36th Annual Workforce Management Briefing

Managing Workforce Compliance in an Unpredictable World

EPSTEIN BECKER GREEN

36th Annual Workforce Management Briefing

Managing Workforce Compliance in an Unpredictable World

Managing the Internal Threat: Preventing and Remediating Trade Secret Misappropriation by Disloyal Employees

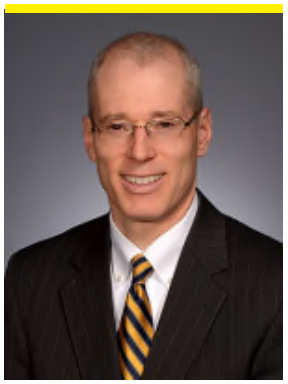
EPSTEIN BECKER GREEN

Panelists

John G. Bates
General Counsel and Chief Information Security Officer
Clarity Insights

Robert J. Hudock
Member
Epstein Becker Green
Washington, DC

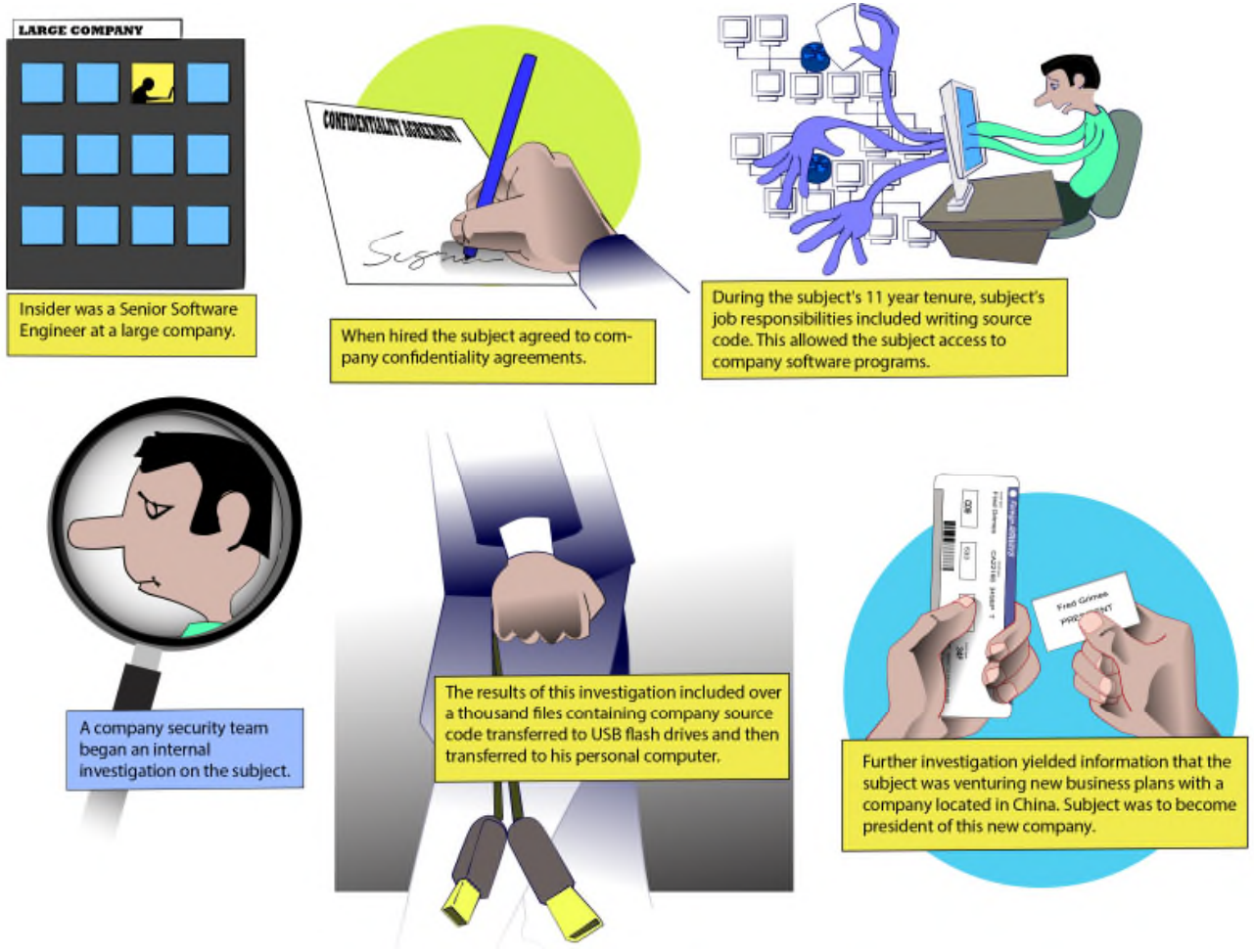
Jeffrey P. Rosier
Senior Employment Counsel and Director of State Government Relations
Marsh & McLennan Companies



