IT Track Keynote: IRM – Risk as a New Currency

Gavin A. Grounds, Executive Director. Information Risk Management & Cyber Security Strategy, Verizon

GRC SUMMIT 2019
BALTIMORE, JUNE 2-5
Hosted by MetricStream

PERFORM WITH INTEGRITY ™

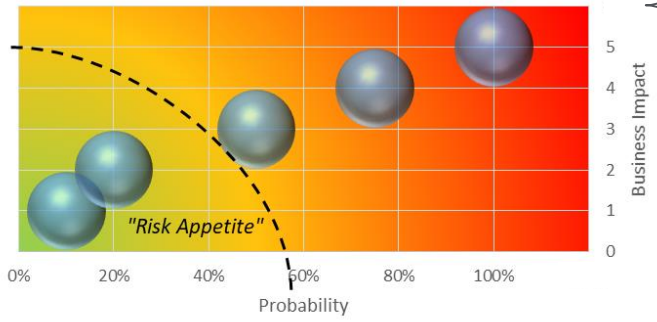
IRM – Risk as a New Currency

Most IRM Models Do Not Adequately Support Cyber Security Objectives

Typical 5x5 Cyber Security Risk Representation:

"Risk Appetite" applied on a per-risk basis

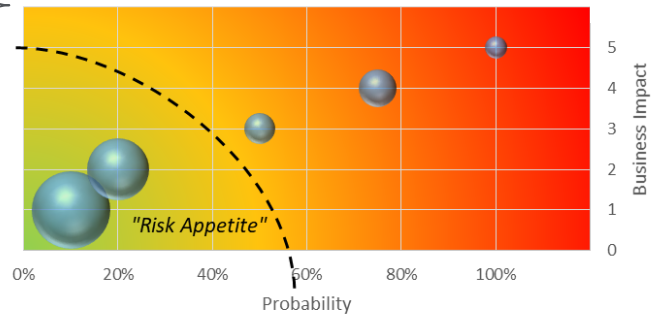
Singular Probability	Business Impact	Individual Risk Count
10%	1	1
20%	2	1
50%	3	1
75%	4	1
100%	5	1



- Lacks clear business context
- No clear fiscal impact view
- Risk "portfolio" not quantified
- Lacks clear prioritization
- Typically a Bottom-Up perspective
- Complex probability & impact aggregation
- Point-in-time perspective: Not predictive
- Lacks risk forecasting

"Risk Appetite" applied on a portfolio view

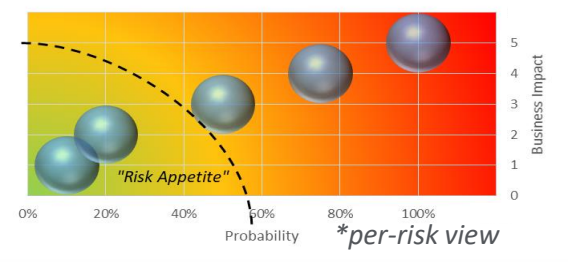
Singular Probability	Business Impact	Individual Risk Count
10%	1	13
20%	2	8
50%	3	2
75%	4	3
100%	5	1



