MISUSE INTRUSION ARCHITECTURE: PREVENT, DETECT, MONITOR AND RECOVER EMPLOYEE FRAUD

Norman Tinyiko Baloyi

ISACA, ISC2

Box 28289 Sunnyside 0132
ntbaloyi@netscape.net
27 12 678 7575

ABSTRACT

Despite the popular image of the hacker breaking into a computer system from the outside, most computer intrusions are committed from within the organization by employees. This research study proposes misuse intrusion architecture of information system (IS) security effectiveness that prevents, detects, monitors and recovers employee fraud. IS security effectiveness, in this architecture, refers to the ability of IS security measures to protect against unauthorized or deliberate misuse of IS assets by people. Misuse of IS assets (hardware and software) includes theft or modification of software, damage to hardware, modification of data or embezzlement, Internet abuse and unauthorized use or purposeful interruption of computer services. This architecture effectively safeguards organization’s data and assets as it follows a holistic approach that embraces all aspects of security to combat employee misuse problems, namely, managerial, operational and technical security controls.

KEY WORDS

Misuse, fraud, intrusion detection system, managerial security controls, operational security controls, technical security controls,

MISUSE INTRUSION ARCHITECTURE: PREVENT, DETECT, MONITOR AND RECOVER EMPLOYEE FRAUD

1 INTRODUCTION

Computer crimes come in many forms, all of which can have equally serious consequences where a business is concerned. This can include the alteration, destruction or misappropriation of data, the introduction of viruses or other malicious code, and the importation of pornographic, or other inappropriate material, into the organization and its dissemination. With so many business critically processes now deeply entrenched in networks, databases and computer storage, the threat posed by computer crime has become very real (Dowland *et al*., 1999). There is now a growing realization that a significant fraud threat comes from inside, and not outside, the organization (Porter, 2003). Generally, a thief with inside knowledge of an organization can cause more damage than outsiders.

Internal fraud can best be described "as the use of one's occupation for personal enrichment through the deliberate misuse of the employing organization's resources or assets" (Porter, 2003). This is typically achieved by abusing a position of trust and exploiting poor processes, systems and inadequate internal controls. Misuses of resources also include Internet misconduct in the work environment such as online pornography viewing, excessive web surfing and email spamming. After pornography, Web chats rooms (26%), and personal email browsing (23%) were the most common complaints that Human Resource departments have received complaints from discontent colleagues, complaining about their co-workers' Internet antics (Computer Fraud & Security, August 2002). It is worth noting that widespread fraud and computer abuse is much more likely to happen in an atmosphere of mistrust and resentment, but happy and motivated staffs are far less likely to commit opportunistic computer fraud (Sekar *et al*., 1999). Perpetrators are typically opportunistic individuals placed in organizations by organized criminals who are immune to, and will exploit, an organizational culture of trust and caring.

Threats from internal users (insiders) can be classified as either malicious or inadvertent. The former relates to a thief with inside knowledge of an organization who gains unauthorized access to the information systems for personal gains. The thief may intend to sell the information as was the case in Computer Fraud & Security (September 2002), when three insiders revealed customer's online bank account. The latter is a result of well-meaning employees who can cause severe outage or information compromise as a result of inadvertent or ill-advised actions (Casey, 2003).

Practically speaking, there are two methods of containing any kind of fraud: prevention and detection. Prevention focuses on controls designed to reduce the opportunity for unauthorized use of corporate resources. Detection focuses on the controls designed to alert the appropriate personnel of the fraud detected.

