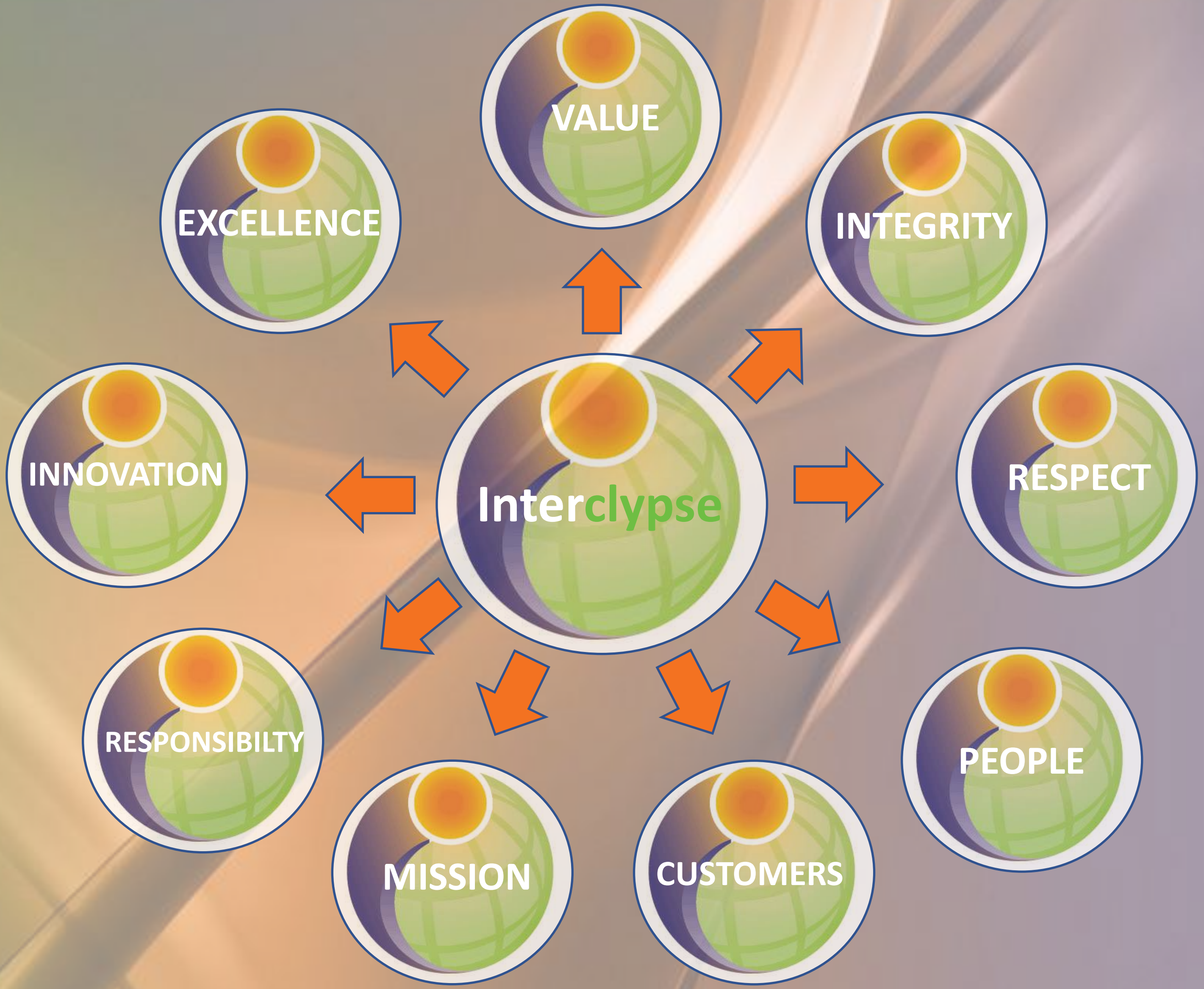
Interclypse

Richard Norwood

Interclypse, Charleston – Division
Senior Engineer / Division Manager

P: 843-608-8221
E: se-sales@interclypse.com



Interclypse

VALUE

INTEGRITY

RESPECT

PEOPLE

CUSTOMERS

MISSION

RESPONSIBILTY

INNOVATION

EXCELLENCE

We are Not Unique

Interclypse

Cyber

CND

Systems Administration

Server Solutions

System Design

Cyber Analytics

CNE

Mission Support

System Implementation

Storage Solutions

Software Engineering

Dev Ops

As A Service

Configuration Management

Data Center Solutions

Management

Agile Development

Highly Configurable

