IBM Watson Health

Managing Security Risk with Business Leadership

Carl Kraenzel

Vice President, Distinguished Engineer

CISO for IBM Watson Health

Linking IT security risk to business risk is not easy

- The problem:
  - Talking past each other across discipline and up/down the chain, leads to poor management of IT security risks
- One possible approach:
  - Construct KPIs linked to IT metrics and a business impact model, within your existing risk management methods
- The potential outcome:
  - A living governance your leadership team can use to manage IT security risk holistically alongside other business priorities

Leadership needs to manage in terms of business risk

To be properly stated, a business risk will always consists of:

An identified “Threat” or “Exposure”

- *some act,* done by *someone,* with *some thing* as a target

A Likelihood or “Probability” of occurrence

- The chances of it going wrong

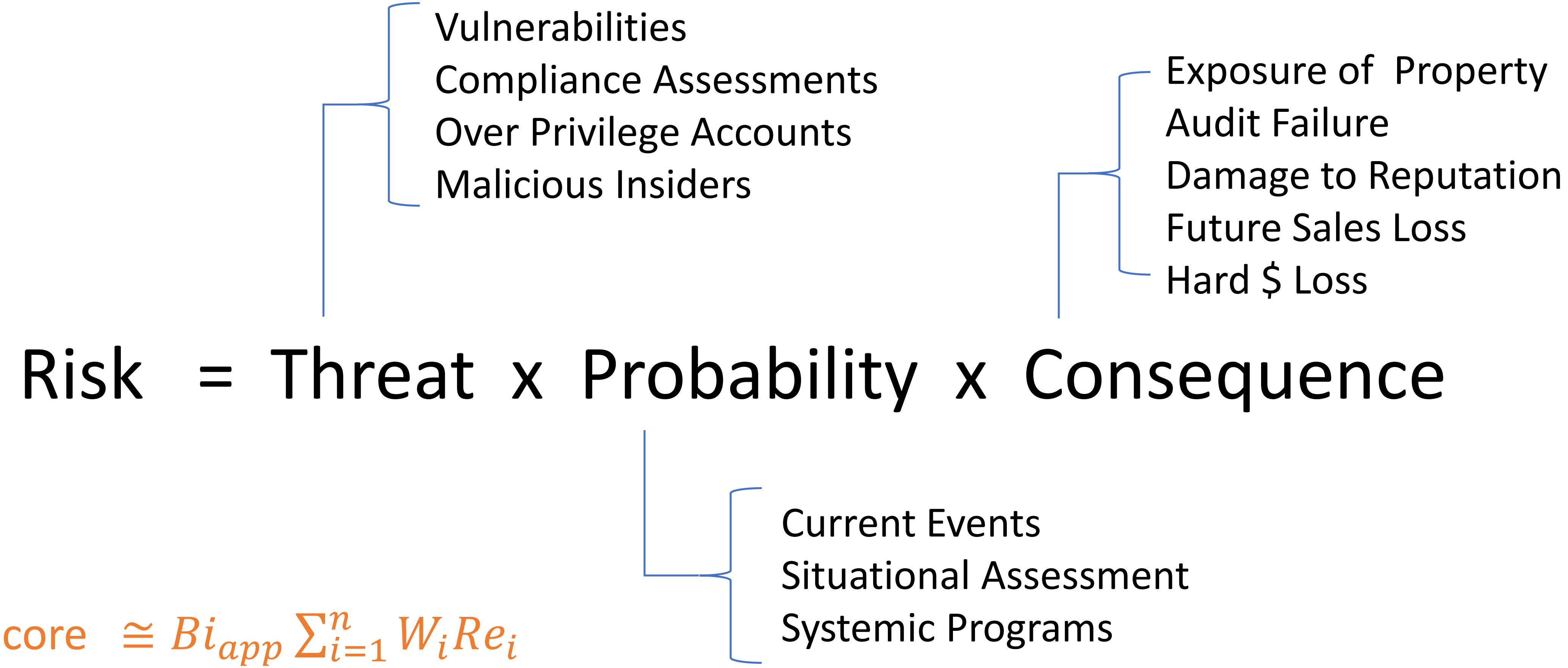
A Business “Consequence” or Impact

- The price you will pay if it goes wrong

Example: “There is a high probability that a malicious insider could expose customer PII resulting in significant fines and damage to our reputation.”

Yet “significant” is not quantitative!