Databases have been developed to deal with misuse problems, namely, Detection of Misuse In Database System (DEMIDS) (Chung *et al.*, 1999) and Detecting Intrusions in Database through Fingerprinting Transactions (DIDAFIT) (Low *et al.*, 2002). DEMIDS attempts to profile working scopes based upon user access patterns in relational databases. The approach assumes that a user will not typically access all attributes and data in a database schema, and therefore their access patterns will form some working scopes, which are set of attributes usually referenced together with some values. Based upon this assumption, DEMIDS uses the notion of a distance measure between sets of attributes that consider both the structure of the data and user behaviour. This notion is then used to guide the search for regular patterns that describe user behaviour in a relational database. DIDAFIT monitors anomalous SQL queries by generating fingerprints of authorised queries. These fingerprints are sequences of SQL queries along with variables that the user should not change, ensuring that the queries are executed in proper order and only on the restricted range of records.

It should be noted that some of the technological approaches in the domain of insider attack detection are not as mature as those relating to other aspects of security. The United States of Naval Research funded a project to investigate the insider threat and how it can be mitigated (Thompson *et al.*, 2004).

This paper proposes an integrated architecture for preventing, detecting, monitoring and recovering employee misuse intrusions. The architecture is the mixture of human and technology measures. The organization of the paper is as follows: the reality of internal fraud, the sources of internal security threat, attack vectors, misuse strategic solutions, architecture, and recommendations and conclusions.

2 THE REALITIES OF INTERNAL FRAUD

All significant research into internal fraud indicated that the greatest source of threat on corporate assets comes from management and employees instead of third parties. The statistics on internal fraud are startling. Internal fraud and abuse cost US business $600 billion in 2001 (Porter, 2003). In Europe, the figure for 2002 was bigger than the $2.16 billion reportedly lost to internal fraud in 2000 (Porter, 2003). Insiders accounted for 52% of all large-scale frauds over 1000 pounds with management grades accounting for 40 % and more junior employees 12%. Within UK plc, 40 million pounds a day is lost to corporate fraud in which 80% can be attributed to employees (Thomson, 2002).

The US Federal Bureau of Investigation (FBI) survey reported that the average cost of a successful attack by an external hacker was $56,0001, whereas that by an insider attack was reported at $2.7 million, nearly 50 times greater (Thompson *et al.*, 2004). Further, it is estimated that over 80% of information security incidents for the past 5 years is as the results of insiders (Thompson *et al.*, 2004).

The number of attacks in network computer systems is growing exponentially and there is a high possibility that most incidents are not reported, since most organizations are afraid to loose customers' confidence (Dowell and Ramstedt, 1990). For some organization it is estimated that the cost of internal fraud can be as high as 6% of turnover. The vast majority of internal fraud goes undetected and is often only discovered by accident or whistle-blowing, with the average detection time being an astonishing 18 months (Porter, 2003).

Around 60% of frauds perpetrated from within, 58% of this fraud were uncovered by accident. The recovery rates remain low with as few as 20% of organization able to recover half or more of the losses suffered as a result of fraud (Philippsohn, 2003).

No organization can afford to be complacent about the possibility of falling victim of crime. Apart from potentially huge monetary losses, any breach of network security can fatally undermine customer confidence and cause widespread damage to any organization's image and reputation (Lichtenstein, 2000).

3 THE SOURCES OF INTERNAL SECURITY THREAT

The internal security threat encompasses a broad range of events, incidents and attacks, all connected by being caused by organization's own staff, its authorized IT users. This threat area covers user errors and omissions, negligence and deliberate acts against the company (Leach, 2003). The staff's lack of awareness of threats and vulnerability and inadequately trained staff can easily make errors. The internal threat is predominantly the result of poor user security behaviour such as forgetting to apply security procedures, taking inappropriate risks because of not appreciating or believing the level of risk involved (e.g. leaving the PC unattended in an open office without logging off), deliberate acts of negligence (i.e. users knowingly failing to follow essential security processes), and deliberate attacks by technically- literate abusing their positions in order to commit fraud (i.e. users purposefully acting against the organization's interests). Another internal security threat can be as a result of competing business pressures resulting in "tactical shortcuts" with management overriding control or worse acting as participants in a fraud (Porter, 2003).

