

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

ISSA LA

2017-06-21



#whoami

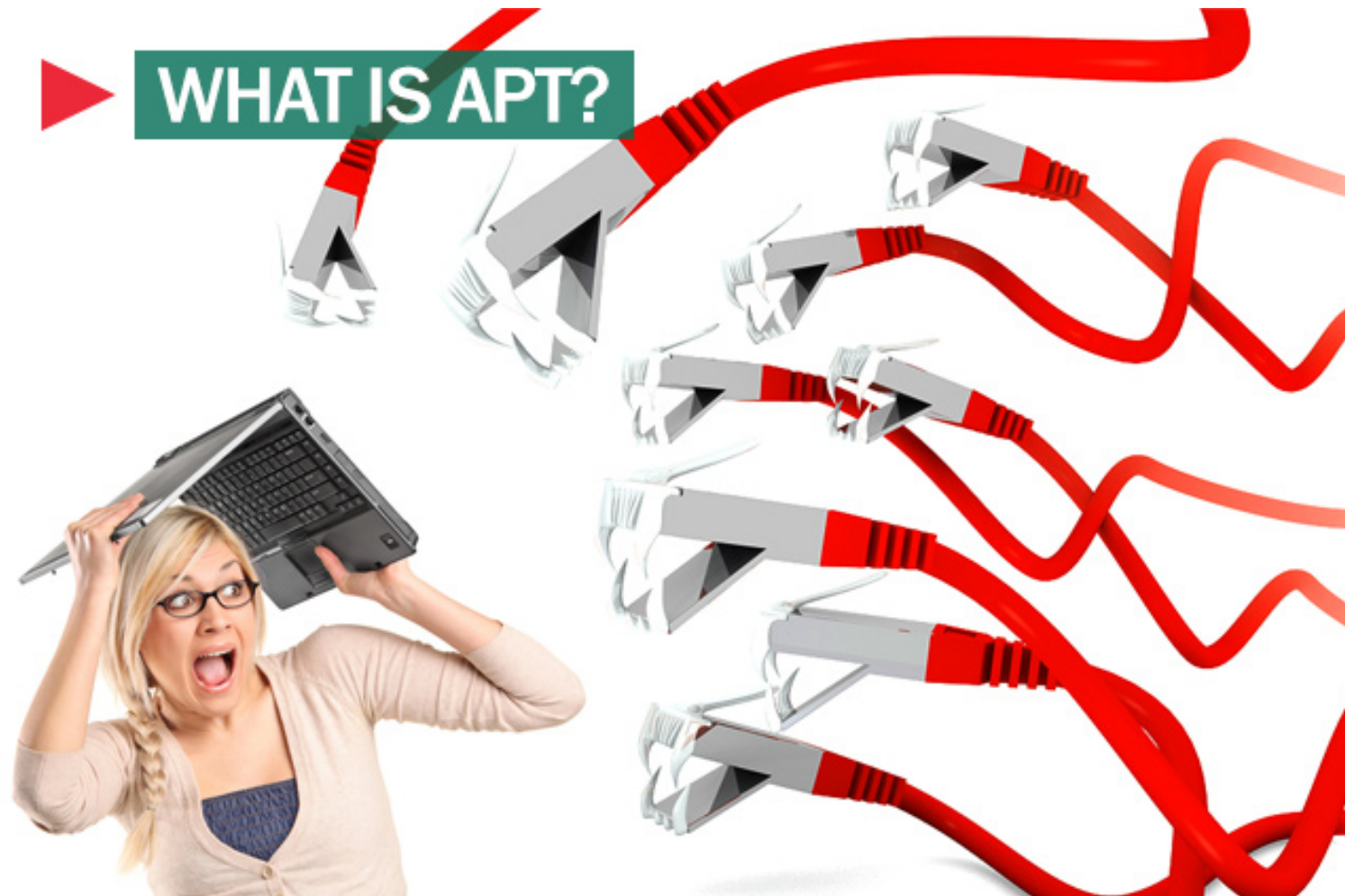
- Josh Sokol
- Information Security Program Owner @ NI
- Creator and CEO of SimpleRisk
- OWASP Board Member
- Email: josh@simplerisk.com
- Twitter: [@joshsokol](https://twitter.com/joshsokol)













