Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers?

Danny Vande Putte* and Marc Verhelst**

Received (in revised form): 28th October, 2013

National Bank of Belgium, De Berlaimontlaan 14, 1000 Brussels, Belgium
*Tel: +32 2 221 4629; Fax: +32 2 221 3131; E-mail: danny.vandeputte@nbb.be
** Tel: +32 2 221 3419; Fax: +32 2 221 3131; E-mail: marc.verhelst@nbb.be

Danny Vande Putte

Marc Verhelst

Danny Vande Putte *is a civil engineer in electro mechanics. Since 2006, he has been responsible for business continuity management (BCM) at the national Bank of Belgium. Since 2011, he has also been responsible for the operational issues of the Belgian financial sector. He has been a member of the European System of Central Banks BCM task force since 2008 and in 2012 took over as its chairman.*

Marc Verhelst *is a commercial engineer who graduated in finance and management. Since 2006, he has become a key actor in operational crisis management for the Belgian financial sector. He is also a member of the European System of Central Banks BCM Task Force.*

ABSTRACT

Risk management has never been easy. Finding efficient mitigating measures is not always straightforward. Finding measures for cyber crime, however, is a really huge challenge because cyber threats are changing all the time. As the sophistication of these threats is growing, their impact increases. Moreover, society and its economy have become increasingly dependent on information and communication technologies. Standard risk analysis methodologies will help to score the cyber risk and to place it in the risk tolerance matrix. This will allow business continuity managers to figure out if there is still a gap with the maximum tolerable outage for time-critical business processes and if extra business continuity measures are necessary to fill the gap.

Keywords: cyber risk, cyber threat, cyber crime, risk analysis, risk taxonomy, business continuity management

Journal of Business Continuity & Emergency Planning
Vol. 7 No. 2, pp. 126–137
© Henry Stewart Publications, 1749–9216

INTRODUCTION

Risk management has never been easy. Identifying measures to mitigate risks is one thing, but finding efficient mitigating measures that can be justified with cost-benefit analysis is much more complicated. Cyber crime and cyber threat, however, represent a really huge challenge for management and IT security experts because the criminals' techniques and threats are changing all the time. As the sophistication of cyber crime increases, so too does its potentical impact on business. This means that cyber crime is also a huge concern for business continuity managers.

Cyber crime is an increasingly common way of stealing, threatening and blackmailing organisations all over the world. It is affecting the integrity, the confidentiality and/or the availability of the IT environment of organisations. General risk analy-

sis methodologies can be used to make a complete cyber risk cartography. This cartography is vital for business continuity managers to judge whether current cyber risk mitigation measures are compliant with the risk tolerance of the organisation.[1]

Cyber crime affects the confidence that customers, professionals and government demonstrate towards the organisation. This means that although the organisation's corporate and financial objectives are not the direct target they are nonetheless at significant risk. There is even a potential risk of the organisation going bankrupt.

Many preventive measures can be taken to tackle the root causes of cyber crime. But business continuity managers are particularly interested in knowing what measures can be taken to limit the loss of IT systems, documents and data in the case of a cyber incident.

Society and its economy have become increasingly dependent on information and communication technologies (ICT). This dependence has grown even further because many critical and crucial business processes are provided through solutions using IT systems and web connections. Managing these business processes often means managing huge databases with crucial and confidential data and having access to a lot of crucial and confidential documents.

In addition, many industrial processes are also controlled, monitored and managed by ICT. Complex systems, equipment and technologies, indispensable for the management of industrial processes, are linked up and are able to communicate, coordinate, cooperate and take action without the need for human intervention. These machine-to-machine applications are also common in critical infrastructure sectors. The availability and effectiveness of complex IT systems has become crucial for the operation of critical infrastructures such as energy, water, transport, finance and the health sector.

Clearly, if these sectors' ICT infrastructures are damaged or unavailable, intentionally or not, it can have significant consequences for individuals, organisations, the economy and society as a whole. As a result, a safe internet that is available 24 hours per day and seven days per week is essential.

Even if business managers have developed contingency measures that do not use ICT systems, these measures will only be able to guarantee the service that customers and stakeholders are expecting for a very short time. Often, business continuity plans, which are necessary to effect after the disaster has occurred, will depend on ICT tools.