4 IDENTIFYING ATTACK VECTORS

Attack targets considered in this study are security controls and audit applications that ship with any operating system. These obvious targets for malicious insiders must be very well protected. To identify malicious behaviour, actions on the documents (i.e. any file that contains modifiable data such as a source code file, text file, image or binary) can help distinguish between legitimate and malicious actions (Thompson *et al.*, 2004). This means considering document's environment as well as actions on the groups of documents.

Properties of the individual documents as they accessed must be observed to show how long it took the intruder to locate desired information on the system. This will help to determine intruder's skill, knowledge of targets and intent (Casey, 2003). Accessed document's properties includes time of use, length of time opened, how they are copied or moved, actions inside document (altering of data, clipboard actions etc.), their copying to external media or network shares, environment of the system such as processes and applications that access the document, network interactions of any applications used to view the documents and many other characteristics. Whenever the document is seen as a member of a group, actions on the group can be recognized as malicious (e.g. downloading the entire directory structure from a network share).

5 MISUSE STRATEGIC SOLUTIONS

In order to be effective, misuse strategic solutions must be implemented. These solutions consist of prevention, detection, monitoring and recovery.

5.1 Prevention

One aspect of prevention can relate to predicting whom such attacks might arise from (Furnell, 2004). This is with respect to previous research that indicated that psychological characteristics, such as introversion, may make an individual a more likely candidate for committing misuse (Shaw *et al.*, 1998). Danger signs from this perspective are not easy to identify, more especially if we desire an automated solution.

There are some other characteristics that can be measured and assessed at the system level in order to yield a metric for the estimated potential threat posed by different users (Magklaras and Furnell, 2002). These findings could feed into other processes, such as assignment and review of access rights, as well as monitoring and supervision of user activity.

Misuse prevention can also include perimeter defence technology such as firewalls, website/email content scanners and identity card access controls. They also include recruitment screening, segregation, supervision, and training. Many organizations rely heavily on such mechanisms. However a prevention-centric strategy will only succeed if the prevention mechanism has been proved to be flawless. Otherwise, its weaknesses will be exploited and bypassed by people who know the system.

5.2 Detection

While it may seem easy to commit illegal acts, cyber criminals are frequently unaware that it is also possible to detect them (Stevenson, 2000). Intrusion detection is a viable and practical approach for providing a different notion of security in our huge and existing infrastructure (possible insecure) computer and network systems. Misuse detection includes internal auditing, whistle-blower hotlines, and authorization. On the technical side, there are automated systems such as intrusion detection system (IDS). The combination of IDS systems, namely, network-based IDS and host-based IDS should be used to detect insider attacks (Einwechter, 2002).

Since insiders are in a much better position to disable, turn off, or otherwise interfere with IDSs, relying on IDS output alone for insider attack detection is fundamentally risky. Collecting and analysing data that are likely to yield multiple indicators are in fact the only viable direction given how subtle insider attack patterns often are. The potential indicators include: deliberate markers, meaningful errors, preparatory behaviour, correlated usage patterns, verbal behaviour and personality traits (Schultz, 2002).

5.3 Monitoring

It is sometimes difficult to control or prevent misuse as the perpetrators concerned may not be violating any system-side access rules. At this point, the type of control needs to move from prevention towards monitoring. Monitoring employees and other third parties can be used to prevent and detect fraud at the network level, operating system level and application level.

Misuse activities visible at *network level* that need to be monitored include access to prohibited content, downloading of inappropriate material, spamming, and play network games (Furnell, 2004).

Monitoring at the *operating system level* includes using events such as system calls, CPU usage, and file access, alongside data sources such as audit trails and event logs (Furnell, 2004). Incidents discernable at this level may include breaches of privacy, installation of unauthorized software and storage of inappropriate materials.

At the *application level*, monitoring includes monitoring of interaction with the applications such as request-response, access patterns, user input, application output, and utilization of application functions (Furnell, 2004). Application level would be the most appropriate level for determining misuse such as disclosure of confidential information, malicious data modification, and fraud. Application level monitoring is more likely to provide the most relevant data for the purposes of detecting the most significant and damaging classes of insider misuse.

