

# The Insider Threat

Gary L. Tagg, CISSP

### NOTES FOR STUDENTS IN PROF KABAY'S CLASSES:

Scholarly papers, including student project reports ("term papers") must conform to academic standards of proper research, quotation, and referencing.

In Prof Kabay's classes, You are NOT required to use a particular style for your references or for your headings - just be consistent within your document.

You do, however, need a reference for every assertion of fact. Prof Kabay recommends footnotes because they cannot be confused with parenthetical comments. Do NOT put bibliographic details in a footnote: those belong in the Works Cited section, which is generated automatically when you use proper bibliographic functions.

This document, originally submitted as a chapter for the 6<sup>th</sup> Edition of the *Computer Security Handbook*\* (for which Prof Kabay was the technical editor) illustrates options for documenting substantive assertions using footnotes and citations based on a bibliographic database such as the **WORD References | Manage Sources** tool or the **EndNote** tools.

For more guidance, see also

- "CATA: Computer-Aided Thematic Analysis,"
- "On Writing,"
- "Tips for Using MS-WORD Effectively," and
- "Frequently Corrected Errors" on the Methods page at

< <http://www.mekabay.com/methodology/index.htm> >

---

\* Bosworth, S., M. E. Kabay, & E. Whyne (2014), eds. *Computer Security Handbook*, 6th Edition. Wiley (ISBN 978-0471716525). 2 volumes, 2240 pp.  
AMAZON < <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/> >

# The Insider Threat

---

## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2</b>	<b>THREATS FROM INSIDERS .....</b>	<b>5</b>
2.1	HOW COMMON ARE INSIDER ATTACKS? .....	5
2.2	EXAMPLES OF INSIDER ATTACKS .....	6
2.3	TYPES OF INSIDER THREATS .....	7
2.3.1	<i>Accidental Threats</i> .....	7
2.3.2	<i>Malicious Threats</i> .....	8
2.3.3	<i>Non-Malicious Threats</i> .....	9
2.4	INTERNET-BASED SYSTEMS .....	9
2.5	SERVICE-PROVIDER THREATS.....	10
2.6	SYSTEM-ADMINISTRATION THREATS.....	10
<b>3</b>	<b>MITIGATING THE INSIDER THREAT .....</b>	<b>11</b>
3.1	SYSTEM AND ASSET INVENTORIES.....	11
3.2	DATA-LOSS PREVENTION (DLP) .....	11
3.2.1	<i>Email Data Leakage</i> .....	12
3.2.2	<i>Data Leakage using Cloud Storage</i> .....	12
3.2.3	<i>Difficulties with DLP</i> .....	12
3.2.4	<i>Legal issues with DLP</i> .....	12
3.2.5	<i>Remote-Access Solution</i> .....	13
3.3	INTERNAL HONEYPOTS .....	13
<b>4</b>	<b>CONCLUDING REMARKS .....</b>	<b>14</b>
<b>5</b>	<b>WORKS CITED.....</b>	<b>15</b>
<b>6</b>	<b>FOR FURTHER READING.....</b>	<b>17</b>

# The Insider Threat

## 1 INTRODUCTION

An insider is someone who has been given a role within your organization and has access to premises, and/or internal systems and information. There are many types of roles, some are core to the business and performed by employees, whilst others are non-core and contracted out to service providers such as cleaning, maintenance, or information technology (IT).

Figure 1 provides a summary of insiders which are then discussed in following sections.