Cloud Migration

Database Solutions

Cloud

Information Assurance

What makes us unique?

Interclypse

Our desire is to be the technical "geeks" behind the scenes to assist our partners to successfully solving their customer needs.

We love supporting our customers as a sub-contractor.

Interface: thing or circumstance that enables separate and sometimes incompatible elements to coordinate effectively.

Eclipse: to make less outstanding or important by comparison; to surpass.

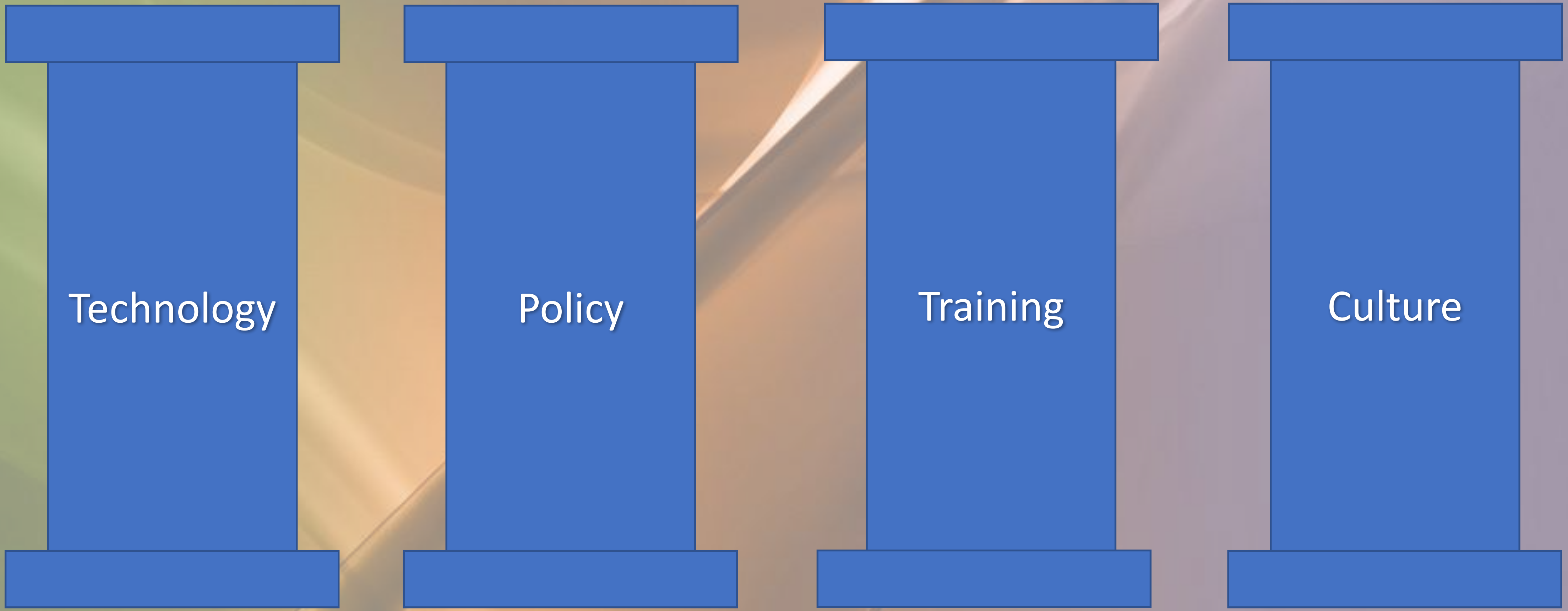
Headline (2016-06) – NSA cases highlights growing concerns over insider threats.

