

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: GRC-F01

Do You Know Your Organization's Top 10 Security Risks?

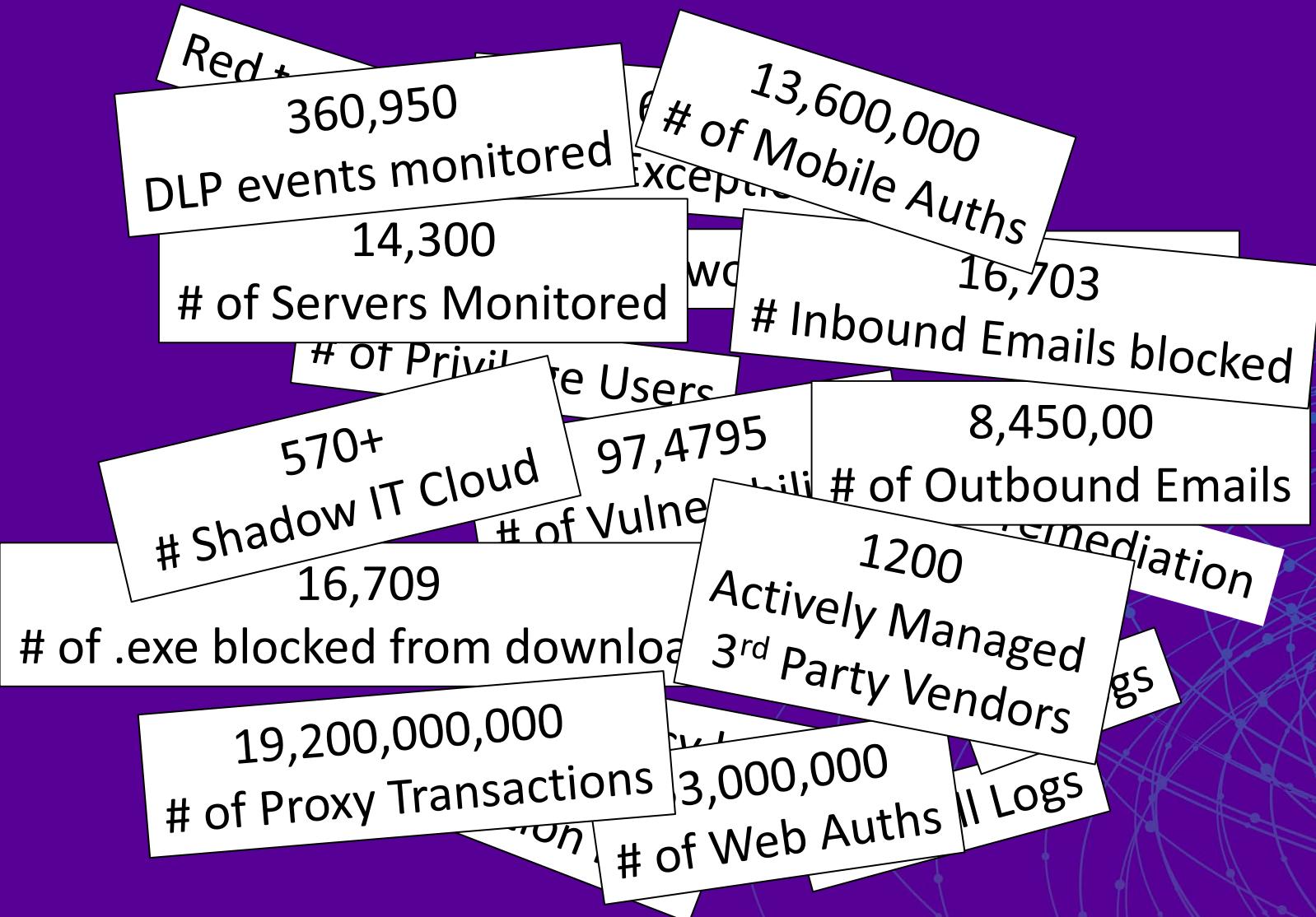
Min-Hwei Liu

Director, Information Security, Aetna



#RSAC

RSA® Conference 2019



What does the data tell you about your organization's Top Security Risks?



Agenda

Aetna's custom approach

- 5 Steps to identifying/determining Top 10 security risks
- Key factors to success and metrics
- Steps to kick off a similar program in your organization

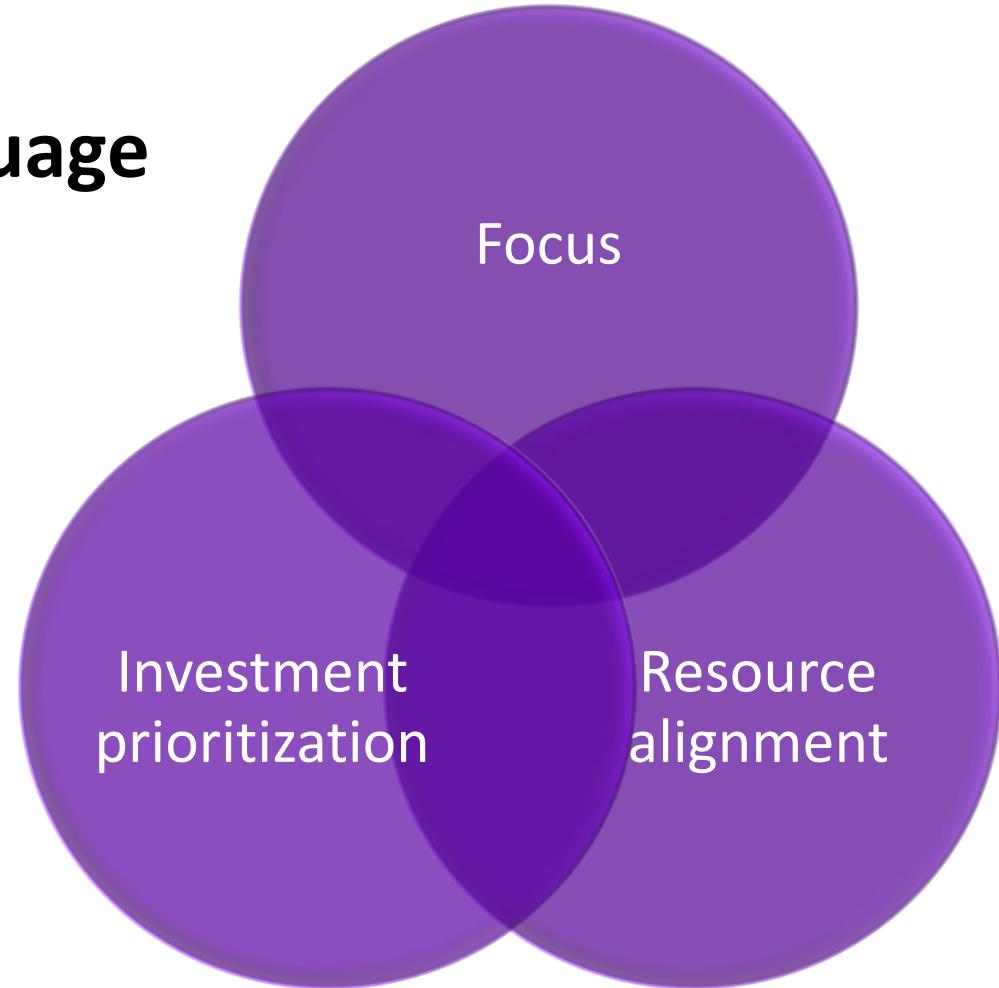


5 Steps to Identifying/Determining Top 10 Security Risks



5 Steps to Top 10 Security Risks

1. Establish a **governance process**
2. Define a **common security risk language**
3. Identify **risk input**
4. Transform **risk input**
5. **Prioritization**



1. Governance

Security Steering Committee, Enterprise Risk Management, Compliance, Internal/External Audit, etc.