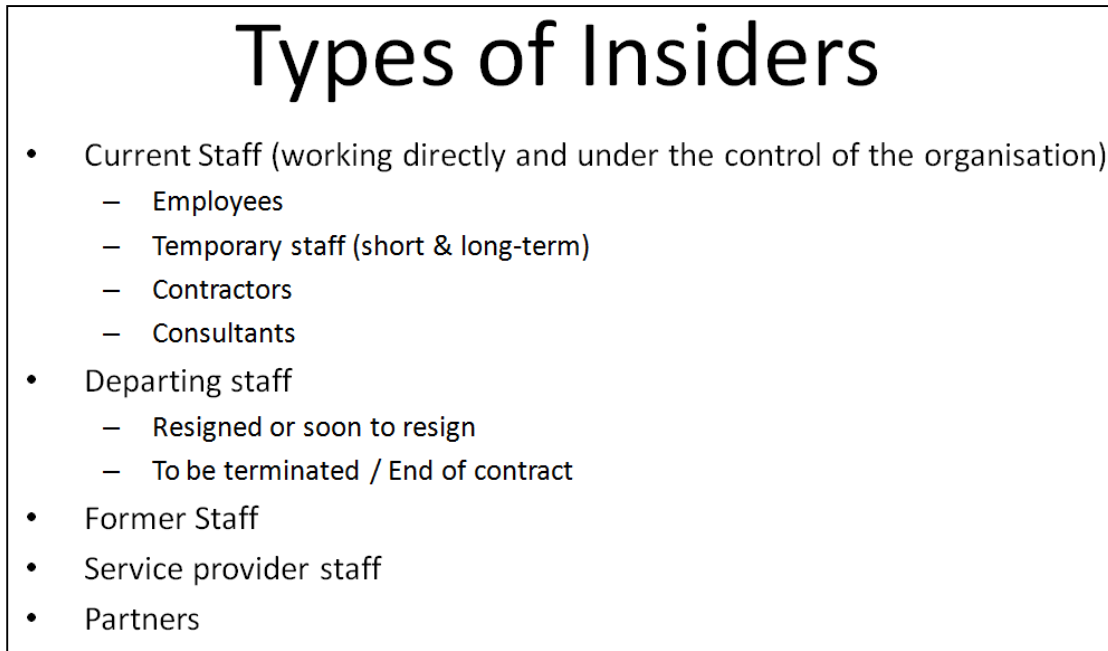


Figure 1.1 Types of insiders

*Current staff* work directly for and under the control of the organization's management. This category includes employees as well as temporary staff, contractors and consultants. Most of these people are located on the organization's premises and are connected to the internal network with access to internal information.

*Departing staff* represent one of the highest risks to an organization. These people consist of employees who have or are planning to resign, temporary staff, contractors or consultants coming to the end of their contract, as well as all the people whose employment or services are being ended by the organization. These people still have access to internal information, and may be motivated to take that information with them when they leave or to commit sabotage in revenge for perceived wrongs.

*Former staff* are those that are no longer employed by or providing services to the organization. This group still has their insider knowledge, and without mitigating controls they can do substantial damage long after they have left the organization. Former staff can be highly motivated to attack their former employers.

*Service-providers:* Organizations have many roles that are necessary for the smooth running of the business but that are not core to the company's mission. Examples of these roles are cleaning services, maintenance and IT. Over the last 20 years, service providers have steadily moved up the service stack to perform core functions as well. It is now common for service providers to perform business operations and even to be the first point of contact with customers. Although not all service providers will need access to premises or internal systems, there are many roles that do.

The key distinction between service providers and staff is that staff (who can be provided by service providers), are working under the control of the organization's management and

## The Insider Threat

---

subject to its policies and procedures; in contrast, service providers are providing a specified service and all personnel are the responsibility of the service provider. This situation increases risk to the organization as they have little control over service-provider staff, but the threats are the same as from internal staff.

Partners: Organizations are partners when they work together on a business venture. Access to information goes up to senior business leaders within the partners. Partnerships may be short or long term, and partners may be competitors at the same time as being partners. This situation creates risk for the organization, which has to share information relevant to the partnership but not other internal information.

The term *partner* is sometimes used where service providers are performing key functions for an organization and success of the service is essential. For these key contracts it is good practice to treat the service provider more like a partner than a vendor, but for insider threat purposes they are service providers.

## 2 Threats from Insiders

Successful organizations need to have people in many different roles, with the primary distinction between business roles (business management, sales, customer services & product design) and support/infrastructure roles such as IT, finance, logistics, human resources, etc.

The people in each role need access to information and systems to perform their role, and the key point to make at this stage, is that the impact on the organization of an insider attack is related to the role. A salesman leaving an organization to join a competitor will have had access to customer and product related information, whereas someone in product design is likely to have access to valuable intellectual property on current and future products. Customer Service center staff are likely to have access to customers' personally identifiable information (PII) that can be used to commit identity fraud.

IT is a high risk area, and is essential to the efficient running of the business. Most of an organization's information is stored in its IT systems, and without proper controls, IT administrators could have access to everything.

### 2.1 How common are Insider Attacks?

According to the 2011 CyberSecurity Watch Survey<sup>1</sup>, 21% of electronic crime events were conducted by insiders, with 58% by outsiders, and 21% unknown. Of the insider events, 76% were dealt with internally without legal action or law enforcement, which is likely a reason that external attacks are more often in the news.

The 2012 UK *Information Security Breaches Survey*<sup>2</sup> provides some interesting statistics.

- 6% of the responding 447 organizations reported staff sabotage of systems, with some organizations experiencing incidents on a weekly basis
- 19% of large organizations reported that staff used systems to commit theft or fraud, and this figure had doubled since the survey in 2010
- With regard to other incidents caused by insiders, large organizations were more likely to experience incidents, with 82% reporting incidents versus 45% for small organizations
- 61% of large organizations reported unauthorized access to systems or data
- 45% reported a breach of data protection laws or regulations
- 36% reported misuse of confidential information
- 47% reported loss or leakage of confidential information.

