Business Continuity Management

Cyber Security importance

by Ashraf Hasanov
Business Continuity Expert
BCMS BS25999 Lead Auditor
Regional Disaster Response Team Member of IFRC

What could stop your business?

Human couse:

- Hacking, Cyber attack
- Terrorism
- Corruption
- …

Natural Disaster:

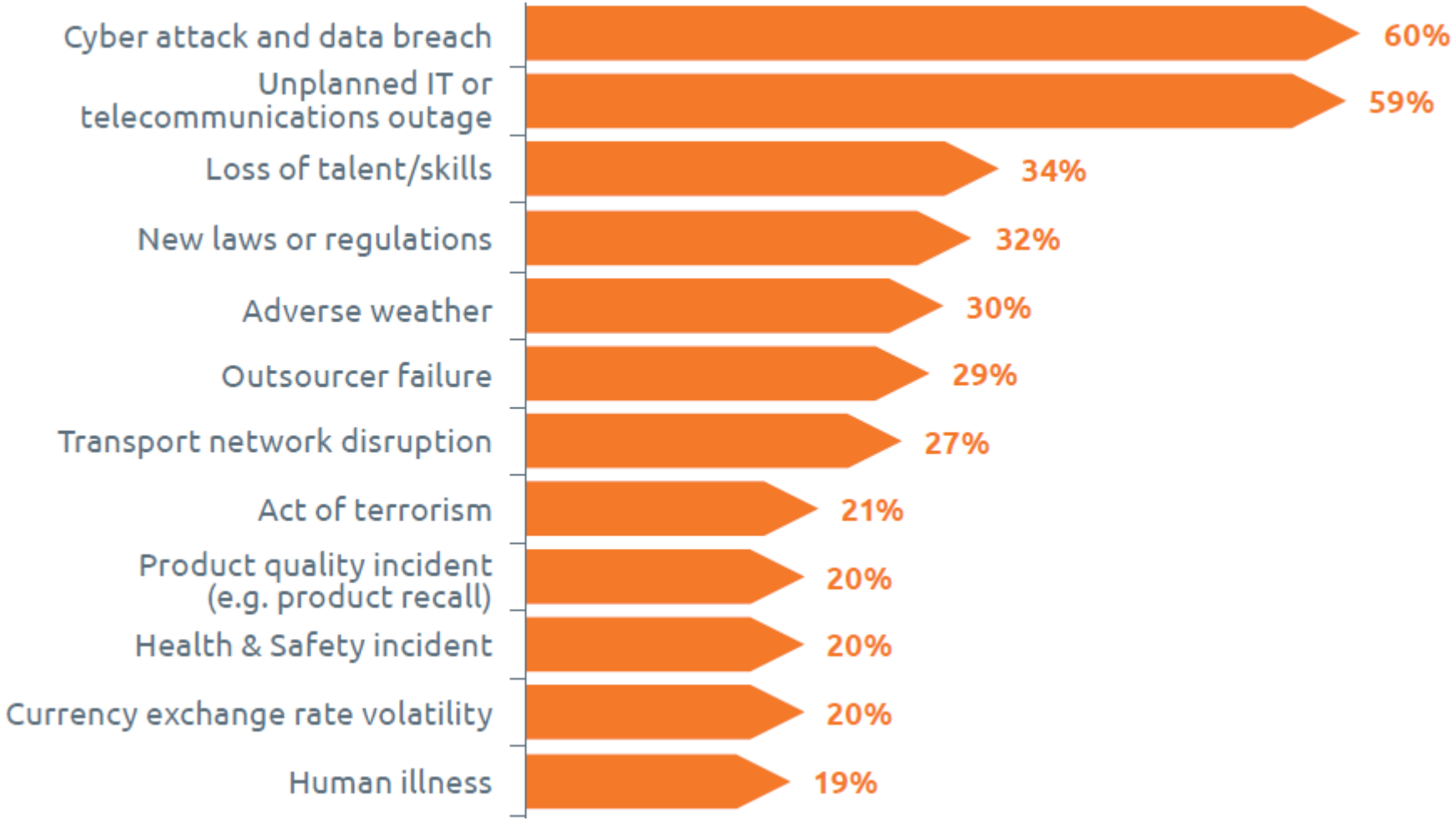
- Earthquake
- Flood
- Extreme weather
- …

Industrial Disaster:

- İT-Telecom outage
- Energy outage
- Technology explosion
- …

What could stop your business?

Business Continuity Institute report 2017: Threat and trends



What could stop your business?

BCİ report 2017: Top threat by business sector

Rank	Financial & Insurance Service	Professional Services	IT & Communications
1	Unplanned IT or telecommunications outage (69%)	Loss of talent/skills (39%)	Unplanned IT or telecommunications outage (62%)
2	Cyber attack and data breach (43%)	Unplanned IT or telecommunications outage (37%)	Cyber attack and data breach (49%)
3	Loss of talent/skills (34%)	Cyber attack and data breach (34%)	Loss of talent/skills (43%)
4	Outsourcer failure (33%)	New laws or regulations (32%)	Outsourcer failure (41%)
5	Adverse weather (33%)	Energy scarcity (32%)	New laws or regulations (38%)

Cybersecurity is not just an IT problem — it's a business risk that needs to be accounted for in the business continuity plan.

