Situational Awareness of the Risk Assessment (RA) Process

Kelly M. Yamaguchi, MS IS, CISSP
A Quick Introduction

How this talk today came about:

-Comments made in an earlier Software SIG resonated with the attendees of that particular meeting.

-The comments were based on findings from a study by Jyrki Kontio, Gerhard Getto, and Dieter Landes titled “Experiences in improving risk management processes using the concepts of the Riskit Method”.

... and why the analogy to situational awareness?
Just as prehistoric man needed to be aware of many cues regarding threats in the environment for survival...

developing and maintaining secure information systems too requires a great degree of situational awareness.

Reference: See the Endsley and Mahway, 2000 empirical study using Situational Awareness Theory
In the face of changing threats, there is a need for knowledge of “why” certain defenses (countermeasures, safeguards, or controls) have been (or plan to be) deployed in an information system to better ascertain the respective level of residual risk at any given time and reduce maintenance and redesign costs (Sindre and Opdahl, 2000).
• Need to ask/answer when, what, how, who, why
• Then answer “what’s the loss?”
• Followed by “Do we care”? 
• “If so how much?”
• “what (optimally) can we do about it?

IA is all about having Situational Awareness of Risk
When is it time to admit there is a problem??

“Traditional security risk analysis techniques do not necessarily lead to a complete list of all potential vulnerabilities and threats to consider at a component/environmental level” (McGraw, 2004, p. 79).

According to Buyens, De Win, and Joosen 2007, the process is frequently biased. Different types of bias (i.e., recency effect) have been proven to affect decision making.

Threats are hard to find and not easily known or understood regarding electronic information assets (business processes, network architecture, application, host OS, middleware, firmware). Finding vulnerabilities is at least automated (using scanners like Nessus); however, scanners aren’t able to find vulnerabilities stemming business logic flaws.

Entire categories of threat might be missed (the insider threat may be overlooked or underestimated) (Baskerville, 1993).

Incomplete information leads to lack of quality, in turn leading to a lack of understanding about risk, in turn leading to poor decision making in the selection of counter measures…
Tools: Methods/Techniques

- They often fail to describe in detail how to conduct underlying sub-processes (Verdon and McGraw)
- Complexity and information overload & our limitations with working memory
- We don’t always know why a control is in place, what exactly it is trying to prevent.
- Data that decision makers receives commonly includes high level summary info only (Price, 2007)
- There is an over-reliance on probability based on “Mathmatical guesses” (Price, 2007).
- Beachboard writes that users of RA techniques have no real “means of making an a' prior evaluation of the quality of the final output - need to subject methods/techniques to empirical validation” (2002).
- Metrics
Unaware → Advanced Performance

"Improvement actions are actually initiated if poor process performance is encountered."

What works? Some thoughts

- NIST SP 800 series publication guidelines and DISA STIGS/baseline controls
- Graphical visual models can facilitate communication about stakeholders and decision makers leading to more sound decision making about which safeguards to consider implementing (need to factor cost too of course) Khatri, Vessey, Ram and Ramesh 2006).
- Decision makers/validators must have the details at a lower level of abstraction to guard against subjectivity and bias that is inherent to the process as it involves people.
- Threat modeling: threat trees, attack vector analysis models, misuse cases, boundary analysis diagrams, attack surface analysis in addition to all the great tools from MITRE CVEs, CAPAC, etc…
- Explicitly consider and make transparent normative judgments underlying measures upon which their decisions about risks are made (Harper, King, Meersman, Reichman, Breen and Lynch, 2010).
Findings from Empirical Research


- “risk management should start before the project starts”;
- “different risks require different documentation”;
- “Graphs related to risks result in visual, more formal documentation of the risks, resulting in better communications and deeper, qualitative understanding of them”;
- “stakeholders and goals play a critical role in risk management; a common risk management framework makes risk management efficient”;
- “the RISKIT process increases the confidence in risk analysis results,”
- “intuitive risk management produces different results as compared to systematic explicit risk management process, and lastly, “;
- “risk identification requires special attention and a different mindset from other project and risk management activities”;

.
Empirical Studies cont.

