

Information Security White Paper  
Insider Threats to Acme Widgets plc  
(A multinational organisation expanding into China)

Stuart King MBA M.Inst.ISP

## **TABLE OF CONTENTS**

<b>1. INTRODUCTION</b>	<b>3</b>
The nature of the risk	3
<b>2. EXAMPLES OF REAL INCIDENTS</b>	<b>4</b>
<b>3. THE INTERNAL RISK ASSESSMENT</b>	<b>6</b>
<b>4. INSIDER THREAT SCENARIOS</b>	<b>7</b>
<b>5. PROTECTING IP IN CHINA</b>	<b>11</b>
<b>6. CONCLUSIONS</b>	<b>12</b>
Recommendations	12
<b>7. APPENDIX A - CHECKLIST</b>	<b>12</b>
<b>8. APPENDIX B – INCIDENT EXAMPLES</b>	<b>15</b>
<b>9. REFERENCES FOR THIS DOCUMENT</b>	<b>19</b>

# 1. Introduction

This paper addresses the potential risks and threats posed by former or current employees of Acme Widgets (AW) who may be motivated to act maliciously towards the organisation.

Research into corporate fraud and numerous case studies have been used to derive an assessment of the potential risk to AW from individuals who may be motivated to cause harm to the company because of a grievance, some negative work-related event, a desire for revenge against another individual (e.g. a manager), or to profit from the consequences of their actions.

The aim of this document is to present a clearly stated description of the risks to AW plc from dishonest, malicious, and motivated current and former employees.

The objectives are

- i) Assess current and future insider risks to AW PLC across the full scope of operations
- ii) Assess existing controls within AW PLC that mitigate insider threats
- iii) Describe additional controls for instances where the existing risk mitigation measures fall short of providing adequate protection

This paper is intended to be read by senior management and other executive stakeholders within the business.

DISCLAIMER: The company ( Acme Widgets plc) described within this document is fictional and any similarity to actual companies is wholly accidental.

## ***The nature of the risk***

Most commonly when thinking about information security we consider how to prevent intrusion into our business from the outside. The facts and statistics tell a different story. 62% of large businesses in the UK [2] have dealt with a security incident instigated by a current or former employee. Another study [6] reveals that 54% of UK company employees would be willing to gain illegal access to sensitive information from their employer's IT systems, while 22% admitted to already having done so. Human Resources and payroll details were found to be the most desirable targets, followed by manager's and colleagues' personal notes.

A study by Carnegie Mellon's CERT program reported that 75% of the 40 proprietary and confidential information thefts studied between 1996 and 2002 were committed by current employees. Of those current employees committing intellectual property thefts, 45% had already accepted a job with another company. The majority of the thefts occurred between the time the employee received an offer and the time they officially left the company.

For AW plc, the risks are exacerbated by the global spread of the business and the varying attitudes to information security that have been observed to range from *concerned* to *flippant*.

High turn-over rates (30% in the UK) of sales and marketing staff, and a dependency on temporary and contract workers who have no company loyalty adds to the risk.

For the purpose of this paper Insider threats will be categorised as follows:

**Level 1.** Trivial, temporary and commonplace

Examples:

- Exceeding the company Internet browsing policy of “reasonable personal use” (Research performed by Bruce Schneier at schneier.com states that approximately 10% of employees will be doing this).
- Exceeding the company Email policy of “reasonable personal use.”
- Using fax and telephone services for personal use

**Level 2.** Potentially serious for personal financial gain

Examples:

- Expense fraud
- Selling company assets (e.g. computing equipment)
- False inputs into accounting systems (e.g. purchase orders)

**Level 3.** Serious short-term impacts, motivated by revenge.

Examples:

- Unauthorised re-configuration of IT systems
- “logic bombs”
- Deletion or alteration of customer data

**Level 4.** Serious long-term impacts, motivated by revenge or personal gain

Examples:

- Selling customer database to a competitor
- Revealing financial results, acquisition or divestiture information to third parties ahead of official announcements
- Stealing customer credit card data

**Level 5.** Catastrophic impacts

Examples:

- Arson
- Permanent, irretrievable, destruction of critical data assets

In a paper entitled *Balancing the insider and outsider threat* [1], Walton states that *insiders enjoy privileged access that enables them to do serious damage far more easily than anyone attacking from outside... The essential feature of an insider attack is that the perpetrator has legitimate access to the information asset being attacked. This inherently limits the role of technical counter-measures.*

## 2. Examples of real incidents

Examples of incidents involving company insiders are frequently reported.