In other words, cyber risk cannot be ignored by business continuity managers. This paper will try to demonstrate that, whatever the originality of cyber threats and cyber crime, a general risk approach (such as that of ISACA[2] or the Information Security Forum[3]), based on a general risk taxonomy, general impact and likelihood scoring tables is very helpful for business continuity managers to deal with today's cyber risks. This paper is based on the authors' knowledge and experience with operational risk management and business continuity management (BCM) acquired during their daily responsibilities at the National Bank of Belgium. In respect of the confidentiality rules of the bank, precise details about the cyber risk analysis of the bank cannot be given in this paper.

CYBER CRIME IS EFFECTIVE: SOME EXAMPLES

In the last ten years, cyber crime has become an increasingly common way of stealing, threatening and blackmailing organisations the world over. The following are some examples:

- A significant number of PCs, essentially private consumers' computers, have been frozen by ransom-ware viruses, demanding money in order to unlock the computers.
- Companies are also victims of this kind of cyber blackmailing. For example, one banking institution has been affected by cyber crime and the criminals claimed a financial ransom from the bank in order not to make public the clients' data they had stolen.
- Over the five last years, there have been several waves of online banking attacks. Recent attacks have been based on Trojan horses, botnets, (phishing websites and social engineering. Botnets (affected networks or groups of infected computers[4]) constitute the infrastructure used by cyber terrorists for such illegal activities as distributing spam, company and customer spying, execution of fraudulent transactions, server sabotage and systems interruption or destruction through distributed denial of service (DDoS) attacks.
- Nowadays, it is not difficult to become a cyber criminal. Even people operating on their own can do it. The knowledge and tools needed for cyber attacks are easy to find on the web. With limited tools, the internet allows spying, sabotage, subversion, terrorism, propaganda and military cyber operations. Current technology even allows criminals to hide their identity so that supervision and control by the authorities becomes difficult or impossible.
- New threats are now rising, such as mass hacktivism for political and ideological reasons aimed at published confidential information. Hacktivism capitalises on social media and networking and is extremely fast, leaving little time for response. In general, cyber hacktivist groups do not have a formal structure; they can, however, benefit from an umbrella brand name such as Anonymous. For example, in early 2012, a world steel group became the most noteworthy victim of a group ostensibly affiliated to this hacker network. Since then, many other hacktivists have used the same techniques.
- Other recent developments include cyber spying for economic and political reasons. The spies try to steal strategies, patents, data stocks in big companies (oil and energy companies, financial institutions, etc) as well as in various centralised departments in every country. In general, this spying goes undetected for months or years and it is not known precisely what information has been stolen.
- One last cyber crime development is the destabilising or immobilising of critical and essential infrastructures. Specific malwares allow systems and data to be managed from outside or enable some industrial facilities to be sabotaged. This type of cyber warfare can be targeted at national authorities. For example, in 2012, the Sality.gen computer virus affected the central administration and the control offices of a public service. The origin of this attack still remains unclear. A second example is in April 2009, when hackers managed to enter the US electricity network with the power to influence the national network. In May 2012, the super spy virus Flame was discovered. Flame had infected more than 1,000 computers in the Middle East, with victims including governmental organisations, educational institutions and private individuals and was able to steal passwords and take possession of microphones and Skype conversations.

On 21st December, 2012 the European Council of Ministers approved the idea of developing a national cyber strategy.[5]

National computer emergency response teams (CERTs) and a European CERT were set up to this end. The European Cyber Security Directive[6] requires all companies managing critical networks (energy, banks, health) to report every IT cyber incident that has affected their normal functioning. This is certainly not the end of the story; for example, in February, 2013, the European Commission tabled a proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the EU.[7] One of the main conclusions of the international conference organised by the European Union Agency for Network and Information Security in September 2013 was that there is a strong call for better cooperation within and between public and private sectors as the challenges faced are strikingly similar.

CYBER RISK ANALYSIS IN THE GENERAL RISK APPROACH

Cyber crime is appearing under the guise of many different kinds of incidents:

- with a wide variety of consequences and impacts affecting the integrity, confidentiality and/or availability of IT systems, documents and data;
- with a wide variety of targets from private people to private and public organisations.

Instead of developing specific risk analysis models and taxonomies for cyber risks, however, it is worth trying to use the general risk model accepted for the whole organisation and all business processes. This is the only mode of operation guaranteeing an efficient and coherent risk analysis for cyber risks and ensuring that the correct risk procedure will be followed when the management has to decide which risk mitigation measures to implement in the cyber threat and crime domain.

