Business continuity management

2 March 2015
Alan Ross – Zurich's Strategic Risk Management Practice
College Development Network

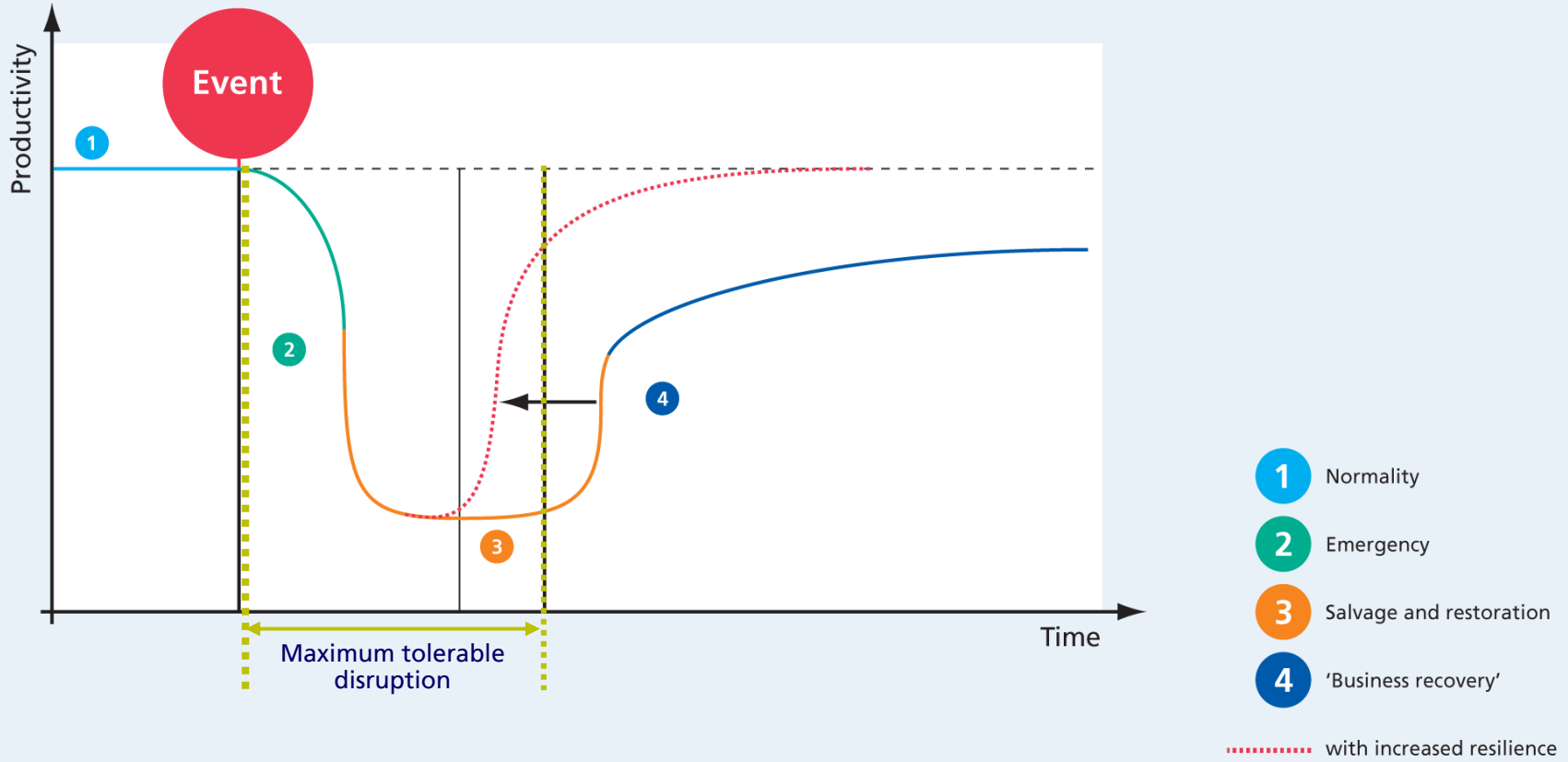
Zurich Risk Engineering

alan.ross@uk.zurich.com
07764 149330
Twitter: @ZurichMunicipal

Objectives for Today

- What does effective business continuity look like
- What risks should you consider?
- Challenges you might face in responding
- Maintaining business continuity plans