- A study of 112 large (i.e. more than 250 employees) by ProofPoint [6] discovered that more than 70% had disciplined staff for violations of email usage policies during the previous 12 months, and more than a third had fired them.

- Research from a Microsoft-commissioned survey amongst 2,226 UK employees revealed that, if the opportunity arose, 54% would be willing to gain illegal access to sensitive information from their employer's IT systems, while 22% admitted to already having done so. Human Resources and payroll details were found to be the most desirable targets, followed by manager's and colleagues' personal notes.

- One of the most infamous recent insider attacks occurred at DuPont in 2005. According to court filings, a research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22 000 sensitive documents and viewed an additional 16 706 documents in the company's electronic library. The employee used his privileged access to harvest information over a period of five months. He took this data consisting of trade secrets and proprietary information worth over roughly £250 million to his new employer.

- A study by Carnegie Mellon's CERT program reported that 75% of the 40 proprietary and confidential information thefts studied between 1996 and 2002 were committed by current employees. Of those current employees committing intellectual property thefts, 45% had already accepted a job with another company. The majority of the thefts occurred between the time the employee received an offer and the time they officially left the company.

More specific to UK based businesses is the 2006 DTI Information Security Breach Survey [2]. This found that 52% of the worst security incidents suffered by large businesses (250 or more employees) occurred internally. 32% of large businesses (65% of UK based large businesses ) had an incident relating to staff misuse of systems. 45% of large businesses reported theft or fraud relating to computer use. The survey concludes that staff misuse is the largest cause of incidents for large organisations.

Here's a summary of the types of reported employee misuse.

Type of misuse	Level	Large businesses	Overall
Misuse of web access	1	62%	17%
Misuse of email	1,4	43%	11%
Unauthorised access	2,3,4,5	18%	4%
Breaches of data protection laws or regulations	4	8%	2%
Misuse of confidential information (e.g. IP or customer data)	4	9%	2%
Any of the above		65%	21%

Refer to Appendix B of this document for a long list of documented incidents relating to the malicious insider.

### 3. The Internal Risk Assessment

Identifying employees who might be the cause of insider risk is difficult. Some literature on the subject places employees into one of the following three categories:

**Unauthorised and malicious** users are described as individuals within an organisation that mask their identity, their behaviour, or both, for the purpose of compromising the security of the database.

**Authorised and intelligent** users are described as privileged internal employees that use IT resources appropriately and in accordance with the defined security policies of an organisation.

**Authorised and dangerous** users are described as privileged internal employees that make unintentional mistakes that appear as malicious or fraudulent and compromise the defined security policies of an organisation.

Actual quantitative, empirical data relating to the number of employees who might fall into one or other of the categories is the subject of debate. For some organisations the numbers have been quoted as high as 15% of the employee base who might be willing to behave dishonestly where both the risk of being caught and the consequences are low.

According to Porter[8] “businesses where there are high levels of organizational or process change will be particularly vulnerable.” This is applicable to AW plc and equally applicable to newly acquired businesses being assimilated into the AW PLC culture, processes and networks. Porter goes on to make the point that insiders “know the controls and how to bypass them, and are often well-versed in the investigative process and know to hide any incriminating evidence”

Research performed at Carnegie Mellon [9] considered some the activities and motivations of malicious employees as follows:

- Most malicious actions are triggered by a negative work-related event
- Sixty-two percent of incidents studied in the research were planned in advance.
- Eighty percent of the insiders exhibited unusual behavior in the workplace prior to carrying out their activities.
- Fifty-seven percent of insiders exploited systemic vulnerabilities in applications, processes and/or procedures.
- Thirty-nine percent used relatively sophisticated attack tools.
- Sixty percent of insiders compromised computer accounts, created unauthorized backdoor accounts or used shared accounts in their attacks.
- Most incidents were carried out via remote access.
- Less than half of the insiders (43%) had authorized access at the time of the incident.
- Insider activities caused financial losses (81%), negative impacts to business operations (75%) and damage to the organizations' reputations (28%).

