12 Months of Disruption, 12 Months of Learning

Brian Zawada (FBCI)
Managing Director and Chief Visionary Officer
Avalution Consulting LLC

June 2018
Introduction

• Here’s what I do:
  – Help build business continuity programs
  – Help manage business continuity programs
  – Lead or participate in the response to disruption
  – ISO volunteer (TC 292)
Agenda

- Review recent disruptions
- Discuss BCI research report findings
- Introduce my “Top 5” recommendations
- Talk about two more things
- Discussion
Caveats

• I don’t advocate that anyone build threat specific plans

• However, evaluating threats helps us:
  – Eliminate blind spots
  – Field executive questions
  – Build better exercises
  – Determine if we need any specialized response procedures
  – Learn from others’ mistakes
Avalution.participoll.com
What worries you the most?

A. Cyber attack
B. IT Disruption
C. Utility Disruption
D. Supply Chain Disruption
E. Adverse Weather
F. Terrorism
Drug production in Puerto Rico still disrupted, FDA says

By Ned Pagliarulo  •  Oct. 26, 2017

Dive Brief:

• Hurricane Maria’s effects on drug manufacturing in Puerto Rico continue to be felt, even as many drugmakers say their operations on the island are returning to normal production levels with only modest disruption.

• “For most facilities, we understand that manufacturing is running at minimal levels, and certainly far from full production,” testified Food and Drug Administration
Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear

28 JUN 2017

Following reports of a malware attack, a DLA Piper spokesperson said: "On June 27, 2017, our advanced-warning system detected suspicious activity on our network, which, based on our investigation to date, appears to be related to the global cyber event known as "Petya". Our IT team acted quickly to prevent the spread of the suspected malware and to protect our systems.

DLA Piper
Hackers Crashed a Bank’s Computers While Attempting a SWIFT Hack

By Catalin Cimpanu

June 6, 2018 05:18 PM

Hackers have used a disk-wiping malware to sabotage hundreds of computers at a bank in Chile to distract staff while they were attempting to steal money via the bank’s SWIFT money transferring system.

The attempted hack took place on May 24, this year. On that day, the Banco de Chile, the country’s biggest bank, reported all-around systems failures that affected the computers at several of its branches.
BCI Horizon Scan Report (2018)

Top 10 disruptions

1. Unplanned IT and telecom outages
2. Adverse weather
3. Interruption to utility supply
4. Cyber attack
5. Availability of talents/key skills
6. Security incident
7. Transport network disruption
8. New laws or regulations
9. Fire
10. Supply chain disruption

Top 10 threats

1. Cyber attack
2. Data breach
3. Unplanned IT and telecom outages
4. Interruption to utility supply
5. Adverse weather
6. Act of terrorism
7. Security incident
8. Fire
9. Supply chain disruption
10. Transport network disruption
<table>
<thead>
<tr>
<th>Year</th>
<th>Top five threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>1. Cyber attack</td>
</tr>
<tr>
<td></td>
<td>2. Data breach</td>
</tr>
<tr>
<td></td>
<td>3. Unplanned IT &amp; telecom outages</td>
</tr>
<tr>
<td></td>
<td>4. Act of terrorism</td>
</tr>
<tr>
<td></td>
<td>5. Security incident</td>
</tr>
<tr>
<td>2017</td>
<td>1. Cyber attack</td>
</tr>
<tr>
<td></td>
<td>2. Data breach</td>
</tr>
<tr>
<td></td>
<td>3. Unplanned IT &amp; telecom outages</td>
</tr>
<tr>
<td></td>
<td>4. Security incident</td>
</tr>
<tr>
<td></td>
<td>5. Adverse weather</td>
</tr>
<tr>
<td>2018</td>
<td>1. Cyber attack</td>
</tr>
<tr>
<td></td>
<td>2. Data breach</td>
</tr>
<tr>
<td></td>
<td>3. Unplanned IT &amp; telecom outages</td>
</tr>
<tr>
<td></td>
<td>4. Interruption to utility supply</td>
</tr>
<tr>
<td></td>
<td>5. Adverse weather</td>
</tr>
</tbody>
</table>
BCI Supply Chain Resilience Report (2017)
How many supply chain incidents would you estimate your organization experienced in the past 12 months that caused a significant disruption?

- 51%: 0
- 25%: 1-5
- 8%: 6-10
- 3%: 11-20
- 2%: 21-50
- 1%: 51+
- 10%: I don’t know
My Top 5 Recommendations

1. Proactively influence strategy (rather than react to risky decisions)
2. Make vulnerability transparent
3. Do something about the supply chain
4. Plan with the CISO
5. Be threat agnostic
**BCI Horizon Scan Report (2018)**

If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

- **54%** Use ISO 22301 as a framework but don’t certify.
- **16%** Use ISO 22301 as a framework and certify against it.
- **10%** Don’t currently use ISO 22301 as a framework but we intend to move towards this during 2018.
- **13%** Don’t use ISO 22301 as a framework and have no plans to move towards this during 2018.
- **7%** N/A
Before We Conclude...
The Business Impact Analysis...

A. I think the BIA is important because it helps my organization identify business continuity requirements
B. The BIA is an out of date practice because estimating impact is a guess (at best)
C. The BIA is an out of date practice because defining business requirements is situation dependent
D. Other (ask me later)
What is the hardest part of our job as a business continuity practitioner?

A. Designing the business continuity program
B. Implementing the business continuity program (performing the business continuity planning process)
C. Managing the business continuity program long-term (continually improving the outcomes and staying engaged with management)
Questions and Discussion