Peter A. Steinmeyer
Member
Epstein Becker Green
Chicago

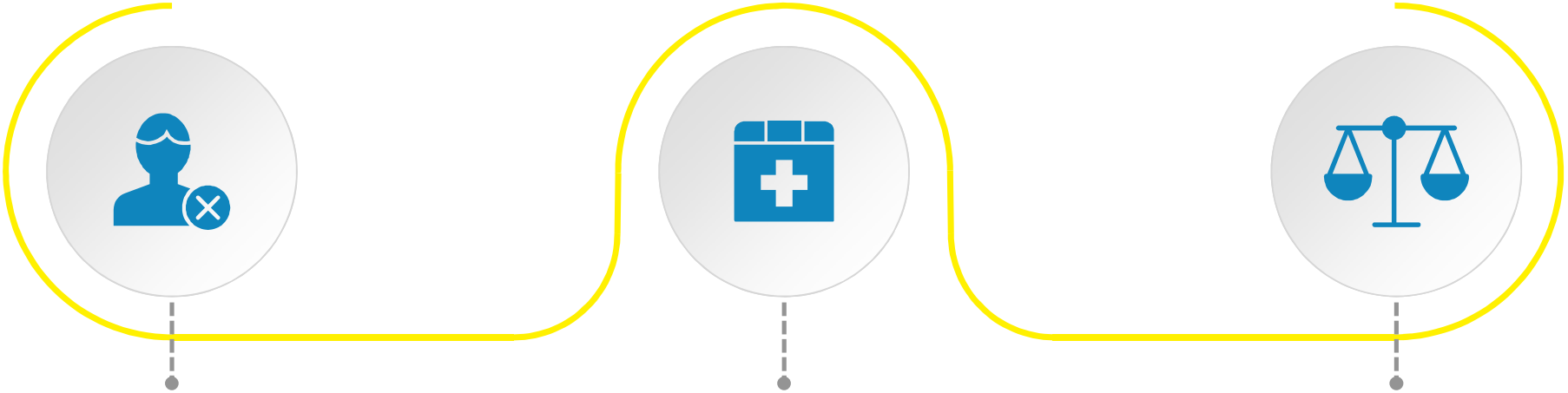
EPSTEIN BECKER GREEN

True Story: SWE – Failure to Restrict Access



EPSTEIN BECKER GREEN

Insider Threats: The Bad News



Most data breaches are caused by employees and other insiders (e.g., vendors), whether intentionally or inadvertently

One company found that insiders were responsible for 68% of all network attacks targeting health care data in 2016

74 percent of corporate counsel named data breaches as their top data-related legal risk

