MSC Forensic Accounting
Electronic Crime

Keeping Your Business Running
in the event of a criminal attack:
Prevention, Protection & Continuity measures

Paul Senior
Student ID: 14031395
8th May 2008 – Version 2

CONTENTS

1. Introduction

Over the past two decades, computer technology has seen enormous growth. Prior to this, business decisions were made that determined **if** the use of technology or PC's were required. Contrast this with today's high-tech world, where decisions are now influenced by the technology available.

Home computers were seen as a luxury item less than a ten years ago (Vacca, 2005, p21), but are now a major part in many people's lives. The rise of computer technology has obviously enhanced our lives in many ways, such as enabling improved productivity and efficiency at work, school, and home. Anyone with access to a computer and the Internet now has unparalleled opportunities.

The Internet is almost certainly one of the greatest business tools ever invented. Merchants, trading partners and online retail shoppers are presented with a greater selection of goods and along with the convenience of use and greater competition leading to lower prices, it has revolutionised how business is conducted today.

However, despite the Internet's many advantages and opportunities, it also raises some new risks for businesses – including that of electronic crime. A survey carried out by Get Safe Online (Carter, 2006), revealed that fear of Internet crime is now more prevalent than concerns about more conventional crimes such as burglary, mugging and car theft. This is quite an astonishing fact, given that these more conventional crimes appear to be more widespread.

In this paper I will review what organisations need to do to identify the risks to their business, and subsequently what they can do to protect themselves in preparation against such risks, looking at systems and tools available for this purpose.

I will then review the business continuity processes that organisations can employ, which will look at types of approaches used to ensure minimal business disruption in the event of an incident occurring. Finally, I will consider the next steps an organisation can take to ensure they are prepared, whilst covering the investigative tools available.

2. Cyber/Electronic Crime

2.1. What is Cyber/Electronic Crime?

Unfortunately, with the increase in computer skills and knowledge, it has led to an increase in people looking to take advantage of the vast array of information available to them and the opportunities this provides.

Sharon Lemon, the head of e-crime for the UK's Serious Organised Crime Agency (SOCA), is warning that cyber-crime is so widespread it features in nearly every criminal investigation, as reported by the continuity forum in March 2008.

So what exactly is cyber-crime or electronic crime (e-crime)? Vacca (2005, p154) views electronic crime as something which 'occurs when information technology is used to commit or conceal an offence', or any 'illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them'.

Volonino, Anzaldua and Godwin (2007, p6) use additional terms when talking of cyber-crime. These are *computer crime* and *high tech crime,* and most people including the courts and the legal profession use these terms interchangeably.

Throughout the world today, huge amounts of data is held in digital format with the majority of paper-based systems being phased out and replaced by either electronic systems or document management solutions. This leaves a frightening amount of personal data in digital format.

Before use of the Internet became so widespread, most attacks were carried out as pranks or vandalism, but now, the focus is on generating profit through means of extortion or fraud.

Computer crime along with computer supported criminal activities is booming business and many organised criminal gangs are getting in on the act. Criminals are increasingly targeting cyberspace as more and more people shop online and use Internet banking services.

2.2. Categories/Methods of Attacks

There are several categories of cyber-crime and the method of attacks used by criminals will be dependent on the reasons for the attack. According to Vacca (2005, p154), such attacks include:

- Sabotage of data or networks
- Theft of proprietary information
- System penetration from the outside
- Denial of Service (DoS)
- Unauthorised access by insiders
- Viruses

Of these, the most common criminal activities are:

Financial - crimes that disrupt a businesses' ability to function either by committing a DoS attack and restricting its operating abilities or by making financial demands on an organisation to 'prevent' an attack from happening.

Gambling sites are major targets for online criminals and regularly suffer DoS attacks. Paddypower.com reported an attack on its site, following an extortion demand, which led to it being offline for several hours in February 2004 as reported by The Register.

Piracy - the act of copying copyrighted material. Online theft is defined as any type of 'piracy' that involves the use of the Internet to market or distribute creative works protected by copyright. Software and movie piracy is huge business for online 'entrepreneurs'! As you can see from this, the driver behind piracy is also financial.

Hacking - the act of gaining unauthorised access to a computer system or network and in some cases making unauthorised use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed, and is seen as the most damaging method of attack.

