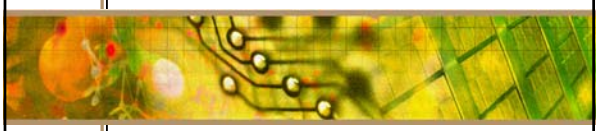
PURDUE UNIVERSITY

Assessing Risk for Fun and Profit



Presented by:
David Seidl, CISSP

SECURE PURDUE

What is risk assessment?

- In terms of this presentation, Risk assessment is the process of enumerating risks, determining their classifications, assigning probability and impact scores, and associating controls with each risk.

SECURE PURDUE

What is NOT risk assessment?

- Vulnerability Scanning
- Penetration testing
- Security reviews

SECURE PURDUE

Types of Risk Assessment

- Qualitative – measure in terms like "high, medium, and low" for probability and impact. Look at relative value, risk.
- Quantitative – measure in dollars and formulas.
- ITSP uses a qualitative, customized, expedited version of the Facilitated Risk Assessment Process (FRAP) called EFRAP.
- The government has switched to more qualitative processes – quantitative processes tend to take a very long time and while they generate "hard" data, they are rarely completed!

A quick vocabulary lesson

- Risk: potential events that have a negative impact on the Integrity, Confidentiality, and Availability of information.
- Vulnerability: condition of a missing or ineffectively administered safeguard or control that allows a risk to occur with a greater impact or frequency or both.
- Impact – the potential effect a risk may have on an asset.
- Control – measures taken to prevent, detect, minimize, or eliminate risk to protect the Integrity, Confidentiality, and Availability of information.
- Probability – the likelihood of the event occurring, rated from 0 (yeah, right, that'll never happen) to 1 (I am currently experiencing this event, I wish I had conducted a risk assessment).

What is a risk assessment?

- Risk Assessments measure the risk, the potential loss, and the probability that the loss will occur.
- For the formula folks – Risk (R) = Loss value (L) * Probability (P)

  R=L*P

A quick example

- People do risk assessments every day and don't even think of them that way.
- "If I don't get my wife a Christmas present, she's going to kill me"
  - Risk = Loss (life) * probability (definitely going to happen = 1)
  - In this example, an appropriate control is buying a gift, right?

A quick example (part 2)

- Part of any risk assessment is determining appropriate controls.
- There can be alternate controls
  - A pair of diamond earrings
  - Dinner out
  - Cookie cooling racks.
- Some controls may not be as effective, and assessments should recommend effective controls!

Dealing with risk

Accept the risk

- You accept responsibility and acknowledge awareness of the risk.
- Not always an acceptable alternative
- Who would you rather be?
- Formal acknowledgement can be a useful tool!

Dealing with risk

- Address and control the risk
- Determine appropriate controls, from both a risk remediation and a cost and effort to implement standpoint

Denial?

Why would I bother?

- Risk assessments are required for compliance
- Risk assessments provide direction for security controls
- Assessments can help justify resource expenditure
- Assessments can provide greater insight into process and architecture

PURDUE UNIVERSITY

So, how do we do an assessment?

SECURE PURDUE

PURDUE UNIVERSITY

Meta process

- Sponsor
- Scope
- Team
- Risk enumeration
- Risk classification and rating
- Control identification
- Report
- Action plan and execution

SECURE PURDUE

PURDUE UNIVERSITY

Risk Assessment Foundation

A strong foundation is essential to the success of a risk assessment!

SECURE PURDUE

Now we're ready to assess risk!

- Sponsorship
  - A key factor in the success of your risk assessment is having an effective sponsor.
  - The sponsor should be in charge of the area or system being assessed.
  - Sponsors should be willing to take responsibility for the assessment and to use its findings.

Risk Assessment

- Scope
  - Carefully scope your assessment
  - Write a scope statement and make sure your group understands it.
  - Use scope to keep on topic during brainstorming, but do not limit brainstorming.

Choosing a team

- Diversity
- Expertise
- Sanity
- Leadership
- Numbers

Diversity and Expertise

- Get the people who know the system or area
- Don't pick your top administrator
- Don't forget the people who use the system!
- Look for different viewpoints

Ever elusive sanity…

- Don't pick the two people who cannot ever get along
- Do pick people with differing viewpoints
- Remember, you want information from your team – pick people who will contribute!