The traditional way of monitoring of malicious behaviour is through intrusion detection systems. One other method is to take the network monitoring model into the intranet and modify policies (Thompson *et al.*, 2004). File system filter driver on the Windows platform is another way to monitor activities of rogue insiders which intercepts all action on a specific document (Thompson *et al.*, 2004). This mechanism intercepts suspicious behaviour before it is executed on a host computer and coupled with process monitoring, data is generated to train statistical models.

5.4 Recovery

It is vital that organizations implement a policy and procedure which allows employees to report fraud and take the appropriate steps to deal with a fraud once it has occurred. The civil court is one route open to a company in order to stop the fraudster, locate the assets and to freeze and recover them once judgment has been obtained (Philippsohn and Thomas, 2003). Organizations must ensure proper fraud evidence collection and interpreting behaviour represented in the digital evidence to ensure that the evidence would be admissible to court. The life cycle of evidence include: identification and collection of evidence, analysis, storage, preservation, transportation, and presentation in court (Harris, 2002).

6 ARCHITECTURE

This section starts by discussing the components of the architecture, integrates the architecture and then discusses the results of the architecture.

6.1 Architecture components

The components of the misuse intrusion prevention and detection architecture, namely, managerial, operational, technical controls and other controls (honeypot and culture) are discussed in this section. The details of these controls can be found in Baloyi (2005).

6.1.1 Managerial controls

Managerial controls are usually management's responsibilities such as drafting rules and ensuring that these rules are enforced.

- Preventive managerial security controls include: security policies, procedures, standards, screening personnel, effective hiring practises, performing security awareness training and classifying data.

- Detective managerial security controls include: job rotation, mandatory vacations, establishment of incident response capability, ongoing risk management and professional security review.

6.1.2 Operational controls

Operational controls are used to correct operational deficiencies that could be exercised by potential threat-sources.

- Preventive operational security controls include: limit external data distribution, control data media access and disposal, safeguard computing facility and control software viruses.

- Detective operational security controls include: reviewing audit logs and closed-circuit television monitoring.

6.1.3 Technical controls

Technical controls are logical (software and hardware) mechanisms used to restrict subject's access to resources.

- Preventive technical security controls include: call-back systems, constrained user interface, security software, database view, clipping levels, antivirus, and data integrity software.

- Detective technical security controls include: audit, restore secure state, virus detection and eradication, proof of wholeness, intrusion detection and containment.

6.1.4 Other controls

Honeypot strategy is also deployed in this architecture. The honeypot is a computer that could have many open ports, exploitable vulnerabilities, and limited security features installed on it, so that the attacker would be drawn to it (Staniford-Chen and Heberlein, 1995). In actuality, the computer would have no useful information on it and no direct connections to important services, but when the attacker attempts to connect to the device, the organization would be watching and recording. Honeypot or enticement is an effective method of learning about attack techniques and possibly prosecuting computer criminals.

Culture of respect, loyalty and responsibility will have wider productivity benefits to an organization to prevent misuse activities.

6.2 The integrated misuse intrusion architecture

As security cannot be described by a list of security controls, Figure 1 provides an integrated misuse prevention and detection architecture that integrates the above-mentioned security controls.