Dedicated resources for governance

Security Leadership Team

Consistency is the key

Security Risk Owner

Establish a governance workflow

Security Risk Management

Review and monitor risks and related mitigation efforts

Provide metrics and analysis to Leadership Team

Upstream and downstream risk communication

Stakeholders, Affiliates, Third Party Partners, Employees

2. Common security risk language – security risk categories

Driven by Security framework(s)



- Frameworks (see Appendix A)
 - NIST 800–53 (Government)
 - COBIT (General)
 - ISO 27001 (Certificate)

Security Risk Categories

=

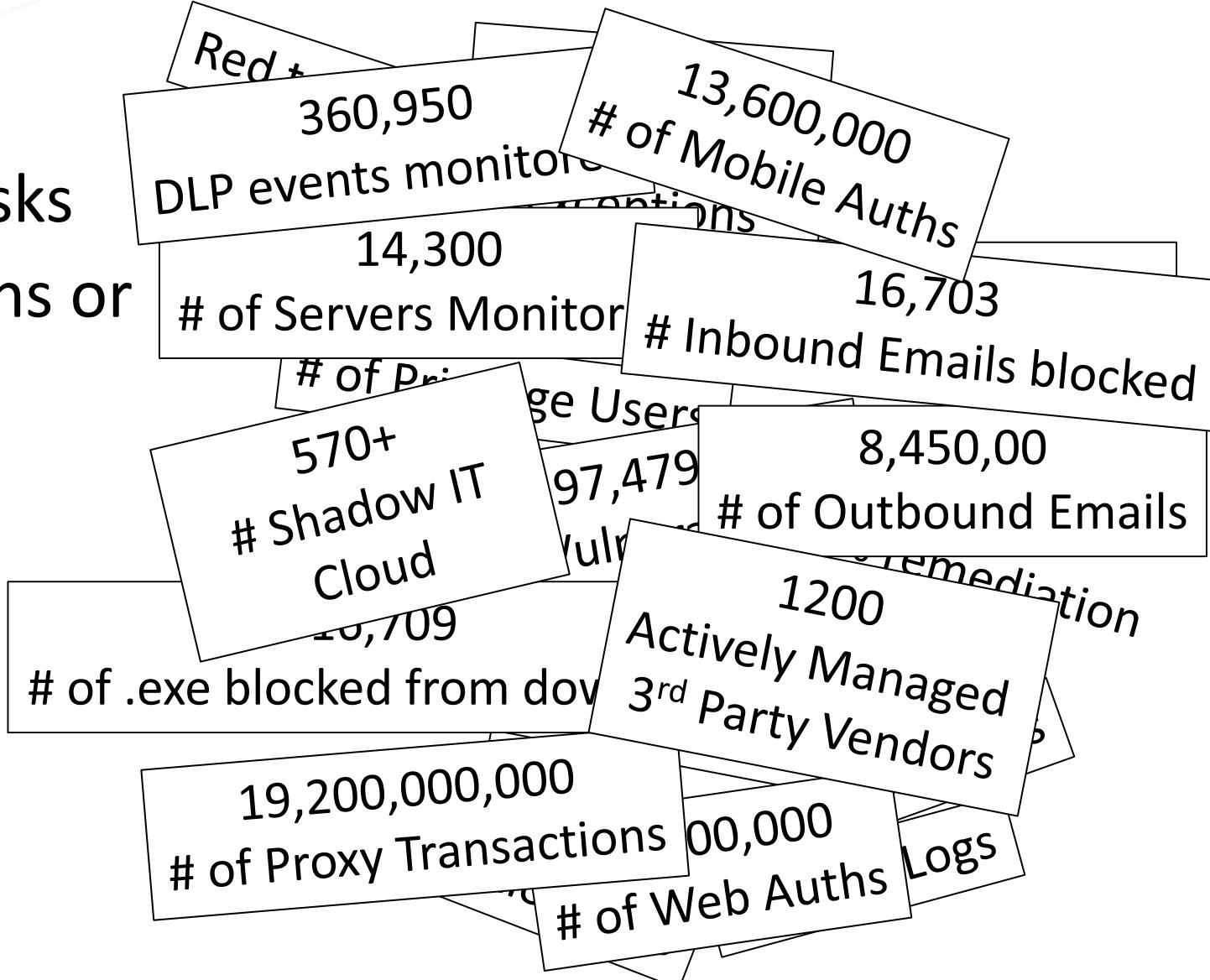
Family of control standards

2. Common security risk language – risk categories

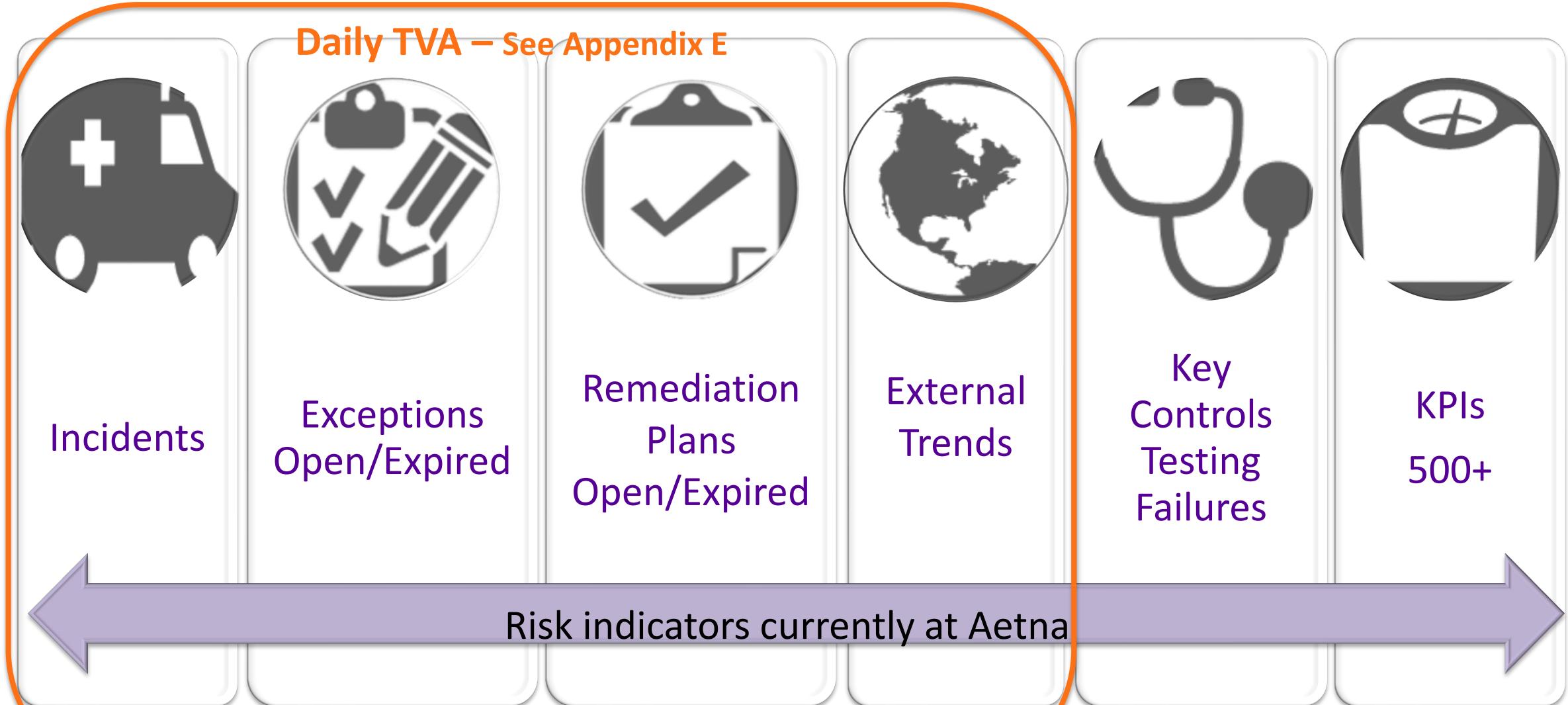
Aetna risk categories			
Access Management	Data Protection Management	Network & Communications Security	Security Intelligence
Audit and Accountability	Endpoint Protection	Personnel Security	Security Management
Business Continuity Management	Event, Incident, & Problem Management	Physical Security	Security Operations
Crisis Management	IT Hygiene	Risk Management	Software Security
16 high-level categories, 30 sub-categories – See Appendix B			

3. Risk input

- Indicators of Security Risks
- Risk Management Actions or Controls Activities
- External Trends



3. Risk input –your company's indicators of risks



3. Risk input– your company's control activities



Control
Standard
600+



Exceptions –
Closed



Remediation
Plans – Closed



KPIs
500+



Analytic
Models
300+

Control activities currently at Aetna

4. Transforming risk input - why and how?



Risk data are facts, numbers, evidence



Risk data trended and interpreted is
risk information



Risk information + insight/experience =
risk knowledge

(See Appendix A on Knowledge Management)

4. Transforming risk input – how? (see Appendix A)

Sources of risk input
Incidents
Key Controls Testing failure
Open/Expired/Closed Exceptions
Open/Expired/Closed Remediation Plans
of Control Standards
of KPIs
Data Analytics Models



Aetna - risk categories			
Access Mgmt.	Data Protection Mgmt.	Network & Comm. Security	Security Intelligence
Audit and Accountability	Endpoint Protection	Personnel Security	Security Mgmt.
Business Continuity Mgmt.	Event, Incident, & Problem Mgmt.	Physical Security	Security Operations
Crisis Mgmt.	IT Hygiene	Risk Mgmt.	Software Security