The 2013 UK *Information Security Breaches Survey*<sup>3</sup> includes the following relevant information for this chapter (quoting directly from the Executive Summary – note UK spelling):

- 36% of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff)
- “57% of small businesses suffered staff-related security breaches in the last year (up from 45% a year ago)”
- “17% of small businesses know their staff broke data protection regulations in the last year (up from 11% [in the 2012 report])”

---

<sup>1</sup> (CMU/SEI 2011)

<sup>2</sup> (PwC 2012)

<sup>3</sup> (PwC 2013)

# The Insider Threat

---

- 14% of large organisations had a security or data breach in the last year relating to social networking sites
- 9% of large organisations had a security or data breach in the last year involving smartphones or tablets
- 4% of respondents had a security or data breach in the last year relating to one of their cloud computing services
- 4% of the worst security breaches were due to portable media bypassing defences.

## 2.2 Examples of Insider attacks

To get an understanding of the types of insider events, a number of organizations maintain databases and publish results. The FBI maintains an *Insider Threat* page on their Website<sup>4</sup> containing a list of prosecuted insider theft cases. A short summary of these cases follows:

- Retired research scientist conspired with current and former employees to steal trade secrets from his former employer, and sell them to companies in China.
- Employee working for two different US companies stole trade secrets from both companies which were used to benefit Chinese Universities.
- A research scientist stole trade secrets from her employer and made them available for sale through her own company.
- An employee stole customer and employee lists, contract information and other trade secrets to provide to a foreign government, but instead gave them to an undercover FBI agent.
- A computer programmer working for a financial firm copied proprietary software during his last few days at the company.
- An employee who was fired had kept copies of trade secrets. These trade secrets were then sold to a rival company.
- An employee stole and attempted to sell trade secrets that provided everything needed to start a competing business.
- Over a two-day period, an employee copied hundreds of technical documents from her employer which were found in her luggage during a check at the airport.
- Spies working for US defense companies stole internal information about the space shuttle, Delta IV rocket, the C-17 military plane, submarine propulsion systems along with other information. This information was provided to the Chinese government.

In a summary of the “Top Five Insider Attacks of the Decade,” the Linux.com editorial board listed the following cases:<sup>5</sup>

- Roger Duronio was convicted in 2006 to eight and a half years in federal prison<sup>6</sup> for his actions in 2002 when, apparently in a fit of pique at not receiving what he considered an adequate annual bonus, he sabotaged the computer systems of his employer, UBS PaineWebber. “UBS was hit on March 4, 2002, at 9:30 in the morning, just as the stock market opened for the day. Files were deleted from up to 2,000 servers in both the central data center in Weehawken, N.J., and in branch offices around the country. Company representatives never reported the cost of lost business but did say it cost the company more than \$3.1 million to get the system back up and running. Duronio worked at UBS as a systems administrator until he quit a few weeks before the attack. Witnesses testified that he quit because he was angry that he didn't receive as large an annual bonus as he expected. Investigators

---

<sup>4</sup> (U. S. Federal Bureau of Investigation 2014)

<sup>5</sup> (Linux.com Editorial Staff 2011)

<sup>6</sup> (Gaudin, Ex-UBS Systems Admin Sentenced To 97 Months In Jail 2006)

# The Insider Threat

---

found copies of the malicious code on two of his home computers and on a printout sitting on his bedroom dresser.”<sup>7</sup>

- In 2005, a sting operation by a *The Sun* reporter from Britain netted him confidential details of more than a thousand “...accounts, passports and credit cards ...” from NatWest and Barclays banks. led to investigations of call centers in India when criminals “...boasted of being able to provide details of as many as 200,000 bank accounts in a month, which, he further said, came from more than one call center.”<sup>8</sup>
- The “Athens Affair” was discovered when investigators looked into the apparent suicide of an electrical engineer, Costas Tsalikidis, in his Athens apartment. The inside job by Tsalikidis, the head of network planning, and unknown others compromised the Vodafone-Panafon company (“Vodafone Greece”) using malware and may have resulted in monitoring and recording of conversations involving “...the prime minister, his defense and foreign affairs ministers, top military and law-enforcement officials, the Greek EU commissioner, activists, and journalists.”<sup>9</sup>
- San Francisco network administrator Terry Childs locked other employees out of the city’s network in July 2008 because he claimed that his supervisor was unqualified to have administrative control. He was sentenced to four years in California state prisons. “Prosecutors characterized the former network administrator as a power hungry control freak who couldn’t be managed.”<sup>10</sup>
- Bradley Manning, a 22-year-old US Army intelligence analyst, was arrested in May 2010 and charged in July 2010 with leaking nearly half a million classified US videos and cables to the WikiLeaks project.<sup>11</sup> He was charged with “aiding the enemy” in February 2012<sup>12</sup> and accused of aiding the terrorist group al-Qaida through his actions.<sup>13</sup> In January 2013, the trial was rescheduled until June 2013<sup>14</sup> and Manning was denied the opportunity to justify his actions using a whistleblower defense.<sup>15</sup>
- *The Sunday Times* reported in 2012 that “Confidential personal data on hundreds of thousands of Britons is being touted by corrupt Indian call centre workers, an undercover investigation has discovered. Credit card information, medical and financial records are being offered for sale to criminals and marketing firms for as little as 2p.” Records of 500,000 Britons were apparently for sale, many of which were supposedly less than 72 hours old and included “...sensitive material about mortgages, loans, insurance, mobile phone contracts, and Sky Television subscriptions....”<sup>16</sup>

## 2.3 Types of Insider Threats

There are three main classifications of insider threats: accidental, malicious and non-malicious.

