Communicating Risk
to Executive Leadership

Andrew Plato, *President/CEO*, Anitian

Professional Techniques – T11

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

2014 Fall Conference - "Think Big"

CRISC

CGEIT

CISM

CISA

Overview

Intent

- Define the challenges of communicating risk to leadership
- Outline a new approach to risk communication

Outline

1. Failure of current risk assessment practices
2. Business risk intelligence – a new way to communicate risk

The Failure of Current Risk Assessment Practices

Something Is Not Right Here

Business leaders are fed up with security & risk assessment:

“Why does this take so long?”

“Why don’t the security controls we bought last year work any more? ”

“What am I supposed to do with this big risk report?”

“How serious are these threats?

“Where are the real problems and how do we fix them?”

“Are we *really* in danger?”

“What do all these numbers, charts and worksheets mean?”

“This is just a meaningless regulatory requirement!”

“What does it cost?”

The Problem

- Current security and risk practices are…
  - Too slow
  - Too complex
  - Overly focused on compliance and technology
  - Dither in details, or blather in concepts
  - Incomprehensible to leadership
  - Fail to provide clear actionable steps to reduce risk

…But Why?

Security Language is Incomprehensible to Leadership

- Language affects not only comprehension, but also acceptance.
- Complex, arcane language is inefficient and inaccessible.
- Nitpicking paperwork busywork that nobody reads.
- Definition from OCTAVE[1] for *Defined Evaluation Activities*:

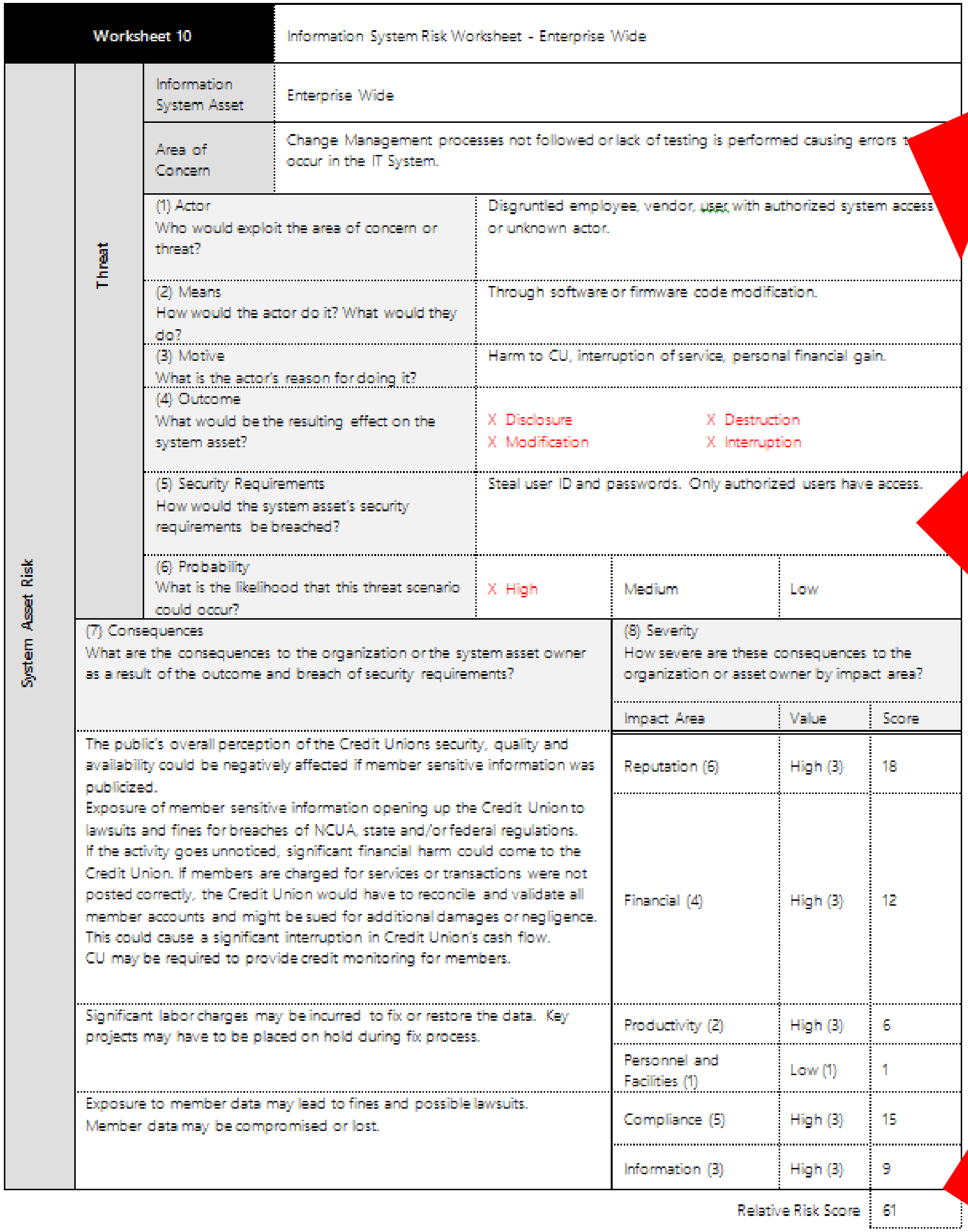
  > *Implementing defined evaluation activities helps to institutionalize the evaluation process in the organization, ensuring some level of consistency in the application of the process. It also provides a basis upon which the activities can be tailored to fit the needs of a particular business line or group.*

