October 24, 2024

ZwillGen

AON

The Do's and Don'ts of Monitoring and Surveillance

Corporate Insider Threat Programs and Employee Privacy

Marci Rozen, Senior Legal Director, ZwillGen PLLC

Brian Resler, Vice President, Stroz Friedberg

ZwillGen

AON

Insider Threats

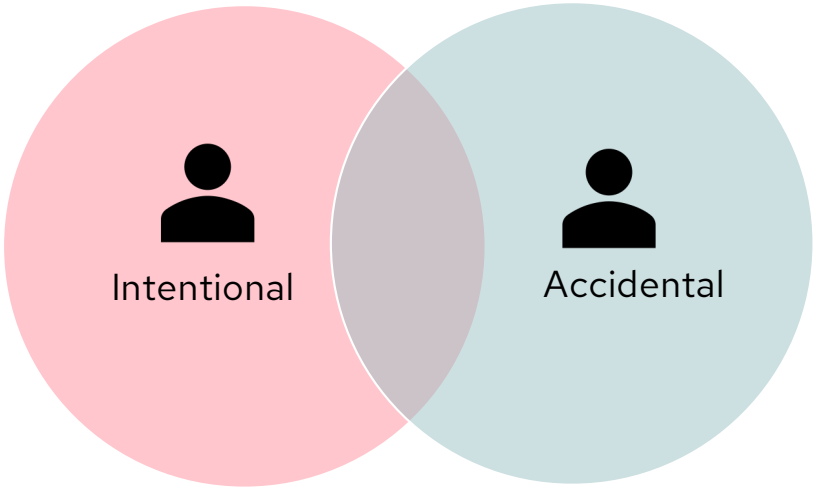
Definitions, Impact, and Detection

Insider Threats

Definitions

An insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

Source: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats



Insiders may also act in concert with external threat actors whether intentionally or unwittingly.

Insider Threats

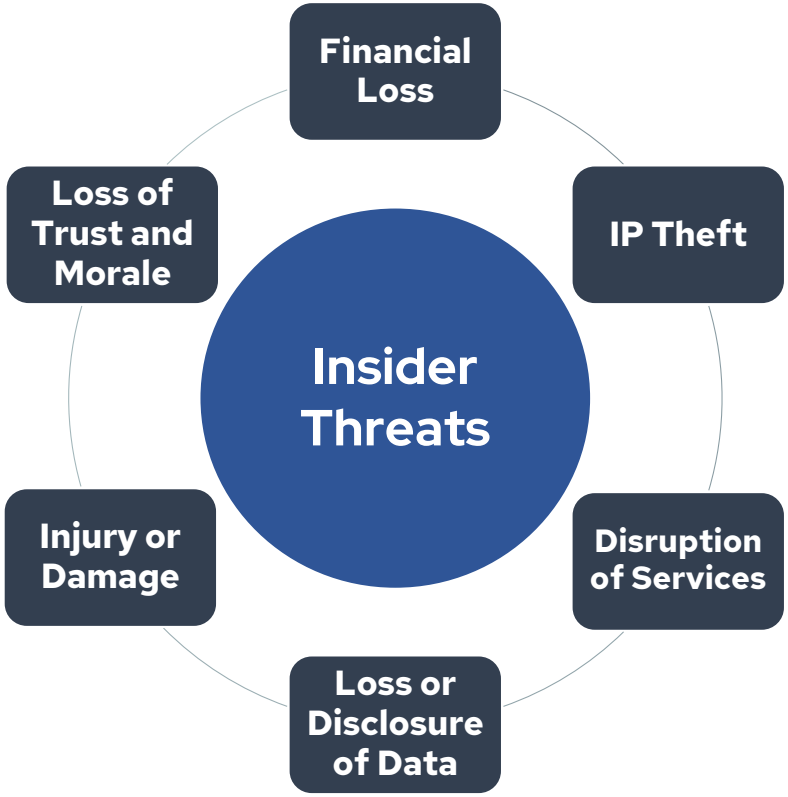
Consequences

Approximately 7% of breaches in 2023 were from *malicious* insiders.
Costs from these attacks almost 10% higher than average for cyber incidents and required longer to identify and resolve.

Source: IBM Security Cost of a Data Breach Report 2024

However, 75% of all insider attacks were from *non-malicious* insiders.