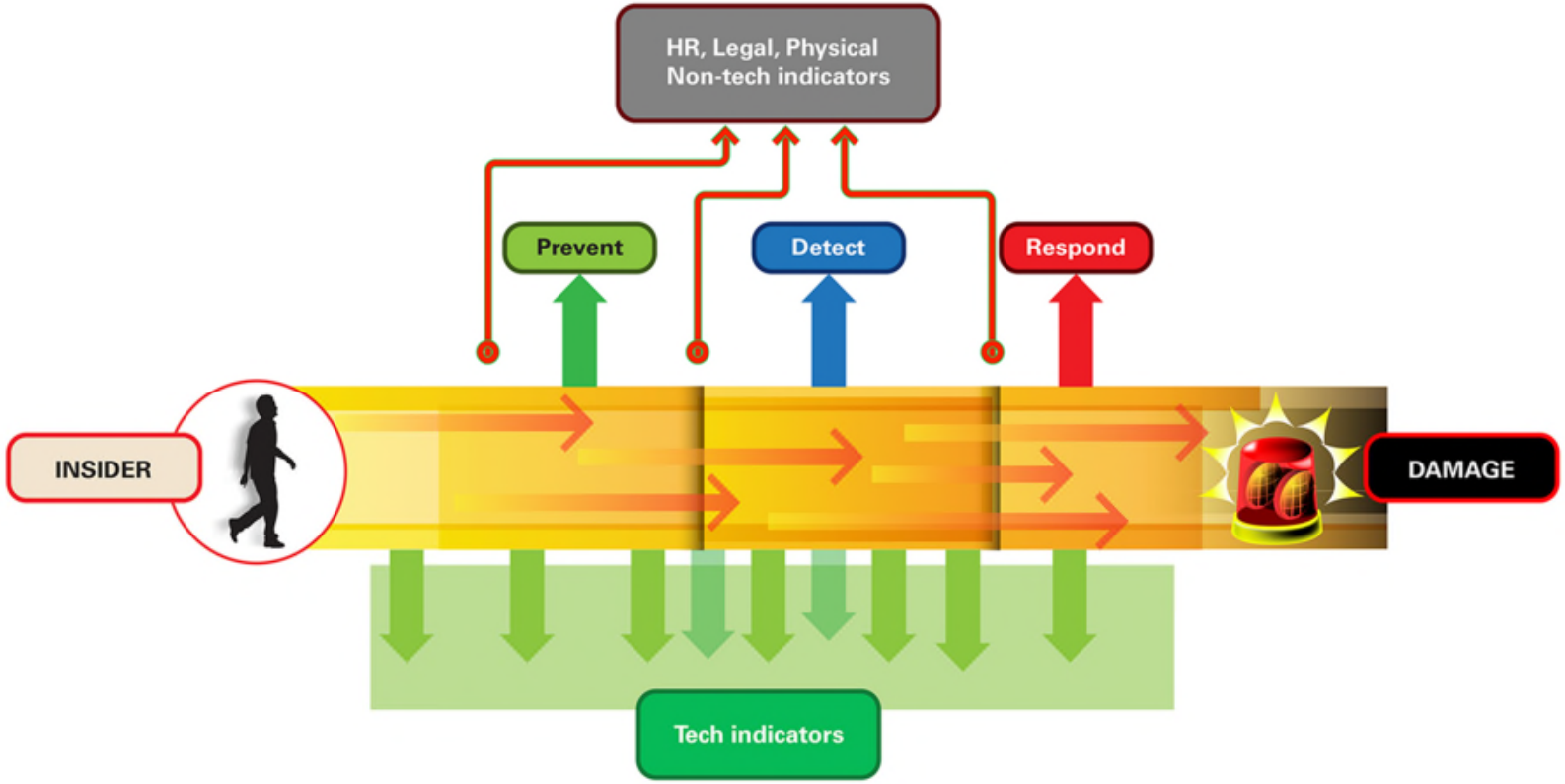
EPSTEIN BECKER GREEN

Insider Threats: The Good News

Many insider data breaches are *preventable*

EPSTEIN BECKER GREEN

Timeline of Insider Activity



Opportunities for preventing, detecting, and responding to an insider attack

EPSTEIN BECKER GREEN

How to Prevent Insider Threats?

Formalized,

Well-documented, and

Consistently applied insider threat program compliant with applicable law, including

- Screening
- Monitoring, and
- Regular training of employees

EPSTEIN BECKER GREEN

What Are Insider Threats?

