Cybersecurity Risk Management

Through the Cybersecurity Framework

March 2018
There are hundreds if not thousands of controls and standards for implementing cybersecurity.
Defining cybersecurity programs is typically done through compliance.
Compliance does not always mean secure
Other times security is not commensurate with the risk
Our Cybersecurity Framework assessments uses all three components of the Framework:

1. **Framework Core**
2. **Implementation Tiers**
   - Tier 1 - Partial
   - Tier 2 - Risk Informed
   - Tier 3 - Repeatable
   - Tier 4 - Adaptive
3. **Framework Profiles**

---

**Framework Core**
- Function: [Details]
- Category: [Details]
- Subcategory: [Details]
- Informational Reference: [Details]

**Implementation Tiers**
- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

**Framework Profiles**
- Function: [Details]
- Category: [Details]
- Subcategory: [Details]
- Priority: [Details]
- Org Policy: [Details]
- Org Trustee: [Details]
- Status: [Details]
- Comments: [Details]
The Cybersecurity Framework defines a seven step implementation process.
The risk register ensures proper cybersecurity considerations are prioritized and defined.

Security Risks are prioritized in the register:
- Business objectives are addressed timely
- Properly define security countermeasures

**STEP 4:** **Conduct a Risk Assessment**

<table>
<thead>
<tr>
<th>Risk #</th>
<th>Example Actor/Source</th>
<th>Risk Area</th>
<th>Risk Event</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Sensitive privacy-related electronic data</td>
<td>is wrongly disclosed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Sensitive research data</td>
<td>is corrupted or modified without authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Staff member(s) or 3rd Party Provider(s) fail to comply with legal, contractual or regulatory requirements</td>
<td>is wrongly disclosed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Sensitive research data</td>
<td>is corrupted or modified without authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Sensitive research data</td>
<td>is deleted without authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Internal (accidental, e.g., hw/software failure), Internal (deliberate), External (deliberate, e.g., malware, ransomware), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Sensitive research data</td>
<td>is deleted without authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Internal (accidental, Internal (deliberate), External (deliberate), 3rd Party (accidental), 3rd Party (deliberate)</td>
<td>Staff member(s) or 3rd Party Provider(s) fail to comply with legal, contractual or regulatory requirements</td>
<td>is wrongly disclosed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Likelihood**: Identifies how often the threat is expected to act on resources

**Impact**: Assesses the effect the security risk will have on business functions and operations
The implementation steps conclude with an action plan for improving the cybersecurity program.

**Step 5:**
Create a Target Profile

**Step 6:**
Determine, Analyze, and Prioritize Gaps

**Step 7:**
Implement Action Plan
Now you're ready to successfully use the Framework to improve your cybersecurity program.
Questions?

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@G2-inc.com
(443) 292-6679

Visit us at: ManageTheRisk.com