MAKING BUSINESS SENSE OF TECHNOLOGY RISK

Norman Marks
2019
Cyberattacks and massive data fraud both appear in the list of the top five global risks by perceived likelihood.

Attacks are increasing, both in prevalence and disruptive potential.

Cyber breaches recorded by businesses have almost doubled in five years, from 68 per business in 2012 to 130 per business in 2017.
A 2017 study of 254 companies across seven countries put the annual cost of responding to cyberattacks at £11.7 million per company, a year-on-year increase of 27.4%.

The cost of cybercrime to businesses over the next five years is expected to be US$8 trillion.
WHY SHOULD I INVEST IN CYBER?

- Possibility of a cyber breach
- High likelihood of great ROI on another investment
- Average cost of a cyber breach (Ponemon, 2018) is $3.86 million
85% of board members believe that IT and security executives need to improve the way they report to the board.

59% say that one or more IT security executive will lose their job as a result of failing to provide useful, actionable information.

54% agree or strongly agree that reports are too technical.

Osterman Research, 2016
40% of IT and security executives believe the information they provide the board is actionable. 33% believe the board comprehends the cyber security information provided to them.

39% believe they are getting the help they need from the board to address cyber security threats.

37% agree or strongly agree that organizational risk is reduced as a result of their conversations with and reports to the board – in fact, 5% either disagree or strongly disagree that risk is reduced.

Osterman Research, 2016
WHAT ARE WE TRYING TO DO?

- Manage risk?
- Manage the business?
- Achieve enterprise objectives
- Make intelligent and informed decisions
- Provide *actionable* information
ISO 27005/2018

“A list of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks”

Are we managing risks or the business?
“After determining the Probable Loss Magnitude (based on “the worst-case scenario as well as the most probable scenario(s) of loss” and the Loss Event Frequency, those values are entered into a matrix to determine the Risk Magnitude.”

“The six rows reflect Probable Loss Magnitude, ranging from Very Low to Severe. The five columns are for Loss Event Frequency and range from Very Low to Very High. If the risk is in the top right quadrant of the matrix it is considered Critical. If it is in the lower left it is Low. The rest are either Moderate of High.”
“The real challenge has to do with articulating this risk value to the decision-makers.”

“In some circumstances high-risk is entirely acceptable (e.g., in cases where the potential for reward outweighs the risk). In other situations, a relatively low-risk condition may be unacceptable.”

“In summary, risk articulation must meet the needs of the decision-makers.”
A BETTER WAY

- How could a technology issue affect the business?
- Comparable to other business risks
- $$$ impact?
- Effect on enterprise objectives
<table>
<thead>
<tr>
<th></th>
<th>Consequences of a breach</th>
<th>Likelihood of the effect</th>
<th>Monetary damages</th>
<th>Effect on objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Post graffiti on a web page</td>
<td>12%</td>
<td>$10,000</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>Bring down the web page</td>
<td>10%</td>
<td>$20,000</td>
<td>0%</td>
</tr>
<tr>
<td>3</td>
<td>Steal customer data related to their use of the web services</td>
<td>8%</td>
<td>$120,000</td>
<td>3%</td>
</tr>
<tr>
<td>4</td>
<td>Penetrate the global network and steal all customer data</td>
<td>7%</td>
<td>$500,000</td>
<td>25%</td>
</tr>
<tr>
<td>5</td>
<td>Steal critical intellectual property</td>
<td>6%</td>
<td>$2,000,000</td>
<td>75%</td>
</tr>
<tr>
<td>6</td>
<td>Bring down the global network and ask for ransom</td>
<td>5%</td>
<td>$500,000</td>
<td>35%</td>
</tr>
<tr>
<td>7</td>
<td>Use the network to attack and cause serious physical damage</td>
<td>2%</td>
<td>$1,000,000</td>
<td>10%</td>
</tr>
<tr>
<td>8</td>
<td>Take actions that result in the loss of life</td>
<td>1%</td>
<td>$5,000,000</td>
<td>25%</td>
</tr>
</tbody>
</table>
Post graffiti on a web page
Bring down the web page
Steal customer data related to their use of the web services
Penetrate the global network and steal all customer data
Steal critical intellectual property
Bring down the global network and ask for ransom
Use the network to attack and cause serious physical damage
Take actions that result in the loss of life

Monetary damages
Effect on objectives
BUT....

- Any decision has to consider multiple risks
- Multiple technology-related risks
- Other business risks
- What is the big picture?
OPENING A NEW PRODUCT DEVT OFFICE

- Cyber
- Ability to hire and retain
- Power supply
- Compliance issues
- Employee morale
- ... and more
OPENING A NEW PRODUCT DEVELOPMENT OFFICE

- Cyber – 7% chance of $10m loss
- Ability to hire and retain – 10% of $1m
- Power supply – 10% of $5m

Likelihood of at least one?
24.67%
OPENING A NEW PRODUCT DEVT OFFICE

- Cyber – 7% chance of $10m loss
- Ability to hire and retain – 10% of $1m
- Power supply – 10% of $5m

Likelihood of all 3?
0.07%
A DIFFERENT APPROACH

- Manage the business not just risk
- Effect on enterprise objectives
- Integrated performance and risk report
- Focus on enabling informed and intelligent decisions
<table>
<thead>
<tr>
<th>OBJECTIVE</th>
<th>YTD ACHIEVEMENT</th>
<th>FALL SHORT</th>
<th>ACHIEVE TARGET</th>
<th>EXCEED TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue growth of 10%</td>
<td>9.85%</td>
<td>15%</td>
<td>80%</td>
<td>5%</td>
</tr>
<tr>
<td>EPS improvement of 5%</td>
<td>8.00%</td>
<td>10%</td>
<td>80%</td>
<td>10%</td>
</tr>
<tr>
<td>Maintain customer satisfaction levels</td>
<td>98.00%</td>
<td>8%</td>
<td>90%</td>
<td>2%</td>
</tr>
<tr>
<td>Improve market share by 5%</td>
<td>5.00%</td>
<td>20%</td>
<td>70%</td>
<td>10%</td>
</tr>
<tr>
<td>Introduce new product on time and budget</td>
<td>72.00%</td>
<td>30%</td>
<td>65%</td>
<td>5%</td>
</tr>
</tbody>
</table>
ANOTHER APPROACH

- $$$ when comparing different initiatives and their cost, reward, ROI
- Otherwise, effect on objectives
- Same methodology for all sources of business risk
- Potential for loss or benefit from technology
- Don’t forget range of consequences
1. INSERT KEY INTO IGNITION
2. SHIFT INTO DRIVE
3. PRESS FOOT FIRMLY ON THE THROAT OF MEDIOCRITY
THANK YOU!

Norman Marks, CPA, CRMA
Author; Evangelist for Better Run Business; OCEG Fellow; Honorary Fellow of the Institute of Risk Management

nmarks2@yahoo.com
http://normanmarks.wordpress.com/
Twitter: @normanmarks