Key capabilities of today’s Cyber Bounty Hunter

Renault Ross CISSP,MCSE,VCP5,CHSS

- Distinguished Engineer | Chief Security Business Strategist

THE DOG

CYBER
WARRIOR
Information Technology World
EfenDi 2007
Cyber-Warrior TIM

The Cyber Skills Gap

> *By 2020, security industry will be shortage of millions of information security professionals, with this shortage interestingly cited by half of cyber-security staff as a key reason for data breaches (48%).*

-(ISC)²

Today's Threat landscape is Increasingly More Challenging

General Breach and Cyber-Threat Trends

429M

Records comprised

400M

Unique malware

$158

Cost per record

8.8M

Ransomware

Education Institutions are breaking records in data breaches

UNIVERSITY OF MARYLAND 18 56

300 000

Student, Faculty and Staff records compromised

BUTLER UNIVERSITY INDIANAPOLIS 1855

200 000

Student, Faculty and Staff record exposed

NORTH DAKOTA

300 000

Student, Faculty and Staff records hacked

SIGILLUM UNIVERSITATIS INDIANENSIS LUX ET VERITAS MDCCCXX

146 000

Student, Faculty and Staff record exposed

Source:
The Huffington Post

These Key Trends Pose Security Challenges EdU Already faces today

48%

of incidents involved a malicious or criminal attack

25%

caused by negligent employees or contractors

27%

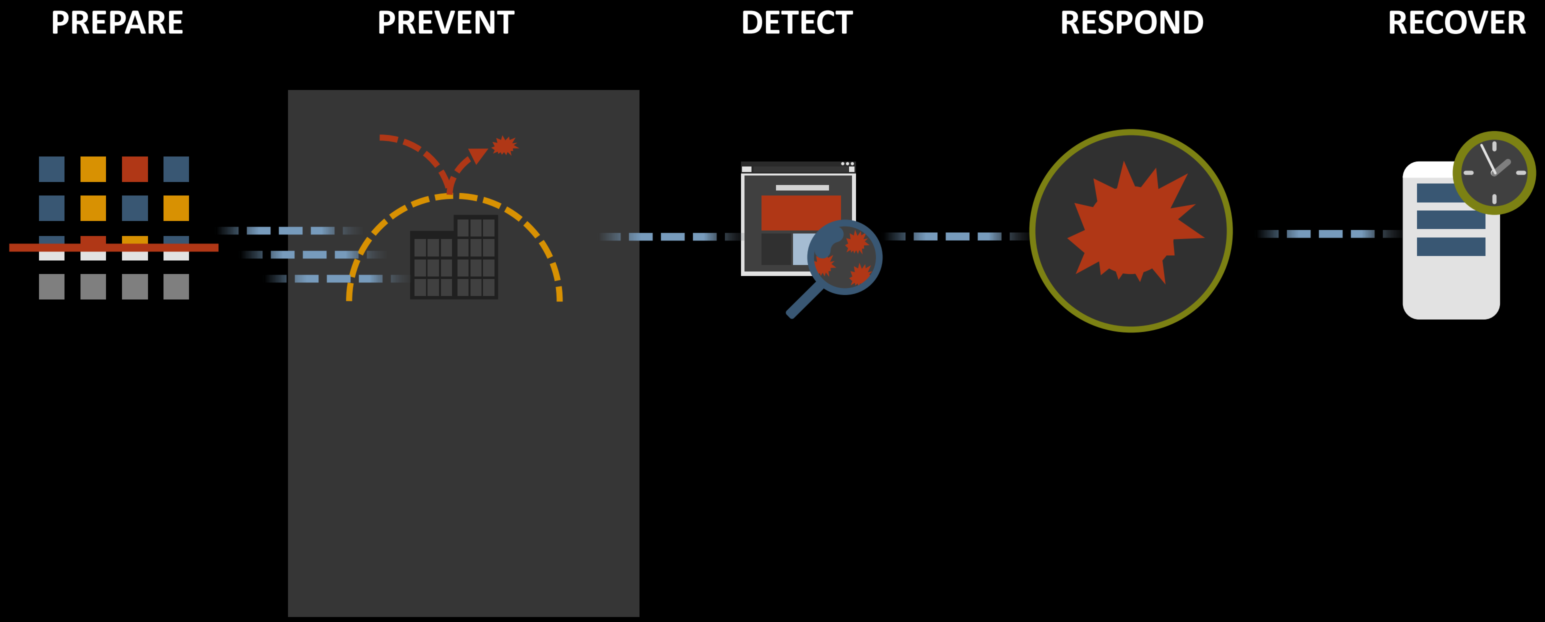
involve system glitches

Top 7 Education Security Challenges

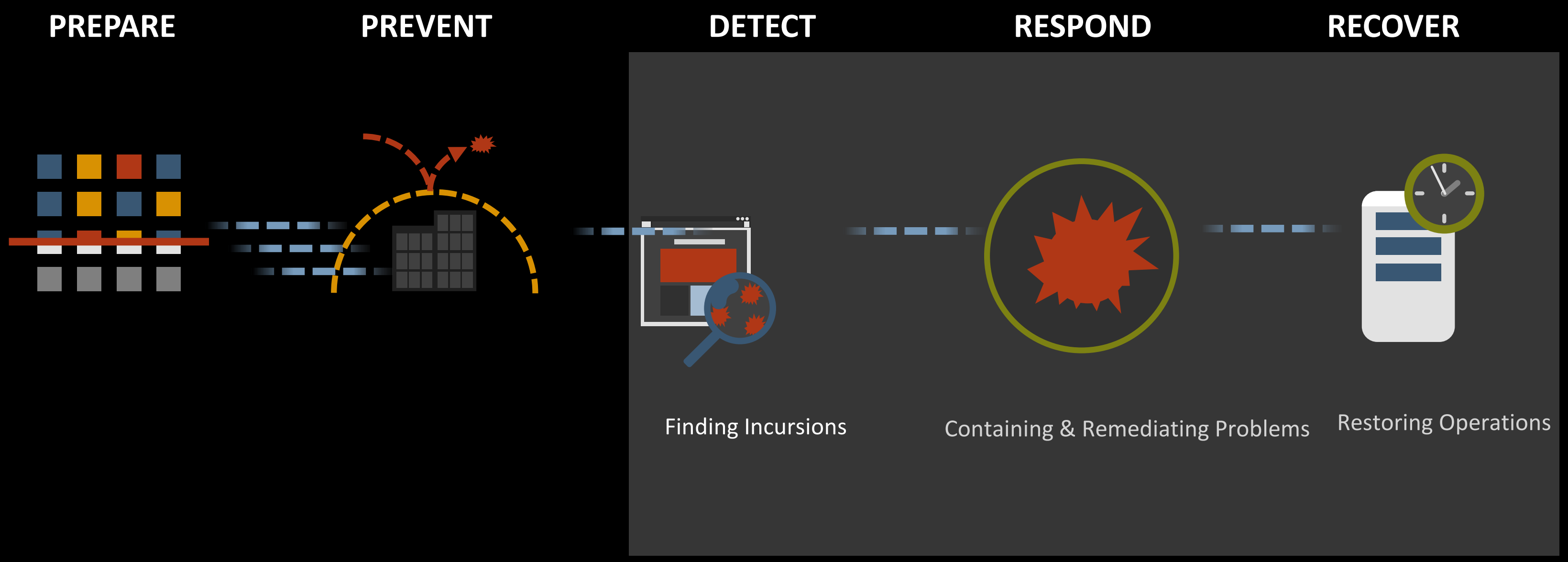
1. Phishing and Ransomware
2. Cloud Security
3. Identity and access Management/P2P
4. Governance over data security
5. Unsecure personal devices
6. Social Network Targeting
7. Next-Gen security platform

Source:2016 Ponemon Institute Research Report
Verizon 2016 Data Breach Investigation Report

CAN YOU STOP ALL THREATS?



DETECTING, RESPONDING & RECOVERING IS THE KEY!



ENTERPRISE TOOLKIT

1 Planning & Strategy

2 Stakeholder Requirement

3 Technologies / Security Controls

4 Communicate Risk in Business Terms

What are you measuring against?

