Convincing Your Management, Your Peers and Yourself that Risk Management Doesn't Suck

ISSA LA
2017-06-21
#whoami

- Josh Sokol
- Information Security Program Owner @ NI
- Creator and CEO of SimpleRisk
- OWASP Board Member
- Email: josh@simplerisk.com
- Twitter: @joshsokol
WHAT IS APT?
Talk Motivations

• Most risk management talks focus on process...BORING.
• Issues convincing management to undertake security projects.
• Issues getting peers to disclose vulnerabilities.
• Proper risk management is about using risks to drive organizational improvements.
• It can be interesting and extremely valuable.
Personal Risk Management

- door/window protection
- carbon monoxide detectors*
- motion detectors
- smoke and heat sensors*
- personal emergency
- keychain touchpad
- water sensors*
- freeze sensors*

*optional upgrades
# Threats and Consequences

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Low Consequence</th>
<th>Medium Consequence</th>
<th>High Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Loss</td>
<td>Business unit manager could contain the anticipated loss in operational budget.</td>
<td>Corporate GM could contain the anticipated loss by shifting funds and priorities.</td>
<td>Recovery from the anticipated loss would be handled by the CEO and board as a special item.</td>
</tr>
<tr>
<td>Reputation damage</td>
<td>Significant adverse publicity is anticipated.</td>
<td>Significant loss of market capitalization, revenue, or customers is anticipated.</td>
<td>Felony prosecutions of personnel, class-action civil suits, or withdrawal from market sectors or geographies are anticipated.</td>
</tr>
</tbody>
</table>
## Threats and Consequences (cont)

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Low Consequence</th>
<th>Medium Consequence</th>
<th>High Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory noncompliance</td>
<td>Routine fines, warnings, or adverse audit findings are anticipated.</td>
<td>Substantial fines, consent decrees, or limitations on business practices are anticipated.</td>
<td>Regulatory injunction or loss of license to conduct business is anticipated.</td>
</tr>
<tr>
<td>Business interruption</td>
<td>Business operations could continue indefinitely at increased cost or decreased efficiency.</td>
<td>Suspension of some business operations would be required within one week.</td>
<td>Suspension of business operations would be required within one day.</td>
</tr>
<tr>
<td>Safety hazard</td>
<td>Compensable damage to property is anticipated.</td>
<td>Recoverable illness or injury to humans, or reparable environmental harm is anticipated.</td>
<td>Permanent injury or death of humans, or irreparable environmental harm is anticipated.</td>
</tr>
</tbody>
</table>
A prioritization process is followed whereby the risks with the greatest loss (impact) and the greatest probability (likelihood) of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order.
Risk Management Methodologies

- NIST SP 800-30 Framework
- ISO 27005 Framework
- ISO 31000 Risk Management Principles and Guidelines
- PRISM Framework
- OWASP Risk Rating Methodology
- COSO Enterprise Risk Management-Integrated Framework
- OCTAVE
- ISF Information Risk Assessment Methodologies (IRAM)
- ISACA Risk IT
- ...
Problem

• These are somebody else’s vision of what risk management should be.
• At best they are a guideline to give you examples of what others are doing.
• At worst they make risk management look overly complicated and make it difficult to get started.
Defining Risk

**RISK** is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).
Risk Can Apply To:

- Economic risk
- Health, Safety, and Environment
- IT and InfoSec
- Insurance
- Business and Management
- Finance
- Security
Risk Is a Combination of

- Likelihood: The probability of something occurring.
- Impact: The expected loss if that event occurs.
Risk Formula

“Classic” Risk Formula: RISK = LIKELIHOOD x IMPACT

Note: In SimpleRisk we want every risk score to be a 0 through 10 value.

Likelihood: Credible (3)
Impact: Major (4)

Risk = (3 x 4) x (10/25) = 4.8
Make Your Risk Formula Fit You

- Weighted Impact: \( RISK = LIKELIHOOD \times IMPACT + IMPACT \)

A larger impact will result in a higher risk score.

Likelihood: Credible (3)
Impact: Major (4)

Risk = \((3 \times 4 + 4) \times (10/30) = 5.3\)
Make Your Risk Formula Fit You

- Weighted Likelihood: $\text{RISK} = \text{LIKERIHOOD} \times \text{IMPACT} + \text{LIKERIHOOD}$

A larger likelihood will result in a higher risk score.