The Resilience Curve



Characteristics of crises & BC incidents

3 broad characteristics:

1. They pose a threat to the organisation; there is potential for significant harm to the reputation, financial sustainability or long term success of the organisation

2. They usually happen without warning – or previous warnings have been ignored or not dealt with

3. They put significant pressure on decision makers to act quickly, possibly with imperfect information

“It won’t happen to us”

“It won’t happen to us”

Incidents, Near Misses & Lessons Learned

- Dumfries & Galloway College
- City University London
- University of Southampton
- University of Strathclyde
- London Metropolitan
- “Near misses”

What type of incidents could cause disruptions or crises?

- Perception of negligence or wrong doing, e.g. ‘climate-gate’, by an individual or group
- Links to ‘controversial’ figures , groups or businesses
- Violence against staff or students
- Other health & safety incident where staff or students are affected
- Misconduct or deception, e.g. large scale fraud or bribery
- Process failure
- Negative publicity over a policy or action taken
- Pressure group protest
- ‘Gaffs’ by senior staff
- Extreme weather
- Loss of IT or communications infrastructure
- Transport disruption
- Loss of a building (temporary or permanent loss)
- Loss of key person or skills
- Failure of a key supplier or partner organisation
- Loss of Utilities
- Environmental incident

Response Issues

- Assumptions
- Roles & responsibilities not clear
- Plans are useless, planning is indispensable - get your team in a room on day 1 and plan!
- Use expertise available, e.g. insurers & loss adjustors, disaster recovery experts
- Understand your Business Interruption policy – additional expenditure & stillage conditions
- Insurance – what can you spend money on?
- Secondary incidents – building services can be linked
- Avoiding further damage
- Key suppliers location
- Staff location and ability to get to a location
- Communicate, communicate, communicate
- Secondary incidents
- Think about where your critical infrastructure and assets are
- Identify alternatives for long lead time equipment
- Security – including data – post incident
- Business as usual – e.g. procurement – hampers recovery
- Staff overburdened / single points of failure
- Human impact
- Duty towards other site users?
- Set up process to monitor & react to weather warnings
- Conflict between departments
- Poor record keeping
- Learn lessons for future

Considerations & Challenges for Relocation

- Suitable options for relocation
- Asset protection at incident site
- Asset recovery from incident site
- Asset transfer
- ICT configuration and hardware
- Stakeholder management & communication
- Liaison with Incident Management Team
- Health & safety risk assessments & induction
- Modifications & alterations to premises, e.g. for disable access
- Timetabling
- Specialist & non-specialist learning & teaching spaces
- Ability of special events to run / not run
- Travel information and facilities for staff & students, e.g. prioritise car sharing
- Access to financial support for students?
- Switchboard & reception functions
- Decision making: who makes the call to relocate?
- Capacity of facilities at relocation site: toilets, catering, child care, parking, storage, computer labs & libraries
- Staff co-ordination
- Office space & meeting rooms
- Impact on 3rd party site users
- Issues monitoring and management

Maintenance of plans

- How do we maintain business continuity plans?
  - Regular reviews (annual?) although contact details may be more regular
  - Exercises: live or desktop
  - Training & awareness

Summary

- Review risks – what can disrupt your critical infrastructure and assets?
- What services will be disrupted as a result? What's critical and non-critical?
- Is there a documented, clear plan that you understand?
- What have you done to identify gaps? 3rd party review, training of staff, & exercising
- Engage with your insurance providers