PERFORM WITH INTEGRITY ™

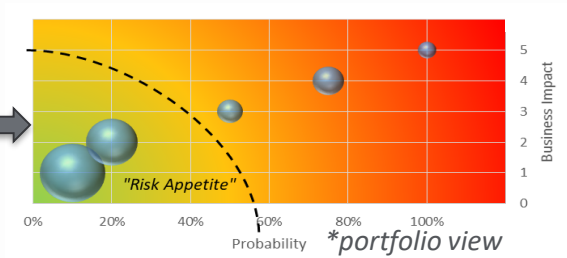
IRM – Risk as a New Currency

Most IRM Models Do Not Adequately Support Cyber Security Objectives – Example



*per-risk view

Gravity of Accepted risks based on 5x5 out-weighs focus area for remediation



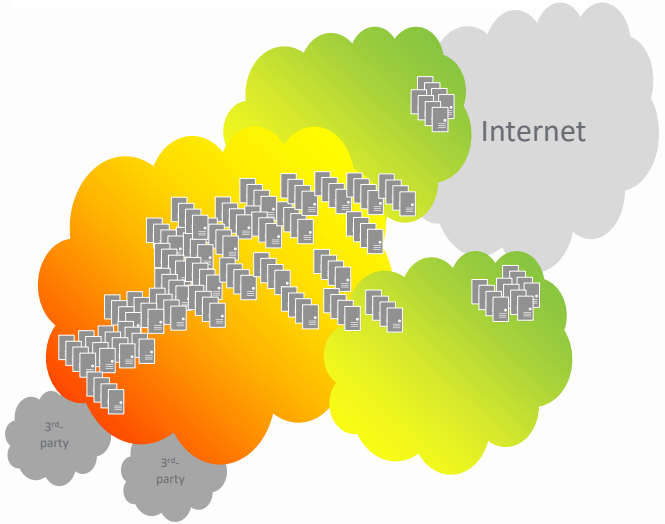
*portfolio view

Example:

- Impact defined primarily by technical context, not business context:
  - Internet-facing?
  - Public Cloud-Based?
  - Private Cloud-Based?
- Probability based on "gut feel" or insular history:
  - Has it happened to *us* before?
  - Technical view of mitigating controls
  - Limited-to-no factoring of external stats

Outcome:

- Apps / Systems supporting critical business processes may be left vulnerable
- Contractual / Regulatory obligations may be missed
- 3rd-party Inter-connections not adequately addressed
- "Proximity" Risks (East-West –v – North-South) increased to critical systems

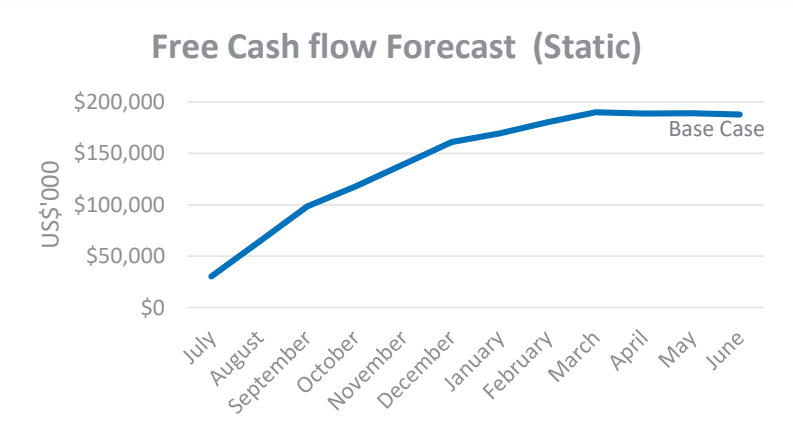


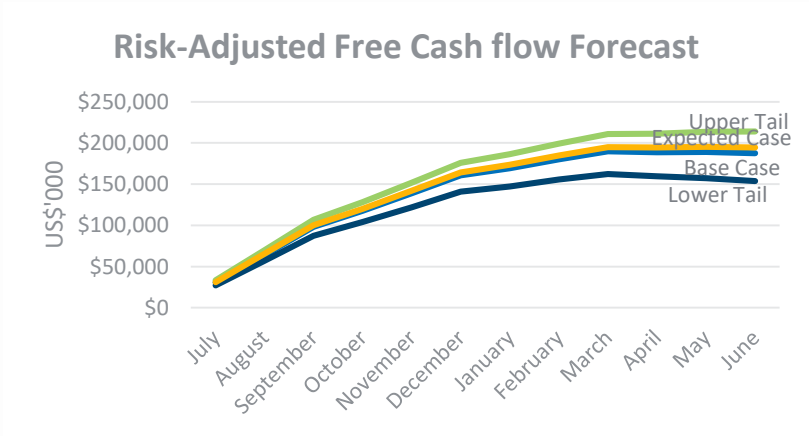
PERFORM WITH INTEGRITY ™

IRM – Risk as a New Currency

Cyber risk today has tangible revenue, margin and shareholder impact

To speak the “language” of the business, must be represented in a business context:





