

The Inside Job:

Cyber Threats from Inside Your Own Organization



Joseph C. Santiesteban | Partner, Orrick

Kevin T. Faulkner | Vice President, Palo Alto Networks Unit 42

Speaker Introductions



Joseph Santiesteban

Partner

Orrick Herrington & Sutcliffe LLP

jsantiesteban@orrick.com



Kevin Faulkner

Vice President

Palo Alto Networks Unit 42

kfaulkner@paloaltonetworks.com

Agenda

- **Why It Matters**
- **How It Happens**
- **Prevent and Detect**
- **Respond**
- **Resources**

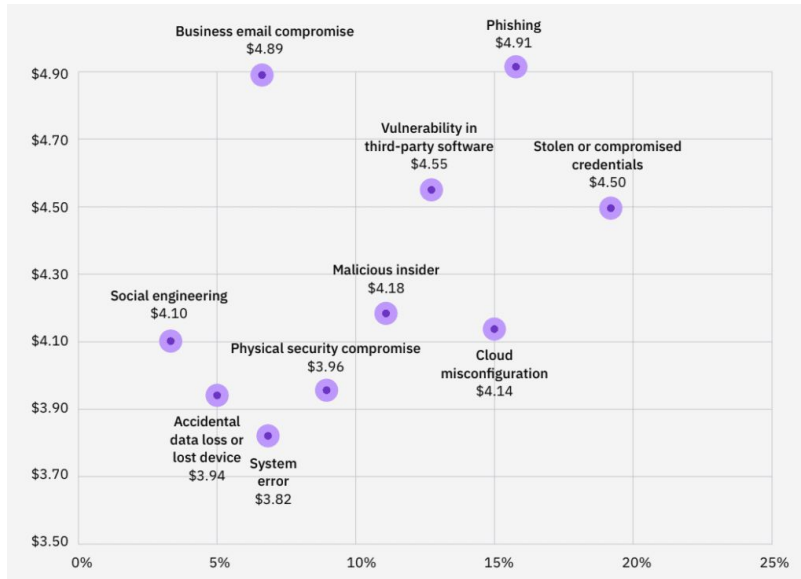


Why This Matters



Costs and Frequency

Average cost and frequency of data breaches by initial attack vector

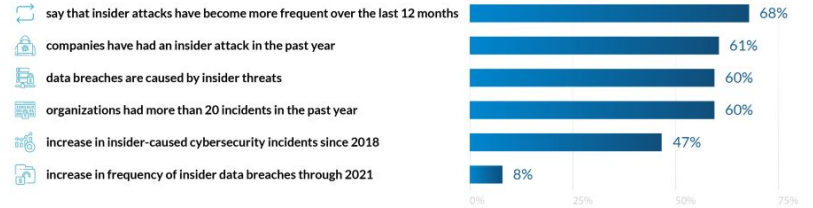


Source: Cost of a Data Breach Report 2022, IBM Security

3 Insider Threat Statistics You Should See