KRIs – Key Risk Indicators

MTTR – Mean Time To Resolution

MTBI – Mean Time Between Incidents

Actionable Intelligence

IOCs – Indicator of Compromise

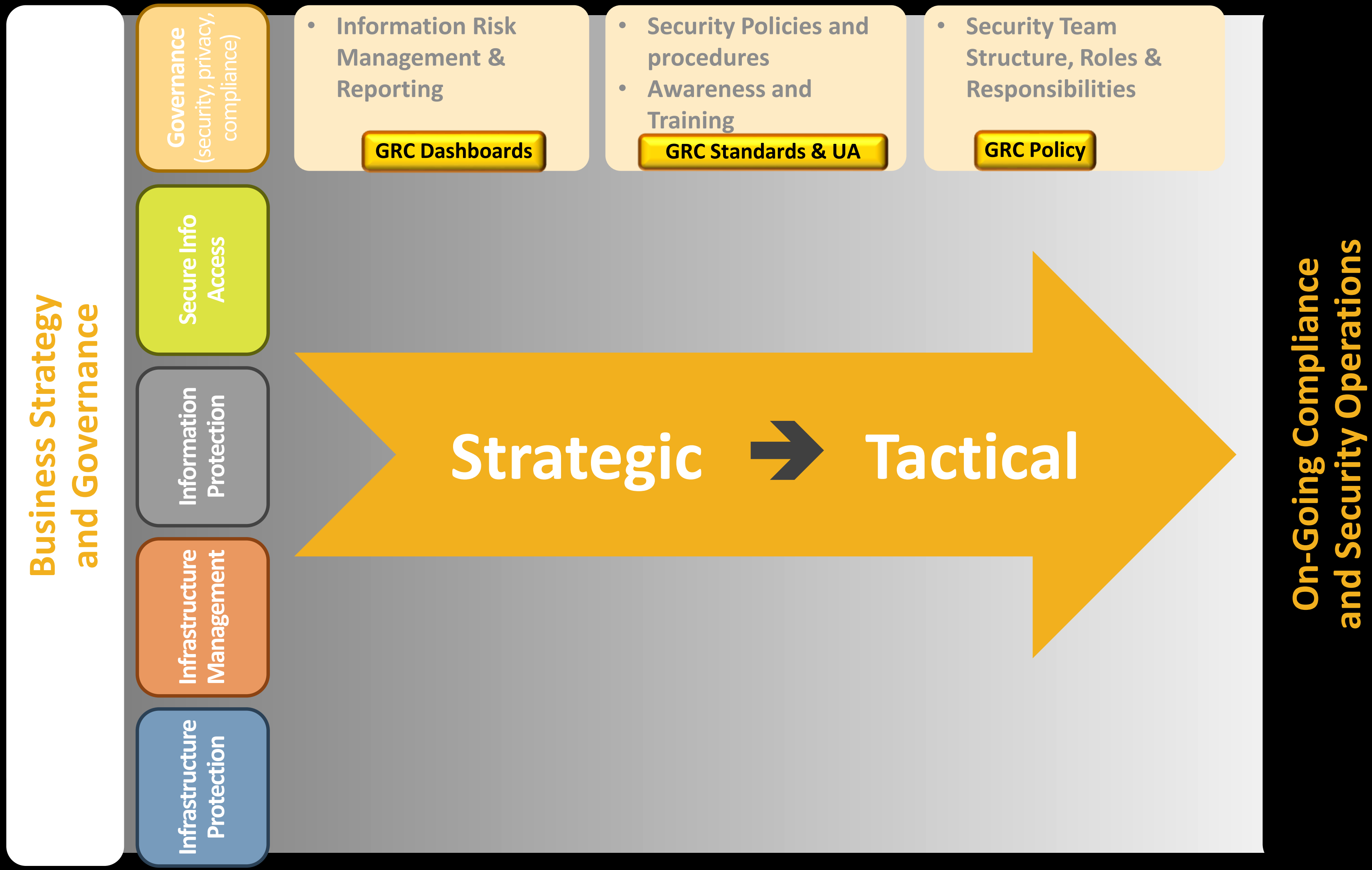
UBA – User Behavioral Analytics

Five Key Principles Security

	Key Capabilities	*Technologies*
Governance (security, privacy, compliance)	• Information Governance • Management Dashboard • Risk Mgmt. & Compliance • Audit & Reporting	**GRC** • Policy Management • Standards Management • Vendor Management
Secure Information Access	• ID Mgmt. & Protection • Authentication • Access Management • Usage & Activity	**Trust Services** • Two factor & MPKI • Assurance Authentication (LOA3) • Cloud Gateway
Information Protection	• Cloud • Endpoint & Mobile • Email & Messaging • Storage	**Data Protection** • Data Loss Prevention • Data Classification • Encryption
Infrastructure Management	• Inventory • Deployment & Patching • Asset Management • Contracts & Licenses	**Operational Management** • IT System Management • Asset & Deployment • Workspace Streaming
Infrastructure Protection & Security	• Security Management • Infrastructure Protection • Threat Intelligence • Security Analytics	**Advance Threat Protection & Cyber Security Services** • Gateway (ATP, email & web) • Endpoint w/ EDR • MSS, IR & Cyber-Simulation

ENTERPRISE TOOLKIT: A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations

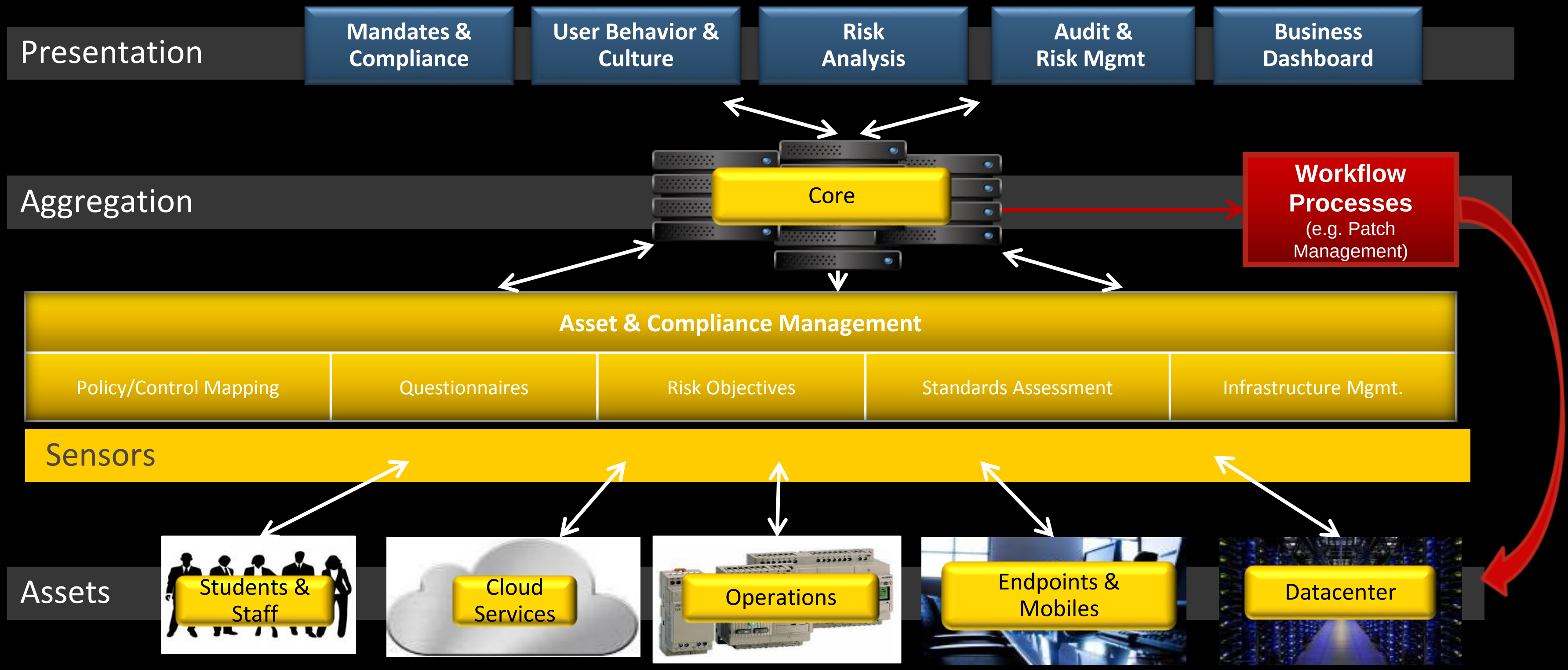

Business Strategy and Governance
Governance (security, privacy, compliance)
Secure Info Access
Information Protection
Infrastructure Management
Infrastructure Protection
GRC Dashboards
GRC Standards & UA
GRC Policy
Strategic ➔ Tactical
On-Going Compliance and Security Operations

