Blind Spots: A New Cyber-Security Metric for Measuring Incident Response Readiness

Benjamin Aziz, Ali Malik & Jeyong Jung
Content

• Introduction
• Existing Metrics
• Our New Metric
• Future Work
• Conclusion
Introduction

- Cyber-security
- Metrics
- Risk metrics are beneficial
Exiting Metrics

- ITU-T\(^1\)
- CIS\(^2\)
- Payne\(^3\) suggested 7 steps toward security metrics
• Two closely related Cyber-security metrics defined in CIS:
  ➢ **Mean Time Between Security Incidents** (MTBSI)
  ➢ **Mean Time to Incident Recovery** (MTIR)
Cont...

- MTBSI

\[
MTBSI = \frac{\sum_{i=1}^{n-1} (Date_{-Occurrence}(incident_{i+1}) - Date_{-Occurrence}(incident_i))}{n-1}
\]
Cont...

- MTIR

\[ MTIR = \frac{\sum_{i=1}^{n} (\text{Date of Recovery}(\text{incident}_i) - \text{Date of Occurrence}(\text{incident}_i))}{n} \]
Our New Metric

- **The Mean Blind Spot Metric MBS**

\[
MBS = \frac{\sum_{i=1}^{n-1} (\text{Date of Occurrence}(\text{incident}_{i+1}) - \text{Date of Recovery}(\text{incident}_i))}{n - 1}
\]

**EX:**

<table>
<thead>
<tr>
<th>Incident Number</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occurrence</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>02.06</td>
<td>02.06</td>
<td>02.06</td>
<td>02.06</td>
</tr>
<tr>
<td>Date/Time</td>
<td>12:10</td>
<td>12:50</td>
<td>14:00</td>
<td>14:56</td>
<td>18:30</td>
<td>18:35</td>
<td>07:20</td>
<td>09:20</td>
<td>12:30</td>
<td>19:40</td>
</tr>
<tr>
<td>Recovery</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>01.06</td>
<td>02.06</td>
<td>02.06</td>
<td>02.06</td>
<td>03.06</td>
</tr>
<tr>
<td>Date/Time</td>
<td>13:55</td>
<td>14:40</td>
<td>19:30</td>
<td>19:05</td>
<td>20:10</td>
<td>21:30</td>
<td>11:10</td>
<td>13:50</td>
<td>15:50</td>
<td>00:15</td>
</tr>
<tr>
<td>Blind Spot Interval</td>
<td>-65</td>
<td>-40</td>
<td>-274</td>
<td>-35</td>
<td>-95</td>
<td>590</td>
<td>-110</td>
<td>-80</td>
<td>230</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3.** An Example Showing Incidents’ Occurrence, Recovery and Blind Spots Times

\[
MBS = \frac{((-65)+(-40)+(-274)+(-35)+(-95)+590+(-110)+(-80)+230)}{9} = +13.44
\]

mins/blind spot interval
• **Approximated Mean Blind Spot AMBS**
  
  It can be calculated directly using MTIR and MTBSI

\[
AMBS = \frac{MTIR}{MTBSI}
\]
• **Ratio of Blind Spot RBS**

  - This is not strictly based on the MBS, but more fundamentally based on the concept of blind spot.

\[
RBS = \frac{\text{card}\{y : y = \frac{BS}{BSA} \land y > 1\}}{n - 1} \times 100\%
\]

  - Blind Spot Appetite BSA is required (Ex: \( \cdot 60 \))
  - The ratio BS/BSA represents how far a blind spot from the appetite value.
Based on the previous definition, RBS will capture the BS/BSA values >1

\[ \text{RBS} = \frac{\text{card}\{1.08, 4.57, 1.58, 1.83, 1.33\}}{9} \times 100\% = 56\% \text{ (Risky)} \]
Future Work

- The Vocabulary for Event Recording and Incident Sharing \( \text{VERIS} \)
  http://veriscommunity.net/vcdb.html
- Validate our proposed metric
- Propose new metrics based on the \( \text{VERIS} \)
Conclusion

✓ Cyber-security metrics are crucial for business organisations.

✓ Blind Spot concept proposed as a new risk metric.

✓ Three variants of the new proposed metric are defined.
References


2. for Internet Security, T.C.: Cis security metrics v1.1.0 (Nov 2010)

Thank you all
Any Question ?