### 2.3.1 Accidental Threats

Accidental threats are generally caused by mistakes; for example, staff may not follow operating procedures through careless or disregard for policies or due to a lack of training and

---

<sup>7</sup> (Gaudin, Ex-UBS Sys Admin Found Guilty, Prosecutors To Seek Maximum Sentence 2006)

<sup>8</sup> (SiliconIndia News 2005)

<sup>9</sup> (Prevelakis and Spinellis 2007)

<sup>10</sup> (McMillan 2012)

<sup>11</sup> (McGreal 2010)

<sup>12</sup> (McVeigh 2012)

<sup>13</sup> (Associated Press 2012)

<sup>14</sup> (Gabbatt and Pilkington 2013)

<sup>15</sup> (Pilkington 2013)

<sup>16</sup> (Gardner 2012)

# The Insider Threat

---

awareness of the right thing to do. An example is a customer service representative who accidentally breaches client confidentiality by emailing client information to the wrong email address. Such errors may be caused by the use of email clients that have an auto-complete feature on the email address; staff under pressure to keep up with the volume of work may not notice the error before they send the data. This error is a particularly high risk for financial services organizations where in some jurisdictions a client confidentiality breach is a criminal offence.

Other typical examples include a database administrator who accidentally deletes a database table during maintenance, a systems administrator allowing a programmer to modify a production system without proper approvals, or an operator reformatting a disk drive without having two full, verified backups.

## 2.3.2 Malicious Threats

Malicious threats deliberately try to damage the organization or to benefit the attacker. Disgruntled IT administrators can sabotage IT systems, bringing an organization to a halt. There have been many incidents where both current and former administrators have deliberately caused system issues for various motives. These motives vary from enjoying the lifestyle of travelling around the world in luxury to fix the problems they created, extorting money from the organization, or simply to cause as much damage as possible.

Some company information is highly valuable and specifically targeted by attackers. PII is one category that is sometimes illegally copied by staff to conduct identity theft and fraud, or to sell it to criminals. Another category is intellectual property (IP) such as trade secrets. Staff may take this information to help them with their next job or to sell to competing companies. This crime is thought to be common with IT developers who often seek to take their source code with them. Industrial espionage sponsored by rival companies or foreign governments is another common threat to IP (see Chapter 11 in this *Handbook* for examples).

Information can leave an organization by being copied to removable storage such as USB Flash or hard drives and CD/DVD-Writers. Portable 3TB drives are now readily available, which means entire databases can be copied to a drive measuring less than 7x5 inches in size. With gigabit Ethernet becoming standard, the time required to copy this data is rapidly decreasing. Other common channels include emailing attachments to external email addresses, uploading files to external email services and to Internet Websites, and using cloud backup and cloud storage tools. To address these data-leakage channels, products known as data-loss prevention (DLP) systems are increasingly being installed in organizations.<sup>17</sup>

There are also the common physical threats such as taking printed information from people's desks or from the office printers. Where logical access controls are strong, staff intent on stealing information can take photographs of documents or information on screen with the high resolution cameras in today's mobile phones.

There are some incidents where the motive may be conscience based as well as a desire to damage an organization. Since the financial crisis in 2008, governments have increased their efforts to reduce tax avoidance, and are aggressively pursuing the use of foreign tax havens. There have been a number of publicized incidents where insiders have provided lists of offshore clients and accounts to country tax authorities<sup>18,19</sup>.

---

<sup>17</sup> (Ouellet 2013)

<sup>18</sup> (BBC 2012)

<sup>19</sup> (BBC 2011)



# The Insider Threat

---

## 2.3.3 Non-Malicious Threats

Non-malicious threats are actions taken deliberately by people without intent to damage the organization. Often, the motive is to increase productivity, and the mistakes occur due to a lack of training or awareness of policies, procedures and the risk. There have been many incidents where staff have loaded internal information onto Internet based systems, some of which have no access controls. This error makes the information available to anyone who uses the sites and is often found and indexed by search engines.

One incident occurred in the early days of cloud computing. A drug researcher was given a lengthy lead time by his internal IT department for the delivery of infrastructure to conduct simulations. What he did instead was use his credit card to buy time on cloud-based systems and ran the simulations there instead. This put valuable intellectual property at risk had these Internet systems been compromised. This information was also sitting on the cloud provider's storage systems; what if the cloud vendor were to fail to reinitialize the storage when reallocating released storage to another customer, and the next user of the storage were to understand the value of what came pre-loaded on their system – and be dishonest?