A very common risk model is shown in Figure 1. The figure shows the three main risk domains: confidentiality, integrity and availability (also known as the CIA Triad).[8] If these are related to the three domains of information security, the definitions can be narrowed as follows:

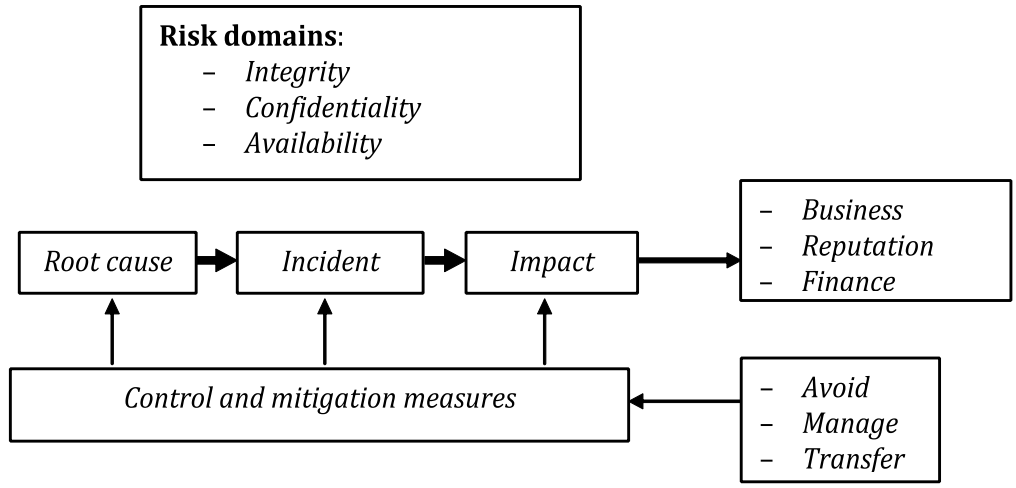
(1) *Confidentiality* is the assurance of documents and data privacy. Only the intended and authorised recipients may read the documents and data. Disclosure to unauthorised entities, for example, using unauthorised network sniffing, is a confidentiality violation.
(2) *Integrity* is the assurance of non-alteration of documents or data. Document and data integrity is ensuring that the information has not been altered during transmission, from origin to recipient, and during storage.
(3) *Availability* is being sure of the timely and reliable access to documents and data services for authorised users. It ensures that information or resources are available when required.

If one tries to analyse an incident, one can look both upstream and downstream:

- Looking upstream means trying to find out what the possible root causes may be or, after the incident has occurred, what the root causes were, which may be easier.
- Looking downstream means trying to see what impact can be expected during and after the incident.

Keeping in mind this relationship between root causes, the underlying reasons why a risk event occurs, the incident itself and the possible impact of the incident on the

Figure 1:
Common risk model



organisation are fundamental to the success of the risk analysis.

RISK TAXONOMY

People often imagine a great number of root causes for incidents. Perhaps, during their risk analysis, line managers will be too inventive, resulting in a chaotic list of possible root causes. Brainstorming sessions are a good forum for risk analysis, but to help business managers analyse the root causes of an incident in a structured way, it is practical to classify root causes in the form of a risk taxonomy.[9] This classification also helps to avoid some root causes getting insufficient attention or even being forgotten. The following are examples of typical classifications:

- *Staff:* Are they well qualified, sufficient in number, correctly managed, motivated, applying the ethics and policies of the organisation, permanent or temporary staff?
- *Governance of the organisation:* Is its strategy risk averse or risk-taking? What is the willingness to be legally compliant?
- *The kind of business processes with which the organisation is involved:* Does the organisation have to deal with operational processes, with project management or support services like facilities, security, etc?
- *The use of and dependence on IT systems and other infrastructures:* Considerations include buildings, offices, specific technical installations, etc.
- *External events:* For example, human (cyber) threats and natural catastrophes.

It is clear that all these aspects have to be taken into account when thinking about the root causes for cyber crime incidents.

Listing the kind of incidents that can happen is often an easier way of starting a risk analysis. During a brainstorming session, asking the question 'what kind of incidents can happen in your business entity?' will result in a plethora of incidents. But it can also be very helpful for business managers to use the organisation's taxonomy and to carry out the analysis according to a classification of incidents. Examples of a typical classification comprise human error, human failure, occupational incidents, infrastructure disruptions, fraud, disasters and attacks.