4. Transforming risk input – example

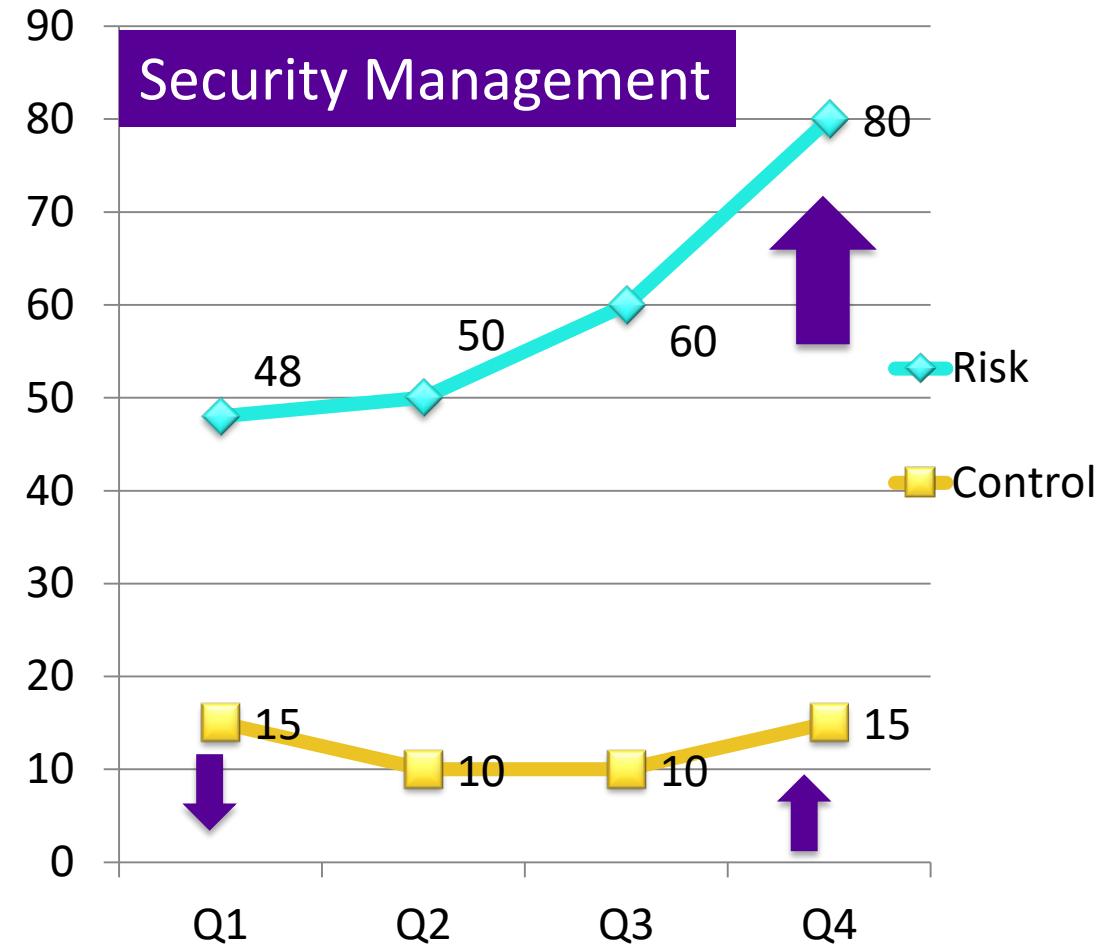
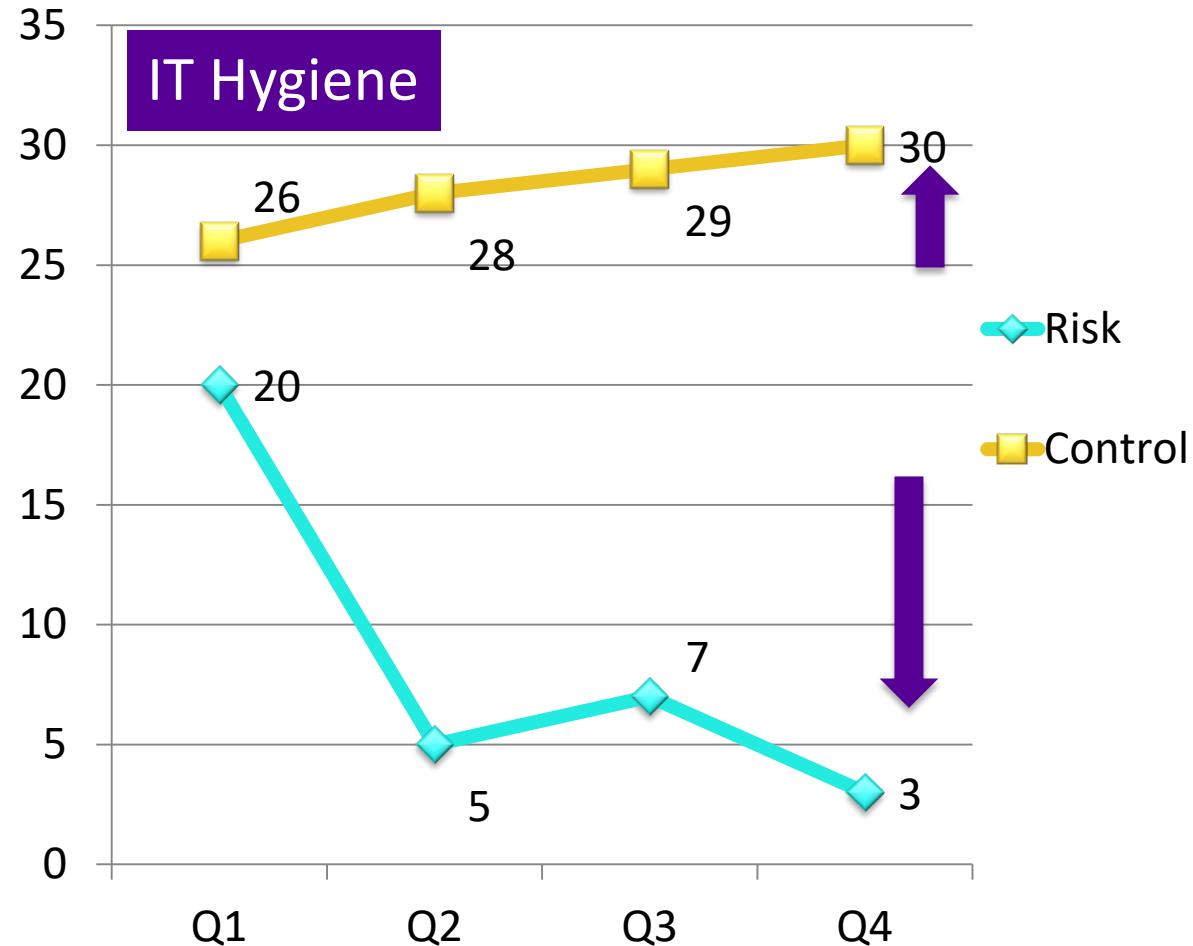
Illustrative Only

Risk Input	Security Risk Category				
	Access Mgmt.	Data Protection Mgmt.	IT Hygiene	Network and Comm. Security	Security Mgmt.
Incidents	5	3	7	1	25
Key Controls Testing Failures	0	0	3	1	8
Open/Expired Exceptions	10	20	1	1	5
Open/Expired Remediation plans	5	15	4	0	10
# of Control Standards	1	4	2	3	0
# of KPIs	4	3	2	3	0
Closed Exceptions	5	15	3	5	10
Closed Remediation Plan	10	2	20	2	5
Data Analytics Models	5	5	1	1	0
Projects Closed	1	1	2	0	0

4. Transforming risk input

Illustrative Only

Hypothesis and deeper dive



5. Prioritization (see Appendix C)

Impact	
Critical (5)	>\$10M loss; >10% market share loss Loss of executive life Severe impact on reputation/brand/member Severe/catastrophic harm to individuals Severe degradation operational performance. >7.5% of member accounts affected.
	\$5M - \$10M loss; 7-10% market share loss Significant impact on reputation/brand/member Long-term negative media coverage Severe/catastrophic harm to individuals Severe degradation in mission capability 5% of member accounts affected
	\$1M - \$5M loss Some impact on reputation/brand/member National short-term negative media coverage Significant harm to individuals Significant degradation in mission 2.5% of overall member accounts affected
	\$500k - \$1M loss Limited impact on reputation/brand/member. Minor harm to individuals. Limited impact on operations 1-2.5% of all member accounts affected
	<\$500k financial loss No reputational/brand/member damage Negligible adverse effect on operations <1% of all member accounts affected

Likelihood	
Almost Certain (5)	> 75% chance of occurring Sophisticated adversary almost certain to initiate. Error, accident > 49 times a year
Probable (4)	50-75% chance of occurring Sophisticated adversary highly likely to initiate Error, accident 24-49 times a year
Possible (3)	25-50% chance of occurring Less sophisticated adversary likely to initiate Error, accident 12-23 times a year
Unlikely (2)	<25% chance of occurring Unsophisticated threat actor unlikely to initiate Error, accident 3-14 times a year
Rare (1)	<5% chance of occurring Unsophisticated adversary unlikely to initiate Error, accident 1-2 times a year

Control Effectiveness	
Mostly Ineffective (1)	< 10% of the population
Rarely Effective (0.8)	10-20% of the population
Ocasionally Effective (0.6)	21-50% of the population
Mostly Effective (0.4)	51-75% of the population
Highly Effective (0.2)	75% of the population

Priority Risk Score :
 $(((\text{Impact} + \text{Likelihood})/2) * \text{Control Effectiveness})$

5. Prioritization example

Illustrative Only

Risk Category	Q4 Risk	Q4 Control Effectiveness	Q4 Residual Risk
Access Management	3	0.4	1.2
Data Protection Management	3	0.6	1.8*
IT Hygiene	4	0.4	1.6*
Network and Communications Security	3	0.2	0.6
Security Management	4	0.6	2.4*

