RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-R04

The Measure of Success: Security Metrics to Tell Your Story

MODERATOR: **Lisa Lee, CRISC, CISA, IAM**

IT Examiner
Office of the Comptroller of the Currency
@lisainmiami

PANELISTS:

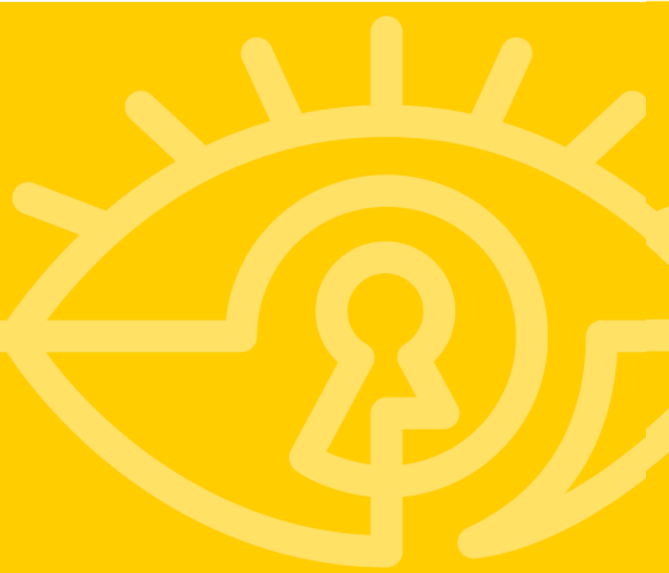
Julie Bernard
Principal – Cyber Risk Services
Deloitte
@juliein10A

Wendy Frank
Principal, Advisory, Cybersecurity, Privacy & Risk, PwC

#RSAC

How to Tell Your Story

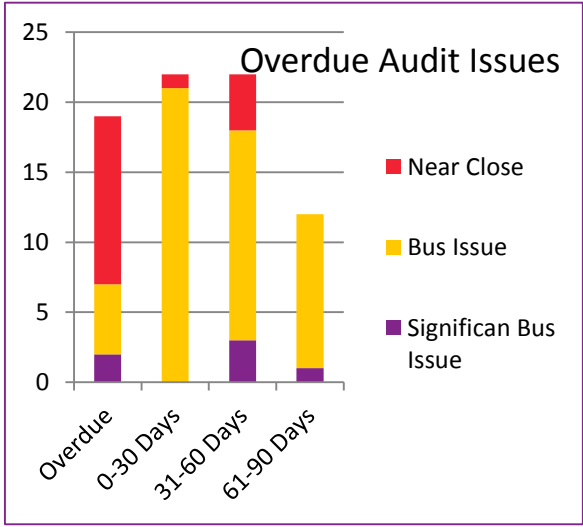
- Audience
- What Good Looks Like
- Responsibility and Accountability
- Data Availability
- Single Source of Truth & Repeatability
- “As Is” State
- Frequency