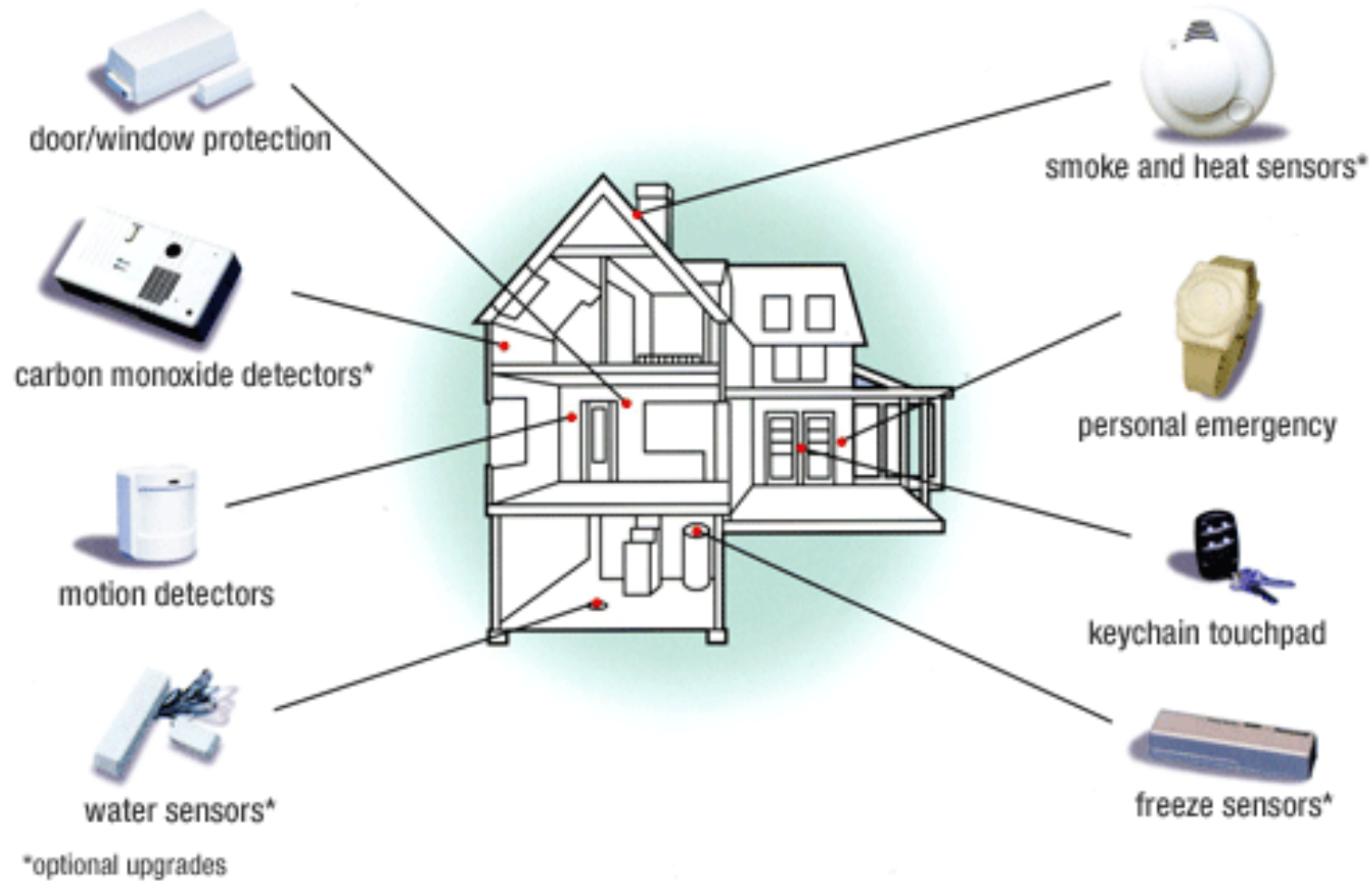


Talk Motivations

- 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





Threats and Consequences

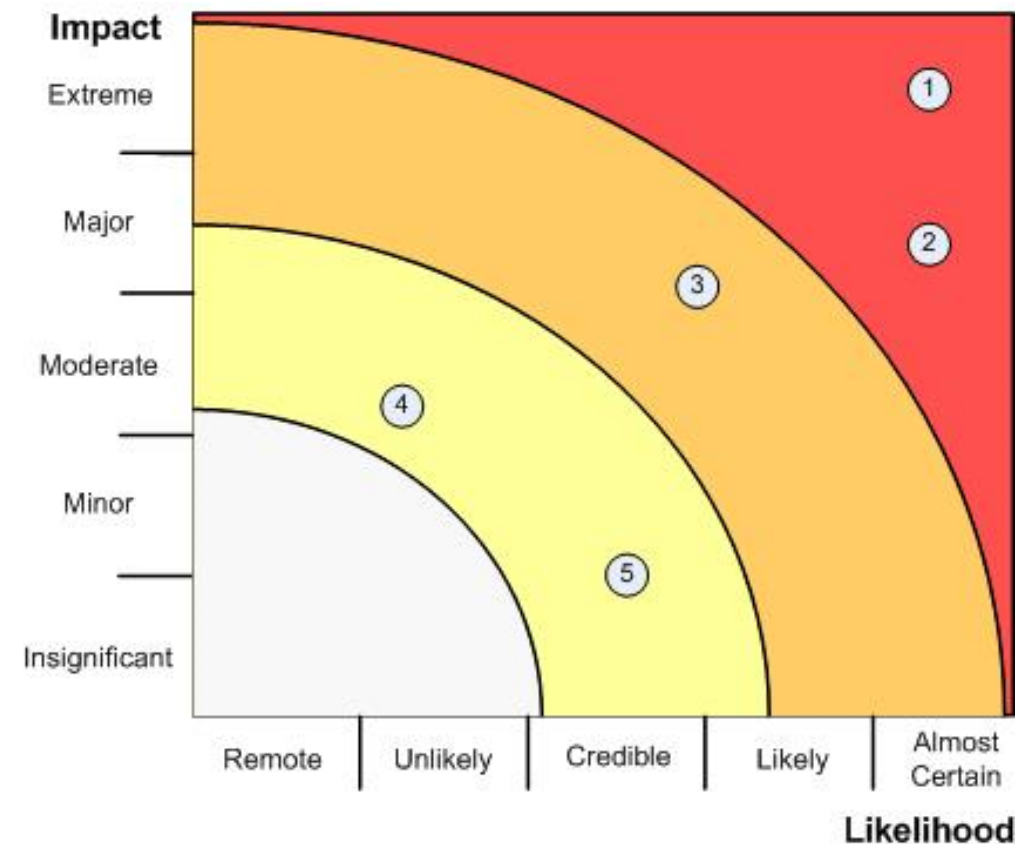
Risk Type	Low Consequence	Medium Consequence	High Consequence
Financial Loss	Business unit manager could contain the anticipated loss in operational budget.	Corporate GM could contain the anticipated loss by shifting funds and priorities.	Recovery from the anticipated loss would be handled by the CEO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

Threats and Consequences (cont)

Risk Type	Low Consequence	Medium Consequence	High Consequence
Regulatory noncompliance	Routine fines, warnings, or adverse audit findings are anticipated.	Substantial fines, consent decrees, or limitations on business practices are anticipated.	Regulatory injunction or loss of license to conduct business is anticipated.
Business interruption	Business operations could continue indefinitely at increased cost or decreased efficiency.	Suspension of some business operations would be required within one week.	Suspension of business operations would be required within one day.