Another example that is often reported in the media is the loss of PII when staff copy information to laptop computers or to removable storage devices such as USB drives or CDs/DVDs, which are then lost or stolen<sup>20</sup>.

One common insider threat that can be done for both malicious and non-malicious reasons is to email internal information to their home email address. Once on the staff member's own computer, the information is vulnerable to theft, successful attack on the computer or email account, or recycling of the machine by donating it to charity, or giving it away to family or friends. There have been many media reports of people finding sensitive information on secondhand computer hard disks.<sup>21</sup>

The non-malicious motive is often to enable the employee to work from home, or the information is needed for a business trip. The malicious motive is to take the information with them, for reasons covered earlier.

## 2.4 Internet-Based Systems

The growing trend to use outsourced applications available over the Internet rather than internal systems can contribute to insider crime. With internal systems, when someone leaves an organization, they no longer have physical access to premises, and their network and application user-ids are supposed to be disabled immediately, removing access to corporate networks, computers and applications. Appropriate action makes it difficult for even maliciously motivated former staff to access confidential systems and their information.

But with Internet-based systems, the former staff member may still have access to confidential data via any Internet connection. It is very difficult to ensure all application accounts are promptly closed when someone leaves, creating a high risk of continued access to these systems. The people concerned may be deterred by the risk of being prosecuted for misusing their rights after leaving the organization, but their risk can be reduced if they use a former colleague's log-on account.

Organizations don't have to avoid using these external services; indeed, these external services are often among the best available, and can be provided at a much lower cost to hosting it internally. However, security officers must coordinate closely with their human resources departments and the IT people responsible for maintaining the lists of external

---

<sup>20</sup> (BBC 2008)

<sup>21</sup> (BBC 2009)

# The Insider Threat

---

providers to ensure that access by former employees to external services is shut down as quickly as access to internal systems.

## 2.5 Service-Provider Threats

Even organizations with strong personnel controls that reduce the risk from internal staff may have no protection from external service-provider staff. Although organizations commonly include their policies, standards and procedures into contracts and treat this precaution as sufficient to address risk, the service provider may not consistently perform all the required controls, either through attempts to maximize profit or through poor management.

For example, a service provider faced with high staff turnover might bypass pre-employment checks to get replacement staff quickly onto a service, particularly, if there are service performance issues. Similarly, poor standards for handling termination of employment at the service provider could lead to compromise of clients.

In cases where an entire IT service is being provided by a service provider, the service provider's staff and IT administrators may have access to all the client organization's information. Email is a particular risk which may contain a great deal of an organization's intellectual property and which has powerful search facilities to easily target individuals and specific information.

## 2.6 System-Administration Threats

System administrators have privileged access to an organization's IT infrastructure and, in poorly managed systems, may have access to critical and sensitive information on the systems. System administrators may deliberately attack the availability of an organization's systems even if they cannot access the data themselves. Administrators may destroy individual data sets, applications, or entire systems and networks -- and may be able to destroy system backups to make the organization's recovery more difficult. This risk is most acute in smaller organizations where one person may do everything from managing the servers, applications, networks, email, backups, and perhaps even user administration. In larger organizations it is much easier to segregate these roles as they should be, to limit the access and damage one person can cause.

Even in large organizations with thousands of servers with effective segregation implemented, an administrator may be able to submit a job that can be run simultaneously on every server to wipe every hard disk. This type of threat highlights the importance of controlling the access and scope administrators and preventing unauthorized changes from being implemented.

## 3 Mitigating the Insider Threat

This section describes at a high level a few of some specific mitigating controls and how they address the insider threat.

For more details on the wider range of controls, refer to the detailed information in other chapters in this *Handbook* such as Chapter 15 (Penetrating Computer Systems and Networks), Chapter 28 (Identification and Authentication), Chapter 31 (Content Filtering and Web Monitoring), Chapter 45 (Employment Practices and Policies), Chapter 52 (Application Controls), Chapter 53 (Monitoring and Control Systems), Chapter 54 (Security Audits and Inspections), Chapter 55 (Cyber Investigation), Chapter 56 (Computer Incident Response Teams), and Chapter 68 (Outsourcing and Security).

### 3.1 System and Asset Inventories

If you don't know what you have you can't manage it. Without an inventory of servers you can't ensure they are patched enabling an insider to compromise them and use them for their own purposes. Without a list of applications running on each server, you may have unnecessary servers sitting on your network being used for unauthorized purposes. The active systems on the network also need to be correlated back to the inventory. An administrator who doesn't remove a redundant system in your Internet DMZ could use it to bypass all of your network perimeter controls after he has left the organization.

In particular, one of the most dangerous tools for insider crime is the unauthorized and undetected wireless access point – easily purchased from any electronic store for at low cost, and capable of transferring data from an internal network to unauthorized devices within the corporate facilities or even to external agents within a modest radius outside the building. See Chapter 33 in this *Handbook* for discussion of wireless network security.

