Stronger Together:
Deploying cross-sectoral collaboration to overcome the global preparedness gap

Chloe Demrovsky
President & CEO, DRI International

Global Platform for
Disaster Risk Reduction
Geneva, Switzerland

Disaster Recovery Institute

We are the non-profit that helps organizations prepare for and recover from disasters.

DRI

Train. Prepare. Recover.

What we do

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

15,000+
Certified Professionals

Certified Professionals in
100+
Countries

ANSI ACCREDITED PROGRAM CERTIFICATE ISSUER

Classes offered in
14
Languages

Courses held in
50
Countries

CQI | IRCA
APPROVED TRAINING PARTNER

What threats should we plan for?

Global Risk & Resilience Report Identifies Top Risks

A worldwide survey of business continuity professionals revealed the following top risks:

1 Major **IT Disruption** (deliberate)

2 Severe **Data Breach**

3 Extreme **Natural Disaster**

4 Major **IT Disruption** (accidental)

5 **State** Sponsored **Cyber** Attack

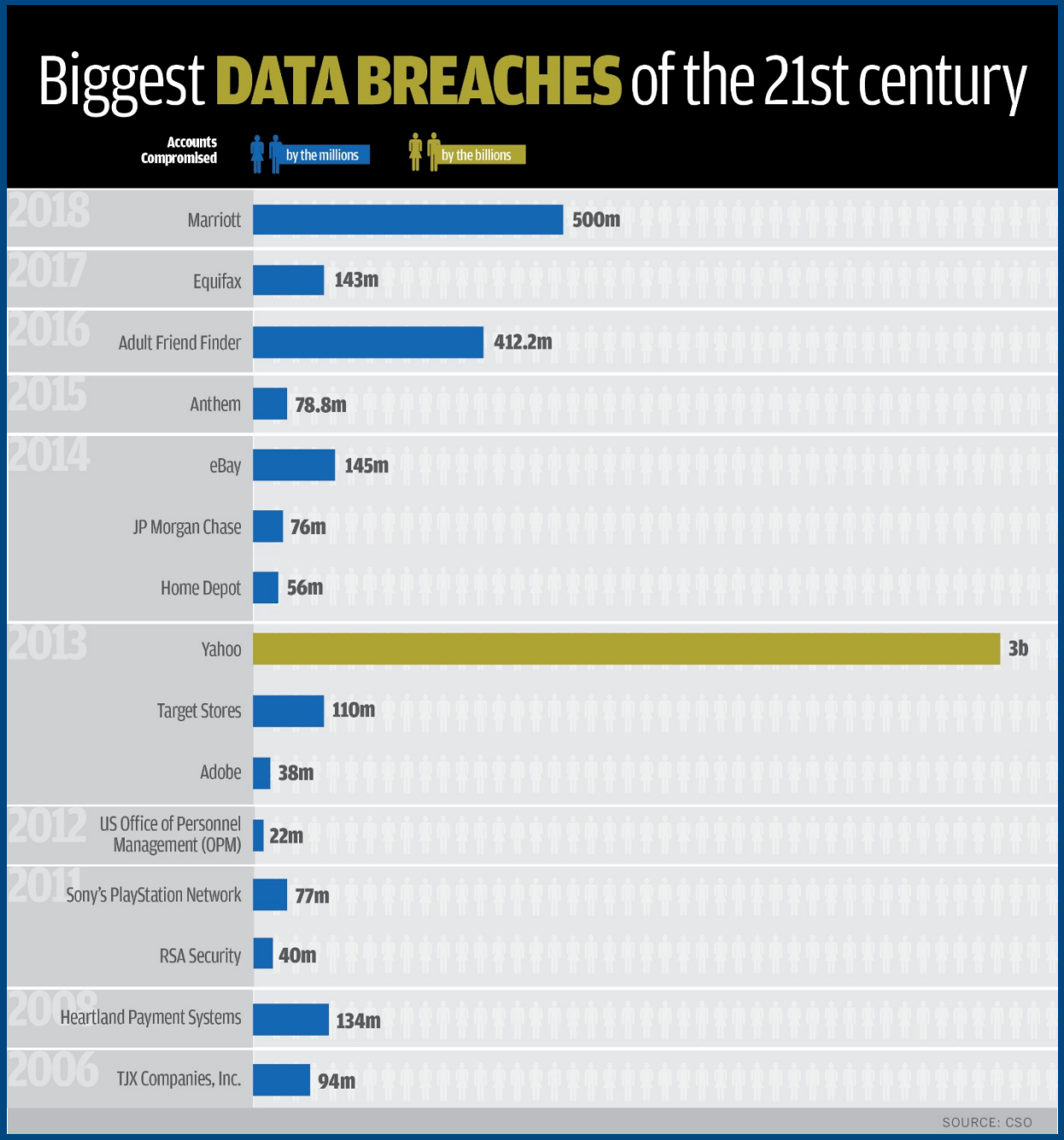
6 **Cyber Terrorism** on Operational Technology (OT)