1 Insider Threat Frequency of Attacks

Sources: Goldstein, CyberSecurity, ObservIT, Shey, Bitglass, IBM



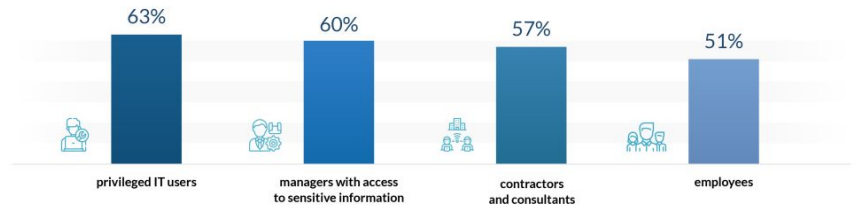
2 Top Motivations for Insider Attacks

Source: Fortinet



3 Top Insider Threat Actors

Source: Cybersecurity Insiders, Bitglass



Source: <https://financesonline.com/insider-threat-statistics/>

Types of insider threats



Unintentional

- Negligence
- Accidental action or inaction



Intentional

- Malicious Insider
- Harm for personal benefit or grievance

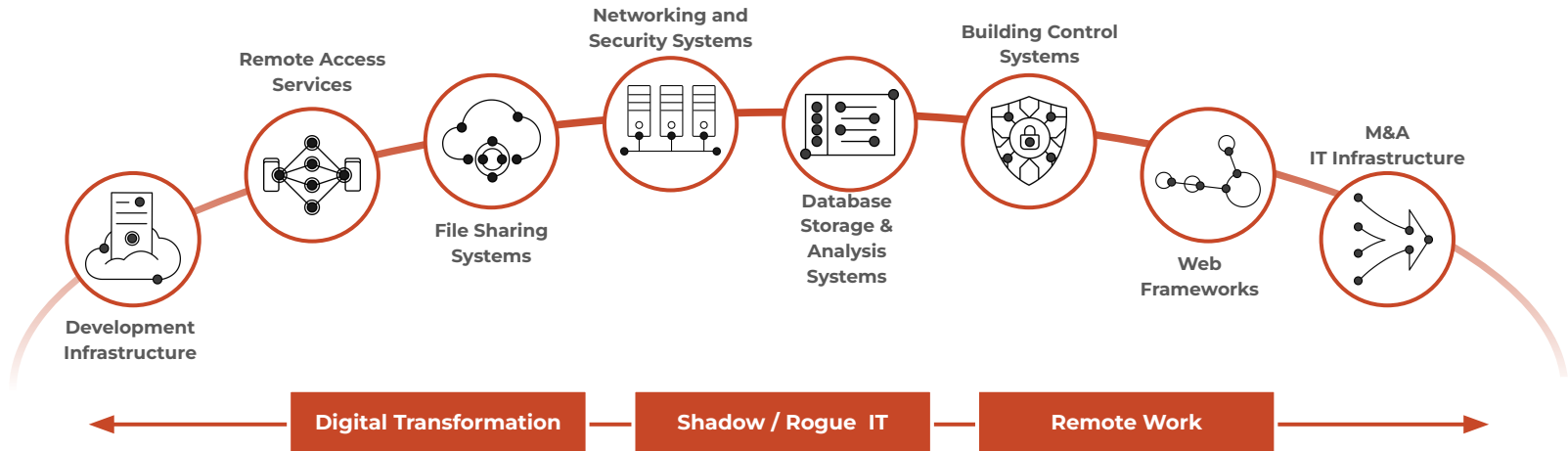


Other

- Collusive Threats
- Third-party Threats
 - Direct
 - Indirect

IT infrastructure has changed to support remote work, simplify access, and migrate to the cloud.

More flexibility also creates more risk for companies that aren't prepared.



