CYBER SECURITY MANAGEMENT, THE BIG PICTURE

KHALID MUHSEN ALMUTAIRI

MAY 2017

Short Bio

Senior Manager, Global IT Security Enablement at SABIC; 13 years experience in various Information Technology fields of which 9 years in Cyber Security. Obtained my BS degree in Computer Engineering from KFUPM, Saudi Arabia. Hold the following professional Certifications: CISSP, SABSA Charted Architect at Foundation Level (SCF), Certified International Project Manager (CIPM), Project Management Professional (PMP), Lean Six Sigma (Green Belt), CISCO Certified Security Professional (CCSP) and more.

Today I am managing the global it security program and governance @ SABIC.

CYBER SECURITY MANAGEMENT; HOW ☹?

Security Analytics

Defense In Depth

Intrusion Prevention

Penetration Testing

Risk assessment

Phishing Emails

Firewalls

Secure Coding

DDOS

Vulnerability Management

Compliance

Identity Management

Passwords

Password Management

Security Awareness

Patch management

DLP

Data Classification

Anti Virus

Deep Inspection

Security monitoring

Incident Response

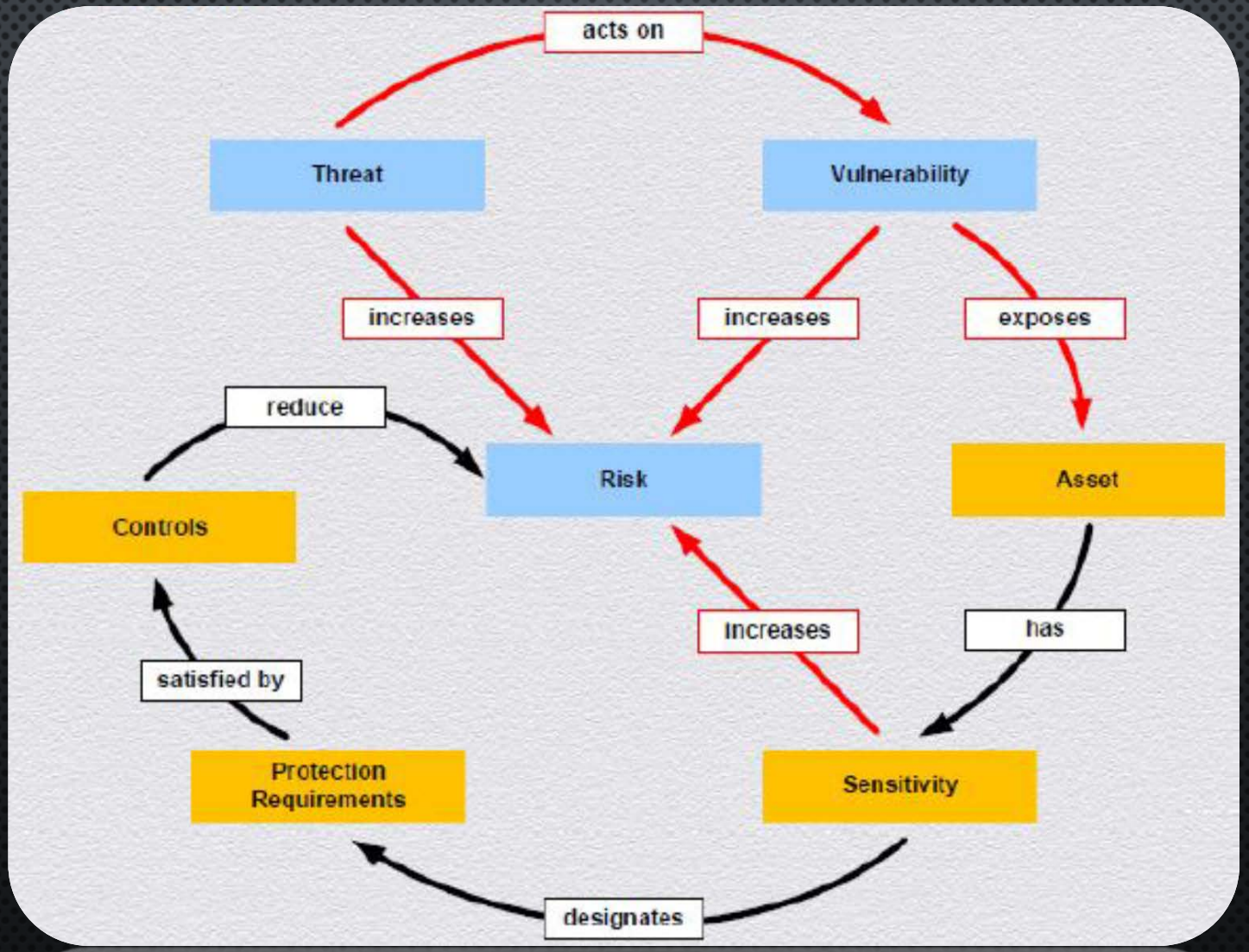
ISO 27001

Multifactor authentication

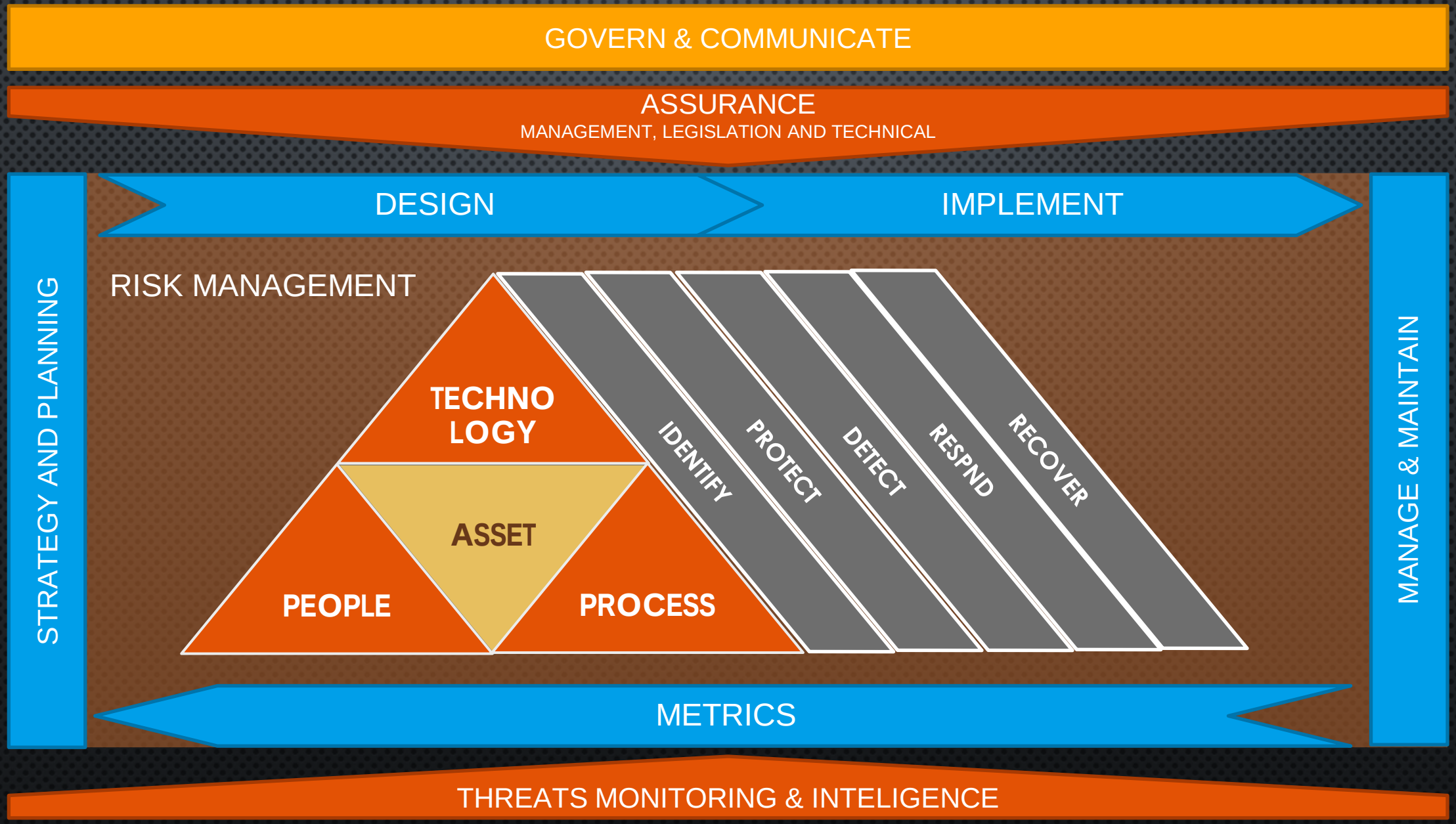
Symptoms of Bad Cybersecurity Management

- Driven by fear and directed by vendors
- "It's an IT issue" mindset
- Duplicate security controls
- Security metrics are basics or missing
- Majority of actions are ad hoc or reactive
- The security approach is not comprehensive
- There is no single authoritative asset inventory
- Security knows that there are unresolved security gaps
- There are frequent major security incidents

CYBERSECURITY MANAGEMENT AS A BUSINESS RISK



CYBERSECURITY MANAGEMENT FRAMEWORK (MY VIEW)