5. Security risks example – Deeper dive

Illustrative Only

Security Risks	Q4 Risk	Q4 Risk Management	Q4 Residual Risk
Security Management – vendor/3 rd party security governance	4	0.6	2.4
Data Protection – data protection program among vendors/3 rd parties	3	0.6	1.8
IT Hygiene – asset integration from newly acquired company	4	0.4	1.6

Now Create

(See Appendix D)

- Quarterly Top 10 Security Risk Review Including
 - Top 10 security risks supported by
 - Aggregated data and trends with
 - Risk scoring for each Top 10 Risk, adding
 - Company insight + experience to
 - Prioritize top security risks, and
 - Emerging risk discussion
- Communicate, communicate, communicate



RSA®Conference2019

Key Factors to Success and Metrics



Key Factors to Success

- Senior leadership buy-in
- Dedicated resources
- Consistent language of risk
- Educate, educate, educate
- Automate, automate, automate



Key Metrics

Existing

- # of risk inputs with embedded risk categories
- Risk score by Top Security Risks

Future - Formal and more granular

- Risk score by Security Risk Categories
- Emerging Risk Insight by Security Risk Categories

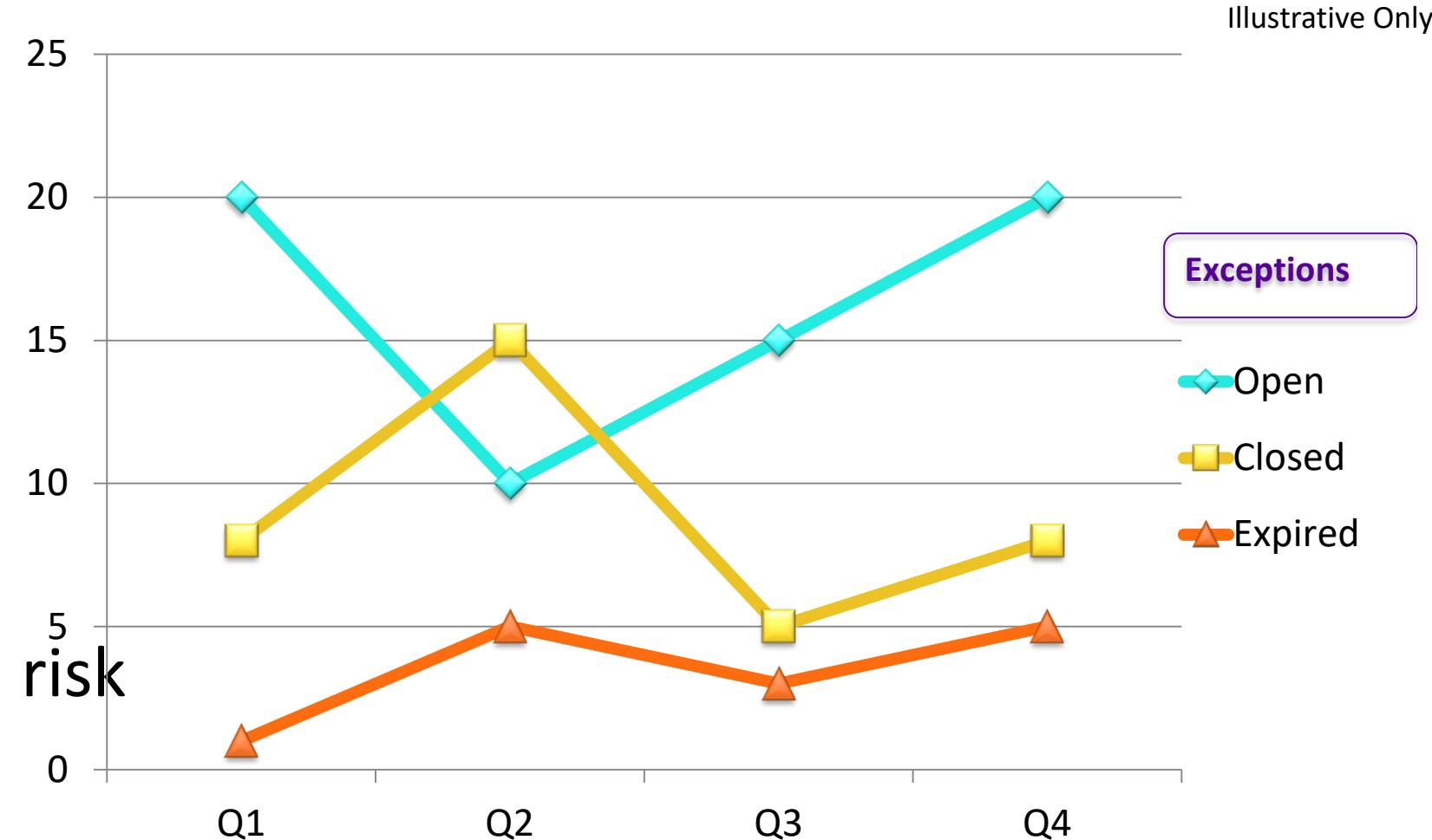


**Steps to kick off a similar Program in
your organization**

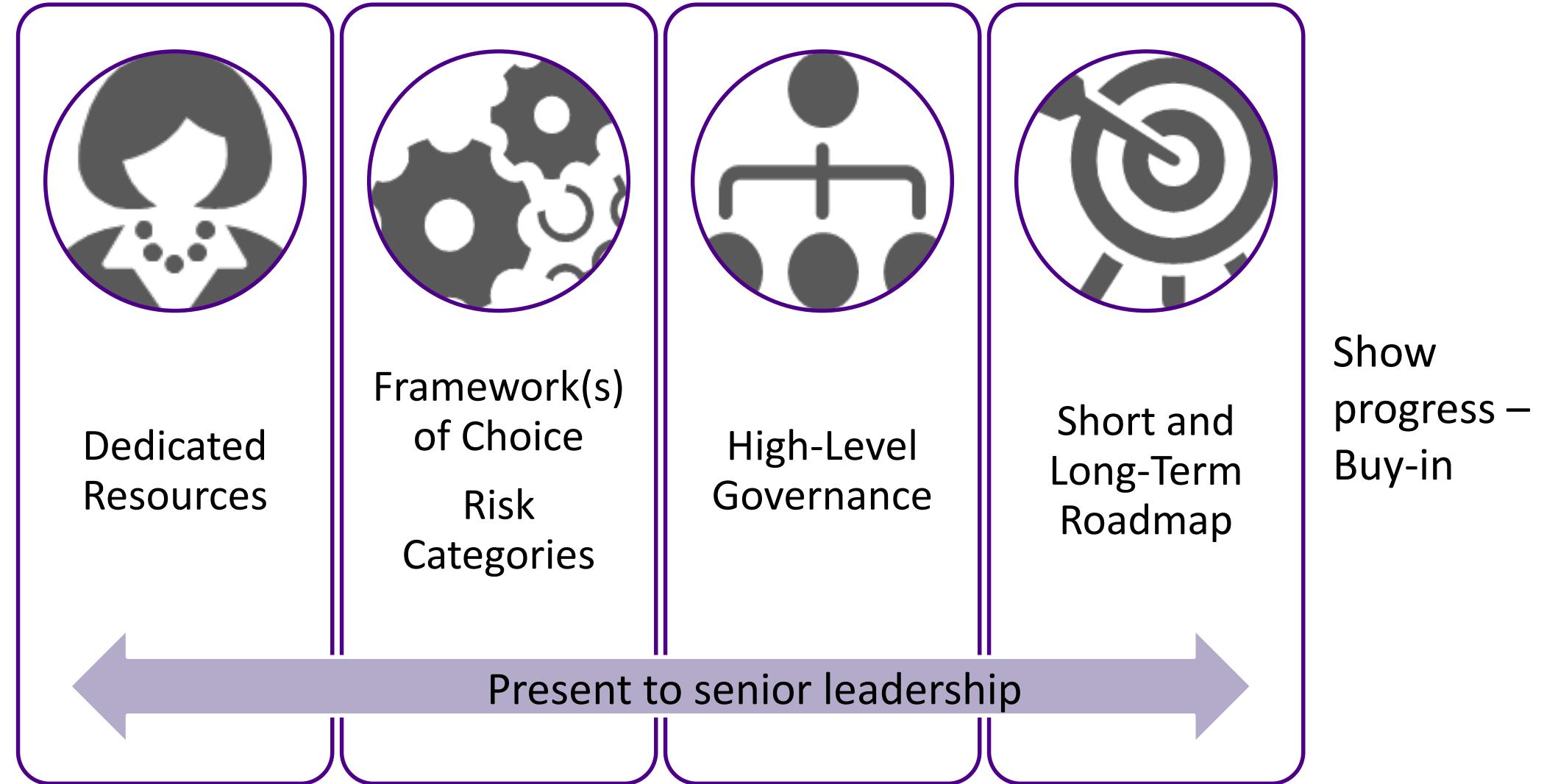


Apply: Next Week – determine what you already have

- Input
 - Measurements
 - metrics or
 - Key Performance Indicators
- Risk Trends
- Reporting (risk and risk management)



Apply: First three months



Apply: within six months

- Align risk categories to risk input (could lengthy)
- Educate, educate, educate
 - Owners of risk inputs
 - Contributors to risk input
- Report and determine improvement opportunities (e.g., automation)
- Repeat with the cycle

Questions?