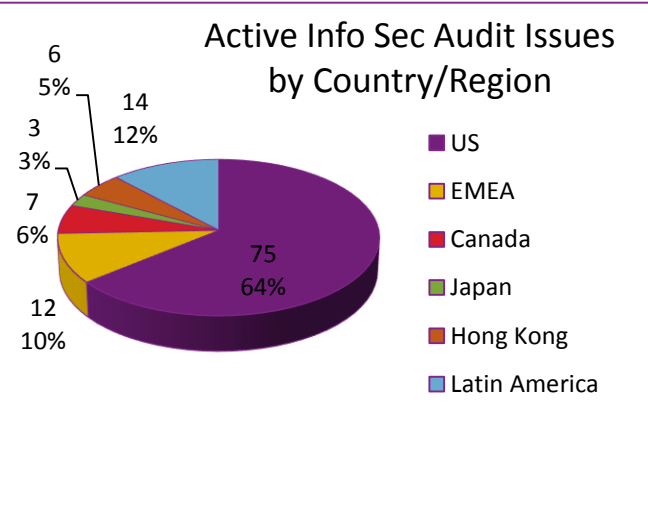


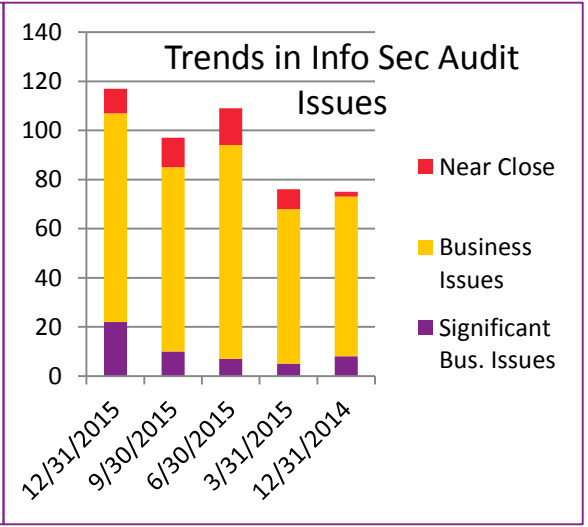
Operational Report Examples

Operational Report Examples

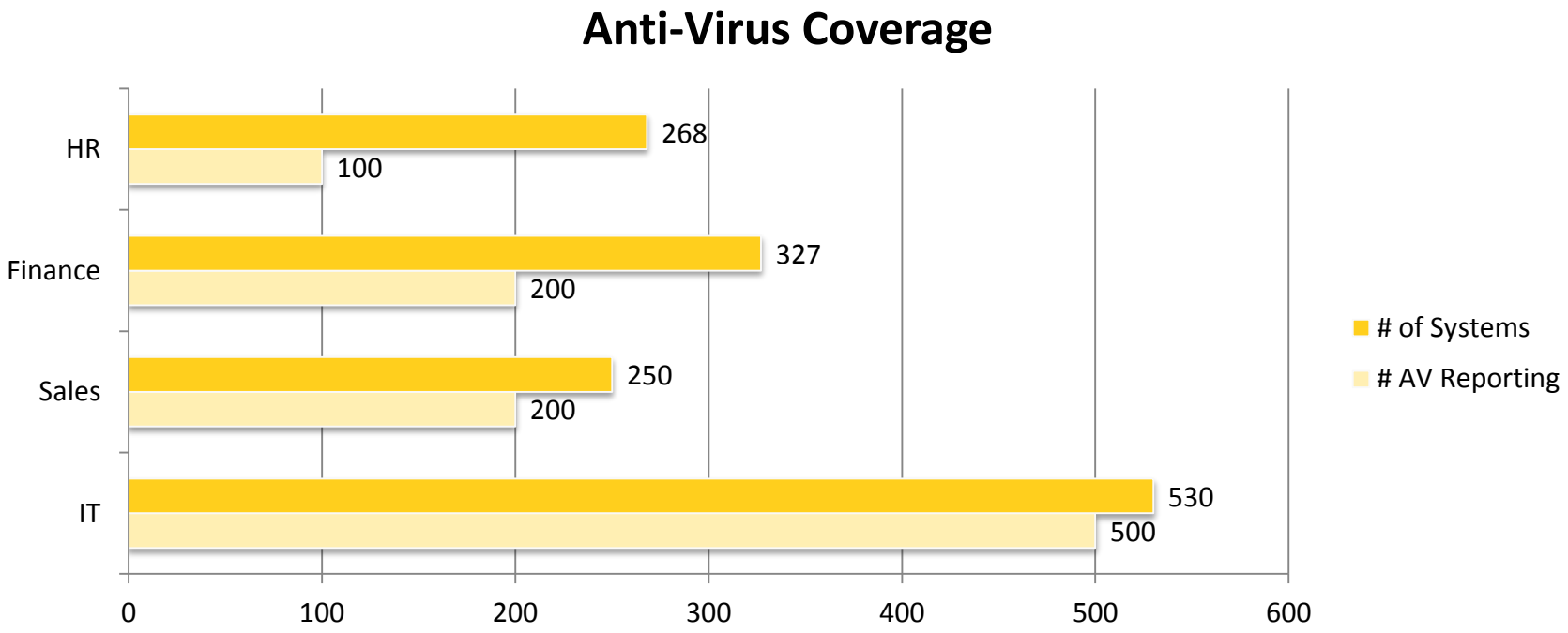
Information Security Audit Issues



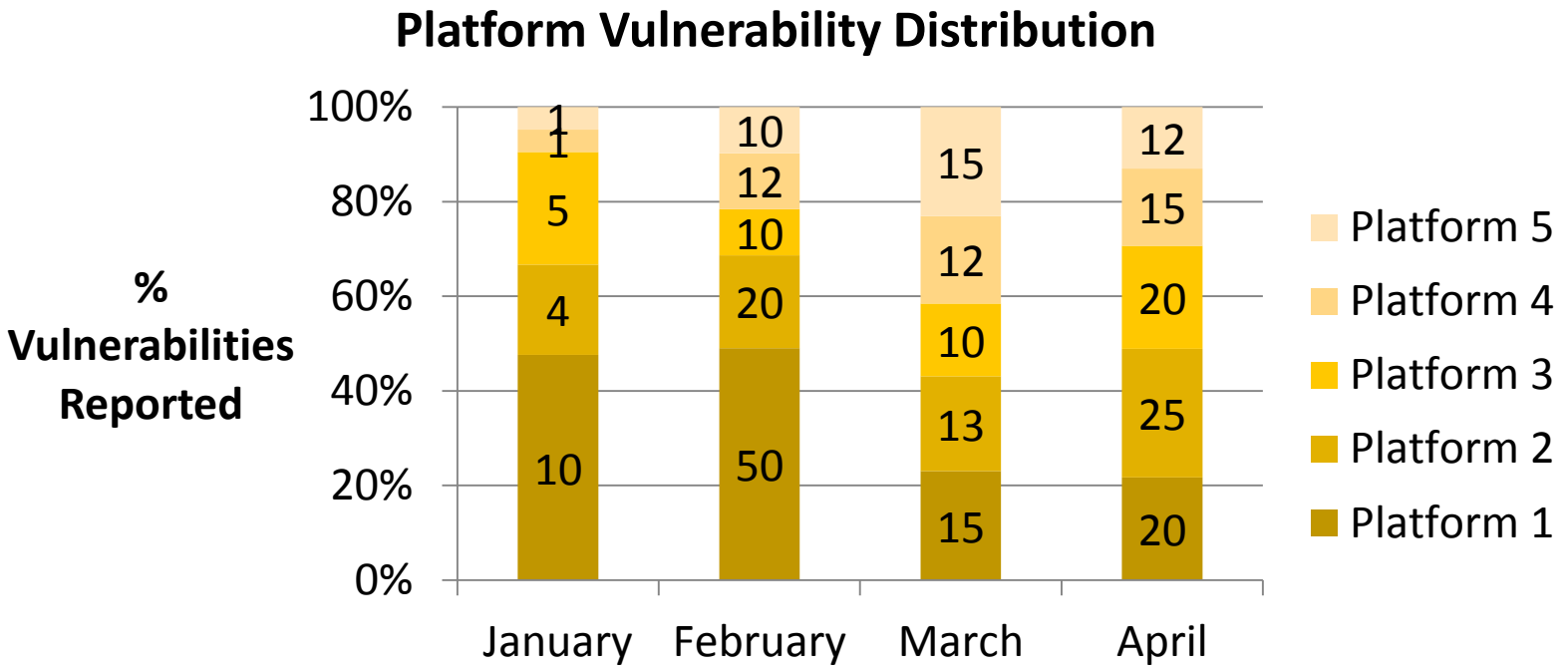




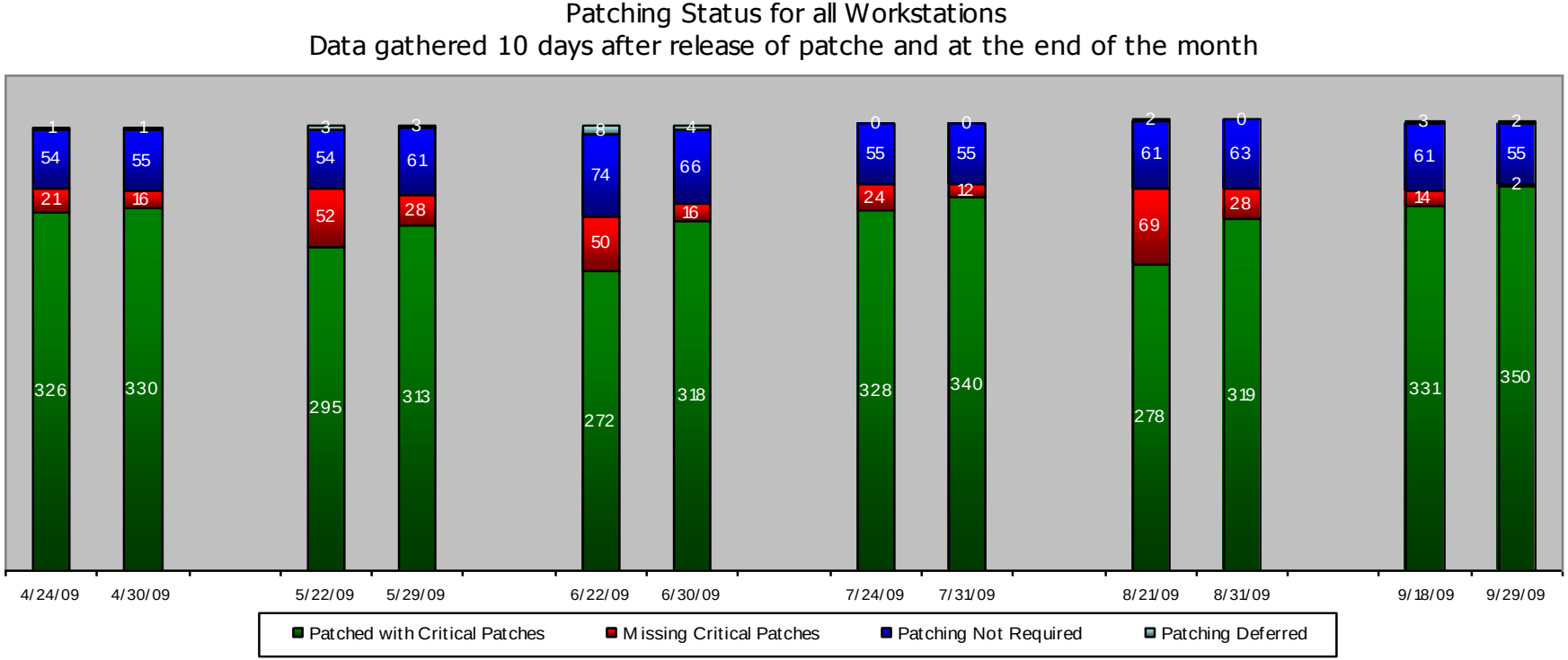
Operational Report Examples