- Business leaders need risk language they understand.

[1] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Numbers Can Lie

- Using numbers does not make analysis more “true”.
- If a number is arrived at from a subjective assessment, then its use in any calculations is equally subjective.
- Charts full of numbers may “feel” empirical, but they’re not.
- It’s impossible to establish true value for IT asset.
- Misleading, creates a false sense of accuracy.
- Creates a false scale that does not translate into real-world thinking.
- Leadership cannot digest all the numbers and charts.



Worksheet 10			Information System Risk Worksheet - Enterprise Wide		
System Asset Risk	Threat	Information System Asset	Enterprise Wide		
		Area of Concern	Change Management processes not followed or lack of testing is performed causing errors t occur in the IT System.		
		(1) Actor Who would exploit the area of concern or threat?	Disgruntled employee, vendor, user with authorized system access or unknown actor.		
		(2) Means How would the actor do it? What would they do?	Through software or firmware code modification.		
		(3) Motive What is the actor's reason for doing it?	Harm to CU, interruption of service, personal financial gain.		
		(4) Outcome What would be the resulting effect on the system asset?	X Disclosure X Modification	X Destruction X Interruption	
		(5) Security Requirements How would the system asset's security requirements be breached?	Steal user ID and passwords. Only authorized users have access.		
		(6) Probability What is the likelihood that this threat scenario could occur?	X High	Medium	Low
	(7) Consequences What are the consequences to the organization or the system asset owner as a result of the outcome and breach of security requirements?		(8) Severity How severe are these consequences to the organization or asset owner by impact area?		
			Impact Area	Value	Score
	The public's overall perception of the Credit Unions security, quality and availability could be negatively affected if member sensitive information was publicized. Exposure of member sensitive information opening up the Credit Union to lawsuits and fines for breaches of NCUA, state and/or federal regulations. If the activity goes unnoticed, significant financial harm could come to the Credit Union. If members are charged for services or transactions were not posted correctly, the Credit Union would have to reconcile and validate all member accounts and might be sued for additional damages or negligence. This could cause a significant interruption in Credit Union's cash flow. CU may be required to provide credit monitoring for members.		Reputation (6)	High (3)	18
			Financial (4)	High (3)	12
	Significant labor charges may be incurred to fix or restore the data. Key projects may have to be placed on hold during fix process.		Productivity (2)	High (3)	6
			Personnel and Facilities (1)	Low (1)	1
	Exposure to member data may lead to fines and possible lawsuits. Member data may be compromised or lost.		Compliance (5)	High (3)	15
			Information (3)	High (3)	9
				Relative Risk Score	61

Huh?