Head Line (2017-08) – Tech giant employee is arrested after he tried to sell secret codes tracking the locations of DEA agents to ‘Mexican drug cartel’ because he didn’t get a raise.

2018 Insider Threat Report
Key Findings

- Ninety percent of organizations feel vulnerable to insider attacks.
- Many organizations say insider threat attack have become more frequent.
- Organizations are shifting their focus on detection of insider threats.
- The most popular technologies to deter are DLP, encryption and identity management.
- A larger majority of organizations already have or are building insider threat programs.

INSIDER THREAT



Technology

Policy

Training

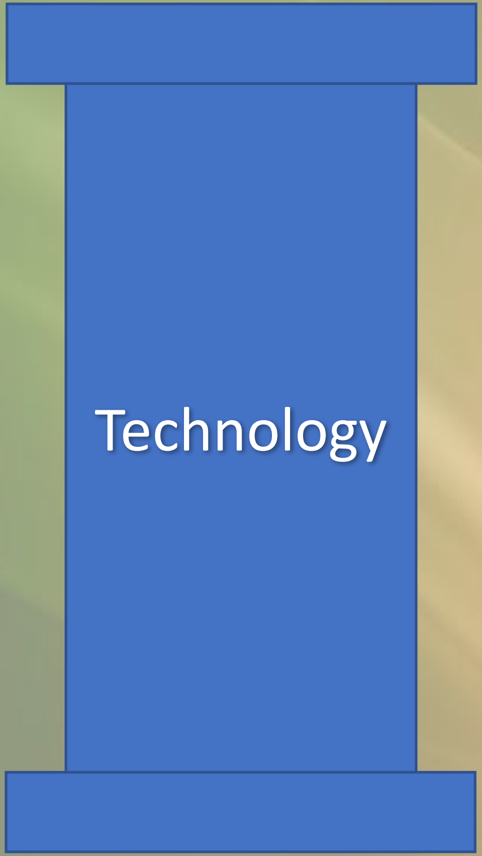
Culture

Common Technologies

Common Technologies

1. Logging and Auditing
2. Key Stroke and Video Monitoring
3. Real Time Incident Awareness
4. Sandboxing – VDI Solutions
5. Configuration Management
6. Role Based Access Control
7. SIEM (Security Incident and Event Management)

Technology: The Security Reality Check

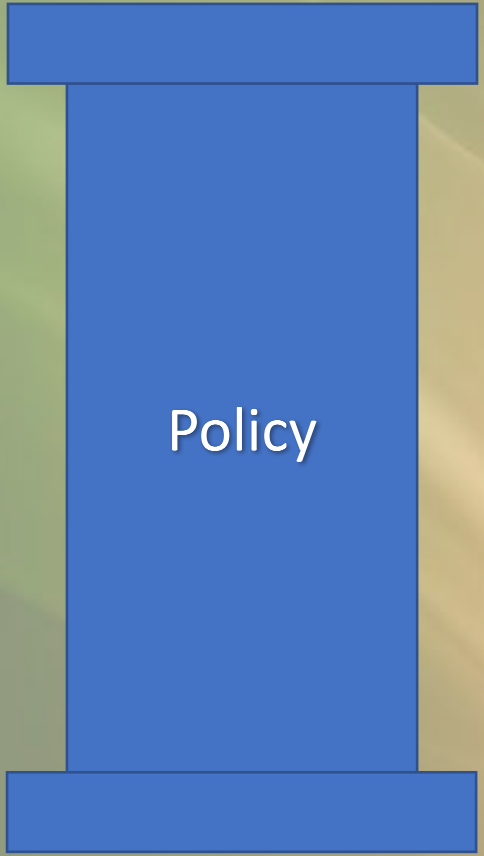


Typical security programs focus on perimeter defenses and are completely ignoring problems that come from the insider threat.