The Legal Side



**Data Breach
Exposure**



**SEC and FINRA
Guidance**



HHS Guidance



**Customer
Expectations /
FedRAMP**



Privacy

How It Happens



Progression of an intentional insider

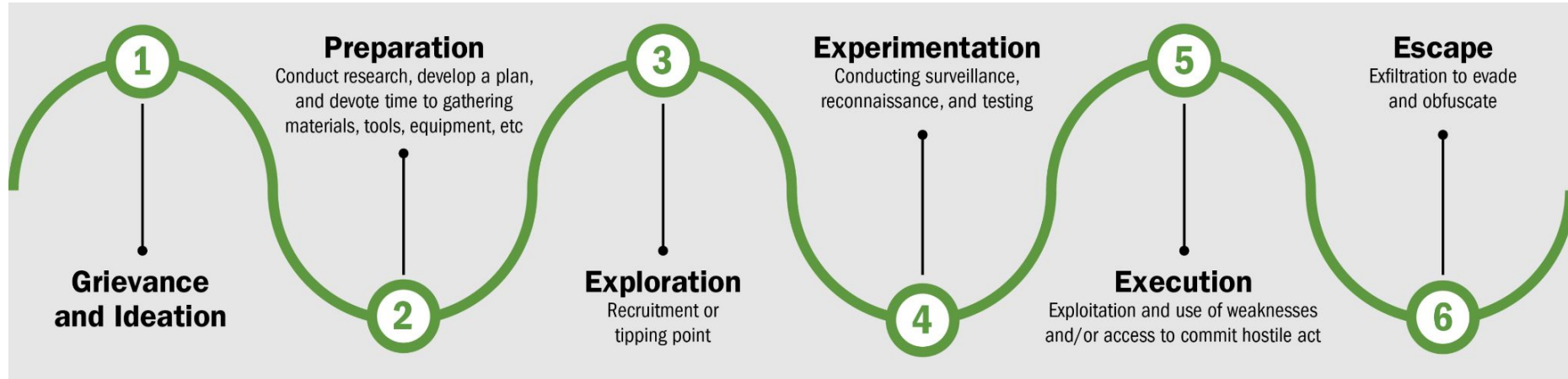


Image source CISA.gov

Exfiltration Methods - How Data Gets Out



Digital

- Email
- File transfer
- File sharing sites
 - Google Drive
 - Sharepoint
 - Box



Physical

- Devices
- Photocopies
- USB drives
- Hard drives



Other

- Pictures
- Video
- Verbal

Prevent



Prevention



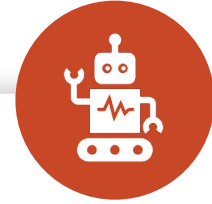
Governance & Training

- Know what data you have
- Know where your data is stored
- Train employees



Risk Assessment

- Find and mitigate your risks
- Repeat as your environment is never really static



Technologies

- IAM / Applications
- Endpoints
- Network Layer

Detect



Detection



Early Detection & Reporting

- If you see something, say something



Monitoring & Alerting

- EDR/MDR
- DLP
- UAM

Respond



Prepare to Respond



Incident Response Planning

- Involve the right groups of people
- How will teams respond?



Playbooks

- Develop plans and document how to operationalize a response into playbooks



Tabletops


- Practice response scenarios with all involved groups

Digital forensic analysis can uncover user actions



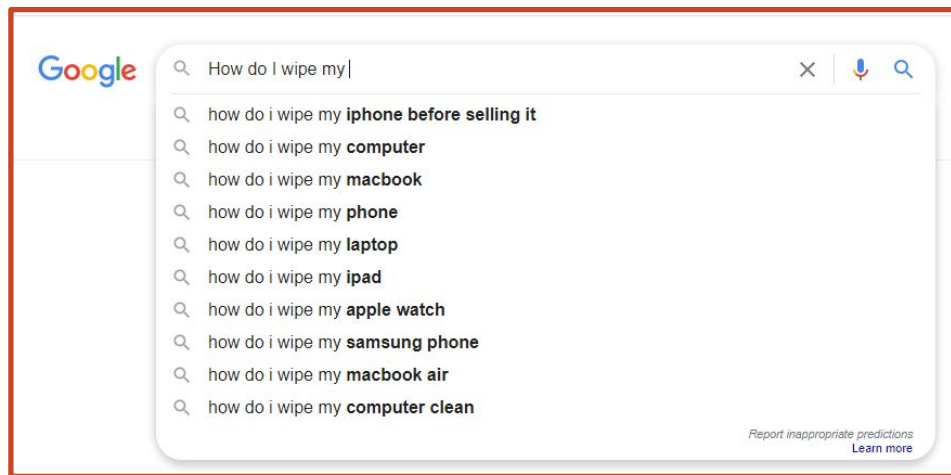
- External device connections
- File and folder creation, modification, and access dates
- Copying of files and folders
- Anti-forensic measures
- Internet history
- File and folder deletion

Examples of some digital forensic artifacts



- **Jumplist**
- **LNK file**
- **Shellbag**
- **Internet History**
- **Creation Date**
- **Modification Date**
- **Last Access Date**
- **File path**
- **Logs**

Even technical insiders may look for help



Get into the thought process:

- What might they take?
- How might they take it?
- How might they cover their tracks?

Resources



Helpful Resources

- <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>
- <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>
- <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/resources-and-tools>
- https://www.finra.org/compliance-tools/Industry_Risks_and_Threats/Effective_Controls_and_Practices



Thank you



paloaltonetworks.com

paloaltonetworks.com/unit42

orrick.com/en/Practices/Cyber-Privacy-and-Data-Innovation

