ETHICS AND BUSINESS CONDUCT
EXCELLENCE THROUGH INTEGRITY

Supply Chain Risk Management

Helping Our Suppliers Manage Ethics and Security Risks

LOCKHEED MARTIN

PIRA #CHQ2023030023

Presenting Today

Rob Barbour

Counterintelligence Lead, ITPSO

David Gebler

Principal, Ethics Engagement

Jonathan Mouzon

Supply Chain Security Manager

Scott Sperling

Lead, Supply Chain Counterintelligence

PIRA #CHQ2023030023

Agenda

- Why Does LM Want to Help Suppliers Manage Risk?
- The Importance of a Security and Insider Threat Program
- The Importance of an Ethics and Compliance Program
- Next Steps: Taking Action to Reduce Risk

Why Does LM Want to Help Suppliers Manage Risk?

LM suppliers may be targeted by adversaries

Emerging Supply Chain Risk Management (SCRM) requirements

Risks to suppliers are risks to LM

PIRA #CHQ2023030023

The Importance of a Security and Insider Threat Program

Counterintelligence

What is it?

- The practice of identifying intelligence threats facing an organization and developing mitigation strategies to counter (address and neutralize) those threats.

Why is it important?

- Trust, Reliability, National Security
- Adversaries are targeting the US Defense sector and global supply base

US Tech

Foreign Clones

DETER – DETECT - MITIGATE

PIRA #CHQ2023030023

External Threats

- Foreign Intelligence Services
- Competitors
- Terrorist Groups
- Extreme Activist Organizations
- Criminal Enterprises

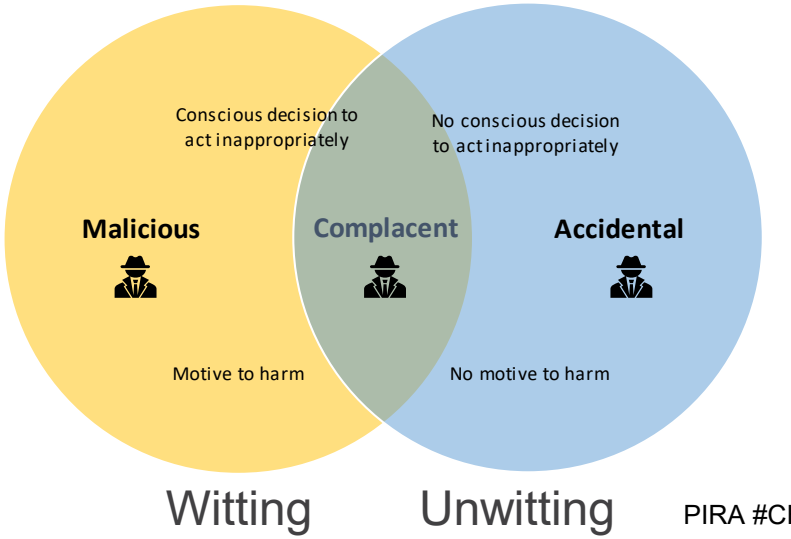
…often targeting insiders (employees)

PIRA #CHQ2023030023

Internal – Insider Threats

An **Insider** is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.

Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.



PIRA #CHQ2023030023

Types of Insiders

Malicious Insiders. These are the real bad guys -- malicious, disgruntled employees who purposely abuse their internal access to wreak havoc. They typically have the knowledge, access, information, and desire needed to bypass existing security solutions to complete their task. Malicious insiders are often the most difficult to detect and the costliest to clean up after.

Complacent Insiders. Most are not malicious but they are dangerous. Employees whose lax approach to policies, procedures, and information security exposes the organization to external risks. It could be the result of lack of oversight and direction, or extreme focus on customer support (mission-itis) at the expense of security procedures.

Accidental/Unknowing Insiders. Employees whose lack of awareness of organizational security policy, procedures, and protocols exposes the organization to external risks.

