ChiBrrCon 2022

The Power of Cyber Economics

May 2022
What is Cyber Economics?

Cyber economics, derived from applied economics, is the combination of traditional economic theory and specific field-based statistical methods and data to project the financial impacts of cyber-based events.
Loss Categories of Cyber Risks Behind The Economic Impacts Of Cyber Losses

- Data Breach
- Business Interruption
  - Denial of Service
  - Accidents, Mistakes, or Misconfigurations
- Ransomware
- Misappropriation
  - Theft of IP
  - Payment Fraud
  - Theft of Services
The Inherent Cyber Risk Facing a Company (Including 3rd Party) Adjusted For Cyber Capabilities

E (Cyber Loss) = \sum_{i=1}^{7} \left( \text{Financial Impact} \times \text{Residual Cyber Risk}_i \right) \times (P) \times \text{Residual Cyber Risk}_i

(Business Impact \times Threat Context) \times (1 - Control Effectiveness)

Loss Categories Driving the Overall Exposure Value
- Data Breach
- Business Interruption - Denial of Service
- Business Interruption - Non-DoS
- Misappropriation - Intellectual Property
- Misappropriation - Funds/Assets
- Misappropriation - Services
- Ransomware
Variable #1: INHERENT CYBER RISK

Business Impact
- Revenue at risk
- IP at risk
- Fines, fees & response, recovery, litigation costs
- Revenue recovery

Threat Context
- Cyber attacker group activity
- Cyber attack patterns and tactics
- Industry-specific targeted activities

INHERENT CYBER RISK* = (Business Impact) x (Threat Context)

*The intrinsic amount of cyber loss exposure expressed in $’s for the company.

Keys to Success
- Having independent and objective data sources (i.e., DHS, Dept of Treasury, Insurance Claims, etc.)
- Using existing cyber operational data
- Structuring the cyber threat landscape (i.e., VERIS taxonomy)
Variable #2: RESIDUAL CYBER RISK

Inherent Risk*:
* The intrinsic amount of cyber loss exposure expressed in $’s for the company.

Control Effectiveness:
- Assessed cyber controls (i.e., NIST CSF, FFIEC CAT, SOC2, ISO27001/2)
- CISO team digital business system insights
- Cyber operations results enrichment

RESIDUAL CYBER RISK* = (Inherent Risk) x (1-Control Effectiveness)

*The control adjusted cyber loss expressed in $’s for the company.
What’s in a Model?

- Categorical Outcome Analysis (COA)
- Value at Risk (VaR)
- Factor Analysis of Information Risk (FAIR)/OpenFAIR
- Back of the Napkin
- Scientific Wild-assed Guessing
- Feverish Hand Waving
- Others?
4 Choices For Treating Risk

- Avoid
- Accept
- Mitigate/Reduce
- Transfer
Telling the Cyber Economic Story

Annual Expected Loss

- Total: $197M
- Interruption: 39%
- Ransomware: 23%
- Data Breach: 33%
- Misappropriation: 1.83%

Risk Level: Moderate

Annual Expected Loss:
- Interruption: $45.9M
- Ransomware: $77.3M
- Data Breach: $8.6M
- Misappropriation: $65.5M
## Implementation Values per Control / Max. Internal Loss Improvement Potential per Function

<table>
<thead>
<tr>
<th>Category</th>
<th>Implementation Values</th>
<th>Max Loss Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Configuration of Enterprise Assets and Software</td>
<td>56%</td>
<td>$18.5M</td>
</tr>
<tr>
<td>Audit Log Management</td>
<td>52.4%</td>
<td>$16.9M</td>
</tr>
<tr>
<td>Network Monitoring and Defense</td>
<td>61.2%</td>
<td>$15.2M</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>56.4%</td>
<td>$14.3M</td>
</tr>
<tr>
<td>Incident Response Management</td>
<td>56.4%</td>
<td>$13.4M</td>
</tr>
<tr>
<td>Data Protection</td>
<td>56.4%</td>
<td>$13.4M</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>53.5%</td>
<td>$12.9M</td>
</tr>
<tr>
<td>Malware Defenses</td>
<td>55.9%</td>
<td>$11.9M</td>
</tr>
<tr>
<td>Continuous Vulnerability Management</td>
<td>54.8%</td>
<td>$11M</td>
</tr>
<tr>
<td>Account Management</td>
<td>62%</td>
<td>$10.8M</td>
</tr>
<tr>
<td>Security Awareness and Skills Training</td>
<td>73.5%</td>
<td>$9.8M</td>
</tr>
<tr>
<td>Inventory and Control of Enterprise Assets</td>
<td>52.3%</td>
<td>$9.8M</td>
</tr>
<tr>
<td>Inventory and Control of Software Assets</td>
<td>51.1%</td>
<td>$8.9M</td>
</tr>
<tr>
<td>Access Control Management</td>
<td>63.2%</td>
<td>$8.2M</td>
</tr>
<tr>
<td>Application Software Security</td>
<td>59.8%</td>
<td>$6.6M</td>
</tr>
<tr>
<td>Email and Web Browser Protections</td>
<td>60.6%</td>
<td>$6.3M</td>
</tr>
<tr>
<td>Service Provider Management</td>
<td>52.2%</td>
<td>$4.6M</td>
</tr>
<tr>
<td>Network Infrastructure Management</td>
<td>55.7%</td>
<td>$3.6M</td>
</tr>
</tbody>
</table>
Telling the Cyber Economic Story:

Cyber ROI

Improvement by Control

- Inventory and Control of Enterprise Assets: $3.6M
- Inventory and Control of Software Assets: $3.4M
- Data Protection: $4.2M
- Secure Configuration of Enterprise Assets and Software: $5.9M
- Account Management: $2.3M
- Access Control Management: $1.5M
- Continuous Vulnerability Management: $3.7M
- Audit Log Management: $6.3M
- Email and Web Browser Protections: $1.5M
- Malware Defenses: $3.8M
- DTA Recovery: $4.6M
- Network Infrastructure Management: $1.1M
- Network Monitoring and Defense: $3.4M
- Service Provider Management: $1.7M
- Application Software Security: $1.7M
- Incident Response Management: $4.2M
- Penetration Testing: $4.5M

© 2022 Secure Systems Innovation Corporation Proprietary & Confidential All Rights Reserved
Telling the Cyber Economic Story:

The Role of Risk Transfer
Telling the Cyber Economic Story: How Bad Would It Be If…..?

Data Breach
Volume of records lost
5M
Probability 0.27%

Interruption: DoS Attack
Duration (Hrs)
12
Probability 0.44%

Interruption: Other
Duration (Hrs)
0.5
Probability 119.46%

Ransomware
Duration (Hrs)
12
Probability 3.39%

Worst-case: $89M
Things to Take Back With You

- Maturity scores are not enough... A financial lens imperative to the future of cyber risk management.
- Independent industry data is critical to the defensibility of a cyber economic approach.
- From Board and business leadership discussions to meeting SEC and other regulatory requirements, cyber risk financial transparency is the future of cyber risk management.
- Getting started can be easy – and you don’t have to solve all of the world’s problems on day 1. Pick a group or two to start, and build around that analysis.
Thank you!

Kevin Richards
krichards@x-analytics.com
847-334-4654