Our top ten list of business continuity/disaster recovery trends for 2014

Mike Prewett IEng, FIET, MBCS | Camtek CSI, London, England.

Many businesses, particularly small to medium sized enterprises, do not have a business continuity plan (BCP) in place. It may be that they think they do not need one, that it is an unnecessary expense to develop one, or that they do not know what one is.

Disasters, particularly climate related ones, are becoming more and more frequent which make business continuity management more and more important to consider. The following list highlights an industry view of what the top ten issues are likely to be in 2014.

"The only thing harder than planning for an emergency is explaining why you didn't". anon.

10

Increase in natural disasters worldwide

Since the 1970's natural disasters have increased, including climate-related ones such as floods, storm surge, and coastal flooding. For example, in the UK the Thames barrier was closed 29 times between December 2013 and February 2014, to protect London from the most stormiest and wettest period for a century.

This means that you should review your BCP relating to flooding if your building is in a low lying area or has a basement containing strategic utility systems. Be aware also, that staff may have difficulty getting to work, and therefore may require to work from home requiring access to paper-based records to avoid reliance on broadband networks which may be disrupted.

If you are served by a telephone exchange situated in a low lying area or next to a river it may be subject to flooding and cause outages in telephony and broadband, such as what hit the BT telephone exchange in Guildford in March 2014. You should have access to alternative telecoms and broadband, for example mobile phones, or combined 3G/DSL router for broadband communications and VoIP telephony channels.

09

Malicious cyber-attacks and malware are on the increase

Over the last year, apart from the normal proliferation of computer malware, there has been a steady growth in that affecting mobile phones and tablets, including those which use Android operating systems. According to virus experts McAfee, mobile malware increased by 33 per cent during 2013-4.

Not only do you need to protect your personal computers and servers by maintaining program patches and anti-virus definitions, but you should also be aware that custom viruses can attack automated industrial machinery, such as what happened with the Stuxnet virus in June 2010.

On 8 April 2013, Microsoft stopped producing security patches for Windows XP and Office 2003, which means that these systems are now more prone to attack than ever. Businesses therefore should ensure that they adopt up-to-date software where necessary.

All unprotected networks and computers are susceptible to viruses and malware which may allow access to: cyber criminals wanting to make money through fraud, industrial competitors and foreign intelligence services interested in gaining a competitive advantage; and hackers with a political message to make.

08

Technology and weather disruptions

Companies continue to rely on massive amounts of technology, computers, servers, mobiles, tablets, fibre and mobile broadband. These can become increasing vulnerable to geomagnetic storms and solar flares, particularly systems that rely on global positioning satellites. You should be looking at back-up systems and uninterruptable power supplies and ensure that staff are trained in disaster recovery. And, remember data needs to be backed-up regularly and stored in more than one location, one being off-site.

07

Plan for disruption, don't think it will not happen

Interruptions to business caused by weather, man-made or technical glitches should be considered a normal occurrence, not a one off. The Thames Barrier was closed 29 times between December 2013 and February 2014 – compared to 35 closures during the whole of the 1990's. Early 2014 saw flooding in Guildford, Staines, Egham and other parts of the South East. BTOpenreach, who maintain the telecoms network, declared a 'Matters Beyond Our Reasonable Control' (MBORC) across several regions including several towns in Surrey.

06

Over reliance on cloud-based services and storage

More and more services are using cloud-based technologies utilising powerful server-based software which enables users to work from multiple locations without the need for it to be resident on a local computer. It is important to note that all of these services rely on a resilient network and broadband connection, which can fail during many conditions, particularly during bad weather. It is therefore important to consider backing up your data and disk images locally as well as remotely. It should also be realised that data held on servers outside your local jurisdiction may not be legally protected to the same degree that it may be in the EU, and that it may be open to cyber-attack and your intellectual property or commercial secrets may be compromised. Care needs to be taken on how you store and protect your commercially sensitive data including intellectual property and financial information.

According to the EU's cyber security strategy, it is expected that threats will become more innovative and sophisticated, particularly with the increased use of cloud computing and bring-your-own-device schemes.

The British Computer Society report that only 17 per cent of UK business leaders consider cyber security a major priority compared with 41 per cent of business leaders in the United States, and that only 58 per cent of IT executives globally thought that their boards underestimated the importance of cyber security.