Cyber-terrorism – As with conventional terrorism, `e-terrorism' is classified as such, if the result of hacking is to cause violence against persons or property, or at least cause enough harm to generate fear. This particular crime has increased significantly post September 11th 2001.

Volonino, Anzaldua and Godwin (2007, p6) believe there are two specific categories of offences involving computers, dependent on how the computer is used or attacked:

The Computer as an Instrument – When the computer is used to commit a crime. There are many types of crimes committed in this way and many are traditional crimes such as fraud, theft, forgery, and stalking. The use of a computer in this manner assists the crime taking place.

Cyber-crimes committed using the computer as an instrument usually tend to be profit motivated, financial frauds (Volonino, Anzaldua and Godwin, 2007, p64), and investigators of such crimes require not only knowledge of how the computer system is supposed to function but a further understanding of accounting and auditing practices – which is an investigative field known as forensic accounting.

Manning (2005, pV) believes that forensic accounting in its basic form, is classed as 'the science of gathering and presenting financial information in a form that will be accepted by a court of jurisprudence against perpetrators of economic crimes'.

Essentially, it is for a forensic accountant to dissect crucial financial information and provide it in a format that is easy to understand. For this method of investigation, there are software tools available to assist with computer interrogation. Packages such as the Forensic Toolkit (FTK) and EnCase, are invaluable for investigators.

The second category is when the computer is used as an agent for crime by being used as an 'instrument' to perform the offence(s):

The Computer as a Target – When a computer, or the data stored on it is the target of a crime. Such crimes include attacks on networks, which can cause them to crash or grind to a halt and include things such as Malware (worms, viruses, spyware etc), unauthorised access, and hacking.

The first reported incident of a destructive computer worm was in November 1988, when the *Morris worm* was unleashed on the Internet by Robert Tappan Morris Junior. Volonino, Anzaldua and Godwin, (2007, p4-5) report that this worm infected over 10% of servers on the Internet. The outbreak caused estimated damages of between $10 million and $100 million at the time.

There are still many instances of large-scale viruses and worms being released and in recent years there have been major outbreaks such as the *ILOVEYOU* virus, released in 2000 (BBC news, 2000). This was reported to have affected 10% of the population and caused approximately $5.5bn worth of damage in recovery costs – contrast that to the cost of the Morris worm only 12 years previously!

2.3. Drivers of E-Crime

As I've highlighted, the cost of e-crime is rising. Lemon (2008) states cyber-crime is recognised as a major problem for many organisations, especially in the financial services sector, and cost the UK £2.4bn in 2004 the last time the impact was measured. This is a truly astonishing figure, and potentially, this will continue to rise.

According to Volonino, Anzaldua and Godwin, (2007, p7) when computer crime involves money, it is referred to as electronic fraud, and its growth is continuing at an alarming rate.

In a recent US industry survey Vacca (2005, pxxv) reports that 94% of respondents detected cyber attacks on their business. This resulted in a staggering 617 organisations reporting over $600 billion in financial losses – and these are just the reported cases.

Statistics show that the value of computer crime compared to that of physical crime is vastly different. Vacca (2005, p5) details an FBI survey carried out in 2003 which reported the average bank robbery netted the perpetrator $6900, whereas the average computer crime netted a staggering $900,000! These figures are frightening, and you can see why criminals are targeting this area.

The intention of a criminal attack is regularly focussed on the interruption of service, and in today's business world, where e-business is a main driver, many organisations cannot afford to be out of service for any period of time. This is why organisations need to prepare themselves.

3. Preparing the Organisation

Whilst an organisation may not think it will be a target for attack, it should take precautionary steps to ensure it doesn't fall foul of the criminals (Brown, 2006, p9). For such organisations, it is paramount to keep their business running with the least impact to the services that they provide.

Companies therefore need to think about what to do to both protect themselves in the event of an attack or a disaster, and what action or steps they need to take to recover from such an attack if the perpetrators are successful in their attempts. Various methodologies are available to assist with this planning.

3.1. Risk Management

According to Barnes (2001, p57), there are a number of important considerations that an organisation has to make when assessing the dangers to its business, and these fall under the banner of 'Risk Management'.