Safety hazard	Compensable damage to property is anticipated.	Recoverable illness or injury to humans, or reparable environmental harm is anticipated.	Permanent injury or death of humans, or irreparable environmental harm is anticipated.

Ideal Risk Management

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: $RISK = LIKELIHOOD \times IMPACT$

■ Very High Risk ■ High Risk ■ Medium Risk ■ Low Risk □ Insignificant

Impact	Extreme/Catastrophic	5	2	4	6	8	10
	Major	4	1.6	3.2	4.8	6.4	8
	Moderate	3	1.2	2.4	3.6	4.8	6
	Minor	2	0.8	1.6	2.4	3.2	4
	Insignificant	1	0.4	0.8	1.2	1.6	2
			1	2	3	4	5
			Remote	Unlikely	Credible	Likely	Almost Certain
			Likelihood				

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

Likelihood: Credible (3)

Impact: Major (4)

$$Risk = (3 \times 4) \times (10/25) = 4.8$$

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)

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

		Likelihood				
		1	2	3	4	5
Impact	Extreme/Catastrophic	3.3	5	6.7	8.3	10
	Major	2.7	4	5.3	6.7	8
	Moderate	2	3	4	5	6
	Minor	1.3	2	2.7	3.3	4
	Insignificant	0.7	1	1.3	1.7	2
		Remote	Unlikely	Credible	Likely	Almost Certain