- Information Risk Management & Reporting

- Security Policies and procedures
- Awareness and Training

- Security Team Structure, Roles & Responsibilities

Use Case: EDU Governance & Compliance Strategy



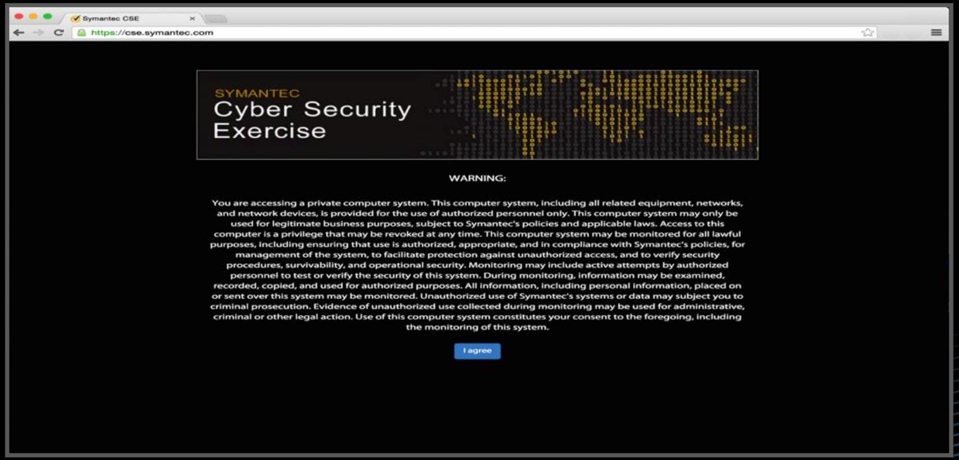
Security Awareness

Create campus-wide security literacy

- Role-based training approach
- Engaging and relevant topics
- Meet compliance mandates
- Regular content refresh
- Unique quizzing methodology

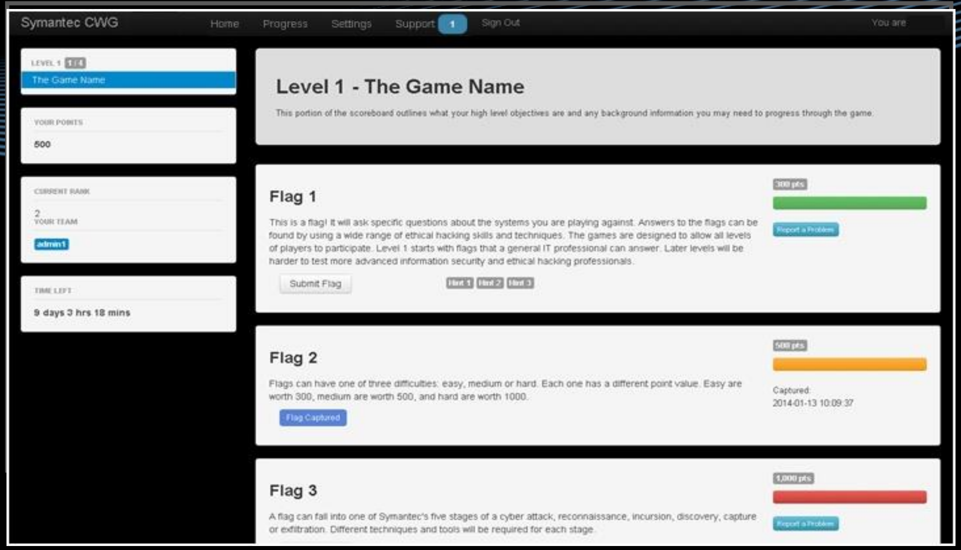
Cyber Security Exercise

Continuous skills development for Security Teams



WARNING:

You are accessing a private computer system. This computer system, including all related equipment, networks, and network devices, is provided for the use of authorized personnel only. This computer system may only be used for legitimate business purposes, subject to Symantec's policies and applicable laws. Access to this computer is a privilege that may be revoked at any time. This computer system may be monitored for all lawful purposes, including ensuring that use is authorized, appropriate, and in compliance with Symantec's policies, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring may include active attempts by authorized personnel to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Unauthorized use of Symantec's systems or data may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other legal action. Use of this computer system constitutes your consent to the foregoing, including the monitoring of this system.



YOUR POINTS: 500

CURRENT RANK: 2

YOUR TEAM: admin1

TIME LEFT: 9 days 3 hrs 18 mins

Level 1 - The Game Name

This portion of the scoreboard outlines what your high level objectives are and any background information you may need to progress through the game.

Flag 1 — 300 pts

This is a flag! It will ask specific questions about the systems you are playing against. Answers to the flags can be found by using a wide range of ethical hacking skills and techniques. The games are designed to allow all levels of players to participate. Level 1 starts with flags that a general IT professional can answer. Later levels will be harder to test more advanced information security and ethical hacking professionals.

Flag 2 — 500 pts

Flags can have one of three difficulties: easy, medium or hard. Each one has a different point value. Easy are worth 300, medium are worth 500, and hard are worth 1000.

Captured: 2014-01-13 10:09:37

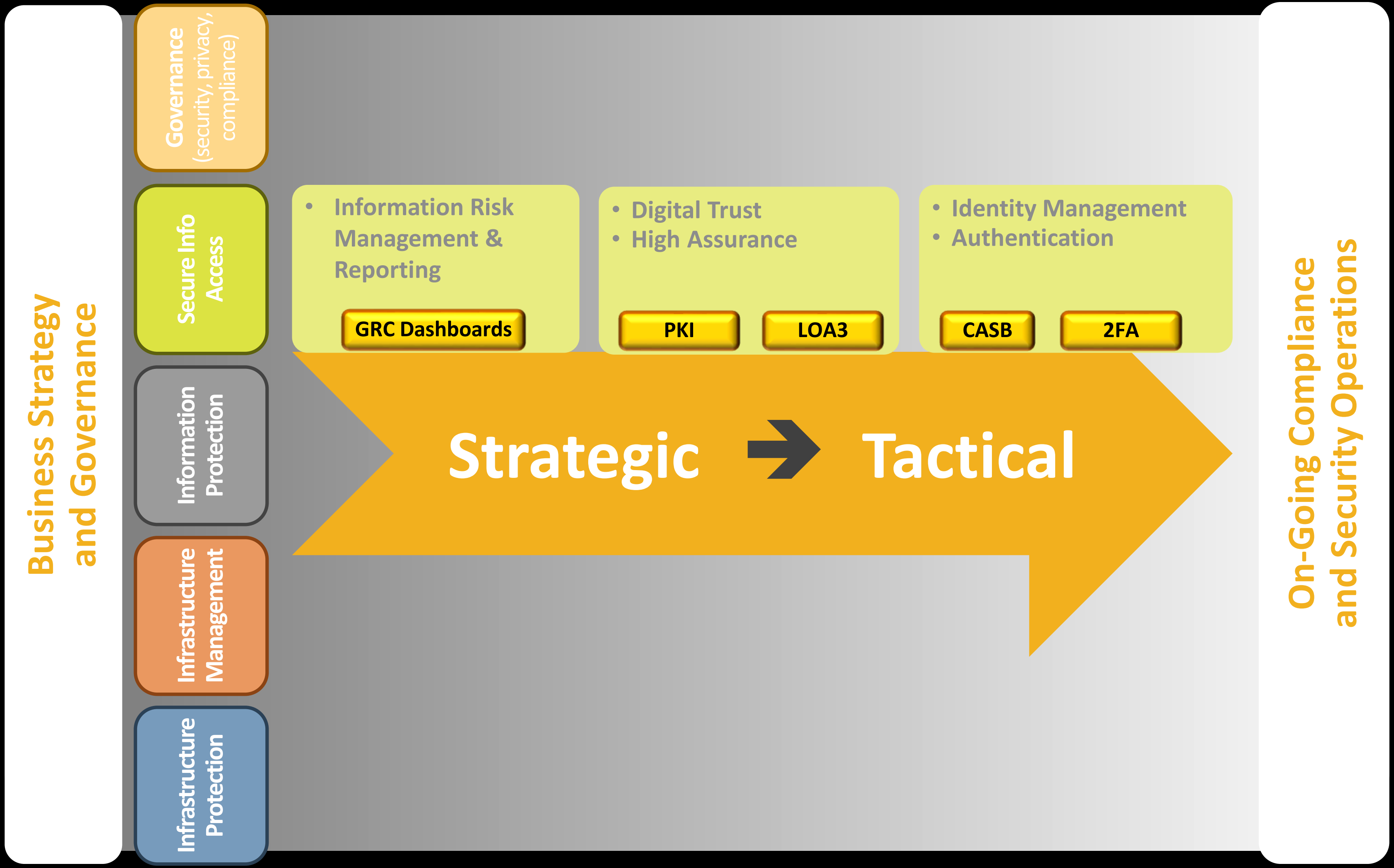
Flag 3 — 1,000 pts

A flag can fall into one of Symantec's five stages of a cyber attack, reconnaissance, incursion, discovery, capture or exfiltration. Different techniques and tools will be required for each stage.