In risk management, organisations can determine the importance of critical systems and the impact the loss of such systems will cause. This is achieved by carrying out a Business Impact Analysis (BIA). This requires input from key business areas who will firstly determine the importance of a system or application, and will then identify the potential impact of its loss.

This is a critical part of planning for business continuity, and Elliott, Swartz and Herbane (2002) state that Meredith believes this leads to the formation of the 'backbone of the entire business continuity exercise'. This is true – as you need to understand your businesses needs before you can plan for business continuity.

A further key area to focus on is that of risk assessments which aims to identify gaps and/or weaknesses in the system(s). An organisation must determine the potential risks to the business whilst identifying mitigations of those risks.

Barnes proposes a number of key objectives when carrying out a risk assessment. These include quantifying the potential business impacts following a disruption, reviewing the disaster recovery strategies and recovery timelines and identifying procedural change if and where necessary.

These objectives are relevant to most organisations and it is important to review the impact specific risks will have on business operations. What the risk process can also help with is identifying areas for improvement be they processes, procedures, or even strategies.

In my own organisation (EDS), we use the ABCD risk methodology to carry out our initial risk assessments. This methodology assists you in categorising the risks to your organisation, and measures them against the probability of occurrence, thus allowing us to make informed decisions on the level of protection required.

The ABCD methodology is a simple tool to help you categorise risks. High risk situations are placed in box D, low risk in A. Figure 1 shows the risk table example, as provided by De-risk, the people behind the methodology.

During the assessment, the risks are categorised and rated against the stability of the system and the sensitivity of data.

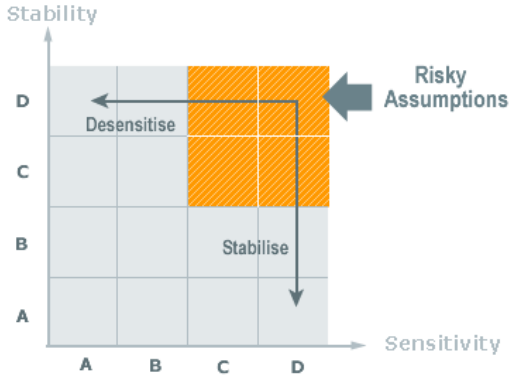

Figure 1 – ABCD Risk Methodology

For example, a banks payment system would have highly sensitive data, so would be classed as D for sensitivity. You then assess the stability of the system, and say the server it resides on was just in a standard network, you'd class the s tability as a risk, so perhaps categorise as D also.

A DD rating would mean that the system is at high risk, and corrective actions would be needed, such as moving the server into a more secure network such as a de - militarised zone (DMZ) or putting addi tional security layers in front of it.

Barnes (2001, p77) believes that risk assessments are an important element in identifying the level of protection a system requires as they often highlight alarming shortcomings in the current setup.

By evaluating the effects of the risks, combined with an estimate of the probability of occurrence, organisations can make an informed decision on mitigating actions (Woods, Kajüter and Linsley, 2008).

Having been involved in the risk management process in my own organisation, one thing I have learnt is that risk assessments are an extremely important element of business planning, and should be carried out thoroughly by a skilled assessor(s). Once the risks are identified, the business should consider whether to eliminate or protect against a risk, rather than planning to recover from a problem later.

3.2. Protection Methods

Due to the rapid pace of technological change, the increased spread of computer literacy and the growth of e-commerce, the challenge of restricting and protecting against cyber-crime is certainly a daunting one (Vacca, 2001).

According to industry surveys, it is predicted that there will be 794 million people online throughout the world by 2009 (Vacca, 2005, p5). This represents a huge amount of data transmitted over the global virtual world. Unfortunately, many businesses do not know how to properly protect their sensitive data, and this leaves them at risk of being victims of e-crime.

So how do organisations go about protecting themselves against such occurrences? Once the risk assessment has been carried out, the next step is to look at mitigating actions against those risks. For financial organisations, the risk that an attack would result in financial impact would be quite high.

There are a number of key areas that an organisation needs to think about when considering protection, including investment in prevention and detection systems (e.g. firewalls), education of its employees, and keeping its software up to date (Vacca, 2005, p156).

In our organisation, we have invested heavily in hardening the perimeter environment of our client's networks to ensure we provide the best prevention and protection possible. Investment in routers, firewalls, intrusion detection and prevention equipment, and perimeter security measures, helps us protect our clients against attacks.