Operational Report Examples



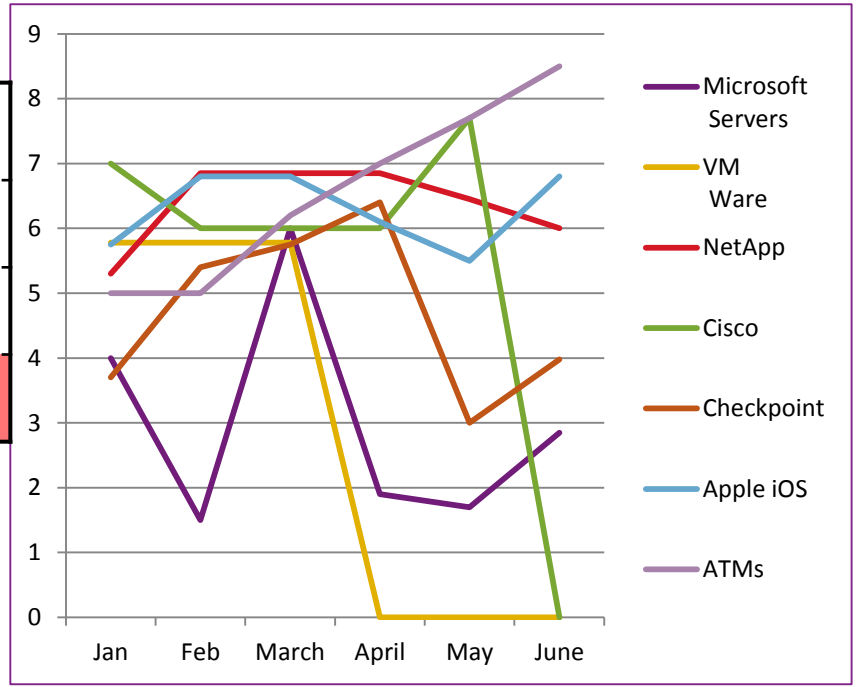
Operational Report Examples



Operational Report Examples

Patch Management Risk by Platform*

	Microsoft Servers	VM Ware	NetApp	Cisco	Checkpoint	Apple iOS	ATMs
GREEN (0-3)		0.00%	2.34%				
YELLOW (4-7)	5.32%			4.40%		7.25%	
RED (8-10							7.98%



