



Insider Threat- Real or Myth?

PN Narayanan – Chief Information Officer
Keith Hartung – Information Security Officer

30M/
\$100B

Payments worth more than \$100 Bn last fiscal year.

\$15Bn

In State Assets Managed by IT Systems

PA 529

The PA 529 College and Career Savings Program has \$4.8 billion in assets with over 231,000 accounts as of September 30, 2018.

Unclaimed Property

Collected \$422 million and returned nearly \$228 million, generating nearly \$194 million for the General Fund in FY 16-17.

What is an insider threat?

A malicious insider is a current or former employee, contractor, or business partner who intentionally or unintentionally cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

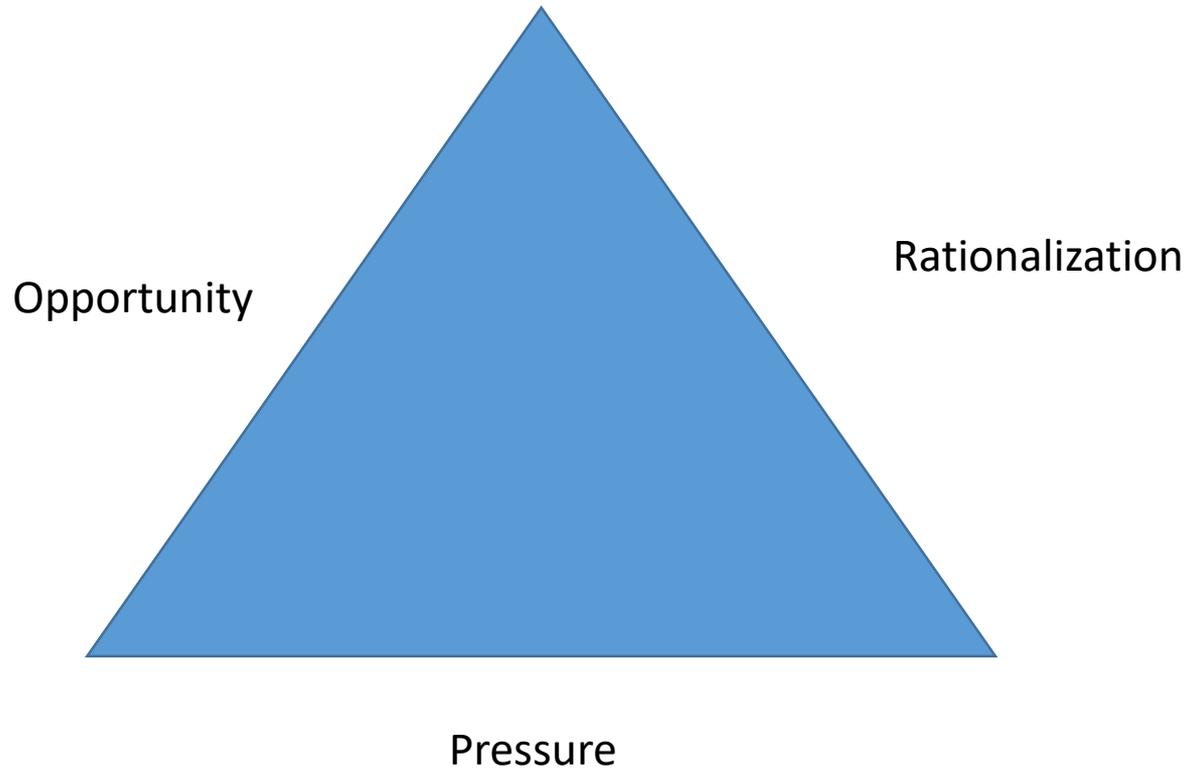


Common Sense Guide to Mitigating Insider Threats, Fifth Edition - The Software Engineering Institute – Carnegie Mellon University

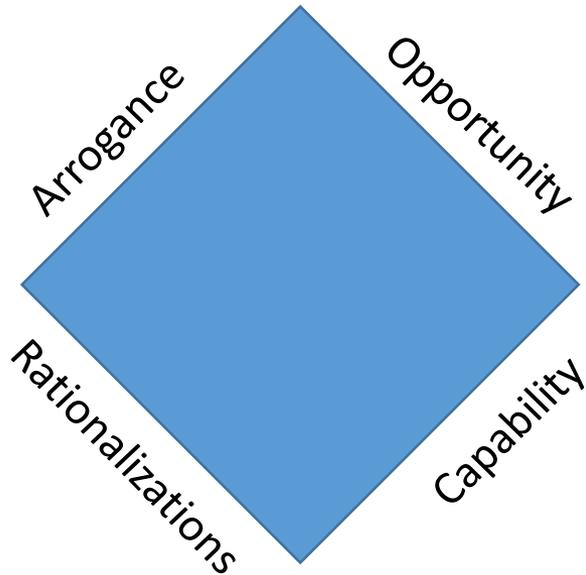
1. In May 2015 a, former employee of the US department of energy and US Nuclear Regulatory Commission sent spear phishing mails to 80 specific DOE employees to gain classified information that he intended to pass on to foreign embassy.
2. Edward Snowden – do I need to go any further?