LOL Whut?

Risk assessment practices are confusing to leadership!

A 61? 61 WHAT?

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Stale Data

- IT risk is volatile, dynamic and has a short shelf life.
- Any risk assessment over 90-180 days old is stale.
- NIST[1], OCTAVE, FAIR[2] are too time consuming.
- Risk assessments need to be done in 30 days or less.
- Surveys and questionnaires do not work, people ignore them.
- Risk assessment is not a consensus of opinions.
- Leadership needs timely threat intelligence to fuel decision-making.

[1] National Institute of Standards and Technology (NIST)

[2] Factor Analysis of Information Risk (FAIR)

Lack of Evidence

- Risk assessment methodologies focus heavily on process, and very little on evidence.
- Custodians and business process owners withhold information.
- The security of an environment can be tested in a controlled, rational manner.
- Without testing, the entire analysis is one-sided.
- Testing can cut through conjecture and prove (or disprove) the severity of a threat.
- Leaders must be able to trust the intelligence.

The Challenge

- How do we improve risk assessments to make them more…
  - Accurate
  - Relevant
  - Actionable
  - Timely

..to business leadership?

Business Risk Intelligence
A New Way to Communicate Risk

Leadership Needs Business Risk Intelligence

- Business needs more than *big data*, they need *intelligence.*
- Threats and risk metrics must be distilled down to something leadership can quickly consume.
- Business Risk Intelligence is:
  - The ability to aggregate, assess, and communicate all the disparate information that defines risk
  - Risk expressed in business terms, that leadership can understand, conceptualize, and use
  - A decision making tool

1. Start with Common Language: The Core Six

- Risk is an over-used word that is often misunderstood.
- Get everybody using proper risk terminology.

Threat:	Something bad that *might* happen.
Vulnerability:	A weakness a threat could exploit.
Impact:	How bad a threat can damage the business.
Probability:	How likely a threat is in a given timeframe.
Control:	Something that mitigates threat.
Risk:	An assessment of a threat based upon its probability and impact in relation to the relevant controls.

2. Categorize the Scope

- Complex environments are too difficult to understand as a whole.
- Organize assets into categories and then apply threat analysis to the category rather than individual items.
- Common lenses include:
  - Data type
  - Systems
  - Business unit
  - Applications
  - Regulations
  - User groups

2. Category Example – Data Type

- Confidential Data: User passwords, social security numbers, payroll information, financial records.
- Personally Identifiable Information (PII): Health care records.
- PCI Data: Payment card numbers.
- Restricted Data: Price lists, business plans, product designs.
- Public Data: Web site contents, marketing documents.
- *What threats apply to confidential data? PII? public data?*

3. *Chase the Rabbit*

- Talk with your people: leadership, IT, HR, devops, etc.
- Focus the discussions on *harm* and *weakness*
- Ask big, open-ended questions:
  - How would you harm this company?
  - What has you concerned?
  - Where are the weaknesses?
  - What is valuable to us?
  - How do you do your job? Why do you do it that way?
  - What would happen if…
- Avoid "forward-looking statements" – focus on the now.
- What is the person's intention and feelings?