Firewalls are usually the first line of defence for an organisation when protecting their network, comprising of a system, or group of systems that enforce access control policies between networks (Vacca, 2005, p100). Firewalls are a necessary tool in the protection of an organisations network, as they are generally configured to protect against unauthorised logins from the outside world.

A limitation of firewalls however is the level of protection and detection they provide, and this is why intrusion detection systems (IDS) have evolved. An IDS looks for anomalies or out of the ordinary activity on the network (Volonino, Anzaldua and Godwin 2007, p320). This provides administrators with prior warning of potential issues, and corrective action if required can be taken following an attack.

All these tools can be used together to provide added security and protection to a company's network. It is advised that you should consider a number of solutions when investing in security tools, and Vacca agrees that you should not rely on one security solution (2005, p102). He argues that good security is usually found in layers, and these layers should consist of a variety of security products and services.

This is certainly true in my organisation as we use a number of different products from leading suppliers such as CISCO Systems, eTrust® and Checkpoint Systems, using both hardware and software protection, to safeguard our clients networks and servers.

Whilst the focus has moved more to hardware protection, investment in software protection is still vitally important and as a minimum, organisations should use security software such as McAfee security suite or Norton Internet security .

These software packages provide valuable protection tools including firewall and anti virus and it is vitally important that the software is kept up to date to ensure the most vigorous protection. Protection does require investment – but that investment may save considerable amount of money, time, and effort in the future.

4. Keeping Your Business Running

4.1. Business Continuity Management

As well as trying to protect your organisation from attacks, it is also important to consider what your organisation needs to do IF you are attacked. This is known as Business Continuity Management (BCM). So, what is BCM and why is there a need for it?

A good definition of the process is that created by UK resilience, a government news and information service for emergency practitioners:

> BCM is a process that helps manage risks to the smooth running of an organisation or delivery of a service, ensuring continuity of critical functions in the event of a disruption, and effective recovery afterwards

The key point in this definition is that it is the actions following a disruption that must be considered – to ensure effective recovery for an organisation. The main goal of BCM is to prepare organisations for a multitude of incidents, whilst concentrating on ensuring the continuity of the business or service during this time.

Some of these risks can be minimised through management efforts but it is impossible to eliminate them all. Continuity strategies are designed to extenuate the risk to systems and service availability by devising procedures and steps to be taken in case of such risks coming to fruition.

Some UK companies embraced BCM early, and by 1995, BT, Lloyds TSB & Nationwide had put a BCM programme in place, followed in 1997 by the likes of Royal & Sun Alliance, Great Universal and Woolwich (Elliott, Swartz and Herbane 2002, p53).

However, the focus on BCM grew significantly in the late 1990's. The major Y2K scare got many organisations thinking carefully about what could happen (Barnes, 2001, p1). Whilst the scare led to a virtually non-existent incident, the increased level of focus enabled businesses to realise just what impact a serious incident could have on their organisation.

4.2. BCM Recovery Strategies

BCM recovery strategies help determine the arrangements for alternate facilities to use during an incident. Providing guidelines to assist in restoring IT operations quickly and effectively following a service disruption, such strategies should address disruption impacts and allowable outage times identified in the BIA.

Preparation is key, and figure 2 shows what comprises a good BCM strategy. Know your business, carry out risk assessments, create BCM plans, and most importantly, test the plans.

Figure 2 – BCM process

Elliott, Swartz and Herbane (2002, p53), believe there are three basic strategies underlying business continuity provision, these being reactive, proactive and interactive. Each approach provides different options on how to deal with BCM.

A reactive approach is where an organisation will take no, or minimal precautionary measures and react only when an incident occurs. This is a dangerous strategy and should be avoided, certainly for medium size organisations and above.

Smaller operations may choose this approach due to the costs involved in implementing protection methods – usually being of the opinion that spending money on protecting themselves against something that actually might not happen is false economy. However, this should be avoided if possible.

The most common strategy is that of a proactive approach which is a more hands on strategy, taking the initiative by acting rather than reacting to events. The majority of organisations, including EDS, adopt this strategy. The focus is on ensuring you are prepared, by taking corrective measures in readiness for the unexpected.

