The CERT Top 10 List for Winning the Battle Against Insider Threats

Dawn Cappelli
CERT Insider Threat Center
Software Engineering Institute
Carnegie Mellon University

Session ID: STAR-203
Session Classification: Intermediate

Notices

Could this happen to you???

Actual insider incidents:

- *Night time security guard plants malware on organization's computers*
- *Programmer quits his job and takes source code back to his country of birth*
- *Group of employees work with outsiders to carry out lucrative fraud scheme*

These are only a few examples of the types of insider threats we are tying to prevent!!

Outline of the Presentation

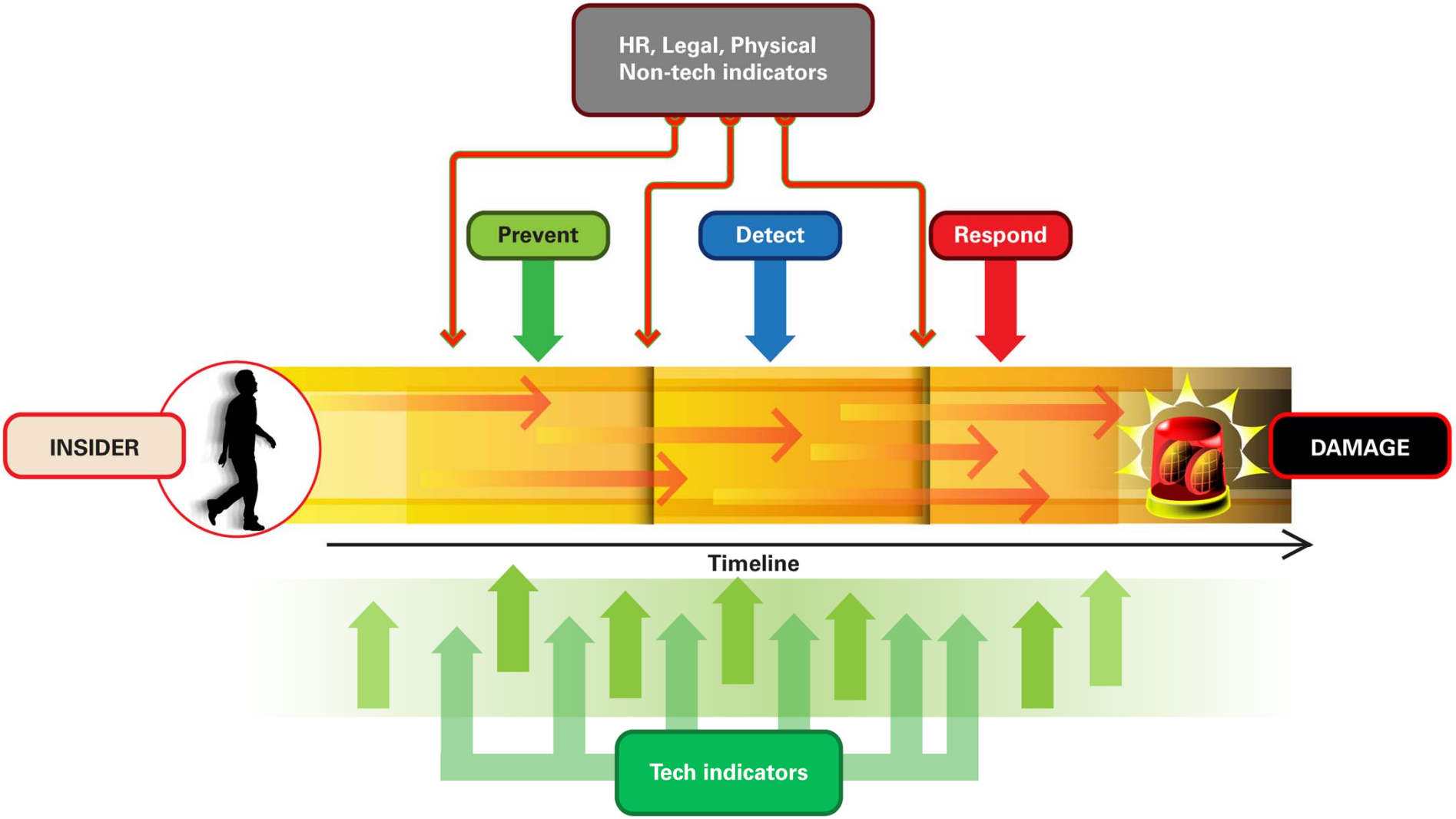
- Introduction
- Structure of this presentation
- Top 10 List
- Questions / Comments

What is the CERT Insider Threat Center?

