Business Continuity Management

Aart Bitter - 14 januari 2014

Praktijk case

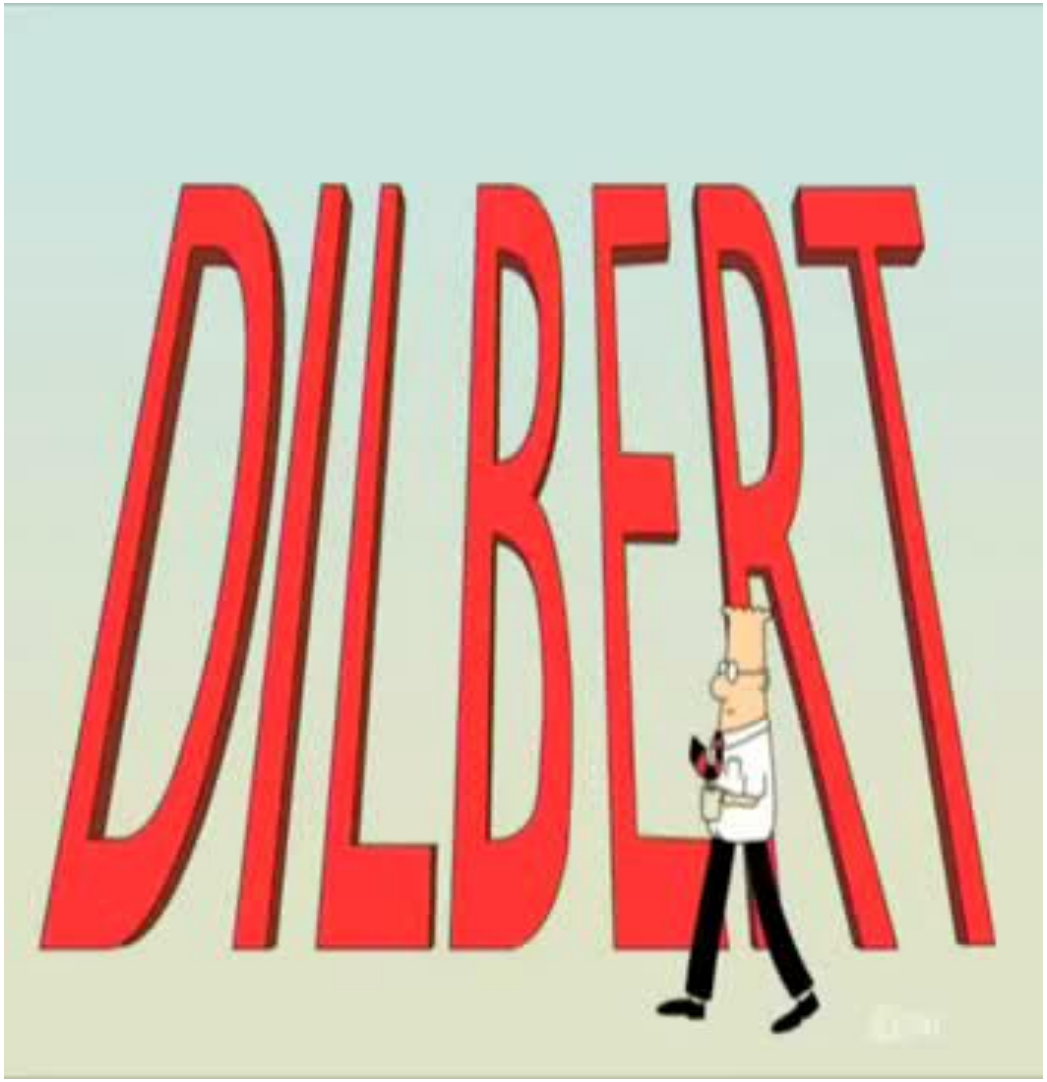
- Wij zijn als bierbrouwerij voorgedragen om onze producten te leveren aan het Holland House tijdens het WK 2014 in Brazilië
- De FIFA wil met ons een langlopend contract aangaan voor levering tijdens alle komende EK's en WK's
- Voorwaarde: wij moeten onze producten continu kunnen leveren

- **Hoe gaan we zorgen dat we de continuïteit van ons bedrijf en de levering van onze producten kunnen garanderen?**

- *Hint: laten we een **management systeem** voor Bedrijfscontinuiteit inrichten (conform ISO 22301)*

Bedrijfscontinuïteit met een Business Continuity Management System (BCMS)