Figure 1 below is a classification of insiders as described by Magklaras and Furnell [4] in their paper entitled “Insider Threat Prediction Tool: Evaluating the probability of IT misuse”

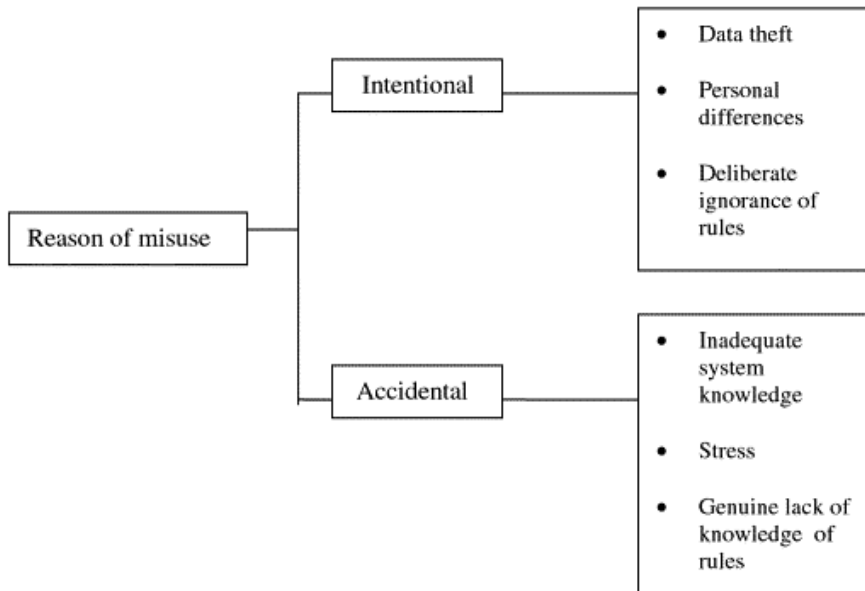


Figure 1. Classification of misusers by reason

As figure 1 shows, some misuse may be accidental and the result of inadequate knowledge of how to correctly use systems, stress, or other non-malicious factors. For example, a person working to tight deadlines and under pressure to complete a difficult task is more likely to make errors that might result in outcomes similar to those that might appear to be malicious.

## 4. Insider threat scenarios

This section considers insider threat scenarios relevant to AW plc together with an assessment of their risk likelihood, the potential consequences, and controls for mitigating the risk.

**Scenario 1.** Deliberate compromise of company critical data. For instance data pertaining to a planned acquisition being taken from company networks and used for profit or competitive advantage of another organisation.

**Attack vectors.** Acquisition data is stored on private network drives and laptop computers. Information about acquisitions is also stored within email. Network administrators have the capability to access any of these resources, including private drives on laptop computers when they are connected to the network. Network shares, if not correctly configured, may allow access to individuals who do not need to know the information being stored. Emails about acquisitions

are not secure once sent out of the network and could be compromised en route to the recipient and at the recipients server or personal computer.

**Likelihood** There is empirical evidence to suggest that such data is frequently targeted and company insiders most likely to be the source of data leaks. For AW PLC, a compromise could be accidental or the result of curiosity when an individual who should not have access to the data chances upon a particular file. With a high rate of acquisition, private data about processes taking place could be compromised at the target company – particularly if individuals within the organisation in question feel disgruntled about the proceedings.

**Controls.**

1. Use encryption and password protect files containing private data
2. Do not send private data by email unless encrypted. Ensure that passwords to unlock files are not sent with the files – telephone the recipient with the password
3. Verify access permissions on private directories
4. Ensure that individuals with a requirement to work on sensitive and private data understand how to keep it protected

**Scenario 2.** Deliberate sabotage of IT systems resulting in lost productivity and/or data

**Attack vectors.** Network administrators and software developers are usually the individuals with the opportunity to cause damage to IT systems. They will have access and knowledge as to how to make changes likely to cause the most inconvenience or damage. There are regular news reports of such events occurring with the most common being the “logic bomb” – this is where a software developer or network administrator plants some code or an application designed to activate at a later date – either by gaining external access through a “back-door” once the individual has departed from the organisation or when a certain events (such as a specific date or time) occurs. A motivated employee with appropriate knowledge and access – particular one disgruntled through a negative work related experience – could change passwords or delete vital data files causing a degree of inconvenience while the situation is resolved.

