What Does the Future Look Like for Business Continuity Professionals?

October 26, 2016

Brian Zawada, FBCI
President, US Chapter of the Business Continuity Institute
Agenda and Objectives

• Change
  – Standards
  – People
  – Threat Environment
  – Organizational Resilience
• The Evolution of Our Role
• Conclusions / Discussion
BCI 20/20 Objectives

• The goal of the Business Continuity Institute has been to promote a more resilient world
• When the Institute celebrated its 20th anniversary in 2014, the focus was not on our past achievements but our vision of the future.
• From that vision emerged the BCI 20/20 Think Tank, a worldwide group of thought leaders with a passion to drive the profession forward
Our Profession Has Changed (is changing)!
When It Comes to Standards...

• From planning to engagement
  – Management
  – Strategy
  – Continual Improvement
Connecting a discipline to organizational strategy through executive management
ISO Standards

- **ISO 22301**: Business Continuity Management Systems – Requirements
- **ISO 22313**: Business Continuity Management Systems – Guidance
- **ISO 22316**: Organizational Resilience – Principles and Guidelines
- **ISO 22398**: Guidelines for Exercises
- **ISO 22317**: Business Continuity Management Systems – Business Impact Analysis
- **ISO 22318**: Business Continuity Management Systems – Supply Chain Continuity
- **ISO 22330**: Business Continuity Management Systems – Human Aspects
- **ISO 22331**: Business Continuity Management Systems – Strategy Determination
Our Profession Is Changing!

Source: U.S. Census Bureau
When It Comes to People...

• Learn to work together
• Acknowledge each other’s strengths
• Be open to changing the way we work
• Knowledge transfer (growing the next generation of BC professionals)
The Threat Environment Has Changed!
Just Last Week...
Too Big to Fail?
Just Last Month...
Threats & Risks We Don’t Know Haunt Us and Our Senior Leadership Team
We Must Master...
Introduction to Horizon Scanning

• As a key ‘protective discipline’, business continuity aids organizational resilience by building an effective response to disruptive events.
• Horizon scanning is a useful tool that can provide an objective perspective on threats and uncertainties that may lead to business disruption.
• These conclusions inform – or even confirm – strategies undertaken by organizations to prepare for disruption (helping to eliminate blind spots).
Issues Concerning Us in 2016

- Use of Internet for malicious attacks (e.g. cyber...) 83%
- Influence of social media (e.g. reputation...) 63%
- Loss of key employee 56%
- New regulations and increased regulatory scrutiny 55%
- Prevalence and high adoption of Internet dependent... 50%
- Potential emergence of a global pandemic (e.g. Ebola) 48%
- Increasing supply chain complexity 47%
- Political change (e.g. change in government or... 42%
- Changing consumer attitudes and behavior (e.g.... 36%
- Energy security and the transition to sustainable... 29%
Top 10 Based on Concern Level

- Cyber attack (e.g. malware, denial of service): 48% Extremely concerned, 37% Concerned, 13% Somewhat concerned, 0% Not concerned, 0% Not applicable
- Data breach (i.e. loss or theft of confidential information): 41% Extremely concerned, 39% Concerned, 16% Somewhat concerned, 40% Not concerned, 0% Not applicable
- Unplanned IT and telecom outages: 35% Extremely concerned, 42% Concerned, 19% Somewhat concerned, 0% Not concerned, 0% Not applicable
- Act of terrorism: 19% Extremely concerned, 36% Concerned, 30% Somewhat concerned, 14% Not concerned, 1% Not applicable
- Security incident (e.g. vandalism, theft, fraud, protest): 17% Extremely concerned, 38% Concerned, 34% Somewhat concerned, 10% Not concerned, 1% Not applicable
- Interruption to utility supply (i.e. water, gas, electricity, waste disposal): 16% Extremely concerned, 41% Concerned, 32% Somewhat concerned, 10% Not concerned, 1% Not applicable
- Supply chain disruption (up and downstream): 16% Extremely concerned, 34% Concerned, 28% Somewhat concerned, 18% Not concerned, 4% Not applicable
- Adverse weather (e.g. windstorm/tornado, flooding, snow, drought): 14% Extremely concerned, 41% Concerned, 29% Somewhat concerned, 15% Not concerned, 1% Not applicable
- Availability of talents/key skills (e.g. ‘bench strength’): 13% Extremely concerned, 34% Concerned, 36% Somewhat concerned, 17% Not concerned, 1% Not applicable
- Health & Safety incident: 11% Extremely concerned, 25% Concerned, 42% Somewhat concerned, 20% Not concerned, 1% Not applicable
Tracking Threats - Cyber

• Ranking #1 was Cyber Attacks in both 2016 and 2015, which were ranked third in 2013 and second in 2014 (not surprising given all the incidents we hear about almost daily)

• Most DRJ attendees agreed this was and is a major concern and acknowledged the close association with Data Breach, Terrorism and Security, increasing the relevance of this threat

So how does this affect us as BC Professionals?
• Recognition that this threat has IT availability and even business continuity implications
• Leverage crisis management and crisis communications processes in response
Tracking Threats – Data Breaches

• Ranking #2 was data breaches which were ranked third in 2015. Similar to cyber, not surprising given all the incidents we hear about.

• DRJ discussion surrounded the fact that data breaches come in many forms, both cyber / internet related as well as the old fashion stealing of reports and copying files to a flash drive.

• Data breach related exercises are a key focus of attendees as well as differentiating IT related response plans from incorporating breach response into crisis management plans.

So how does this affect us as BC Professionals?

