Ernst & Young
FROM THOUGHT TO FINISH.™

Computer Forensics

Response versus reaction

An expert paper by Ernst & Young's Computer Forensics specialists

Response versus reaction

Cyber crime potentially costs Australian businesses millions, if not billions of dollars in un-realised profits and exposes organisations to significant risk. And it is on the rise. In 2000, the Australian Computer Emergency Response Team reported a four-fold increase on the number of computer security incidents reported in 1999 .

As information technology and the Internet become more integrated into today's workplaces, organisations must consider the misuse of technology as a real threat and plan for its eventuality. When cyber crime strikes, the real issue is not the incident itself, but how the organisation responds to the attack.

In this paper Ernst & Young Computer Forensic experts look at how a swift and measured response, drawing on sound policies, tools and forensic support, allows an organisation to contain the potential damage of an attack and effectively seek compensation or prosecution.

What is cyber crime?

Cyber crime occurs where information technology is used to commit or conceal an offence.

Computer crimes include:

- financial fraud;
- sabotage of data and/or networks;
- theft of proprietary information;
- system penetration from the outside; denial of service;
- unauthorised access by insiders; employee misuse of Internet access privileges; and
- to viruses which are the leading cause of unauthorised users gaining access to systems and networks through the Internet.

Cyber crimes can be categorised as either internal or external events. Typically, the largest threat to organisations have been employees and insiders which is why computer crime is often referred to as an 'insider' crime. Ernst & Young's global research has found that 82 per cent of all identified frauds were committed by employees, almost a third of which were by management .

Internal events are committed by those with a substantial link to the intended victim, for example a bank employee who siphons electronic funds from a customer's account. Other examples include downloading or distributing offensive material; theft of intellectual property; internal system intrusions; fraud; or intentional or unintentional deletion or damage of data or systems.

However, as advances continue to be made in remote data processing, the threat from external sources is on the rise. In the 2000 *CSI/FBI Computer Crime and Security Survey*, 38 per cent of respondents reported their internal systems as a frequent point of attack while 59 per cent reported Internet connections as the most frequent point of attack.

An external event is committed anonymously. A classic example was the Philippine-based 1999 'I love you' e-mail attack. Other types of external cyber crime include computer system intrusion, fraud or reckless or indiscriminate deliberate system crashes.

Internal events can generally be contained within the attacked organisation as it is easier to determine a motive and therefore, simpler to identify the offender. However, where the person involved has used intimate knowledge of the information technology infrastructure, obtaining digital evidence of the offence can be difficult.

An external event is hard to predict, yet can often be traced using evidence provided by, or available to, the organisation under attack. Typically, the offender has no motive and is not even connected with the organisation, making it fairly straightforward to prove unlawful access to data or systems.

Cyber detectives

> In many cases, forensic investigations lead to calling in law enforcement agencies and building a case for potential prosecution, which could lead to a criminal trial.

A specialised and fast growing field of investigation known as computer forensics is a leading defence in the corporate world's armoury against cyber crime. Forensic investigators detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanisms and, potentially, identify the culprit.

A forensic expert needs to be qualified in both investigative and technical fields and trained in countering cyber crime. They should also be knowledgeable in the law, particularly legal jurisdictions, court requirements and the laws on admissible evidence and production.

In many cases, forensic investigations lead to calling in law enforcement agencies and building a case for potential prosecution, which could lead to a criminal trial. The alternative is pursuing civil remedies as opposed to criminal prosecution, for instance pursuing breach of trust, and loss of intellectual property rights.

The legal issues

The most common legal difficulty faced by organisations seeking to redress cyber crime in the courts is having digitally-based evidence accepted. Notwithstanding the technical expertise of IT teams, most companies are ill-equipped to investigate cyber crime in a way that results in the collection of admissible evidence. For example, data collected for the purposes of evidence must be shown to be untampered and accounted for at every stage of its life from collection to presentation in court. In other words, it must meet the requirements of the jurisdictions Law of Evidence.

Another issue is the lag time between legislation and the dynamic pace of change and improvements in technology. As a result, law enforcement organisations and computer forensic experts alike are forced to use archaic and non-specific laws to fit often unusual circumstances.

For example, to commit 'theft' in the Australian state of Victoria, a person must permanently deprive the victim of property. However, if an organisation's database is copied by a disgruntled employee and sold to a rival company, the organisation is not permanently deprived of the data therefore, technically, no offence of 'theft' has been committed. In addition, it is unclear whether 'data' fits into the legal definition of property

However, even in cases where there is a clearly defined crime, corporations are often hesitant to pursue a criminal conviction because of the time, cost and reputation risk involved in reaching a legal outcome.