Very High Risk High Risk Medium Risk Low Risk Insignificant

Likelihood

Make Your Risk Formula Fit You

- Weighted Likelihood: $RISK = LIKELIHOOD \times IMPACT + LIKELIHOOD$

■ Very High Risk
 ■ High Risk
 ■ Medium Risk
 ■ Low Risk
 ■ Insignificant

Impact	Extreme/Catastrophic	5	2	4	6	8	10
	Major	4	1.7	3.3	5	6.7	8.3
	Moderate	3	1.3	2.7	4	5.3	6.7
	Minor	2	1	2	3	4	5
	Insignificant	1	0.7	1.3	2	2.7	3.3
			1	2	3	4	5
			Remote	Unlikely	Credible	Likely	Almost Certain
			Likelihood				

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

Acceptable	Transferable	Reducible	Action
No	No	No	Do not engage in this – avoid the risk
No	No	Yes	Propose controls and reevaluate
No	Yes	No	Transfer or avoid the risk
No	Yes	Yes	Balance costs of control vs. transfer
Yes	No	No	Accept or avoid the risk
Yes	No	Yes	Balance costs of control vs. acceptance
Yes	Yes	No	Balance costs of transfer vs. acceptance
Yes	Yes	Yes	Balance all three and optimize

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

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

Special Publication 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



Word Docs and Excel Spreadsheets

National Instruments Information Security Program

Risk Management Form

Risk Management Form		
Probability: Low	Project: NIWC Content Synchronization Process	
Impact: Medium	Risk Title: Unencrypted SSH Key	
Time Frame: Ongoing	Originator: David Nelson	Origination Date: 1/12/2010
Severity: Low	Assigned to: Josh Sokol	Report Date: 5/26/2010
Risk Assessment		
Risk Statement: The identity file used to authenticate the NIWC Sync process' connection as weblog from the clutch tier to the webstage tier contains an unencrypted SSH key that could potentially be used, if obtained, for a malicious user to make connections as weblog to other servers where that user exists. A malicious user could also tamper with daemons/processes (primarily bttd and java) across production, test, and development systems. A malicious user could also change privileges to 'monolith' via sudoers and execute specific scripts. Also, there are sudoers entries that allow accounts to change privileges to weblog , without prompting for a password, and exercise those privileges with all available commands and files owned by weblog .		
Risk Context/Analysis: The NIWC Sync process was deployed into Production during the April 2007 Q2 release. This process provides the static includes files that ni.com uses to provide unique content based on a visitor's language preferences. Prior to this release, the NIWC Sync process was run on the STAGE database servers and sync'd out from there as the iasweb user. Since a purpose of the clutch tier is to handle batch jobs and a purpose of webstage is to do file synchronization, it was decided that NIWC Sync should be moved to those platforms. Recent scans have identified the identity file providing authentication for this process as a cause for concern. Proper permissions were used to protect this file so that only those with access to weblog should have been able to access it, but there is a known exploit with NFS that could potentially allow a malicious user to subvert that protection. David Nelson and Josh Sokol spent some time trying to modify the process to instead use an encrypted key, but ultimately abandoned this effort as we were unable to uptake this process without introducing additional risk by adding wildcards to the sudoers entry in order to make it work. No other solutions have been identified though we have not considered a complete architecture as a viable solution at this point.		
Risk Planning		
Strategy: <input type="checkbox"/> Research <input checked="" type="checkbox"/> Accept <input type="checkbox"/> Mitigate <input type="checkbox"/> Watch	Action Items Though architecture may be an option, we believe that the minimal risk is not enough to justify further action on this issue.	

1

National Instruments Information Security Program

Risk Tracking		
Event/Action/Commitment: Further research may be warranted in fixing the underlying NFS exploit that allows a malicious user to subvert file-level permission controls.		
Review Cycle:	<input checked="" type="checkbox"/> Semi-Annual <input type="checkbox"/> Annual	
Next Review Date:	7/1/2011	
Risk Resolution		
Sign-off:	Sign-off:	Sign-off:
Sign-off Date:	Sign-off Date:	Sign-off Date:

2



Lotus Notes





Several Futile Attempts at Purchasing a GRC
















So finally I wrote what I needed...



