The Unspoken Threat:

Ransomware Infections via the Insider Threat Vector

Brett Tucker, Technical Manager, Cyber Risk

Randy Trzeciak, Acting Technical Director, Security Automation

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0832

Assessing Insider Threat for Ransomware May Impact the Entire Organization

All attendees will walk away with a greater appreciation for risk:

Educate + Learn = Apply

- Apply Principles of Risk Interdependency to Show that Insider Threat is a "Team Sport"
- You will recognize your own organizational challenges with a Ransomware example
- You will gain practical ideas to manage risk and be educated on insider threat

Bottom Line: Insider Threat is a "Team Sport" where its application may reduce exposure across the enterprise

In a World of Great Uncertainty

What is Certain?

- Risk environment will not contract – number of risks and **complexity will increase**
- Organizations must get better at "**surviving**" uncertainty
- **Knowledge and awareness of risk issues** must be pervasive throughout the organization
- Traditional tools, techniques, and methods may not work and will need to **evolve**
- Organizations must be **agile** enough to adapt

Information Security Risk Management

Risk = Probability (Threat exploits Vulnerability causing Unwanted Outcome)

Threat = External, Internal, Human, Non-Human, Malicious, Non-Malicious

Insider Threat Mitigation

Insider Incident

Prevent / Detect

if detected

Respond/Recover

Insider Threat

Identify / Deter

if detected

Consistent Response

Insiders

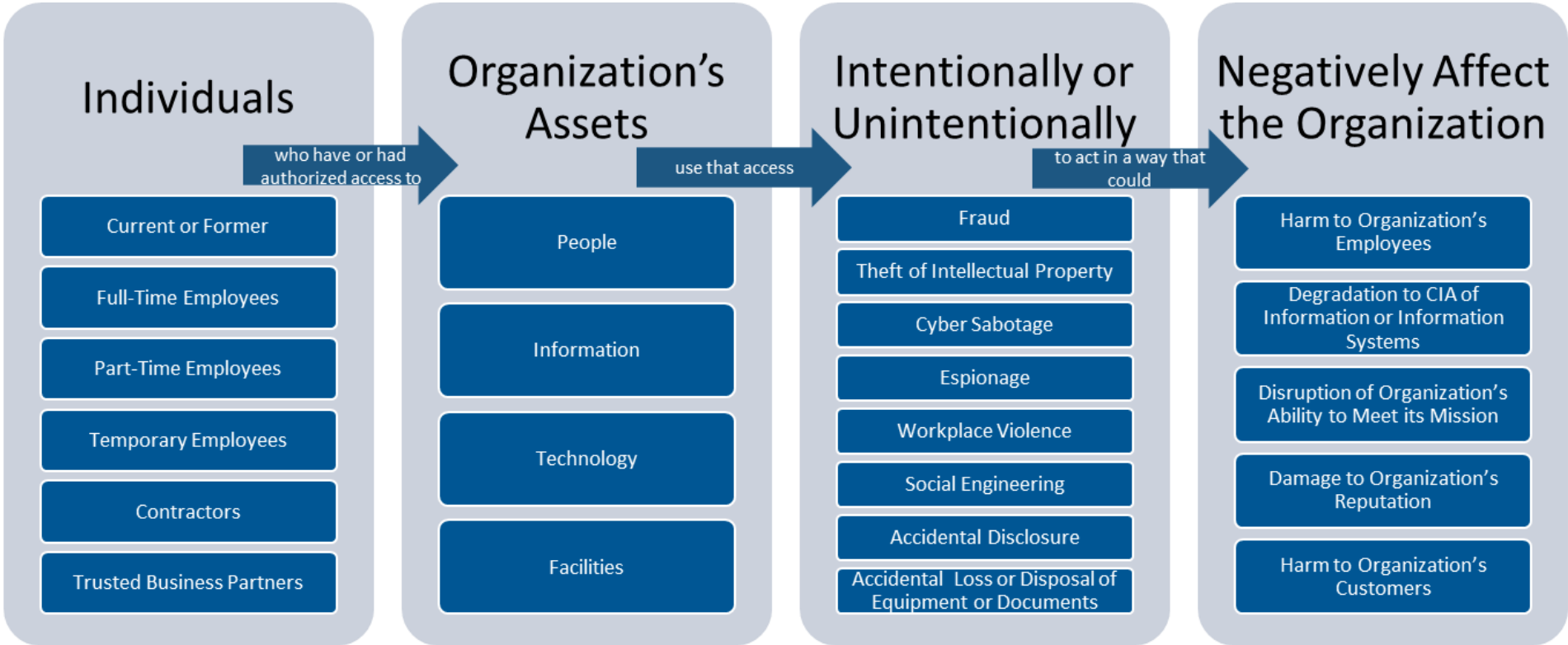
Not Alienate

Insider Threat Program

CERT's Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

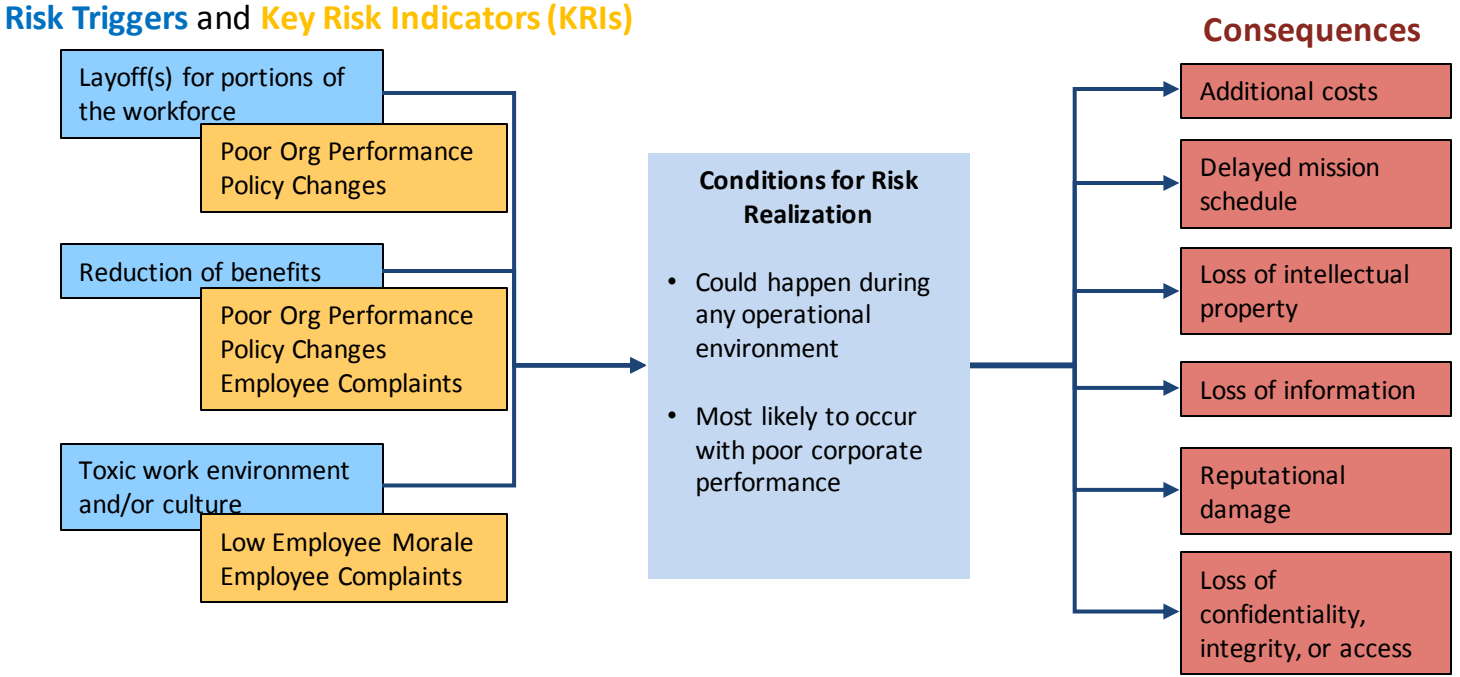
Insider Threat to Critical Assets



Qualifying the Insider Threat Risk

Operations: Insider Driven Disruption