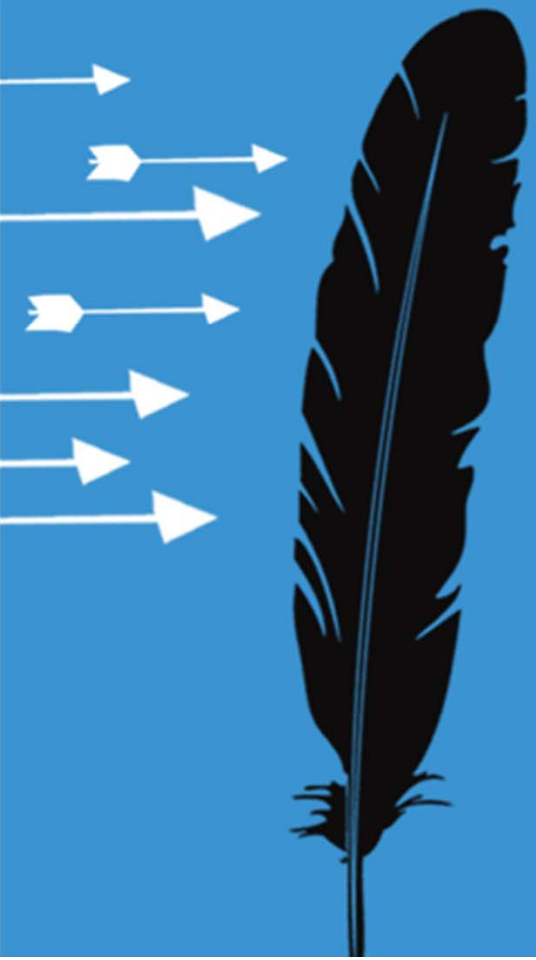
Center of insider threat expertise established in 2001

Our mission: ***The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats***

CERT Insider Threat Center Objective



Opportunities for prevention, detection, and response for an insider attack



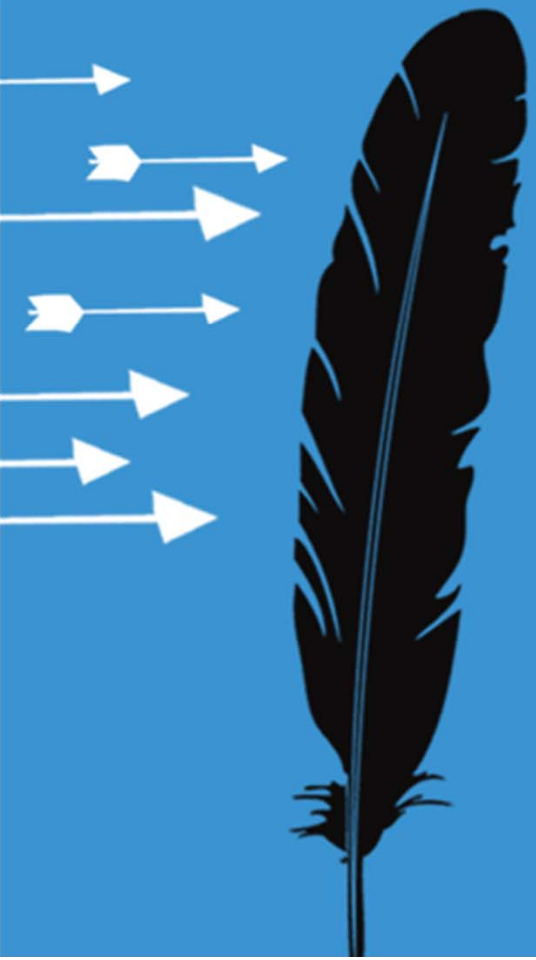
Structure of the Presentation

Structure of the Presentation

Compelling real case examples to reinforce why each item made the Top 10 list and ***WHY YOU SHOULD CARE!!***

