Research Paper: Managing Insider Threat

By: Iris Cheung

Course: ACC 626
Professor: Malik Datardina

01 July 2011
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Why has insider threat become such a big issue?</td>
<td>3</td>
</tr>
<tr>
<td>Ways that insiders can attack</td>
<td>4</td>
</tr>
<tr>
<td>IT Sabotage</td>
<td>5</td>
</tr>
<tr>
<td>Fraud</td>
<td>5</td>
</tr>
<tr>
<td>Theft of Intellectual Property</td>
<td>6</td>
</tr>
<tr>
<td>National Security Espionage</td>
<td>7</td>
</tr>
<tr>
<td>The Unintentioned</td>
<td>7</td>
</tr>
<tr>
<td>Key Controls</td>
<td>8</td>
</tr>
<tr>
<td>Preventative Controls</td>
<td>8</td>
</tr>
<tr>
<td>Detective Controls</td>
<td>10</td>
</tr>
<tr>
<td>Balancing internal security and morale</td>
<td>11</td>
</tr>
<tr>
<td>Privacy issues in employee monitoring</td>
<td>12</td>
</tr>
<tr>
<td>Insider threat from trusted business partners</td>
<td>13</td>
</tr>
<tr>
<td>Growing insider threats in the financial institutions section</td>
<td>14</td>
</tr>
<tr>
<td>Conclusion</td>
<td>14</td>
</tr>
<tr>
<td>Appendix I: CERT’s model of insider IT sabotage</td>
<td>16</td>
</tr>
<tr>
<td>Appendix IIA: CERT’s model of the Entitled Independent (Part I)</td>
<td>17</td>
</tr>
<tr>
<td>Appendix IIB: CERT’s model of the Entitled Independent (Part II)</td>
<td>17</td>
</tr>
<tr>
<td>Appendix III: CERT’s model of the Ambitious Leader</td>
<td>18</td>
</tr>
<tr>
<td>Appendix IV: Controls relating to specific types of insider attacks</td>
<td>19</td>
</tr>
<tr>
<td>Bibliography</td>
<td>20</td>
</tr>
<tr>
<td>Annotated Bibliography</td>
<td>23</td>
</tr>
</tbody>
</table>
Executive Summary

Insider threat has always existed within each organization. In the recent years, insider threat has become a more prominent issue because of the emerging trends in the workplace. This change to a more flexible and productive workplace environment allows employees to easily gain access to an organization’s critical and sensitive information. While the risk of insider threat has certainly increased, organizations have not deployed enough controls to mitigate this risk either because they believe that the frequency of such threat is very low or because they feel powerless to do so. The downside of this is that more opportunities are created for insider attacks. Insiders can attack in five different ways: IT sabotage, fraud, theft of intellectual property, national security espionage and employee negligence. Organizations are advised to implement a layered defence approach to prevent and detect insider threats. Some key controls include: taking an inventory of the business’ assets, documenting policies and controls, monitoring suspicious behaviour, implementing proper access management and segregation of duties, being extra cautious with system administrators, logging and monitoring employee access, and devising a plan to respond to insider threats. While these controls will help prevent and detect insider threat, organizations must also consider the effect of these controls on employee morale and potential privacy issues that arise.

The purpose of the paper is to inform C-suite executives of the increased risks in insider threat, the different types of attacks and behaviours that these insiders exhibit and some controls that executives should use to mitigate such risks. Organizations are encouraged to revise their existing plans so that they are sufficient enough to mitigate the increased risks of insider threat.
Introduction

An insider threat is defined by the Computer Emergency Response Team at Carnegie-Mellon University (CERT) as "a malicious insider who is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information system". ¹ While insider threats may be from such malicious insiders who intentionally cause harm for their personal gain or revenge, insider threat can also be posed by trusted employees who unintentionally, through negligence, cause financial or reputational damages to the organization. According to Jeffrey Jones and Ryan Averbeck from CSO Online, there are three classes of insiders: "trusted unwitting insider, trusted witting insider, and the untrusted insider". The trusted unwitting insider is one that has appropriate and authorized access to a computer system, but lacks judgement and is careless in performing their job. For example, this type of insider may find a USB drive in the washroom and want to return it to the owner. To find out who the USB belongs to, this employee would open the USB on the company computer not knowing that this USB drive was actually left behind by a hacker who intentionally wanted to use this type of employee to install the malicious software on the network. The second type of insider is the trusted witting insider. This type of employee also has legitimate access and authorization to the company network, but intentionally chooses to provide privileged information to third parties for personal gain. This type of insider matches CERT’s definition of a malicious insider. Lastly, the untrusted insider is one who does not have legitimate access or authorization to the network. Instead, he/she has taken the credentials and role of a trusted employee.² In this paper, only the first two types of insiders will be discussed.