Scope Statement: If the organization suffers a major interruption in operations or impairment from an internal actor, then mission and lives could be jeopardized. Opportunistically, if all malign insider action is avoided, then resources could be saved, reputation could elevate, and mission success could improve.



Ransomware Fundamentals

Threat actors use strong encryption to limit availability of your technology assets.

- Decryption keys may be provided upon payment of a ransom

Ransomware is evolving such that most threat actors do not need to be as technical

Targets vary greatly for both the public and private sectors.

Resource: Midler, O'Meara, Parisi, "Current Ransomware Threats", Software Engineering Institute, Carnegie Mellon University (cmu.edu), 2020.

How Does Ransomware Get In?

Ransomware attackers typically leverage email as a vector for infection

- Exploit failures in email filtering
- Exploit users through opened attachments
- Seek out unpatched systems and other vulnerabilities once enabled

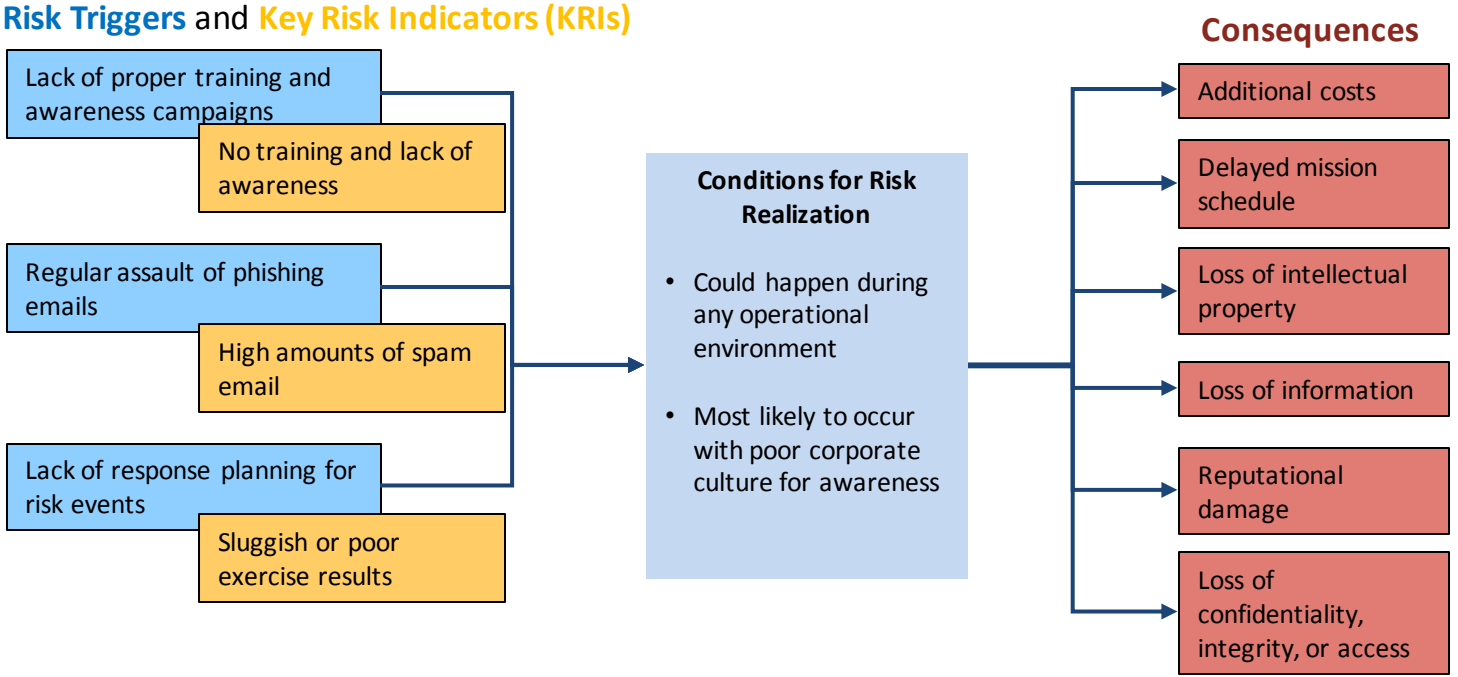
Insiders can be especially dangerous in this regard.