Min-Hwei Liu

Minhwei.liu@aetna.com

860-273-3481

Appendix A

Additional Resources

Resources

NIST 800-53

- <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

COBIT 5

- <https://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>
- <https://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/>
- <http://www.isaca.org/cobit/pages/info-sec.aspx>

ISO 27001

- <https://www.iso.org/isoiec-27001-information-security.html>
- <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>

Resources

Knowledge Management

- <https://searchdatamanagement.techtarget.com/feature/Defining-data-information-and-knowledge>
- <http://www.knowledge-management-tools.net/knowledge-information-data.html>

Other good resources about Security Risk Management

- New York DFS Cybersecurity
<https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>

Transforming risk input - example

Illustrative Only

Data ?

- 150,000 events seen in DLP daily
- 1,000,000,000 of transactions logged at Web Proxy daily
- 300 applications containing the crown jewels

Information ?

- 60% of DLP events pertain to Third Parties/Vendors
- 89% of applications with crown jewels have no security defects
- 3 websites of risk score 7 or higher are blocked in June

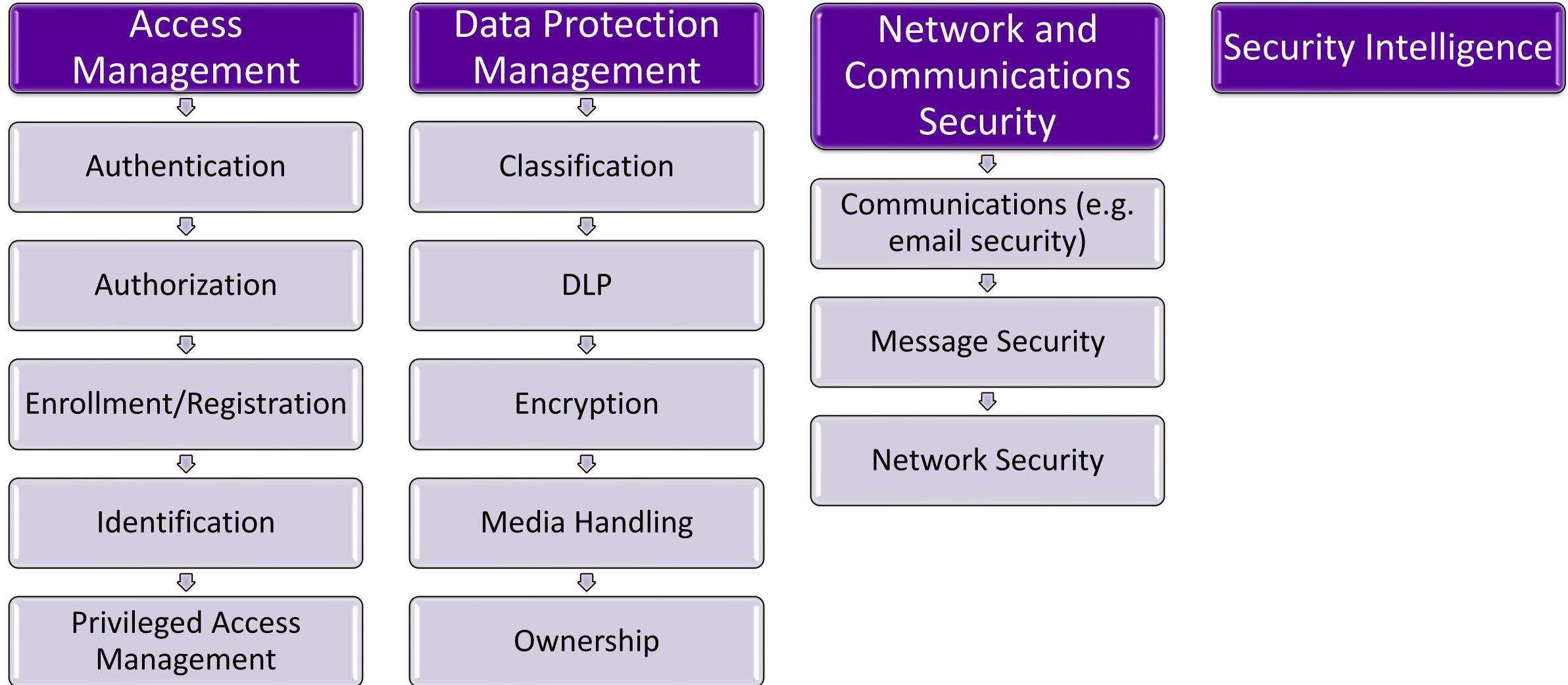
Knowledge ?

- Increased third party vendor use of cloud
- Active exchange of crown jewel data via email

Appendix B

Aetna Security Risk Categories - Subcategories

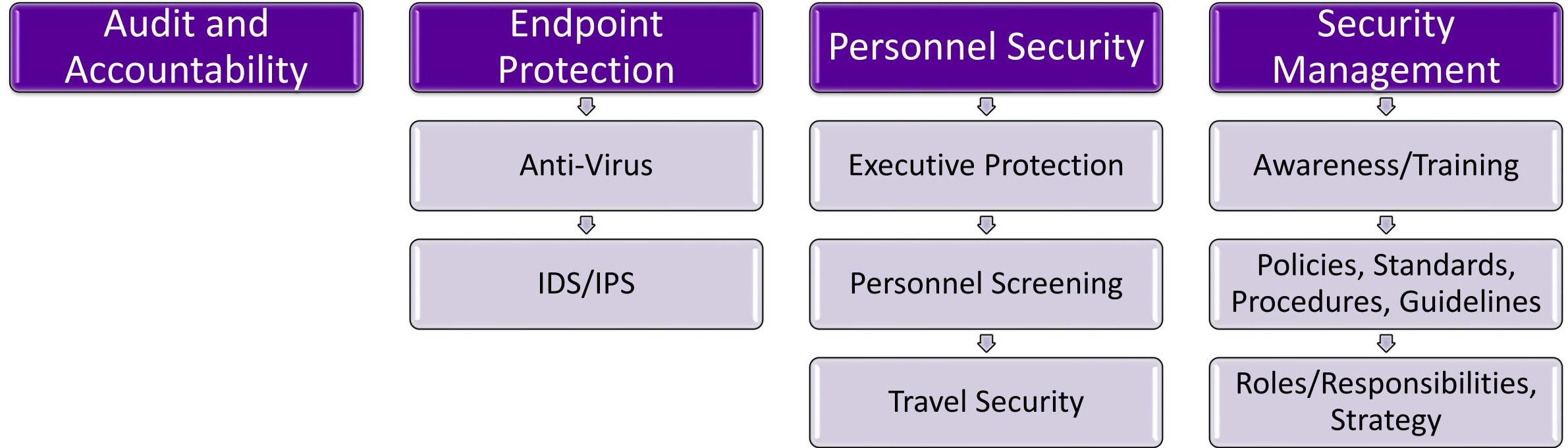
Common Risk Language - Security Risk Subcategories



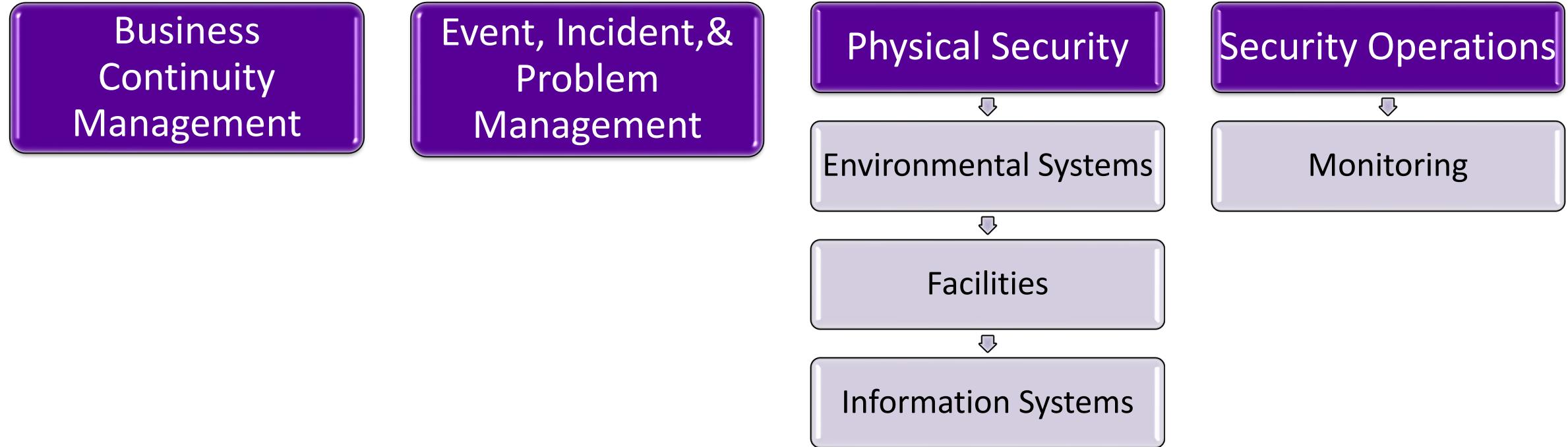
Risk Category definitions

Access Management	Authorization and authentication of personnel prior to granting them access to information resources.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Decision given to authorize a user, process, or device based on an agreed-upon set of security controls.
Enrollment / Registration	The enrollment process is based on a set of policies or is manually controlled by the owner of the resource.
Identification	Creation, management, and deletion of identities without regard to access or entitlements.
Privileged Access Management	The management of the processes to control/monitor a user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform.