7 Critical National **Infrastructure** (CNI)(CNI) **Failure**

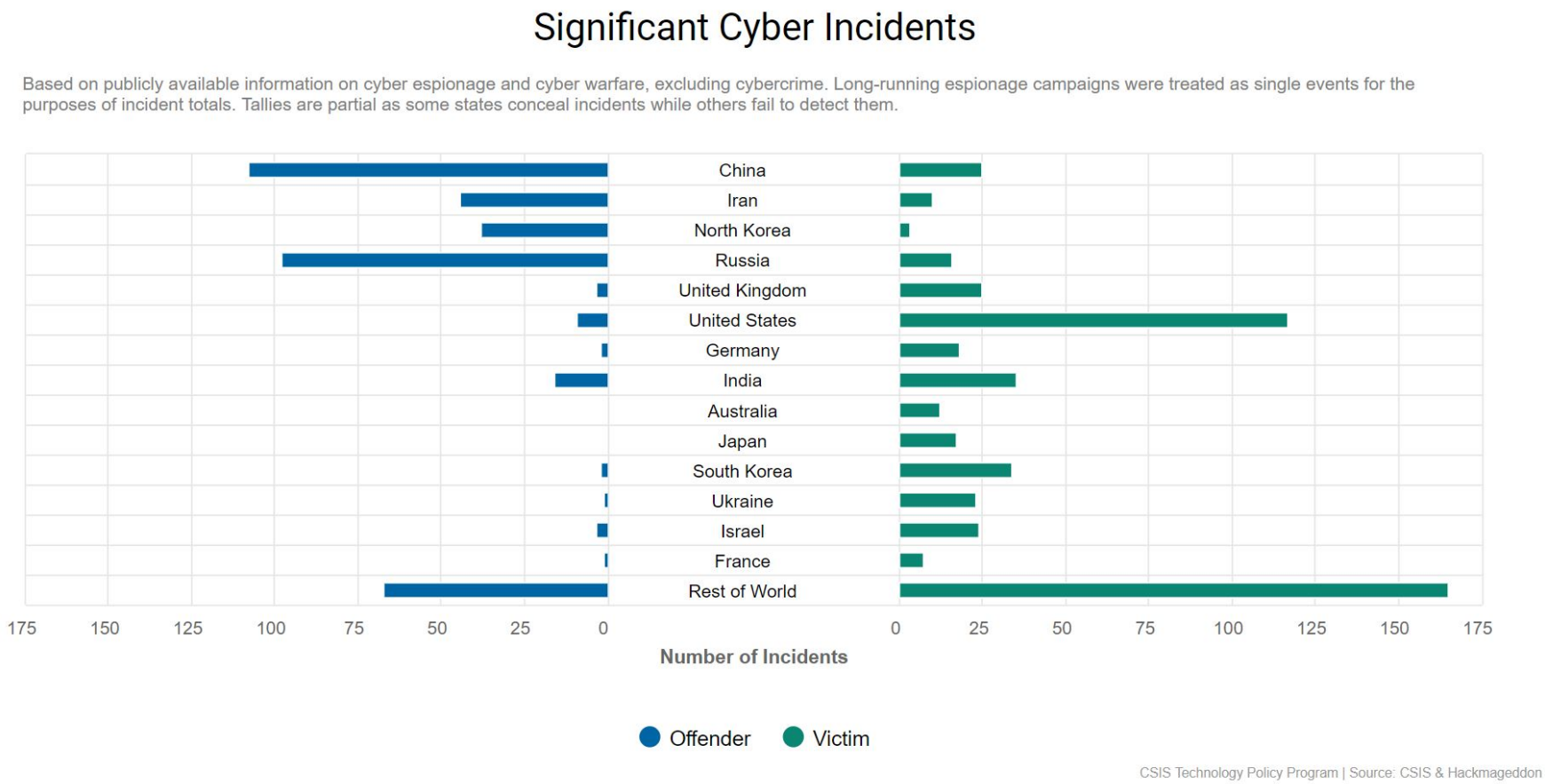
8 Serious **Supply Chain** Disruption

9 **Man-made Major** Disasters

10 Global **Financial** Crash


Biggest DATA BREACHES of the 21st century
Accounts Compromised
by the millions
by the billions
2018
Marriott
500m
2017
Equifax
143m
2016
Adult Friend Finder
412.2m
2015
Anthem
78.8m
2014
eBay
145m
JP Morgan Chase
76m
Home Depot
56m
2013
Yahoo
3b
Target Stores
110m
Adobe
38m
2012
US Office of Personnel Management (OPM)
22m
2011
Sony's PlayStation Network
77m
RSA Security
40m
2008
Heartland Payment Systems
134m
2006
TJX Companies, Inc.
94m
SOURCE: CSO

5: State-Sponsored Cyber Attack



This timeline records significant cyber incidents since 2006, focusing on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

7: Critical National Infrastructure Failure

- 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

Top Probabilities by Region

North America | Latin America | Europe | Asia | Rest of World





Issue	North America	Latin America	Europe	Asia	ROW