- Exploiting known vulnerabilities
- Do not have to rely upon human failure and lapses of awareness

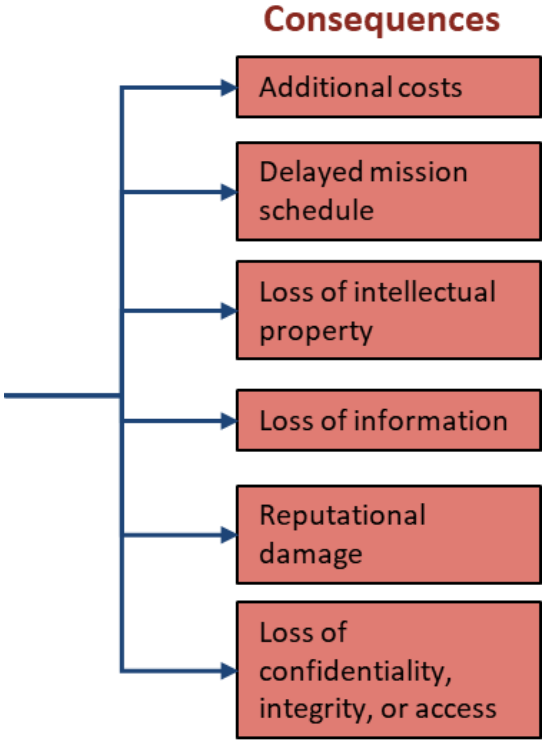
Qualifying Ransomware Risk

Operations: Ransomware Event

Scope Statement: If the organization suffers a major loss of confidentiality, integrity, or availability, then the survival of the organization could be jeopardized. Opportunistically, if ransomware events are avoided, then resources could be saved and reputation could improve.



Seeing the Interdependence of Risks…



Note that the consequences of the insider threat risk and the ransomware risk are alike from these analyses.

Risk managers should exploit these dependencies to reduce efforts in risk response planning.

- Response plans should not automatically assume email threat vectors
- Frequent exercises—tabletop and otherwise—may improve response actions and limit impacts from these consequences
  - Do our back up strategies work?

Getting Ahead of Ransomware

Zero Trust Architectures (ZTA) may help an organization get ahead of both internal and external threat actors.

- Response plans should emphasize Zero Trust principles especially in terms of:
  - Granting access on per session basis
  - Resource access determination with dynamic policy
  - All authentication and authorization is strictly enforced
  - Continuous collection of data and timely update of security posture