*Data is not actual

Operational Report Examples

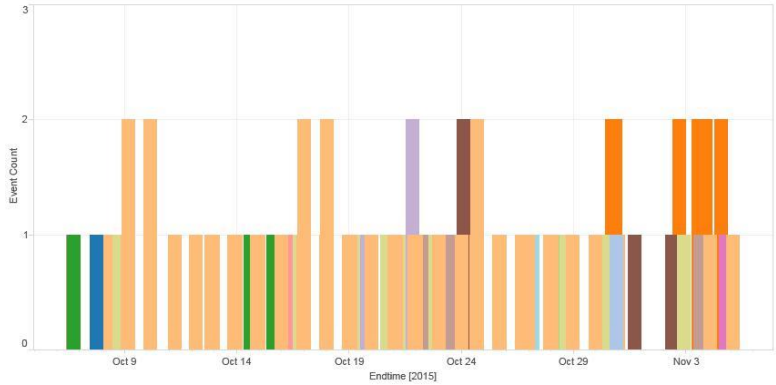
Malware Detected by Geo Location

Malware Event Name

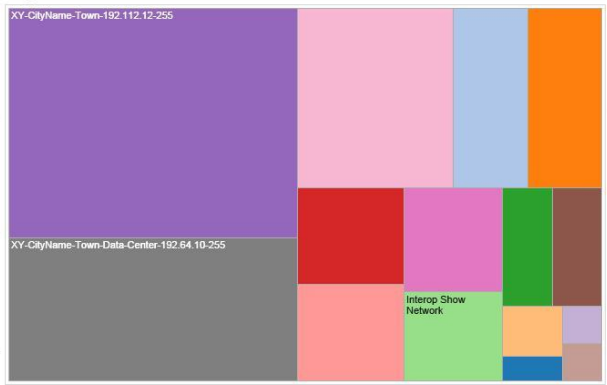
Endtime

Malware Name - By Day

Malware vs Time



Target Zone



Attacker Address

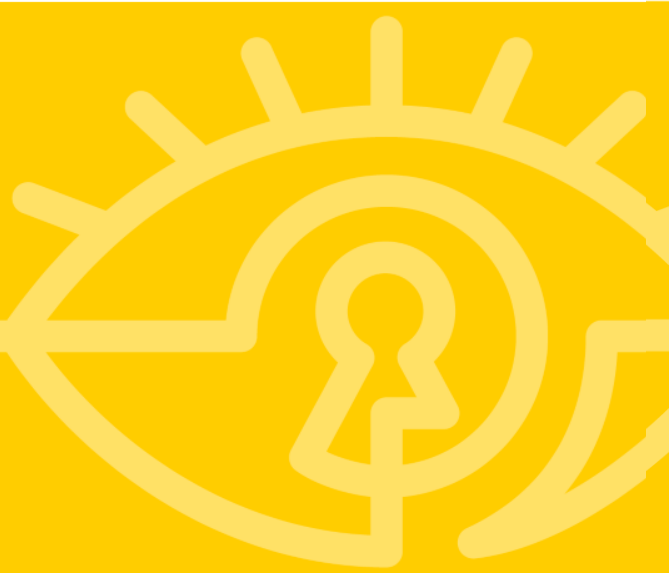
192.0.215.45
192.14.244.252
192.15.160.20
192.20.106.192

Target Address

192.9.225.35
192.10.10.110
192.13.4.242
192.24.10.209
192.30.14.25

Malware Name List

Android.Riskware.Deng..
Backdoor.Generic.9163..
Bot.Conficker.D
Exploit.Kit.Angler
iOS.Malware.XcodeGho..
iOS.Malware.XcodeGho..
Local.Callback

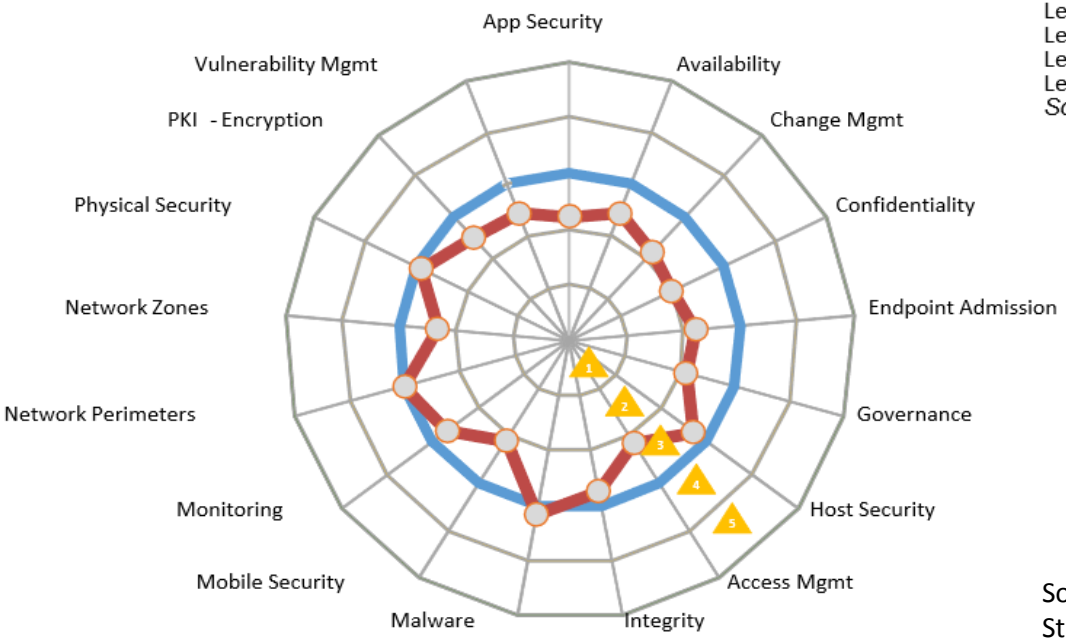


Executive Discussions

Executive Discussions

Security Assessments Conducted 2011 through 2014

Over 40 Agencies comprising over 80% of State FTEs



Maturity Level Definitions

Level 1: Initial/Ad Hoc
Level 2: Developing/Reactive
Level 3: Defined/Proactive
Level 4: Managed
Level 5: Optimized
Source: Gartner