**Likelihood** There is a high likelihood of such an event – such events are frequently recorded and have previously occurred within AW plc.

**Controls.**

1. Perform background checks and follow up on references of all temporary and permanent staff whose role will require them to have privileged access to resources
2. Ensure that change control processes are strictly adhered to
3. Ensure that all accounts are disabled and deleted as soon as possible after an employee

<p>resigns or is fired. Shared accounts to which the individual had access should also have their password changed</p> <ol style="list-style-type: none"><li>4. Promote ethics and ensure that all employees are aware of corporate policies relating to acceptable use of company systems</li><li>5. Promote a good working atmosphere – value employees, listen and react to complaints, treat employees fairly and equally. Reduce the risk of having disgruntled workers.</li><li>6. Log and audit administrative access to systems</li><li>7. Review all developed code before it is deployed to a production environment</li></ol>
<p><b>Scenario 3.</b> Theft of company intellectual property (IP) for personal gain or as “revenge.”</p>
<p><b>Attack vectors.</b> Numerous types of IP that could be vulnerable to theft. Some examples</p> <ul style="list-style-type: none"><li>- Information about mergers and acquisitions revealed or sold to a third party that has conflicting interests – data possibly compromised from a network share where access permissions have not been correctly set.</li><li>- IP sold for profit or because of a grudge by somebody who has legitimate access to the data</li><li>- Copy of a customer database copied to USB memory stick by an individual with legitimate access, and auctioned for sale on an “underground” Internet bulletin board</li><li>- Source code for an online product developed and paid for by AW plc copied by a developer and re-used for a personal or other commercial project</li><li>- Word document containing employee contract data attached to a personal email account (e.g. Hotmail) and sent to an unauthorised third party</li></ul>
<p><b>Likelihood.</b> There is a high likelihood of such an event, with plenty of empirical evidence to support.</p>
<p><b>Controls.</b></p> <ul style="list-style-type: none"><li>- Directory permissions – “need to know” access principles</li><li>- Security awareness education for all employees</li><li>- Use of encryption and password protected documents</li></ul>

<ul style="list-style-type: none"> <li>- Blocking file upload access to non-corporate online resources</li> <li>- Formal change control process for all code moved into production environments</li> </ul>
<p><b>Scenario 4.</b> Fraudulent use by an employee of credit card data held within AW plc databases or manual systems</p>
<p><b>Attack vector.</b> Credit card data is handled or accessible by a relatively high proportion of AW plc employees. In some instances the data is received by fax, post, or telephone. In other instances the data may be stored in a database accessible to a small number of trusted individuals. In all instances the threat exists of an employee, motivated by personal gain, making dishonest use of the data.</p>
<p><b>Likelihood.</b> The presence of credit card data may be temptation for an employee with financial difficulties. Such data also has black-market trading value.. The prevalence of credit card related crime in society as a whole makes this a threat to be taken seriously.</p>
<p><b>Controls</b></p> <ul style="list-style-type: none"> <li>➤ Background, credit, and reference checks on all employees whose role brings them into contact with credit card data</li> <li>➤ Limit storage of card data and ensure that all electronic systems meet PCI compliance requirements</li> <li>➤ Do not store card data if there is no business requirement to do so</li> <li>➤ Security awareness training to remind employees on how to handle confidential data.</li> </ul>

[3] See section 2 on Safeguards/Deterrents/Attributes for offending/organisational context

Research by Willison [3] reinforces the value of security awareness and also ensuring that security responsibilities and roles are documented. Willison goes on to state the importance of deterrent controls. From an AW plc perspective this would include

- Ensuring that the consequences of actions contrary to company policy are documented and communicated
- That consequences are seen to be applied consistently where necessary across the organisation
- Communicating to employees a description of the controls that are in place for logging, monitoring and auditing

## 5. Protecting IP in China

This section is specifically focused on the challenges of operating on China and the associated risks to AW plc IP from employees.