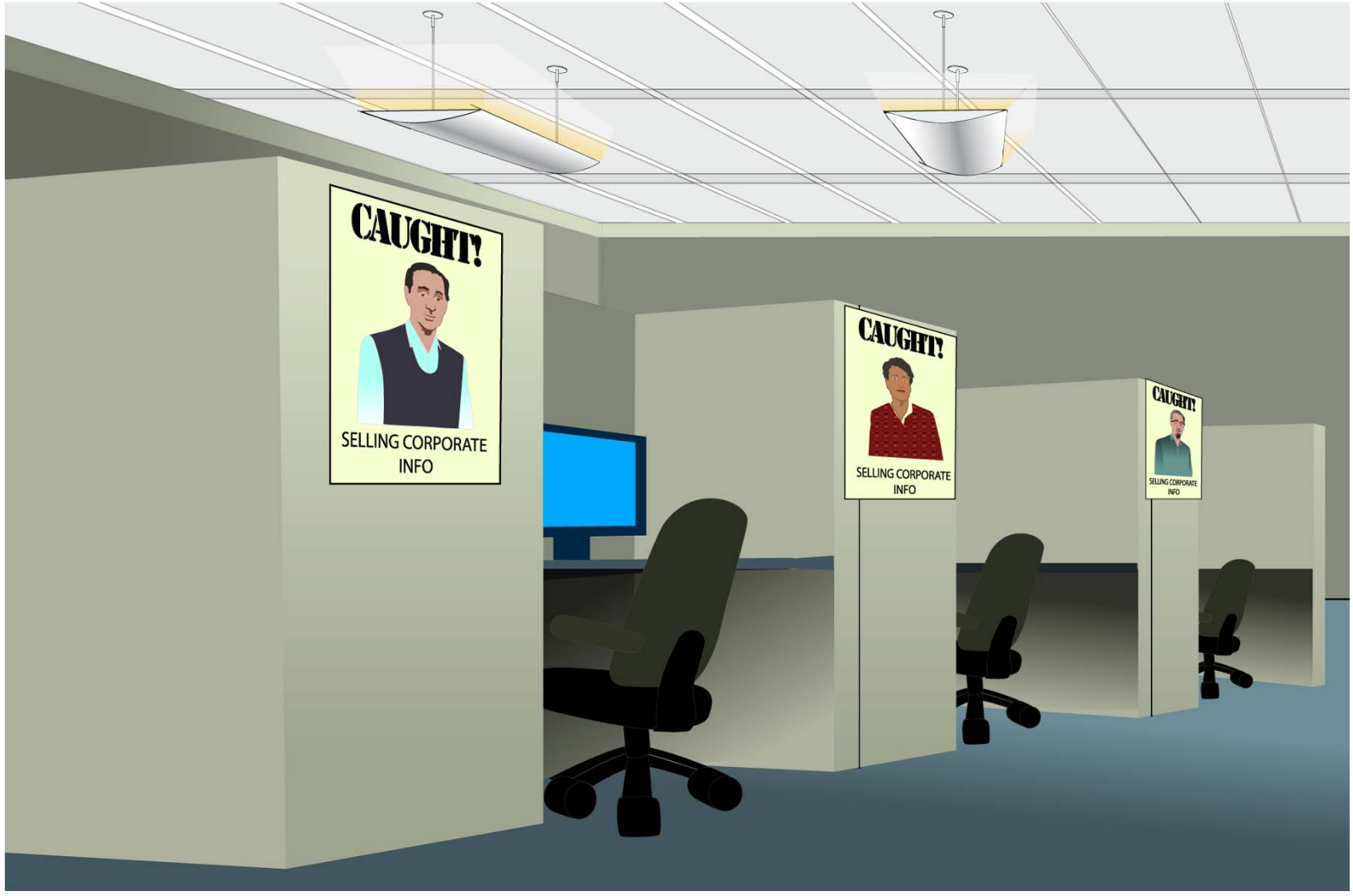
Explanation of each mitigation strategy

- What other organizations are doing
- Details you need to consider



Top 10 List….