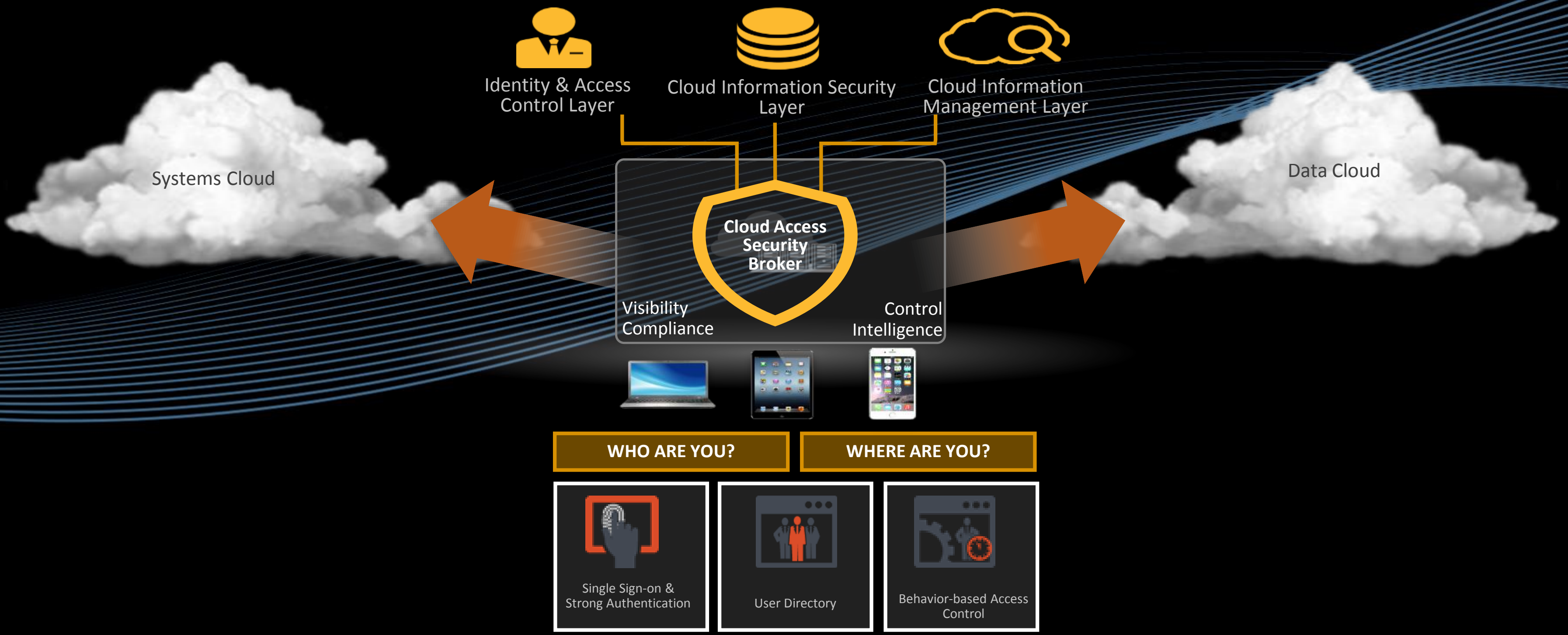
- Fully managed SaaS and Platform-as-a-Service offering with global coverage
- Comprehensive scoring and reporting functionality
- Over 600 hours of live system challenge scenarios, covering different industry verticals
- Over 7,000+ participants in 30+ countries
- Scenarios designed for different levels of difficulty
- Exercises can be run 1 day monthly, quarterly or yearly

A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations


Business Strategy and Governance
Governance (security, privacy, compliance)
Secure Info Access
Information Protection
Infrastructure Management
Infrastructure Protection
Information Risk Management & Reporting
GRC Dashboards
Digital Trust
High Assurance
PKI
LOA3
Identity Management
Authentication
CASB
2FA
Strategic → Tactical
On-Going Compliance and Security Operations

Use Case Example: Secure Information Access



Identity & Access Control Layer

Cloud Information Security Layer

Cloud Information Management Layer

Systems Cloud

Data Cloud

Cloud Access Security Broker

Visibility Compliance

Control Intelligence

WHO ARE YOU?

WHERE ARE YOU?

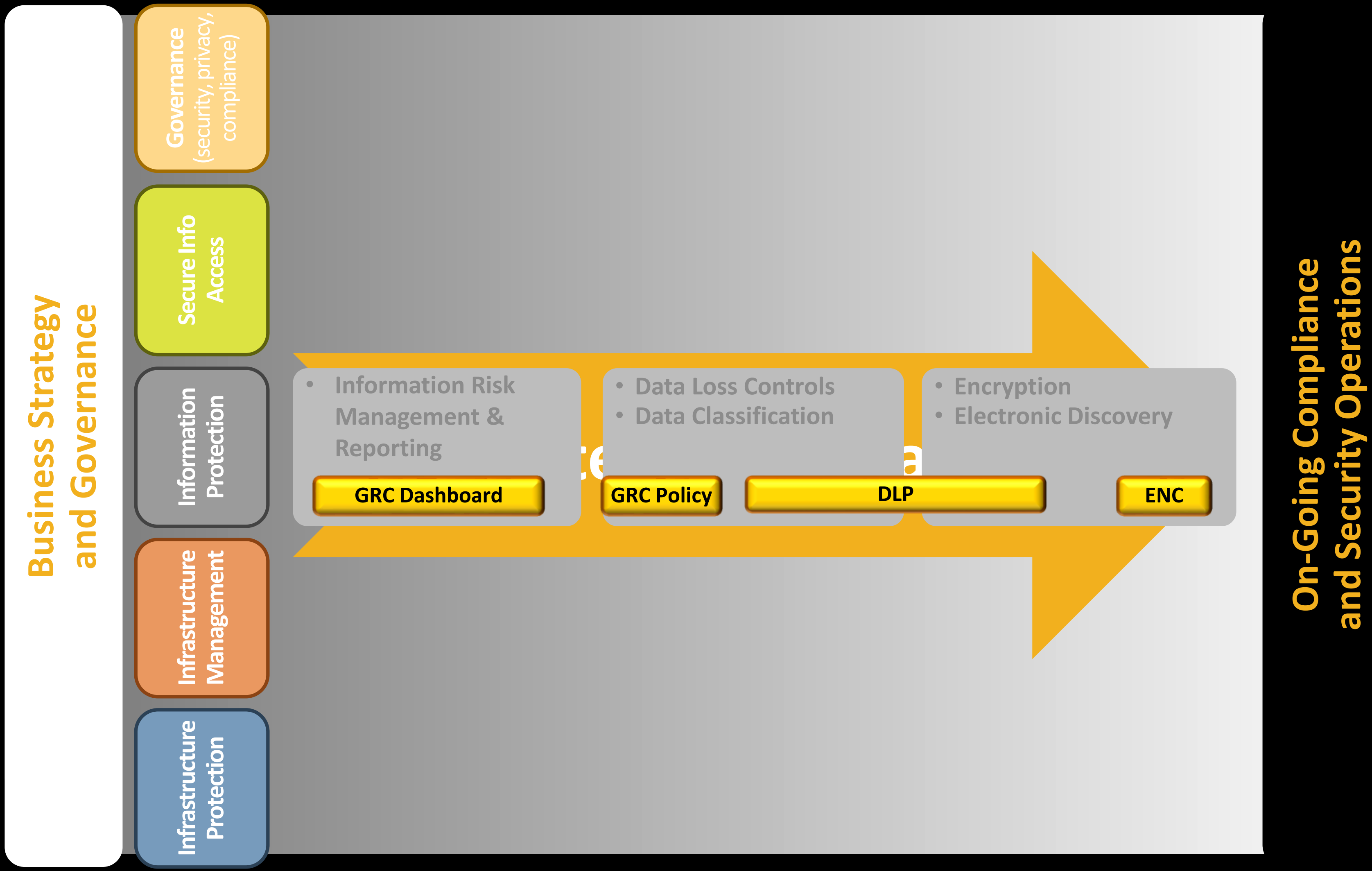
Single Sign-on & Strong Authentication

User Directory

Behavior-based Access Control

A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations



Business Strategy and Governance

Governance (security, privacy, compliance)