A **malicious** insider is a current or former employee or a business partner who has or had authorized access to an organization's network 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

EPSTEIN BECKER GREEN

What Are Insider Threats? (Cont'd)

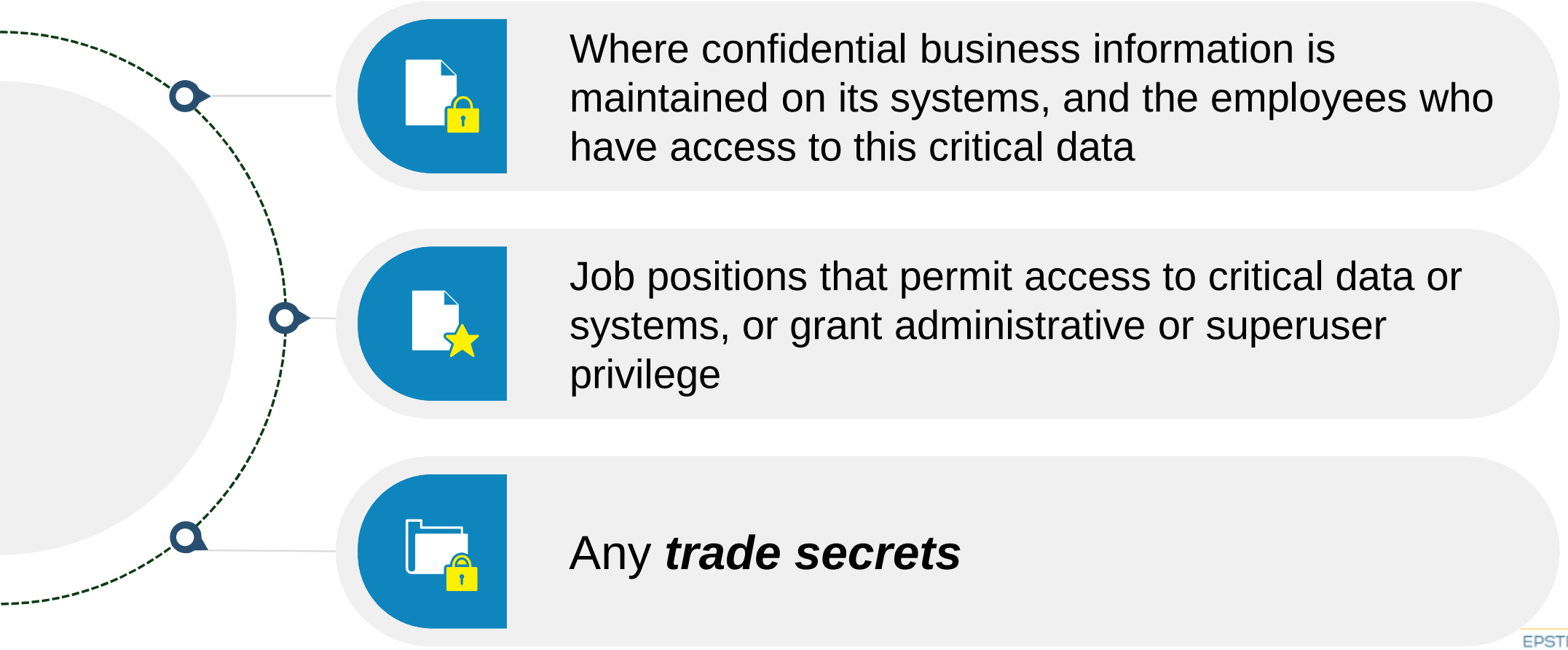
An **unintentional** insider is someone who, through his or her action/inaction without malicious intent, causes harm or substantially increases the probability of future harm to the confidentiality, integrity, or availability of the information or information systems

EPSTEIN BECKER GREEN

What Should the Employer's First Step Be?

Conduct a vulnerability assessment to evaluate risks according to job position and to the most sensitive data

What Should Employers Identify?



- Where confidential business information is maintained on its systems, and the employees who have access to this critical data
- Job positions that permit access to critical data or systems, or grant administrative or superuser privilege
- Any ***trade secrets***

EPSTEIN BECKER GREEN

What Constitutes a Trade Secret?

