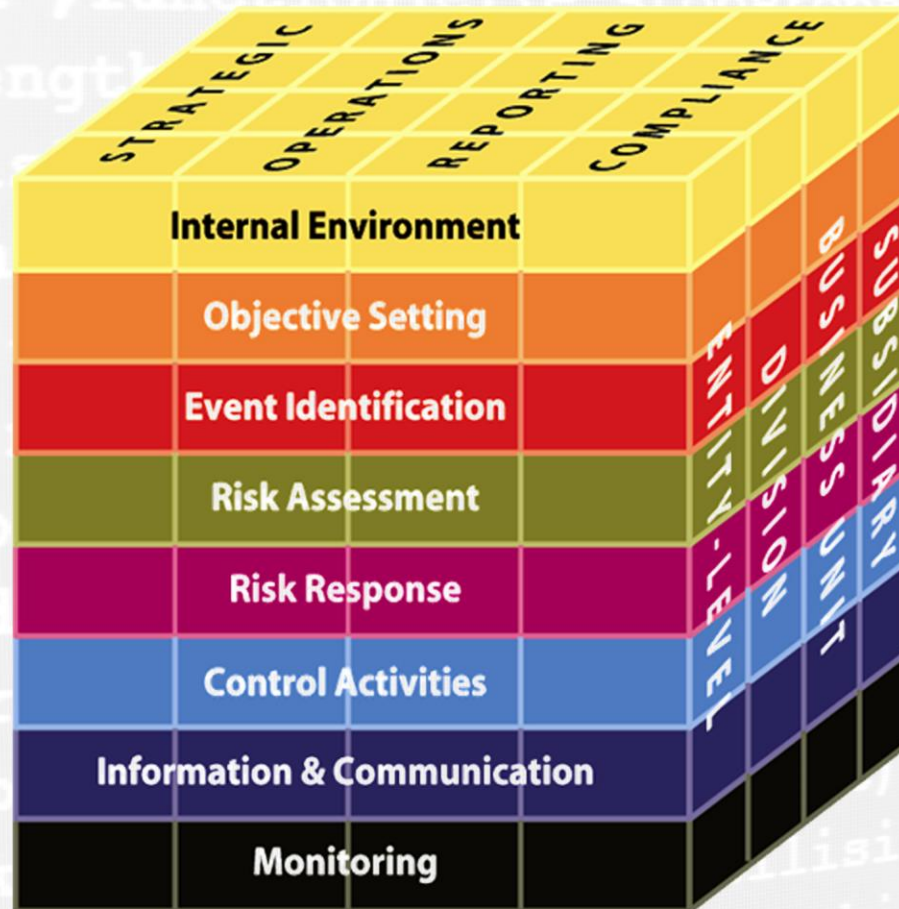
Protect critical assets

Detect the occurrence of a cyber event

Respond to detected event

Recover from a cyber event

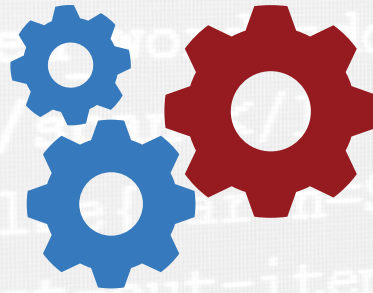
The COSO Framework



Principles of COSO



Select



Develop



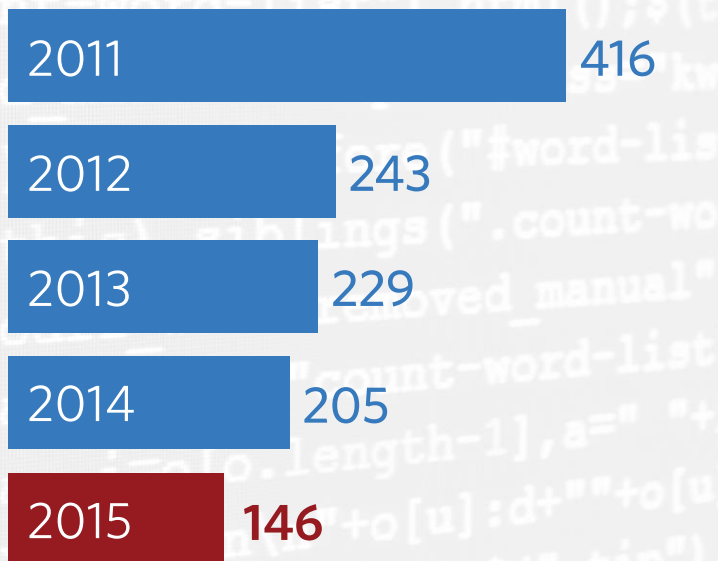
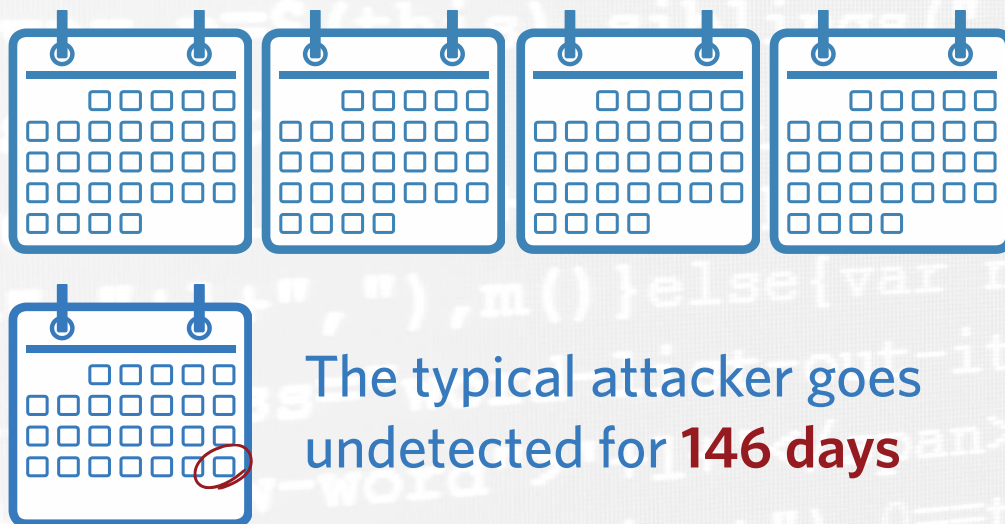
Deploy

A close-up photograph of two people in business attire. One person, wearing a light blue shirt and a dark tie, is holding a silver tablet. Another person, whose arm shows a gold bangle, is pointing at the tablet with a blue pen. The background is slightly blurred, showing a desk with papers and a yellow sticky note.

