Embracing a Risk Adaptive Approach to Data Protection

Charles Keane, CISSP

Data Protection SME

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

The Insider?

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. (https://www.insaonline.org/wp-content/uploads/2018/10/INSA_InsiderThreat_definition-Flyer.pdf)

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. (https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html)

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

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



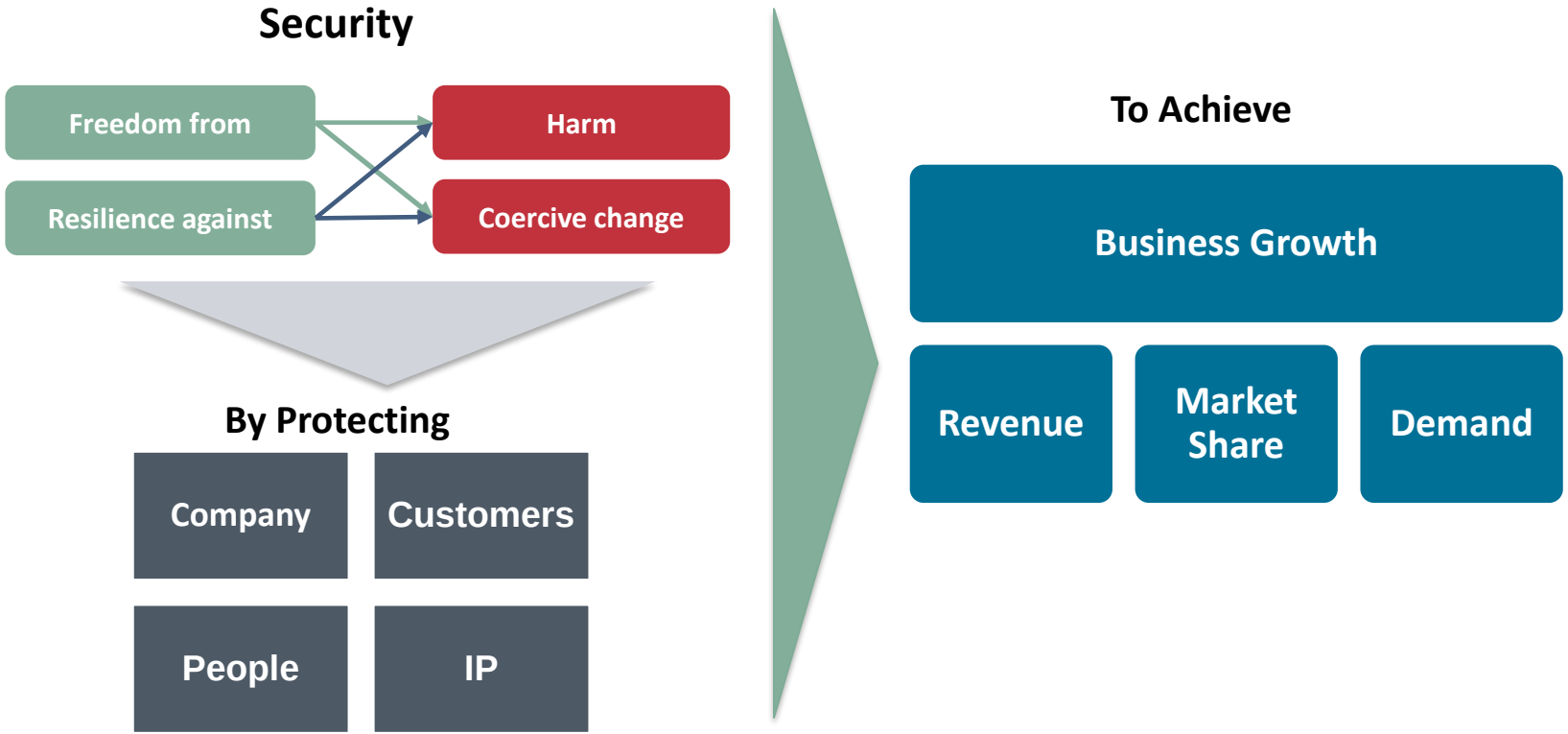


The World Changes… But There Are Two Constants

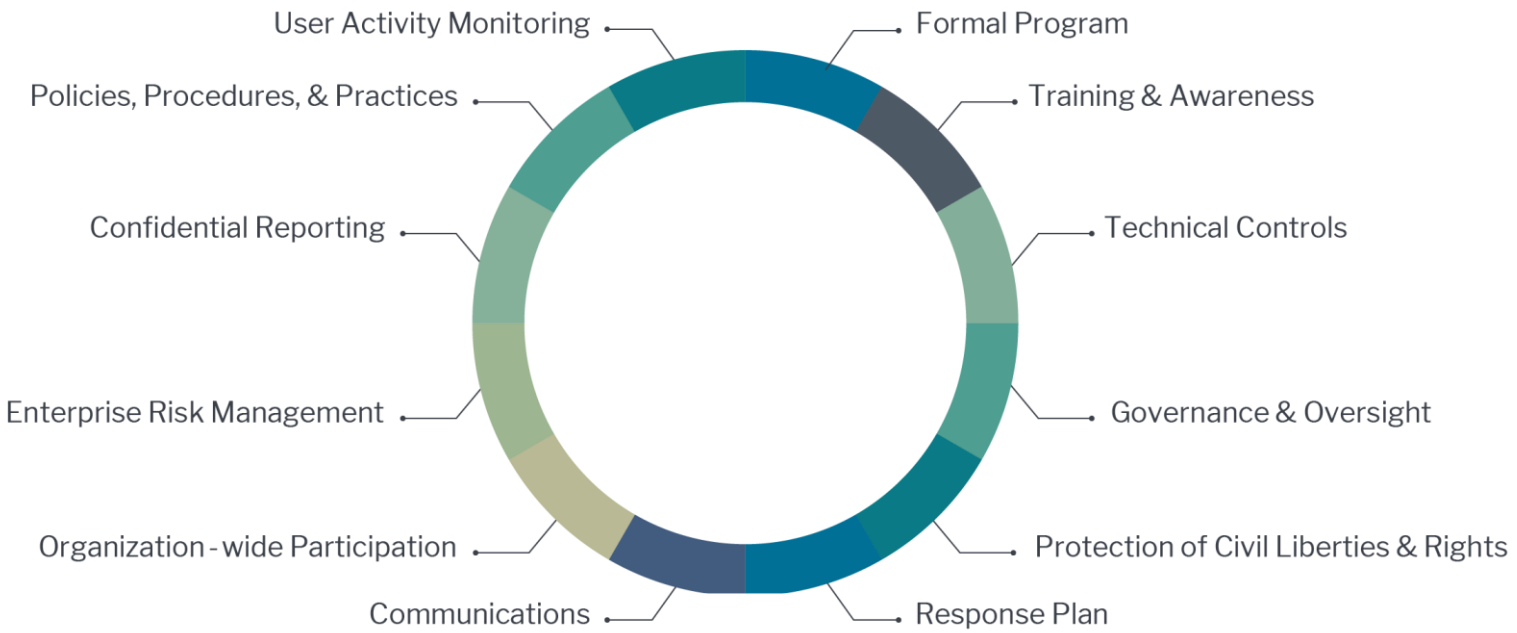
People

Data (IP)