Fighting cyber crime with risk management techniques

The rate of technological change, the spread of computer literacy and the growth of e-commerce collaboration, such as alliances and marketplaces, make the challenge of restricting cyber crime damage daunting.

With legislation lagging behind technology, businesses have had no choice but to absorb the responsibility for the security of their most valuable asset - their information. Risks range from expensive downtime, sales and productivity losses to corrupted data, damage to reputation and consumer confidence and loyalty, to hefty compensation payments or lawsuits for breaches of client information.

The best approach for organisations wanting to counter cyber crime is to apply risk management techniques. The basic steps for minimising cyber crime damage are creating well-communicated IT and staff policies; applying effective detection tools; ensuring procedures are in place to deal with incidents; and having a forensic response capability.

Effective IT and staff policies

Well-communicated and 'plain English' information technology policies educate staff about their rights and obligations in the workplace. The goal of these policies is to create a security solution that is owned by all staff, not just those in the IT division.

To be effective, IT policies should make plain what an individual employee can and cannot do on the organisation's systems, and the legal implications of misuse. It is also vital to make a continuing investment in policies, which must keep evolving and be supported by ongoing training initiatives.

Effective policies diminish the risk of internal attack, particularly unintentional attack. In addition, where attack does occur, these policies clearly define what constitutes a breach of security, making it easier to prosecute or seek compensation from the perpetrator.

Tools of the trade

While internal policies will not dissuade external cyber criminals, the right tools will detect an external attack and alert the organisation to the threat. These tools are programs that either analyse a computer system to detect anomalies, which may form the basis of an attack, or locate data that can be used as evidence supporting a crime or network intrusion.

Choosing the right cyber crime detection tools is essential for risk management in all organisations, but like most applications associated with an organisation, the question is - what is the right tool?

The right tools are those that deliver appropriate information that the forensic expert can interpret to achieve the best outcome. Ultimately, the evidence must withstand the rigours of legal proceedings. To deliver the information needed, software tools should be probing (without compromising the target of interrogation), concise, able to report findings fully, supported and easy to use. Such tools will save forensic experts valuable time and allow them to concentrate on data interpretation.

The 2000 *CSI/FBI Computer Crime and Security Survey* shows a significant increase in companies using intrusion detection systems from 42 per cent in 1999 to 50 per cent in 2000.

While some attacks will not be prevented, damage such as financial loss or negative publicity can be contained with early warning.

As with all of today's technology, detection tools date quickly as new threats emerge. Effective detection tools need to constantly evolve to counter these threats and must be engineered around best-practice risk management associated with vulnerabilities, system configurations and viruses.

Some online products and services currently in the market provide efficient, cost effective solutions by accessing computer vulnerabilities, specific to an organisation’s IT environment.

Effective procedures

Even in an organisation that has implemented the hardware, installed the software, produced the policies and employed competent staff to run an effective IT environment, it is not possible to prevent an incident from occurring.

However, the attack itself does not have the greatest impact on a company. How the business responds to that attack does. Without the appropriate procedures in place to counter detected attacks, an organisation is exposed to the risks of lost data, financial loss, network damage and loss of reputation.

While many different types of attacks may occur, the majority require the same basic steps of response. For example, the simple process of ensuring the right people know about the incident when it happens enhances an organisation's response, both in time and effective handling.

Forensic response capability

When an incident occurs, an organisation needs an appropriate forensic response in place. By appointing a forensic expert to manage the response to an incident, organisations ensure all avenues are canvassed, all evidence located and handled correctly, and all those involved are treated impartially.

Planned forensic response —a case study

This case study illustrates the organisational benefits of a planned forensic response.

Scenario one

An IT manager reviews a detection tool report that indicates a company employee is accessing restricted Internet sites and downloading objectionable material.

After discovering the activity, the IT manager remotely accesses the employee's personal computer to obtain evidence. The employee is then dismissed, based on the evidence located and obtained.