Major IT Disruption (deliberate)	1	3	1	7	1
Severe Data Breach	2	6	2	2	2
Major IT Disruption (accidental)	3	7	3	9	3
Critical National Infrastructure (CNI) Failure	4	12	4	4	5
Cyber Terrorism on Operational Technology (OT)	5	14	8	10	6
Extreme Natural Disaster	6	1	11	1	4
Lack of Crisis Management Expertise	7	2	9	3	7
Global Financial Crisis	10	4	5	8	9
Loss of License by Regulators	9	5	6	5	8
Global Financial Crisis	11	9	5	5	8

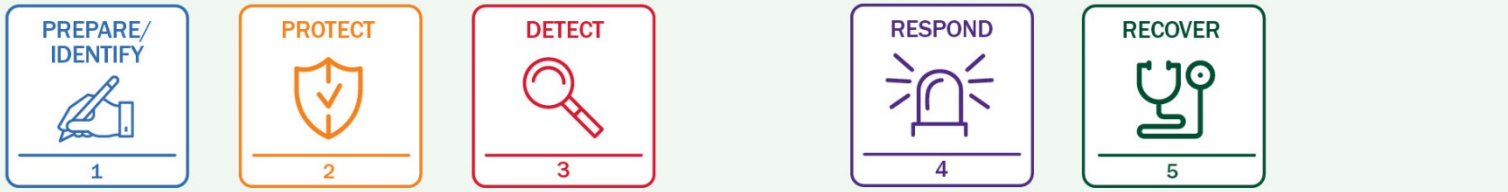
Cross-sectoral Collaboration

- Neither sector can address these challenges alone
- Natural disasters affect every type of organization so response must be collaborative
- Private organizations now find themselves on the front lines of the cyber battlefield, too
- Governments should provide leadership and cohesion for a national strategy
- Governments should work to understand the private sector model to better support, defend – and leverage -- it

Cyber Resilience

A FORMULA FOR CYBER-RESILIENCE

Follow this simple formula (cybersecurity + business continuity) to achieve cyber-resilience.



Cybersecurity (Elements 1-3)

