36th Annual Workforce Management Briefing

Managing Workforce Compliance in an Unpredictable World

Combating Internal Cyber Threats: An Insider Threat Prevention Program Is an Employer's Best Defense

EPSTEIN
BECKER
GREEN

Panelists

Brian G. Cesaratto

Member

Epstein Becker Green

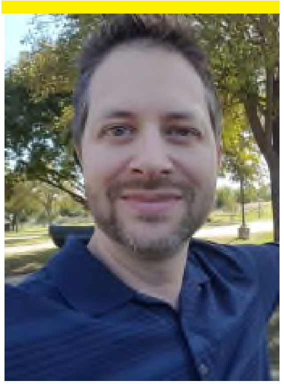
New York

Robert J. Hudock

Member

Epstein Becker Green

Washington, DC



Jason Penney

Vice President IT Risk

Press Ganey

Stewart Scott III

Chief Legal Officer and Managing Director

Daiwa Capital Markets America Inc.

EPSTEIN
BECKER
GREEN

Cyber Security Is Everyone’s Responsibility

Risks to Your Information: Malicious and Unintentional Employees and Other Insiders

A **malicious insider** is a current or former employee, third-party contractor, or other business partner who has or had authorized access to an organization's network, system, or data and **intentionally** exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems. **This includes disgruntled employees.**

EPSTEIN
BECKER
GREEN

Risks to Your Information: Malicious and Unintentional Employees and Other Insiders

An **unintentional insider** is a current or former employee, third-party contractor, or other business partner who has or had authorized access to an organization's network, system, or data and who, through his or her **action/inaction without malicious intent,** causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. **This includes employees who unknowingly or negligently cause a data breach or enable a cyber attack (e.g., social engineering, phishing, or spear phishing).**

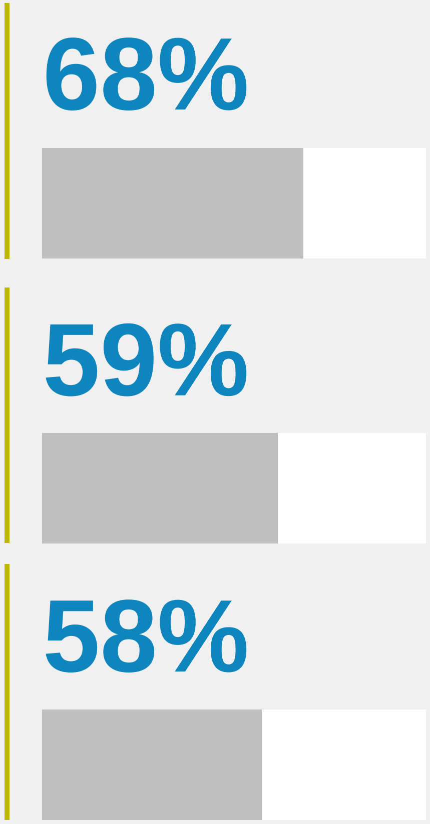
Most Data Breaches Are Caused by Insiders—Whether Intentionally or Inadvertently*

Insiders caused

Network Attacks Targeting Healthcare Data
(IBM Security, "Security trends in the healthcare industry: Data theft and ransomware plague healthcare organizations")