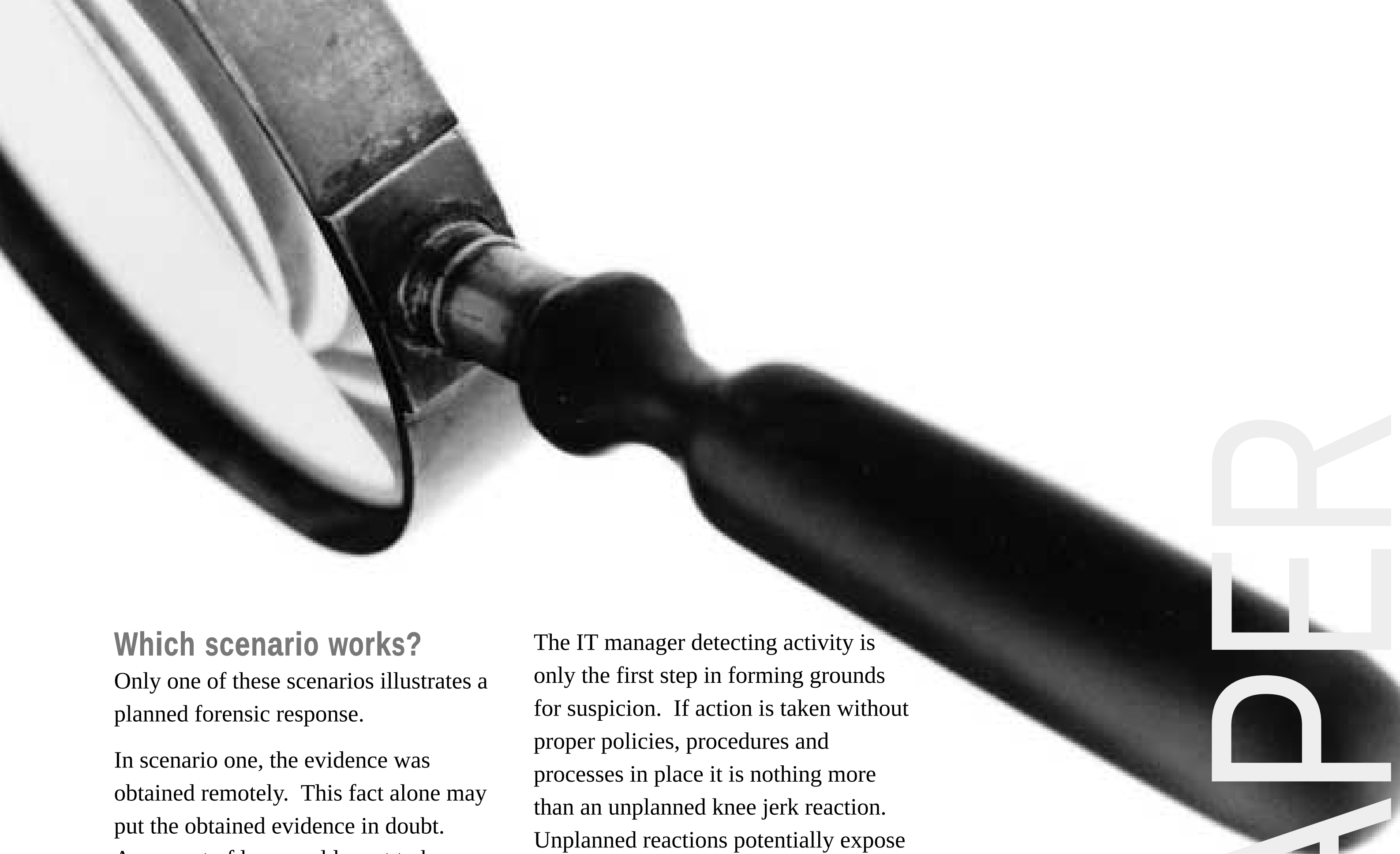
Scenario two

An IT manager reviews a detection tool report indicating a company employee is accessing restricted Internet sites and downloading objectionable material.

After discovering this activity, the IT manager follows procedures, reporting his suspicions to the nominated computer incident response contact, in this case the Chief Information Officer (CIO).

The CIO then invokes the company's incident response plan by contacting the Incident Response Team, which includes computer forensic experts. This team isolates the 'offending machine'; conducts a forensic examination of the computer system following methodologies known to be acceptable to criminal, civil and arbitration courts or tribunals; and establishes where the material came from, how often, and who else knew about it.

By following its effective policies and procedures, the organisation (via the CIO) is in an excellent position to take immediate, legal and decisive action based on all the available facts and evidence.



Which scenario works?

Only one of these scenarios illustrates a planned forensic response.

In scenario one, the evidence was obtained remotely. This fact alone may put the obtained evidence in doubt. Any court of law would want to know whether there were policies and IT infrastructure for ensuring the IT staff member knew the correct PC was accessed. Other issues surround the need for evidence to prove that a particular employee's PC was responsible for downloading the objectionable material? Can it be proved that the objectionable material was viewed on a particular PC? Who else had access to that PC? It is likely that there is not adequate evidence in this scenario to answer these questions.