### 3.2 Data-Loss Prevention (DLP)

There have been technology adoptions over the last 10 years which have made it much easier for staff to both accidentally and deliberately breach the confidentiality of organizational and client information. Data loss prevention (DLP) is a class of IT security system increasingly being implemented by organizations to help address these risks. A typical DLP system needs to address the following vulnerabilities at a minimum:

- Mobile storage devices/removable media such as USB memory sticks and hard drives, mobile phones, memory cards, CD/DVD writers, along with Infrared, Bluetooth, Firewire and SCSI connected storage.
- File uploads – including encrypted data – to external Websites via the standard protocols within Web browsers such as ftp, http and https. These controls may be enforced at both the Internet gateway as well as on the desktop.
- Detection of when laptops are not on the corporate network and preventing files being copied to non-corporate file shares.

For the majority of staff, the DLP system can be configured to block attempts to copy and upload data to these data-leakage channels. However, for most of these channels there are going to be some people who have a genuine business need to copy and upload information, resulting in exceptions to the policy. The DLP system can help manage this risk by creating a log of what has been copied to support incident investigation or to allow review what a staff member has copied out of the organization. These facilities can be particularly useful when an employee hands in his resignation.

# The Insider Threat

---

## **3.2.1 Email Data Leakage**

Once the low-hanging fruit of removable storage and file uploads are blocked, staff begin to export information via email. The motive may not be malicious, but it still results in the organization's losing control over the information. To address this risk the DLP system can be configured to report on people sending attachments to home email addresses, which is the usual destination for information, or to any unauthorized email address. These reports can then be used to increase staff awareness about policy or to support disciplinary processes for deliberate data leakage.

However, the true benefit from DLP comes when the business areas are engaged, because DLP can drive a process of identifying and defining the critical information that has to be protected. For example, the IT development group could have a DLP rule that blocks emails containing source code, to prevent developers taking their work with them when they leave. Even if source code is placed in an encrypted zip file to try and avoid detection, the metadata (e.g. filenames and identifiers of file creators) may still be readable and can trigger the rule.

For other areas of the business, client information, business strategy, business results, intellectual property, PII such as credit card numbers and Social Security Numbers can be configured into the DLP system.

## **3.2.2 Data Leakage using Cloud Storage**

Widespread availability of external data storage facilities (e.g., Dropbox and Google Docs) adds to the complexity of DLP. Careful application of Web monitoring and blacklisting specific URLs may be helpful, but determined opponents of the regulations may circumvent such methods using a variety of proxy avoidance Websites which mask the destination of the HTTP request. Security administrators should be on the lookout for new sites so they can add them to the corporate blacklists for outbound communications through their firewalls.

## **3.2.3 Difficulties with DLP**

DLP is not a panacea. It is difficult if not impossible to prevent someone determined to leak data, but with a DLP system, one can make it difficult for them to do so without detection, and this barrier usually deters the majority of people.

With email DLP, it is very difficult to identify safe blocking rules that prevent data leakage. For example, if employees routinely send emails to customers, some of these customers are going to be using their home email addresses, which means that a hard block (blacklisting) of emails sent to home email addresses won't be feasible.

## **3.2.4 Legal issues with DLP**

With the implementation of DLP, an organization progresses from investigating reported incidents to actively monitoring for breaches of company policy. One of the major issues with implementing a global DLP system is that active monitoring may be subject to privacy and workplace laws, and failure to comply with these laws in some countries is a criminal offence.

Additionally, with customer and organization information being captured in DLP logs, consideration needs to be given as to where the log files are stored and who will be reviewing them. As an example from the financial-services industry, some information is price sensitive and there are strict requirements on who can access it, to prevent insider dealing. Client information within the logs files may be covered under banking-secrecy laws and regulations. If the log files for one country are stored on a server in another country, then outsourcing regulations need to be complied with as well and planners must identify the most stringent regulations to ensure efforts for compliance. Data protection laws have been enacted in many countries that require data subjects to give their agreement to their information being

# The Insider Threat

---

processed and for defined purposes; therefore, monitoring of communications may need to be included in customer contracts and other data-protection declarations.

Despite all of these hurdles, for most countries, it is possible to rollout a DLP system. As part of the project planning stage the organization needs to commission a legal investigation for each country to understand whether it is lawful to actively monitor corporate email, but more important, the pre-conditions for any monitoring to lawfully take place. For countries that forbid email monitoring or any form of workplace surveillance, then it is usually possible to implement blocking controls on writing to removable storage along with uploads to external Websites, provided no log files are kept.

## 3.2.5 Remote-Access Solution

A commonly implemented remote access solution is the provision of Webmail from home PCs. With Webmail you need to configure the system to prevent staff opening attachments within local applications on the home PC. If this is not blocked then staff can copy corporate information by saving the open attachment to their local hard drive. In addition, any use of the Remote Desktop Protocol (RDP) also needs to be properly configured to prevent local USB resources being mapped to the remote computer.