Secure Info Access

Information Protection

Infrastructure Management

Infrastructure Protection

- Information Risk Management & Reporting

GRC Dashboard

- Data Loss Controls
- Data Classification

GRC Policy

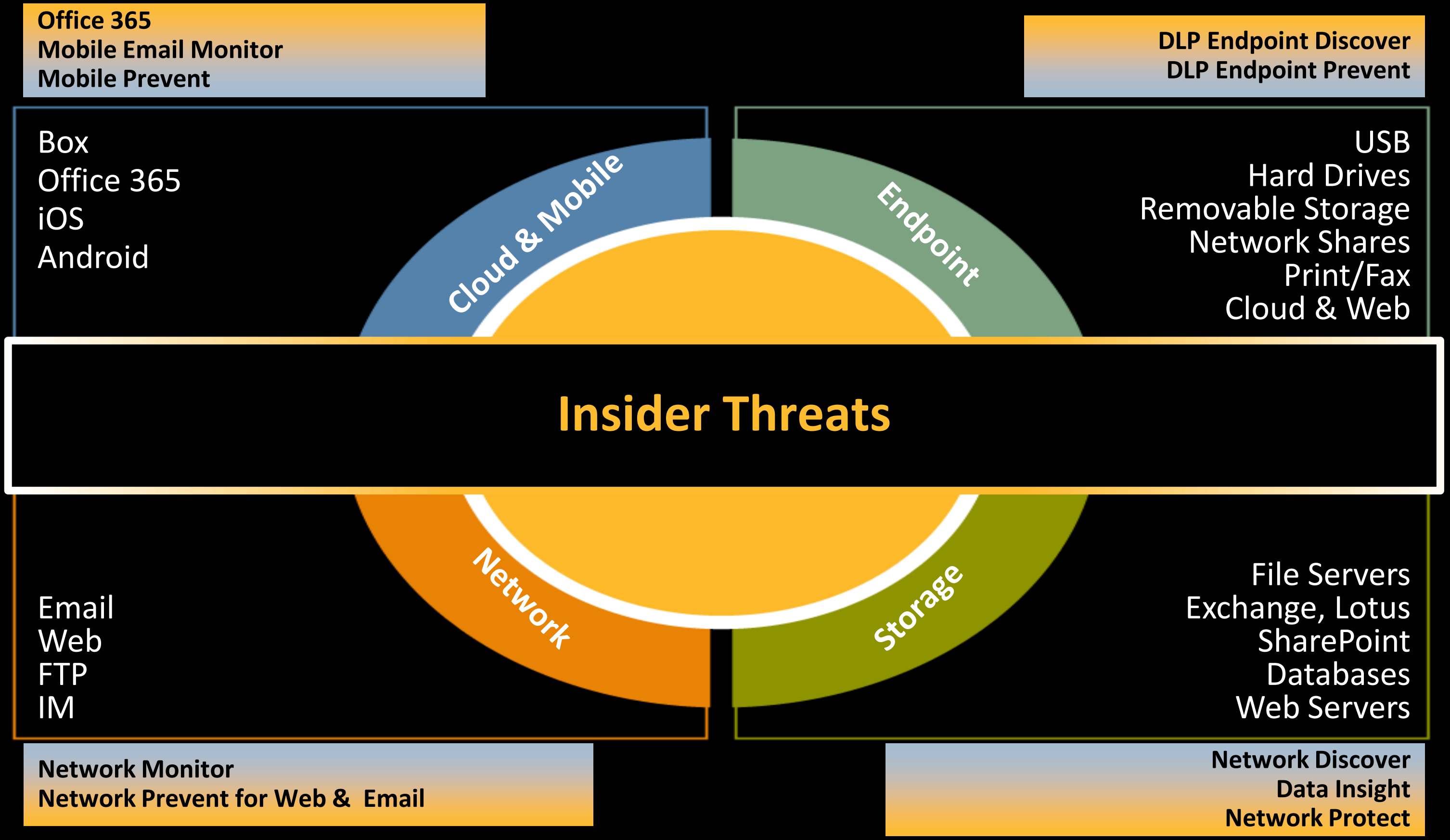
DLP

- Encryption
- Electronic Discovery

ENC

On-Going Compliance and Security Operations

Use Case : Information Protection



Office 365
Mobile Email Monitor
Mobile Prevent

DLP Endpoint Discover
DLP Endpoint Prevent

Box
Office 365
iOS
Android

USB
Hard Drives
Removable Storage
Network Shares
Print/Fax
Cloud & Web

Insider Threats

Email
Web
FTP
IM

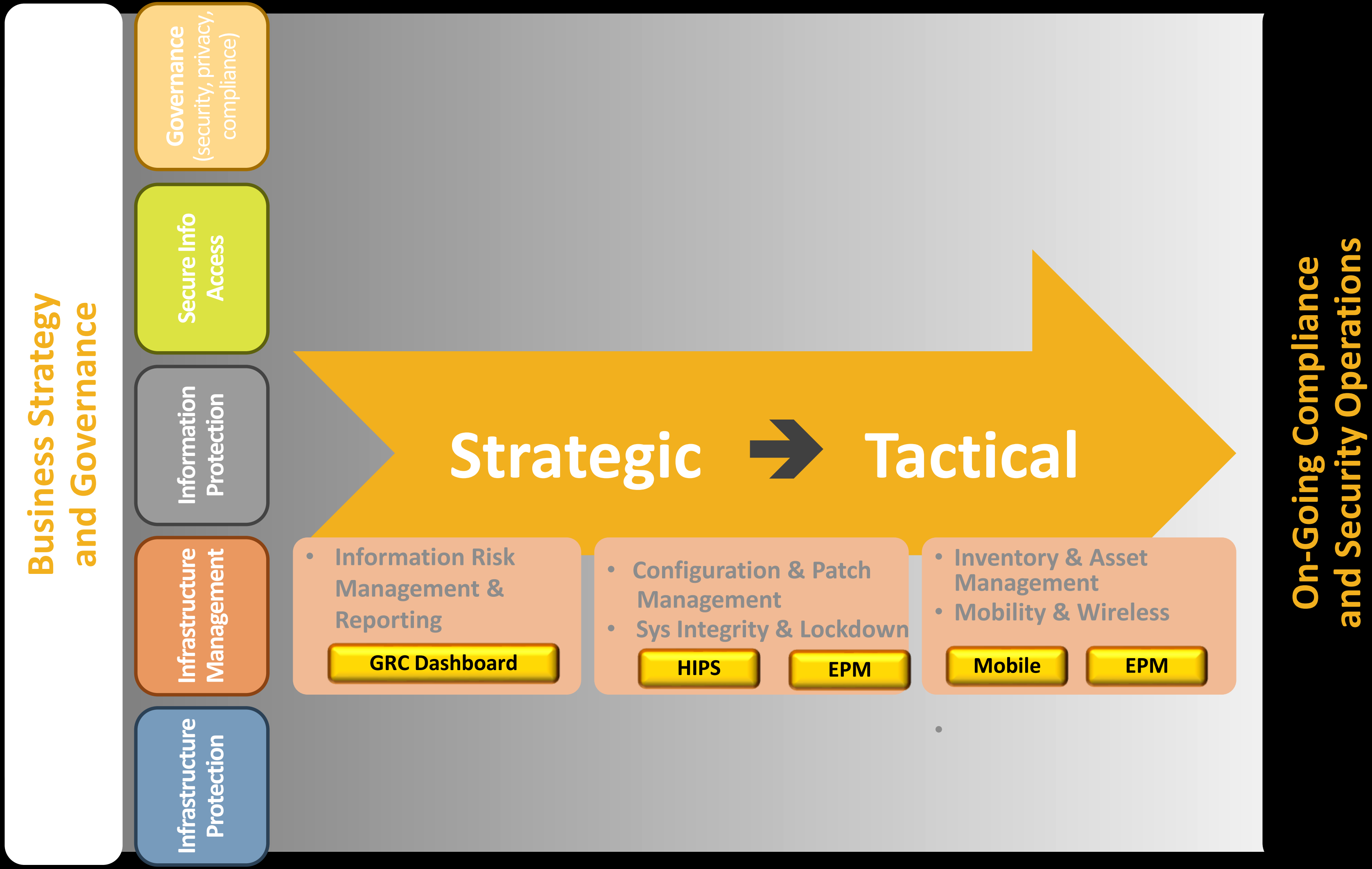
File Servers
Exchange, Lotus
SharePoint
Databases
Web Servers

Network Monitor
Network Prevent for Web & Email

Network Discover
Data Insight
Network Protect

A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations


Business Strategy and Governance
Governance (security, privacy, compliance)
Secure Info Access
Information Protection
Infrastructure Management
Infrastructure Protection
Strategic → Tactical
On-Going Compliance and Security Operations

