Quantifying and Communicating Cyber-Risk Exposure to the Board

Ryan Jones
Director of Cyber Risk Intelligence
BMS Group
@ar_em_jay
Introduction

Video Placeholder
By the end of the presentation you will know

- Why quantifying cyber risk is important
- How to start quantifying cyber risk
- How to communicate cyber risk to the board
War Story #1
The Time I Disarmed A Room of IT Professionals
That Time I Disarmed A Room of IT Professionals

- As a consultant I was brought in to help with a cyber insurance buying decision. I found...
  - Cyber insurance buying based on plenty of fear but little rationale
  - No communication between departments regarding cyber risk
  - A kickoff meeting to an IT management team who were told I was an auditor

I could hear the snarling from the elevator.
At that kickoff meeting and over the next week...

- I asked them how tall they thought I was
- I broke the 2-day engagement into focused 5-45 minute workshops with people all over the business asking them to estimate factors well within their range of expertise
- Presented a report that lead to a board-level decision to renew their former cyber policy and extend its cover in both scope and limit

I work for an insurance broker now because “that is how organizations should be buying cyber insurance.”
The report expressed their cyber exposure in terms of probable outcomes with dashboard output that looked something like this...
And what it’s made of...

And broke down that exposure into categories so that cyber insurance cover could be tailored to fit.
Lesson #1
How To Start Quantifying Cyber Risk
State your assumptions.

Define your words.
Models are important
Definitions are important

Speed = Distance / Time

Risk = Probable Frequency x Probable Magnitude of Future Loss
Revisit the Basics

- Probability vs. Possibility
- Quantitative vs. Qualitative
- Subjectivity vs. Objectivity
- Accuracy vs. Precision
Get to Know a Model

This one is called F.A.I.R. (Factor Analysis of Information Risk)
How much risk is associated with a malicious employee stealing client credit card details?

How much risk is associated with hackers bringing down our website for 24 hours?

How much risk is associated with a cryptolocker attack against a limited number of our company machines? Against our servers?
Beware of some pitfalls

OUR RISK MANAGEMENT SOFTWARE SAYS YOUR IDEA IS TOO RISKY.

TRY REDUCING ONE OF THE INPUTS.

WHICH ONE?

HONESTY. I JUST THREW UP IN MY MOUTH.

www.dilbert.com
War Story #2
That Time I Got Thrown Out Of The Boardroom
AND
That Time I Became Indispensable to the Board
That Time I Got Thrown Out of the Boardroom

- Presenting the 1st “Top 10 Risk Report” to the Board
  - Didn’t vet the conclusions with the board members ahead of time
  - Didn’t vet the report format
  - Presented data rather than intelligence
  - Missed the opportunity to enable risk owners to report on their own areas of exposure to their peers

Was cursed out of the room and told to go try again.
That Time I Got Thrown Out of the Boardroom
This is Data, Not an Intelligence Summary

The following is one of seven (7) scenarios run through a stochastic engine. This is the most significant exposure forecasted and assumes a total breach of customer data.

*The other scenarios are available upon request though excluded from this report for the sake of brevity.

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Average</th>
<th>Most Likely</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss Events / Year</td>
<td>0.08</td>
<td>0.32</td>
<td>0.21</td>
<td>0.85</td>
</tr>
<tr>
<td>Loss Magnitude</td>
<td>$54,227</td>
<td>$831,549</td>
<td>$769,869</td>
<td>$2,622,546</td>
</tr>
<tr>
<td><strong>Secondary</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss Events / Year</td>
<td>0.07</td>
<td>0.27</td>
<td>0.28</td>
<td>0.75</td>
</tr>
<tr>
<td>Loss Magnitude</td>
<td>$138,652</td>
<td>$830,145</td>
<td>$280,062</td>
<td>$3,139,860</td>
</tr>
<tr>
<td>Total Loss Exposure</td>
<td>$46,136</td>
<td>$495,026</td>
<td>$274,184</td>
<td>$2,348,853</td>
</tr>
</tbody>
</table>

Not expected to happen often (~1/5 years)

Could be expensive when it does happen (~$5.5M)
That Time I Became Indispensable to the Board

- Presenting the **2nd** “Top 10 Risk Report” to the Board
  - Vetted the conclusions with the board members ahead of time
  - Vetted the report format
  - Enabled risk owners to report risk intelligence to their peers

Received a standing ovation.
Lesson #2
How To Communicate Cyber Risk to the Board
Not by Parroting Other Sources

RMP Top 5 Cyber Risks
- Data Breaches
- Reputational Damage
- Reliance on IT Systems
- The Potential Cost of a Cyber Attack
- Inadequate Insurance Cover

CNBC Top 5 Cyber Risks
- Ransomware
- The Internet of Things
- Cyber Espionage
- Cyber Theft
- Unsecure Passwords
Report YOUR Cyber Risk to the Board

- **Analyze**
  - Have a series of conversations to triage your cyber risk scenarios
    - Is it more about confidentiality and protecting data or,
    - Is it more about availability and keeping your systems up?
  - Determine the top 3-5 scenarios and quantify the potential impacts/severity
    - Break these into different categories of loss and go to people in the business that know the most about those categories (For example, for legal fines/regulatory penalties, go to your legal counsel.)
    - Talk to IT about the frequency, get “calibrated” estimates/forecasts

- **Report**
  - Walk board members through the parts of the analysis that are most relevant to them
  - Don’t just talk about the ranges and the forecasts, focus on potential solutions (such as risk transfer)
  - As long as they are willing, enable board members to report to their peers on aspects of cyber risk that are most relevant to them (the COO could present the business interruption scenario as a result of a DDoS attack)
  - Dig into the details as necessary and have them available for debate
Report YOUR Cyber Risk to the Board
Next week you should:
- Identify and prioritize the top 3 cyber risk scenarios for your organization and explain your process for doing this to a peer within the company
- Take a look at your cyber insurance cover (just for fun)

In the first three months following this presentation you should:
- Explore the F.A.I.R. methodology through the FAIR Institute or;
- Read “Measuring and Managing Information Risk, A FAIR Approach” by Jack Freund and Jack Jones

Within six months you should:
- Approach your board with a presentation on cyber risk whilst having an understanding of the quantum of the exposure
Now you know

- Why quantifying cyber risk is important
  - Meaningful measurements lead to effective comparisons lead to better decisions
  - And cyber risk is *business* risk

- How to start quantifying cyber risk
  - Model your problem
  - Estimate/forecast using frequency and financial impact
  - Look into the FAIR methodology

- How to communicate cyber risk to the board
  - Quantify the exposure,
  - Then enable the board members to report and communicate to and with each other
  - Focus on presenting solutions rather than just data
Ryan Jones
Director of Cyber Risk Intelligence
ryan.jones@bmsgroup.com
Quantifying and Communicating Cyber-Risk Exposure to the Board

Ryan Jones
Director of Cyber Risk Intelligence
BMS Group
@ar_em_jay