• Leverage crisis management and crisis communications processes in response.
Tracking Threats – Unplanned IT Outages

- Ranking #3, IT outages are still a top 10 issue, and are a key focus in most IT DR and BC programs.
- While most respondents see emerging threats such as cyber and data breaches as more impactful, IT outages are still a major focus.
- Discussion among the DRJ attendees focused on the changing face of IT, as software as a service, cloud computing and outsourced IT change the landscape and require differing strategies, often outside of the organizations direct control.

So how does this affect us as BC Professionals?
- SaaS is not inherently recoverable by default.
- Recognize the risks and opportunities presented by the cloud.
Tracking Threats – Terrorism

• With a huge jump from #10 to #4, Terrorism has leaped up into the focus of Resilience and Continuity professionals.
• This increase may be attributed to the recent terrorist attacks which occurred during the survey period.
• Most participants acknowledged the threat, and felt it was driving attention to incident response and crisis management plans, plus a focus on tracking.

So how does this affect us as BC Professionals?
• Indirectly, recent events are creating protectionist measures impacting global operations and trade (Brexit).
• Adding to the puzzle we mentioned earlier, along with cyber and data breaches, Security is clearly an area of concern for organizations. Ranking 5<sup>th</sup> in the 2016 scan, up from 6<sup>th</sup> in 2015

• Part of the senior level discussions at DRJ had to do with organizational issues and placement of security vs continuity and recovery in organizations

So how does this affect us as BC Professionals?
• Security events impact travel and facility availability
• No issues of placing BC in Security as long as there is a recognition of more than response, business-aligned strategies still necessary
Our World Has Changed!

Organizational Resilience

“The adaptive capacity of an organization in a complex and changing environment”

ISO/DIS 22316:2016
Resilience – adaptive capacity of an organization in a complex and changing environment (ISO 22316)

- Business continuity is not the same as organizational resilience.
- The effective enhancement of organizational resilience will require a collaborative effort between many management disciplines.
- No single management discipline can credibly claim ‘ownership’ of organizational resilience, and organizational resilience cannot be described as a subset of another management discipline or standard.
- Business continuity principles and practices are an essential contribution for an organization seeking to develop and enhance effective resilience capabilities.
- The wide range of activities required to develop and enhance organizational resilience capabilities provide an opportunity for business continuity practitioners to broaden their skills and knowledge, building on the foundation of their business continuity experience and credentials.
BCI’s Statement on Resilience

Business Continuity is NOT the same as organizational resilience
BCI’s Statement on Resilience

A collaborative effort between disciplines is required
The Evolution of Our Role

In the context of an ever-increasing focus on resilience and the engagement of multiple disciplines, what’s the business continuity professional’s role?

Owner  Facilitator  Participant

IT DEPENDS ON THE RISK OR THREAT!
Responsibilities

Increases the organization’s preparedness for disruptive incidents by implementing capabilities to enable the continuation of product and service delivery at acceptable predefined levels.

Collaborates with other disciplines to create a more resilient organization, taking ownership of assigned risks and participating as a team member in mitigating other risks.
A Proposed Job Description (cont.)

Duties

• Engages management to establish appropriate business continuity requirements

• Enables the selection of effective capabilities to respond to and recover from disruptive incidents

• Leads the evaluation of response and recovery capabilities, as well as the development of the competencies necessary to plan and respond effectively

• Implements the processes necessary to drive continual improvement and manage the effects of organizational change
### A Proposed Job Description (cont.)

<table>
<thead>
<tr>
<th>Skills</th>
<th>Business Continuity Analyst</th>
<th>Business Continuity Leader</th>
<th>Resilience Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Oral and written communications</td>
<td>• Sales (including relationship building)</td>
<td>• Facilitation techniques</td>
<td></td>
</tr>
<tr>
<td>• Inquiry</td>
<td>• Strategic and tactical thinking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Project management</td>
<td>• Management (in general)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enablers</th>
<th>Business Continuity Analyst</th>
<th>Business Continuity Leader</th>
<th>Resilience Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Knowledge of the organization and its resources</td>
<td>• Knowledge of the organization’s products and services and customer usage</td>
<td>• Knowledge of other management and risk disciplines</td>
<td></td>
</tr>
<tr>
<td>2016 HORIZON SCAN TOP 10</td>
<td>OWNER</td>
<td>FACILITATOR</td>
<td>PARTICIPANT</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Cyber Attack</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breach</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unplanned IT / Telecom Outages</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act of Terrorism</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Incident</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interruption of Utility Supply</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Disruption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adverse Weather</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability of Talents / Key Skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health and Safety Incident</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Where Do We Fit Into Resilience?

<table>
<thead>
<tr>
<th>RISK CATEGORY</th>
<th>OWNER</th>
<th>FACILITATOR</th>
<th>PARTICIPANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Availability Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractual Risk</td>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>Credit Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Risk</td>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>Health / Safety Risk</td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Product / Marketing Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Risk</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Risk</td>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>Regulatory Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational Risk</td>
<td></td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>Security Risk</td>
<td></td>
<td></td>
<td>○</td>
</tr>
</tbody>
</table>
Revisiting...
• Standards are connecting us to other risk disciplines and focusing us on continual improvement
• We need to engage with the next generation and adapt our approaches to engage and grow them as our successors
• Threats are real and expanding, leading to increased business risk
• All these changes are leading to changes in our profession
• Our success will be based on our knowledge of the organization and its business environment, including customers and their expectations
Open Discussion and Questions

BCI USA – The Business Continuity Institute US Chapter

BCI_US_Chapter

@BCI_US_Chapter

www.thebci.org/index.php/home/us-chapter-home

USAcommunications@bcichapter.net

Join the debate!