Resilience is a competitive advantage: How to be a reliable supplier

Chloe Demrovsky
Executive Director, DRI International

Electrical Safety, Reliability and Sustainability Conference
April 7, 2017

Who we are

- We provide education, accreditation, and thought leadership in business continuity and related fields.
- Founded in 1988, we are the oldest and largest organization of our kind.
What we do

• We offer in-depth courses ranging from introductory to masters level, as well as specialty certifications.

<table>
<thead>
<tr>
<th>15,000+ Certified Professionals</th>
<th>100+ Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes offered in 14 Languages</td>
<td>Courses held in 50 Countries</td>
</tr>
</tbody>
</table>

What we aim for

• To not only educate those in our field, but also to disseminate the importance of preparedness to other professions and the general public.

• To reach and engage as many audiences as possible using broad media coverage to provide a forum for discussion.
International Organization collaboration

- ARISE Initiative Founding Member: Private Sector Working Group of the United Nations Office for Disaster Risk Reduction:
  - UNISDR presented at DRIKL2016 in Kuala Lumpur, Malaysia
  - ARISE Philippines sponsoring 2017 DRI Collegiate Conference in Manila, Philippines
  - DRI helping to found ARISE chapters in Canada and USA
- Participating in the Global Platform in May 2017
- DRI sat on the Disaster Management Terminology Committee.
- Business and Industry Delegation Member for the Sendai Framework for Disaster Risk Reduction negotiations
- We are an International Organization Liaison Observer for the International Standards Organization’s Technical Committee 292 for Societal Security

Career Tracks

- Get certified. Prove your expertise.
- Become an MRCP DRI’s highest level of certification.
- Create a robust risk management program.
- Add a skill with our ANSI-accredited, case-study based courses.
- Protect your agency’s mission-essential functions.
- Protect service delivery, safeguard records, maintain compliance.
- Healthcare Continuity
- Public Sector Continuity

Training with DRI

Corporate options
Certifying individual professionals and teams:

- 93% of all Fortune 100 companies employ DRI Certified Professionals
- Over 40% of Fortune 100 companies have 5+ DRI-Certified employees
- Over half of all Fortune 500 companies have DRI-Certified employees

- Resilient Enterprise Assessment Program: Allows for the evaluation of BC programs within organizations and provides detailed recommendations for improvement with the goal of strengthening the programs and organizations as a whole.
- Hub of Resilience: Brings together community, industry, and public sector leaders to discuss how to best affect preparedness through information-sharing.

DRI Foundation: Charitable giving and volunteerism

Vision
Resilient communities worldwide.

Mission
To promote disaster risk reduction through partnerships and education.
To aid recovery efforts through fund-raising and volunteerism.
“As the certified professionals conference, you know the folks you’ll be interacting with, that you’ll be networking with, come with a level of experience, a level of expertise, and a level of education that are on par with a certified professional.”

Reasons for Disaster Recovery and Business Continuity

Disaster Recovery Institute
Concerns for 2017

Likely in 2017
- Cyber espionage - state-sponsored
- Random acts of extreme violence
- Problems from higher dependency on on-line technology
- Cyber fraud – commercial
- Cyber theft – commercial
- Active shooters
- Cyber attacks including ransomware
- Investment levels in information security
- Growth of fundamentalist extremism
- Increased wide-scale flooding

Likely and High Impact in 2017
- Problems from higher dependency on on-line technology
- Cyber attacks including ransomware
- Investment levels in information security
- Cyber theft – commercial
- Cyber fraud – commercial
- Growth of fundamentalist extremism
- Investment levels in overall IT resiliency
- Man-made disaster (oil, gas, chemicals)
- Increased wide-scale flooding
- Random acts of extreme violence

Worst-case Impact in 2017
- Nuclear reactor failure/meltdown
- Problems from higher dependency on on-line technology
- Banking systemic failure
- Cyber attacks including ransomware
- Investment levels in information security
- Increasing resistance to antibiotics
- Power shortages and wide-scale outages
- Systemic failure of critical infrastructure
- Cyber theft – commercial
- Investment levels in overall IT resiliency