Disaster Recovery Plan



Bedrijfscontinuïteit

- Waarom is het belangrijk
- Wat is het
- Voordelen voor bedrijven, die het geïmplementeerd hebben
- Wat kan ik als adviseur voor mijn klant betekenen
- Waar lopen we (de klant en de adviseur) tegenaan

Noodzaak voor bedrijfscontinuïteit

Fysiek

- Brand
- Overstroming
- Stroomuitval
- Onrust/staking

Operationeel

- Onderbreking van productie
- Onderbreking van distributie

3rd Party-Outsourcing

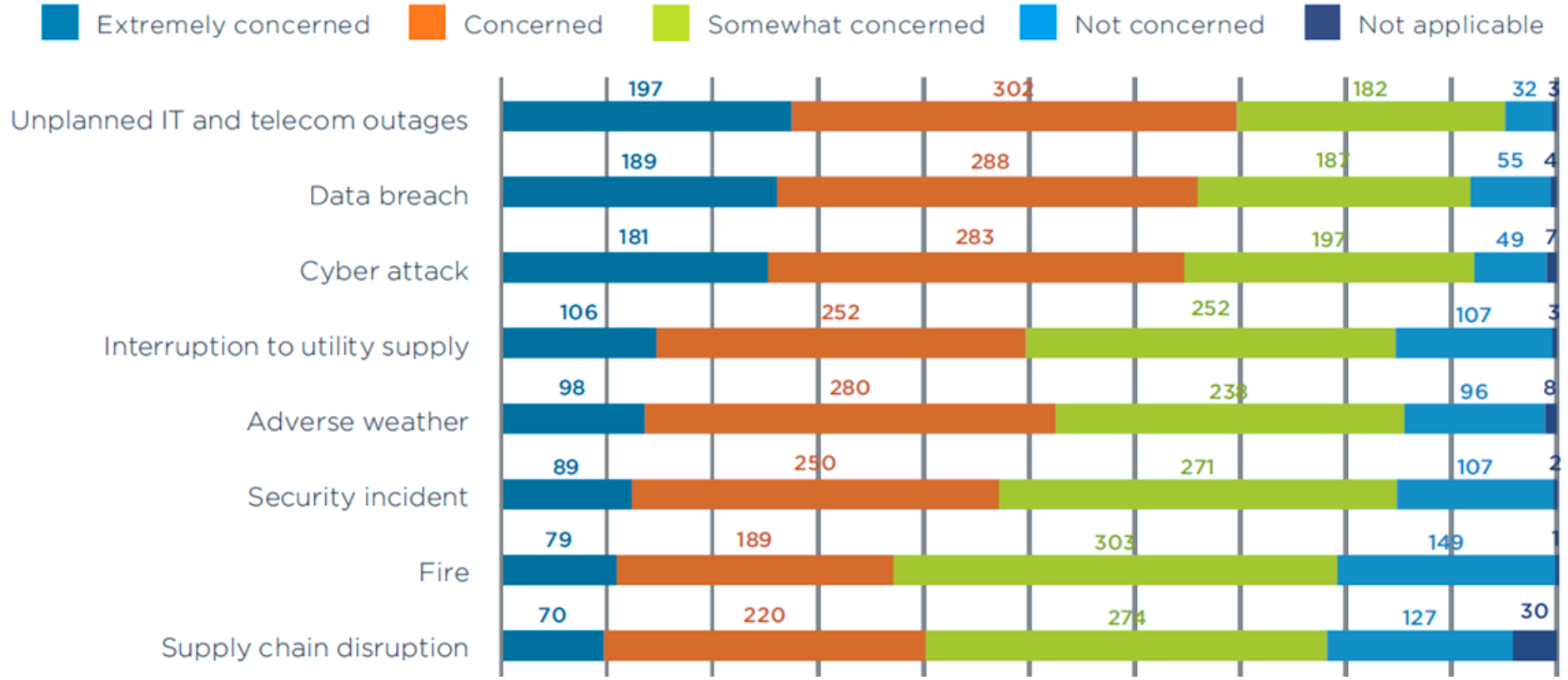
- Verlies van 3rd party warehouse
- Commitment van leverancier aan bedrijfs-continuïteit