China is singled out because of the apparent lack of regard for the security or value of IP. However, this same situation is also true of other emerging markets. The business of AW PLC is rapidly expanding within China, hence the importance of identifying IP protection as a significant business issue.

The following detail is adapted for AW PLC requirements from a paper by Greguras [5] published in the Computer Law and Security Report journal.

- i) Make IP protection a primary responsibility of the entire China management team. Everyone needs to buy into the importance of such protection.
- ii) Register IP rights in China. No patent or trademark protection is available until the patent or trademark is issued in China.
- iii) Ensure separation of duties to ensure that no single individual has access to a complete set of data but can only see the information that they need in order to perform their job.
- iv) Conduct regular security audits. Check the security processes (physical and electronic), policies and training, employee retention rates and financial status of a third party service provider. Training should include on IP protection. *NB. An undercapitalized service provider is more likely to cut corners on IP protection practices.*
- v) Perform reference checks on management and key employees.
- vi) Have employees sign confidentiality agreements.
- vii) Have third party service providers' sign contracts that contain assignments of ownership, rights to audit and waivers of moral rights. Make sure such contractors have the proper contracts in place with their employees to implement the company-to-company contract.
- viii) Conduct regular audits third party service providers to look for vulnerabilities that are causing or could cause IP leakage.
- ix) Keep a close watch on departing employees and the competition to detect IP leakage. Implement a practice of departure interviews and a written reminder to departing employees to remind them of their obligations.

## 6. Conclusions

The insider risk to AW plc is something that must be taken into account in terms of the potential impact in the event

- That private data were to be compromised, misused or sold for personal gain
- Of critical systems being sabotaged
- Fraud were to be perpetrated by an employee

This document has discussed numerous scenarios and described some of the controls that might be effective. What is clear from reading details of the acts described in Appendix B is that the insider risk is very real and causes damage to businesses on a frequent basis. AW plc is a business that exhibits factors known to increase risk. More specifically those being a high staff turn-over, rapidly changing work environment, and operations on a global scale.

## *Recommendations*

To end this document, the following are my own recommendations to apply to AW plc. Given the nature of the organisation there is likely to be a difference in how the recommendations are applied across some of the diverse cultural environments in which AW PLC operates.

1. Actively promote security awareness, in native languages, with an emphasis on data protection and corporate ethics.
2. Ensure that a formal employee leaver process is applied across the organisation to ensure that user accounts are disabled as soon as possible after an employment contract is terminated.
3. Regularly verify access controls around network directory shares that contain confidential data
4. Ensure that change control processes across network infrastructure and software development environments are rigorously followed
5. Ensure that references are followed up for all contract and permanent employees
6. All contract and permanent employees to sign confidentiality agreements
7. Records of incidents that relate to the insider threat to be collated and regularly reviewed

## 7. Appendix A - Checklist

Here is a checklist of questions [7] that point to best practices for managing insider threats. This is a straight quote from the cited document.

1. Does the organization's established policies and actual practices exhibit a real caring for the well-being, safety and security of the work force? If they don't, how do you expect to elicit loyalty?

2. Does your organization offer competitive salaries and benefits packages for your industry and region? If not, there is extra incentive to cross the line into criminality.
3. Does your organization incorporate the evaluation of an employee's compliance with security policies, standards and procedures into annual performance reviews? There is no more compelling way to communicate the importance of such compliance than to tie it to compensation.
4. Are all newly hired employees provided with an introductory presentation on what is expected of them in regard to security, and is it followed with periodic reminders and appropriate training? And if so, are they required to sign-off on having received this training and acknowledging its importance? Such measures go a long way in removing the "I did not know I was breaking any laws or violating any corporate policies" excuse as either a legal defense or psychological rationale. It also lets them know up front that you are conscious, and that you are watching.
5. Does your organization cover employees responsible for handling sensitive or secret information with some sort of fidelity bond or other insurance?
6. Does your organization inquire into the background of potential employees (e.g., academic, personal and professional references) in more than just a rudimentary way? In other words, if there is something that doesn't add up in the person's stated job history, do alarms go off? Does your organization go further with due diligence on potential employees who will be entrusted with vital roles (i.e., solicit thorough, independent background investigations).
7. Does your organization have an effective way to promptly and efficiently eliminate the user IDs (both cyber and physical) of people who have retired, been terminated or hired away, or otherwise left the firm?
8. Does your organization issue tamper-resistant ID badges that include a photograph, and a unique number (e.g., employee number), and require that they are worn by employees at all times?
9. Are business partners, vendors, third-party contractors, etc. who will be on-site for extended periods of time issued and required, like all employees, to wear tamper-resistant ID cards that include a photograph, and a unique number?
10. Does your organization conduct exit interviews, with employees who are being terminated, to ensure that the person returns all laptop computers, cellular telephones, smart cards and other equipment, as well as files (both paper and electronic), keys, ID badges, etc. that are the property of the organization?
11. Are terminated employees immediately escorted from the premises? Is their network and information access immediately cancelled? Are they prohibited from returning physically or virtually?
12. When employees take annual vacations or are otherwise absent with minimal network access, does your organization take advantage of the opportunity to expose unauthorized activity?