Most Likely to Impact Resilience Pros in 2017
- Problems from higher dependency on on-line technology
- Systemic failure of critical infrastructure
- Cyber attacks including ransomware
- Investment levels in information security
- Power shortages and wide-scale outages
- Cyber fraud – commercial
- Cyber theft – commercial
- Investment levels in overall IT resiliency
- Pandemic flu or similar viruses
- Man-made disaster (oil, gas, chemicals)
- Non-compliance on privacy or data protection laws

Log in at drii.org and download the latest report to see how we did on our 2016 predictions!

What is business continuity?

Business Continuity
An ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services. (NFPA 1600)

- Information technology and disaster recovery
- Physical security

Combining Disciplines

Under the umbrella of

Business Continuity Management

- Business Continuity
  (Relocation)
- Disaster Recovery
  (IT Recovery and Continuity)
- Emergency Response
  (Life Safety)
- Crisis Management
  (Reputational Protection)

Integrated Solution

Why Business Continuity Matters

- To safeguard human life
- To minimize confusion and enable effective decisions in a time of crisis
- To reduce dependency on specific personnel
- To minimize the loss of assets, revenue, and customers
- To ensure the survival of the organization
- To satisfy any legal or regulatory requirements
- To ensure that you are doing your due diligence
- To facilitate the timely recovery of critical business functions
- To maintain the public image and reputation of the organization
Reasons for Business Continuity

**External Drivers**
- Demands from customers
- Increased regulatory and self-regulated requirements
- Recent Loss and/or Business Interruption
- Pressure from audit committees
- Pressure from financial institutions
- Pandemic concern
- New threats and risks in the 21st century

**Impacts**
- Loss of customers or inability to attract new customers
- Regulatory sanctions
- Audit’s recommendation
- Loss of revenue
- Loss of assets and employees
- Decrease in stock value
- Increase of insurance premiums

Business Continuity Laws, Regulations, and Standards

**Pre-9/11**
- Consumer Credit Protection Act
- OMB Circular A-130
- FEMA Guidance Document
- Paperwork Reduction Act
- ISO 21000 (Previously ISO 17799)
- FFIEC BCP Handbook
- Computer Security Act 12 CFR Part 18
- Presidential Decision Directive 67
- FDA Guidance on Computerized Systems used in Clinical Trials
- ANSI/NFPA Standard 1600
- Turnbull Report (UK)
- ANAO Best Practice Guide (Australia)
- SEC Rule 17 a-4
- CAR
- JBAC

**Post-9/11**
- Sarbanes-Oxley Act of 2002
- HIPAA, Final Security Rule
- Fair Credit Reporting Act
- NIST Standard on BCP
- NIST Contingency Planning Guide
- FSA Handbook (UK)
- MAS Proposed BCP Guidelines (Singapore)
- MAS Standard, PAS 36 (UK)
- Civil Contingencies Bill (UK)
- NFRD: 2001/78/EC-2010-2015-16

**FSA**
- Sarbanes-Oxley
- 2005 Safety Act
- FDIC-15
- NYSE Circular Letter 7
- ASIS
- State of NY Firmware on CP
- NIST Standard Practice (Telecoms)
- Australian Prudential Standard on BCM
- HB292
- HB221
- HB230
- HB231
- HB222
- SS507 – SS540
- TR15
- CA Z146
- SSA/PAS 22238
- NY Tech Act of 2015
- NZ 2015
- NZ 2015
- FMAA 1270
- LWC
- SEC - Compliance Programs
- Dodd-Frank Wall Street Reform Act
- HB221

1991-2001 2002-present
What are the Implications of failing to mitigate or prevent?

Preparation
- Structure, planning, resources, testing

Execution
- Relocation, operating under duress

How to approach the incident

Focusing on Effects, Impacts, Consequences

Facilities
- Fire
- Flood
- Bomb scare
- Pandemic: SARS, H1N1, H5N1
- Terrorism
- etc.