Likelihood: Likely (4)
Impact: Moderate (3)

Risk = $(4 \times 3 + 4) \times (10/30) = 5.3$
Be Flexible!

- Risk Management needs to be a custom fit for your organization and your formula needs to reflect that.
- Your formula can (and likely will) change.
- Wherever you are tracking risks should be able to dynamically update risk based on the updated formula.
  - No Word documents
  - No Excel documents
  - No static formats
Convincing Your Management

• Risk management will **FAIL** if you do not have management participation.

• Management speaks risk. Not CVE. Not attack vector. Not threat tree. RISK.

• Your responsibility as a Security Professional is to collect and convey risk to management.

• Management’s responsibility is to evaluate how to respond to the risks (accept, transfer, or reduce).

• If you do a good job of guiding management through risk analysis, then the result is a list of priorities for project planning.
Convincing Your Peers

• Risk management will **FAIL** if you do not have peer participation.
• Management can only be proactive in addressing risk if they are aware that it exists.
• Undocumented risk means that you and your peers shoulder the responsibility if it happens.
• Documented risk means that management acknowledges that the risk exists and any action (or inaction) is now on their shoulders.
Determining Your Risks

• Convince your peers that documenting risks is CYOA and you’ll have more risks than you know what to do with.

• Network vulnerability scanners

• Application vulnerability scanners

• Security mailing lists

• Security blogs

• Code Reviews

• Twitter! No, seriously.
Evaluating a Risk

• Is the risk acceptable?
  • Is the likelihood or impact low enough that I’m willing to simply accept the consequences if it happens.

• Is the risk transferrable?
  • Could I purchase insurance or some other measure to transfer the impact of the risk to another party.

• Is the risk reducible?
  • Is there some sort of mitigation that could be put in place to reduce the impact or likelihood of the risk.
## Determining a Response

<table>
<thead>
<tr>
<th>Acceptable</th>
<th>Transferable</th>
<th>Reducible</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Do not engage in this – avoid the risk</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Propose controls and reevaluate</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Transfer or avoid the risk</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Balance costs of control vs. transfer</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Accept or avoid the risk</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Balance costs of control vs. acceptance</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Balance costs of transfer vs. acceptance</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Balance all three and optimize</td>
</tr>
</tbody>
</table>
Risk Management is Not

• It is not a process for avoiding risk.

• The aim of risk management is not to eliminate risk, rather to manage the risks involved in business activities to maximize opportunities and minimize adverse effects.

• Note: Risk management is not the management of insurable risks. Insurance is an important way of transferring risk but most risks will be managed by other means.
Risk Management Should...

• Support strategic and business planning
• Support effective use of resources
• Promote continuous improvement
• Explicitly address uncertainty (fewer shocks and unwelcome surprises)
• Allow for a quick grasp of new opportunities
• Enhance communication between the business, IT, and senior management
• Reassure stakeholders
• Help focus internal audit programs
Risk Management Should...

• Create value.
• Be an integral part of organizational processes.
• Be part of decision making.
• Be systematic and structured.
• Be based on the best available information.
• Be tailored.
• Take into account human factors.
• Be transparent and inclusive.
• Be dynamic, iterative, and responsive to change.
Risk Management is Continuous

• In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions.
• Personnel changes will occur and security policies are likely to change over time.
• These changes mean that new risks will surface and risks previously mitigated may again become a concern.
• The risk management process is ongoing and evolving.
Risk Management Best Practice

• The risk assessment process is usually repeated at least every 3 years for federal agencies.

• Risk management should be conducted and integrated in the lifecycle for IT systems because it is good practice and supports the organization’s business objectives or mission.

• There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted.
Pro Tip!

• If you own the risk management process, then you should schedule monthly meetings with management for regular risk reviews.

• Do not schedule all of these monthly meetings a year in advance unless you want them to continually be deferred for other priorities.
Risk Review Process

• May depend on how lean your organization is on management structure.