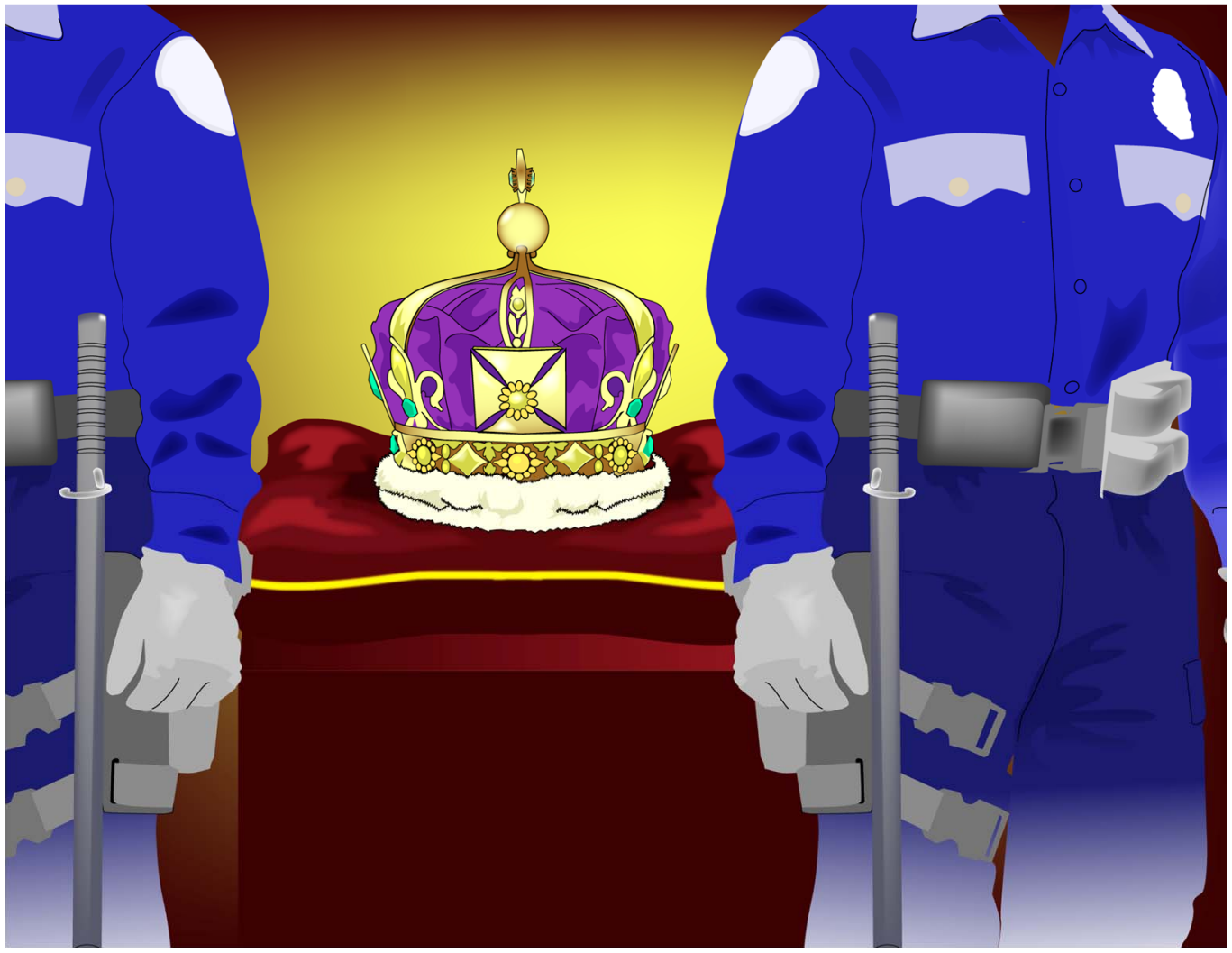
#10: Learn from past incidents



#10: Learn from past incidents

- Some organizations experience the same types of insider crimes more than once
- When you have an attack, implement controls to catch it next time
- Some organizations:
  - Create formal teams to examine past incidents and implement new controls