- Information Risk Management & Reporting

GRC Dashboard

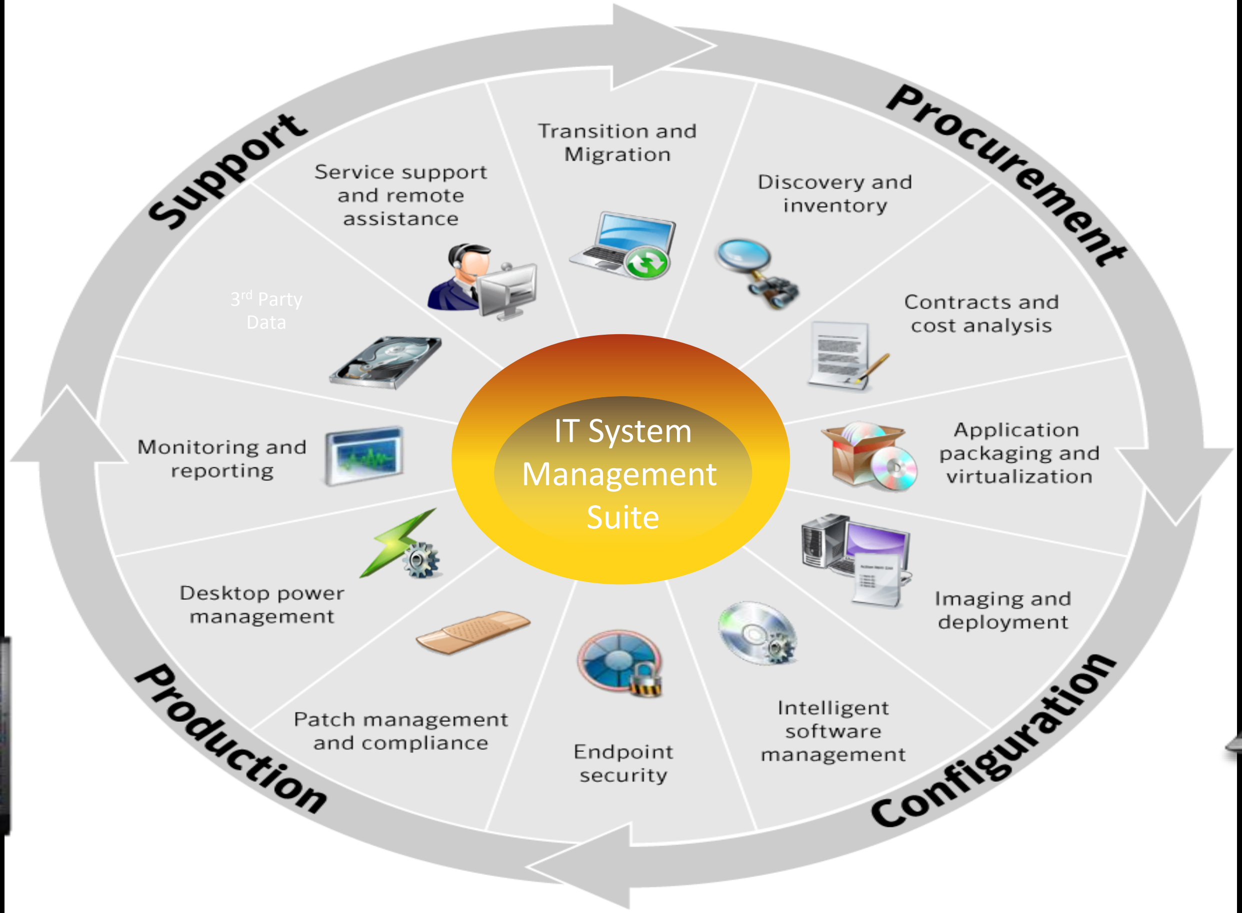
- Configuration & Patch Management
- Sys Integrity & Lockdown

HIPS | EPM

- Inventory & Asset Management
- Mobility & Wireless

Mobile | EPM

Use Case Example: Infrastructure Management



IT System Management Suite

Support

Procurement

Configuration

Production

Transition and Migration

Discovery and inventory

Contracts and cost analysis

Application packaging and virtualization

Imaging and deployment

Intelligent software management

Endpoint security

Patch management and compliance

Desktop power management

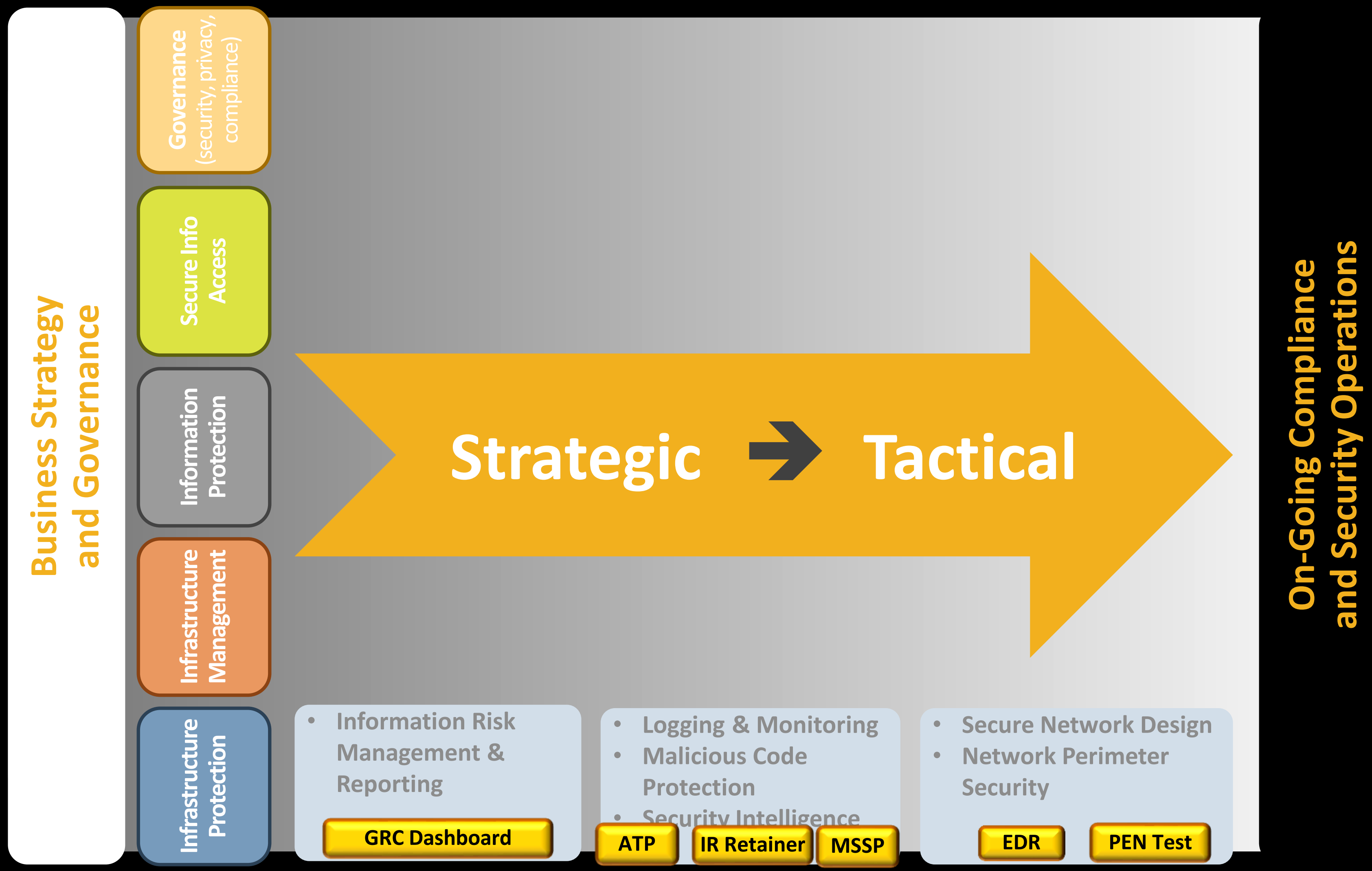
Monitoring and reporting

3rd Party Data

Service support and remote assistance

A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations



Business Strategy and Governance

Governance (security, privacy, compliance)