• Raise the visibility of high level risks.
  • High Risk = VP
  • Medium Risk = Director
  • Low Risk = Area Manager

• Risks should be re-reviewed regularly.
  • High Risk = Monthly
  • Medium Risk = Semi-annually
  • Low Risk = Annually
Risk Management is Not

• It is not a process for avoiding risk.
• The aim of risk management is not to eliminate risk, rather to manage the risks involved in business activities to maximize opportunities and minimize adverse effects.
• Note: Risk management is not the management of insurable risks. Insurance is an important way of transferring risk but most risks will be managed by other means.
Deriving Value

• Order by risk level.
• Group if mitigations are the same.
• Pass back to various teams stating that project X was approved for consideration in next budget cycle.
Tools for Enterprise Risk Management

• Most enterprise tools fall into a category called “GRC” (Governance, Risk, & Compliance). These tools are easily $100k+.
  • BWise GRC Platform
  • RSA Archer eGRC
  • SAP GRC
  • Oracle GRC
• Spreadsheets. 😞
• eRamba
• OpenFISMA
• DIY
My Journey in Risk Management
NIST SP 800-30

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa
Lotus Notes

Yeah, it can do that too
Several Futile Attempts at Purchasing a GRC
So finally I wrote what I needed...
And released it under MPL 2.0 at BSides Austin in 2013...
About SimpleRisk

Designed with security in mind:

• Parameterized Database Queries
• Input Validation
• HTML Output Encoding
• Hashed and Salted Passwords
• n-Tier Architecture Capable
• Per-Risk and All-Changes Audit trail
SimpleRisk Statistics

- SimpleRisk Core is licensed under MPL 2.0 and contains everything you need to get started with risk management.
- Written in PHP with a MySQL database back-end.
- Available for download as a tarball or VM.
- 39 releases to date with most recent on 6/14/2017
- Almost 12k downloads.
- Used around the world by companies large and small.
- Full-time developer and support
What is your organization using for risk management?

• Nothing
• Spreadsheets/Word/Similar
• SimpleRisk
• A GRC Tool
• Something Else
What is your organization using for risk management?

<table>
<thead>
<tr>
<th>Option</th>
<th>Votes</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nothing</td>
<td>495</td>
<td>32%</td>
</tr>
<tr>
<td>Spreadsheets</td>
<td>677</td>
<td>44%</td>
</tr>
<tr>
<td>SimpleRisk</td>
<td>87</td>
<td>6%</td>
</tr>
<tr>
<td>Something Else</td>
<td>132</td>
<td>9%</td>
</tr>
<tr>
<td></td>
<td>138</td>
<td>9%</td>
</tr>
</tbody>
</table>

77% - OMG Suck!

6% - These guys likely spent $500k+!

Huh?

Free. Open Source. Evangelize!
TIME FOR A LIVE DEMO
WHAT COULD GO WRONG?
Notes on SimpleRisk

• SimpleRisk will **NOT** perform your risk assessment for you.

• SimpleRisk **WILL** provide you with a framework to capture your risks, plan mitigations, perform management reviews, plan projects, and report on risks in your environment.
Notes on Risk Management

• Risk management gives us a common language to use when speaking with the business.
• Risk management drives visibility into issues that were previously skeletons in our closet.
• Risk management drives accountability up the business chain of management.
A Note on Naming Risk

You’re going to call me WHAT!?
Bad Example

“Customer database is not backed up.”
Better Example

“Customer data lost or corrupted due to poor backup processes.”

The professionals must set a good example.

A. Bartlett Giamatti

meetville.com
A Note on Granularity

• I’ve had people propose to have SimpleRisk suck in vulnerabilities from network scanners, application scanners, and more.

• The problem is that having 100 XSS vulnerabilities documented as a risk is just unnecessary paperwork and management doesn’t care.

• Instead, create a single risk documenting that “XSS vulnerabilities lead to user account compromise”.

• After all, having one XSS vulnerability is as good to an attacker as having 100.
Risk Management Roadmap

• Start by getting buy-in from all of your stakeholders (including individual contributors)
• Schedule risk assessment meetings with the teams and capture their risks in the system
• Schedule time for regular reviews with management
• Encourage people to submit their own risks to make it a continual process
Thank You!

josh@simplerisk.com
@joshsokol

https://www.simplerisk.com
http://www.webadminblog.com