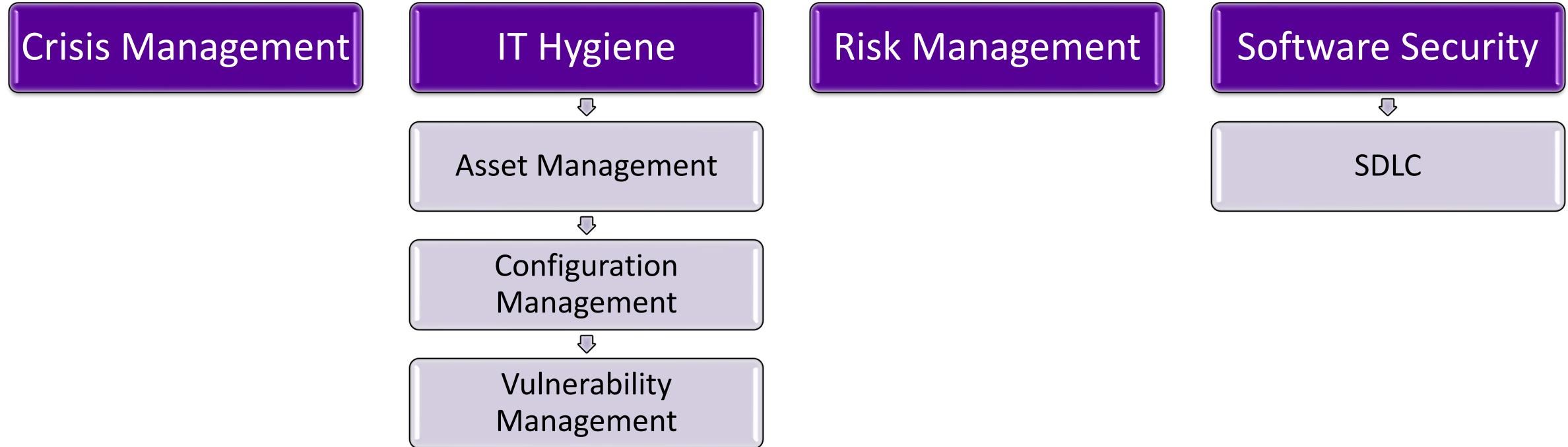
Common Risk Language – Security Risk Subcategories



Common Risk Language - Security Risk Subcategories



Common Risk Language - Security Risk Subcategories



Appendix C

Risk Scoring

Risk Scoring References

- OWASP -
[https://www.owasp.org/index.php/OWASP Risk Rating Methodology#Step 2: Factors for Estimating Likelihood](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood)
- NIST - [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview/security-categorization](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview/security-categorization)

Prioritization

Global Security Risk Scoring Tool

Impact	Likelihood	Control Effectiveness
<input checked="" type="radio"/> Critical (5)	<input checked="" type="radio"/> Almost Certain (5)	<input type="radio"/> No controls in place or mostly ineffective (1.0)
<input type="radio"/> High (4)	<input type="radio"/> Probable (4)	<input type="radio"/> Controls are rarely effective (0.8)
<input type="radio"/> Medium (3)	<input type="radio"/> Possible (3)	<input type="radio"/> Controls are effective on some occasions (0.6)
<input type="radio"/> Low (2)	<input type="radio"/> Unlikely (2)	<input type="radio"/> Controls effective on most occasions (0.4)
<input type="radio"/> Very Low (1)	<input type="radio"/> Rare (1)	<input checked="" type="radio"/> Controls are highly effective (0.2)

Inherent Risk - 5.0

$$(\text{Impact} + \text{Likelihood})/2 = (5+5)/2 = 5$$

Residual Risk – 1.0

$$\text{Inherent Risk} * \text{Control Effectiveness} = 5 * 0.2 = 1$$

Risk Scoring

Impact	
Critical (5)	>\$10M loss; >10% market share loss Loss of executive life Severe impact on reputation/brand/member Severe/catastrophic harm to individuals Severe degradation operational performance. >7.5% of member accounts affected.
	\$5M - \$10M loss; 7-10% market share loss Significant impact on reputation/brand/member Long-term negative media coverage Severe/catastrophic harm to individuals Severe degradation in mission capability 5% of member accounts affected
	\$1M - \$5M loss Some impact on reputation/brand/member National short-term negative media coverage Significant harm to individuals Significant degradation in mission 2.5% of overall member accounts affected
	\$500k - \$1M loss Limited impact on reputation/brand/member. Minor harm to individuals. Limited impact on operations 1-2.5% of all member accounts affected
	<\$500k financial loss No reputational/brand/member damage Negligible adverse effect on operations <1% of all member accounts affected

Likelihood	
Almost Certain (5)	> 75% chance of occurring Sophisticated adversary almost certain to initiate. Error, accident > 49 times a year
Probable (4)	50-75% chance of occurring Sophisticated adversary highly likely to initiate Error, accident 24-49 times a year
Possible (3)	25-50% chance of occurring Less sophisticated adversary likely to initiate Error, accident 12-23 times a year
Unlikely (2)	<25% chance of occurring Unsophisticated threat actor unlikely to initiate Error, accident 3-14 times a year
Rare (1)	<5% chance of occurring Unsophisticated adversary unlikely to initiate Error, accident 1-2 times a year

Control Effectiveness	
Mostly Ineffective (1)	< 10% of the population
Rarely Effective (0.8)	10-20% of the population
Ocasionally Effective (0.6)	21-50% of the population
Mostly Effective (0.4)	51-75% of the population
Highly Effective (0.2)	75% of the population

Top security risks - example

Illustrative Only

Risk: Use of third parties to host data and provide cloud services.

Impact: Critical (5) -

- Severe impact to member and reputation
- Severe degradation in mission, not able to perform primary function

Likelihood: Almost Certain (5) –

- Impacting factors outside the control of the organization
- Complex internal process with minimal checks and balances

Known Mitigations - Control Effectiveness (0.4) = Controls are mostly effective

- Third-Party Penetration Testing
- Tiered Security Assessments
- Third-Party Security Controls
- Annual Aetna Global Security Third-Party Conference

Inherent Risk = (5+5) / 2 = 5.0 (Critical)

Residual Risk = 5.0 * 0.4 = 2.0 (Low-Medium)

Appendix D

Quarterly Top Security Risks

Q4



Current Top Security Risks

Illustrative Only

Risk Themes	Impact	Likelihood	Inherent Risk	Control Effectiveness	Residual Risk	
1. Use of third parties to host data and provide cloud services	Medium (3)	Almost Certain (5)	High	Mostly Ineffective (1.0)	4	High
2. Asset inventory is not complete	Critical (5)	Almost Certain (5)	Critical	Occasionally Effective (0.6)	3	Medium
3. Handling of sensitive data within business processes	Critical (5)	Almost Certain (5)	Critical	Occasionally Effective (0.6)	3	Medium