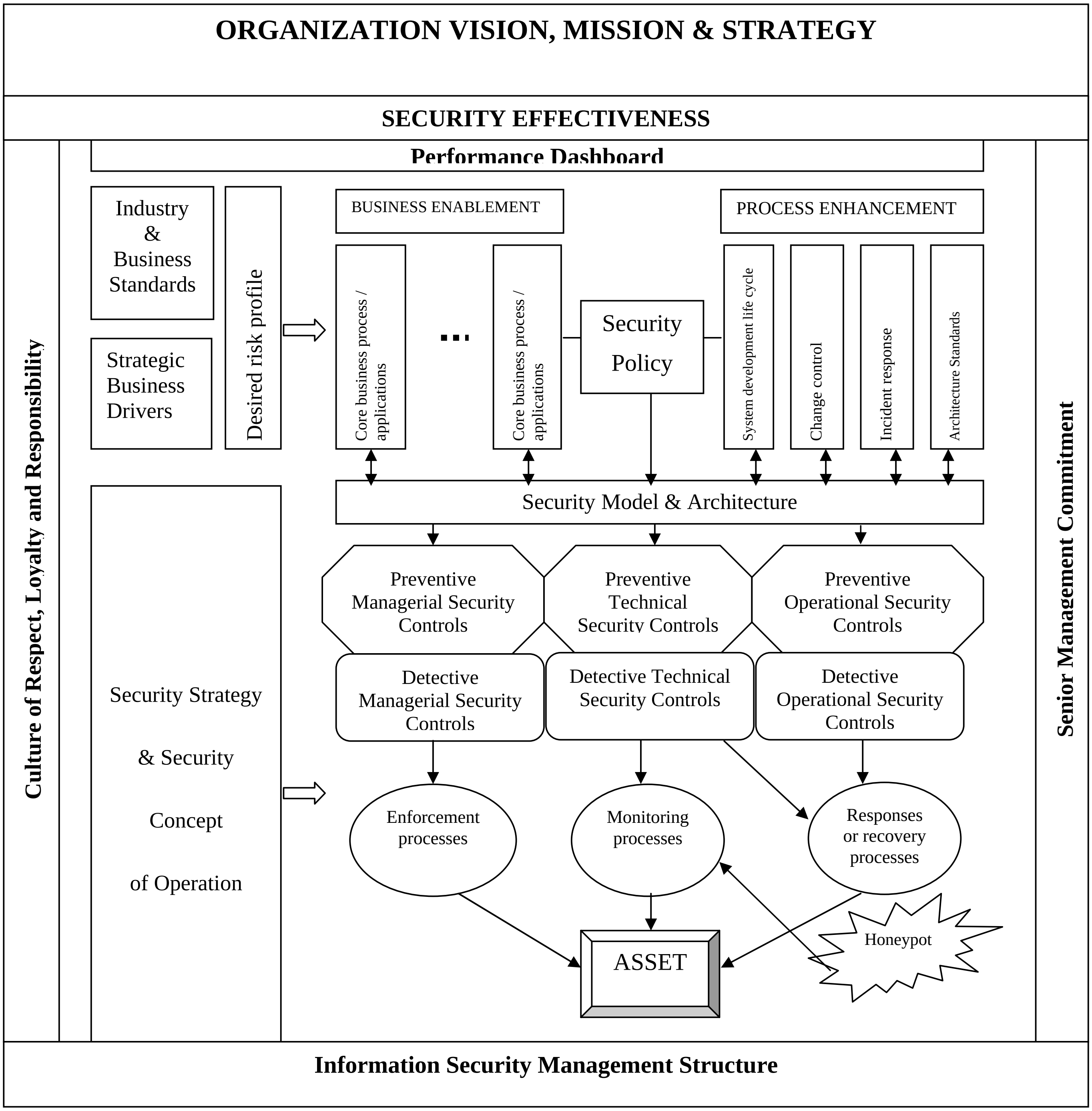
ORGANIZATION VISION, MISSION & STRATEGY
SECURITY EFFECTIVENESS
Performance Dashboard
Culture of Respect, Loyalty and Responsibility
Senior Management Commitment
Industry & Business Standards
Strategic Business Drivers
Desired risk profile
BUSINESS ENABLEMENT
PROCESS ENHANCEMENT
Core business process / applications
...
Core business process / applications
Security Policy
System development life cycle
Change control
Incident response
Architecture Standards
Security Model & Architecture
Preventive Managerial Security Controls
Preventive Technical Security Controls
Preventive Operational Security Controls
Detective Managerial Security Controls
Detective Technical Security Controls
Detective Operational Security Controls
Security Strategy & Security Concept of Operation
Enforcement processes
Monitoring processes
Responses or recovery processes
ASSET
Honeypot
Information Security Management Structure

Figure 1: Integrated intrusion prevention and detection architecture.