In cyber crime, most incidents can be classified as human failure in the application of security measures, infrastructure disruptions caused by the cyber criminal, internal fraud that helps cyber criminals to prepare their attacks and massive attacks from the outside, all simply aimed to hurt the organisation.

The impact of an incident can be classified into three different dimensions: achieving (or not achieving) business objectives, reputational damage and the financial situation of the organisation. To estimate the financial impact of an incident, both the direct and indirect impact must be considered. Stealing money from a bank by either a 'classic' robbery or via cyber crime will have a direct impact on the financial situation of the bank. An incident damaging the reputation of a company, eg a very controversial declaration by the CEO, will have no direct financial impact, but it can be the reason why customers lose their confidence in the company with a huge impact on sales, which will surely have a negative influence on the company's financial results.

These three impact dimensions are definitely applicable in for-profit companies. But non-profit organisations and public organisations cannot make abstract risk analysis. The documents and data they receive, transmit and store often contain confidential information and they have to guarantee this confidentiality. Facing a confidentiality breach would probably mean them losing their reputation, being stigmatised and criticised by the public or their 'clients'. In these circumstances, a possible consequence is for the whole board to be fired. Non-profit organisations and public administrations, whatever their non-profit objectives, have to accomplish their mission and deliver their goods and services to the public and professionals on time. As such, they must also analyse the need for business continuity plans in case of cyber attacks.

THE DIFFERENCE LIES IN THE TAIL

Business continuity professionals know that with threats such as natural disasters, terrorist attacks with classic explosives, mass disease epidemics and huge fires and explosions, their stakeholders will not necessarily blame them if they see that the business continuity measures guarantee only a minimum service. Cyber crime, however, seems to produce a different reaction from stakeholders, and blame might well be laid at the door of the business continuity professionals even if the only result of a cyber attack is a temporarily reduced service level.

Theft of data, information or electronic money will directly affect the financial situation of the organisation. This can be organised by cyber terrorists through social engineering (false web friends, for example), through malware on customers' computers, phishing or identity theft. Phishing can take the form of e-mails requesting personal information or even phone calls asking for personal data. In essence, the organisation has done nothing wrong, but when it is known by the public that customers' money has been stolen via the organisation's ICT infrastructure, it can result in the public and media blaming the organisation for carelessness. This, in turn, can damage its reputation in such a way that other customers also lose their confidence in the organisation, with a subsequent impact on its business and financial objectives.

A confidentiality breach will certainly affect the organisation's reputation first and this could result in a loss of confidence among its clients, public or professionals, who might stop doing business, with a predictable impact on the organisation's financial situation.

When a cyber terrorist successfully breaks into internal IT systems, they can

Table 1: Impact and likelihood scoring table

	Score if			*Likelihood*
Score	*Level of availability of the business*	*Reputation affected for*	*Financial loss (€m)*	*Score if incident occurs*
5	Service no longer available	>3 years	>10m	Every year
4	Only partial service available	1–3 years	1–10m	Every 1–2 years
3	Service available but quality not guaranteed	3 months–1 year	100,000–1m	Every 2–5 years
2	Service delivery could be affected	1 week–3 months	10,000–100,000	Every 5–10 years
1	Service quality could be affected	<1 week	<10,000	Max every 10 years

surely cause system, application or data storage unavailability. But even worse, the cyber terrorist can paralyse the IT environment from outside, even without entering it, by using the technique of a DDoS attack. Even if the public or the media cannot blame the organisation for being the victim of such an attack, the attack may still have a lasting impact on business objectives and income, as well as damaging its reputation over a longer period.

IMPACT SCORING TABLES

Other important elements of the risk taxonomy are the impact and likelihood scoring tables. The scoring tables usually comprise five levels (see column 1 of Table 1). Some organisations prefer more levels for a more granular score. This can be useful if the line management can rely on adequate information during the risk analysis to make the right distinction between the different levels. Three levels seems to be easy but is probably inadequate for making a good selection between the 'must have' and 'nice to have' mitigation measures.

A scoring table for business objectives will depend on the kind of business in which the organisation or company is involved. For a central bank, score 5 will be given for a total failure in delivering statutory tasks, such as regulating the liquidity of the financial markets. Score 1 is given when only internal expectations are not achieved.