13. Does your organization provide detailed job descriptions, which includes an unambiguous statement concerning related security responsibilities, to all employees who access information systems or other communications resources?
14. Does your organization's information security team have a mission statement, which has been published, made visible to all employees, and is endorsed by the executive leadership?
15. Is there a single individual within your organization who is responsible for information security throughout the enterprise?
16. Do your organization's employees, and other responsible individuals, e.g., third party contractors working on-site, know how to properly report security vulnerabilities, suspicious behaviour or possible breaches of law or corporate policy?
17. Is your organization willing to seek the prosecution of employees, or others, who it believes to have consciously committed a crime?
18. Does your organization maintain adequate expertise on staff (established via training, professional certifications, etc.) to provide executive leadership and investigative authorities with actionable information concerning activity on its networks and information systems?
19. Have all your employees and relevant third-party personnel signed confidentiality agreements, and are copies of these agreements maintained appropriately?

## 8. Appendix B – Incident Examples

The following incidents are reported in the Carnegie Mellon Insider Threat Study, May 2005. There is no similarly detailed report for UK businesses.

**A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software. Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the critical software from the company's server. The company estimated the cost of damage in excess of \$10 million, which led to the layoff of some 80 employees.**

*An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's web pages, changing text and inserting pornographic images. He also sent each of the company's customers an email message advising that the website had been hacked. Each email message also contained that customer's usernames and passwords for the website. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords and changed 4,000 pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay \$48,600 restitution to his former employer.*

**A city government employee who was passed over for promotion to finance director retaliated by deleting files from his and a coworker's computers the day before the new finance director took office. An investigation identified the disgruntled employee as the perpetrator of the incident. City government officials disagreed with the primary police detective on the case as to whether all of the deleted files were recovered. No criminal charges were filed, and, under an agreement with city officials, the employee was allowed to resign.**

### **Negative Work-Related Events**

After more than four years of successful service marked by stellar performance reviews, management commendations, and nomination for the organization's executive training program, a female employee filed multiple complaints with human resources against her male supervisor and male coworkers. She claimed her coworkers had made sexual remarks, overridden her technical decisions regarding databases (an area in which she was considered an expert), and contacted her team's contractors regarding her projects without her knowledge. No action was taken by human resources, and the actions by her coworkers continued. The employee's performance reviews declined sharply in the next two years, and she was demoted. Subsequent complaints to her supervisor resulted in a suspension for insubordination. Almost a year following her written complaint to human resources, she resigned and began employment with another

organization. Two months later, she learned that only her more recent, negative performance reviews had been forwarded to her new employer. She used one of several shared DBA accounts to delete critical table spaces in the organization's Oracle database, deleting crucial data. Due to a coincidental problem with database backups during the same time period, 115 employees had to spend 1800 hours to recover and re-enter the lost data.

**A company disabled access for a software engineer just prior to his firing. However, he had logged into the system from home earlier in the week and maintained his connection. After being terminated, he went home to find his remote connection still open. His remote access had been disabled so he could not make any new connections, but he used the existing open connection to delete several critical files from the company's manufacturing application. The company lost over four hours of manufacturing time and had to load backup data to restart the manufacturing process.**

*A temporary employee with system administrator access applied for a permanent position and was rejected. He reacted with an angry email and was dismissed as a result. However, the organization did not change the system administrator passwords. This enabled him to log in and delete accounts, change passwords, and clear the security logs.*

A shared account was used to manage a company's voice mail system. The account required a password for administrative access. Upon the departure of one of its employees, the company overlooked changing the password of the account. The terminated employee, who possessed that password, used the password to enter the account and make changes that directed certain customers to a pornographic telephone service.