IT risico's

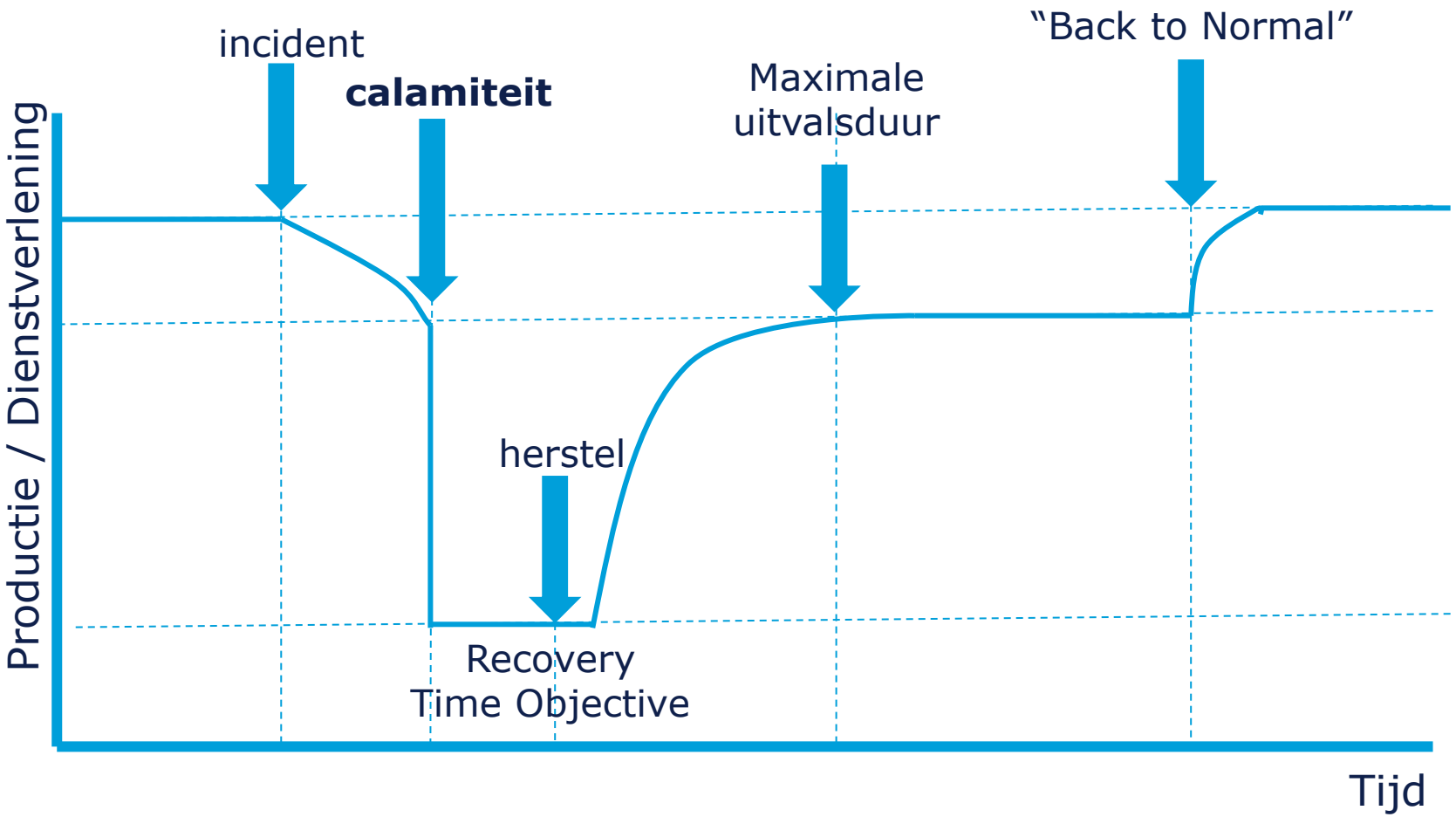
- Storing van IT diensten
- Storingen in kritieke systemen, netwerken, databases, etc.

BCI Survey: Horizon scan January 2013

Figure 3.1 - Based on your analysis, how concerned are you about the following threats to your organisation in 2013? (730 responses)



Wat is Business Continuity Management



ISO 22301

- Nieuwe (2012) internationale standaard voor BCM
- **B**usiness **C**ontinuity **M**anagement **S**ysteem – **Eisen**
- Aansluiting bij andere management systemen (ISO 27001, ISO 9001, …)
- Certificeerbaar
- Internationale BCM "best practice"
  - Input en aanbevelingen van vele BC professionals en experts
  - Niet opnieuw uitvinden van het wiel

- ISO 22301 - **Societal Security** – BCMS - Eisen
- Het belang van BCM in de maatschappij en te garanderen dat we een calamiteit aankunnen.

