Incident management

An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions. **Incident management** (**IcM**) is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. These incidents within a structured organization are normally dealt with by either an incident response team (IRT), an incident management team (IMT), or Incident Command System (ICS). Without effective incident management, an incident can disrupt business operations, information security, IT systems, employees, customers, or other vital business functions.[1]

Description

An incident is an event that could lead to the loss of, or disruption to, an organization's operations, services or functions.[2] Incident management (IcM) is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. If not managed, an incident can escalate into an emergency, crisis or disaster. Incident management is therefore the process of limiting the potential disruption caused by such an event, followed by a return to business as usual. Without effective incident management, an incident can disrupt business operations, information security, IT systems, employees, customers, or other vital business functions.[1]

Physical incident management

National Fire Protection Association states that incident management can be described as, '[a]n IMS [incident management system] is "the combination of facilities, equipment, personnel, procedures and communications operating within a common organizational structure, designed to aid in the management of resources during incidents".[3][4]

Physical incident management is the real-time response that may last for hours, days, or longer. The United Kingdom Cabinet Office has produced the National Recovery Guidance (NRG), which is aimed at local responders as part of the implementation of the Civil Contingencies Act 2004 (CCA). It describes the response as the following: "Response encompasses the actions taken to deal with the immediate effects of an emergency. In many scenarios, it is likely to be relatively short and to last for a matter of hours or days – rapid implementation of arrangements for collaboration, coordination and communication is, therefore, vital. Response encompasses the effort to deal not only with the direct effects of the emergency itself (eg fighting fires, rescuing individuals) but also the indirect effects (eg disruption, media interest)".[5][6]

International Organization for Standardization (ISO), which is the world's largest developer of international standards also makes a point in the description of its risk management, principles and guidelines document ISO 31000:2009 that, "Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment".[7] This again shows the importance of not just good planning but the effective allocation of resources to treat the risk.

Computer security incident management

Today, an important role is played by a Computer Security Incident Response Team (CSIRT), due to the rise of internet crime, and is a common example of an incident faced by companies in developed nations all across the world. For example, if an organization discovers that an intruder has gained unauthorized access to a computer system, the CSIRT would analyze the situation, determine the breadth of the compromise, and take corrective action. Computer forensics is one task included in this process. Currently, over half of the world's hacking attempts on Trans National Corporations (TNCs) take place in North America (57%). 23% of attempts take place in Europe.[8] Having a well-rounded Computer Security Incident Response team is integral to providing a secure environment for any organization, and is becoming a critical part of the overall design of many modern networking teams.

Roles

Incidents within a structured organization are normally dealt with by either an incident response team (IRT), or an incident management team (IMT). These are often designated beforehand or during the event and are placed in control of the organization whilst the incident is dealt with, to restore normal functions.

Usually, as part of the wider management process in private organizations, incident management is followed by post-incident analysis where it is determined why the incident happened despite precautions and controls. This analysis is normally overseen by the leaders of the organization, with the view of preventing a repetition of the incident through precautionary measures and often changes in policy. This information is then used as feedback to further develop the security policy and/or its practical implementation. In the United States, the National Incident Management System, developed by the Department of Homeland Security, integrates effective practices in emergency management into a comprehensive national framework. This often results in a higher level of contingency planning, exercise and training, as well as an evaluation of the management of the incident.[9]

Root cause analysis

Human factors

During the root cause analysis, human factors should be assessed. James Reason conducted a study into the understanding of adverse effects of human factors.[10] The study found that major incident investigations, such as Piper Alpha and Kings Cross Underground Fire, made it clear that the causes of the accidents were distributed widely within and outside the organization. There are two types of events: active failure—an action that has immediate effects and has the likelihood to cause an accident—and latent or delayed action—events can take years to have an effect and are usually combined with triggering events that then cause the accident.