Insider threat has become a significant issue. There have been considerably more reported insider threat incidents over the past few years. According to the 2009 e-Crime Watch Survey in which 523 organizations were involved, 51% of the organizations experienced an insider attack, which increased from 39% three years ago.³ Since these were only reported incidents of attacks, it is likely more than 51% of organizations experience such attacks. From the recent Cyber-Ark Global Survey conducted in the spring of 2011 with 1,422 IT staff and C-level professionals, 16% of the surveyed individuals believe that insiders have stolen highly sensitive and valuable intellectual property, such as customer lists and product information, which have been transferred or sold the organizations’ competitors.⁴

From the above statistics, one can see that while insider threat has always existed in organizations, it has increasingly become a significant issue that should be better managed. Managing insider threat may be difficult as insider threats are influenced by a combination of technical, behavioural and organizational issues. This requires organizations to devise layered defence plans, consisting of policies, procedures and technical controls. The objective of this paper is to equip C-suite executives with a better understanding of insider threats, its consequences and ways to manage such threats. The paper will first explore the chief concerns about insider threats followed by the different insider attacks, some key controls that can be implemented and how to balance internal security, morale and privacy.

**Why has insider threat become such a big issue?**

Insider threat has always been present but it has become ever-so important to manage and for executives to devise a plan that will help to reduce and mitigate insider threats. Employees have endless opportunities to access company information and at the same time, steal information that is sensitive, private and valuable to an organization. There are several macro trends that have contributed to increasing the risk of insider threats. Technology has evolved the workplace into one that is highly distributive and mobile in nature. Information is everywhere, and employees can access all types of information online. The decreased cost in data storage online has made it cheaper for organizations to store all their data as opposed to sorting through all data and storing only the necessary files. Furthermore, because data storage costs are so low, data can be easily hacked by malicious attackers. As more people study IT and gain skills in this area, the sophistication of attacks increase, whereby, organizations find it difficult to discover trails of information theft. The workforce is now highly distributed as organizations strive to improve employee productivity by allowing employees to work from home, other local offices, and even coffee shops. With this increased flexibility comes a new set of risks. Employees access sensitive information through multiple channels such as through wifi and the 3G network, and this new set of risks must be managed to restrict unauthorized access. Furthermore, insider threat has grown because the value of company data has increased, giving insiders more incentive to abuse their trust in the company.

While the environment has made insider threat more vulnerable to organizations, organizations have not really changed the way they deal with such threats. Organizations have implemented a high level of technology but while this technology has become really good at “keeping outsiders out, the
insiders walk right in everyday. According to Dr. Mike Gelles, a director with Deloitte Consulting, many companies today agree that insider threat attacks have a very high impact, but at the same time, believe that the likelihood of occurrence is very low. Thus, managing insider threat does not become a priority for many organizations today. On the other hand, some security professionals, such as chief security officers, do recognize the importance of protecting against this type of threat but feel that insider threat is too difficult to manage. CSOs feel powerless to defend against insider threats because insiders can access the network without passing through the perimeter. The attacks are planned much in advance which allow them to cover their tracks and these insiders act based on a wide range of motivations that may be hard to predict. Since insider attacks are much more targeted because they know where the information is located, these attacks are likely to impose a greater impact compared to external attacks.

As we can see from the growing number of insider threat incidents, such attitudes that organizations have against insider threats are no longer permissible. In fact, the 2010 Verizon Data Breach Investigations Report along with other studies concluded that it is more costly to fix insider attacks compared to external attacks. This is also confirmed by the e-crime Survey and Ponemon Institute's 2010 Cost of Cyber Crime Study. Therefore, it is critical for organizations to shift their mindset towards implementing a plan that will proactively prevent and detect these insider attacks.

Ways that insiders can attack

In order for organizations to devise a plan to mitigate and detect insider threats, organizations need to first understand the type of ways that insiders can attack and the types of people that make such attacks. CERT's insider threat team researches technical and behavioural aspects of insider threats using actual insider attack cases that have occurred in the US. Understanding the insiders' behaviours and

---

10 Ibid.
motivations is crucial to identifying the employees that might attack the organization. From all of the cases
that CERT has thoroughly analyzed, CERT categorized malicious and intentional insider attacks into four
broad categories: IT sabotage, fraud, theft of intellectual property (IP) and national security espionage\(^\text{15}\).