SimpleRisk

And released it under MPL 2.0 at BSides Austin in 2013...

 simplerisk-20130315-001.tgz	Remaining files	3 years ago
 simplerisk-20130319-001.tgz	Remaining files	3 years ago
 simplerisk-20130415-001.tgz	Remaining files	3 years ago
 simplerisk-20130501-001.tgz	Remaining files	3 years ago
 simplerisk-20130718-001.tgz	Remaining files	3 years ago
 simplerisk-20130827-001.tgz	Remaining files	3 years ago
 simplerisk-20130915-001.tgz	Remaining files	3 years ago
 simplerisk-20130916-001.tgz	Remaining files	3 years ago
 simplerisk-20130929-001.tgz	Remaining files	3 years ago
 simplerisk-20131024-001.tgz	Remaining files	3 years ago
 simplerisk-20131117-001.tgz	Remaining files	3 years ago

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



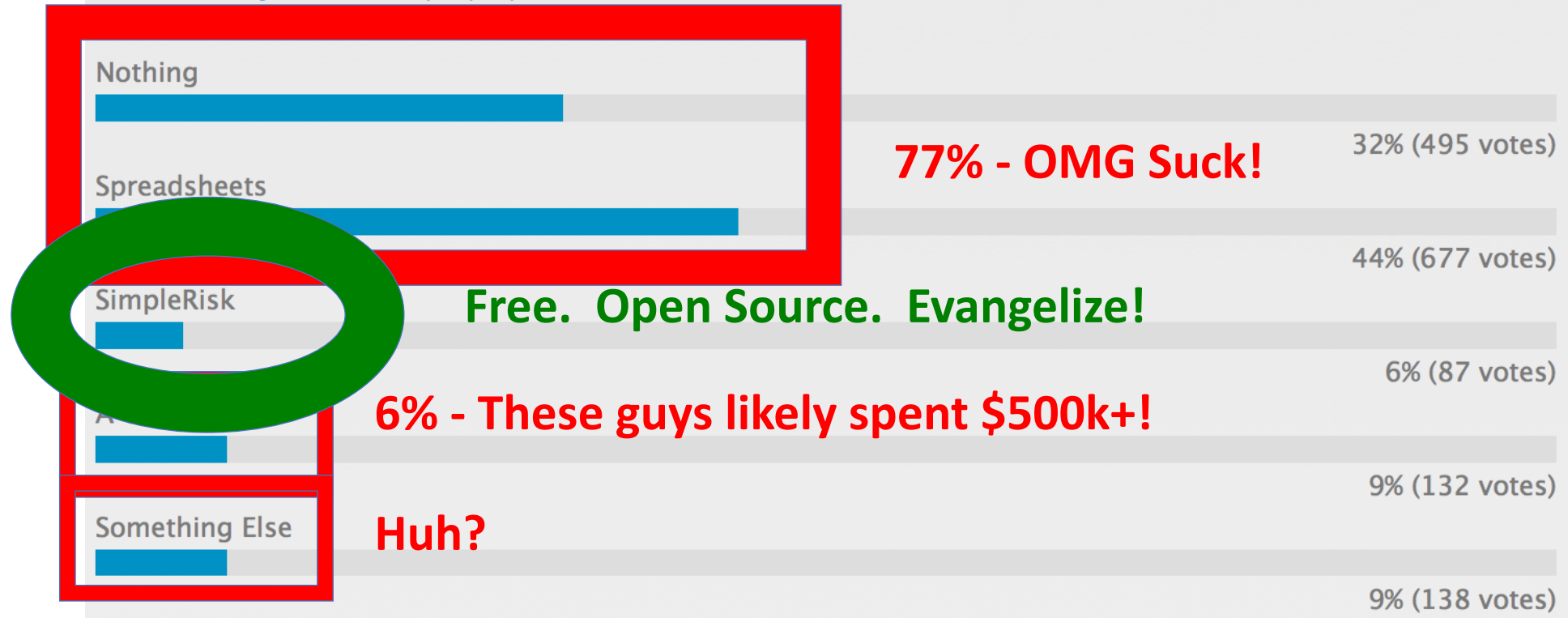
What is your organization using for risk management?