Source: Ponemon Institute 2022 Costs of Insider Threats Global Report



Insider Threats

Costs – Value of Lost IP

The FBI's IC3 reported that cybercrime cost the U.S. economy approximately $12.5B USD in 2023, with actual losses estimated to be much higher.

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

In contrast, an FBI report in 2019 estimated the annual cost to the U.S. economy from counterfeit goods, pirated software, and theft of trade secrets to be between $225B and $600B USD.

Source: https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf

Insider Threats

Physical Security

Controls and records of possession, access and use:

- equipment
- sensitive areas
- monetary instruments
- passes/tickets/badges
- logging systems
  (visitor records, cameras, locks, etc.)
- visitors

Insider Threats

Network Security

Controls and records for access, use and dissemination of information:

- email / communications
- systems and data
- sensitive information
- connected devices
- applications
- personal devices / apps
- other users' information or security controls

Insider Threats

Managing Sensitive and Trade Secret Information

- Identification and valuation of TSI
- Cataloging and auditing of TSI
- Implementation of classification, tracking and security protocols

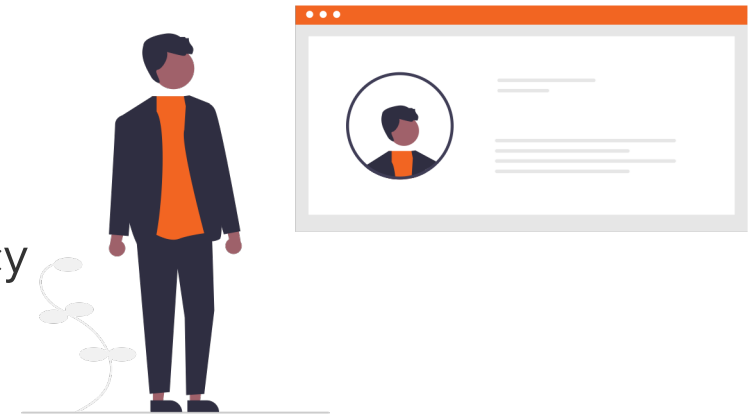
ZwillGen

AON

Employee Privacy Laws

A Patchwork of Federal and State Statutes

State Privacy Laws



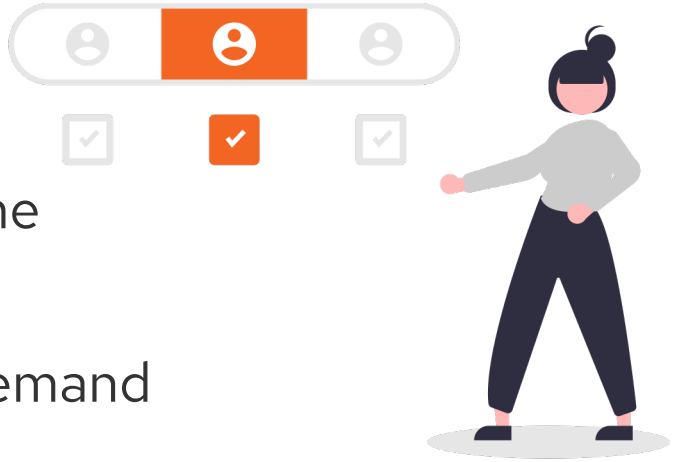
- California Consumer Privacy Act (CCPA):
  - First generally-applicable, comprehensive privacy law in the US; took effect in 2020, was amended by the CPRA in 2022.
  - 19 more states have now enacted similar privacy laws
  - Grants consumers rights with respect to "personal information" - defined broadly to include any information reasonably linkable to a consumer *or device* – including device IDs.
  - Rights include access, correction, deletion, "sale" opt out, sensitive data limits
  - All states **except California** exempt employee data.