Finally, the interactive strategy is what Elliott, Swartz and Herbane believe would be the approach in an ideal world, where organisations consider business needs in relation to organisational and environmental pressur es, and make the necessary provisions.

Whereas the proactive strategy looks at preparing for an event, an interactive strategy will work closely with the business leads. According to Woods, Kajüter and Linsley (2008), Lorange states that interactive strategies are integrated into the overall process of strategic objective setting.

Elliott, Swartz and Herbane (2002, p97), believe it is important to consider a number of alternative solutions when developing the strategy all of which will be determined by cost and allowable downtime.

This is true, and the selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system l ife cycle.

Technology can improve business continuity with, for example, data -mirroring and off-site backups. Also important are 'battle boxes'. These should be stored offsite and hold vital information to assist the recovery, such as critical manuals, processes, software cd's and software licence information.

In my own organisation we have a mixture of recovery methods in place, dependent on the criticality of the system, its allowable outage time and its location. The BIA will determine all this.

Specific recovery methods may include commercial contracts with cold, warm, or hot site vendors such as Sungard or IBM. Cold, warm and hot sites or standby servers are an important function of business continuity, and I will explain in more detail about these below:

Cold Standby/Site – Where one or more data centres or offices are readily equipped with a prepared environment (power, network connectivity, space) to accommodate the installation of equipment in the event of a loss of server or service (Nash, 2000, p73).

In EDS we use this strategy for less critical systems, hosted outside of our data centres, and are primarily File and Print servers. In the event of the loss of such a server, we would call in a replacement server from our third party conti nuity provider, Sungard.

Sungard would then deliver the server to the designated cold recovery site, which is readily prepared and we would configure for use. This method really should only be used for less critical services – and key applications shou ld utilise a solution with quicker and easier recovery capabilities.

Warm Standby/Site – This is a partially equipped site with hardware, communication links, power etc being readily available. In the event of an incident, the warm standby/site can be ac tivated, and servers can be brought online fairly quickly.

From then, data restores and software updates will be required. In this instance, in the event of an attack that requires the invocation of a warm standby server or site, resources will be mobi lised to go to the site, and bring the services back online.

Hot Standby/Site – Third party recovery specialists such as Sungard or IBM can provide hot sites. At EDS we have a contract in place with Sungard to provide recovery to one of 4 hot sites across the country. This is only used for our larger client sites (such as London) and can include server and network recovery as well as people recovery to a prepared work area.

An example of such a mobilisation of this strategy would be a criminal attack that damages the network at a client site. We could then invoke our contract with Sungard, and arrange for the recovery to take place.

There are also differing levels of hot site capabilities. You can either use a hot site that is directly connected to the company network, but only activated at the time of an incident, or you could add a hot site as an additional live connection, and arrange for data synchronisation to ensure up to date data recovery. However, this is an expensive option, and at EDS, we activate the recovery site as and when an incident occurs.

Mirrored Sites – Also, in EDS we have what is known as a mirrored site, set up as a Dual Data Centre in the North East (for the purpose of the paper, I'll refer to them as DC1 & DC2). This is a key service offering EDS provide to all of its clients.

DC1 is deemed the primary site and all critical applications are installed at this location. DC2 is a replica of DC1, and applications and servers are configured as such that in the event of the loss of one data centre, we can easily fail over to the other, providing a continual service.

This is done mainly via clustering software to 'cluster' the servers together. Data is held on a Storage Area Network (SAN), which is also mirrored across the two sites providing data resilience.

Therefore, if for example there were an attack on servers or applications on the clients network (and the attacker managed to penetrate our stringent perimeter security), then we would isolate DC1, failover to DC2, thus allowing the continuity of service for our clients.

For this operation, we guarantee recovery to our clients within 30 minutes. This itself is the best method of ensuring business continuity, as it is both the quickest recovery strategy, and ensures no loss of data. However, this is also the most expensive strategy.

These recovery methods allow organisations to be prepared for any eventuality. Preparation, as previously mentioned is vitally important in the fight against cyber - crime.

An organisation that prepares is an organisation that will be successful if it ever becomes a target. But as well as preparing for any eventuality it is important to actually test yourselves – to see if your preparation has been worthwhile.