Latent failures are created as the result of decisions taken at the higher echelons of an organisation. Their damaging consequences may lie dormant for a long time, only becoming evident when they combine with local triggering factors (e.g., the spring tide, the loading difficulties at Zeebrugge harbour, etc.) to breach the system's defences. Decisions taken in the higher echelons of an organization can trigger the events towards an accident becoming more likely, the planning, scheduling, forecasting, designing, policymaking, etc., can have a slow

burning effect. The actual unsafe act that triggers an accident can be traced back through the organization and the subsequent failures can be exposed, showing the accumulation of latent failures within the system as a whole that led to the accident becoming more likely and ultimately happening. Better improvement action can be applied, and reduce the likelihood of the event happening again.[11]

See also

- National Incident Management System in the United States
- Coordinated Regional Incident Management (Netherlands) in the Netherlands

References

1. *UK, Small Business Service, Kingsgate House, 66-74 Victoria Street, London SW1E 6SW. "What qualifies as an 'incident'? | Business Link" (http://webarchive.nationalarchives.gov.uk/20110615004920/http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1084688800&r.l1=1073861197&r.l2=1075408323&r.l3=1084688133&r.s=sc&type=RESOURCES) . webarchive.nationalarchives.gov.uk. Archived from the original (http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1084688800&r.l1=1073861197&r.l2=1075408323&r.l3=1084688133&r.s=sc&type=RESOURCES) on 2011-06-15. Retrieved 2018-01-04.*
2. *Glossary of Terms, The Business Continuity Institute Good Practice Guidelines 2010 Global Edition (http://www.thebci.org/glossary.pdf) Archived (https://web.archive.org/web/20150430185226/http://www.thebci.org/glossary.pdf) 2015-04-30 at the Wayback Machine. thebci.org Retrieved on 2015-09-03.*
3. *"List of NFPA Codes and Standards" (http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600&cookie_test=1) . www.nfpa.org. 2013. Retrieved 10 April 2013.*
4. *"Incident Management | Ready.gov" (http://www.ready.gov/business/implementation/incident) . www.ready.gov. 2012. Retrieved 10 April 2013.*
5. *"National Recovery Guidance - GOV.UK" (https://www.gov.uk/national-recovery-guidance) . www.gov.uk. 2007. Retrieved 10 April 2013.*
6. *"Civil Contingencies Act 2004" (http://www.legislation.gov.uk/ukpga/2004/36/contents) . www.legislation.gov.uk. Expert Participation. 2012. Retrieved 10 April 2013.*
7. *"ISO 31000 Risk management" (http://www.iso.org/iso/home/standards/iso31000.htm) . www.iso.org. 2009. Retrieved 13 April 2013.*
8. *Hacking Incidents 2009 – Interesting Data – Roger's Security Blog – Site Home – TechNet Blogs (http://blogs.technet.com/b/rhalbheer/archive/2010/03/12/hacking-incidents-2009-interesting-data.aspx) . Blogs.technet.com (2010-03-12). Retrieved on 2012-11-17.*

9. *About the Contingency Planning and Incident Management Division | Homeland Security (https://www.dhs.gov/xabout/structure/gc_1230910518359.shtm) Archived (https://web.archive.org/web/20120402131642/https://www.dhs.gov/xabout/structure/gc_1230910518359.shtm) April 2, 2012, at the Wayback Machine. Dhs.gov (1999-02-22). Retrieved on 2012-11-17.*
10. *Reason J (June 1995). "Understanding adverse events: human factors" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1055294) . Quality in Health Care. **4** (2): 80–9. doi:10.1136/qshc.4.2.80 (https://doi.org/10.1136%2Fqshc.4.2.80) . PMC 1055294 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1055294) . PMID 10151618 (https://pubmed.ncbi.nlm.nih.gov/10151618) .*
11. *O'Callaghan, Katherine Mary, Incident Management: Human Factors and Minimising Mean Time to Restore (http://dlibrary.acu.edu.au/digitaltheses/public/adt-acuvp272.01032011/index.html) Archived (https://web.archive.org/web/20110917053506/http://dlibrary.acu.edu.au/digitaltheses/public/adt-acuvp272.01032011/index.html) 2011-09-17 at the Wayback Machine, Ph.D. Thesis, Australian Catholic University, 2010.*

External links

- National Incident Management System Consortium (http://nimsc.org/) in the United States
- United Kingdom Government legislation, Civil Contingencies Act (CCA) 2004 (http://www.legislation.gov.uk/ukpga/2004/36/contents) . (2012)
- Federal Emergency Management Agency (FEMA) (http://www.ready.gov/business/implementation/incident) . (2012)

Further reading

- Adam Krug (2014-09/16), "Incident Management Software System Case Studies (https://web.archive.org/web/20140910200104/http://cmo-software.com/resources/case-studies/) ", Case Studies 1 – 34
- Wearne S H & White-Hunt, K (2010), Managing the Urgent and Unexpected, Gower Publishing – Case studies

Last edited 2 months ago **by** Astute geek