The IT manager detecting activity is only the first step in forming grounds for suspicion. If action is taken without proper policies, procedures and processes in place it is nothing more than an unplanned knee jerk reaction. Unplanned reactions potentially expose an organisation to risk. Clearly, any investigation must not only be thorough and methodical but staff need procedures for reporting the activity, conducting the investigation and appointing investigators.

In scenario two, the established policies let the organisation clearly identify the incident and carry out appropriate immediate action. This places the organisation in a comfortable position to resolve the situation, contain the potential damage and effectively seek compensation or prosecution.

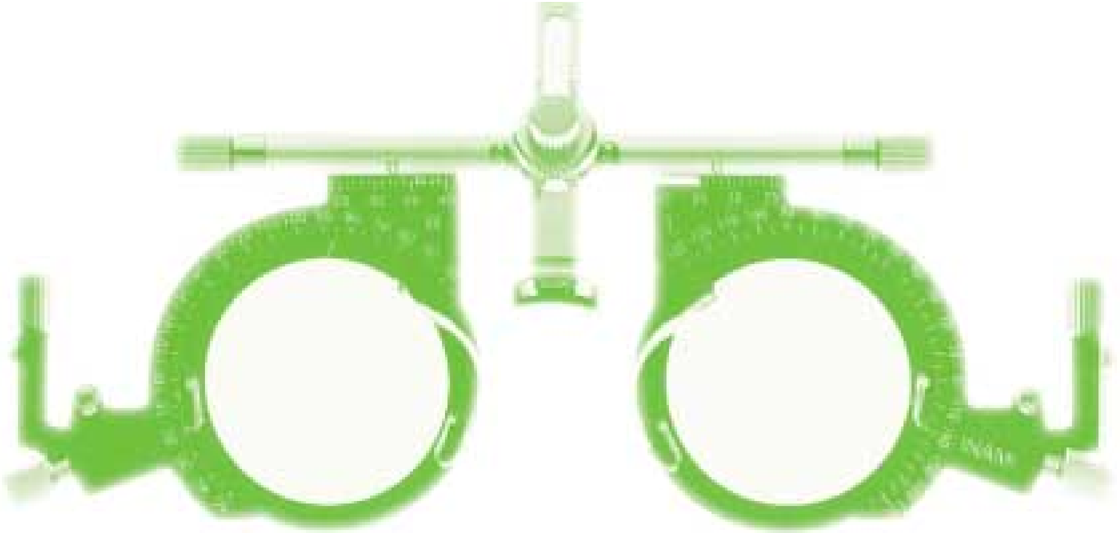
Without the appropriate procedures in place to counter detected attacks, an organisation is exposed to the risks of lost data, financial loss, network damage and loss of reputation.

Don’t react, respond

Organisations wanting to counter cyber crime need to apply risk management techniques that allow a speedy response and minimise harm.

Cyber crime is rapidly increasing and is striking at the heart of many organisations. By ensuring measures such as effective policies, rapid response capabilities, excellent information technology security positioning and forensic support exist, businesses can respond quickly, minimising the risks of lost data, financial loss, network damage and loss of reputation.

Organisations wanting to counter cyber crime need to apply risk management techniques that allow a speedy response and minimise harm. While organisations can't prevent cyber attack, they can have a planned response and even turn e-crime preparedness, or effective security, into a new competitive advantage.



Adelaide
Roger Milton
(08) 8233 7032
roger.milton@ernstyoung.com.au

Brisbane
Tim McGrath
(07) 3011 3227
tim.mcgrath@ernstyoung.com.au

Canberra
Allan Scerri
(02) 6267 3943
allan.scerri@ernstyoung.com.au

Bruce Morris
(02) 6267 3930
bruce.morris@ernstyoung.com.au

Melbourne
Graeme Conn
(03) 9288 8358
graeme.conn@ernstyoung.com.au

Eric Keser
(03) 9288 8554
eric.keser@ernstyoung.com.au

Scott Mann
(03) 9288 8350
scott.mann@ernstyoung.com.au

Perth
Peter Murdoch
(08) 9429 2127
peter.murdoch@ernstyoung.com.au

Sydney
John Thackray
(02) 9248 9267
john.thackray@ernstyoung.com.au

ERNST & YOUNG

www.ey.com/au/ITRMA

This communication provides general information current as at the time of production.   It is not intended that the information provide advice and should not be relied on as such. Professional advice should be sought prior to actions on any of the information contained herein.

Liability limited by the Accountants Scheme, approved under the Professional Standards Act 1994 (NSW).

Business Development EYA (MEL015139)