#9: Focus on protecting the crown jewels



#9: Focus on protecting the crown jewels

- One third of CERT's insider theft of IP cases involve a foreign government or organization
- What would happen if your IP was stolen and taken out of the country???
- Most insiders use authorized access to steal IP
  - But they don't always require the access!
- Some organizations:
  - Implement extra controls for THE most critical IP
  - Protect against "erosion of access controls"

#8: Use your current technologies differently

#8: Use your current technologies differently

- Some organizations
  - Create an insider threat team or train Security Operations Center (SOC) staff about insider threat
  - Use Intrusion Detection Systems (IDS) to examine data going out as well as in
  - Tailor use of tools to reduce information overload (Data Leakage Protection, host based controls, change controls)
  - Create signatures in Security Information and Event Management systems (SIEMs) / log correlation tools to detect suspicious insider activity
    - After-hours reconnaissance activity by privileged system users who are “on the HR radar”
    - Exfiltration via email within 30 days of resignation

#7: Mitigate threats from trusted business partners

#7: Mitigate threats from trusted business partners

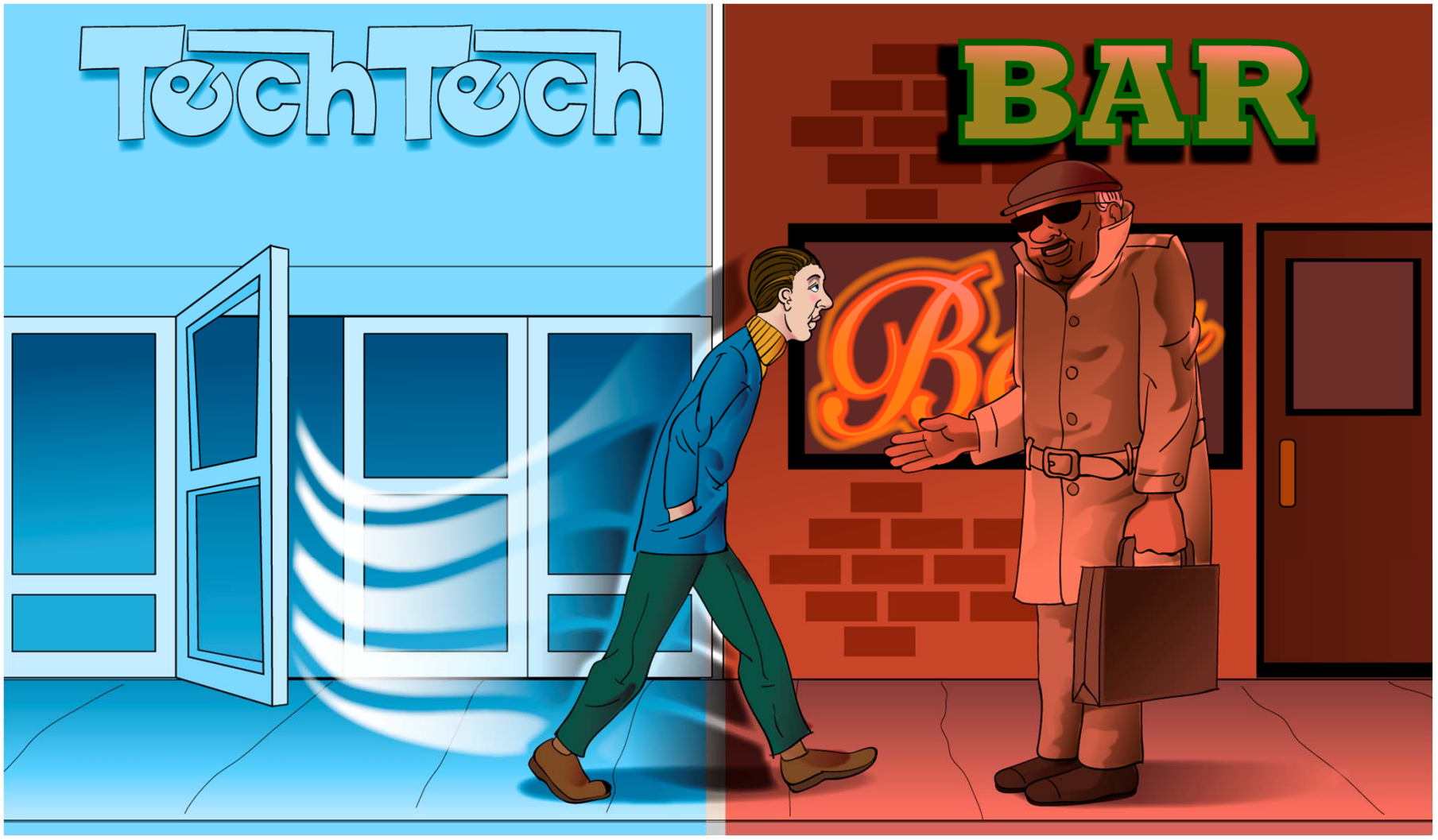
- Trusted Business Partners (TBPs) include
  - contractors
  - outsourced companies
- Some organizations:
  - Specify information security controls in contracts
  - Require the same controls for their TBPs as they require internally
  - Audit TBP policies and procedures
  - Require same policies and procedures for contractors as for employees