ASSESSMENTS

Compromise Assessments

Undetected attacks



Attacks are **hard** to detect

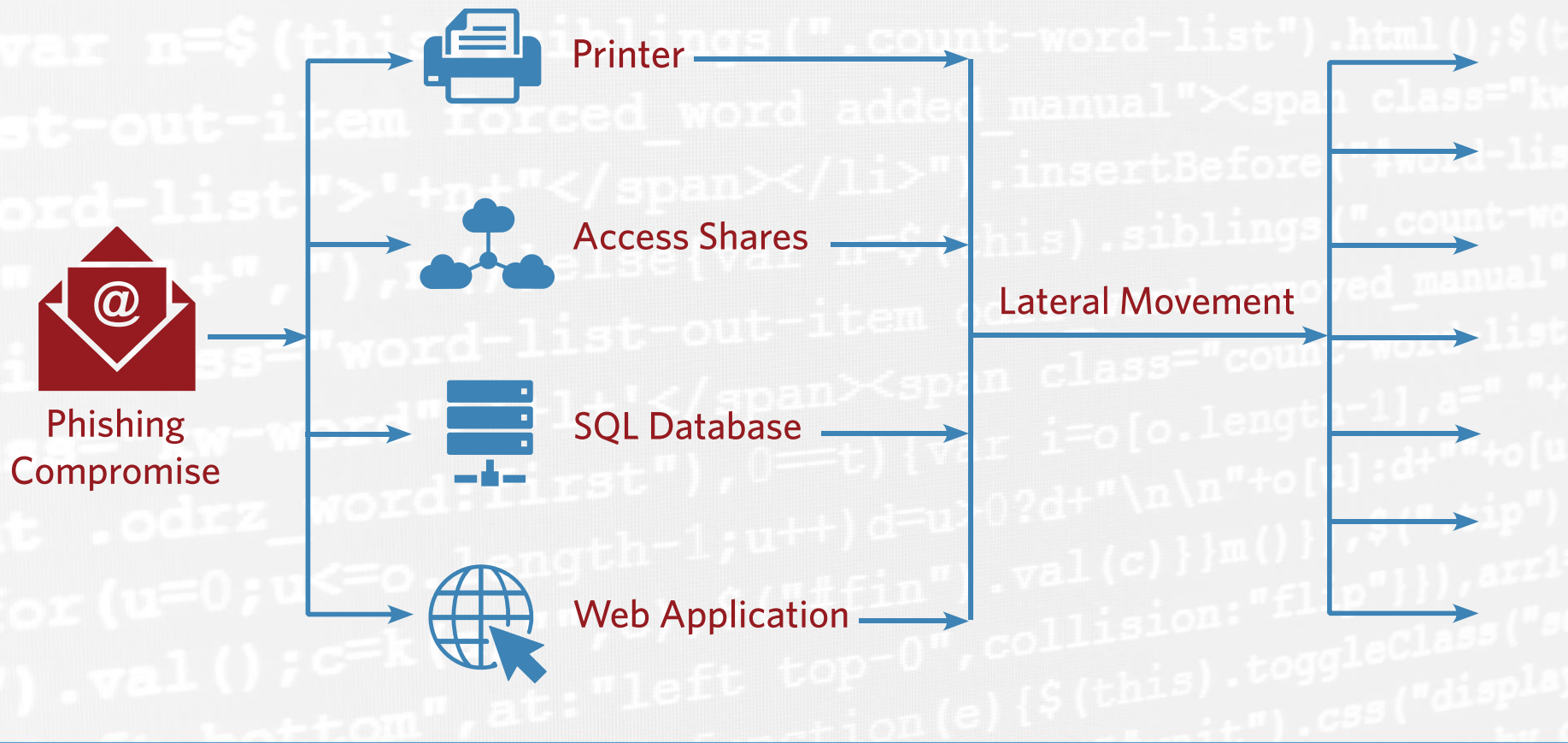


Only **3 in 10** organizations detected the breach on their own, the other seven were notified by external entities



Penetration Test

How are you **targeted**?





Applying the NIST Cybersecurity Framework

Identify cybersecurity risks and vulnerabilities

Protect critical assets

Detect the occurrence of a cyber event

Respond to detected event

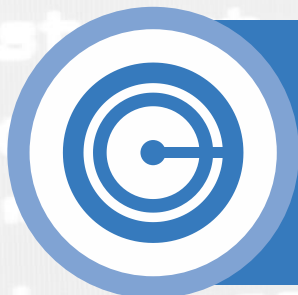
Recover from a cyber event

Review for continual improvement



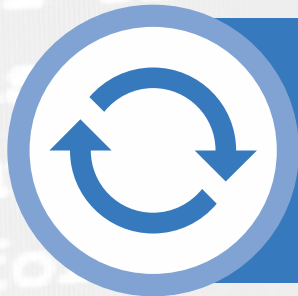
PROTECT

- Security Roadmap Program
- Background Checks
- Cybersecurity Tabletop Exercises



DETECT

- Cyber Warriors
- Security Operations Center
- Security Information Event Management



RESPOND

- Security Incident Response Plan
- Information Sharing/Partnerships
- Trained Crisis Manager

CYBER WARRIOR CULTURE

Education, Training, and Outreach

Board of Administration

Executive

Members

Stakeholders

Staff

Takeaways

1

It's not a matter of if, but when



2

You can't throw money at it to make it go away



3

Compliance does not mean you are secure



4

Operationalize strategy based on risk appetite



5

Holistic approach: people, process, technology



Education
Training
Outreach

Cyber
Warriors

Risk
Intelligence



Best
Practices

Threat is
Evolving

Operationalizing
Strategy

Vigilance

Threat
Landscape

Protection

THANK YOU