Business or Operational
- Supply chain
- Process error
- Transit strike
- Pandemic: SARS, H1N1, H5N1
- Labor strike
- etc.

Technology
- Network problem
- Application error
- Hardware failure
- Virus
- Power problem
- etc.

Organization
- Merger and acquisition
- Succession
- Intellectual property issue
- Audit issue
- Financial problem
- etc.

Effect categories
<table>
<thead>
<tr>
<th>The Professional Practices for Business Continuity Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Program Initiation and Management</td>
</tr>
<tr>
<td>2. Risk Assessment</td>
</tr>
<tr>
<td>3. Business Impact Analysis</td>
</tr>
<tr>
<td>4. Business Continuity Strategies</td>
</tr>
<tr>
<td>5. Incident Response</td>
</tr>
<tr>
<td>6. Plan Development and Implementation</td>
</tr>
<tr>
<td>7. Awareness and Training Programs</td>
</tr>
<tr>
<td>8. Business Continuity Plan Exercise, Assessment, and Maintenance</td>
</tr>
<tr>
<td>9. Crisis Communications</td>
</tr>
<tr>
<td>10. Coordination with External Agencies</td>
</tr>
</tbody>
</table>

**Partnering for a Resilient Supply Chain**

**Disaster Recovery Institute**
Case Study: Nokia vs. Ericsson – March 17, 2000

Pre-Incident Ranking

- Nokia (32%)
- Motorola (22%)
- Ericsson (12%)

Post-Incident Ranking

- Nokia shipments grew by 10.5 percent over the previous year, to 140 million units.
- Motorola shipments dropped by 1.7 percent to 59 million units.
- Siemens shipments grew by 10.2 percent to 30 million units.
- Samsung shipments grew by 36.8 percent to 28 million units.
- Ericsson shipments dropped by 35 percent to 27 million units, spins off into joint venture with Sony

On July 20, 2000, Ericsson reported that the fire and component shortages had caused a second-quarter operating loss of $200 million in its mobile phone division. Total loss $400 million

Case Study: Why Nokia Gained and Ericsson Lost

Considered solutions before event occurred
Understood the need
Implemented recovery at other Nokia plants
Believed early reports of little damage and interruption
Smart people will find a solution
Case Study: Better Business Continuity Means More Reliable Suppliers

Motorola Business Interruption and Recovery Plan

Supplier will provide Motorola with a detailed, written business interruption and recovery plan, including business impact and risk assessment, crisis management, information technology disaster recovery, and business continuity. Supplier will update the plan annually. Supplier will notify Motorola in writing within twenty-four (24) hours of any activation of the plan.

Source: Motorola Corp 2002

Footnote: Nokia hangs on

- Nokia sells its handset division to Microsoft for a total purchase price of $9.4 billion in 2015
- Nokia handset technology used to run Microsoft smartphone software

International Business Resilience Survey

- We asked about organizations’ attitudes toward business risks and the processes they have in place.
- Benchmarking data consisted of a survey of 200+ individuals from medium and large-sized companies across Europe.
- Individuals had the following responsibilities:
  - C-suite executives
  - Risk professionals
  - Business continuity managers
Seen as having the highest impact on organizational reputation

Emerging Supply Chain Risks

Source: Risk and Insurance Magazine
Safety at work in the supply chain

- What happens when there is an excess of demand for the supplier?
- A bottleneck is created in the supply chain:
  - Puts stress on the supplier to produce faster
  - Supplier can lose buyer if targets are not met
  - Potential threat to quality control
  - Can delay buyer’s sales targets
  - Consumer-facing buyer can lose customers and revenues

Bottleneck Solutions

**Buyer’s Options**
- Reduce order
- Explore additional manufacturing options
  - In-house capacity
  - Demand additional output from existing suppliers
- Expand supplier base
  - Managed by buyer
  - Managed by supplier

**Supplier’s Options**
- Refuse additional orders
- Increase production capacity
  - Expand operational capacity with efficiency improvements
  - Improve or expand facility
  - Increase employee output and /or hours
  - Hire additional labor
  - Engage a subcontractor or third-party supplier
Many Suppliers are Small Businesses

While small and mid-sized businesses often have the most to lose in a disaster, they are often the least prepared.