Organizations often underestimate insider threats and the damage they can do.

“The Cloud,” BYOD and remote work are here.

Policy



Used to communicate acceptable user, data and system restrictions.

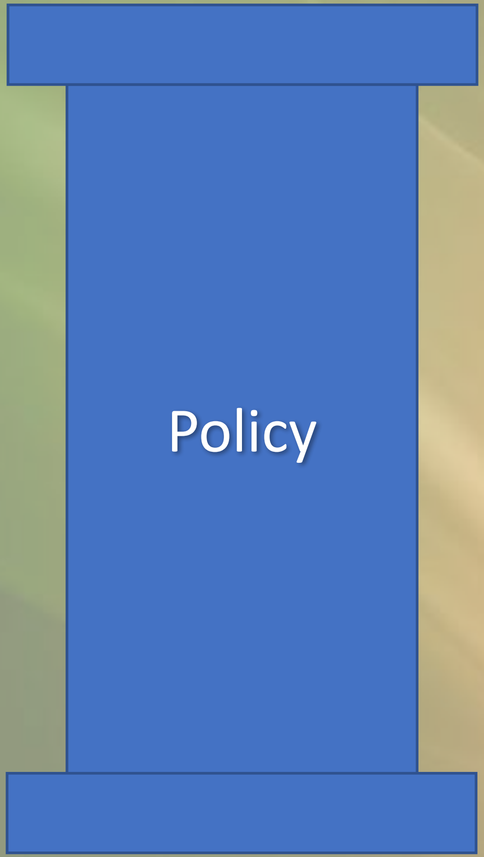
Bridges the gaps between technical controls and solutions.

Define the Threat, Identify Policies, Define the Rules and Policies.

All must comply.

INSIDER THREAT

Policy: Privacy Snafu



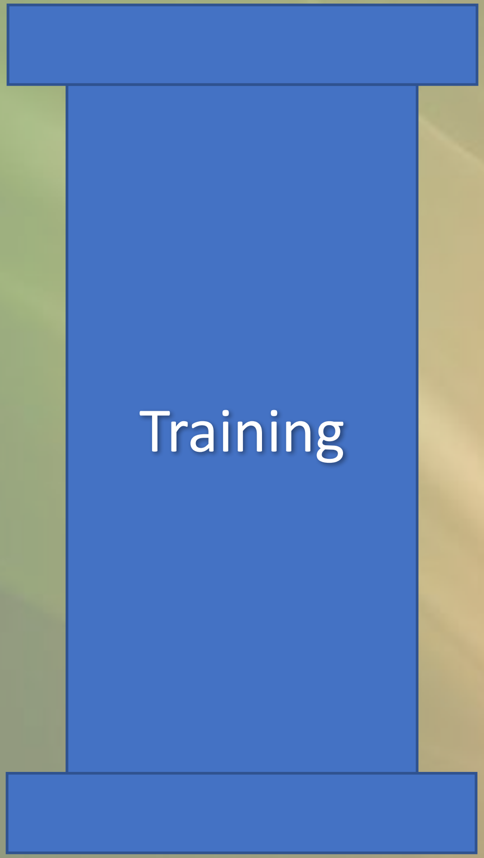
Policy

Article: Thousands of Military Vets' Details Exposed in S3 Privacy Snafu.

Demonstrates the importance to vet and audit at all levels.

Third Party Individuals – Treated just like a normal user.