Has commercial and economic value precisely because it is not generally known

Is the subject of reasonable efforts to maintain its secrecy

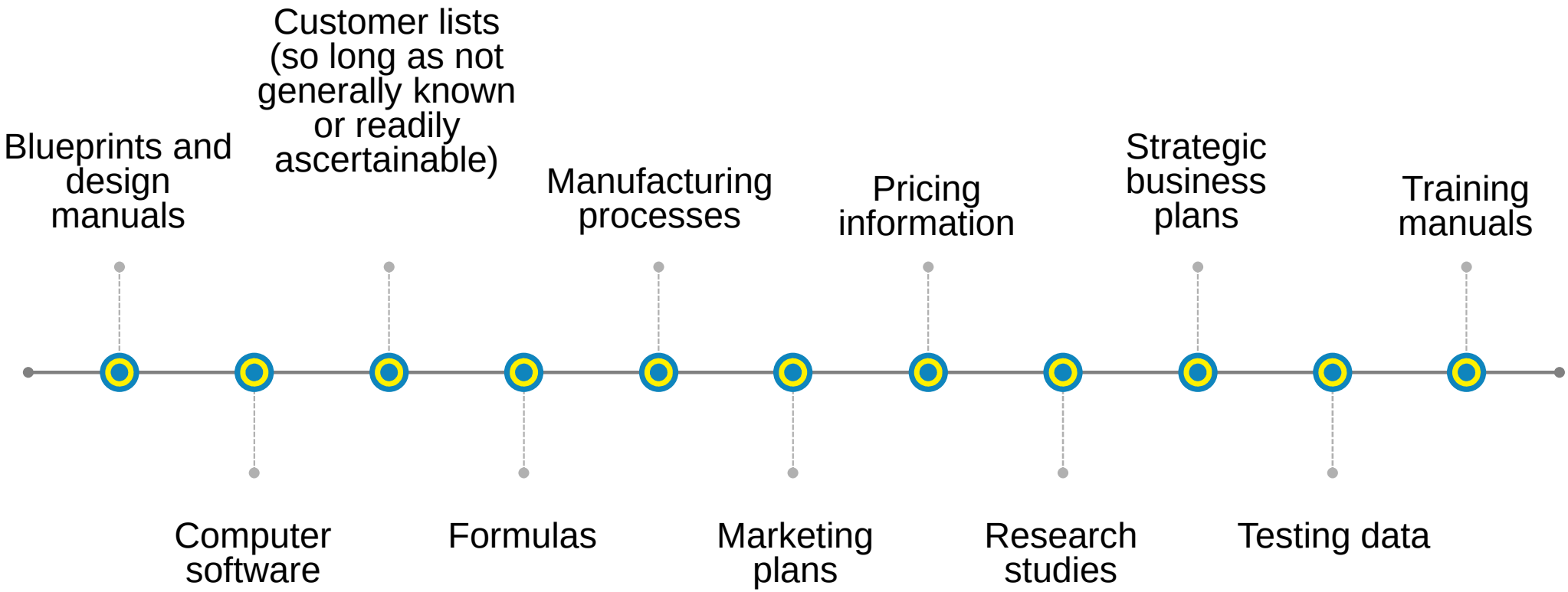
EPSTEIN BECKER GREEN

What Type of Information Can Be a Trade Secret?

- Technical or non-technical data
- Compilation
- Device
- Technique
- Process
- Formula
- Program
- Method
- Drawing
- Financial data

EPSTEIN BECKER GREEN

Examples of Trade Secrets



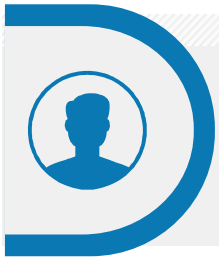
Once the Vulnerability Assessment Is Conducted and Trade Secrets Are Identified, What's Next?

The employer's program should be tailored to

- Prevent
- Detect, and
- Mitigate the identified risks by employees and to key data

EPSTEIN BECKER GREEN

Once the Vulnerability Assessment Is Conducted and Trade Secrets Are Identified, What's Next? (Cont'd)



Program should include personnel policies, including:

- Pre-hire and periodic background checks and credit monitoring
- Employee training
- Access control and electronic monitoring of employee system use
- Strong passwords
- Acceptable use policies
- Employer controls on the Internet of Things (IoT) in the workplace and Bring Your Own Device to Work (BYOD)

EPSTEIN BECKER GREEN

Once the Vulnerability Assessment Is Conducted and Trade Secrets Are Identified, What's Next? (Cont'd)