#6: Recognize concerning behaviors as a potential indicator

#6: Recognize concerning behaviors as a potential indicator

- Concerning behaviors are the 4th most common issue of concern in the CERT Insider Threat Database
- Negative employment issues are the 8th
- Most prevalent in insider IT sabotage and theft of IP
- Some organizations
  - Educate management staff on insider threat indicators
  - Communicate employees “on the HR radar” to security staff
  - Integrate cyber insider threat mitigation with their workplace violence program

#5: Educate employees regarding potential recruitment



#5: Educate employees regarding potential recruitment

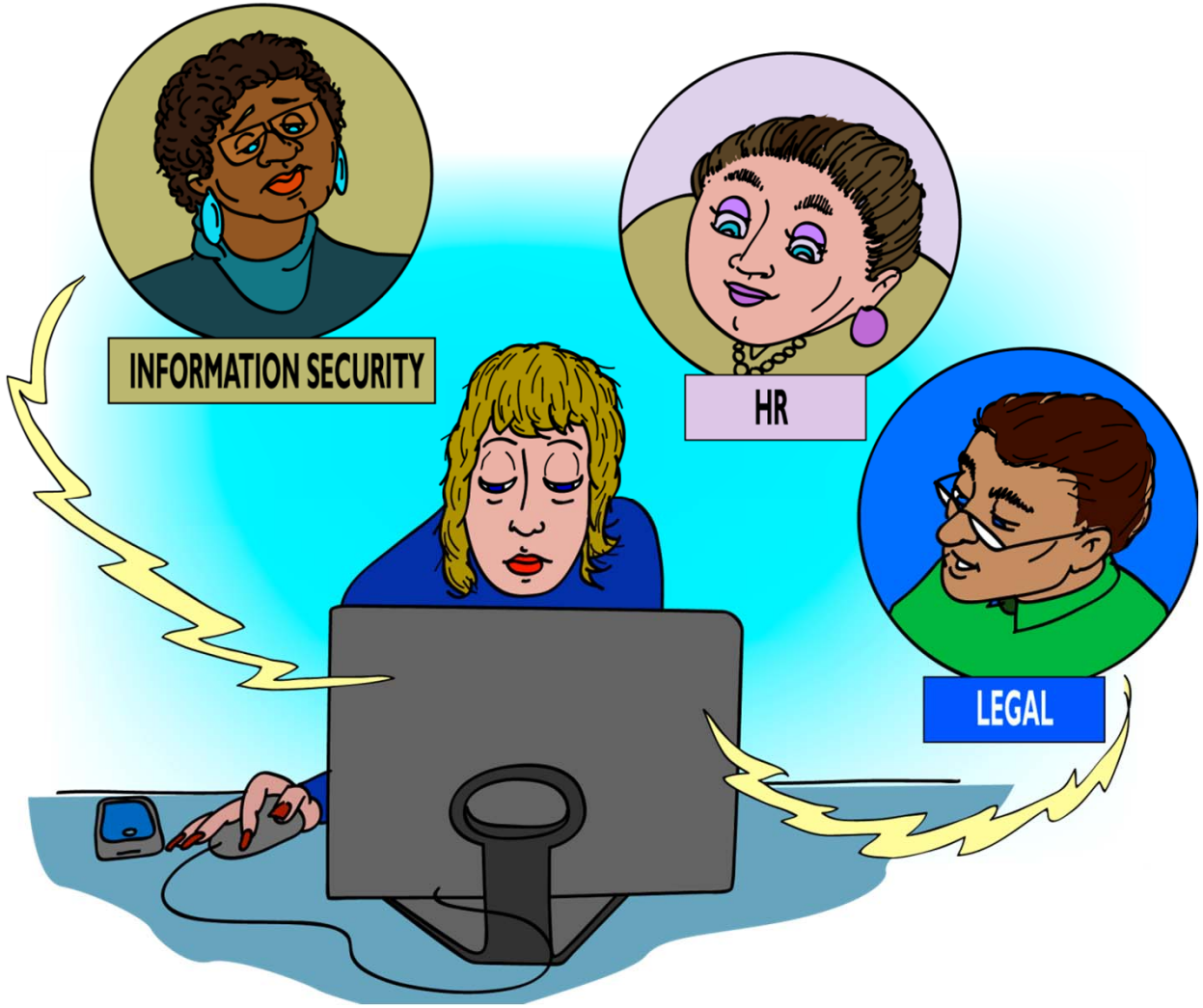
- Recruitment is the 3rd most common issue of concern in the CERT Insider Threat Database
- Carefully consider: do you have any systems or data that an insider could be paid to steal or modify?
  - Financial, Personally Identifiable Information (PII), identity documents, utility bills, food stamps, credit histories ,…
- Some organizations:
  - Perform periodic background checks for existing employees