Training



Training

Benefits

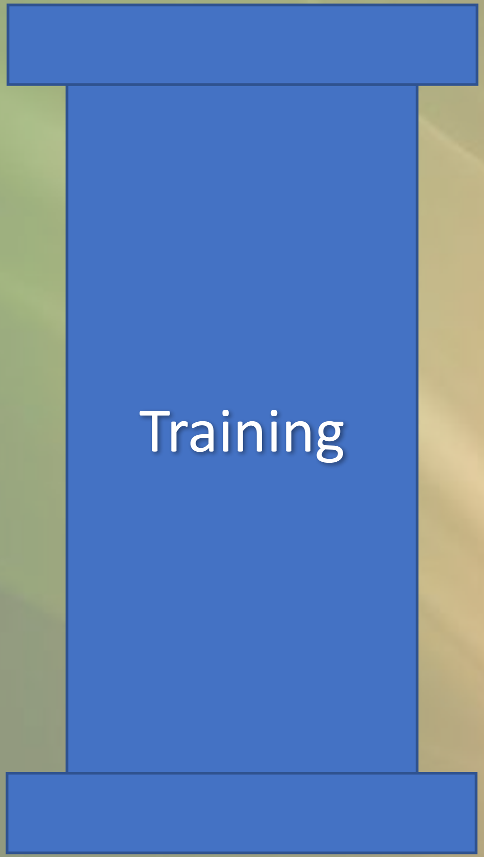
- Increases the understanding of acceptable behavior
- Increases the ability to recognize

Five Key Elements

- Purpose
- Rules
- Description of the Threat
- Examples of the Threat
- Responding to Incidents

INSIDER THREAT

Training: Top Five Signs



Training

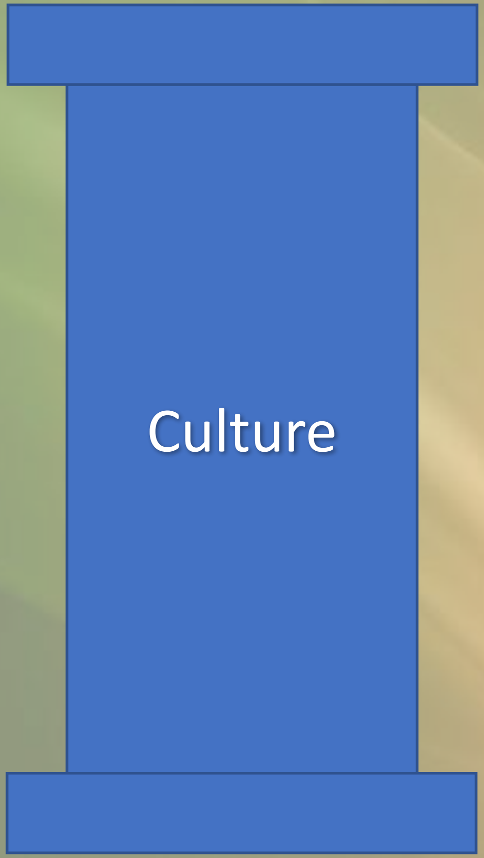
Businesses must remain vigilant to prevent data breaches from occurring within their own organization.

Article: Top 5 signs that your employees are engaging in risky behavior.

Insiders (Malicious, Negligent)

