VALUE AT RISK: DECISION MAKING IN CYBERSECURITY INVESTMENTS

Sateesh Bolloju

Principal Architect,
Product Security, Inflyt Experience
Thales Avionics Inc.
@s_bolloju
Views and opinions expressed in this session are mine and not those of Thales, RSA or any other entity.
Video with visuals and themes which highlights value at risk concept

Value at Risk - Theme Video
Digital is

The Economy
What’s at risk?

- Financial Risk
- Business Disruption
- Regulatory & Compliance
- Customer Trust
You heard this?
Polling question?

- Session ID: CXO-W12
- You are challenged to justify security investments
  - Agree
  - Neutral
  - Disagree

Poll Results
Decision making
Cyber Security Investments
Challenge today

Cyber Security Investments

What?  Where?  How much?
What’s the answer?

Value at Risk (VaR): A measure to quantify the potential loss over a specific time frame.
Framework & Methodology

Threats
- Hacktivism
- Data Loss/Breach
- Malware/Ransomware
- Internal/3rd parties

Vulnerabilities
- Mistakes
- Lack of controls/Tools
- Products
- Poor practices

Value at Risk
- Assets Value
- Brand Value

Parameters
- Risk
  - Loss Event Frequency
  - Vulnerability
- Loss Magnitude
  - Threat Event Frequency
  - Primary Loss
  - Secondary Risk

Lose no more than $$$$$ amount over a period of time with 95% confidence with a successful attack
Quantify Risks

Value at Risk =

Expected Loss * Probability * Frequency

Standardize VaR model based on identified parameters, environment, specific to the company and cyber maturity
Value at Risk in Action

Scenario
Lack of privileged access controls for an infrastructure leads to data loss

Expected loss = $116.3 million
- $110 million (Say 500,000 customers’ data breached, $221/record**)
- $1 million (Incident response, recovery, liability/legal fees)
- $5 million (Brand value, 1% percent of annual revenue)
- $300,000 (Productivity loss to manual and inefficient PAM processes)

Probability = 10% (3% after investment)
Frequency = 1 in 3 years (0.2 after)

Before

Value at Risk (VaR) $11.63 million

After

Investment $3 million

Value at Risk (VaR) $0.7 million

Benefit = VaR (B) – VaR (A)

** Cost per record for US, refer to 2016 Cost of Data Breach Study by Ponemon/IBM research
<table>
<thead>
<tr>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product design documents stolen by rogue employee (IP loss)</td>
<td>Exploited known CVE (Apache, Android or Open SSL) disrupted business services</td>
<td>Lack of privileged access controls for an infrastructure leads to data loss</td>
</tr>
<tr>
<td>Expected loss = $21.6 million</td>
<td>Expected loss = $13.5 million</td>
<td>Expected loss = $116.3 million</td>
</tr>
<tr>
<td>- $20,000,000 (10% of revenue loss)</td>
<td>- No data loss</td>
<td>- $110 million (Say 500,000 customers data breached, $221/record**)</td>
</tr>
<tr>
<td>- $350k, Incident response, recovery, &amp; communications</td>
<td>- $500k, Incident response and discovery analysis due to lack of automated AIM tools</td>
<td>- $1 million, Incident response, recovery, liability</td>
</tr>
<tr>
<td>- $250k, Productivity loss</td>
<td>- $2 million due to fines for not providing services</td>
<td>- $5 million, Brand value loss (1% percent of annual revenue)</td>
</tr>
<tr>
<td>- $1 million, Loss due to secondary risk</td>
<td>- $1 million due to productivity loss</td>
<td>- $300,000, Productivity loss to manual and inefficient PAM processes)</td>
</tr>
<tr>
<td>- No additional brand value loss</td>
<td>- $10 million (10% of potential contract loss)</td>
<td></td>
</tr>
<tr>
<td>Probability = 5%</td>
<td>Probability = 10%</td>
<td>Probability = 10%</td>
</tr>
<tr>
<td>Frequency = 1 event in 3 years</td>
<td>Time frame = 2 events in 3 years</td>
<td>Time frame = 1 event in 3 years</td>
</tr>
<tr>
<td>Value at Risk = $1.08 million</td>
<td>Value at Risk = $2.70 million</td>
<td>Value at Risk = $11.33 million</td>
</tr>
</tbody>
</table>

**Cost per record for US, refer to 2016 Cost of Data Breach Study by Ponemon/IBM research**
How much should be invested in Cybersecurity?
Optimal Cyber Investments?

Benefits > Cost of Investment

Invest no more than 1/3 of Value at Risk

* Adapted from Gordon-Loeb Model
TO SUMMARIZE...
Summary

- Understand product security threats
- Quantify cyber risks
- Determine VaR
- Decide ‘What, Where and How much’ to invest
Lessons Learned

- Keep it simple
- Make it realistic and apply to your situation
- Educate your stakeholders
- Don’t fall in love with products or technologies
- Always ask what’s the “Value at Risk”
How to apply?

1. Understand VaR model
2. Determine applicability
3. Identify scenarios and adopt
4. Socialize and obtain buy-in
5. Implement VaR
Questions?

sateesh.bolloju@us.thalesgroup.com
www.linkedin.com/in/sateeshbolloju
@s_bolloju
Thank you!