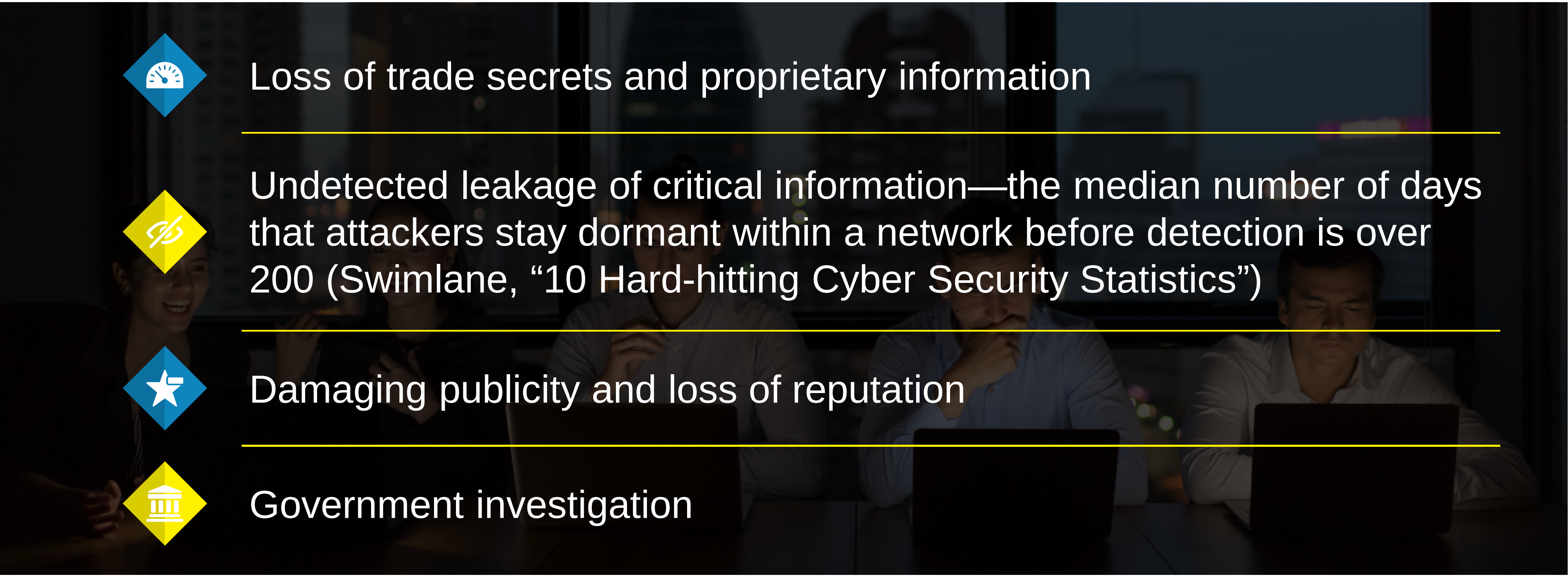
Patient Health Record Privacy Violations
(Protenus, "31 Health Data Breaches Disclosed in January as HHS Fines for Late Reporting")

Attacks in Financial Services
(IBM Security, IBM X-Force Threat Intelligence Index 2017)



*Ponemon Institute Research Report, 2016 Cost of Insider Threats: Benchmark Study of Organizations in the United States.

What Keeps Us Awake at Night?



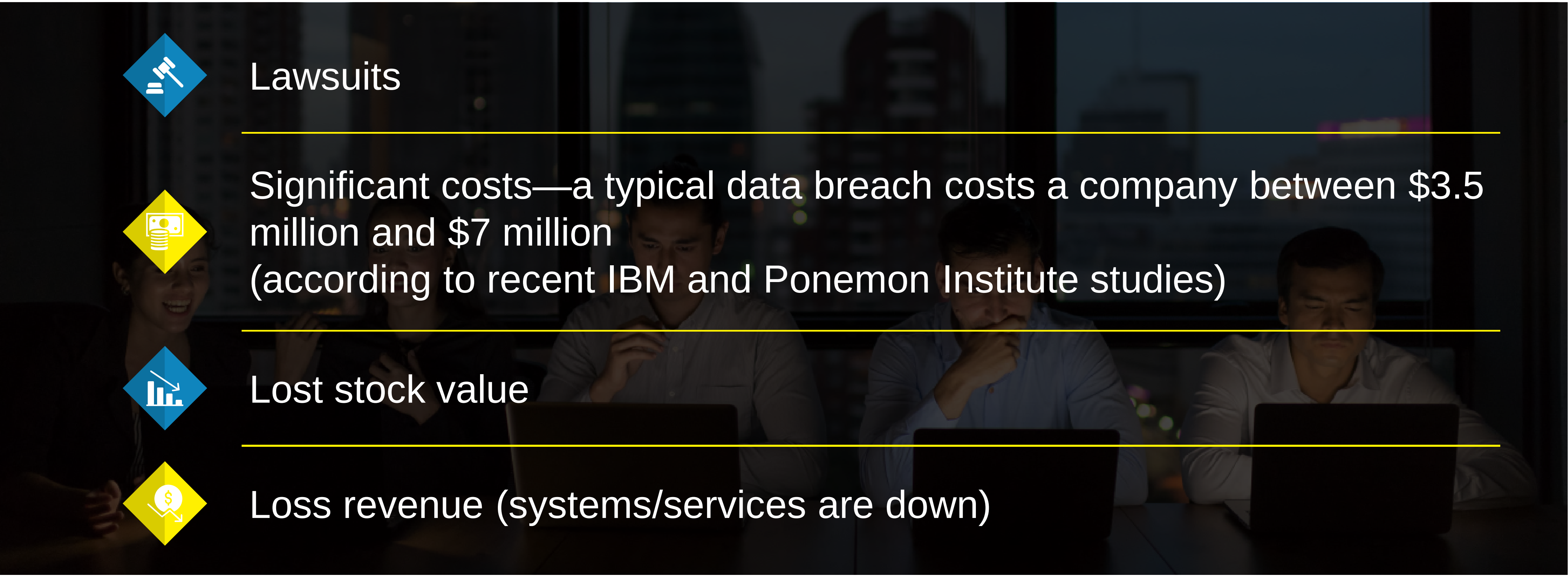
- Loss of trade secrets and proprietary information

- Undetected leakage of critical information—the median number of days that attackers stay dormant within a network before detection is over 200 (Swimlane, “10 Hard-hitting Cyber Security Statistics”)

- Damaging publicity and loss of reputation

- Government investigation

What Keeps Us Awake at Night?