Symptoms of a good cybersecurity management

- Driven & directed by risk level while following a well structured management fraework
- "It's a business risk" mindset
- Having a well structured view and architecture for controls placement (defense in depth, less controls duplication, etc)
- Majority of actions are risk driven (strategic and tactical) with clear prioritization
- There is an authoritative assets inventory
- few major security incidents with faster, well managed response.
- Meaningful security metrics that leads to improvements and decision making

TAKEAWAYS

- Our goal is to identify, manage and reduce cybersecurity risks effectively and in a comprehensive manner
- Adopt a framework and start from wherever you are
- Managing cybersecurity might be seen as overwhelming and tough; however it's possible once we see "the big picture"
- Managing cybersecurity is not a destination, it's journey; choose to enjoy it ;-)

ANY QUESTIONS…?

THANKS

EXTRA STUFF:

DENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset management	Access control	Anomalies and events	Response planning	Recover planning
Business environment	Awareness and training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection process	Analysis	Communications
Risk assessment	Information protection and procedures		Mitigation	
Risk management strategy	Maintenance		Improvements	
	Protective technology			

Popular frameworks:

- COBIT
- CIS (SANS Top 20)
- ISO 27000 Series
- NIST SP 800 Series
- NIST CSF
- OCTAVE
- SABSA

PHISHING KILL CHAIN

WHAT MAKES A GOOD METRIC?

- Easily **measured**
- Easily **understood**
- Enables **decision-making**
- **Meaningful**
- **Consistent**
- **Quantitative**