Motivating Factors

- Greed or financial need; excessive debt or overwhelming expenses
- Frustrations over problems at work; lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff
- Anger or vengeance; disgruntlement to the point of wanting to retaliate against the organization
- Divided loyalties; allegiance to another person or company, or to a country besides the United States
- Thrill or ingratiation; intrigued by the clandestine activity, “James Bond wannabe”
- Ideology; a desire to help the “underdog” or a particular cause
- Vulnerability to blackmail or coercion; extra-marital affairs, gambling, fraud

Targeted Information

- Proprietary Information
- Third Party Proprietary Information
- Marketing strategies
- Investment data
- Business phone and email directories
- Passwords
- Personal Information
- Export Controlled Information
- Computer access protocols
- Acquisition strategies
- Customer data (classified and unclassified)
- Employee data
- Supplier Information
- Pricing strategies
- Proprietary formulas / business processes
- Technical components and plans
- Corporate strategies
- Corporate financials

Anything legitimately NOT publicly available

PIRA #CHQ2023030023

Types of Incidents

Theft
Use of insider access to steal or exploit assets (information, data, products, technology)

Workplace Violence
Use of violence or threats of violence to influence others and impact the health and safety of an organizations workforce

Security Compromise
Use of access to facilitate and override any security countermeasures (incl. physical and cyber)

Espionage
Use of access to obtain sensitive information for exploitation that impacts national or corporate security

Terrorism
Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes

Sabotage
Intentional destruction of equipment or IT to direct specific harm (counterfeits, inserting malicious code, etc)

Supplier Incident
Any incident that could also affect suppliers and impact business (FOCI*, data exfil/spill, insider incident, suspicious contact, etc)

Other
Captures the evolving threat including emerging threats or anything not covered

*FOCI = Foreign Ownership, Control, or Influence

PIRA #CHQ2023030023

The Importance of an Ethics & Compliance Program

Lockheed Martin's Perspective

Many elements of an effective ethics program are required by law or regulation and can reduce penalties in event of misconduct.

Allegations of misconduct can damage the reputation of a single company or the entire industry.

An effective ethics program can help identify and address issues before they affect quality, cost or schedule.

Ethics programs reduce risk to your business and ours – and to the missions we serve.

PIRA #CHQ2023030023

Ethics Statement in our Purchase Orders

…encourages all suppliers to implement an effective ethics program, including adopting a written code of conduct. …both parties are expected to conduct themselves in a manner consistent with the principles expressed in Lockheed Martin's Supplier Code of Conduct…

Compliance with the Supplier Code of Conduct

We expect that all of our suppliers will adhere to the provisions of the Supplier Code of Conduct.

PIRA #CHQ2023030023

What's in the Supplier Code of Conduct?

Bribery & Corruption

Gifts & Business Courtesies

Fair Competition

Conflicts of Interest

Export/ Import

Counterfeit Parts

Human Rights

Protecting Information

Financial Records

Human Trafficking & Child Labor

Non-Discrimination

Conflict Minerals

Environment

Harassment

Drug-Free Workplace

Reporting

Supplier Diversity

Codes of Conduct & Sub-Tier Suppliers

Employee Safety & Health

Could your company use some guidance in meeting these expectations?

PIRA #CHQ2023030023

Our Supplier Ethics Mentoring Program

Why Supplier Mentoring?

ETHICS PROGRAMS REDUCE RISK

COMPONENT OF OUR BUSINESS PARTNERSHIP

- Ethics Statement in all Lockheed Martin purchase orders

ADOPTING EFFECTIVE ETHICS PROGRAM ELEMENTS

- Develop a culture in which employees *feel empowered to speak up* – responding to issues before they negatively impact your business.

SELF-SERVICE RESOURCES

Work 1:1 with a Lockheed Martin Ethics Officer

Take advantage of the free resources available on our Supplier Ethics website

Our 1:1 Mentoring Program

A series of 3-4 meetings with an experienced Lockheed Martin Ethics Officer

1st Meeting: Introduction to the Mentoring Program and the available resources, including the Self-Assessment Tool

2nd Meeting: Discuss where the supplier would like to start in developing or enhancing their program.