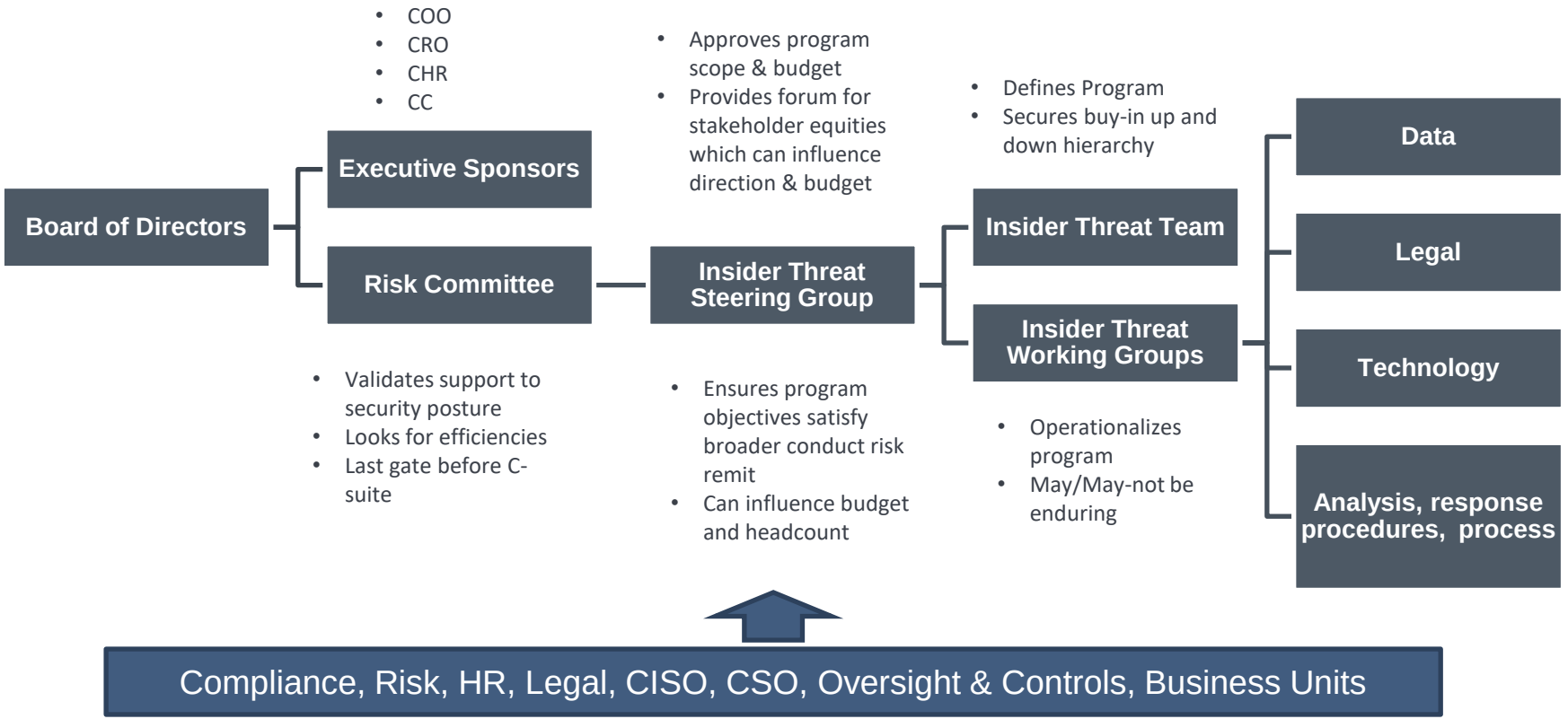
Security As A Business Value Enabler



The Holistic Program



Security Governance



Mission

Move to a more proactive security posture by:

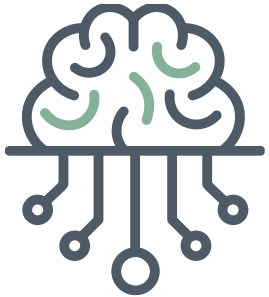
- Increasing situational awareness through context and intent
- Developing a cross-functional/stakeholder security strategy