- Single-point Estimates
- No Quantitative Risk Estimates
- Based on aggregated “best guesses”

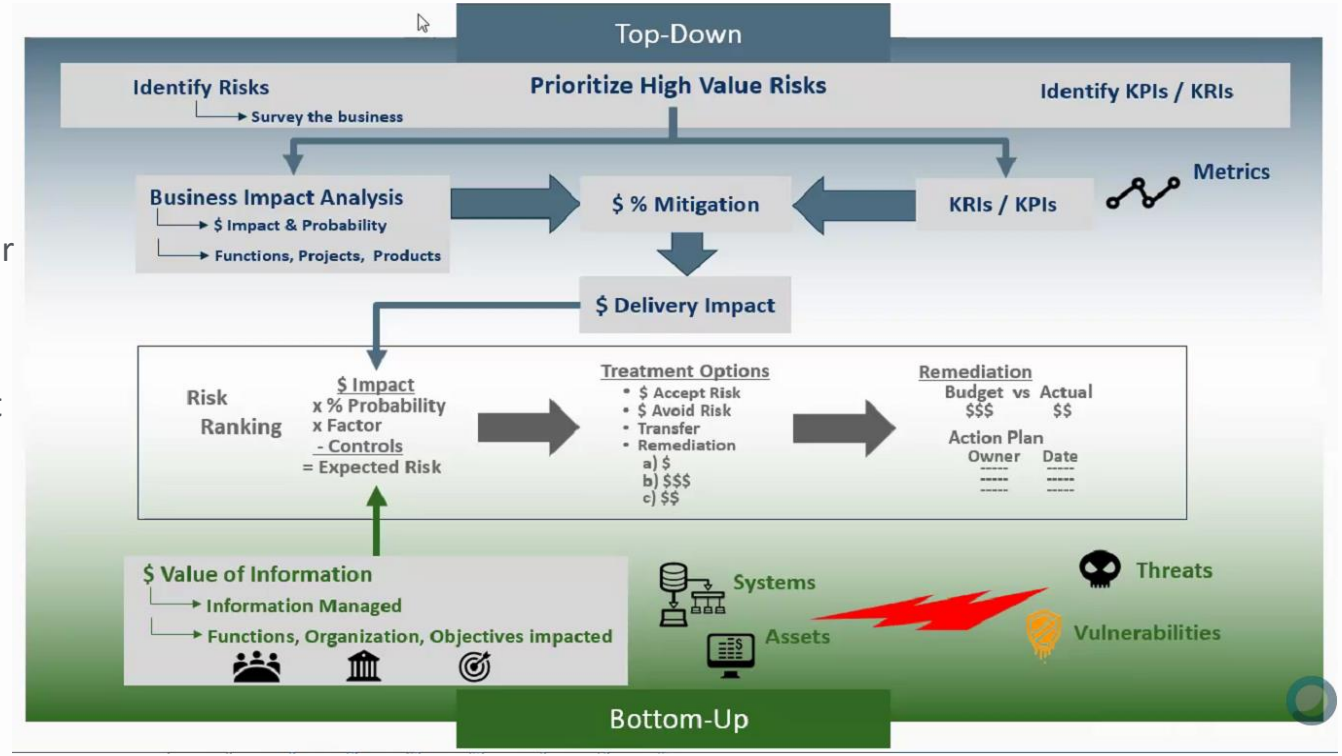
Bottom-up & Top-down Quantitative Risk Estimates, based on multiple variables and probability:

- Currency fluctuation
- Earnings-at-risk
- Cash-flow, DSO & Bad Debt risks
- Un-planned expenses