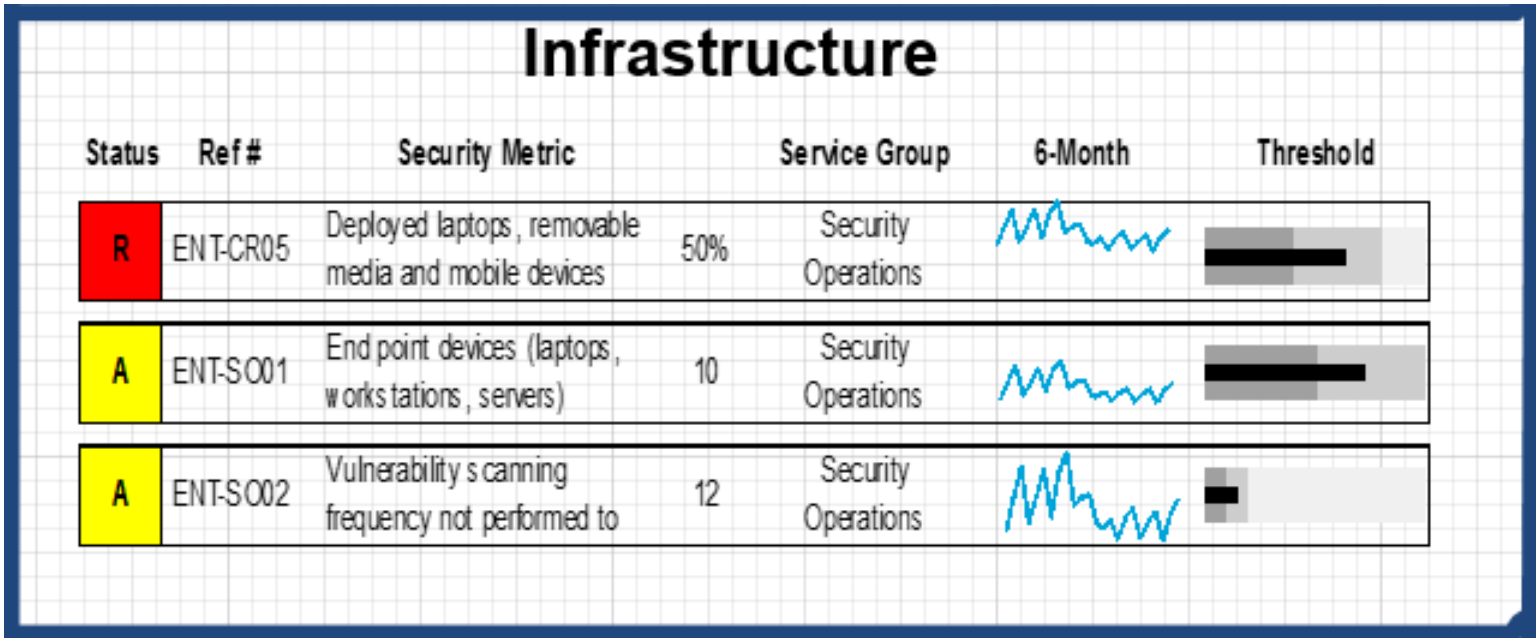
Source: The State of Texas;
State of the State Report, Jan. 2015

Executive Discussions

Compliance & Control

Status	Ref #	Security Metric		Service Group	6-Month	Threshold
R	ENT-CR03	Critical information assets / systems where identified compliance requirements	75%	Security Operations		
R	ENT-CR06	Unresolved legal and/or regulatory IT / IS focused issues (aging list)	50%	Security Operations		
A	ENT-GF03	Unresolved critical internal IT / IS focused audit issues (aging list)	10	Security Operations		