Primary Objective

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

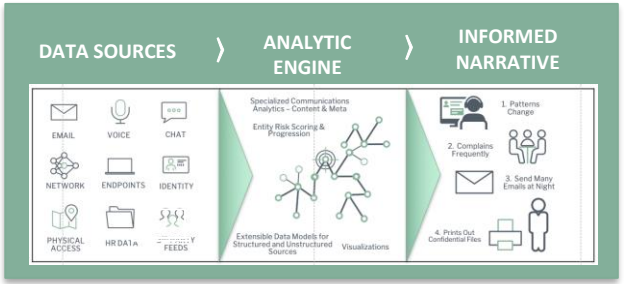
Essential Elements

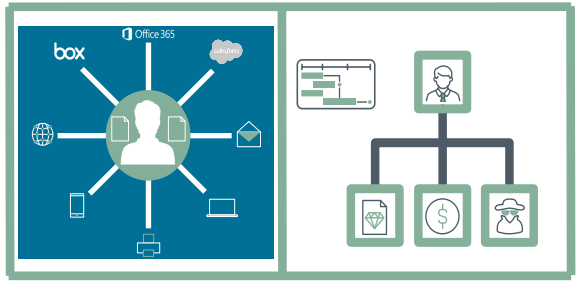
Collect Wide & Deep For Holistic Visibility



Analyze & Model To Understand Intent

Take Action & Reduce Exposure

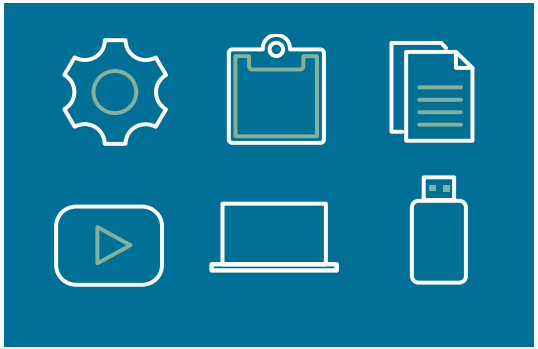




Collect Wide & Deep For Holistic Visibility

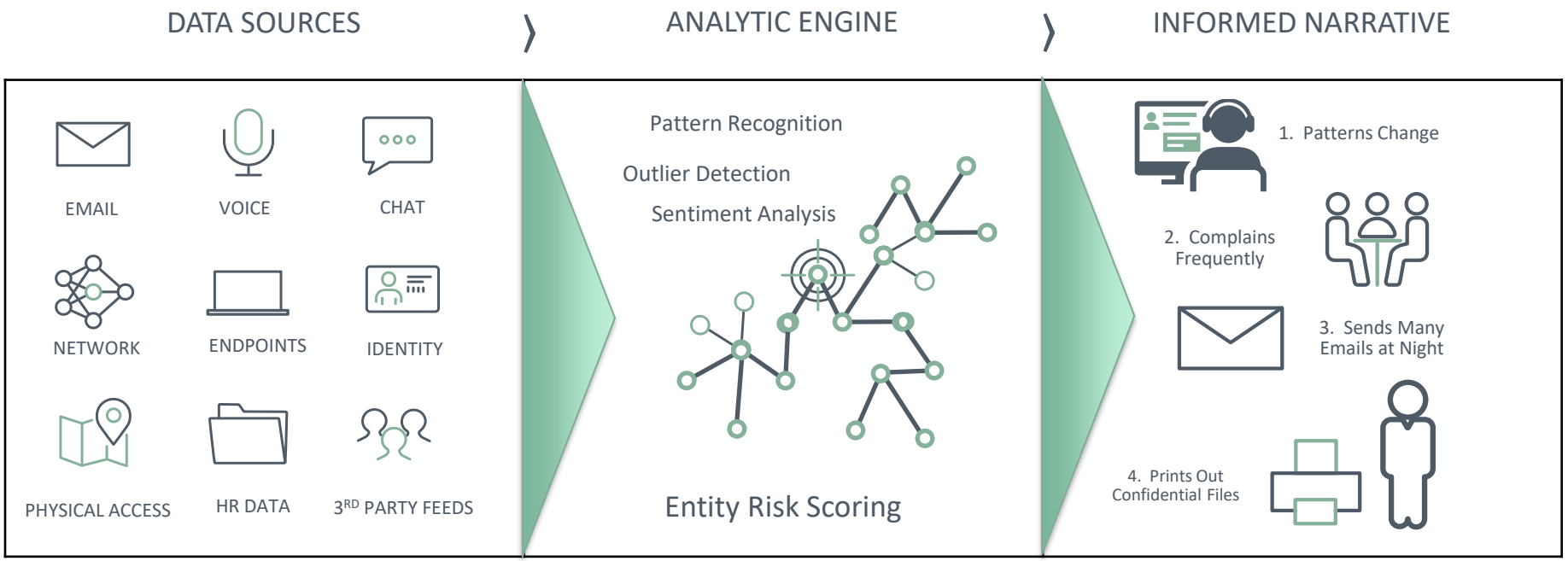
- Use logs from existing security stack such as DLP, NGFW, EDR, SIEM, IAM, PAM, Proxy, IDS, Endpoint
- Additional value from security investments

