Scoring Risk to Take Action
Risk Language Your Executives Can Use
Dan Simanek, SSCP
Stefan Wahe, Deputy CISO

Today’s Take Away
Basics of System Categorization
How to Score Risk
System Categorization

- The classification of an information system based on the type of data, the availability requirements, business processes, and laws & regulations.
- The security controls are determined by the categorization of the system.
- Considered Inherent Risk, or the risk to information before security controls are applied.

System Risk

- The aggregate total of the identified gap in security controls balanced against the product of risk likelihood and risk impact of the gap being exploited by a threat agent.
- The residual risk after the security controls have been applied
- The Risk Executive accepts the level of risk

There are five options for System Categorization

- High
- Moderate-High
- Moderate
- Moderate-Low
- Low

Why Categorization?

Informs the type and level of security controls that should be implemented and maintained.
Examples of Data Classification

<table>
<thead>
<tr>
<th>Restricted</th>
<th>Sensitive</th>
<th>Internal</th>
<th>Public</th>
</tr>
</thead>
</table>
| • Social Security Number
   • Bank Account Number
   • Protected Health Information
   • Student financial account information | • Student Grades
   • Student Schedule / Class Roster
   • Most Research Data
   • Employee Benefits / Garnishments | • Time Sheets
   • Expense Reports
   • Vendors providing research resources
   • Course content | • Final 2019 Football Schedule
   • Approved Employee Directory
   • 2019-20 Course Catalog |
Exercise-1:
Classify these Data Combinations

1. SSN and Name and Date of Birth
2. Class Roster in Student Information System
3. A student’s financial aid file
4. UW-Madison Course Guide
5. An employee’s benefit information
6. Employees performance review
7. Unpublished research results that may lead to a new business idea

Availability Considerations

• What happens to the end-users if the system is not available?
• What are the impacts to the system owner and risk executive if the system is not available?
• What is the loss of opportunity if the system is not available?
• What are impacts to the business processes if the system is not available?
• Can business process still occur if the system is not available?

High
• Required 24x7
• Significant loss of revenue
• Significant impacts to operations if unavailable for more than 24 hours.

Moderate
• Required 9x5
• Moderate loss of revenue
• Moderate operational impacts if unavailable for 2 to 5 days.

Low
• No defined operational hours
• Minor loss of revenue
• Minor operational impacts.
1. Provides life and safety services for faculty, students, and staff.
2. Enrollment management staff use the system during regular business hours (M-F 7:45 AM to 4:30 PM).
3. wisc.edu
4. Server hosting data used for a 12-month research study.
5. System that pays employees at various cycles.
6. The system provides on-line learning modules for accredited courses.

| Exercise-3: Categorize the Information System | | |
| --- | --- | |
| **Human Capital Management System** | **Major Data Elements** | • Employee & Dependent Names  
• Employee & Dependent DoB  
• SSN  
• Address  
• Benefit Information  

**Availability Requirements** | • Required to meet multiple, staggered payroll cycles.  
• Recruitment processes  
• Performance management  

**Business Process** | • Creating new employee records  
• Submitting and approving time reports  
• Paying employees  

**Laws & Regulations** | • Wisconsin State Statute 134.98 |
Exercise-4: Categorize the Information System

Research Protocol Database

| Major Data Elements | • Research number  
<table>
<thead>
<tr>
<th></th>
<th>• Research protocol description</th>
</tr>
</thead>
</table>
| Availability Requirements |  • PI's need access to information during normal operating hours to submit and review proposals.  
|                      |  • IRBs need access to approve research projects. |
| Business Process     |  • Approval to operate a research project on campus.  
|                      |  • Approved protocols can not be changed without review. |
| Laws & Regulations   |  • None |

Introduction to Risk Scoring

• Risks or gaps are identified through document review and testing.
• Test systems to determine alignment with documented processes, configurations, and other controls.
• What is the estimated risk of any controls that are not fully implemented or vulnerabilities identified through testing?
  • Identify the threat related to a risk or a gap.
  • What is the Impact of the gap being exploited?
  • What is the Likelihood being exploited?
## Risk Impact Matrix