4. Define & Categorize Threats

- What was the answer to: *“How would you harm this company?”*
- Simplify them into the *core harm.*
- Categorize the threats to help organize them and focus your analysis efforts :
  - Technical – threat to systems, hardware, applications, etc.
  - Operational – threats that affect practices, procedures, or business functions
  - Relational – threat to a relationship between groups, people or third parties
  - Physical – threats to facilities, offices, etc.
  - Reputational – threats to the organization’s reputation, perception, or public opinion

4. Define Threats - Examples

- Good Threat Definitions:
  - Malware infection
  - Data is leaked to a competitor
  - Sensitive authentication data is stolen
  - Dependent third party resources are unavailable
- Bad Threat Definitions:
  - Lack of alignment to organizational policies with guidelines set forth by the security committee means staff is not properly implementing security controls.
  - Use of telnet among staff is threatening PCI compliance requirements.
  - Missing patches on systems

5. Itemize Vulnerabilities

- Where are you weak? What would allow that bad stuff to happen?
- Get real data on the environment (it’s plentiful!):
  - Penetration tests
  - Configuration analysis
  - Vulnerability scans
  - Incident reports
  - SIEM (Security Information & Event Management) reports
- Connect vulnerabilities to threats.
- How easy is the vulnerability to exploit?
- Compare the data with what people said, and look for inconsistencies.

6. Simplify Probability and Impact Assessment

Probability

Metric	Description
Certain	<95% likelihood of occurrence within the next 12 months.
High	50-95% likelihood of occurrence within the next 12 months.
Medium	20-49% likelihood of occurrence within the next 12 months.
Low	1-20% likelihood of occurrence within the next 12 months.
Negligible	>1% likelihood of occurrence within the next 12 months.

Impact

Metric	Description
Critical	Catastrophic effect on the Data Asset.
High	Serious impact on the Data Asset's functionality.
Medium	Threat may cause some intermittent impact on the Data Asset, but would not lead to extended problems.
Low	Impact on the Data Asset is small and limited. Would not cause any disruption in core functions.
Negligible	Data Asset remains functional for the business with no noticeable slowness or downtime.

7. Build a Threat Matrix

- A spreadsheet that defines each threat with the following attributes:
  - Threat name
  - Threat type
  - Affected assets
  - Vulnerabilities
  - Impact
  - Impact type
  - Mitigating controls
  - Probability
  - Risk
  - Risk mitigation
  - Residual risk
- This document is not for leadership, its for you to organize the threats you have found

Threat Matrix Example

Threat	Threat Type	Affected Systems, Processes or Place	Affected Data Types	Vulnerabilities	Impact	Impact Type	Mitigating Controls	Probability	Risk	Risk Type	Risk Mitigation	Residual Risk
A data center disaster puts the systems offline for an indefinite period of time	•Physical	•SampleCorp •123SampleApp	•ePHI •PII	•The current SampleCorp and 123SampleApp production systems have no geographical diversity	Critical	•Availability	•The IO Data center appears to be a very well designed and well run facility, with multiply redundant power and network connectivity.	Negligible	Medium	•Reputational •Financial •Regulatory •Legal	Implement the following components of the Common Control Framework: •Develop a secondary location with a recent backup copy of the data. Anitian	Low
A disaster interrupts business processes	•Operational	•SampleCorp •123SampleApp	•ePHI •PII	•A formal Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) does not exist for critical systems and applications	High	•Availability	•123SampleApp and SampleCorp are not highly time sensitive applications, and a short-duration downtime would not critically impact business. •Business operations could theoretically be resumed by reconstructing databases from original sources in a moderate amount of time, but no formal business resumption test has been performed.	Low	Medium	•Reputational •Financial •Regulatory •Legal	Implement the following components of the Common Control Framework: •Develop and test a formal BCP and DRP	Low
A disaster interrupts business processes	•Operational •Physical	•All corporate and production systems	•BSD	•A formal Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) does not exist for critical systems and applications •The current SampleCorp and 123SampleApp production systems have no geographical diversity	High	•Availability	•123SampleApp and SampleCorp are not highly time sensitive applications, and a short-duration downtime would not critically impact business. •Business operations could theoretically be resumed by reconstructing databases from original sources in a moderate amount of time, but no formal business resumption test has been performed. •The IO Data center appears to be a very well designed and well run facility, with multiply redundant power and network connectivity.	Low	Medium	•Reputational •Financial •Regulatory •Legal	Implement the following components of the Common Control Framework: •Develop and test a formal BCP and DRP •Develop a secondary location with a recent backup copy of the data. Anitian understands that this is already under consideration, and SampleCorp should move ahead with its plans.	Low

8. Simplify Data into Intelligence Briefs

- Take the top 10 most serious threats and simplify the risk data into five attributes:
  - Threat
  - Vulnerabilities
  - Impact
  - Probability
  - Risk
- Simplify overall risk analysis into a single, concise narrative on each risk type.