**A fired employee had privileged access to the company's collaborative workspace application, which was used to maintain clients' websites. Although his access was disabled upon termination, employees in his group typically shared their passwords among the team for testing purposes. Because of this, he was able to log into the application following his termination using his supervisor's username and password. Having done so, he made malicious, embarrassing changes to the content of their clients' websites – particularly the "high-profile" clients.**

A contractor was able to gain physical access to the organization's Network Operations Center where consoles were left logged in as root with no password-protected screensavers. He then deleted system files, a database, and all software from three of the company's servers, resulting in over two hundred thousand dollars in damage.

## **Denying Physical Access to Terminated Employees**

An insider with system administrator privileges was terminated from a cancer research project that used a single, stand-alone computer. His physical access to the building was immediately disabled. However, he returned to the building after normal working hours, and when his access card denied him entry, another employee let him into the building believing that the insider's access card had malfunctioned. The insider then deleted 18 months of data from the cancer research on which his office had been working.

### **Lack of Fine-Grained Access Control and Separation of Duties**

A programmer was given system administrator access even though system administration was not his responsibility. He used that access to plant a logic bomb on the organization's network that interrupted customer access to the organization's systems.

### **Lack of Separation of Duties or Two-Person Rule**

The sole system administrator at an organization terminated his employment without warning and refused to divulge the administrator passwords until they met his financial demands. Furthermore, he proceeded to change the passwords for all user accounts, preventing anyone in the organization from logging into any of the company's systems. Next, he changed the IP address of its web server so no one could access its website. Finally, he created a backdoor account for later use. After revealing the administrator passwords to the organization two days later, he utilized that backdoor account to run a password sniffer on the organization's network.

### **Absence of Procedural and Technical Controls for System Administrators**

A UNIX network administrator was reprimanded for behavioral issues; his computer accounts and remote access were then disabled. He returned the following business day to turn in his letter of resignation. Before doing so, however, he gained physical access to restricted workstations, logged in as root, and planted a time bomb that deleted all of the files on three company servers several days later. Recovery required the assistance of an outside consultant for five days. Two days following their recovery, the servers were again sabotaged in the same manner. On their second visit, the consultants discovered a destructive script on three of the company's UNIX file servers that was scheduled to run at 3 a.m. every Wednesday. The company estimated the total loss sustained by the business due to the incident at \$237,550. During the investigation, the company learned from a coworker that he and the insider had discovered a backdoor on twenty restricted workstations. On any of those workstations they could gain root access. Because of the trusted host system configuration, they could then access any of the organization's file servers as root.

### **Undetected Use of Sophisticated Attack Tools and Methods**

An insider used a toolkit to install unauthorized backdoors on his employer's systems. These backdoors allowed the insider to gain remote access to the system after his termination, delete the computer accounts of several company executives, change passwords, and clear security logs to conceal his actions.

### **Use of Backdoor Accounts**

One insider, while employed at the victim organization, created VPN accounts for his supervisor, the Chief Financial Officer, and the vice president of sales, but never told them. After his termination, he used those accounts to gain remote access to the system, logging in undetected for two weeks before using them to commit his attack.

### **Physical Sabotage to Harm Electronic Assets**

A well respected employee who prided himself on his outstanding reputation in the company sabotaged the project on which he was working to disguise the fact he was failing to meet his own deadlines. He terminated processes, reformatted disks and cut computer cables, all of which caused failure of the servers on which the company ran its tests of the project.

### **Social Engineering**

An insider used a combination of coercion and intimidation to convince the human resources (HR) manager to give him the only backup tape for the organization's mission critical software,

even though the HR manager was involved in the pending firing of the employee. This action amplified his later attack, when he successfully deleted the software from the production systems.