This architecture requires a whole architecture to be defined to ensure that all the components are properly integrated together and that the whole thing runs smoothly. It also implies that the system is operated correctly.

6.3 Discussion of the architecture

To keep their data secure, organization must be adopt a holistic security strategy that embraces the whole organization and infrastructure. The proposed architecture effectively safeguards organization's data and assets as it follows a holistic approach that embraces all aspects of security, including systems architecture, security policies, and user education.

The security of the organization cannot succeed without the support and commitment from the top management who provides sufficient resources. In support of its vision, mission and strategy, top management should change corporate thinking, cultivate culture of respect and establish sustainable, cost-effective business standards that encompass a common risk language across all departments. This will help engrain security into the organizational consciousness and create blueprint for security, manage process enhancement and change, deploy new business applications within the parameters of the risk profile, and monitor performance. This top-down approach using information provided from the bottom up forms the foundation of a holistic approach to enterprise security.

Holistic security means balancing technology, procedures, and people. It also means balancing factors of mitigating risk, enhancing productivity, reducing cost, and streamlining application development and integration. Implementing a holistic security strategy means moving your organization from a technology-centric to a business-centric security process to assess risk and manage potential threats (Patterson, 2002).

The architecture takes security as core business processes (integrating preventive and detective managerial, operational and technical security controls), appropriate for the organization's culture of respect, loyalty and responsibility that align policy, technology, roles, and structures, operating procedures and key performance indicators that measure efficiency, effectiveness, value and continuous performance improvement of each individual security process.

The key success factor of this misuse architecture is a well-defined, comprehensive security philosophy with a constant vigilant approach.

7 RECOMMENDATIONS

Organization should identify appropriate precautions that can be taken at personnel level to reduce the likelihood of the misuse attacks, which are:

- Check references of prospective new employees before hiring them.
- Ensure that adequate reminders about the "acceptable use" policy are encountered by staff during their day-to-day use of systems.
- Ensure adequate supervision of the staff by line management. Appropriate use of informal monitoring, as well as more formal context such as appraisal, may help to identify disgruntled employees who may be at risk of causing problems.
- Provide a means by which staff can confidentially report misuse of IT systems, without fear of recrimination from colleagues.

When used in combination with technical, operational, and other managerial measures, these procedures may well improve the prevention and detection of insider incident.

8 CONCLUSIONS

The possibility of insider misuse (fraud) is due to hacking or security control loopholes. Theft of the organization's information can be very expensive to recover and repair. Deterrence measures are the most effective means to prevent theft of information. Deterrence measures are attempts to discourage people from criminal behaviour through fear of sanctions. Sanctions are effective if people know that they will definitely be punished for the crime or anti-social acts and that the punishment will be harsh. In the context of IS security, deterrence efforts are policy statements and guidelines on legitimate use of IS assets, security briefings on the consequences of illegitimate use of IS assets, and audits on the use of IS assets. Visible deterrent efforts (e.g. writings on notice boards or after signing on computer systems etc.) are effective active measures that can reduce IS abuses by convincing potential abusers that the probability of getting caught is high. Deterrence efforts are particularly effective if the punishment for IS abuses is also severe.

The likelihood of the insider misuse being successful can be further reduced by implementing security controls, namely, managerial, operational, and technical. The architecture can help move an organization from reactive fire fighting to proactive prevention of financial loss and damage to reputation. The increase in efficiency and effectiveness of the prevention, detection, monitoring and recovery processes will lead to cost savings. But before carrying out monitoring of staff, an organization should seek specialist legal advice tailored to its specific circumstances.