Secure Info Access

Information Protection

Infrastructure Management

Infrastructure Protection

Strategic ➔ Tactical

- Information Risk Management & Reporting

GRC Dashboard

- Logging & Monitoring
- Malicious Code Protection
- Security Intelligence

ATP

IR Retainer

MSSP

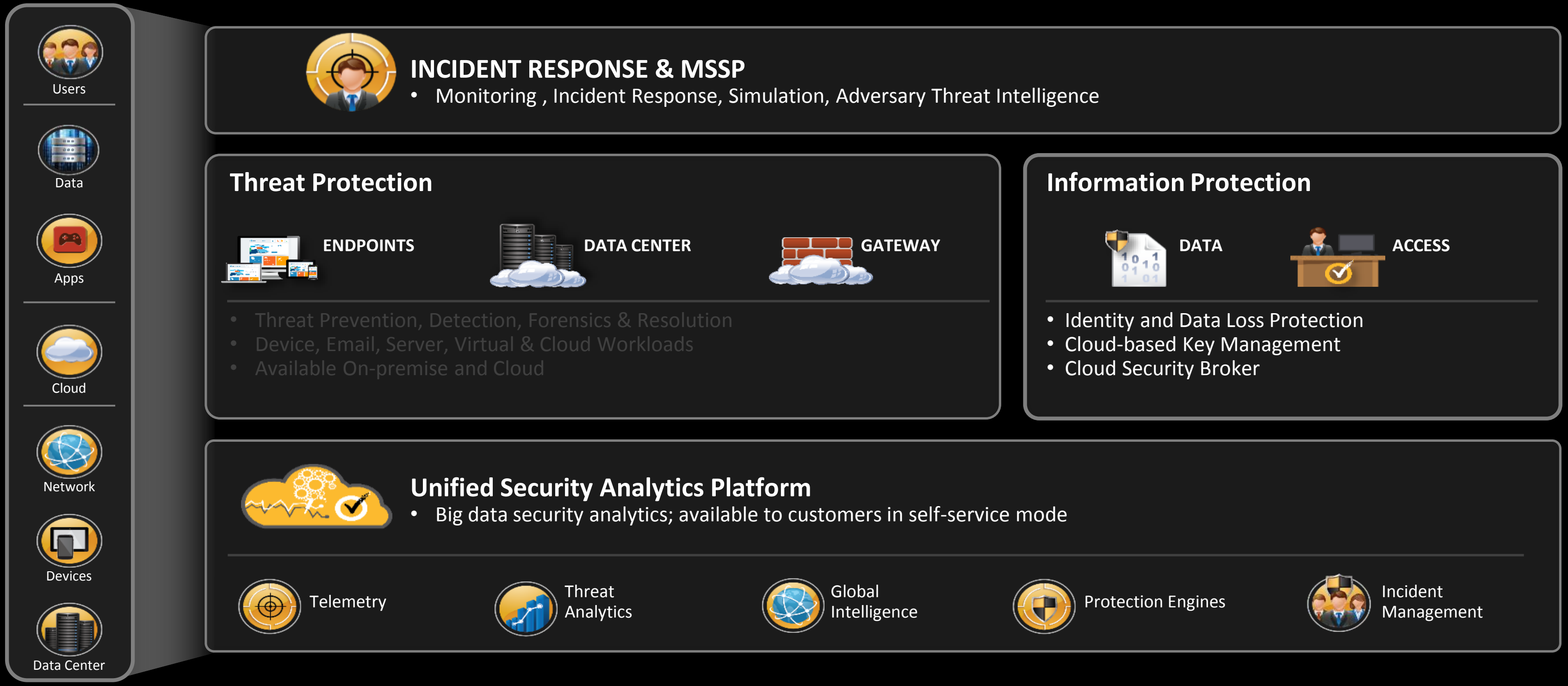
- Secure Network Design
- Network Perimeter Security

EDR

PEN Test

On-Going Compliance and Security Operations

Use Case Example: Infrastructure Protection & Security



INCIDENT RESPONSE & MSSP

- Monitoring , Incident Response, Simulation, Adversary Threat Intelligence

Threat Protection

- Threat Prevention, Detection, Forensics & Resolution
- Device, Email, Server, Virtual & Cloud Workloads
- Available On-premise and Cloud

Information Protection

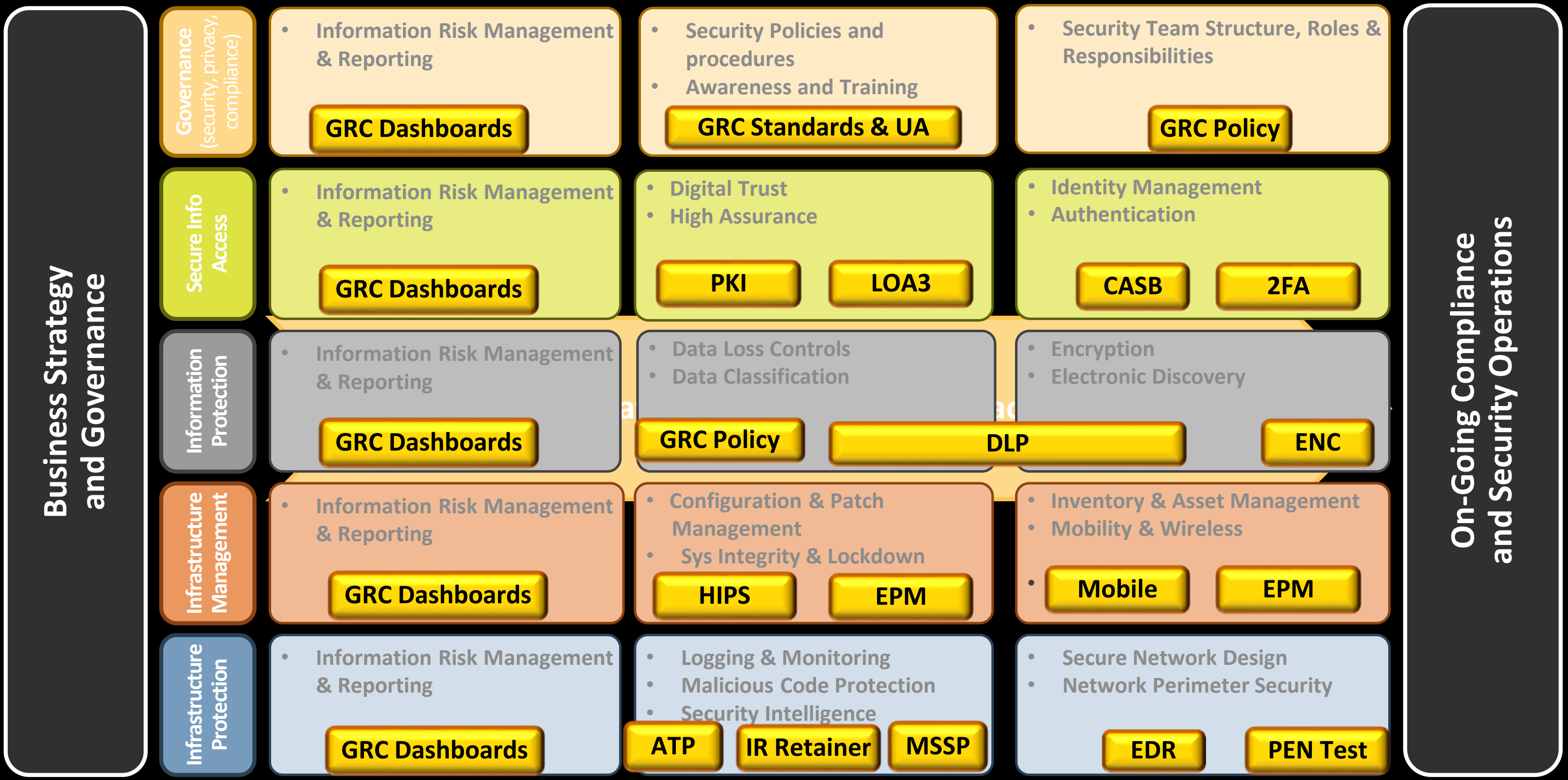
- Identity and Data Loss Protection
- Cloud-based Key Management
- Cloud Security Broker

Unified Security Analytics Platform

- Big data security analytics; available to customers in self-service mode

ENTERPRISE TOOLKIT: A Mature Compliance and Security Model

Business Strategy and Governance driving Security Operations



Business Strategy and Governance

Governance (security, privacy, compliance)	• Information Risk Management & Reporting GRC Dashboards	• Security Policies and procedures • Awareness and Training GRC Standards & UA	• Security Team Structure, Roles & Responsibilities GRC Policy
Secure Info Access	• Information Risk Management & Reporting GRC Dashboards	• Digital Trust • High Assurance PKI LOA3	• Identity Management • Authentication CASB 2FA
Information Protection	• Information Risk Management & Reporting GRC Dashboards	• Data Loss Controls • Data Classification GRC Policy DLP	• Encryption • Electronic Discovery ENC
Infrastructure Management	• Information Risk Management & Reporting GRC Dashboards	• Configuration & Patch Management • Sys Integrity & Lockdown HIPS EPM	• Inventory & Asset Management • Mobility & Wireless • Mobile EPM
Infrastructure Protection	• Information Risk Management & Reporting GRC Dashboards	• Logging & Monitoring • Malicious Code Protection • Security Intelligence ATP IR Retainer MSSP	• Secure Network Design • Network Perimeter Security EDR PEN Test

On-Going Compliance and Security Operations

WHERE TO START:
CYBER SECURITY FRAMEWORK

Improving Critical Infrastructure Cybersecurity

Executive Order 13636

February 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a **cyber environment** that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

FUNCTIONS: HIGH-LEVEL GOALS

Functions		
ID	**Identify**	Develop the **organizational understanding** to manage cybersecurity risk to systems, assets, data, and capabilities
PR	**Protect**	Develop and implement the **appropriate safeguards** to ensure delivery of critical infrastructure services
DE	**Detect**	Develop and implement the appropriate activities to **identify the occurrence** of a cybersecurity event
RS	**Respond**	Develop and implement the appropriate activities to **take action** regarding a **detected** cybersecurity event
RC	**Recover**	Develop and implement the appropriate activities to **maintain plans for resilience** and to **restore any capabilities or services** that were impaired due to a cybersecurity event

CATEGORIES: EXAMPLE OF SPECIFIC ACTIVITIES

Function	Categories		
Identify (ID)	ID.AM	**Asset Management (AM)**	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are **identified** and **managed** consistent with their **relative importance** to business objectives and the organization's risk strategy.
	ID.BE	**Business Environment (BE)**	The organization's **mission**, **objectives**, **stakeholders**, and **activities** are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	ID.GV	**Governance (GV)**	The **policies**, **procedures**, and **processes** to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk.
	ID.RA	**Risk Assessment (RA)**	The organization **understands the cybersecurity risk** to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	ID.RM	**Risk Management Strategy (RM)**	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to **support operational risk decisions**.