Voordelen voor bedrijven

- Veerkracht (“resilience“)
  - Een bedrijf is bestand tegen een calamiteit
- Herstellen van de productie en/of dienstverlening
  - Het bedrijf kan na een calamiteit de belangrijkste producten en diensten herstellen tot een van te voren bepaald niveau en binnen een bepaalde tijd
  - Incident Management Plan: hoe te reageren op een incident
  - Communicatie Plan: waarschuwing en communicatie
  - Business Continuity Plan: het kunnen continueren van de belangrijkste (kritieke) processen
  - Recovery Plan: terugkeren naar “normale” bedrijfsactiviteiten
- Beproefde methode
  - Aantoonbaar door het oefenen en testen
  - Continu verbeteren vanuit het management systeem

Wat kan ik voor mijn klant betekenen?

ISO 22301:2012

- 1 Scope
- 2 Referenties naar andere standaarden
- 3 Termen en definities
- 4 - Context van de Organisatie
- 5 - Leiderschap
- 6 - Planning
- 7 - Ondersteuning
- **8 - Uitvoering**
- 9 - Evaluatie van de uitvoering
- 10 - Verbetering

8. Uitvoering

Continuïteitsplannen

- Rollen en verantwoordelijkheden voor mensen en teams,
- Activeren van de plannen,
- Reactie op de directe gevolgen van een calamiteit,
  - veiligheid / welzijn van individuen en omgeving,
  - voorkomen van verdere schade en uitval;
- Communicatie,
  - medewerkers en hun verwanten, belangrijkste derde partijen en nooddiensten;
- Continueren of hervatten van de bedrijfsactiviteiten,
  - binnen een van te voren vastgestelde periode,
  - op een alternatieve manier (zonder IT systemen); op een andere locatie;
- Hoe om te gaan met (de) media,
- De-activatie van de plannen na de calamiteit.

Business Continuity Plan

- Doel en scope / reikwijdte,
- Doelstellingen,
- Activeringscriteria en -procedures,
- Implementatie procedures,
- Rollen en verantwoordelijkheden,
- Communicatie procedures,
- Interne en externe afhankelijkheden en interacties,
- Resource eisen,
- Informatiestromen en documentatieprocedures.

Testen en oefenen

- De organisatie moet de continuïteitsplannen en -procedures testen en oefenen.

Waarom testen en oefenen?

- Valideren van scope en uitgangspunten,
- Correcte werking van technische faciliteiten,
- Voldoende capaciteit op en van de uitwijk locaties,
- Verkorten van doorlooptijd van de procedures,
- Awareness bij derde partijen,
- Competenties en bewustwording.

Waar lopen we (de klant en de adviseur) tegenaan?

- Geen sprake van een aantoonbaar managementsysteem,
- Scope,
- Geen duidelijke taken en verantwoordelijkheden voor het crisisteam,
- Wanneer wordt een gebeurtenis een incident en/of een calamiteit?
- Er zijn geen gedetailleerde (IT) recovery plannen,
- Teststrategie, testplannen en de uitvoering daarvan.

- **Oplossingen:**
  - aansluiten bij bestaande management systemen,
    - ISO 27001 A.17 Information security aspects of business continuity management
    - ISO 20000 6.3 Service Continuity & Availability Management”,
    - ISO 22000 5.7 Emergency preparedness and response
  - training Implementatie ISO 22301,
  - woon ook eens de oefeningen bij.

Meer informatie

- ISO 22301 Business continuity management systems — Requirements
- ISO 22313 Business continuity management systems — Guidance
- ISO 22398 Guidelines for exercises and testing
- ISO 31000 Risk Management Principles and Guidelines
- ISO 27031 Guidelines for ICT - readiness for business continuity
- ISO 28002 Development of resiliency in the supply chain
- PAS 200 Crisis management – Guidance and good practice
- BCI Good Practice Guidelines 2013
- www.theBCI.org
- http://www.drj.com/
- http://www.continuitycentral.com/

Dank voor uw aandacht !

Vragen

Opmerkingen

Suggesties

Aart.Bitter@isgcom.nl

Contact

Aart Bitter
aart.bitter@isgcom.nl / aart.bitter@information-security-governance.com
+31 599 648 052 / +31 6 573 11 593

www.dnvgl.com

SAFER, SMARTER, GREENER