- 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

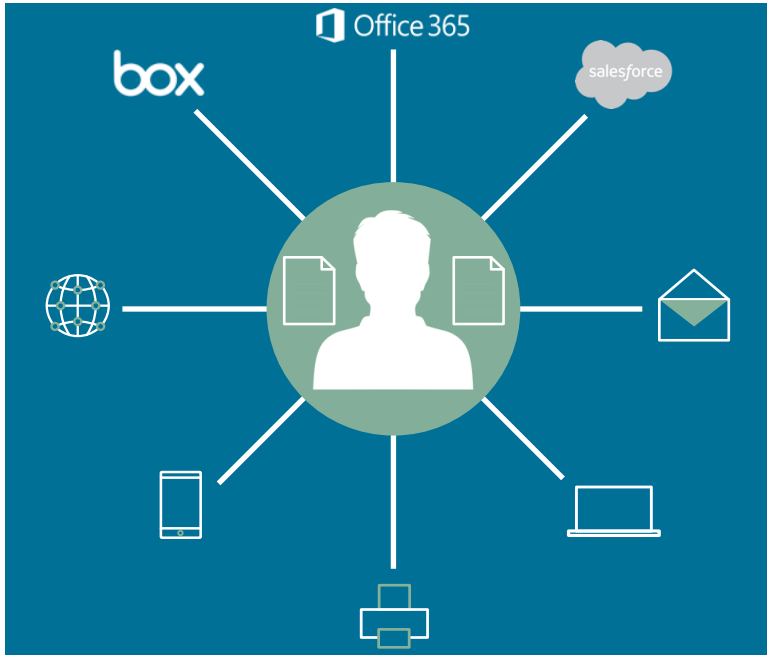
Analyze & Model For Insights



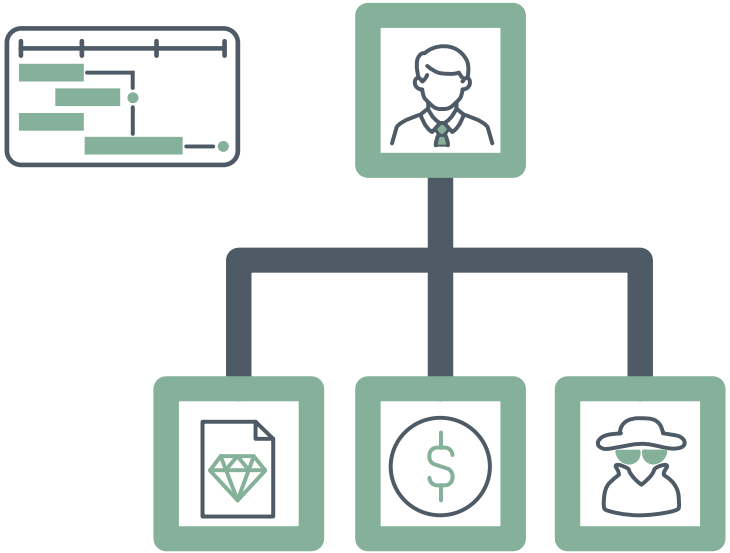
Understand Intent Through Deep Context

Take Action & Reduce Exposure

UPDATE ENFORCEMENT



INVESTIGATE



Thank you

charles.keane@forcepoint.com