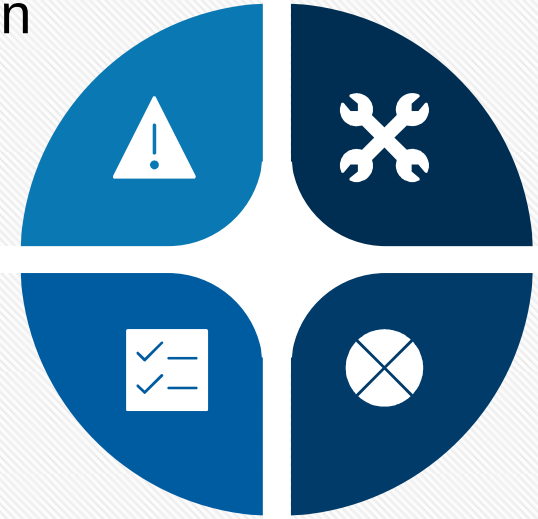
Program should also include:

- Addressing BYOD and IoT risks, including regulating types of *devices* that can be worn or used in the workplace
- Encryption for confidential data in transit and at rest
- Pre-hire and periodic background checks and credit monitoring
- Limiting access to documents
- Safeguarding documents

EPSTEIN BECKER GREEN

Ongoing Training Is Key to Successful Program

Ongoing training is important both in preventing breach and in defending against legal claims if a breach occurs



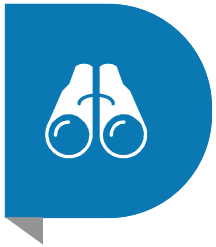
Training should address social engineering attacks (e.g., *ransomware*)

Training should occur *regularly*

Training prevents Events and intrusions

EPSTEIN BECKER GREEN

Documentation and Monitoring as Keys to Successful Program



Risks from disgruntled employees, or employees with a financial motive to participate in a data breach, should be documented and monitored using baselines and other objective measures

A deviation from normal baseline system activity or a high-risk event (e.g., demotion) should result in an objective trigger for increased scrutiny

EPSTEIN BECKER GREEN

Formulate a Response Plan

The program must anticipate the likelihood that a breach will occur and outline a ***response plan***

Forensic artifacts can be used to determine *who*, *what*, *when*, *where*, and *why* something occurred after a breach

The employer's policies in place (e.g., consensual monitoring) should facilitate any future forensic investigation and a quick response time

EPSTEIN BECKER GREEN

Legal and Other Options for Protecting Trade Secrets

- Confidentiality agreements (the *single* most important factor courts will look at when determining trade secret status
- Restrictive covenants, such as *non-compete* and *non-solicit* provisions
- Notification to new employers of restrictive covenants
- Use of "assignment of invention" clauses
- Use of exit interviews

EPSTEIN BECKER GREEN

Insider Threat Capabilities

Data Owners	Human Resources	Information Technology	Legal	Physical Security	Software Engineering	Trusted Business Partners
Access Control	Recruitment	Access Control	Agreements to Protect Sensitive Information	Facility Security	Technical Policies and Agreements	Screening/Hiring of Applicants
Modification of Data, Systems, or Logs	Policies and Practices	Modification of Data or Disruption of Services or Systems	Restrictions on Outside Employment	Physical Asset Security	Modification of Data or Systems	Management of Business Partners
Unauthorized Access, Download, or Transfer of Assets	Training and Education, Evaluation	Unauthorized Access, Download, or Transfer of Assets	Employee Behaviors in the Workplace		Asset Management	Asset Management
Incident Response	Policy and Practice Monitoring and Enforcement Programs	Detection and Identification	Conditions of Hire			Incident Response
Termination	Enforcement and Termination	Incident Response	Property Lending Agreements			Contractor/ Business Partner Agreements
		Termination	Contractor / Business Partner Agreements			

EPSTEIN BECKER GREEN

Conclusion

Cyber security and protection of trade secrets is a shared organizational responsibility—involving IT, Legal, and HR—and best addressed through an insider threat program

Stay vigilant!

EPSTEIN BECKER GREEN