NITTF – National Insider Threat Task Force in the US

Culture



Culture

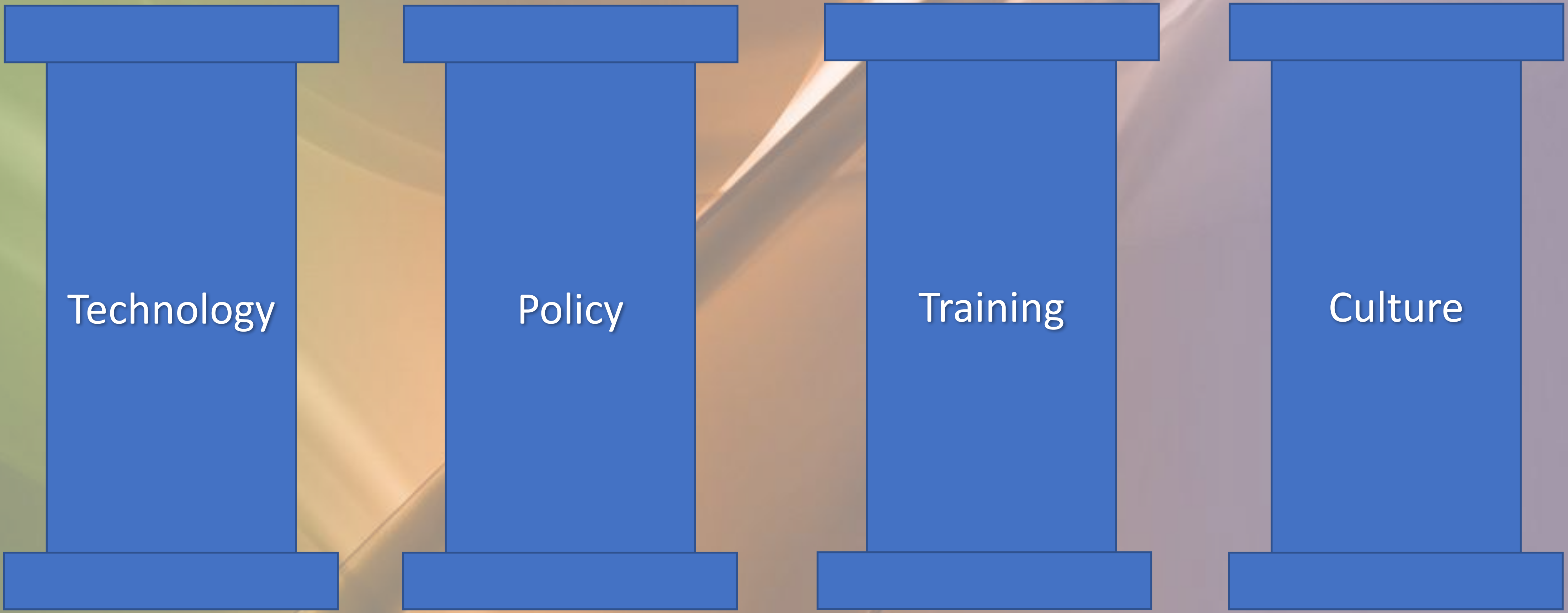
Quote: *"Culture is simply a shared way of doing something with a passion," Brian Chesky, CEO AirBnB*

Culmination of the previous three pillars:

- It uses technology investments
- It uses policy to inform
- It uses training to communicate and grow passion.

Time for a Change: *"Employees should feel comfortable and obligated to report suspected insider threat incidents."*

INSIDER THREAT



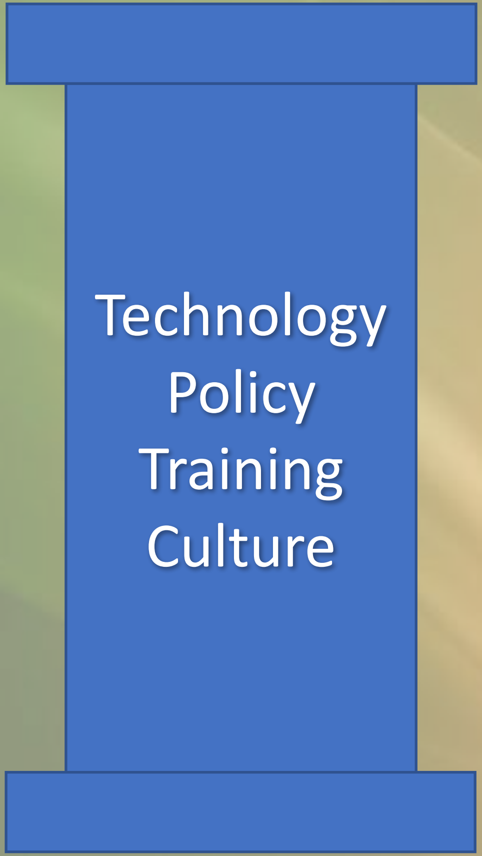
Technology

Policy

Training

Culture

Are You At Risk?