<table>
<thead>
<tr>
<th>Score</th>
<th>Availability</th>
<th>Integrity</th>
<th>Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minor delays in hours</td>
<td>Financial loss or regulatory fines of less than $5,000.</td>
<td>Breach impacting less than 500 records that does not require notification of loss nor financial impacts associated with remediation.</td>
</tr>
<tr>
<td>2</td>
<td>Minor delay in a full day</td>
<td>Financial loss or regulatory fines of between $5,000 and $25,000.</td>
<td>Breach impacting more than 500 records that requires notification of loss and potential financial impacts associated with remediation not exceeding $25,000.</td>
</tr>
<tr>
<td>3</td>
<td>Significant delay of multiple days</td>
<td>Financial loss or regulatory fines of between $25,000 and $50,000.</td>
<td>Breach impacting more than 500 records that requires notification of loss and potential financial impacts associated with remediation not exceeding $100,000.</td>
</tr>
<tr>
<td>4</td>
<td>Significant delays exceeding a week</td>
<td>Financial loss or regulatory fines of between $50,000 and $250,000.</td>
<td>Breach impacting more than 500 records that requires notification of loss and potential financial impacts associated with remediation not exceeding $250,000.</td>
</tr>
<tr>
<td>5</td>
<td>Major delays exceeding multiple weeks to months</td>
<td>Financial loss or regulatory fines of more than $250,000.</td>
<td>Breach impacting more than 500 records that requires notification of loss and potential financial impacts associated with remediation exceeding $250,000.</td>
</tr>
</tbody>
</table>
## Risk Likelihood Matrix

<table>
<thead>
<tr>
<th>Score</th>
<th>Score Description</th>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not Foreseeable / Unlikely</td>
<td>Not once in 3 years</td>
<td>Exploitation of the vulnerability or gap is not reasonable without extensive expertise, time, and resources. The effort level is great enough to discourage most known organized crime groups.</td>
</tr>
<tr>
<td>2</td>
<td>Foreseeable / Somewhat Likely</td>
<td>Once in 3 years</td>
<td>Security controls are in place to stop most attempts by attackers. No automated to remotely discover and execute the vulnerability are known. Exploitation of the vulnerability would require technical expertise or time and resources beyond those of an individual attacker or insider threat.</td>
</tr>
<tr>
<td>3</td>
<td>Repeated / Likely</td>
<td>2 to 3 times in 3 years</td>
<td>Security controls are not implemented to stop attacks with certainty. Tools to remotely discover or execute the vulnerability are not extensively/freely available. Exploitation of method require some expertise, time, and resources to operate to the level that a small organization is likely to be able to gather or an insider is able to operate.</td>
</tr>
<tr>
<td>4</td>
<td>Recurring / Very Likely</td>
<td>More than once a year</td>
<td>Security controls are not implemented to stop or even slow progress of an attempted attack. Known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain or access is available to an inside threat.</td>
</tr>
<tr>
<td>5</td>
<td>Frequent / Almost certain or already occurred</td>
<td>Monthly or greater</td>
<td>Security controls are not implemented to stop attacks, or detect successful exploitation of the vulnerability or gap. The vulnerability or gap is known to be exploitable and discoverable with well-known methods and tools to do so. Evidence discovered during testing indicates that exploitation of the vulnerability may have already occurred.</td>
</tr>
</tbody>
</table>

### Factors to Score Risk

- Threats posed to that asset based on identified gaps.
- The vulnerabilities that expose the asset.
- The impact to any of the UW-Madison mission, values or guiding principles.
- The likelihood that the availability, integrity or confidentiality of the asset will be compromised through a given vulnerability exploited by a threat actor.
- Risks of a should be evaluated individually for Availability, Integrity and Confidentiality (AIC) of the asset.
Research Project Example

1. Review the observation and potential threats for each risk.
2. Score the impact if the threat is realized. Use the impact matrix listed in the Risk Scoring instructions.
3. Score the probability, or likelihood, of the threat occurring. Use the likelihood matrix listed in the Risk Scoring instructions.
4. Multiply the results for the impact score and the likelihood score.

Reverences and Resources

Primary Contact Method: GRC Cybersecurity: grc-cybersecurity@cio.wisc.edu

Risk Management Framework: https://go.wisc.edu/746oog

HIPAA Security Program: https://it.wisc.edu/about/division-of-information-technology/strategic-operations-departments-people/cybersecurity/hipaa-security-program/