5. Next Steps

5.1. Testing Your Systems

Once an organisation has protected itself, and put measures in place for business continuity, the next important consideration is that of actually testing themselves against an attack. There is no point in waiting for a real attack to happen before knowing if your firewall prevents access, or your recovery strategy actually works.

There are many security testing methods, and the best way of doing this is by carrying out penetration testing. This involves testing your networks security by simulating an attack on it by an unauthorised user (Brown, 2006, p73).

By acting as an attacker, these tests allow an organisation to identify any vulnerability in their security. Vulnerabilities can occur for a multitude of reasons – for example, incorrect system configuration, hardware or software flaws, even weaknesses in process or technical countermeasures.

Vulnerabilities are then reported to the organisation, along with an impact analysis and proposals for corrective actions. The intention is to identify gaps in the system before real attackers exploit them. People who carry out these tests are often referred to as ethical hackers (Brown, 2006, p74). Ethical hackers are 'authorised' hackers of the system and use their skills to test system security.

It is also important to regularly test your organisations business continuity plan. This is usually done in a controlled manner but simulates a specific incident and looks at the actions taken following this scenario. Tests such as simulating the loss of a data centre, and failing over to the mirror site, simulating an attack on a server, and the recovery steps involved following this.

This will help give the organisation a level of confidence in their provisions, and identify any issues in a test environ ment as opposed to waiting until a real invocation is necessary.

Both penetration and BCM testing are very important to an organisation. After all, why put all the time and effort in attempting to secure your network, or creating recovery strategies, if you never know if you selected the right ones!

5.2. Investigation Tools

Following an incident, organisations will need to review what caused it. Whilst protection and recovery strategies are vitally important, if an organisation is attacked, then investigation into the root cause of this should be of high focus.

There are many tools available for assisting with this work including software packages such as the Forensic Toolkit (FTK), from AccessData and EnCase, from Guidance Software. These packages provide investigators with single tool for investigating activity and most importantly, collate the information from electronic sources in preparation for production of evidence.

The packages, written to work on a multitude of operating systems, function by allowing you to create an image of the targeted media, and then interrogating inside that image for any rogue data or suspect patterns. The utilisation of pre-written scripts, can save days, if not weeks of analysis (Schweitzer, 2003).

An important element of these tools however, is their reporting capabilities. EnCase for example, pride themselves on the fact that their 'review options allow non-investigators, such as attorneys, to review evidence with ease'. This means you don't have to be a technical expert to understand the results.

Schweitzer (2003) reports that there are also free tools available, such as Disk Investigator, and SectorSpyXP, both which can interrogate hard drives and diskettes. These packages can be used to build your own investigation tool. SectorSpyXP is an excellent freeware package that allows keyword searching, and can retrieve lost and deleted files – even ones that have been removed for the recycle bin. For a free utility, this is invaluable.

Large-scale organisations should invest in the leading packages however, as these provide a superior level of investigate analysis. Within EDS, we have a forensics department who deal with all UK forensic investigations, and we use the FTK package.

Given EDS support a number of UK government accounts, such as the Ministry of Defence, and the Department of Work and Pensions, both regular targets for opportune hackers, this shows how worthwhile a tool we believe the FTK software actually is.

6. Conclusion

Whilst reviewing literature for my report, one key statement stood out when considering the impact major incidents may have on an organisation. Nash, in his publication on Business Continuity said:

> *No company can foretell every event that might blow it off course. But companies that are as big names today as they were 50 years ago – ICI, BP, Unilever – tend to be those that assess both the upside and downside of the big decisions before they take them. They're fully aware of the risk – but they're not afraid of it. And they know that risks may pose threats but also offer the kind of opportunities that can secure their future (2000, p15)*

What this highlights is the fact that you cannot guarantee total protection against natural disasters or man made criminal attacks. But what you can do is be fully aware of the potential for such incidents to happen, and being aware should allow an organisation to prepare for any eventuality.

A difficulty I have found whilst investigating this has been identifying incidents of e-crime activity that has resulted in the invocation of business continuity processes. One criticism I have at present is that many companies do not want it to be known that they have been the recipients of an attack. Hopefully this stigma will be eradicated over time, and the business world can work together to combat the criminals of the computer-age.

Businesses must be aware of the risks that they face in order to survive. As Nash says, do not be afraid of the risk. The methods and tools available to organisations today are invaluable in the fight against electronic crime, and organisations would be foolish to not protect themselves and prepare for risks coming to fruition.