Rigor is key, yet still has to relate to real world metrics



Vulnerabilities
Compliance Assessments
Over Privilege Accounts
Malicious Insiders

Exposure of Property
Audit Failure
Damage to Reputation
Future Sales Loss
Hard $ Loss

Risk = Threat x Probability x Consequence

Current Events
Situational Assessment
Systemic Programs

RiskScore $\cong Bi_{app} \sum_{i=1}^{n} W_i Re_i$

RiskScore: A non-dimensional measure of the level of risk from all sources. This number
Is used for relative comparison of the level of the enterprise’s risk from time to time

And those metrics are hidden inside technical operations

Worlds apart… so how to connect them?

- Collect “exposure metrics” from the technical team
- Structure them into KPIs intelligible to the business team
- Link that to a business impact framework you co-create with the business team
- Plug that into the existing risk management processes of the business
- Team with leadership to employ the results, using it to govern priorities within risk tolerances that now are intelligible and quantifiable
- Iteratively tweak & improve based upon each year’s experience

Here’s an example of constructing a metric-based KPI

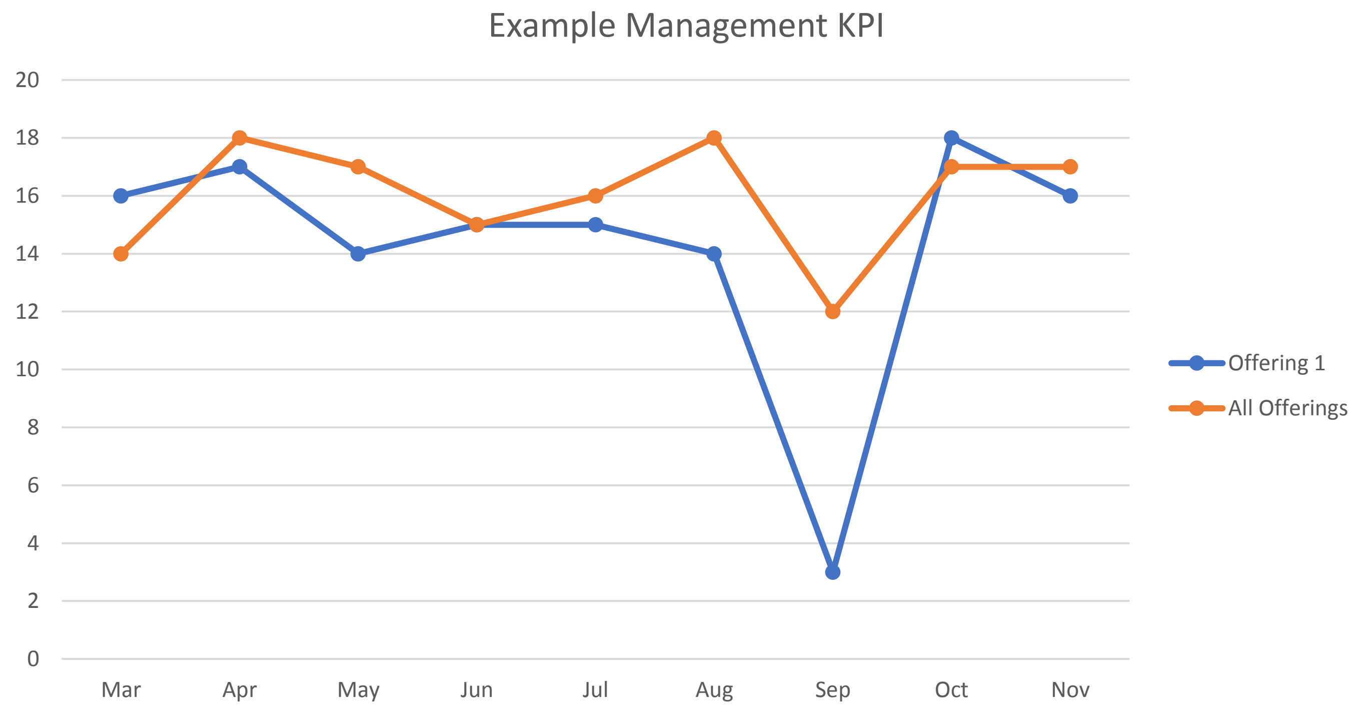
Metric 1	Metric 2	Metric 3	Metric 4	Metric 5				Metric 6				Metric 7				Metric 8				**KPI**
High Sev Security Vulnerabilities in perimeter	Sev1 Security Incident	Aging/ Overdue Security CAPAs	Number of deviations in current month not closed by date due	# of systems internet facing or client data	# of systems out of applicable security policy	% out of policy	Sub Total	VLANs	# with cognitive detector	% without cognitive detector	Sub Total	# of privileged user IDs	# of privileged user IDs that have differentiated access	% of privileged user IDs that have undifferentiated access	Sub Total	# Employees	#Trained (on Security and Privacy SOP)	% not trained	Sub Total	**Total Client Data Integrity Score**