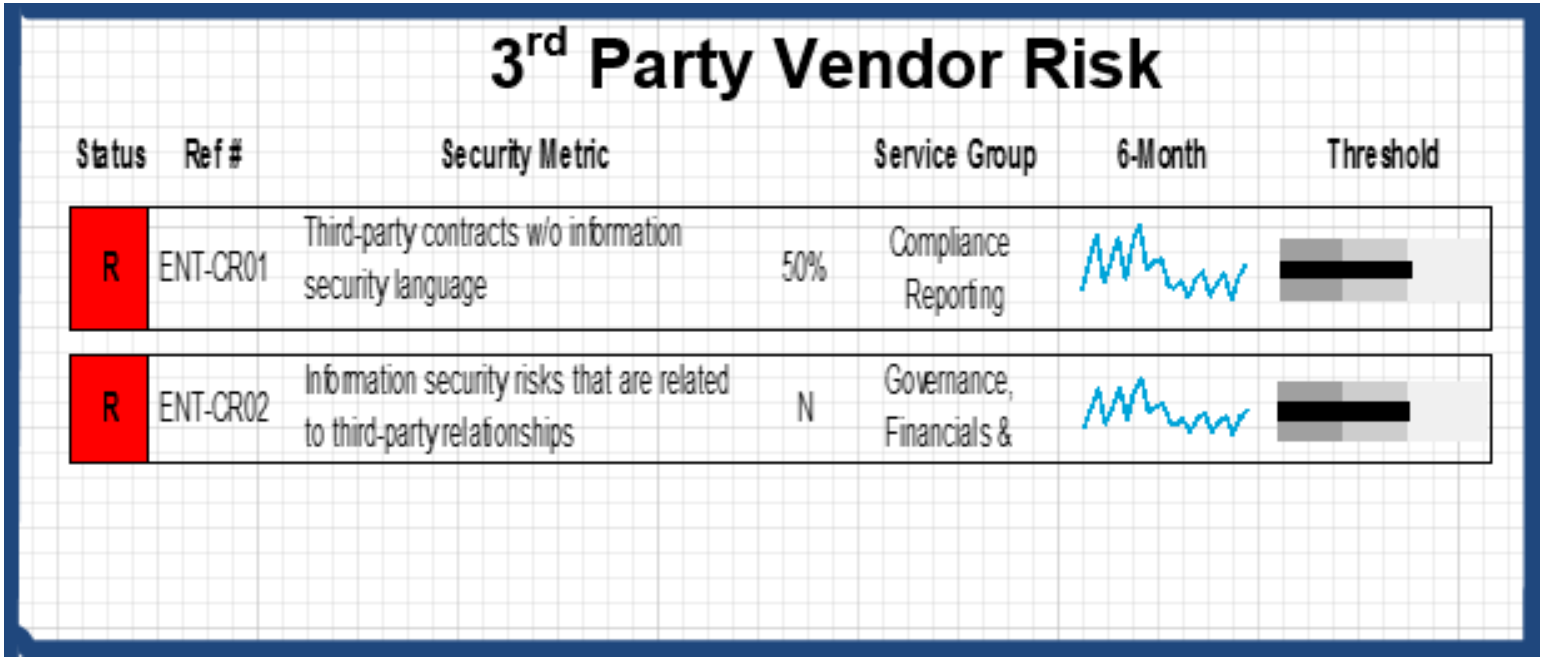
Executive Discussions



Infrastructure

Status	Ref #	Security Metric		Service Group	6-Month	Threshold
R	ENT-CR05	Deployed laptops, removable media and mobile devices	50%	Security Operations		
A	ENT-SO01	End point devices (laptops, workstations, servers)	10	Security Operations		
A	ENT-SO02	Vulnerability scanning frequency not performed to	12	Security Operations		

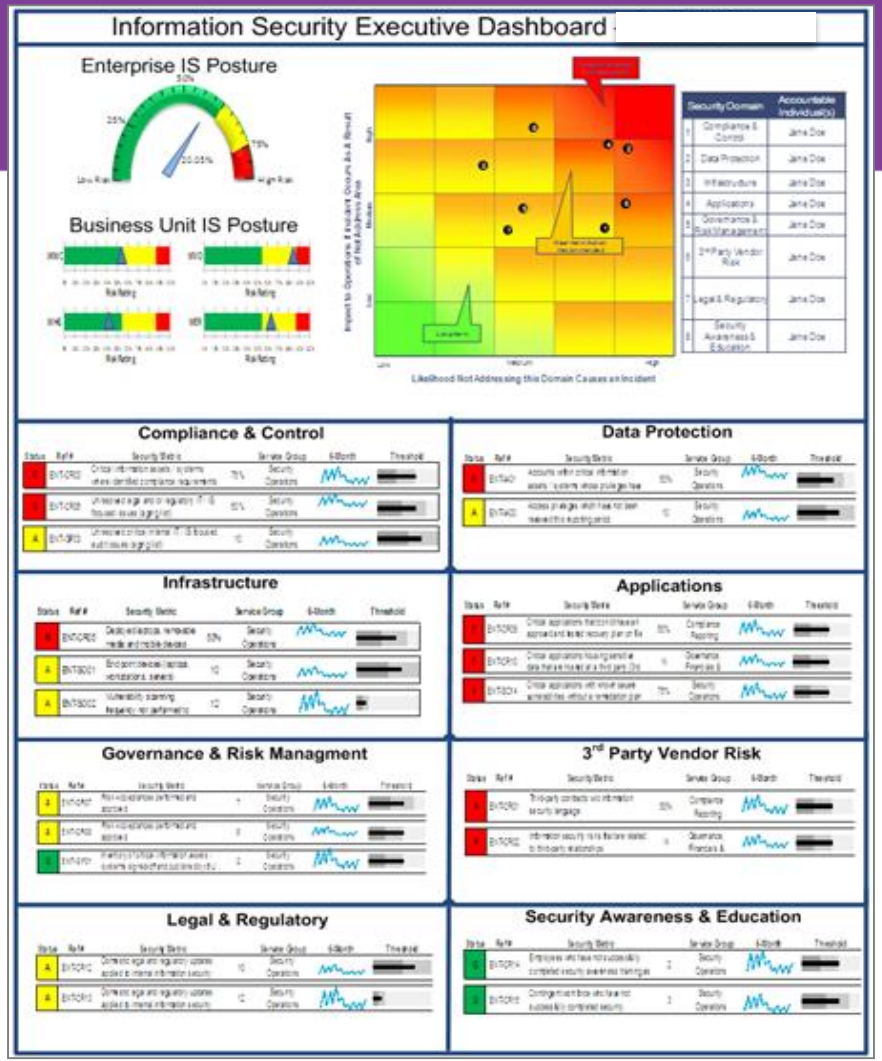
Executive Discussions

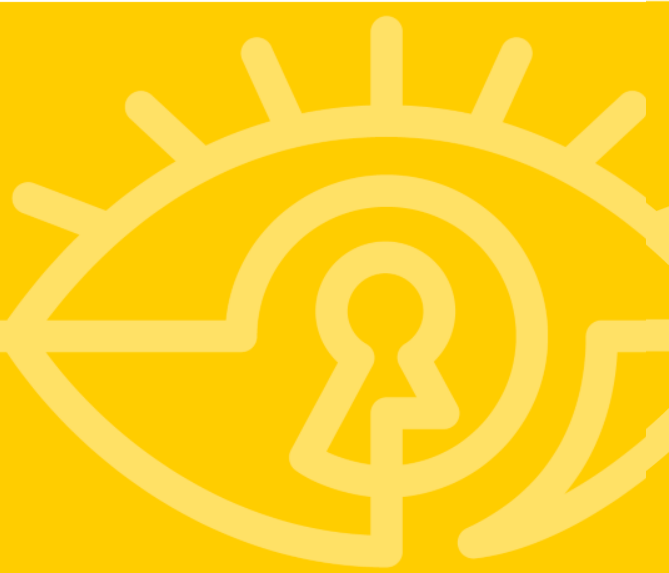


3rd Party Vendor Risk

Status	Ref #	Security Metric		Service Group	6-Month	Threshold
R	ENT-CR01	Third-party contracts w/o information security language	50%	Compliance Reporting		
R	ENT-CR02	Information security risks that are related to third-party relationships	N	Governance, Financials &		