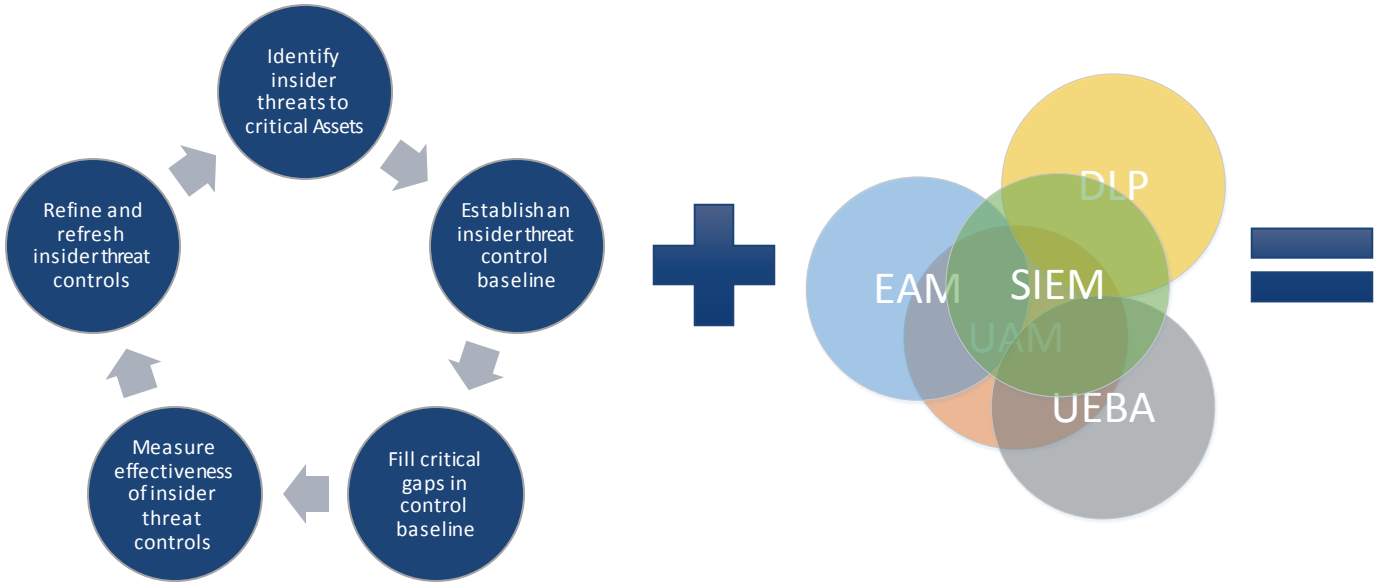
Resource: NIST SP 800-207, SP 800-207, Zero Trust Architecture | CSRC (nist.gov)

Insider Threat Tools Vary in Features and Functions

Insider Threat Tools Vary in Features and Functions

Auditing Host-based Activity	Auditing Network-based Activity	Preventing Data from Leaving Authorized Locations
Preserving Forensic Artifacts	Data Visualization	Rule-Based Alerting
Identity Management / Access Management	Data Correlation / Entity Resolution	Anomaly Detection
Machine Learning	Text Analysis	Risk Scoring
Case / Incident Management	Data Masking / Anonymization	... And More ...

Mitigation Plans to Consider



PROCESS + TOOLS = RESILIENCE

17

Apply What You Have Learned Today

Next week you should:

- Determine the what risk processes are used in your organization
- Identify ownership and state of insider threat management

In the first three months following this presentation you should:

- Understand how risks are managed and who is managing the program
- Apply existing risk management process to insider threat as a use case

Within six months you should:

- Devise response plans to mitigate insider threat and build a business case for necessary resources
- Begin implementation of plan to seek quick wins

Resources and References

- CERT National Insider Threat Center: http://www.cert.org/insider-threat/
- Introduction to OCTAVE Allegro: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
- Podcast for OCTAVE Allegro: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34702
- OCTAVE Version 1.0: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473
- OCTAVE for Smaller Organizations: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795
- US Federal Government, GAO Report on ERM, December 2016: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795
- COSO Direction on Implementing a Cyber Risk Management Framework: https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf
- NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
- ISACA – COBIT 5 Risk Framework: http://www.isaca.org/COBIT/Pages/default.aspx

Any Questions?

Brett Tucker
Telephone: 412.268.6682
Email: batucker@cert.org

Randy Trzeciak
Telephone: 412.268.7040
Email: rft@cert.org