**IT Sabotage**

This type of attack is when the malicious insider damages the company’s network, system or
database. These people are usually former employees who have been recently demoted, fired or formally
reprimanded, and held a technical position such as an IT technician or system administrator and who had
access to privileged accounts\(^\text{16}\). These disgruntled IT employees usually attack after they have left
the company, outside normal businesses hours and from a remote place. The HR department should be able
to identify these high risk former employees and should therefore, keep an eye out for these attackers.

There are some general behaviour patterns that can help identify these types of insiders. Some of these
insiders have had mental predispositions, such as mental health disorders (alcohol and drug abuse and
panic attacks), social skills and decision making bias (unprofessional behaviour and bullying), or a history
of rule violations. Furthermore, most of these insiders have experienced stressful, negative work-related
events such as poor performance evaluations and disagreements about salaries or bonuses, which lead
to revengeful actions against the company.\(^\text{17}\) Appendix I is CERT’s model of insider IT sabotage based on
precursors, events and behaviours that lead to the attacks. As a result of these types of attacks,
organizations experience large financial damages. For example, a disgruntled IT technician with high
privilege levels in the computer systems planted logic bombs into the company’s system, causing the
system to crash. This cost the company approximately $7 million to fix\(^\text{18}\).

**Fraud**

This type of attack usually comes from a small group of non-technical, low-level current
employees or managers. The consequences of these attacks is that employees misappropriate money
from the company through procurement fraud or inflating revenues/deflating expenses through "cooking

---

\(^{15}\) Cappelli, Dawn, and Joji Montelibano. "Combat IT Sabotage: Technical Solutions From The CERT Insider Threat

=309&VName=PQD>.

\(^{17}\) Moore, Andrew P., Dawn M. Cappelli, and Randall F. Trzeciak. "The “Big Picture” of Insider IT Sabotage Across
[http://www.cert.org/archive/pdf/08tr009.pdf].

=309&VName=PQD>.
the books”¹⁹, all because of personal gains obtained by those individuals committing the fraud. While Enron and WorldCom are classic examples of corporate fraud, fraud can occur in smaller and medium sized companies as well. According to the survey of the Association for Certified Fraud Examiners ²⁰, 73% of the fraud is committed by trusted employees in the executive management, procurement, sales, finance and accounting divisions of small, medium, large-sized companies. Again, companies experience financial damages. An example of this is when an accounts payable manager has privileges that allow him to authorize and approve payments, even those that are requested by himself.

**Theft of Intellectual Property**

The types of insiders who steal intellectual property are usually current scientists, engineers or programmers because they believe that they own assets since they were part of the process of creating it. These insiders use the proprietary information stolen to help a new employer or to start their own business. Research shows that they usually take action within 30 days of their resignation announcement.²¹ To steal an organization’s IP, they usually send e-mails to competing firms and download sensitive and secret information to removable devices.²² There are two scenarios that have been found within this type of insider attack: “the Entitled Independent and the Ambitious Leader.”²³ The Entitled Independent is an insider who is acting alone to steal information to get a new job. The insider has invested time and resources into developing the product and senses ownership of the product, which results in him having a sense of entitlement to the product. This can be seen in the R2 circle of Appendix IIA. Other factors such as dissatisfaction with the job and the opportunity to work at a competing organization give the insider motivation to steal the company’s IP (See Appendix IIB). Theft of the company IP’s requires little planning as the insider already has access to the IP²⁴.

The second scenario is the Ambitious Leader model, where a leader recruits insiders to help steal IP within the organization. The motivation for insiders is to either develop a competing product to steal customers away from the victimized organization or to help the new competing employer of the victimized organization. Insiders in this scenario are motivated not by dissatisfaction in their jobs but by the greater rewards that the Ambitious Leader provides if the insider succeeds in obtaining the information that the

---


²⁰ Ibid


²⁴ Ibid
leader wants. The drivers of IP theft is similar to that of the Entitled Independent, but this scenario requires greater planning because the insider must gain increased access to the system, to cooperate with the "leader" and to potentially hire more insiders within the organization (See Appendix III)25.

National Security Espionage
This is a fairly new type of insider attack which has been on the radar for government organizations. The insider leaks out confidential national information, such as those that have been labelled "WikiLeaks". This type of insider forces organizations to look beyond the traditional roles of insider as these people have a different type of motivation. Insiders are motivated to leak national information because of their personal morals. A recent example of such type of data leakage is that of the U.S. State Department where a member of the U.S. Army leaked 250,000 secret diplomatic cables to WikiLeaks. The hacker, Manning, was a trusted employee but he had more access rights than was required to do his job26, which allowed him to access and leak such highly confidential information. He explained that the reason why he leaked the data is because he felt that such information should be made available for the public to make proper decisions.27 Wikileaks has unexpectedly provided a channel for data leakage, which security professionals need to be more aware of because such outlet can really “turbocharge data loss”28 as information can get to the mass market almost instantaneously.