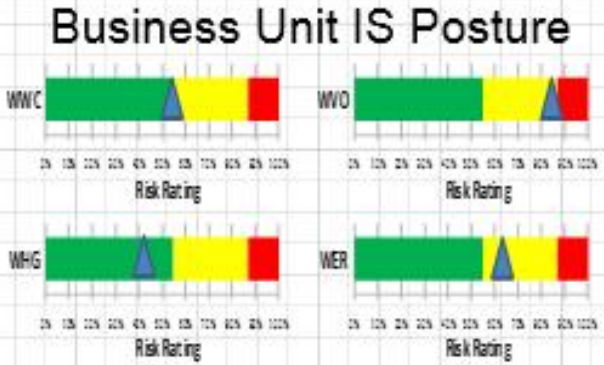
Dashboard

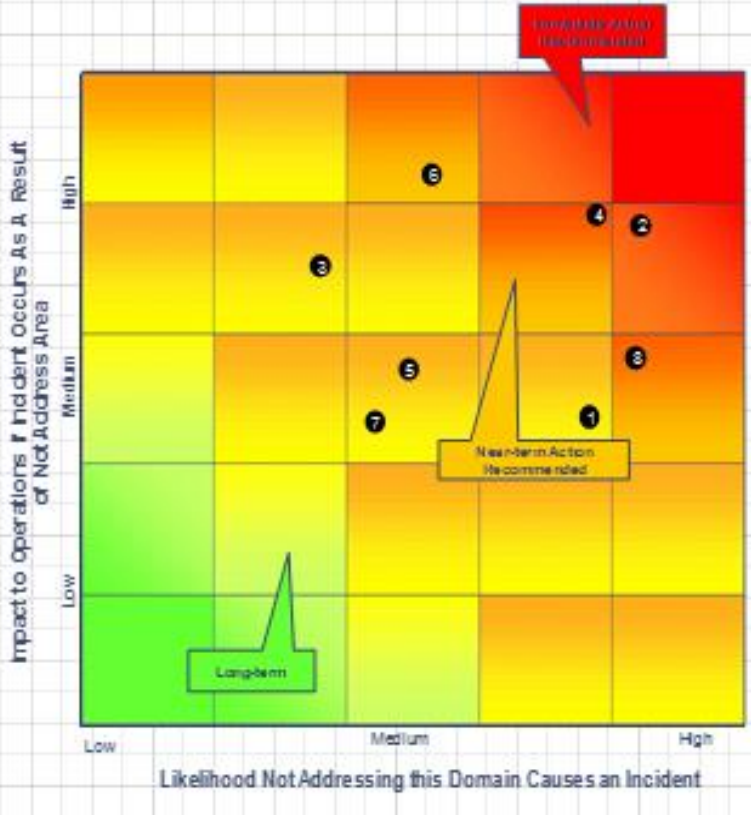

Information Security Executive Dashboard
Enterprise IS Posture
Business Unit IS Posture
Likelihood Not Addressing this Domain Causes an Incident
Compliance & Control
Data Protection
Infrastructure
Applications
Governance & Risk Managment
3rd Party Vendor Risk
Legal & Regulatory
Security Awareness & Education