Current Top Security Risks – illustration only

Illustrative Only

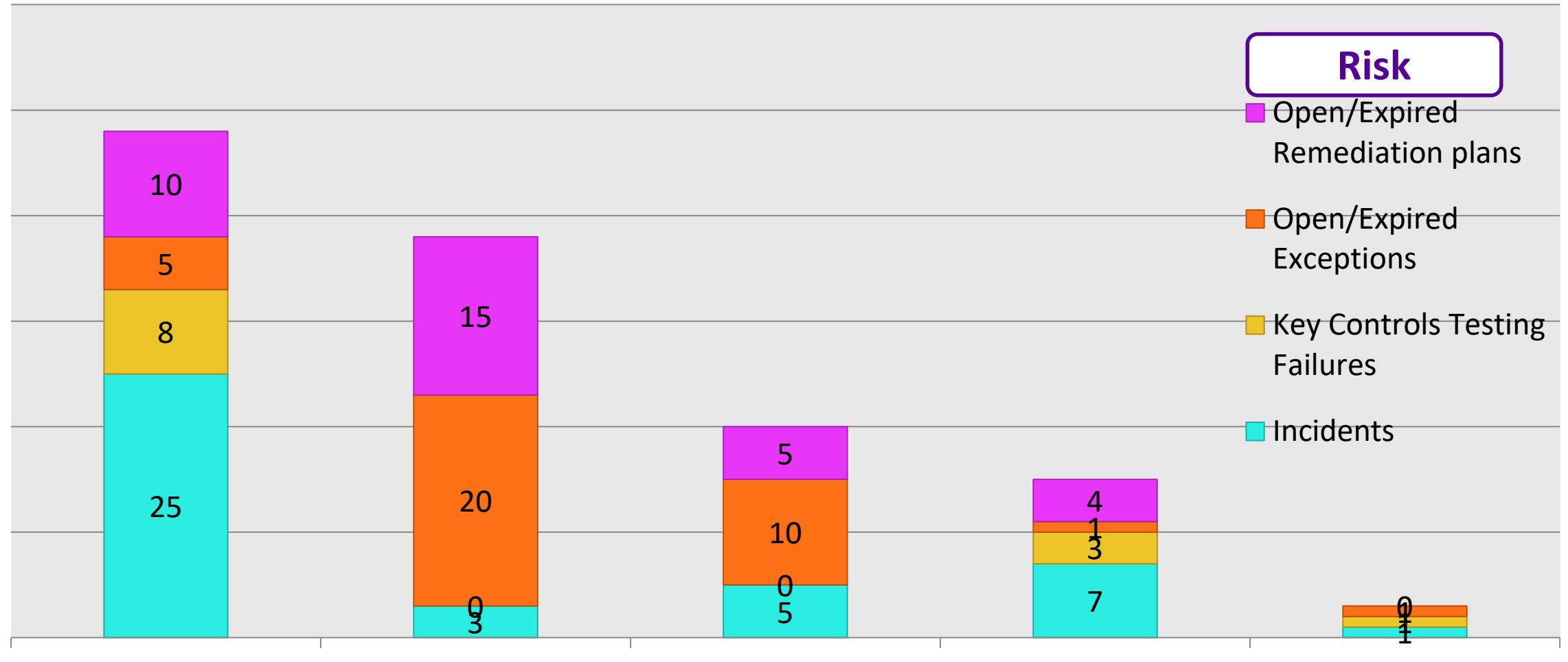
Top Security Risks			Risk	Inputs		Control Inputs						
Q4	Incidents	Key Controls Testing Failures	Open and Expired Exceptions	Open and Expired Remediation plans	Control Standards	KPIs	Closed Exceptions	Closed Remediation Plan	Data Analytics Models	Projects Closed		
1. Use of third parties to host data and provide cloud services	25	8	5	10	0	0	10	5	0	0		
2. Asset inventory is not complete	3	0	20	15	4	3	15	2	5	1		
3. Handling of sensitive data within business processes	5	0	10	5	1	4	5	10	5	1		

Emerging Risk/Risk Categories

Illustrative Only

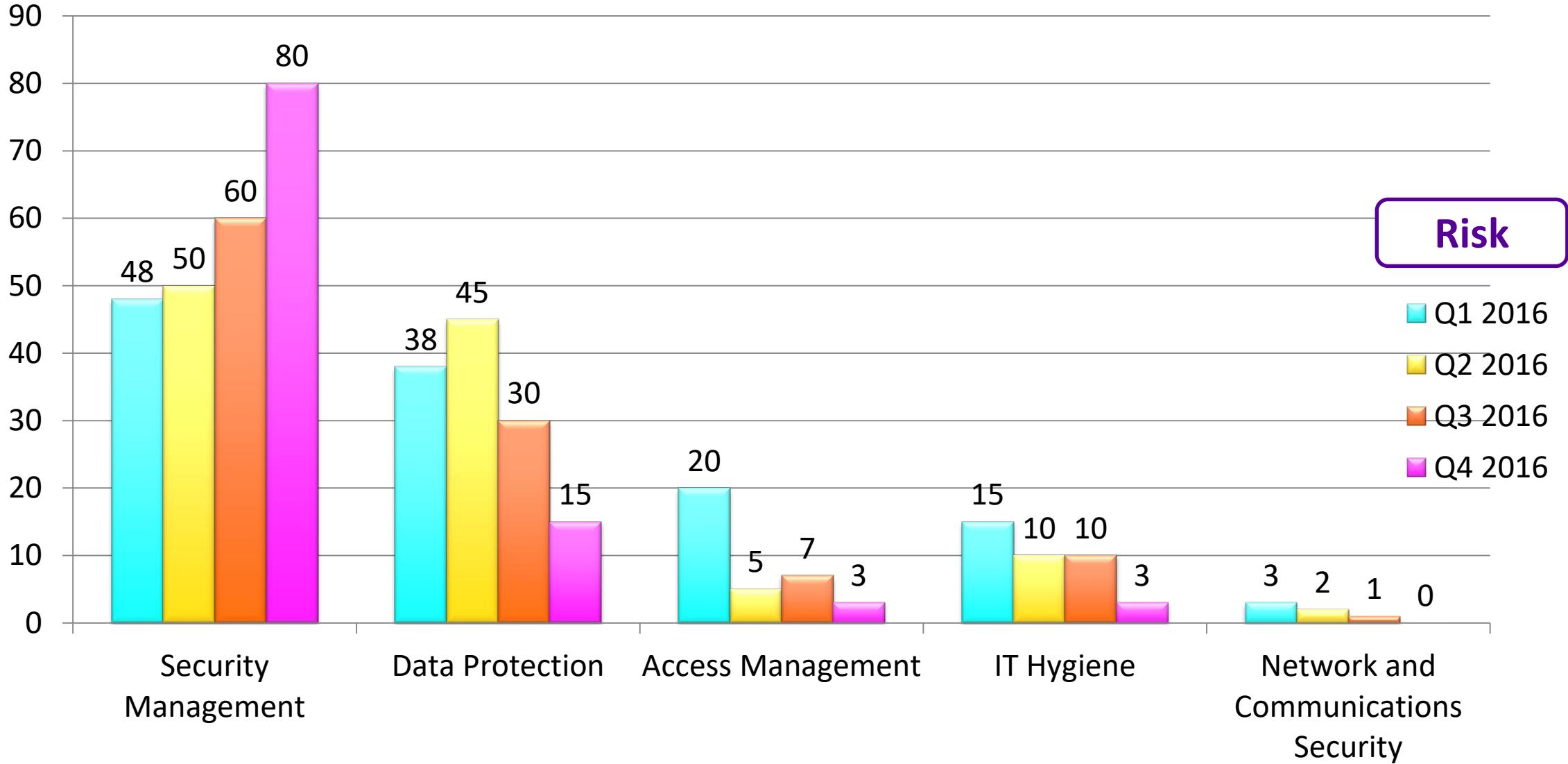
Risk Category	Risk Inputs					Control Inputs					
	Incidents	Key Controls Testing Failures	Open and Expired Exceptions	Open and Expired Remediation plans	Control Standards	KPIs	Closed Exceptions	Closed Remediation Plan	Data Analytics Models	Projects Closed	
Q4											
Security Management	25	8	5	10	0	0	10	5	0	0	
Data Protection Management	3	0	20	15	4	3	15	2	5	1	
Access Management	5	0	10	5	1	4	5	10	5	1	
IT Hygiene	7	3	1	4	2	2	3	20	1	2	
Network and Communications Security	1	1	1	0	3	3	5	2	1	0	

Emerging Risk Categories – Q4 2016 view



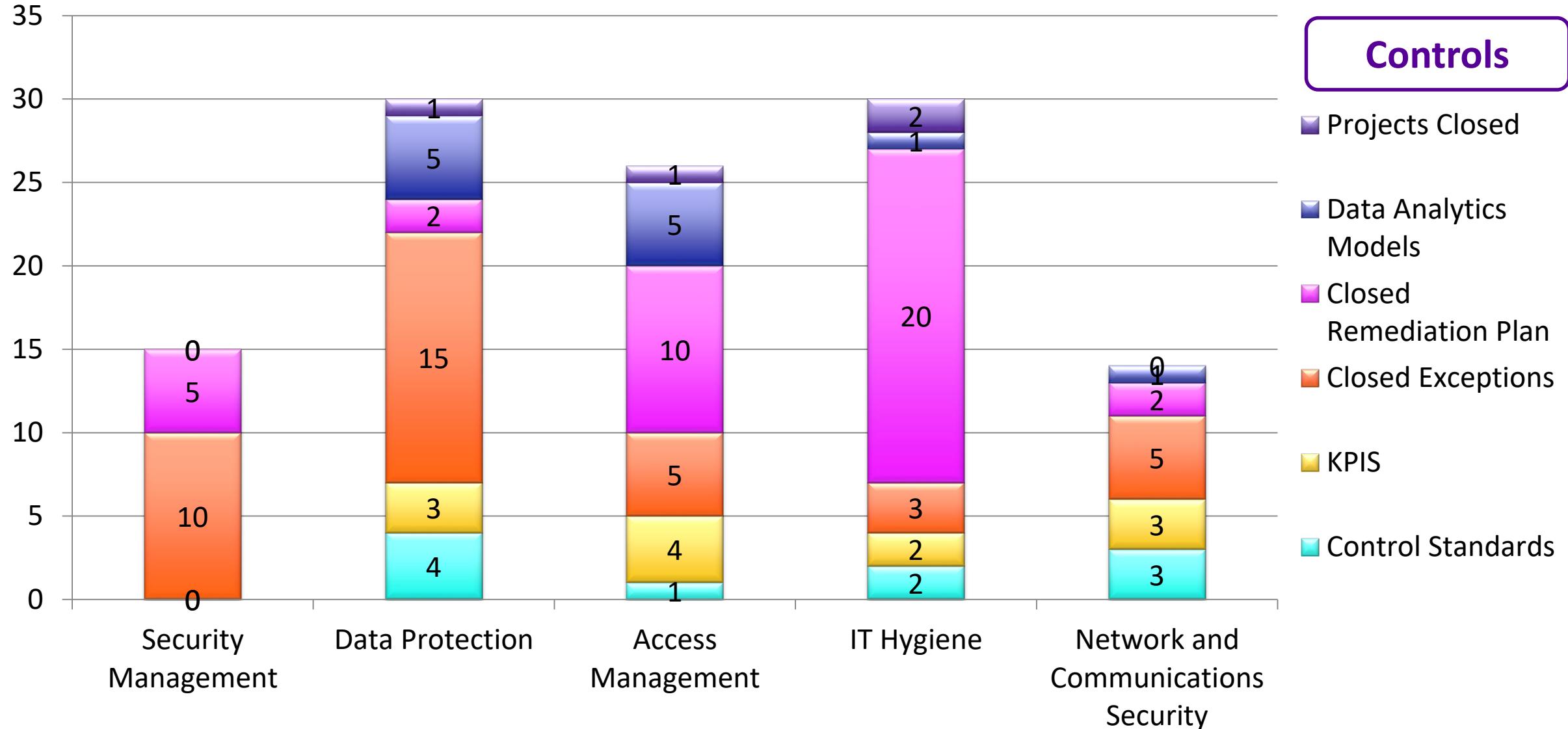
Emerging Risk Categories – Quarterly view

