Metrics for Justifying SOC Investment to the CEO and Board

John Pescatore
Director, SANS Institute
jpescatore@sans.org
Why Do Some Do Better Than Others?

- 980 breaches in 2016
  - What did the other 9,020 of the F10000 do differently?
  - (781 in 2015)
- On average, 36K records exposed per breach
  - What did those who limited breach size do differently?
  - (Average = 215K in 2015)
- Almost invariably, the organizations with the least cyber incident impact have the strongest security teams and processes.

Source: Identity Theft Resource Center
Basic Security Hygiene and a Strong SOC as Foundation

- Mature = Effective and efficient
- Key indicators:
  - Basic security hygiene
  - Security Operations Center processes and tools
  - “Business Security Analysts”
- Integration into procurement, M&A, supply chain decisions
- Cross-industry participation
Communicating to the C-Suite and Board of Directors

• We mostly know **what** to do in security, and we can learn **how** to do **our** part.

• The biggest obstacle to success is getting **others** to do **their** part.

• Support from **above** is the most powerful force to break through.

• Goal: Learn how to inform CEOs and Boards and convince them to back SOC strategies to **drive change and provide measurable improvements in cybersecurity**.

---

**Would you say your company’s Board of Directors has taken an active interest in cybersecurity issues?**

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>30%</td>
</tr>
<tr>
<td>Agree</td>
<td>45%</td>
</tr>
<tr>
<td>Neither agree nor disagree</td>
<td>15%</td>
</tr>
<tr>
<td>Disagree</td>
<td>9%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: PaloAlto Networks
The Messages Back from Directors

• “Security people don’t speak our language. In fact, at each briefing they seem to speak a different language.”
• “The CISO is great at talking about ‘blood in the streets’ but very weak on strategy to avoid disasters.”
• “We know bad things will happen – the CEO and CFO and VPs inform us of business problems frequently. We want to have confidence that basic competence and strategies are in place to reduce bottom line impact.”
• “The Board is not an ATM – we are not here to give you resources.”
• “A big part of being believable and building our trust is showing us how we compare to competitors, other industries, some kind of standards or benchmarks.”
Data Vs. More Horror Stories

• Cybercrime impact is growing faster than most other forms of crime and fraud:
  • Identity theft for new account fraud
  • “Ransomware” – hold information hostage
  • Denial of service – hold Internet connection hostage
  • Industrial espionage
• The vast majority of asset misappropriation (insider threats) are enabled by IT vulnerabilities.
• Cybercrime attack techniques are often adopted by nation states.

SOC Data to Close the Gap

What metrics do CISOs rely on most? What’s reported to the Board? Which do Board members value most?

<table>
<thead>
<tr>
<th>Category</th>
<th>Important to the CISO</th>
<th>Important to the Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>System vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk posture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response metrics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer benchmarks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incidents/events</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance/maturity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business enablement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assets and users</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Focal Point 2017
Delivering Security Efficiency and Effectiveness

Efficiency

• Decrease the cost of dealing with known threats
• Decrease the impact of residual risks
• Decrease the cost of demonstrating compliance
• Reduce business damage due to security failures
• Maintaining level of protection with less EBITDA impact

Effectiveness

• Increase the speed of dealing with a new threat or technology
• Decrease the time required to secure a new business application, partner, supplier
• Reducing incident cost
• Less down time
• Fewer customer defections
• Security as a competitive business factor
Cybersecurity Frameworks

Center for Internet Security Critical Security Controls

Frameworks:
- Critical Security Controls
- NIST Cybersecurity Framework
- ISO 27001
- Industry-specific
  - HIPAA
  - Retail
  - NERC
Power Utility Example

Continuous gap analysis vs. the Critical Security Controls

Critical Control Category

<table>
<thead>
<tr>
<th>QW</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

Compliant
Compliant In Spirit
Work in Progress
Not appropriate for our culture
Gap with no current plan

Plus: Continuous:
1) “Mean time to Detect Incidents” and “Mean time to Contain Incidents”
2) 4 key automated vulnerability metrics
Basic Security Hygiene ROI Example

- **Catch**: malicious software with a whitelist
- **Patch**: applications and operating system
- **Match**: the right people with the right privileges

mitigates at least **85%** of targeted cyber intrusions

---

Australian Signals Directorate

Reveal Their Secrets - Protect Our Own
### Threat Visibility in Action

**Defensive Metrics**
- **WSA**: 6M web transactions/day – 75K blocked automatically
- **IDS/IPS**: 1.5M alerts per day from ~350 sensors
- **ESA**: 5.4M emails inspected, 4.1M blocked
- **Lancome**: 15B NetFlow records analysed per day
- **Passive DNS**: 5.8B DNS records per day
- **Volume**: 27Tb of traffic analysed per day

**Active Metrics**

**Universal Security Metrics**

<table>
<thead>
<tr>
<th>FY</th>
<th>Q1 FY12</th>
<th>Q1 FY13</th>
<th>Q1 FY14</th>
<th>Q1 FY15</th>
<th>Q1 FY16</th>
<th>Q2 FY16</th>
<th>Q3 FY16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Type</td>
<td>FY13</td>
<td>FY14</td>
<td>FY15</td>
<td>1HFY16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco FireAMP – Advanced Malware Detection</td>
<td>34</td>
<td>656</td>
<td>1338</td>
<td>787</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Web Security Appliance</td>
<td>149</td>
<td>631</td>
<td>314</td>
<td>604</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Intrusion Prevention System</td>
<td>72</td>
<td>95</td>
<td>1778</td>
<td>1483</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passive DNS/RIFZ</td>
<td>56</td>
<td>114</td>
<td>530</td>
<td>260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Based IPS</td>
<td>14</td>
<td>107</td>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow</td>
<td>15</td>
<td>54</td>
<td>42</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>320</td>
<td>1630</td>
<td>4209</td>
<td>3530</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Goal**
- Time-to-Detect = 24Hrs and Time-to-Contain = 36 Hrs
Summary

• Mature SOC processes are critical to control risk, **limit business damage and customer impact** – need to **demonstrate**

• Response and recovery effectiveness and efficiency metrics are key to monitor and show improvement – **against business critical functions**.

• Board of Directors can play a role in assessing if cybersecurity in overcoming strategic obstacles – but **you need to get to basic security hygiene first**.

• The C-suite is where the first 80% of the battle will be won – **find a friend**.

• Show how investments in the SOC act as **force multipliers**.

• Be realistically about out-sourcing vs. all DIY>