The Unintentional
Another type of attack comes from those who do not have the intention for malicious attacks but simply those who are negligent and those who violate corporate policy, allowing for unintentional data loss. While these employees are not deliberately causing damage to the company, their actions have given those who want to attack the company an opportunity to do so. For example, employees have become very casual in surfing the web during the workday that even though there are URL filters, hackers have been able to install malicious codes and to steal confidential business information from organizations.29 To perform their job functions, employees come into contact with sensitive information every day, and some employees also send work documents home via e-mail so that they can continue working at home. While these employees are simply doing their job, the risk of transferring sensitive information via e-mail makes the data vulnerable during transmission. Others leave work carrying mobile

25 ibid
28 ibid.
devices, such as flash drives and laptops, which hold a large amount of sensitive information. Loss of such devices would again expose sensitive information to the public. There are many ways in which ordinary, “good employees” can turn into “bad employees” because of the absence of proper controls and policies in the organization to prevent corporate data from being vulnerable.

**Key Controls**

Understanding the broad types of attacks described above can help organizations customize a plan to prevent and detect such attacks from occurring. Below is a list of key controls and tools that will help organizations make such plan. They are organized as either preventative or detective. While some of these controls can be used to mitigate all types of insider threats, some controls are important for specific types of threats. Appendix IV is a chart of these controls and the types of attacks that the particular control can prevent or detect.

**Preventative Controls**

*Know your assets and know what needs to be protected.*

This type of control will help organizations understand what types of assets (intellectual property, customer information, trade secrets, etc.) are important to the company and determine what level of protection is needed for each type of assets. Certain assets will require more protection over other types of assets. This is important because the following controls are costly, and thus, it is important to have a cost-benefit analysis to apply controls to those assets that are mission critical to the company.

*Certainly document and enforce policies and controls. Train employees to raise awareness of such policies and controls.*

Organizations should have policies that are clear, concise, fair and communicated to employees. Employees should know that these policies will be enforced and the consequences following the violation of these policies. These policies should include acceptable-use of the organization’s resources, information and system, ownership of the intellectual property that is created at the organization, evaluation for employee performance and procedures to address employee grievances. This type of control will help mitigate the risk of IT sabotage such that employees will not feel disgruntled due to unmet expectations when expectations are fair, enforced and clearly set out in the procedures. These policies will also help mitigate the risk posed by unintentional insiders because clear and enforced acceptable-use

---


policies will ensure that employees are not accessing malicious websites and transferring sensitive data that will expose the company to unnecessary risks.

**Organizations should monitor and respond to suspicious behaviour, which starts with the hiring process.**

As mentioned above, before insiders make their attacks, they would usually exhibit certain types of behaviour. It is important for organizations to not only understand these behaviours but also to monitor and respond to them so that attacks can be prevented before they occur. Organizations should also be cautious of the type of people they are hiring. They should have mandatory strict background checks that help match the value of the company's assets. Organizations should use this process to weed out those who possess the traits, such as self-centeredness, intolerance to criticisms and mental predispositions, which increase the risk of insider threats, specifically those traits listed under IT sabotage.

**Implement proper access control and account management.**

Proper access management controls are crucial to protecting the assets of a company. Users of the information system should be granted access to the information on a "need-to-know" basis. These controls will ensure that access to the organization’s sensitive assets is controlled against unauthorized users. Requirements to set strict passwords should be balanced with the need to change passwords on a monthly or bi-monthly basis. This will reduce that the ease of malicious insiders stealing passwords and gaining unauthorized access through social engineering of others’ passwords. There should be strict policies in place to remind employees not to share passwords and to automatically execute password-protected screensavers so that insiders would not be able to gain access from unattended computers.

A key control within access management is to deactivate computer access of employees following their termination. As described above, many disgruntled employees attack the company after their termination. Organizations should keep in mind that some employees have multiple access points and accounts to the company's network. Therefore, there should be proper procedures in place to terminate access of former employees from remote access, as well as intranet access. Termination procedures also include termination of physical access to the employer’s premise. This means that keys and access cards should be collected prior to termination. In addition, employees often get promoted, switch roles or gain more responsibilities in the organization. There should be proper access management procedures to ensure that employees are not gaining more access than needed for their current job function. One way to do so is to regularly monitor and update all employee access controls.