- Nothing
- Spreadsheets/Word/Similar
- SimpleRisk
- A GRC Tool
- Something Else



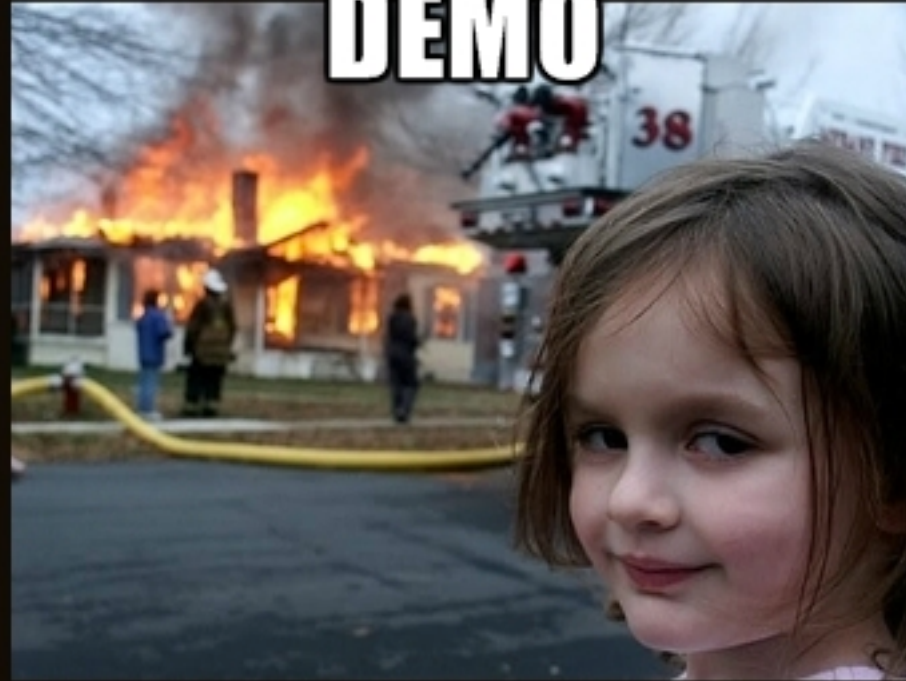
What is your organization using for risk management?

SUBMITTED BY [JSOKOL](#) ON FRI, 01/31/2014 - 23:42





**TIME FOR A LIVE
DEMO**



WHAT COULD GO WRONG?
memegenerator.net

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.



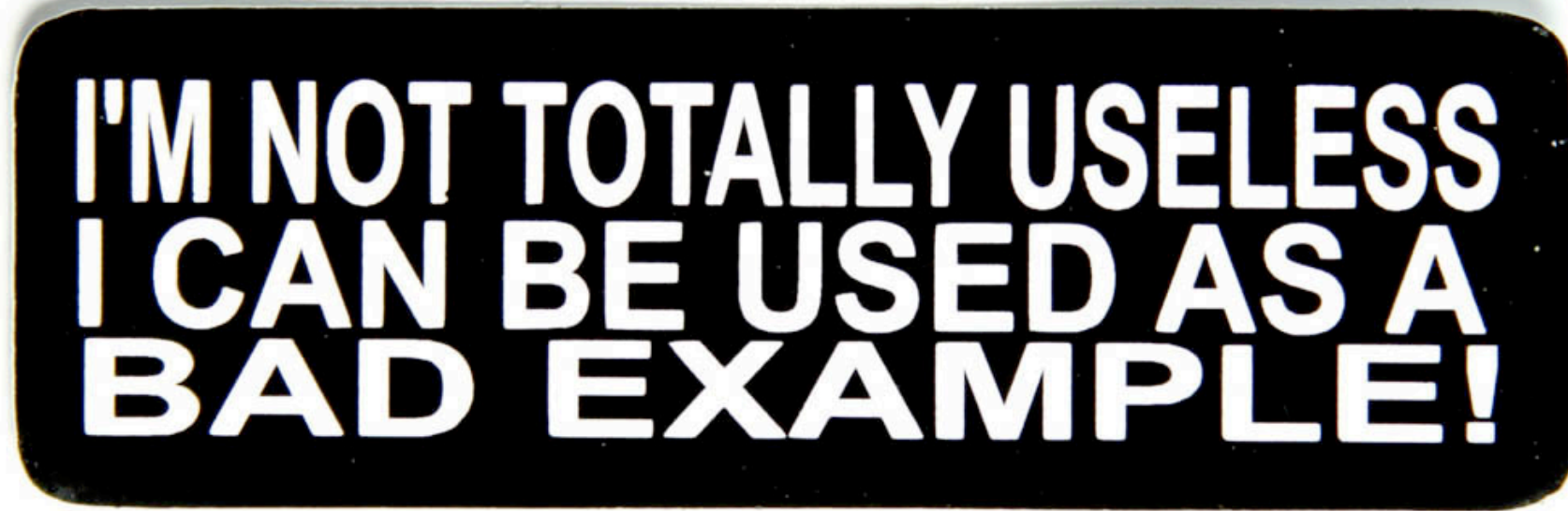
A Note on Naming Risk





Bad Example

“Customer database is not backed up.”





Better Example

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



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

@joshokol

<https://www.simplerisk.com>

<http://www.webadminblog.com>