Board Reports

Board Reports - Dashboard





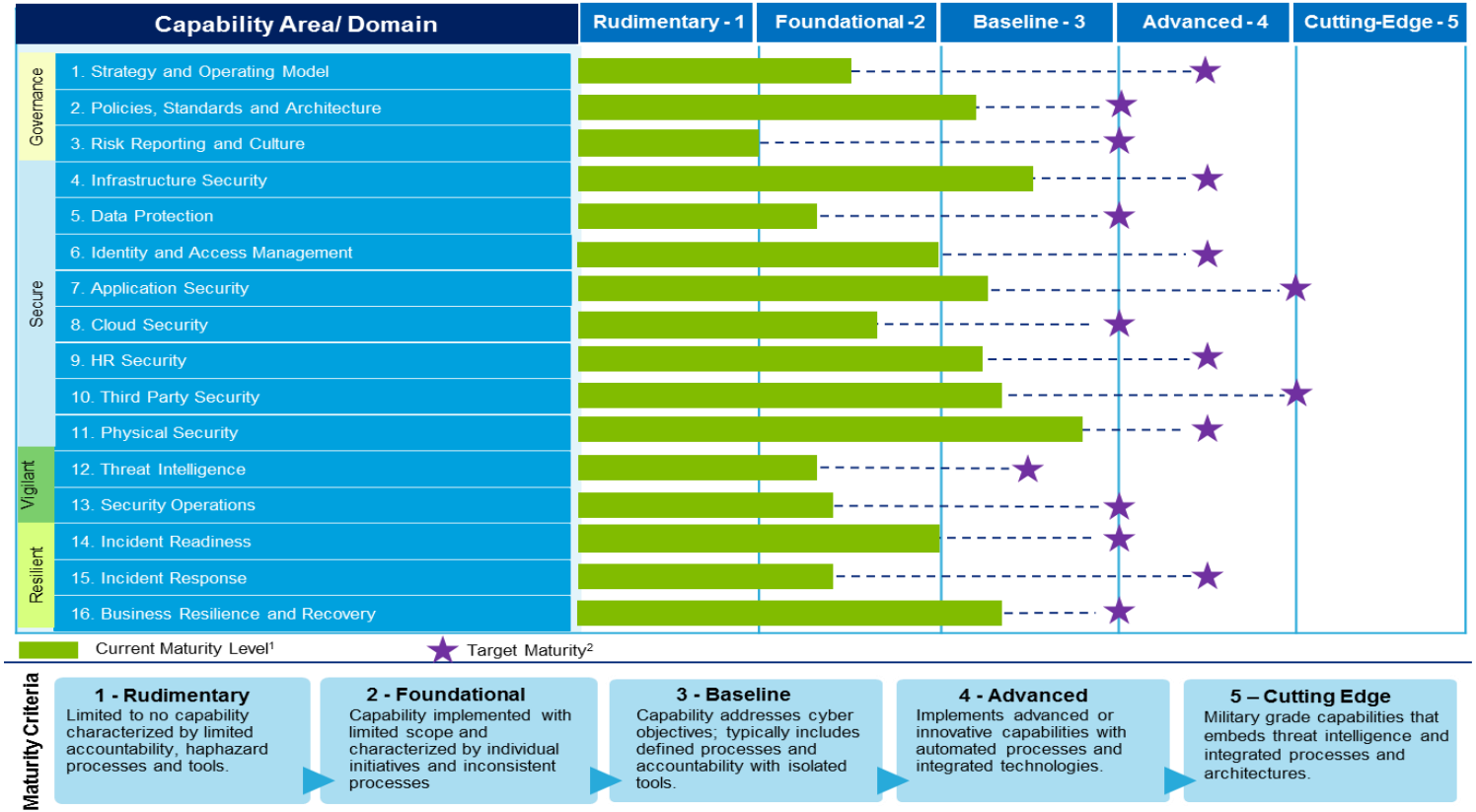
	Security Domain	Accountable Individual(s)
1	Compliance & Control	Jane Doe
2	Data Protection	Jane Doe
3	Infrastructure	Jane Doe
4	Applications	Jane Doe
5	Governance & Risk Management	Jane Doe
6	3rd Party Vendor Risk	Jane Doe
7	Legal & Regulatory	Jane Doe
8	Security Awareness & Education	Jane Doe

Board Reports - Dashboard

#	Key Cyber Risk Metrics	Risk Tolerance		Value				Trend
		Warning	Breach	Q1 2013	Q2 2013	Q3 2014	Q4 2014	
1	# of Severity 1 Cyber Risk Incidents	2	3	4	2	2	2	Steady
2	Financial Impact ($MM) Attributed to Severity 1 or 2 Incidents	$2.5	$5	$6.2	$3.5	$1.3	$1.8	Worse
3	# of Tier 1 Institutional Clients Impacted by a Severity 1 or 2 Incident	5	12	28	11	4	4	Steady
4	# of Retail Gold Clients Impacted by a Severity 1 or 2 Incident	50K	250K	0	0	18K	28K	Worse
5	Open Regulatory MRIAs, MRAs	3	10	8	7	6	5	Better
6	Open Severity 1 Audit Issues	5	8	9	8	6	6	Steady
7	# of Open High Risk Self-Identified Issues	5	10	3	3	3	4	Worse
8	# of Hours of Severe Service Degradation	10	20	18	11	15	9	Better
9	# of Key Open Cyber Risk Positions Not Filled within 120 Days	3	5	0	0	2	1	Better
10	% of Tier 2 Metrics that are Not Green	10	20	11	13	10	9	Better

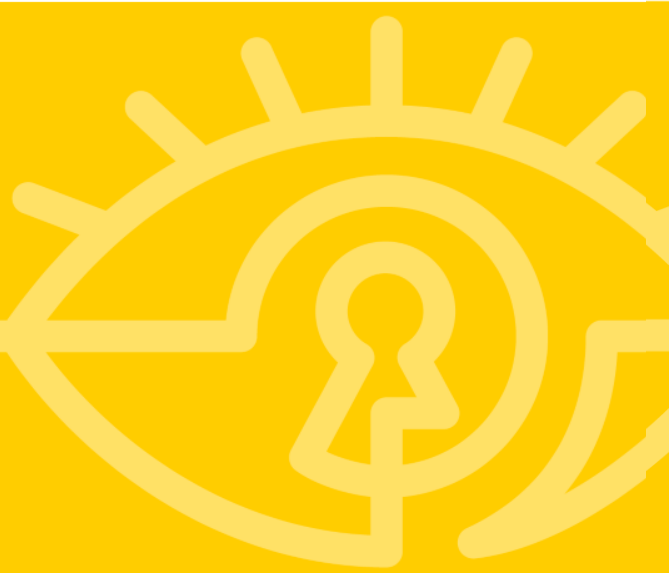
- Metrics within acceptable thresholds
- Metrics above threshold
- Metrics significantly above thresholds

Board Reports – Program Maturity



Board Reports - Measures

- Current threats to business
- Security program strategy
- Key trends in cybersecurity
- Performance against goals & objectives
- Exposure to key 3rd parties
- Spending vs. priorities
- Meeting internal standards
- Security initiatives supporting business objectives
- Management/staff experience
- Tracking key projects



Applying These Examples

Applying These Examples

- **Next week** you should:
  - Identify your audience, their concerns/values, and their language
  - Determine responsibility and accountability
  - Define the metrics that are important to your organization
  - *Start somewhere and improve as needed*

Applying These Examples (cont'd.)

- In the **first month** following this presentation you should:
  - Agree on what "Good" looks like
  - Determine data sources, availability, and repeatability
  - Develop the metrics, KPIs, and KRIs that best align with your objectives
- Within **six months** you should:
  - Design a package of reports for senior committees and the board
  - Determine reporting frequency