Leadership: Herding Cats

- Choose a neutral leader
- Their goal is not to lead so much as to facilitate and keep the group on track. Think debate moderator, not dictator.
- Set rules and follow them

Numbers

What has twenty legs, ten heads, and can't get along with itself for long enough to make a decision?

- Smaller teams are more effective
- Size your team for the scope of the assessment
- Balance a nimble, manageable team with the need to have subject matter experts.
- Our magic number is usually 5-8 participants.

Now you have a crack team – what next?

Formal Risk Assessment

- Introduction - team members introduce themselves and very briefly describe their area of responsibility or expertise relevant to the scope of the assessment.
- Brainstorm - Risks are brainstormed, no idea will be rejected or negatively discussed in the initial brainstorm.
- Identification - risks categorized as affecting Confidentiality, Integrity, or Availability
- Prioritization - risks are prioritized by their impact, and probability
- Controls - controls are identified and recommended based on the risks identified. Controls are prioritized based on cost, priority, and capability to implement.
- Report - a report is prepared by the facilitator and approved by the team.
- Sign-off - the project lead is given the document and signs off on it.

Risk Assessment

- Brainstorm
  - There are no wrong answers
  - Don't contradict
  - Duplicates are ok
  - Keep it moving
  - One person talks at a time
  - Only one person may be angry at a time!

Categorization

- Label each risk as a risk to one or more of confidentiality, integrity, or availability.

Risk Types – CIA, another TLA

- **Confidentiality**: information has not undergone unauthorized disclosure
- **Integrity**: information is as intended, without unauthorized or undesirable modification or corruption.
- **Availability**: protection from unauthorized attempts to withhold information or computer resources.

High, Medium, and Low

- High, medium, and low mean something different to everyone.
- Assign understandable values, then seek group agreement.
- Document thought process if necessary or appropriate.

Assessing Risk Levels

- Confidentiality Risk is:
- HIGH – if unauthorized use or disclosure would severely impact business operations, make a segment of the company unable to function, or cause high monetary loss.
- MODERATE – if use or disclosure does not severely affect operations or does not result in high monetary loss.
- LOW – if use or disclosure does not affect operations or result in significant monetary loss.

Assessing Risk Levels

- Integrity Risk is:
- HIGH - if data inaccuracy, incompleteness or unauthorized modification causes failures of operations, revenue loss, wrong decisions to be made, loss in productivity or loss of customer confidence or market share.
- MODERATE - if it causes inability to make some decisions, but the problem is not difficult to detect and correct, and does not severely impact business operations.
- LOW – if alternative validations of the information make it possible to continue business operations.

Assessing Risk Levels

Availability Risk is:

- HIGH – if unavailable information impairs business operations, affects customer service, or makes it impossible to process revenues.
- MODERATE – if unavailable information causes productivity loss, but does not interrupt customer service or revenue generation.
- LOW – if unavailable information does not severely impact business operations.

Probability and Impact

- Probability
  - How likely is the event?
    - » High: It has happened in the past year, or is happening now.
    - » Medium: It has happened in the past 2 years, or is somewhat likely to happen in the next two years.
    - » Low: It rarely happens, or is unlikely to happen in the next 2 years.
  - Probability ratings should be determined as appropriate to the goals of the assessment!

Probability and Impact

- Impact
  - Financial, reputation, time
    - » High impact: will cost a significant amount of your yearly budget, will consume large amounts of time, will severely hurt your reputation.
    - » Medium impact: will cost some of your yearly budget, will consume some time, or will damage your reputation.
    - » Low impact: negligible effect or cost.

Group example

- Suggest a risk
- Classify the risk
- Rate Probability
- Rate Impact
- Suggest controls

Reporting

- Reports should include risks, probability and impact ratings, and controls for each risk.
- Reports should be signed off on by the project sponsor and the areas that must implement controls.
- Choose a reasonable implementation timeframe and follow up!

Nobody else wants to play

- You can conduct risk assessments on your own
- Mini-assessments are useful as a starting point for projects and to review existing systems and applications
- Beware of your own bias
- Document it!

Next steps in campus RA

- ITSP is working with Prevari to provide a web based compliance and risk assessment tool.
- Early testing will begin late this year.
- Roadmap includes GLBA compliance as our first large scale use.

High risk Q&A

Ask away!

Bonus Risky Behavior

PURDUE UNIVERSITY

Bonus Risky Behavior

PURDUE UNIVERSITY

Bonus Risky Behavior

PURDUE UNIVERSITY

Bonus Risky Behavior