IRM – Risk as a New Currency

BOTTOM-UP / TOP-DOWN:: Business-oriented, Quantitative, IRM

Business Risk
Probability
Key Risk Indicator
Business Failure
Business Impact

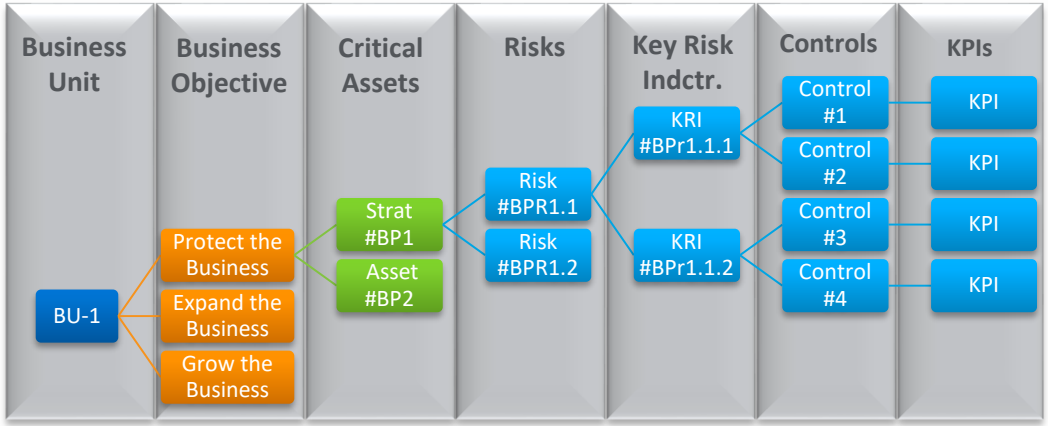


Operating Impact
Compliance Failure
Operating Failure
Patching Failure
Vulnerability

PERFORM WITH INTEGRITY ™

IRM – Risk as a New Currency

Recommended Approach



Business Unit
Each BU has specific business objectives, strategies & risk considerations

Business Objectives
Top-line business objectives that support the BU Strategy

Critical Assets
Critical Business Assets, Processes, Intellectual Property & Critical strategies

Risks
A stated "anxiety" – something that might happen, or fail to happen, that would impact a Business strategy, or critical business asset.

Key Risk Indicators
Measurements or events that, when observed, indicate that a risk is materializing.

Controls
Control framework, policies, standards & services Detect KRI events and prevent realization of Risks

KPIs
KPIs measuring the performance of Controls, Policies, standards and services.

- Establish initial key scope (i.e. Specific function e.g. Billing / Collections / Payments)
- Perform "Bottom-up" walk (***Delivery Risk***)
  - Identify IT / Technology assets
  - Inventory known vulnerabilities, non-compliances, exceptions, etc.
  - Map to specific business processes
  - Map processes to business risks
- Perform "Top-Down" walk (***Business Risk***)
  - Map business function objectives to business assets
  - Identify key assets (*"Crown Jewels"*)
  - Identify / define key risks
  - Quantify risk (impact & probability)
  - Identify / define Key Risk Indicators
- Intermesh Business Impact, Probability and subsequent Priorities

PERFORM WITH INTEGRITY ™

IRM – Risk as a New Currency

Working Example

Bottom-up Approach – How do you Prioritize?:

		NIST SCORING (CVSS 3.0)					Rating						Proliphoration		
Vulnerability	Technology	Source	Rating	Base Score	Impact	Exploitability	C	I	A	Criticality	Composite	I+E	Count	(B+E+I) x #)	Qualitative	Amb?
CVE-2018-8174	Microsoft	MITRE	HIGH	7.5	5.9	1.6	H	H	H	4	15.0	7.5	80,000	1,200,000	5	
CVE-2018-4878	Adobe	MITRE	CRITICAL	9.8	5.9	3.9	H	H	H	5	19.6	9.8	24,949	489,000	1	X
CVE-2017-11882	Microsoft	MITRE	HIGH	7.8	5.9	1.8	H	H	H	4	15.5	7.7	30,845	478,098	1	X
CVE-2017-8750	Microsoft	MITRE	HIGH	7.5	5.9	1.6	H	H	H	4	15.0	7.5	54,844	822,660	3	
CVE-2017-0199	Microsoft	MITRE	HIGH	7.8	5.9	1.8	H	H	H	4	15.5	7.7	50,067	776,039	2	X
CVE-2016-0189	Microsoft	MITRE	HIGH	7.5	5.9	1.6	H	H	H	4	15.0	7.5	51,060	765,900	2	X
CVE-2017-8570	Microsoft	MITRE	HIGH	7.8	5.9	1.8	H	H	H	4	15.5	7.7	65,266	1,011,623	5	
CVE-2018-8373	Microsoft	MITRE	HIGH	7.5	5.9	1.6	H	H	H	4	15.0	7.5	34,924	523,860	1	X
CVE-2012-0158	Microsoft	MITRE	HIGH	9.3	10.0	8.6	C	C	C	4	27.9	18.6	32,893	917,715	3	
CVE-2015-1805	Android	MITRE	HIGH	7.2	10.0	3.9	C	C	C	4	21.1	13.9	4,612	97,313	1	X