Hypothetical September management review would discuss subtractors & steps to resolve

Offering 1’s KPI: 3 out of 20

- -3 for a vulnerable legacy server
- -7 for a Sev 1 security incident
- -3 for three late deviations
- -2 for 20% systems out of policy
- -1 for only 2/3 cognitives deployed
- -1 for 10% shared priv IDs

All offerings average KPI: 13 out of 20



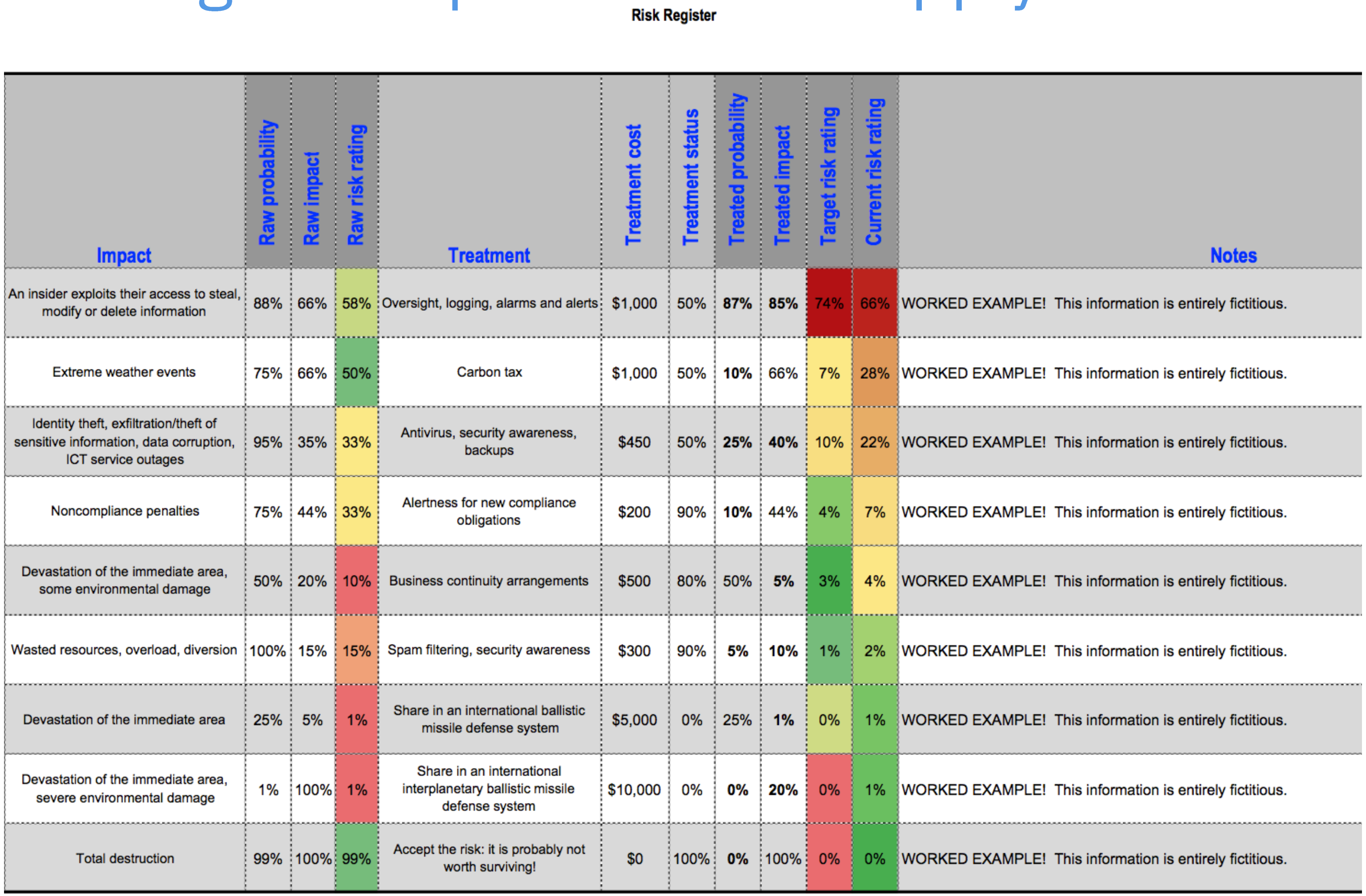
Then leadership team can use such a KPI to model things like “potential direct dollars at risk”