#4: Pay close attention at resignation / termination!

#4: Pay close attention at resignation / termination!

- Change in employment status is the TOP issue of concern in the CERT Insider Threat Database
- BUT… Typically not in fraud cases!
- Some organizations
  - Perform targeted employee monitoring
    - Low performing employees
    - Employees who will be laid off or terminated
  - Implement special controls for their most critical IP

#3: Address employee privacy issues with General Counsel



#3: Address employee privacy issues with General Counsel

- Employee privacy issues present a tricky legal issue
- Laws and regulations differ in private sector, government, and various critical infrastructure sectors
- Some organizations:
  - Have created and implemented insider threat policies and processes by working with Human Resources, General Counsel, Information Security / Information Technology, Security, and top management

#2: Work together across the organization

#2: Work together across the organization

- IT cannot solve this alone!
- Need communication across Management, Information Security / Information Technology, Security, Data Owners, Software Engineering, General Counsel, and Human Resources
- Some organizations:
  - Achieve this communication but only after significant suspicious activity warrants an investigation
  - Have achieved proactive communication between some of these organizational units

#1: Create an insider threat program NOW!

#1: Create an insider threat program NOW!

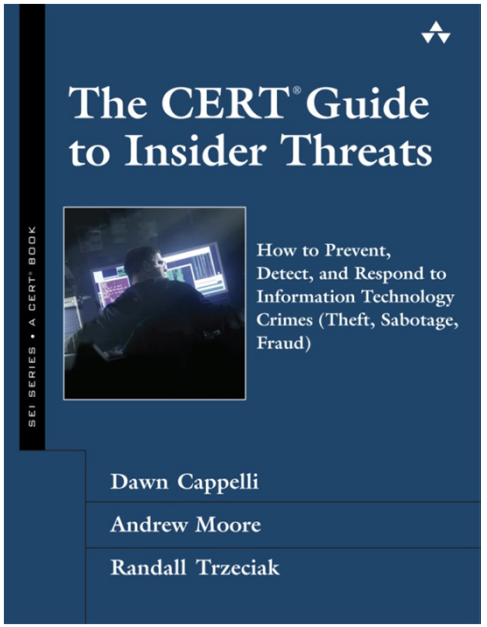
- In the first three months following this presentation you should:
  - Obtain buy-in from top management
  - Form an insider threat team
  - Create policies (approved by General Counsel)
  - Develop processes and implement controls
- Within six months you should:
  - Roll out and consistently enforce the policies
  - Regularly communicate across your organization

#1: Create an insider threat program NOW!

