



www.nascenta.com

NASCENTA
Information Security & Resilience

‘One of our agents is missing’

Incident Management - not just an IT Issue

Martin Cassey

- Introduction
- What is an Incident?
- Incident Management
- Case Study
- Personal Experience
- One of Our Agents is missing
- Where to get help



Nascenta Ltd

- Private Business - evolution of Cambridge Data Safe Ltd (incorporated 1999)
- Re-launched 2015 as Nascenta Ltd
- Information Security & Resilience
Consultancy & Solutions for SMEs
- People Centric approach – People & Technology



What is an Incident?

noun

- An event that is either unpleasant or unusual

adjective

- Touching or hitting the surface of something

Cambridge Dictionary



What is Incident Management?

- **Incident management (IM)** is an IT service management (ITSM) process area. The first goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Wikipedia – 18/1/17



An Alternative View

- **An Incident** is an event that could lead to loss of, or disruption to, an organisation's operations, services or functions and which can't be managed as part of 'Business As Usual' (BAU). - If not managed an incident can escalate into an emergency, crisis or disaster.



An Alternative View

- **Incident management (IM)** is a real-time 'physical' process. To be effective it relies upon effective leadership supported by (often multi-disciplinary) teamwork and timely action.
- **Its primary objective** should be to protect people followed by customers, infrastructure and then the business.



IM vs BC/DR

- Processes are complementary
- If an Incident can't be resolved within an acceptable timescale (typically hours) then progress to BC plan and/or Disaster Recovery



Business Resilience

- Resilience helps organisations live long and prosper.
- Resilience extends way beyond BC or DR.
- Improving resilience should be a core part of business culture.
- Resilience represents a sustainable competitive advantage.
- Resilience is a good way to reduce the incidence of Incidents!



What is Needed to Manage an Incident?

- Leadership
- Authority
- A Plan
- Supportive Team
- Ability to adapt & Innovate
- Strong Nerves & Good Luck



Incident Policy/Procedure

- Establish a Policy/Procedure
- Determine Success Criteria
- Risk Analysis/Identify Scenarios
- Develop Plan/Guidelines around Scenarios



Incident Policy/Procedure/Plan

- Know who to keep informed
- Know how to contact Senior Management, Staff, emergency services, CERT, etc.
- Know when/how/where to get help
- Practice, Practice, Practice



Some Possible Scenarios

- Fire Alarm
- Sickness/Accident at Work
- IT Failure
- Utility Failure
- Bad Weather/Epidemic/Foot & Mouth
- Cyber Attack/Security Breach
- Fire/Flood/Crime/Terrorism



Incident Response Team

- Incident Manager
- Scribe (Recorder)
- External/Internal Communications
- Facilities/Estates
- IT
- Operations
- Security/H&S
- Gophers



Incident Room

- A known place for the IRT to congregate and from which to manage the incident
- Desk, Phone(s), PA system, 2 way radios
- Hard copies of IM Plan, contact lists, etc.
- CCTV
- IT
- White boards, stationery, etc.
- Internet access, Broadcast TV



Timing

- Understand expectations regarding timing for dealing with an Incident
- 'First 24/48/72 hours'
- GDPR requires disclosure within 72 hours of breach discovery



Some Possible Issues

- The root cause of incident may not be obvious.
- IT failure or Cyber attack?
- Your priority is to restore normal service, Law Enforcement may want to preserve evidence.
- What if the press take an interest?
- Consider your Plan to be a guideline!



Case Study - MK Audi

‘Monday 1 June 2015 started like any other day until, around 12:30pm, the team heard a loud bang followed by the sound of a fire alarm. The roof of the workshop was about to collapse, taking 20 cars with it.’

‘Torque’ Iss 8 2015



Some Personal Experiences

Few things can prepare you for the awesome responsibility, fear of failure and panic that sets in when you have to manage your first incident.



Scenario

- Separate 'Compound' within larger Site
- Rural location
- Many Buildings, 500+ staff
- Administrative, Engineering,
Manufacturing and Operational areas



Some Personal Experiences

- Fire Alarm
- Unattended Package
- Partial Roof Collapse
- Missing member of staff



Incident Management training

'One of our agents is missing'



Where to get help

Martin Cassey
Nascenta Ltd
martin@nascenta.com
+44 (0)1223 926 920



Questions?