By understanding the evolution of electronic crime and being aware of the impact it has had, organisations would be in a better position to make the right decisions to secure their future. Sadly, as technology evolves, so do the methods used by criminals. What is evident however is that organisations that take time to protect and prepare are the ones that will fare better should an incident occur.

Word count – 5376 (excluding contents, references, bibliography and figures)

7. References and Bibliography

"2003 Computer Crime and Security Survey" Federal Bureau of Investigation, J. Edgar Hoover Building: quoted in Vacca, J., R. (2005) *Computer Forensics: Computer Crime Scene Investigation* , 2nd ed., Higham, Charles River Media, p5

Barnes, J., C. (2001) *A Guide to Business Continuity Planning,* Chichester, Wiley Publications

Brown, C., L., T. (2006) *Computer Evidence: Collection and Preservation* , Higham, Charles River Media

Elliott, D., Swartz, E., and Herbane, B. (2000) *Business Continuity Management: A crisis Management approach* , London, Routledge

Lorange, P. (1980) *Corporate Planning: An Ex ecutive Viewpoint*, New Jersey, Prentice Hall: quoted in Woods, M., Kajüter, P., and Linsley. P. (2008) *International risk management,* Amsterdam, CIMA Publishing, p54

Manning, G., A. (2005) *Financial Investigation and Forensic Accounting,* 2nd ed., Taylor and Francis Group, pV

Meredith, W. (1999) *Business Impact Analysis* in Hiles, A., and Barnes, P. (eds) *The Definitive Handbook of Business Continuity Management* , Chichesters, Wiley Publications: quoted in Elliott, D., Swartz, E., and Herbane, B. (2000) *Business Continuity Management: A crisis Management approach* , London, Routledge, p79

Nash, T. (2000) *Business Continuity: Helping Directors Build a Strategy for a Secure Future*, Institute of Directors, Kogan Page. p15

Oxford Dictionary of Law. (2006). 6th ed., Oxford, Oxford University Press

Schweitzer, D. (2003) *Incident Response: Computer Forensics Toolkit* , Indianapolis, Wiley Publishing Inc, p117

Vacca, J., R. (2001) *Electronic Commerce: Online Ordering and Digital Money,* Higham, Charles River Media: Vac ca, J., R. (2005) *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed., Higham, Charles River Media, p156

Vacca, J., R. (2005) *Computer Forensics: Computer Crime Scene Investigation* , 2nd ed., Higham, Charles River Media

Volonino, L., Anzaldua, R., and Godwin, J. (2007) *Computer Forensics: Principles and Practices*, New Jersey, Pearson Prentice Hall

Woods, M., Kajüter, P., and Linsley. P. (2008) *International risk management,* Amsterdam, CIMA Publishing, p54

Web References / Online Reports

BBC News (2000). *'Love' virus chaos spreads*: [online] last accessed 22nd April 2008 at http://news.bbc.co.uk/1/hi/sci/tech/736208.stm

Carter, H. (2006) *Internet crime eclipses burglary in survey of perceived risks*: [online] last accessed 1st May 2008 at http://www.guardian.co.uk/technology/2006/oct/09/news.crime

De-Risk, What is ABCD?: [online] last accessed 5th May 2008 at http://www.de-risk.co.uk/abcd.htm

Lemon, S., (2008): quoted on Continuity Forum (2008). *Serious Crime Chief warns of Cyber-crime threat*: [online] last accessed 1st May 2008 at http://www.continuityforum.org/news/2003/soca

The Register (2004). *Extortionists attack Paddypower.com*: [online] last accessed 5th May 2008 at http://www.theregister.co.uk/2004/02/07/extortionists_attack_paddypower_com/

UK Resilience (2008). *Business Continuity Background: Emergency Preparedness* : [online] last accessed 30th April 2008 at http://www.ukresilience.info/preparedness/businesscontinuity.aspx

Images

ABCD Risk Methodology (figure 1)

http://www.de-risk.co.uk/images/diagrams/2.gif

Business Continuity Management process (figure 2)

http://www.walsall.gov.uk/print/business -continuity-management-process.jpg

Cyber-crime (front page)

http://cybercrime.planetindia.net/pic/cybercrime.jpg