	# PII Records	Cur Q	Cur+1 Q	Cur+2 Q	Cur+3 Q	4 Qs of Rev	KPI	Potential Lost Revenue from KPI Driven Delays	Potential Cost of KPI-Driven Fines/Remediation	% likelihood of Impact	**Potential Direct Dollars at Risk**
Offering 1	2000	$1,000	$2,000	$2,500	$3,000	$8,500	20	$0	$10,000	0%	**$0**
Offering 2	0	$10,000	$10,000	$10,000	$10,000	$40,000	10	$20,000	$0	50%	**$10,000**
Offering 3	100000	$1,000	$2,000	$2,500	$3,000	$8,500	5	$6,375	$500,000	75%	**$379,781**
Offering 4	50000	$10,000	$10,000	$10,000	$10,000	$40,000	0	$40,000	$250,000	100%	**$290,000**
Portfolio 1	152000	$22,000	$24,000	$25,000	$26,000	$97,000	9	$66,375	$760,000	100%	**$679,781**
Offering 5	3000	$1,000	$2,000	$2,500	$3,000	$8,500	8	$5,100	$15,000	60%	**$12,060**
Offering 6	50	$10,000	$10,000	$10,000	$10,000	$40,000	18	$4,000	$250	10%	**$425**
Portfolio 2	3050	$11,000	$12,000	$12,500	$13,000	$48,500	13	$9,100	$15,250	60%	**$12,485**
Offering 7	4000	$1,000	$2,000	$2,500	$3,000	$8,500	1	$8,075	$20,000	95%	**$26,671**
Offering 8	900	$1,000	$2,000	$2,500	$3,000	$8,500	20	$0	$4,500	0%	**$0**
Offering 9	18000	$10,000	$10,000	$10,000	$10,000	$40,000	3	$34,000	$90,000	85%	**$105,400**
Portfolio 3	22900	$12,000	$14,000	$15,000	$16,000	$57,000	8	$42,075	$114,500	95%	**$132,071**
Business	**177950**	**$45,000**	**$50,000**	**$52,500**	**$55,000**	**$202,500**	**10**	**$117,550**	**$889,750**	**100%**	**$824,338**

Well known risk management practices still apply

For example, various tools support a Risk Register as well known mechanism for managing and assessing business risks, which can now include IT security risks

Link your metrics-driven management KPI(s) into such established practices to enable more holisitic governance of security risk



Risk Register

Impact	Raw probability	Raw impact	Raw risk rating	Treatment	Treatment cost	Treatment status	Treated probability	Treated impact	Target risk rating	Current risk rating	Notes
An insider exploits their access to steal, modify or delete information	88%	66%	58%	Oversight, logging, alarms and alerts	$1,000	50%	87%	85%	74%	66%	WORKED EXAMPLE! This information is entirely fictitious.
Extreme weather events	75%	66%	50%	Carbon tax	$1,000	50%	10%	66%	7%	28%	WORKED EXAMPLE! This information is entirely fictitious.
Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages	95%	35%	33%	Antivirus, security awareness, backups	$450	50%	25%	40%	10%	22%	WORKED EXAMPLE! This information is entirely fictitious.
Noncompliance penalties	75%	44%	33%	Alertness for new compliance obligations	$200	90%	10%	44%	4%	7%	WORKED EXAMPLE! This information is entirely fictitious.
Devastation of the immediate area, some environmental damage	50%	20%	10%	Business continuity arrangements	$500	80%	50%	5%	3%	4%	WORKED EXAMPLE! This information is entirely fictitious.
Wasted resources, overload, diversion	100%	15%	15%	Spam filtering, security awareness	$300	90%	5%	10%	1%	2%	WORKED EXAMPLE! This information is entirely fictitious.
Devastation of the immediate area	25%	5%	1%	Share in an international ballistic missile defense system	$5,000	0%	25%	1%	0%	1%	WORKED EXAMPLE! This information is entirely fictitious.
Devastation of the immediate area, severe environmental damage	1%	100%	1%	Share in an international interplanetary ballistic missile defense system	$10,000	0%	0%	20%	0%	1%	WORKED EXAMPLE! This information is entirely fictitious.
Total destruction	99%	100%	99%	Accept the risk: it is probably not worth surviving!	$0	100%	0%	100%	0%	0%	WORKED EXAMPLE! This information is entirely fictitious.

So to recap…

- Come up with your own weighted KPI(s) built on exposure metrics
- Link that to an impact framework co-created with business leadership
- Then together use it within existing risk management governance
- Update your KPI and framework at least yearly, evolve from experience

Metrics -> KPI -> Impact Framework -> Risk Management -> Governance -> Iterate

Thank you!

Please contact Diane Hill <dhill@us.ibm.com>

if you wish to discuss how this might be applied in your organization.

Legal Disclaimer

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.