What is BCM?

Business continuity is the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

- *Holistic management process*
- *Identifies potential impacts*
- *Framework for resilience and recovery*
- *Safeguard interests of key stakeholders*

Standards: BS25999, ISO22301

5 reason why BCM need for Cyber security?

1. **May 2018, the Network and Information Systems (NIS Directive)** transposed into national law within EU. The Directive requires operators of essential services (OESs) and digital service providers (DSPs) that support the nation's infrastructure to enhance their cyber security to minimize the impact of incidents and ensure business continuity.
2. **May 2018, the EU's General Data Protection Regulation (GDPR)** required organizations to protect personal data.
3. **Targeted cyber incidents trend**. According to a survey conducted at Black Hat Europe 2017, the biggest cause for concern among cyber security professionals is targeted cyber attacks aimed at their organization, and the detrimental effects these might have.
4. **An increase in cyber attacks on critical infrastructure**. The Not Petya attack and the impact it had on the shipping industry is an example of how substandard security measures can result in devastation.
5. **Increasing natural disasters**. As well as cyber attacks, natural disasters are a real threat to an organization's business resilience and can disrupt information security, networks and systems. Although organizations can protect against a cyber attack and potentially prevent a data breach from happening, an effective BCM helps you to look at and evaluate the environment.

Benefits of BCM

- ***Provides a method*** *of restoring your ability to supply critical services and products following a critical disruption*
- ***Confidence*** *in the ability of your business to survive*
- ***Competitive advantage*** *gained due effective response and recovery of critical disruption*
- ***Early warning and Risk mitigation*** *action of any vulnerabilities in your business*
- ***Improve operational resilience*** *and critical incident management*
- ***Insurance costs improvements***
- ***Win tenders*** *due BCM excellence. (ps: tender of US and German embassies required BCM arrangement)*

What may cause absence of BCM?

- *Impact reputation, loss of customers' trust;*

- *Unexpected growth of recovery costs;*

- *Financial loses, Asset loses, loss of company valuable experts;*
- *Failure to perform contractual obligations;*

- *Possible bankruptcy and dissolution of the company.*

Why we need BCM?

Protect business alive in case of critical incidents and assure customers and shareholders that:

"We have in place comprehensive business continuity procedures to minimize the impact and maximize recovery of any significant business disruption."

Why we need BCM-details?

- *Define critical businesses (processes, services, data, objects) by Business Impact Analyses (BIA) process*
- *Recovery Time of Objectives (RTO) and Maximum Tolerable Period of Disruptions (MTPD) calculation of those critical businesses*
- *Execute Risk Assessment (RA) and prepare risk mitigation plans for each critical businesses*
- *Setup Continuity Strategy of organization (risk mitigation and response recovery plans based on incident scenarios)*
- *Prepare Crises and Disaster Response processes with plans of incident scenarios - Cyber attack as well.*
- *Simulate plans. Cyber Drill.*

Align Business Continuity and Cyber Security response

Cyber security risk and issue, it is not only an IT issue, as organizations are now far too dependent on technology.

Organizations should has leadership approach to cyber security as they do any other business risk:

- ✓ *Financial impact,*
- ✓ *Reputational impact*
- ✓ *Operational impact.*

By integrating Cyber security responses into leadership response strategy, you'll ensure:

- ❑ *leadership has the information necessary to assess and control the overarching business impacts,*
- ❑ *ensuring IT has leadership's support in rolling out selected response strategies.*
- ❑ *Business Continuity response plan scenarios included also Cyber attack which simulated periodically.*

Criticality of information and Recovery Times

Some cases there is misunderstanding to evaluate business criticality of information and depended IT nodes.

For example there could be cases when 5% data generated more than 50% revenue and in that case from IT point of view it is not so critical but in business point of view it is critical.

In that case best solution is Business Impact Analyses (BIA) process which is sub process of Business Continuity. BIA process identified:

- *Criticality level of data based on business criteria (depended financial value, customer %, etc..)*
- *Recovery Time for response planning.*
- *Important justification of Cyber Security risk mitigation plans to meet expected Recovery Time and minimize impacts.*

Business Continuity roadmap

	BCM Lifecycle	*Main Actions*
1	*BCM Program Management*	*Business Continuity (BC) Policy and Scope; BC governance;*
2	*Understanding the Organization*	*Business Impact Analyses (BIA); Risk Assessment (RA);*
3	*Determining BCM Strategy*	*BC Strategy (with Response Recovery Strategy and Risk Mitigation Strategy);*
4	*Developing BCM Response*	*Crisis and Disaster Response process and BC response plans (incl. Cyber Security responses); Execution Risk Mitigation;*
5	*Test, Reviewing and Audit*	*BC testing, simulations, Audit of BCM processes; / External Audit for certification*

*“**If you fail to plan, you are planning to fail**.” Benjamin Franklin*

THANKS!

E-mail: ashraf_hasanov@yahoo.com