1. Identify, assess, and manage the risks
2. Protect information and systems
3. Detect anomalies/cybersecurity incidents

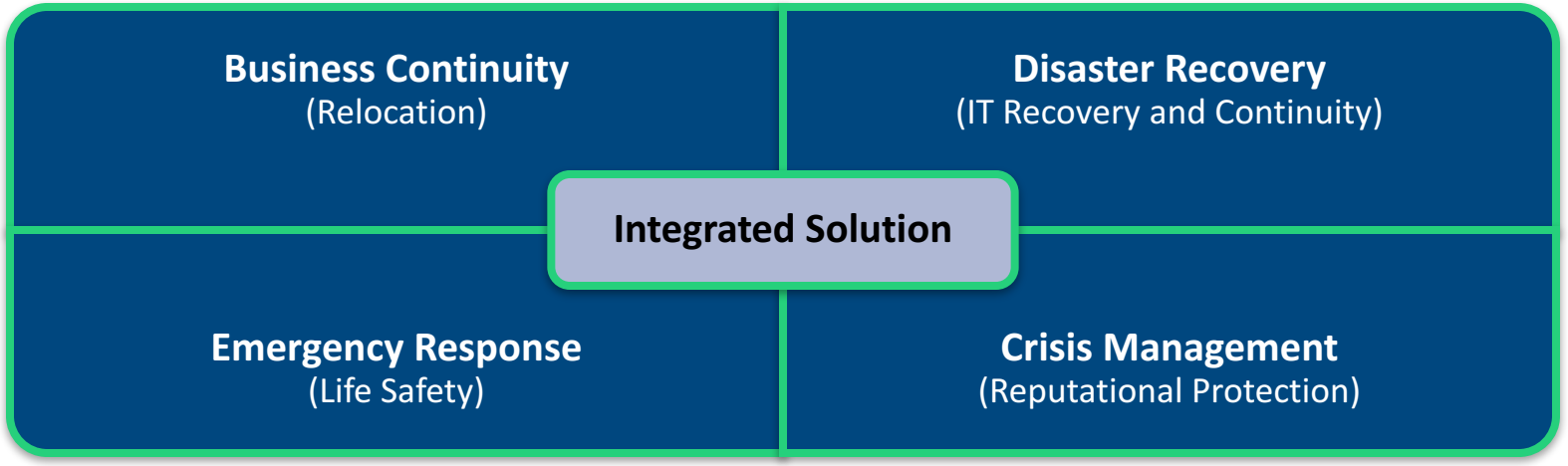
Business Continuity (Elements 4 and 5)

4. Respond with proven capabilities
5. Recover via incident management plan

Continuity is key to building resilience

Under the umbrella of

Business Continuity Management



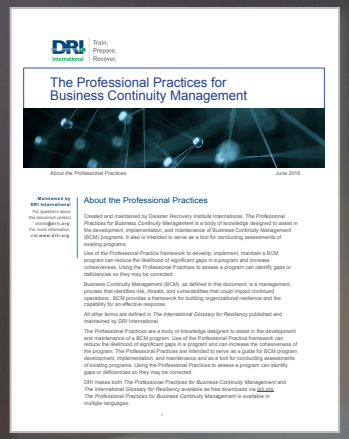
Focusing on effects, impacts, consequences

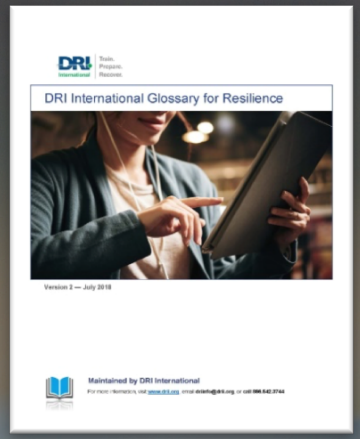
Facilities	Business or Operational	Technology	Organization
• Fire • Flood • Bomb scare • Pandemic: SARS, H1N1, H5N1 • Terrorism • etc.	• Supply chain • Process error • Transit strike • Pandemic: SARS, H1N1, H5N1 • Labor strike • etc.	• Network problem • Application error • Hardware failure • Virus • Power problem • etc.	• Merger and acquisition • Succession • Intellectual property issue • Audit issue • Financial problem • etc.