1. Source : From Fraud-magazine.com July/Aug 2018

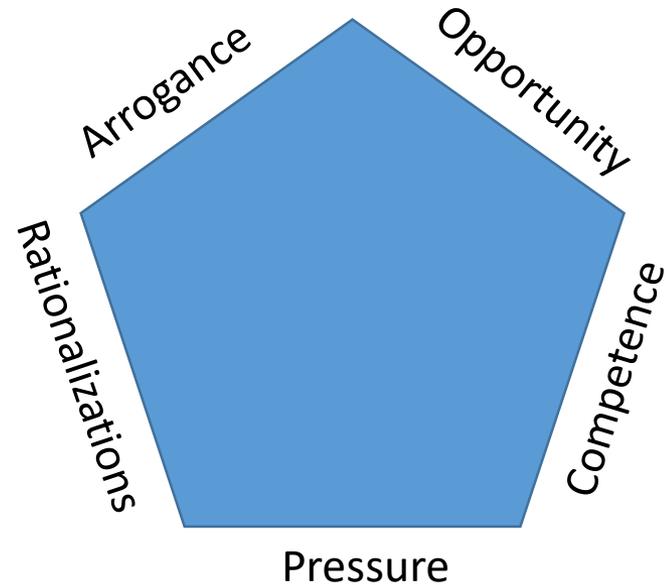




Fraud Diamond



Fraud Pentagon



1. The Fraud diamond – Considering four elements of fraud – David D. Wolfe and Dana R. Hermanson
2. Fraud Pentagon – Crowe Horwath LLP

7 Insider Threats

- Scams work because human beings are susceptible to emotions.
- Technology is helping hackers to exploit human emotions easily through many social media avenues and good old emails....
- Most of the insider threats are due to ignorance, carelessness, and avoidable.
- But, serious damages are caused by users with higher privileges, those in position to intentionally compromise the information assets for personal gains.



Insider threats are black swan events.



Every breach is an unexpected act by an individual whom we bestowed with our trust.



9 Why is it hard?

- Every time people express surprise when an insider breaches confidence.
- He/she is one of us...
- If you don't trust them you don't trust me too
- I am honest, why should I be monitored?
- If you watch everyone morale goes down.

O TRU JUST

Policies

Procedures

Technologies



- Policies and procedures can facilitate or prevent harmful insider actions

Facilitate	Prevent
Not Communicated	Train employees
Misunderstood	Written clearly
Inconsistently enforced	Fair

5 Best Practices to Prevent Insider Threat - The Software Engineering Institute – Carnegie Mellon University

Realities of occurrence

- Reports indicate 23% to 28% of breaches can be attributed primarily to criminal internal actors



On the contrary, 64% of breaches occurred due to insider carelessness.



“Ponemon Institute Insider Threat Global report” & “The 2018 Verizon Data Breach Investigations Report”

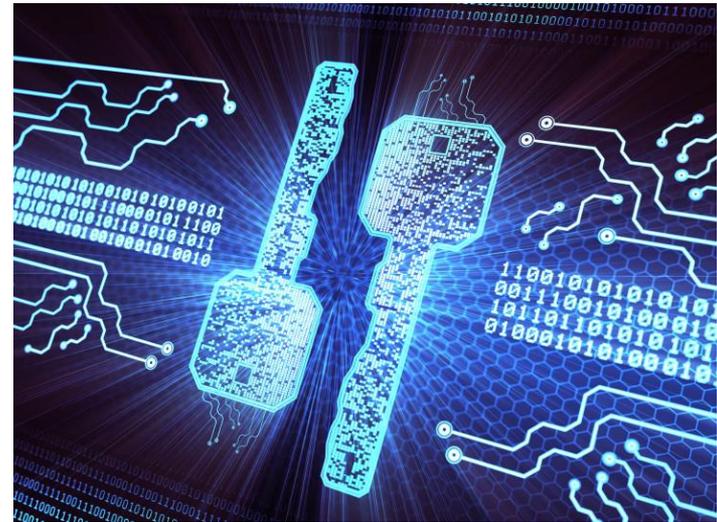
Policy and Procedure are not Enough

- Just 13 percent of government employees believe they have personal responsibility for the security of their work devices or information
- One in three employees believed they were more likely to be struck by lightning than have their work data compromised
- 75% of employees identified the importance of using encryption when sharing confidential documents.
 - Yet, only 16% actually used encryption when sharing confidential documents.

YouGov survey by security services firm Dtex Systems.



- Counter bad actors
- Reinforce good behaviors to counter carelessness
 - Automate
 - Prompt
- Enable Zero Trust



What is Zero Trust?

- The evolution of the old standby: “Trust, but Verify”
- Nothing and no one is automatically trusted.
- Every machine and every user is verified before access is permitted.



- Begins with Policies
- Driven by Procedure
- Enabled by Technologies:
 - Identity Access Management (IAM)
 - Multi-Factor Authentication (MFA)
 - Risk-based Authentication (RBA)
 - Encryption
 - Network Segmentation



Getting Started

- Incremental implementation
- Asset Identification – you can only protect what you know about.



- Asset Classification – enables protection technology
- Cooperation and communication

- Identify normal
 - Remove unnecessary access privileges
 - Enables you to look for the abnormal
- Revisit
 - New processes
 - New technologies



Leverage your existing tools

- Data loss prevention
- Encryption
- Authentication methods
- Log management
- Network monitoring
- Verify licensing



- Data Volume
- Speed
- Coverage 24/7



- Where available use Machine Learning / Artificial Intelligence

Identify Gaps

- Easier said than done
- Don't just focus on technology