Article: Is your organization at risk from insider threats?

“The reality of IT security today is that insider threats, from members of your organization, are just as potent a threat as those from the outside.”

Insider Threat: Negligence Many Forms

- *Cultural Problem*

Insider Threat: Malicious – A little harder

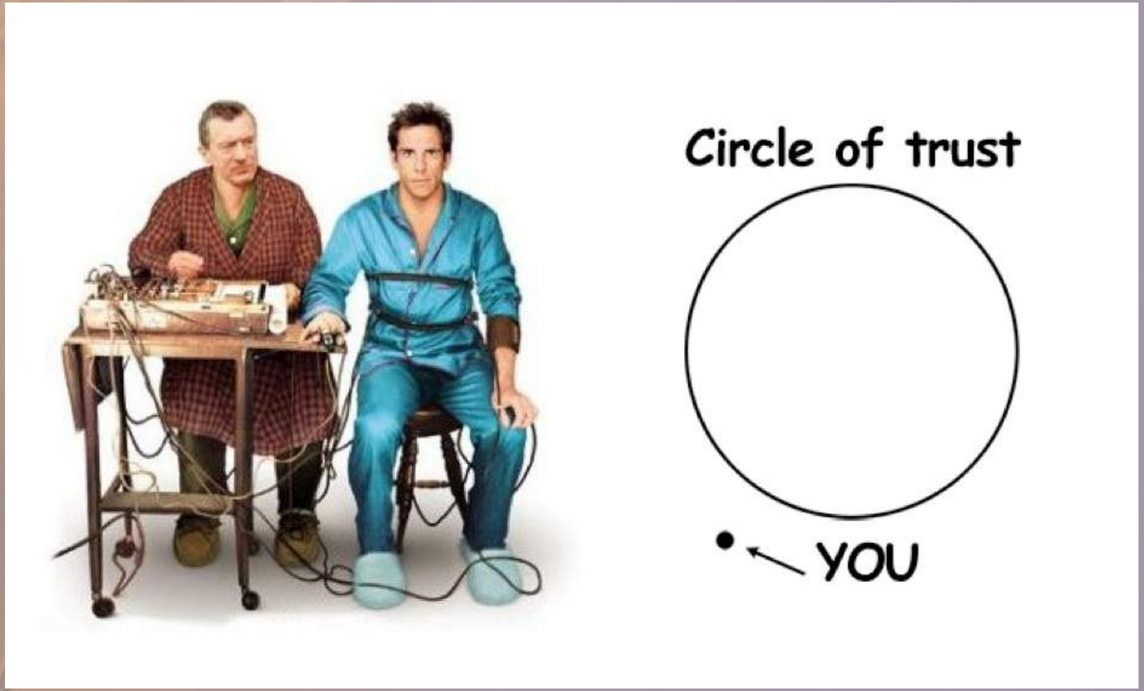
INSIDER THREAT

The Outsider Threat Becomes an Insider Threat

The True Insider Threat

The Outsider Becomes the Insider

Social Engineering Threat



What to do next?

Article: *10 Tips for Reducing Insider Security Threats*

- Established a security incident and response team.
- Make security part of your company culture.
- Perform ongoing risk management
- Use appropriate security software to track and analyze behavior.

- Encrypt confidential information
- Don’t forget to protect your border.