Sample Threat Intelligence Briefing

#	Threat	Vulnerabilities	Impact	Probability	Risk
1.	Malware infection	– Ineffective antivirus end point protection – End users have administrative privileges on endpoint devices – Malware protections not deployed on all device types handling sensitive data – Lack of inline malware protection at corporate office Internet access points – Lack of network segmentation – Lack of security monitoring	**Critical** Malware on high value systems could leak sensitive customer data.	**High** Lack of controls and the sensitivity of the data make infection very likely.	**Critical**

Sample Risk Intelligence Briefing

Issues	Severity	Description
Regulatory Risk	High	Company faces extensive HIPAA regulatory risk due to significant non-compliance, both in technical information security and privacy matters, and in general business process requirements.
Legal Risk	Medium	The global security risks throughout the IT infrastructure expose the Company to potential risk of lawsuits from patients and their employees if PHI is stolen or corrupted.
Reputational Risk	High	Insufficient controls protecting ePHI exposes Company to a high degree of Reputational Risk. Enforcement actions resulting from a failing OCR HIPAA assessment also have a high potential for negative reputational impact.
Financial Risk	Medium	The Company's IT environment is not aligned with most security best practices, increasing the likelihood of a security breach. This includes the potential for fines due to regulatory compliance violations and lawsuits from data owners (patients).
Operational Risk	Low	The Company is at some risk from technical issues, such as the uncertainty of whether an internet outage would cause significant interruption of business. However, there is good redundancy in the environment.

9. Develop an Action Plan

- Define and summarize what must be done to reduce and/or eliminate threats.
- Be specific, no vague hopes.

#	Action	Description	Estimate	Effort
1.	Integrate all critical devices with SIEM	• Complete the SIEM deployment, aggregating system- and application-level logs for all critical application and security monitoring devices. • Tune event correlation, incident thresholds and alerting. • Integrate alerting with incident response plan. • This work is critical because currently there is little or no automated review or alerting for unauthorized access to PHI occurs.	200-280 hours	High

Do Not…

- Try to change the culture of the business.
- Let perfection become the enemy of good.
- Cite any kind of risk management theory; nobody cares.
- Use questionnaires, surveys or spreadsheets; nobody will do them correctly.
- Use a lot of risk terminology; nobody understands them.
- Document indecision; it shows weakness.
- Try to sound “official” and important; nobody is impressed.
- Create phony numbers or equations.
- Use inaccessible matrices, worksheets, or process flows.
- Waste time with sensationalist threats; erodes trust.
- Involve anybody who sells you equipment in the process.

Do

- Present risk in the order an executive thinks:
  1. Threats
  2. Vulnerabilities
  3. Risk
  4. Remediation
- Stay true to the “Core Six”.
- Establish authority with decisive, simple language.
- Identify tangible, actionable recommendations.
- Use simple, business language.

Business Risk Intelligence Enables

- Understanding of the organizational strengths and weaknesses.
- Effective prioritization of investments.
- Informed decision making based on data.
- Compliance initiatives that go beyond compliance box checking, to improve security systemically.
- A rational response to threat.

Anitian

We enlighten, protect and empower great security leaders.

We believe security will make the world a better place.

- Security is necessary for innovation and growth
- Security can be empowering when it is practical and pragmatic
- Good security comes from rational, scientific methods of analysis

Thank You

EMAIL:	andrew.plato@anitian.com
WEB:	www.anitian.com
BLOG:	blog.anitian.com
SLIDES:	http://bit.ly/anitian
CALL:	888-ANITIAN