Creating a scoring table for reputation damage is certainly achievable, but scoring the reputation damage depending on the kind of possible incident will be a very difficult job. As reputation damage is, in principle, highly intangible, there could be a very big difference in scoring intentions between the board, line managers and risk managers. Nevertheless, the organisation must also still have a taxonomy for this impact. For instance, level 1 means that the credibility of the organisation is affected for only a short time, perhaps just a few days, and level 5 means that the credibility is affected for years.

A financial impact scoring table is rather simple: level 1 is worth a certain amount of money; level 2 is, for example, worth ten times more; and so on, up to level 5.

THE LIKELIHOOD OF AN INCIDENT

The final taxonomy to define in this general risk model is the scoring table for the likelihood of an incident happening. For

some incidents, such as natural disasters, historical data can be found to estimate the realistic likelihood of a disaster occurring. For some incidents, such as terrorist attacks, historical data might not exist in the organisation because it has never been the victim of that kind of attack.

Conversely, for cyber crime, it is likely that incidents have happened and the threat is constantly growing. But these observations do not help to correctly score the likelihood of a cyber incident and to determine which extra mitigation measures are worth implementing and which are not.

A solution to the lack of historical data for scoring or estimating the likelihood of the threat is by taking a 'qualitative approach'. The following facets can be taken into consideration for a qualitative approach to cyber crime: what skills are needed? (sometimes very few because the tools are available on the internet); is collaboration needed? (eg with internal staff); are the actions easy to trace to the origin? (some tools can wipe out traces); how much time is needed to commit the crime? (cyber criminals have time, their servers are probably up and running permanently); must the cyber criminal invest a lot of money? (a PC is enough to develop and initiate some attacks).

A quick reflection on these qualitative aspects (see the expressions between parentheses) leads to the conclusion that the likelihood of cyber crime success will range between several times a year for organisations that are not well protected and two to five years for organisations using state-of-the-art protection measures.

MAKING THE LINK BETWEEN THE CYBER RISK ANALYSIS AND THE BCM SYSTEM

In general, an organisation can try to avoid, mitigate or transfer risks. Avoiding the risk by not doing business or not using the IT infrastructure at risk is surely no valid measure for mitigating cyber crime. The same goes for trying to transfer the risks to a third party. As such, an organisation must undertake a large number of measures to mitigate cyber risks — some to limit the likelihood, others to limit the impact.

As Figure 1 shows, risk control and mitigation measures can be developed for each step of a risk event.

For example, the root causes of many cyber risks linked to employees and affecting the integrity of stored data can be mitigated by ensuring that all employees are aware of cyber threats[10] and know how to apply the security guidelines consciously.

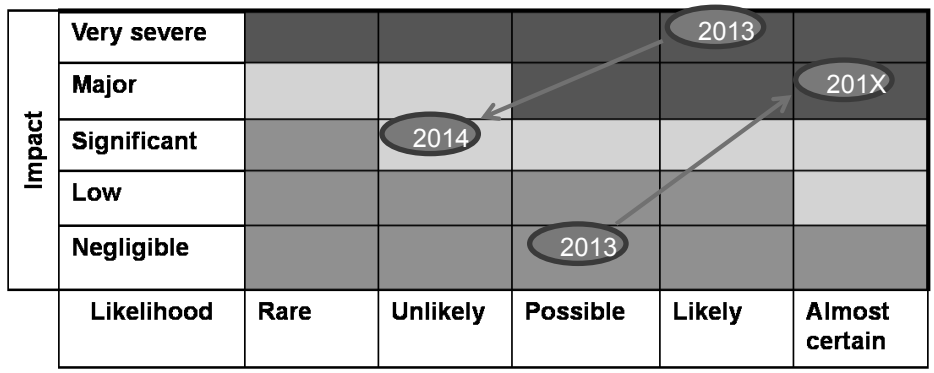
The likelihood of an incident occurring can be lowered by installing and maintaining powerful firewalls or by encrypting confidential data during transmission and storage.

The impact of penetration by a hacker can be limited by segregating the internal networks so that penetration on one part of the network does not necessarily affect another. The affected network segment should easily be isolated from the rest of the system in order to carry out the necessary investigations and cleaning operations. This also resolves business continuity matters because it prevents the complete cessation of business activities as a result of shutting down the entire network.

The result of the cyber risk analysis will place the cyber risks and threats on the risk tolerance matrix, as shown in Figure 2. If the explained methodology is followed, the place in the risk tolerance matrix takes into account all the existing measures. The risk tolerance policy of the organisation can, for example, say that red residual risks have to be accepted by the executive board, yellow by the head of division and green can be the responsibility of the line manager.