INSIDER THREAT

Correct Focus / Finding a Balance

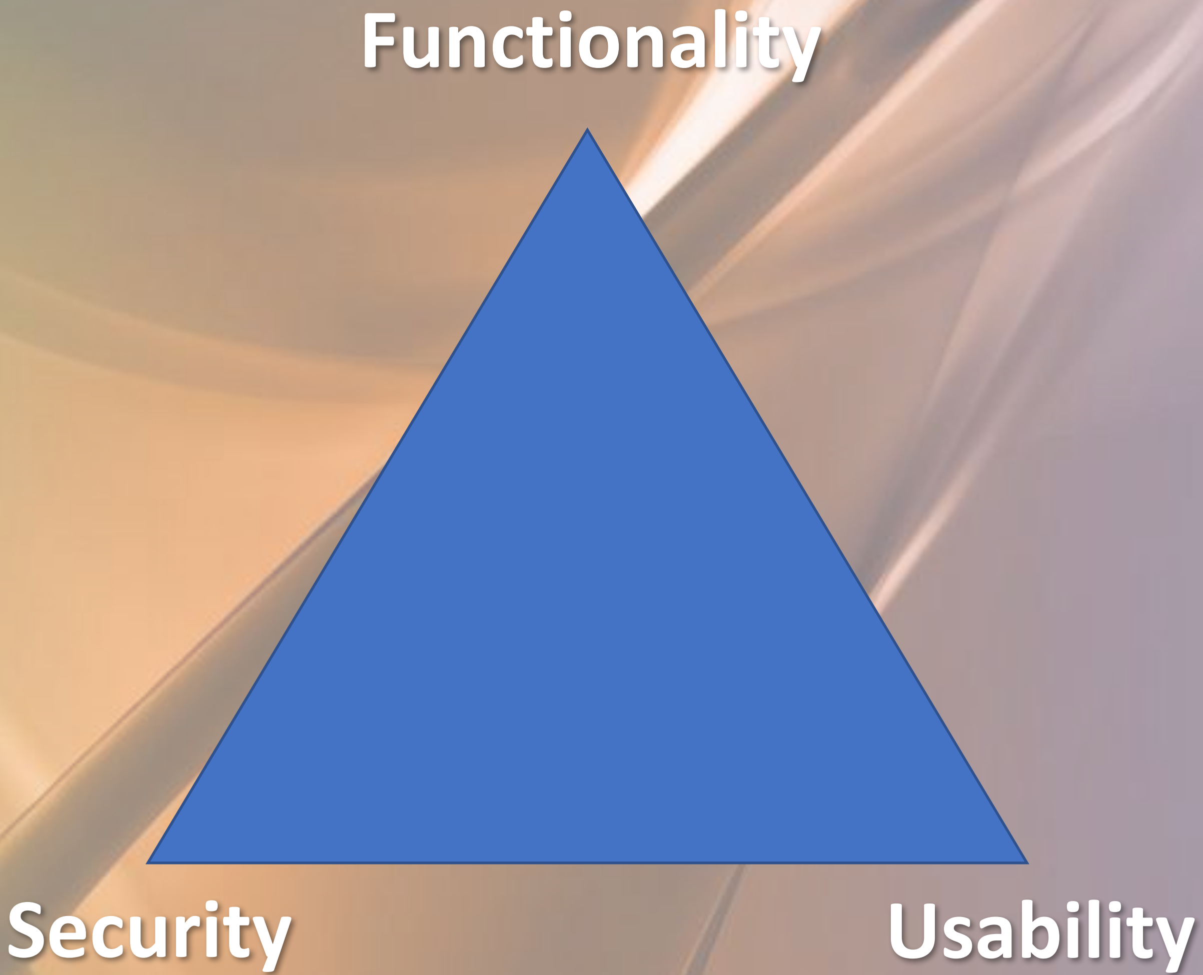
Article: FBI Agent Explains Motivations of Cyber Criminals

Reasons or Types of Attacks

- Hactivism
- Financial Gain
- Insider Threat
- Espionage
- Terrorism

Insiders are not that much different than cyber criminals.

The Triad



Functionality

Security

Usability

ANY
QUESTIONS
?