### **Danger of No Software Characterization or Configuration Management**

An insider modified his employer's premier product, an inter-network communication interface, to insert the character "i" at random places in the supported transmission stream and during protocol initialization. The malicious code was inserted as a logic bomb set to detonate more than six months after the insider left the company.

### **Use of Remote Access with Undetected Precursor Activity**

A computer technician sabotaged a number of customer systems installed by his company. First, he accessed five of the customers' systems using remote access from his home. He replaced the company's programs on the customer systems with new executables that would not run. Second, he planted a boot virus on the systems so that a reboot would render them useless. As planned, the customers could not run the program the next morning, rebooted their computers, and lost the programs completely. As a result, retail operations were shut down at two of the customer sites for two days and his organization's IT staff had to fly to each customer site and spend several days recovering the systems. The investigation showed that he had unsuccessfully attempted to access one of the customer systems remotely on three different occasions prior to the attack.

### **Altering System Logs to Cast Suspicion on Someone Else**

An insider responded to a network disruption, diagnosed the problem, and brought the network back up fairly quickly. At the same time, however, he framed his supervisor by manipulating the system log. First, he downloaded a logic bomb script onto his organization's system, next he created a fictitious entry in the network log falsely showing that his supervisor had downloaded the logic bomb. Although the logic bomb never detonated, he used the presence of the logic bomb and the fictitious log as evidence to implicate his supervisor in the network crash.

### **Danger of no Technical Controls for Protecting System Logs**

An insider was able to insert a malicious code into programs created by his organization and concealed his identity by turning off security settings and erasing log files.

## 9. References for this document

[1] Richard Walton and Walton-Mackenzie Limited, Balancing the insider and outsider threat, *Computer Fraud & Security* Volume 2006, Issue 11, , November 2006, Pages 8-11.  
(<http://www.sciencedirect.com/science/article/B6VNT-4MF2VRX-6/2/8fe22d33787813f4dacd93be3d9a3d94>)

[2] DTI/PWC. (2006). *Information security breaches survey*. London: PWC.

[3] Robert Willison, Understanding the perpetration of employee computer crime in the organisational context, *Information and Organization* Volume 16, Issue 4, , 2006, Pages 304-324.  
(<http://www.sciencedirect.com/science/article/B6W7M-4M69JP8-1/2/450e3bfafbd6c50cfebab3690919212>)

Keywords: IS security; Criminology; Employee computer crime; Perpetration

[4] G. B. Magklaras and S. M. Furnell, Insider Threat Prediction Tool: Evaluating the probability of IT misuse, *Computers & Security* Volume 21, Issue 1, , 1st Quarter 2001, Pages 62-73.  
(<http://www.sciencedirect.com/science/article/B6V8G-452D9TY-C/2/d3ce0be409d1fbb34d981e7f0cfec13>)

Keywords: misfeasor detection; insider misuse; threat prediction; misuse models

[5] Fred Greguras, Intellectual property strategy and best practices for R&D services in China, *Computer Law & Security Report* Volume 23, Issue 5, , 2007, Pages 449-452.  
(<http://www.sciencedirect.com/science/article/B6VB3-4P61NBY-2/2/f9a68a54386c9d2d22cd3c2e137e85ae>)

[6] Steven Furnell, Malicious or misinformed? Exploring a contributor to the insider threat, *Computer Fraud & Security* Volume 2006, Issue 9, , September 2006, Pages 8-12.  
(<http://www.sciencedirect.com/science/article/B6VNT-4M1VWFV-6/2/02b70b04c7b52cb456bed4efede752d7>)

[7] Richard Power and Dario Forte, Thwart the insider threat: a proactive approach to personnel security, *Computer Fraud & Security* Volume 2006, Issue 7, , July 2006, Pages 10-15.  
(<http://www.sciencedirect.com/science/article/B6VNT-4KMG66R-7/2/47ae5ba8eeb09d1e486075473083baa6>)

[8] David Porter, Insider Fraud: Spotting The Wolf In Sheep's Clothing, *Computer Fraud & Security* Volume 2003, Issue 4, , April 2003, Pages 12-15.  
(<http://www.sciencedirect.com/science/article/B6VNT-48BK92G-C/2/0a0337fca8ec58215c56be7aac202685>)

[9] Carnegie Mellon Insider Threat Study, May 2005,