## 3.3 Internal Honeypots

Honeypots are attractive systems or nodes that appear to have valuable confidential data. Roger Grimes, author of a textbook about honeypots,<sup>22</sup> writes,

One of the best things you can do to get early warning of internal attackers is to implement honeypots... because they're low cost and low noise -- and they work!

Because the internal attackers you seek could be trusted IT employees, the entire project must be kept secret. It should be known only to the sponsor, management, and the implementers. Often, we give the project a boring code name like Marketing Business Development, which is used in all documents and e-mails, avoiding terms having anything to do with honeypots. Don't even tell the network security people about it, in so far as you can and still have an operational project. Then take a few computers that are destined for de-provisioning or the scrap heap and turn them into your honeypots.<sup>23</sup>

The point of such a honeypot is that there should be zero access to it: it serves no function and there is never a reference to it in any internal or external documentation. Thus anyone who accesses it is either doing so by pure accident or is violating policies governing unauthorized access to internal data (there *is* no one authorized to access the honeypot). Detailed logging should be in place at all times to provide forensic information immediately; however, administrators should ensure that they can actually visualize exactly what is being done in real time, not simply rely on the detailed log files for after-the-fact analysis. An early-warning system should immediately alert system administrators to the problem (preferably as the access is in progress) via screen messages, voice-messages, and text messages.

---

<sup>22</sup> (R. A. Grimes 2005)

<sup>23</sup> (R. A. Grimes 2009)

## 4 Concluding Remarks

Fighting the insider threat need not be solely reactive. In addition to the entire spectrum of information assurance measures covered throughout this *Handbook*, maintaining an environment of security awareness and of encouragement, trust, fair-dealing and long-term commitment to the welfare of employees must remain among the very best approaches to reducing the risk of insider crime.

# The Insider Threat

---

## 5 Works Cited

- Associated Press. 2012. "Bradley Manning aided al-Qaida with WikiLeaks documents, military says: Manning, charged with aiding the enemy, accused of indirectly aiding terrorist group by leaking thousands of documents." *Guardian*. 15 03. Accessed 05 18, 2013. <http://www.guardian.co.uk/world/2012/mar/15/bradley-manning-wikileaks>.
- BBC. 2008. "Firm 'broke rules' over data loss: Home Secretary Jacqui Smith has blamed a private contractor for losing the details of thousands of criminals, held on a computer memory stick." *BBC News*. 22 08. Accessed 05 20, 2013. [http://news.bbc.co.uk/2/hi/uk\\_news/politics/7575989.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7575989.stm).
- . 2011. "HMRC targets HSBC Swiss accounts: The UK tax authority is targeting 6,000 UK-based Swiss bank account holders who may not have declared all their income and gains." *BBC News / Business*. 13 10. Accessed 05 20, 2013. <http://www.bbc.co.uk/news/business-15292013>.
- . 2012. "HSBC investigating claims of criminal account holders: HSBC bank says it is looking into allegations that criminals have used offshore accounts at its Jersey operation for money laundering." *BBC News / Business*. 09 11. Accessed 05 20, 2013. <http://www.bbc.co.uk/news/business-20265125>.
- . 2009. "Missile data found on hard drives: Sensitive information for shooting down intercontinental missiles as well as bank details and NHS records was found on old computers, researchers say." *BBC / News*. 07 05. Accessed 05 20, 2013. [http://news.bbc.co.uk/2/hi/uk\\_news/wales/8036324.stm](http://news.bbc.co.uk/2/hi/uk_news/wales/8036324.stm).
- CMU/SEI. 2011. "2011 CyberSecurity Watch Survey." *Computer Emergency Response Team Coordination Center*. 04 03. Accessed 05 20, 2013. <http://www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf>.
- Gabbatt, Adam, and Ed Pilkington. 2013. "Bradley Manning trial delayed until June after sentence reduction granted: Judge reschedules US soldier's trial to give more time for review of classified information related to WikiLeaks case." *Guardian*. 09 01. Accessed 05 18, 2013. <http://www.guardian.co.uk/world/2013/jan/09/bradley-manning-trial-delayed>.
- Gardner, Tom. 2012. "Indian call centres selling YOUR credit card details and medical records for just 2p." *MailOnline*. 18 03. Accessed 05 18, 2013. <http://www.dailymail.co.uk/news/article-2116649/Indian-centres-selling-YOUR-credit-card-details-medical-records-just-2p.html>.
- Gaudin, Sharon. 2006. "Ex-UBS Sys Admin Found Guilty, Prosecutors To Seek Maximum Sentence." *InformationWeek*. 19 07. Accessed 05 18, 2013. <http://www.informationweek.com/ex-ubs-sys-admin-found-guilty-prosecutor/190700064>.
- . 2006. "Ex-UBS Systems Admin Sentenced To 97 Months In Jail." *InformationWeek*. 13 12. Accessed 05 18, 2013. <http://www.informationweek.com/ex-ubs-systems-admin-sentenced-to-97-mon/196603888>.
- Grimes, R. A. 2009. "Honeypots: A sweet solution to the insider threat: A honeypot can be a cheap, easy, and effective warning system against the trusted insider gone bad." *InfoWorld*. 01 05. Accessed 05 20, 2013. <http://www.infoworld.com/d/security-central/honeypots-sweet-solution-insider-threat-922?page=0,0>.
- Grimes, Roger A. 2005. *Honeypots for Windows*. Apress. Accessed 05 20, 2013. <http://www.amazon.com/Honeypots-Windows-Experts-Voice-Grimes/dp/1590593359>.