Effect categories

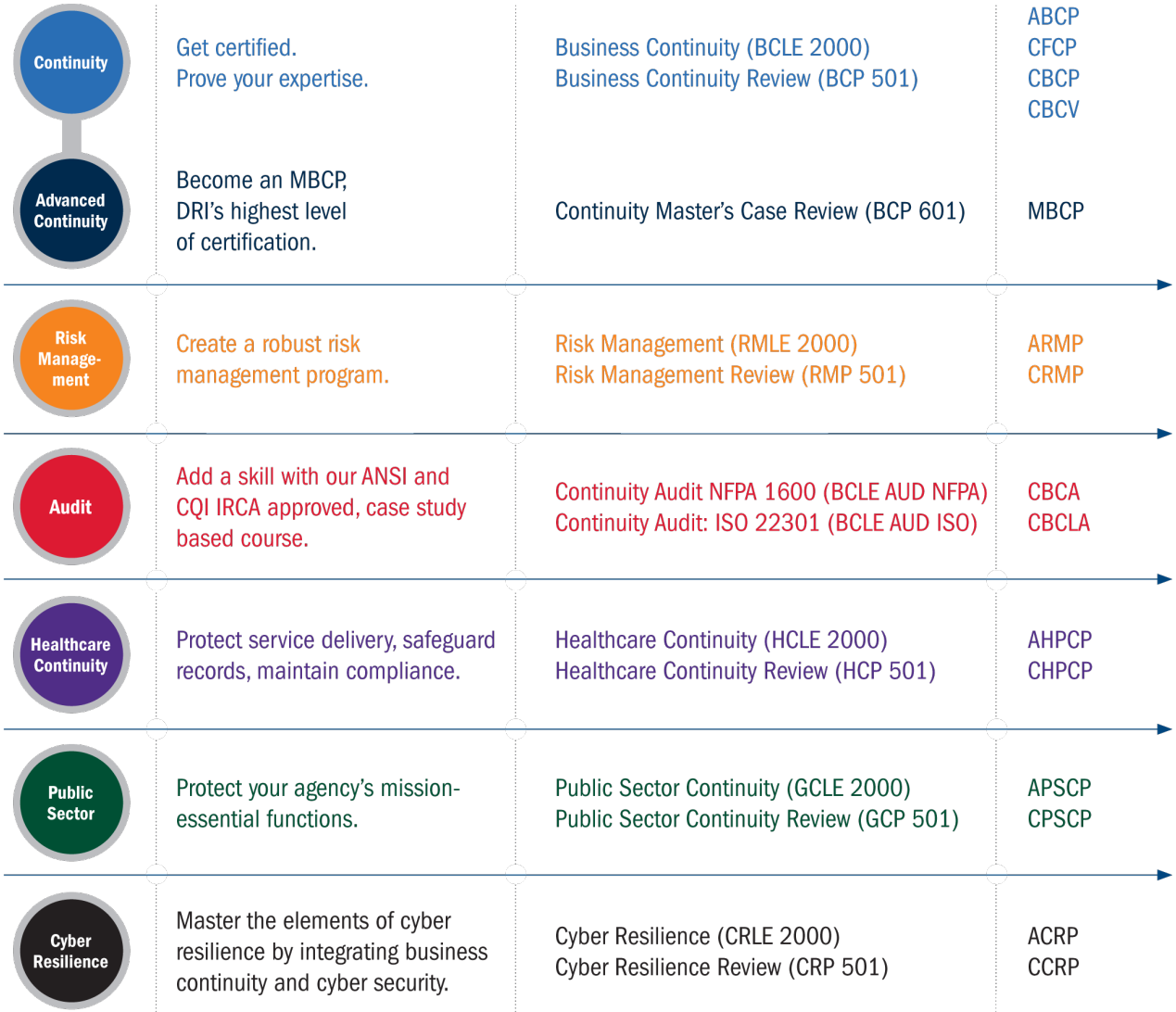
The Professional Practices for Business Continuity Management

1. Program Initiation and Management
2. Risk Assessment
3. Business Impact Analysis
4. Business Continuity Strategies
5. Incident Response
6. Plan Development and Implementation
7. Awareness and Training Programs
8. Business Continuity Plan Exercise, Assessment, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies





Career Tracks



Is Your Organization Certified by DRI?

Resilient Enterprise

- Recognizing organizations that have demonstrated extraordinary commitment to preparedness and resilience by successfully completing our assessment program.

Center of Excellence in Resilience

Recognizing organizations that achieve Resilient Enterprise and:

- Provide a forum for industry-wide thought leadership and information sharing.
- Provide facilities and resources to conduct seminars.
- Disseminate information at times of emergencies.

Thank You

Chloe Demrovsky
President & CEO
DRI International
cdemrovsky@drii.org,

*We can't predict the **future** and we can't control what will happen.*

*What we can control is our **preparation** for it and our **reaction** to it.*