Employer CCPA Obligations for Employee Data

- Employee privacy notice
- Employee rights requests:
  - Access
  - Deletion
  - Correction
  - Right to limit use of "sensitive" personal information

- Processing must be "necessary and proportionate"
- Section 7002 of regulations: Must get consent for processing that is not "reasonably expected" by consumers (including employees)
- Use reasonable security to protect employee data
- Note: CCPA does not override other legal obligations, such as obligation to retain data to comply with state or federal retention requirements

Other Employee Privacy Laws



- ECPA/Wiretap Act – practical requirement for notice of monitoring, either in policies or in real time
- State laws requiring notice of monitoring
- Social media laws – restrict employers' ability to demand access to accounts
- Biometrics privacy
  - General requirement for notice of processing in IL, WA, TX
  - Specific prohibitions on use of facial recognition (MD) and fingerprinting (NY)
  - Notice requirements and restrictions on employers' use of biometrics in CO

Tricky Issues

- No regulations on employee data, but AG conducted investigative sweep focused on employee rights compliance in July 2023
- In the meantime, employers struggle with:
  - Weaponized data requests;
  - How to scope data requests;
  - How to operationalize "Limit Use of Sensitive PI" requests from employees;
  - How to ensure that monitoring is "reasonably expected."
- Level of detail in monitoring policies – need to be specific to be informative and to establish "reasonable expectations," but not so specific as to unreasonably limit employer's ability to investigate novel situations

ZwillGen

AON

Challenges and Best Practices

Creating a Compliant and Effective Insider Threat Program

Calibrating the Scope of Monitoring

- Need to balance the need for comprehensive data collection with “necessary and proportionate” and “reasonable expectations” requirement in CA
- Scope data collection for business-owned devices and systems wherever possible
  - MDM solutions allow narrow scoping on personal devices for BYOD
- Focus on metadata vs. contents

Establish and Document Alerting Criteria

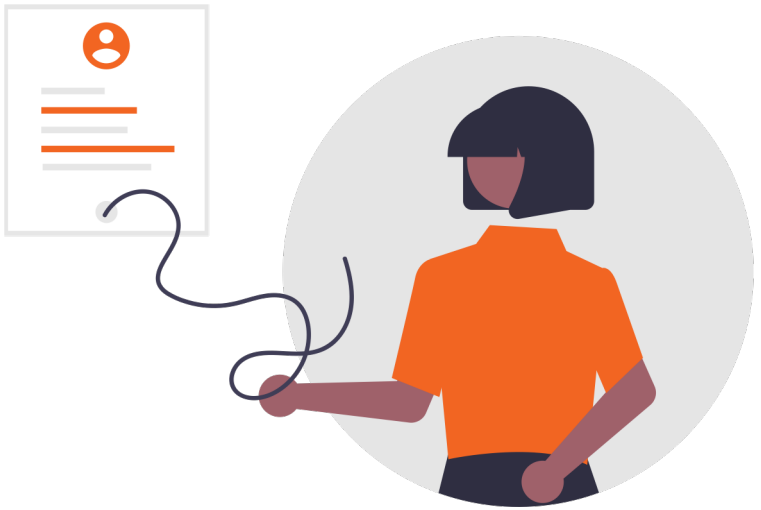
- Not enough just to have an insider threat software solution; you have to configure it
- Establish a baseline of typical behavior using technical tools combined with institutional knowledge
- Then calibrate alerts for some degree of deviation from baseline
- Document criteria to defend against allegations of unwarranted or prejudiced investigations

Document and Socialize Monitoring Policies

- Monitoring notices should include:
  - Types of monitoring used (corporate network, device activity, mobile activity, video, etc.)
  - Examples of the types of information included in routine monitoring
  - An explanation that the company reserves the right to monitor activity on all company-owned devices and networks, and investigate anomalous activity
  - An explanation of the company's BYOD policy and associated monitoring practices, if any
  - A statement that evidence obtained from such monitoring may be used in criminal, security and administrative proceedings.
- Obtain employees' acknowledgement of the policy
- Must pair this with other policies prohibiting use of non-company-issued accounts/platforms for business purposes

Implement Training and Awareness

- Periodic training, review and acceptance of:
  - terms of use for: devices, systems, data, access
  - non-disclosure agreements
  - non-compete agreements
  - assignment agreements
  - security awareness training