# The Insider Threat

---

- Linux.com Editorial Staff. 2011. "Top Five Insider Attacks of the Decade." *LINUX.COM*. 13 01. Accessed 05 18, 2013. <http://www.linux.com/news/technology-feature/security/397143-top-five-insider-attacks-of-the-decade>.
- McGreal, Chris. 2010. "US private Bradley Manning charged with leaking Iraq killings video." *Guardian*. 06 07. Accessed 05 18, 2013. <http://www.guardian.co.uk/world/2010/jul/06/bradley-manning-charged-iraq-killings-video>.
- McMillan, Robert. 2012. "Network admin Terry Childs gets 4-year sentence." *NetworkWorld*. 17 08. Accessed 05 18, 2013. <http://www.networkworld.com/news/2010/080710-network-admin-terry-childs-gets.html>.
- McVeigh, Karen. 2012. "Bradley Manning defers plea after being formally charged with aiding the enemy: No date set for WikiLeaks suspect's trial but Manning's lawyer says he would object to any delay in the trial beyond June." *Guardian*. 23 02. Accessed 05 18, 2013. <http://www.guardian.co.uk/world/2012/feb/23/bradley-manning-defer-plea-charges>.
- Ouellet, Eric. 2013. "Magic Quadrant for Content-Aware Data Loss Prevention." *Gartner*. 03 01. Accessed 05 19, 2013. <https://www.ca.com/us/register/forms/collateral/Magic-Quadrant-for-Content-Aware-Data-Loss-Prevention-2013.aspx>.
- Pilkington, Ed. 2013. "Bradley Manning denied chance to make whistleblower defence: Judge rules that Manning will not be allowed to present evidence about his motives for the leak – a key plank of his defence." *Guardian*. 17 01. Accessed 05 18, 2013. <http://www.guardian.co.uk/world/2013/jan/17/bradley-manning-denied-chance-whistleblower-defence>.
- Prevelakis, Vassilis, and Diomidis Spinellis. 2007. "The Athens Affair: How some extremely smart hackers pulled off the most audacious cell-network break-in ever." *IEEE SPECTRUM*. 29 06. Accessed 05 18, 2013. <http://spectrum.ieee.org/telecom/security/the-athens-affair>.
- PwC. 2012. "2012 Information Security Breaches Survey: Technical Report." *PwC*. 20 04. Accessed 05 20, 2013. [http://bitpipe.computerweekly.com/data/document.do?res\\_id=1335274566\\_413](http://bitpipe.computerweekly.com/data/document.do?res_id=1335274566_413).
- . 2013. "2013 Information Security Breaches Survey: Technical Report." *PwC*. 17 04. Accessed 05 20, 2013. <http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf>.
- SiliconIndia News. 2005. "Indian call centers selling U.K.'s secrets." *SiliconIndia News*. 23 06. Accessed 05 18, 2013. [http://www.siliconindia.com/shownews/Indian\\_call\\_centers\\_selling\\_UKs\\_secrets-nid-28560-cid-2.html](http://www.siliconindia.com/shownews/Indian_call_centers_selling_UKs_secrets-nid-28560-cid-2.html).
- U. S. Federal Bureau of Investigation. 2014. "The Insider Threat: An introduction to detecting and deterring an insider spy." 01 05. Accessed 01 02, 2016. <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat>.



## 6 FOR FURTHER READING

Department of Defense. *DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*. DoD 2000. < <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA39138> > Accessed 2013-05-20

Noonan, T. & E. Archuleta. *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructures*. NIAC 2008. < [http://www.dhs.gov/xlibrary/assets/niac/niac\\_insider\\_threat\\_to\\_critical\\_infrastructures\\_study.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf) > Accessed 2013-05-20.

Silowash, G., D. Gappelli, A. Moore, R. Trzeciak, T. J. Shimeall, L. Flynn. *Common Sense Guide to Mitigating Insider Threats*, 4<sup>th</sup> Edition. CMU/SEI 2012. Technical Report CMU/SEI-20120TR-012. < <http://www.sei.cmu.edu/reports/12tr012.pdf> > Accessed 2013-05-20.

# The Insider Threat

---