- Lawsuits
- Significant costs—a typical data breach costs a company between $3.5 million and $7 million
  (according to recent IBM and Ponemon Institute studies)
- Lost stock value
- Loss revenue (systems/services are down)

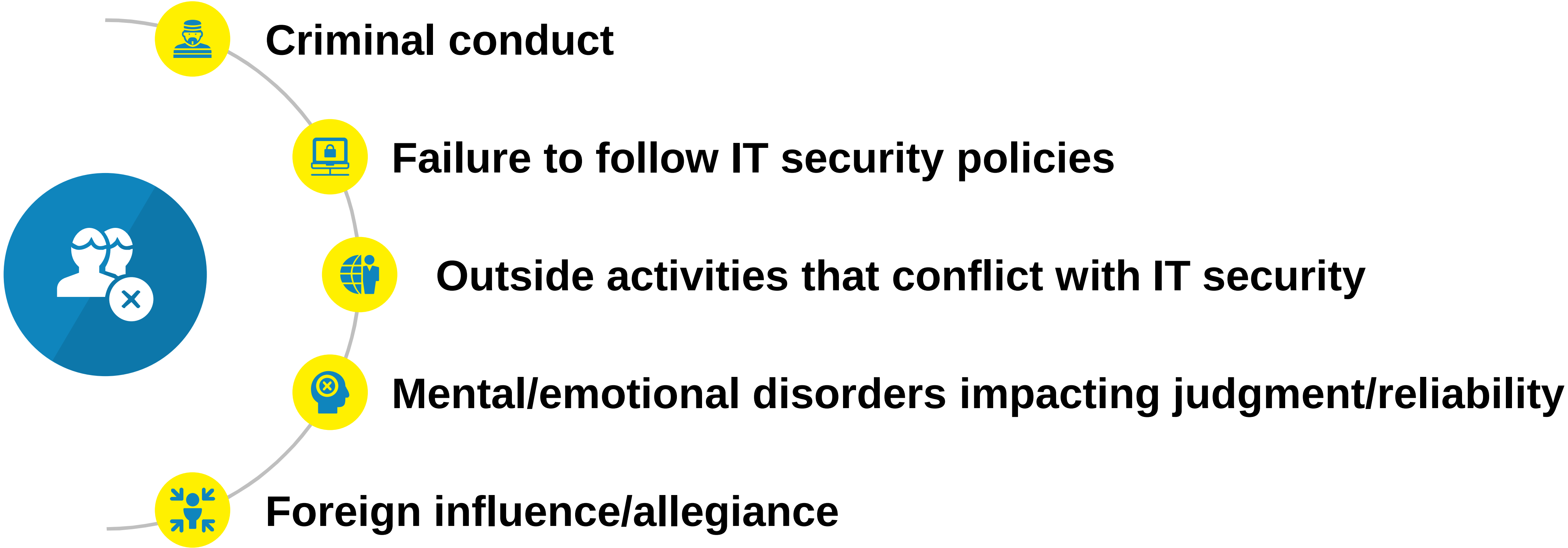
EPSTEIN
BECKER
GREEN

Concerns That Increase Vulnerability to Insider Breach

- **Poor judgment**
- **Dishonesty and unreliability**
- **Financial issues and debt**
- **Misuse of IT systems**
- **Alcohol/drug abuse**

A full version of 32 CFR Part 147 is included in the Supplemental Workshop Materials and available to download.

Concerns That Increase Vulnerability to Insider Breach



Criminal conduct

Failure to follow IT security policies

Outside activities that conflict with IT security

Mental/emotional disorders impacting judgment/reliability

Foreign influence/allegiance

A full version of 32 CFR Part 147 is included in the Supplemental Workshop Materials and available to download.

Best Practices: Coordinated Strategy of Personnel & IT Controls to Address Employee and Insider Risks

Know and protect your critical assets

Develop a formalized and documented insider threat program

Clearly document and consistently enforce personnel and information security policies and controls

Anticipate and manage negative issues in the work environment

Carnegie Mellon University, Software Engineering Institute, the CERT Division, "Insider Threat Best Practices" (a full version is included in the *Supplemental Workshop Materials* and available to download).