2) Jyrki Kontio, Jani-Pekka Jokinen, Esa Rosendahl, "Visualizing and Formalizing Risk Information: An Experiment," metrics, pp. 196-206, 10th IEEE International Symposium on Software Metrics (METRICS '04), 2004

- Risk visualization and documentation methods were compared in controlled experiment
- Research indicated that a defined and sufficiently expressive visualization approach can help capture more of the risk information than less formal methods.
## Previous Risk Management at ORGs

<table>
<thead>
<tr>
<th></th>
<th><strong>Daimler-Benz</strong></th>
<th><strong>Nokia</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Risks listed weekly in every subproject</td>
<td>Risk were listed monthly</td>
</tr>
<tr>
<td>Formality</td>
<td>Reporting at project meetings within status reports</td>
<td>Monthly reporting of top 5 risks required</td>
</tr>
<tr>
<td>Method and tools</td>
<td>Documentation only for project tracking</td>
<td>Risks listed in order of importance</td>
</tr>
<tr>
<td>Identification techniques</td>
<td>By team members without any specific methods or techniques</td>
<td>By program and project managers without any specific methods</td>
</tr>
<tr>
<td>Analysis techniques</td>
<td>no specific analysis techniques</td>
<td>Ranking based on numerical estimates of probability and qualitative estimate of impact on schedule and quality</td>
</tr>
<tr>
<td>Controlling and tracking techniques</td>
<td>Part of normal project management</td>
<td>Part of normal project management</td>
</tr>
<tr>
<td>Training</td>
<td>No specific training for risk management</td>
<td>No specific training for risk management</td>
</tr>
</tbody>
</table>

“Does the description indicate the purpose of the application or component and how it fits into the rest of the system?

- Does the description include a link to the current specification?
- Does the language represent the level of effort the threat modeling team put into the analysis of the component’s security of the system?

- Does the description justify all the security features present in the system (access control/line/full stack walk demands for .NET assemblies, string/data validation, and so on)?

- Could the document be used to focus a code review for the component?

- Are the threat modeling document and source code consistent and aligned?” (p. 140)
“Have all entry points and elements functionally been considered?

Does the document contain issues that are not marked as resolved?

Where was the boundary component? Does the boundary include all functionality that is logically part of the component?

Does the document easily translate into a penetration test plan to ensure all threats are mitigated and determine whether any threats were missed? Also does the document enable a third party to scope an effort to verify the security of components? “ (p. 140)
Wrap up - So how do we get better sit awareness?

The ability to clearly recognize the control or controls that mitigate potential threat is paramount. Information systems risk managers cannot effectively manage risk without such traceability.

The architect of any risk management process needs to be cognizant of risk pertaining to the risk assessment process itself. Information System Risk decision makers need a process providing the right level of abstraction for analysis, the capability to drill-down to the explanatory details as needed.
Wrap up: (cont.)
So how do we get better sit awareness

- Need a trusted process to produce assessment that can be relied upon. Risk prioritization and the “right” set of controls hinges on this.

Scope, time, resources  
(the triple constraint)

security goals (CIA)
info states (trans., storage, processing)
countermeasures (tech., people, policies and pract.)

NIST SP 800 series guidelines plus John Peltier’s FRAAP for increased organizational risk performance, plus continuous monitoring, and a much expanded schema and process for threat assessment leading to better prioritization and mitigation of risk

Final thoughts

- Old security management vs. new model
- Model driven architecture approach needed (SABSA based on Zackman)
- Use of Security patterns for secure software systems
- Build accurate schema (factors affecting effectiveness)
- Use a Threat elicitation methodology to include both unstructured and structured techniques—One example Miller’s (Rockwell Corp) process + MICROSOFT’s STRIDE + Price’s (2008) + McCumber Cube+specific RA methodology(Octave, Octave-S, ISACA’s ect.).*
- Quantitative analysis of threats dependent on qualitative assessment first
- A few words on metrics
- Challenges to threat modeling such as how do we know when finished**


OCC Cubes to Extend the McCumber Cube (based on factors from McCumber 2004)

- Infrastructure threats:
  - Networks
  - Components
  - Software

- Risk to business process factors:
  - Asset relationship to bus, Process
  - Asset to architecture
  - Vulnerability to architecture

- Mode/control strategy:
  - Preventative
  - Detective
  - Deterrent

- Environment based physical threats based on future forecast
- Past experience with incident
- Documented past experience from Peer

- Agent Intent:
  - Effort/time
  - Skill
  - Expense

- Access attributes:
  - Physical
  - Logical
  - Probability or likelihood

- Vulnerability threat pairing:
  - Many to one (M:1)
  - One to Many (1:M)
  - One to one (1:1)

- Manmade:
  - External
  - Internal-accidental
  - Internal-hostile

- Threat Agent:
  - Manmade
  - Environmental (placeholder)