An organization must ensure that employees know exactly what to do, who to report to and the importance of acting quickly to minimise losses, preserve electronic evidence and ensure that the fraudster is never tipped off before steps can be taken. Failure to implement such procedures effectively could eventually lead to organizations failing to recover fraud losses.

9 REFERENCES

Casey, E. (2003). "Determining intent – opportunistic vs. targeted attacks". *Computer Fraud & Security*, pp. 8-11.

Chung, C.Y., Gertz, M. and Levitt, L. (1999). "DEMIDS: a misuse detection system for database system". In *Proceedings of the 3rd International Working Conference on Integrity and Internal Control in Information Systems*, Amsterdam, The Netherlands, November, pp. 18-19.

Dowell, D. and Ramstedt, P. (1990). "The ComputerWatch data reduction tool". In *Proceedings of the 13th National Computer Security Conference*, October, pp. 99-108.

Dowland, P.S. Furnell, S.M., Illingworth, H.M. and Reynolds, P.L. (1999). "Computer crime and abuse: A survey of public attitudes and awareness". *Computers & Security*, Vol. 18, 715-726.

Einwechter, N. (2002). "Preventing and detecting insider attacks using IDS. Online document, http://online.securityfocus.com/infocus/1558.

Furnell, S. (2004). "Enemies within: the problem of the insider attacks". *Computer Fraud & Security*, pp. 7-11.

Harris, S. (2002). *Mike Meyers's CISSP Certification Passport*. McGraw-Hill/ Osborne.

Lichtenstein, S. (2000). "Internet risks for companies". *Computers & Security*, 17, pp. 143-150.

Low , W.L., Lee, J. and Teoh, P. (2002). "DIDAFIT: Detecting intrusions in databases through fingerprint transactions". In *Proceedings of the 4th International Conference on Enterprise Information Systems*, Ciudal Real, Spain, Vol. 2-6, April, pp. 121-128.

Magklaras, G.B., Furnell, S.M. (2002). “Insider threat prediction tool: use”, *Computers & Security*, Vol. 21, no 1, pp. 62-73.

Patterson, T. (2002). “Holistic security: why doing more can cost you less and lower your risk”. *Computer Fraud & Security*, pp. 13-15.

Philippsohn, S. (2003). “Monitoring employees to prevent and detect fraud”. *Computer Fraud & Security*. pp. 12-14.

Philippsohn, S. and Thomas, S. (2003). “Recovering fraud losses”. *Computer Fraud & Security*. March, pp. 6-10.

Porter, D. (2003). “Insider fraud: spotting the wolf in sheep’s clothing”. *Computer Fraud & Security*, April, pp. 12-15.

Schultz, E.E. (2002). “A framework for understanding and predicting insider attacks”. *Computers & Security,* pp. 527-531.

Sekar, R., Bowen, T. and Segal, M. (1999). “On preventing intrusions by process behaviour monitoring”. *Proceedings of the Workshop on Intrusion Detection and Network Monitoring*. California, USA.

Shaw, E.D., Ruby, K.G. and Post, J.M. (1998). “The insider threat to information systems: psychology of the dangerous insider”. *Security Awareness Bulletin*, Vol. 2-98, pp. 27-46.

Staniford-Chen, S. and Heberlein, L.T. (1995). “Holding intruders accountable on the Internet”. *Proceedings of the 1995 IEEE Symposium on Security and Privacy*. Oakland, CA.

Stevenson, G. (2000). “Computer fraud: Detection and prevention”. *Computer Fraud & Security,* pp. 13-14.

Thompson, H.H., Whittaker, J.A. and Andrews, M. (2004). “Intrusion detection: perspective on the insider threat”. *Computer Fraud & Security*, January, pp. 13-15.

Thomson, M. (2002). “Protecting from within”. *Computer Fraud & Security,* October, pp. 8-9.