EPSTEIN
BECKER
GREEN

Best Practices: Coordinated Strategy of Personnel & IT Controls to Address Employee and Insider Risks

Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior

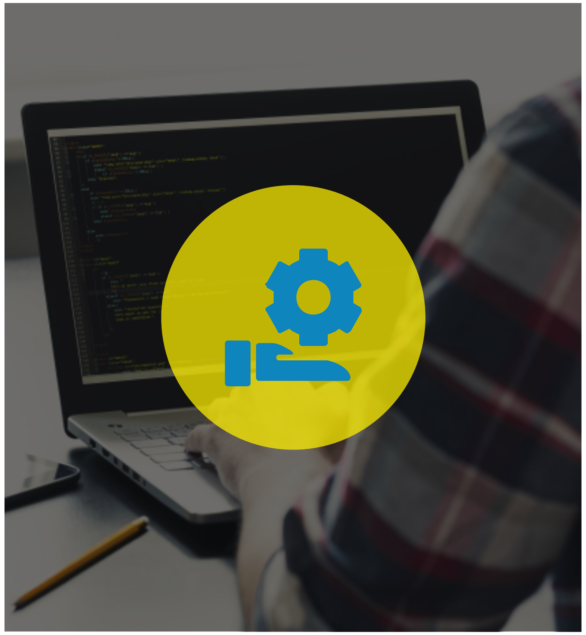
Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees

Develop a comprehensive employee termination procedure

Carnegie Mellon University, Software Engineering Institute, the CERT Division, “Insider Threat Best Practices” (a full version is included in the *Supplemental Workshop Materials* and available to download).

EPSTEIN
BECKER
GREEN

Best Practices: Personnel and IT Controls to Address Employee and Insider Risks



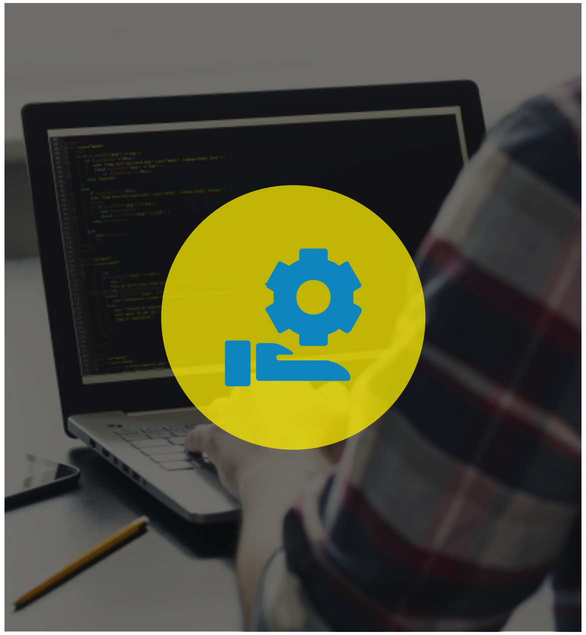
Establish a baseline or normal behavior for both networks and employees

Deploy solutions for monitoring employee actions and correlating information from multiple data sources (e.g., data loss prevention (DLP))

Institute stringent access controls and monitoring policies on privileged users

Carnegie Mellon University, Software Engineering Institute, the CERT Division, “Insider Threat Best Practices” (a full version is included in the *Supplemental Workshop Materials* and available to download).

Best Practices: Personnel and IT Controls to Address Employee and Insider Risks



Close the doors to unauthorized data exfiltration

Enforce separation of duties and privilege

Implement strict password and account management policies and practices

Develop and implement a formalized data breach response plan

Carnegie Mellon University, Software Engineering Institute, the CERT Division, “Insider Threat Best Practices” (a full version is included in the *Supplemental Workshop Materials* and available to download).

EPSTEIN
BECKER
GREEN

Employees and the Internet of Things: Security in the Workplace

IPv6—340 trillion, trillion, trillion IP addresses. That’s enough addresses for many trillions of addresses to be assigned to every person on the Earth.
(APNIC, “More on IP addressing”)

IOT: “A global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a world-spanning information fabric known as the Internet of Things.”
(Pew Research Center, “Digital Life in 2025”)

Employees and the Internet of Things: Security in the Workplace

Every person and device will be connected to the Internet, including (potentially) in the workplace—much of it by wireless connectivity.

Bring your own device (BYOD) on steroids—watches, glasses, contact lenses, wearable fitness tools, televisions, and appliances.