** Simulated Data*

How do you address ambiguity?

- Internet-facing?
- Public Cloud-Based?
- Private Cloud-Based?
- Un-clear business impact

IRM – Risk as a New Currency

Working Example

Top-Down Approach

Application / Infra	Business Process / Asset	Quantitative #	Risk Score Impact	Distribution									
				CVE-2018-8174	CVE-2018-4878	CVE-2017-11882	CVE-2017-8750	CVE-2017-0199	CVE-2016-0189	CVE-2017-8570	CVE-2018-8373	CVE-2012-0158	CVE-2015-1805
Provisioning 1	Delivery / Revenue Gen	186479	84085	4%	7%	5%	6%	9%	9%	6%	3%	8%	7%
Provisioning …n	Delivery / Revenue Gen	699928	394506	6%	4%	10%	9%	8%	10%	9%	4%	10%	8%
Logistics 1	Operations / Revenue Gen	1200000	641389	3%	9%	8%	7%	9%	8%	11%	9%	7%	5%
Logistics …n	Operations / Revenue Gen	292205	169557	8%	11%	13%	8%	7%	10%	8%	9%	4%	7%
Collaboration 1	Intellectual Property	1049274	615259	10%	12%	7%	6%	9%	7%	8%	11%	6%	8%
Collaboration …n	Intellectual Property	81363	49582	15%	9%	5%	8%	6%	7%	10%	5%	7%	4%
Billing & Collections	Cash-flow / DSO / Cost-of-Cash	717928	332722	8%	4%	7%	5%	6%	9%	9%	6%	3%	8%
Other	Various Other	56954	187589	46%	44%	45%	51%	46%	40%	39%	53%	55%	53%

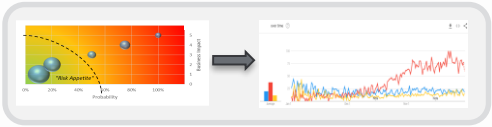
** Simulated Data*

Priorities defined by:

- Quantitative Risk Assessment and Management
- Alignment with Business Criticality
- Protection of Critical Processes and Assets

IRM – Risk as a New Currency

Benefits of Managing Information / Cyber Risk as "Currency"



- Quantitative risk management with Qualitative overlay puts IRM / Cyber Risk in the common ***business language*** –
  - Manage Information Risk in the context of business & fiscal impact
- Manage ***Business Risk*** Score and IT/Technology ***Delivery Risk*** Score from common portfolio
- Facilitate **prioritization** based on true business outcomes
- Establishes standard, quantifiable, reproducible risk assessment methodology
- Delivers Predictive Risk Forecasting, based on real-time operating and project / change reference points
- Reduces losses from threats, illegal activities, exploits & future potential damages
- Supports "Trust" objectives of the business for Customers & Shareholders
- Improved decision-making supporting business outcomes
- Facilitates effective use of resources to address risk & security priorities

Thank You

Continue the conversation on #GRCSummit

GRC SUMMIT 2019
BALTIMORE, JUNE 2-5
Hosted by MetricStream

Gavin A. Grounds – Verizon. Executive Director. Information Risk Management & Cyber Security Strategy
gavin.grounds@verizon.com | @gavingrounds | /in/gavingrounds