UNDERSTAND YOUR MATURITY: SELF ASSESSMENT LED

IDENTIFY	🟥 **ID.BE** Organization	🟪 **ID.AM** Asset Mgt.	🟥 **ID.RA** Risk Assessment	🟥 **ID.RM** Risk Strategy Mgt	🟪 **ID.GV** Governance
PROTECT	🟥 **PR.AT** Awareness Training	🟨 **PR.AC** Access Control	🟨 **PR.DS** Data Security	🟨 **PR.IP** Info Processes &, Procedures	
DETECT	🟩 **DE.AE** Anomalies & Events	🟩 **DE.CM** Continuous Monitoring	🟩 **DE.DP** Detection Processes		
RESPOND	🟪 **RS.RP** Response Planning	🟩 **RS.CO** Response Communications	🟩 **RS.AN** Response Analysis	🟨 **RS.MI** Response Mitigation	🟩 **RS.IM** Response Improvements
RECOVER	🟦 **RC.RP** Recovery Planning	🟨 **RC.IM** Recovery Improvements	🟨 **RC.CO** Recovery Communications		

🟥 **Not At All** 🟧 **Planned** 🟪 **Partially** 🟨 **Mostly** 🟩 **In Place** 🟦 **Optimized**

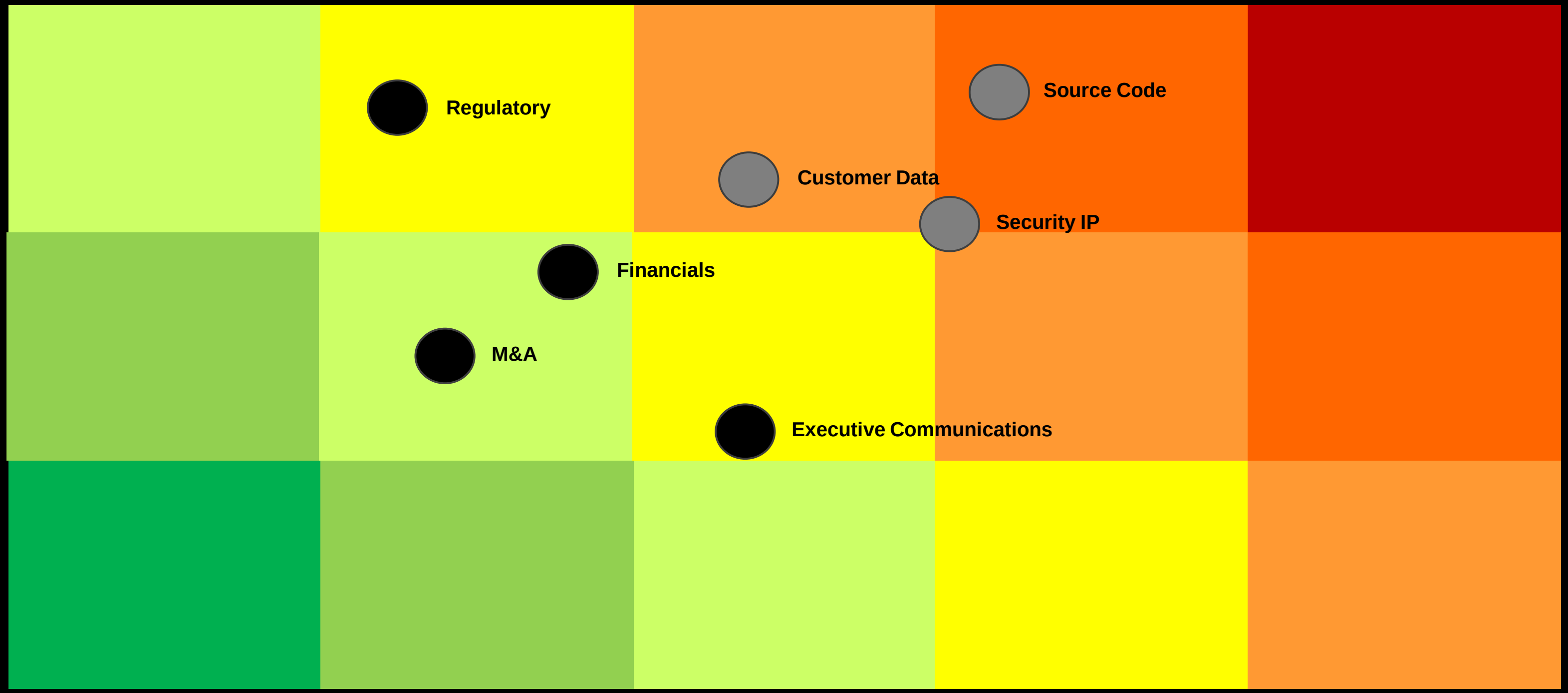
Communication Template:
EXECUTIVE VIEW/REPORTING - RISK MANAGEMENT

Security Risk Posture for Cyber Risks

Asset	Risk	Control Posture	Why are we at risk?	What are we doing about it?
Network (Infrastructure)	HIGH	🔴	• Comes from your threat reports	• Implementing consistent security practices and governance
Web based Application	MED	🟡 🟢		
System (OS)	LOW			

Communication Template:
EXECUTIVE VIEW/REPORTING - PRIORITES

Security Risk Posture for Cyber Risks



Communication Template:
EXECUTIVE VIEW/REPORTING - ACCOMPLISHMENTS

Maturity Model	0 Conceptual	1 Defined	2 Operational	3 Managed	4 Quantifiably Managed	5 Optimizing

	Accomplishments	Risks	Status
Cyber	• Example: Incident Response • Awareness and Phishing Training	• Infrastructure Breach	Managed (3.0)
Physical	• Employee Health/Safety Program	• Executive Protective Services	Operational (2.5)
BC/DR	• Business Impact Analysis	• DR Plan Execution over next 3 quarters	Defined (1.5)

Communication Template:
EXECUTIVE VIEW/REPORTING - DATA CLASSIFICATION

Security Risk Posture for Cyber Risks

Actor	Motivations	Assets	Who are they?	Likelihood of Attack
Nation State	• Economic, political, and/or military advantage	• IP (source code) • Certificates (Trust Services) • Infrastructure	• China • Russia • N. Korea • Other 'combative' nations	High, **Med** or Low
Org. Crime	• Immediate financial gain • Collect info for future financial gains • Identity theft	• IP (source code) • Certificates (Trust Services) • Infrastructure • Customer Data • Operational information	• Multi-skilled, multifaceted virtual criminal networks primarily operated out our eastern Europe and Asia • Sometime in partnership or cooperation with nation states	**High**, Med or Low
Hacktivist	• Impact brand • Expose IP • Further agenda	• IP (source code) • Infrastructure • Brand	• Anonymous • Syrian Electronic Army (SEA) • Electronic Cyber Army (ECA)	**High**, Med or Low
Insider	• Personal gain • Code reuse • IP exposure • Financial gain	• IP (source code) • Brand • Operational information • Customer Data	• Fraud committed by managers consistently causes more actual damage ($200,105 on average) • On average, fraud activity starts 5 years after hiring	**High**, Med or Low
Competitor	• Roadmap discovery • Product releases • Market share dilution • Customer registries	• IP (source code) • Brand • Operational information	• No known competitive adversaries	High, Med or **Low**

Communication Template:
EXECUTIVE VIEW/REPORTING - STRATEGIC FRAMEWORK
Security Risk Posture for Cyber Risks

V

Vision:
A 5 plus year strategic horizon; Communicates a team’s shared view of success

S

Strategy:
The innovative customer value proposition that must be realized to achieve the vision;
Important decisions for where and how to apply resources to accomplish the vision;
The new strategic priorities

E

Execution:
What must be executed each year to realize each strategic priority;
Outlines critical initiatives, programs, or actions that support each strategy

M

Metrics:
Shows how the team measures success and agrees to be held accountable to the execution plan

THANK YOU!