For a cyber risk situated in the red

Figure 2: Risk tolerance matrix



zone, it could be that the board cannot accept this residual risk and decides to implement extra mitigation measures suggested by the IT experts in an attempt to lower the residual risk. Lowering the residual risk can mean lowering the possible impact or the likelihood, or lowering both. On the other hand, as cyber crime is evolving all the time, it could be that a cyber risk mitigated by a number of measures shifts from a green zone (acceptable) to a yellow or even red zone and that new action plans for new measures will be needed.

Taking into account the possible success rate of cyber criminals, it is certainly too optimistic to hope that all the residual cyber risks will be situated in the green zone. It is evident that, without business continuity plans, a number of residual cyber risks will be situated in the red zone because of the impact that the cyber attack can have on the availability of the time-critical business processes. In other words, business continuity plans will be necessary to limit the impact of cyber incidents to an acceptable level.

One of the cornerstones of the BCM system is the list of maximum tolerable outages (MTOs) of the time-critical processes. This paper will not elaborate further on how these MTOs can be established as many possible methodologies are described in BCM best practices (eg those of the Business Continuity Institute). Most of the time they are determined via an inherent risk analysis of the unavailability of the business process.

For critical actors of the financial system (banks, payment systems and settlement systems) a lot of business processes will be considered as very time-critical with short MTOs. MTOs of two and four hours are not unusual.

The next step is to link the MTOs of the business processes to the recovery time objectives (RTOs) of the critical resources that are needed for the execution of these business processes. One of the critical resources necessary for almost every business process will be IT systems, IT tools, applications and databases.

The standard business continuity measures needed to recover the above-mentioned IT components within a short time comprise implementing high-availability protocols that can rely on two similar systems each capable of delivering 100 per cent of the output without any single point of failure, network architectures and system hardware ensuring system reliability and robustness. Business continuity managers are not necessarily IT experts, but if they try to understand the

capabilities of these standard business continuity measures implemented by IT colleagues, they will very quickly understand that, because of the nature of cyber threats and cyber crime, these measures will not guarantee that the organisation will be able to recover, faster than the desired RTO, the IT environment for the time-critical processes.

To reflect further on possible business continuity plans for cyber threats, incidents and attacks, examples are given of three types of cyber crime affecting the availability of the business processes:

(1) A cyber attack blocking access from and to the internet cloud, typically DDoS attacks. All the internal IT systems, tools, applications and databases are in working order, but the employees cannot communicate with the outside world and clients cannot contact the organisation.
(2) A cyber attack where the cyber criminal succeeds in penetrating the IT systems and is able to erase and destroy important parts of the operating system, tools, applications and databases.
(3) A cyber attack where the cyber criminal succeeds in penetrating the IT systems without the intention to erase or destroy but to steal or alter information in documents or databases.

BUSINESS CONTINUITY PLANS TO TACKLE THESE CYBER-ATTACKS

Often, business continuity plans foresee what can be called temporary contingency measures by using 'old-fashioned' manual procedures on paper. But it is well known that these manual procedures, sometimes started in a time frame smaller than the RTO, will allow someone to do only the most essential tasks really necessary immediately after the disaster has occurred. Because of the very great dependency by organisations on IT systems, the IT environment has to be available very quickly in order to guarantee the minimum service an organisation wants to offer its stakeholders before the MTO is exceeded, even after a major incident has occurred.

There exist different IT tools to limit the impact of type 1 cyber attacks. These tools try to block, divert or wipe out criminal traffic trying to consume completely the bandwidth connecting the organisation's IT infrastructure with the internet. Another (old-fashioned) business continuity plan (BCP) for the most time-critical business processes is using private networks, like SWIFT in the financial sector. Applying different network technologies and trying to have at least one network technology independent from the internet can also be a great help.

For a type 2 cyber attack, the main BCP will be to have the backups of the operating systems, tools, applications and databases on tapes, CDs or other independent offline support media, which cannot be directly addressed by the cyber criminal. These backups must be in such a format that they allow start-up from scratch in a shorter time than the MTO of the most time-critical business processes.