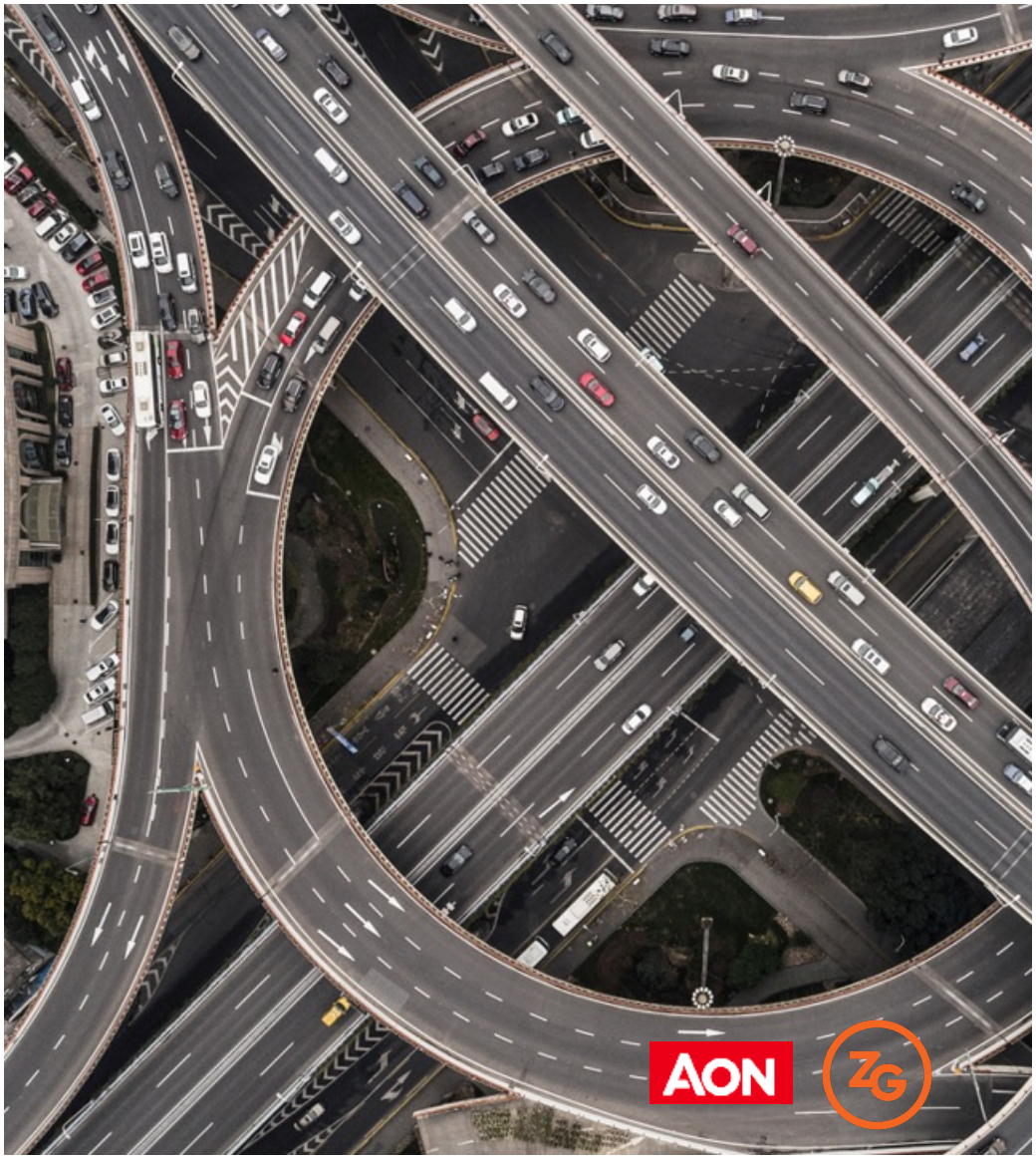


Insider Threats

Policy and Playbooks

Plan and roadmap for onboarding and offboarding, responding to a potential insider threat incident, and periodic review:

- monitoring of employees
- granting and cutting access
- preservation of data, equipment and logs
- when to call counsel and the importance of privilege
- when to call law enforcement
- entry and exit interviews



Respond to Employee Requests

– But Know There Are Exceptions

- AG sweep reminds us that employers need to recognize employee requests and have systems for responding
- But there are a number of exceptions that could be applicable in the employee context to protect against abuse
  - Right to defend against legal claims
  - Right to use sensitive information to ensure security and integrity
  - Employee requests cannot infringe on rights and freedoms of others

Practical. Creative. Trusted.