- Some organizations
  - Follow an enterprise-wide insider threat strategic plan which was created by C-level managers
  - Have designated a Director responsible for the insider threat program
  - Have made a significant investment in an insider threat program

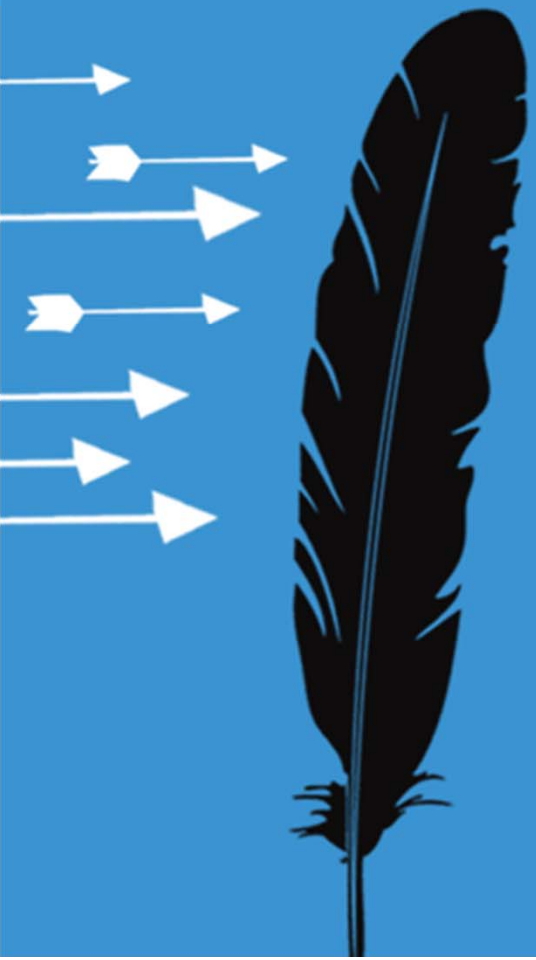
CERT Resources

- Insider Threat Center website (http://www.cert.org/insider_threat/)
- *Common Sense Guide to Prevention and Detection of Insider Threats* (http://www.cert.org/archive/pdf/CSG-V3.pdf)
- Insider threat workshops (http://www.cert.org/insider_threat/docs/workshop.pdf)
- Insider threat assessments (http://www.cert.org/insider_threat/docs/assessment.pdf)
- New controls from CERT Insider Threat Lab (http://www.cert.org/insider_threat/controls/)
- Insider threat exercises
- The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak

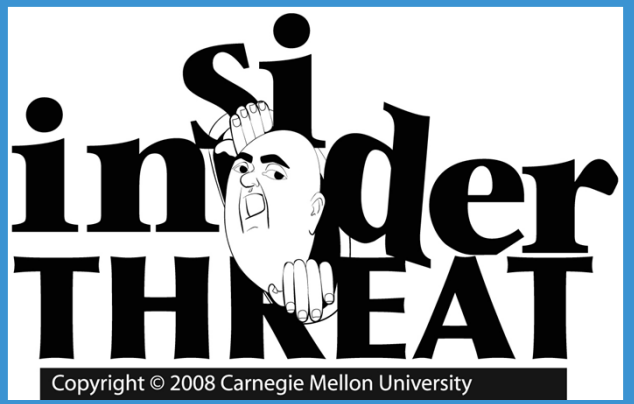


The CERT Top 10 List for Winning the Battle Against Insider Threats

10. Learn from past incidents
9. Focus on protecting the crown jewels
8. Use your current technologies differently
7. Mitigate threats from trusted business partners
6. Recognize concerning behaviors as a potential indicator
5. Educate employees regarding potential recruitment
4. Pay close attention at resignation / termination!
3. Address employee privacy issues with General Counsel
2. Work together across the organization
1. Create an insider threat program NOW!



Questions / Comments



Point of Contact

Dawn M. Cappelli
Director, CERT Insider Threat Center
CERT Program, Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9136 – Phone
dmc@cert.org – Email

http://www.cert.org/insider_threat/