With type 3 cyber attacks, it could be reasoned that, notwithstanding that integrity and confidentiality are important notions in the field of risk analysis and risk mitigation measures, business continuity plans are not needed for such cyber attacks because their availability is not affected. Knowing that it can take a long time to detect this kind of cyber crime, which therefore means that the cyber criminal has had a long time to deeply penetrate the IT environment, the IT security experts will probably suggest that the whole IT environment is isolated from any external access in order to analyse the degree of penetration and infection. To

make it even more complicated, they will probably not guarantee the time needed for the disinfection, which could take hours, days or even weeks, as a result of the complexity of the cyber crime.

As mentioned earlier, network segregation can help as, first, it makes it more difficult for the cyber criminal to penetrate the whole IT environment. Secondly, the isolation, enabling analysis and cleansing, can be organised in layers and will not mean the unavailability of all the business processes at the same time.

Another option to consider is reopening the connections to the internet for the most time-critical business processes during the time that the IT experts are not fully convinced that all the cyber attack traces are cleaned. This means that one cannot exclude the possibility that, for example, the malware will restart its operation and reinfect the IT environment. Only very intensive monitoring of the IT environment and very specialised support of IT security experts will convince the board to take a decision that holds that kind of uncertainty.

CONCLUSION

Society, in general, and its economic processes, in particular, has become more and more dependent on ICT. Many complex business processes are linked together and many emergency solutions also use the same IT tools.

This implies that there is an increasing importance given to incidents that could affect these IT systems. Cyber threats and cyber crime are important root causes. Cyber risk is not a matter for tomorrow — cyber crime is already effective. Recent examples in the field of cyber blackmailing, Trojan horses or botnet attacks, phishing cases or mass hacktivism, prove that the cyber war is taking place with both economic and political objectives.

Standard risk analysis methodologies will help to score the cyber risk and place it in the risk tolerance matrix accepted by the organisation. In the risk tolerance matrix, one can see the residual risk that takes into account all the measures that the IT experts have put in place to defend the organisation against cyber crime. With this information, business managers and business continuity managers, together with IT security experts, can decide if there is still a gap in the MTO for the time-critical business processes and whether the gap of unavailability is too important or unacceptable so that extra business continuity measures become necessary.

Current business continuity plans for major fires, flooding, explosions or IT recovery plans based on duplicated infrastructures are not adaptable and will not be efficient against cyber crime. Business continuity measures protecting the organisation against the most important effects of cyber crime must be as innovative and creative as the cyber attacks themselves. Most of the time, manual procedures can only help for a very short lapse of time. In a very short space of time (and by the next day, at the very latest) the IT environment, at least partially, must be available again.

On the other hand, a number of (old-fashioned?) solutions are conceivable, such as private networks, network segregation and full backups on tape or CD. Another strategy might be to continue to use the least important IT environment necessary for the most time-critical business processes, without having a 100 per cent guarantee that the cyber 'pollution' has been stopped and the IT environment has been completely cleaned, but with very intensive monitoring by IT tools and IT security experts.

NOTES AND REFERENCES

(1) Clarke, J. (2009) 'Resilience under attack: Techniques for continuing online

business in the face of security compromise', *Gotham Digital Science*, 27th February.
(2) Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.
(3) The Information Security Forum (ISF) is the world's leading independent authority on information security.
(4) Herath, H. M. P. S. and Wijayanayake, W. M. J. I. (2009) 'Computer misuse in the workplace', *Journal of Business Continuity & emergency Planning*, Vol. 3, No. 3, pp, 259–270.
(5) Delafortrie, S. and Springael C. (2012) 'Communication relative à la cyberstratégie belge', available at: http://presscenter.org/fr/pressrelease/20121221/communication-relative-a-la-cyberstrategie-belge (accessed 5th November, 2013).
(6) Cyber Security Strategy – securing cyberspace, .be, CMR aanvullende informatie van 18-12-2012
(7) European Commission (2013) 'Proposal for a Directive of the European Parliament and of the Council Concerning measures to Ensure a High Common Level of network and Information Security across the Union, 2013/0027 (COD)', European Commission, Brussels.
(8) Kellep, C. (2012) 'Confidentiality Integrity Availability (CIA) Triad', *Security Orb*, 28th June.
(9) Cebula, J. J. and Young, L. R. (2010) 'A Risk Taxonomy of Operational Cyber Security Risks', Software Engineering Institute, Pittsburgh, PA.
(10) Scully, T. (2011) 'The Cyber Threat, Trophy Information and the Fortress Mentality', STRATSEC.NET PTY LTD., Sydney.