Illustrative Only



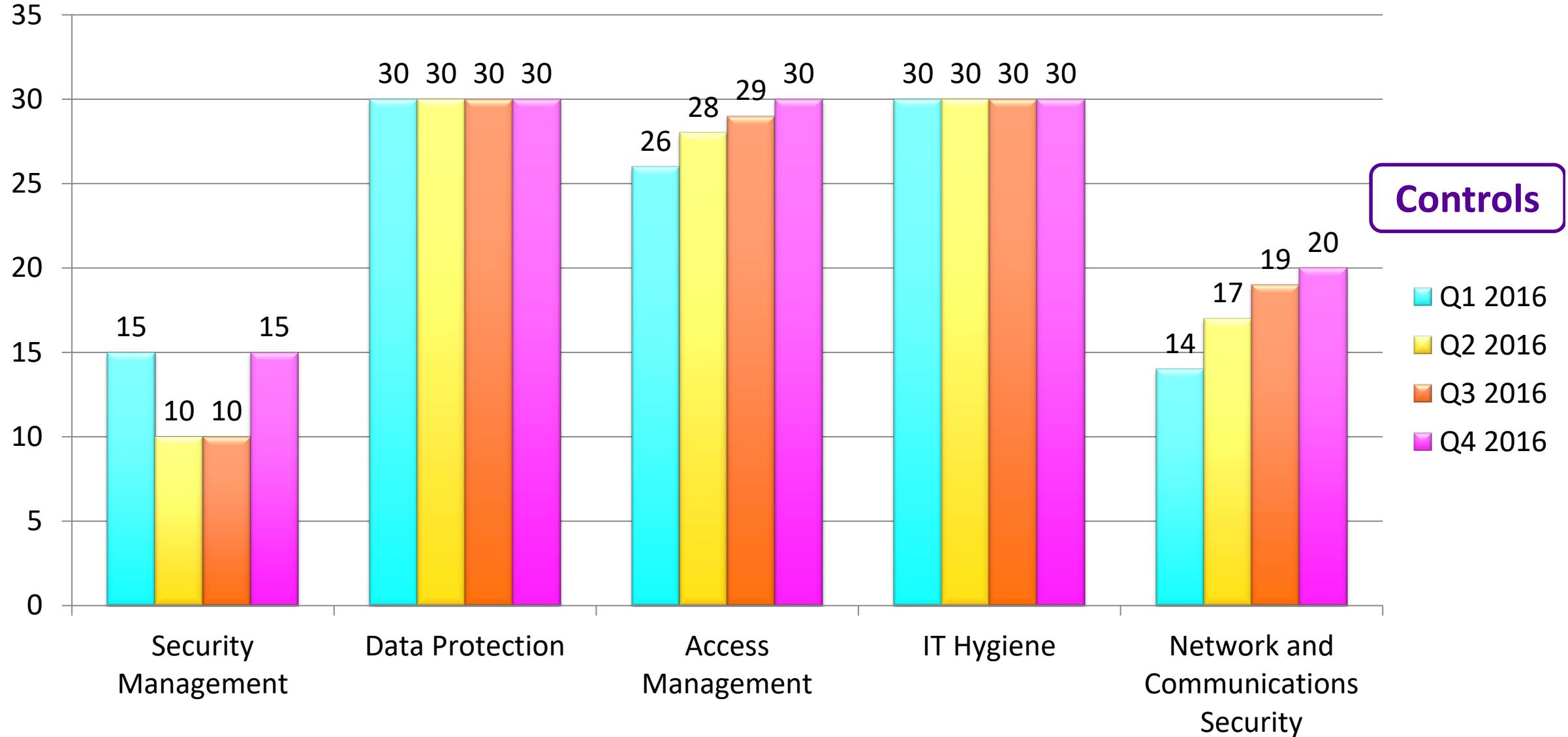
Emerging Risk Categories – Q4 2016 view

Illustrative Only



Emerging Risk Categories – Quarterly view

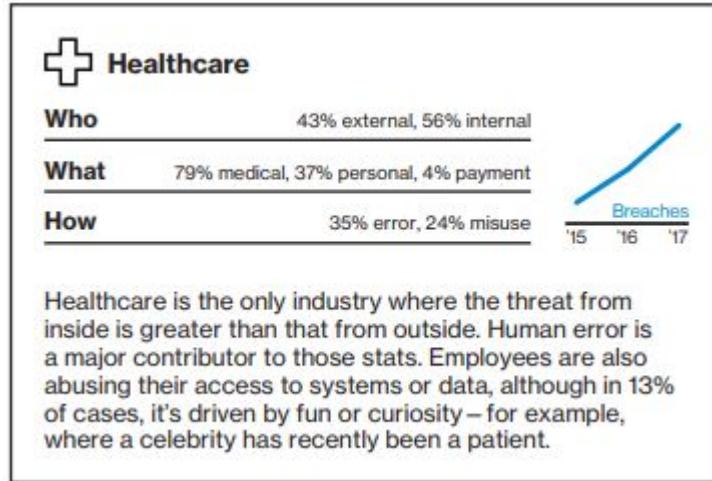
Illustrative Only



Emerging Risk - External Trends Example

Illustrative Only

Healthcare Insider Threats



"Verizon 2018 DBIR" produced by verizon.com

Evolution of Ransomware:

- Used in completely opportunistic attacks affecting individuals' home computers as well as targeted strikes against organizations
- Attempted with little risk or cost to the adversary involved
- Successful with no reliance on having to monetize stolen data
- Deployed across numerous devices in organizations to inflict bigger impacts and thus command bigger ransoms

Discussion points

Example only

Illustrative Only

- 3rd Party/Vendor Management continues to be a leading risk/Top Security risks
- Significant risk management activities on data protection with reduction of risk events.
 - Should this remain a Top 10 Security risk?
- New Emerging risk.....

RSA®Conference2019

Appendix E

Daily TVA



Threat Vulnerability Assessment (TVA) Categories

Input Category	Purpose	Sources
Security Incidents	Review of open security events and incidents requiring corrective actions or remediation plans.	<ul style="list-style-type: none"> Cyber Incidents, tracked via the eGRC Incident Response
Cyber Threat Fusion Center	Monitor and inspect inbound activity for suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.	<ul style="list-style-type: none"> Network IDS Endpoint Malware Detection Phishing Detection
Inside-Out Analysis	Monitor and inspect outbound activity for suspicious or anomalous behavior that may indicate a compromised device or malicious insider.	<ul style="list-style-type: none"> Proxy alerts Data Loss Prevention Enterprise Cloud Risk Usage
Physical Security	Review inputs from Physical Security for potential IT Security impact, including security incident, business disruptions, and world events.	<ul style="list-style-type: none"> Weather Business Continuity Physical on premise incidents Geopolitical events
External Trends	A review of external cyber threats that impact Aetna's threat landscape including brand protection, malware, non-Aetna data breaches, and other threat intelligence items.	<ul style="list-style-type: none"> Commercial Intelligence Industry Sharing Intelligence
Infrastructure	Review infrastructure vulnerabilities and other threats impacting infrastructure health	<ul style="list-style-type: none"> System Patching Vulnerability exploits Infrastructure control gaps
Applications	A review of Application vulnerability remediation tools and processes	<ul style="list-style-type: none"> Vulnerabilities in prod (dynamic) Vulnerabilities in build (static) Application attacks Botnet defense
Internal Composite	A review of internal events impacting Aetna's risk posture.	<ul style="list-style-type: none"> Risk exceptions UBA Workforce Analytics Privacy & Reg. Conference 2019