Embracing a Risk Adaptive Approach to Data Protection

Charles Keane, CISSP
Data Protection SME
The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.

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.

Personnel security is a system of policies and procedures which seek to mitigate the risk of workers (insiders) exploiting their legitimate access to an organization's assets for unauthorized purposes.
(https://www.cpni.gov.uk/personnel-and-people-security)
“Erratic”

Who’s to Blame

- People
- Process
- Technology
# The Insider Risk Landscape

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Attack</th>
<th>Actor</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Fraud</td>
<td>Misuse of access</td>
<td>Employee</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Information system</td>
<td>Theft</td>
<td>Defense bypass</td>
<td>Former employee</td>
<td>Integrity</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>Sabotage</td>
<td>Control failure</td>
<td>Contractor</td>
<td>Availability</td>
</tr>
<tr>
<td>Sensitive data</td>
<td>Violence</td>
<td></td>
<td>Subcontractor</td>
<td>Reputation</td>
</tr>
<tr>
<td>Facilities</td>
<td>Disruption</td>
<td></td>
<td>Supplier</td>
<td>Competitive edge</td>
</tr>
<tr>
<td>Resources</td>
<td></td>
<td></td>
<td>Trusted partner</td>
<td>Financial</td>
</tr>
</tbody>
</table>

- **Asset**: People, Information system, Intellectual property, Sensitive data, Facilities, Resources
- **Threat**: Fraud, Theft, Sabotage, Violence, Disruption
- **Attack**: Misuse of access, Defense bypass, Control failure
- **Actor**: Employee, Former employee, Contractor, Subcontractor, Supplier, Trusted partner
- **Impact**: Confidentiality, Integrity, Availability, Reputation, Competitive edge, Financial
The World Changes... But There Are Two Constants

People

Data (IP)

Value
- Revenue growth
- Consumer Confidence
- Reputation

Risk
- Theft/Loss
- Damage
- Misuse
Security As A Business Value Enabler

Security

Freedom from Harm
Resilience against Coercive change

By Protecting

Company Customers People IP

To Achieve

Business Growth

Revenue Market Share Demand
The Holistic Program

- User Activity Monitoring
- Policies, Procedures, & Practices
- Confidential Reporting
- Enterprise Risk Management
- Organization-wide Participation
- Communications
- Formal Program
- Training & Awareness
- Technical Controls
- Governance & Oversight
- Protection of Civil Liberties & Rights
- Response Plan
Security Governance

Board of Directors
- COO
- CRO
- CHR
- CC

Executive Sponsors
- Approves program scope & budget
- Provides forum for stakeholder equities which can influence direction & budget

Risk Committee
- Validates support to security posture
- Looks for efficiencies
- Last gate before C-suite

Insider Threat Steering Group
- Defines Program
- Secures buy-in up and down hierarchy
- Ensures program objectives satisfy broader conduct risk remit
- Can influence budget and headcount

Insider Threat Team
- Operationalizes program
- May/May-not be enduring

Insider Threat Working Groups
- Data
- Legal
- Technology
- Analysis, response procedures, process

Compliance, Risk, HR, Legal, CISO, CSO, Oversight & Controls, Business Units
Primary Objective

Identify risk at the earliest point of detection to prevent or mitigate exposure.

Mission

Move to a more proactive security posture by:

• Increasing situational awareness through context and intent
• Developing a cross-functional/stakeholder security strategy
Essential Elements

Collect Wide & Deep For Holistic Visibility

Analyze & Model To Understand Intent

Take Action & Reduce Exposure

DATA SOURCES → ANALYTIC ENGINE → INFORMED NARRATIVE

- Email
- Voice
- Chat
- File

Specialist Communication Analytics - Context & Meta
Entity Risk Detection & Progression

1. Identify Threats
2. Control Exposure
3. Remediate

Analyzable Data Model for Informed Narrative - Visualizations
Collect Wide & Deep For Holistic Visibility

- Use logs from existing security stack such as DLP, NGFW, EDR, SIEM, IAM, PAM, Proxy, IDS, Endpoint
- Additional value from security investments

- Leverage your entire IT ecosystem to improve security using data from printers, chat, email, voice, HR, badge reader, AD/LDAP, travel, to name a few
- Wide visibility from structured and unstructured sources

- System Info, Clipboard, File Manipulation, Logon, DVR, Running Processes, Registry Modification, Keystrokes
- Deep visibility of machine and user observables
Analyze & Model For Insights

**DATA SOURCES**
- EMAIL
- VOICE
- CHAT
- NETWORK
- ENDPOINTS
- IDENTITY
- PHYSICAL ACCESS
- HR DATA
- 3RD PARTY FEEDS

**ANALYTIC ENGINE**
- Pattern Recognition
- Outlier Detection
- Sentiment Analysis

**INFORMED NARRATIVE**
1. Patterns Change
2. Complains Frequently
3. Sends Many Emails at Night
4. Prints Out Confidential Files

Understand Intent Through Deep Context
Take Action & Reduce Exposure

UPDATE ENFORCEMENT

INVESTIGATE
Thank you

charles.keane@forcepoint.com