3rd and 4th Meetings: Referrals to resources to help the supplier build their program, including evaluation of the Elements of an Effective Program

PIRA #CHQ2023030023

Next Steps: Taking Action to Reduce Risk

Proactive Steps

Implement Physical Security Safeguards

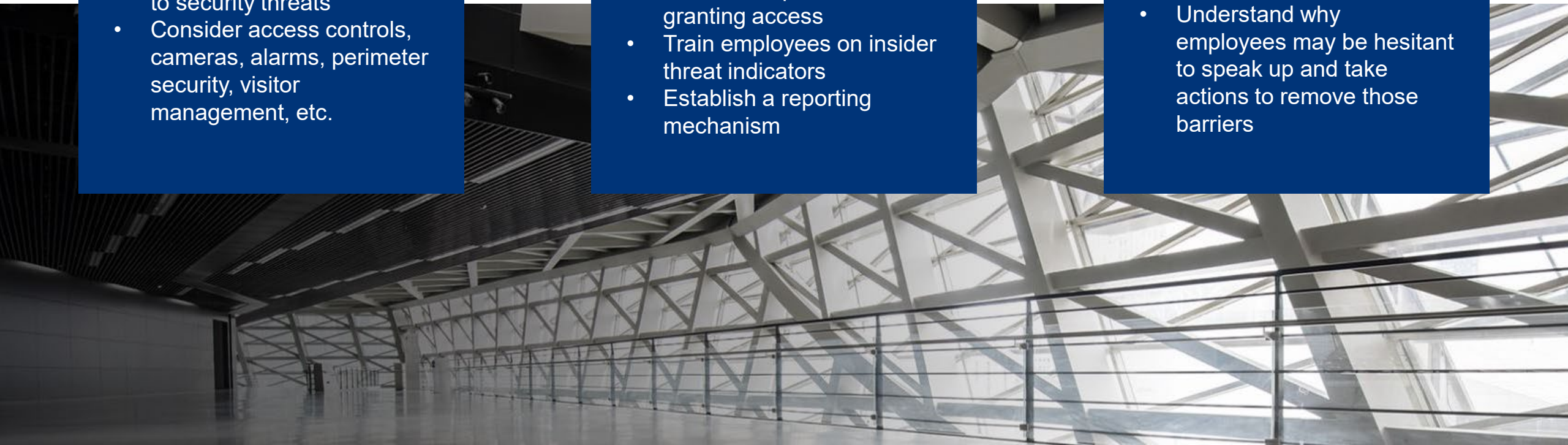
- Safeguards should deter, delay, detect, and respond to security threats
- Consider access controls, cameras, alarms, perimeter security, visitor management, etc.

Build an Insider Threat Program

- Screen employees and contractors prior to granting access
- Train employees on insider threat indicators
- Establish a reporting mechanism

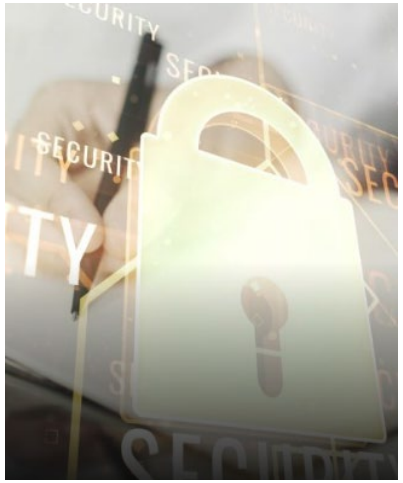
Build an Ethics Program

- Create an environment where employees feel safe to report concerns
- Understand why employees may be hesitant to speak up and take actions to remove those barriers



Ask Lockheed Martin for Help!

Training and Awareness Materials



Supplier Security Liaison Program (SSLP)

Supplier Code of Conduct

Supplier Ethics Mentoring

Partnership Mentality

PIRA #CHQ2023030023