05

Business continuity is here to stay

Companies now realise that it is well worth carrying out a risk assessment and prepare a business continuity plan rather than having to deal with the consequences of a real incident, which can affect not only the company finances but also its reputation, stakeholder confidence.

In March 2013 the Chartered Management Institute produced a report called *Weathering the storm*, which reported that severe weather conditions remain the leading cause of disruption to businesses across the UK for a fourth consecutive year. And, managers in organisations affected by snow in early 2013 reported an average financial cost to their business of as much as £52,770.

04

Broadband and communications

Fibre broadband products are becoming increasingly available and customers want the fastest speed possible even though it might not be strictly necessary. However, it is resilience in the networks and quality of service that are the important things to consider, and for these reasons backup services should also be considered.

03

Social media, love it or hate it

Today companies use social media, such as Facebook and Twitter, simply because everyone else uses it and it is another form of communication. Twitter feeds can send out a carefully crafted messages for staff, stakeholders, customers and suppliers, which is easy and spontaneous but companies need to understand how to use it. These 'calls to action' are more likely to gain the attention of younger employees rather than traditional methods such as email.

02

Don't use the email 'send' button without prior thought

Pressing the send button, unless you use something like Microsoft exchange, means that you will be unable to recall the message once sent. Take care that the message goes to the right recipient, and do not use long cc. lists which can be harvested by 'mail bots', always send to yourself and use the bcc. field for the distribution list. Careless emails have proved embarrassing in the past and even resulted in the resignation of key employees and public figures.

01

The Terminator and Skynet!

It might be something from science fiction and the Terminator films, but having intelligent buildings and domestic homes using smart metering, remotely controlled central heating and even ways to turn televisions on from mobile phones, doesn't make them impervious to the determined hacker . An interesting point to note is that recently a study carried out by a company called *Proofpoint* found that even intelligent home refrigerators, connected to the internet, can send out spam.

Remember to store critical information in paper form as well as electronic and on local devices as well as in the cloud (if you use cloud technology). Keep all your business continuity plans in paper form with key responders having a copy kept at home. These plans should include all the contact details, telephone numbers, mobiles and email addresses. You may need to contact people when your regular network is down, so be prepared for that.

The machines are not in control at the moment but it is really time to consider your cyber security and get advice when necessary.

Camtek CSI assist firms in business issues relating to cyber-security, business continuity/disaster recovery and digital forensics. We can carry out a risk assessment of your company to identify any potential threats which may impact on your ability to successfully operate during a period of crisis, and develop a business continuity plan for you.

Camtek CSI operates mainly in London and the South East, but also takes referrals from the UK nationwide and Europe.

For more information please visit our website at www.camtekcsi.com, or email us at: enquiries@camtekcsi.com .

Further reading:

Daily mail reporter (2014), *'It could be even worse! Thames Barrier has been closed 29 times in the past 10 weeks to protect London – a fifth of its total use since being built in 1983'*, Mail Online, London. Available online at: http://www.dailymail.co.uk/news/article-2557879/It-worse-Thames-Barrier-closed-29-times-past-10-weeks-protect-London-fifth-total-use-built-1983.html (Accessed 15 July 2014).

Jackson, M. (2014), *'UK storm damage gives BTOpenreach engineers a busy start to 2014'*, ISP Review, UK. Available online at: http://www.ispreview.co.uk/index.php/2014/01/uk-storm-damage-gives-bt-openreach-engineers-busy-start-2014.html (Accessed 15 July 2014).

Schneier, B. (2010), *'The story behind the Stuxnet virus'*, Forbes magazine, New York. Available online at: http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html (Accessed 22 July 2014).

Palm, C (2014), *'McAfee labs report sees mobile malware abuse trust in early 2014'*, McAfee, Santa Clara. Available online at: http://www.mcafee.com/us/about/news/2014/q2/20140624-01.aspx (Accessed 15 July 2014).

Musgrave, B and Woodman, P (2013), *'Weathering the storm – The 2013 business continuity management survey'*, Chartered Management Institute, London.

BBC (2014), *'Fridge sends out spam emails as attack hits smart gadgets'*, BBC News Technology online available at http:// bbc.co.uk/news/technology-25780908 (Accessed 31 July 2014).