The American Red Cross estimates that as many as 40 percent of small businesses that experience a disaster never reopen.

According to a study by Datapro Research Company, 43 percent of companies hit by severe crises never open their doors again.

The crises have a rippling effect, which causes another 29 percent to fail within two years.

Small Business Resilience

When a well-prepared business effectively responds to a local disaster...

Corporate self-interest ultimately serves the interests of the broader community.

Aids in overall recovery by not becoming a victim itself

Minimizes employee injury and substantially lessens economic damage to business property as well as community infrastructure

Helps protect jobs, tax revenues, supplier income streams, investor returns and the well-being of its customers

Lessens the response requirements of governments and NGOs.
Case Study: Who turned off half the Internet?

The majority of organizations believe they are better positioned to deal with traditional than non-traditional risks.
Where to invest?

- Everyone supports investment in IT system failure prevention
- Note the disconnect on IP protection

Depiction of the Outages

Photo credit: downdetector.com
DDOS Attacks behind Outages

- Dyn, a company that monitors and routes Internet traffic, hit with a major distributed denial of service (DDoS) attack that flooded its servers with enough requests to crash the system.
- Attack compounded by the increasingly-present Internet of Things.
- Requests from millions of unique Internet-accessible devices infected with the malware Mirai allowed infiltrators to gain access to remote cameras, DVRs, some kitchen appliances, etc.
- Infected devices created a robot network (botnet) that overwhelmed Dyn's servers for hours before they could recover.
- Culprits are still unknown.
- Disruption may have lost companies up to $110 million in revenue and sales.
Dyn’s Response

“It is said that eternal vigilance is the price of liberty. As a company and individuals, we’re committed to a free and open internet, which has been the source of so much innovation. We must continue to work together to make the internet a more resilient place to work, play and communicate. That’s our commercial vision as a company and our collective mission as an internet infrastructure community.”

Kyle York
Chief Strategy Officer
October 22, 2016

XiongMai’s Response

• XiongMai Technologies sells white-labeled DVR, NVR and IP Camera boards and software to downstream vendors for their own products.
• Their entire production line was turned into Botnets. 500,000+ devices on public IPs appear susceptible.
• XiongMai has taken the following steps:
  • recalling some of its earlier products sold in the United States
  • strengthening password functions
  • sending users a patch for products made before April last year.

“Security issues are a problem facing all mankind. Since industry giants have experienced them, Xiongmai is not afraid to experience them once, too.” -- from company statement
Cybercrime and Critical Infrastructure

• Power interruptions cost the US economy roughly $96 billion annually
• Over 95% of outage costs borne by the commercial and industrial sectors
• 67% of these costs from short interruptions lasting less than 5 minutes
• High dependence on electricity as an input factor of production
• Need to protect the US power grid and its vulnerable SCADA systems

We have work to do
Key Takeaways

- Create and maintain a business continuity plan for your organization
- Store your plan and other critical documents in the cloud in case something happens to your facility
- Publicize your efforts. Let your buyers know that you are reliable and have a plan to continue operations under duress
- Participate in joint exercises, drills, table tops, etc. with key customers and suppliers
DRI Resource Library

- Our website contains free informational resources, job listings, and a presentation library.
- The Professional Practices serve as the heart of our teachings and thought leadership and are available in their entirety.

![Image of Professional Practices]

![Image of International Glossary for Resiliency]
Professional Practices

- Project Initiation and Management
- Risk Assessment
- Business Impact Analysis
- Developing Business Continuity Strategies
- Incident Response
- Plan Implementation and Documentation
- Awareness and Training Programs
- Plan Exercise, Audit and Maintenance
- Crisis Communications
- Coordination with External Agencies

DRI International

is an ANSI- Standards Development Organization


Thank You

www.drii.org

Chloe Demrovsky, CBCV
cdemrovsky@drii.org
@ChloeDemrovsky

Disaster Recovery Institute