---


Enforce proper segregation of duties.

Organizations should separate the functions of the company to limit the opportunities of fraud, IT sabotage and IP theft without the collusion of others. It requires organizations to define and separate roles responsible for key business processes. For example proper segregation of duties of authorization, custody of assets, recording and reconciliation will decrease the chances of financial fraud. Another example to prevent IT sabotage would be to have policies that require the verification and validation of a source code by someone other than the programmer before the program can go live\textsuperscript{35}. Organizations should have a code review process implemented in their software development cycles and have logs to control system modifications.

Be extra cautious with system administrators and technical users with privileged access.

According to Network World, the biggest insider threats are performed by those with privileged access and system administrators\textsuperscript{36} because those are the technical employees who have the access and the ability to seriously damage the company’s system and network. As mentioned earlier, IT sabotage and theft of IP attacks are caused by those with technical knowledge and held technical positions within the company. These employees can write or download scripts to plant viruses which can harm the network, create “backdoor accounts”, grant themselves remote access and modify logs. These employees, because of their functions, have greater access to the system than all other employees, allowing them to conceal their actions and usually have oversight and approval responsibilities. Since these employees have access to almost all computer files, encryptions will prevent users from reading or modifying the information. Enforcing segregation duties will also prevent attacks by these employees.

Technical employees are likely involved with the system development lifecycle (SDLC), or can take advantage of the loopholes in the SDLC. Organizations should consider insider threats within the SDLC so that employees will not be able to abuse the system to perform malicious technical attacks.

Detective Controls

Log, monitor and track employee access.

Employee accounts should not be shared so that activity can be traced from the computer account to the individual employee who is associated with that account. Organizations should have a log to track user logins, logouts, and frequency of access and downloading of sensitive information. This type of monitoring can be done through an automated log auditing system that can monitor real-time activity. Sudden changes or significant downloads of sensitive information may indicate that a certain employee

\textsuperscript{35} ibid.

may be stealing intellectual property and sending it off to a potential competitor. Having a system that monitor these activities will help detect potential theft and try to stop the transmission. Organizations should also set thresholds of access for different classes of users so that if access exceeds the threshold, a red flag would be triggered for investigation. While it may be hard to stop the transferring of data immediately, such tools will help trigger an investigation by the organization’s security or forensics team so that action can be taken to minimize the damage of the attack. As mentioned earlier, the organization should also monitor the accounts of those who plan on leaving the company as employees usually like to access and steal large amounts of data within 30 days of their announcement of resignation.

While some organizations may need to install technological tools to properly monitor such activity, organizations actually have a robust network of these tools already in place. For example, a lot of the tools used to prevent hackers or outsiders from attacking the company can be used as monitoring tools for insiders as well. Most organizations already have tools such as packets capturing, intrusion detection systems and firewalls. These tools can be used to monitor a lot of the indicators mentioned above.

*Develop an insider incident response plan*

This type of plan will include procedures to investigate and to deal with malicious insiders when attacks are detected. This plan must be organized and clearly documented. Research shows that a lot of organizations cannot persecute the insiders because they do not have enough information to confidently persecute someone. This type of plan will help gather information to support the accusation. However, a challenge is to decide who to place on the response team since technical knowledge is require for such investigation. These technical people chosen on the team may be insider perpetrators themselves and having knowledge of such plans would allow them to further cover up their attacks.

*Balancing internal security and morale*

At the end of the day, managing insider threat requires the management of employees. If employees are properly managed, compensated and are satisfied with the job, employees may not have the motivation to cause harm to the company. However, in reality, this perfect situation would not be feasible and hence the above discussed controls are required to protect the company’s legitimate business interests. While controls must be in place to a certain extent, organizations have to be alert in pulling a balance between the amount and extent of the controls within the organizations and the reaction and morale of employees. Firstly, having excessive controls in place may disrupt the productivity of employees.

---

40 Ibid.
41 Ibid.
employees. For example, excessive access control management and limitations to the amount of data accessed can significantly hinder an employees’ ability to work when accessing sensitive information is part of the employees’ duties. Therefore, there is a trade-off between protecting against the potential loss of IP and the productivity of the users.

Aside from access management controls that may hinder employee productivity, controls that require employee monitoring, such as monitoring or scanning of employee e-mails to prevent data theft instils a “big brother culture” which decreases employee morale. Some employees feel that such monitoring equates to a lack of trust from the organization. Such lack of trust poisons the organization’s culture. Research shows that employees who feel that they are excessively being monitored tend to have a negative attitude toward their job, which leads to a reduction of productivity, a lack of loyalty to the company and high employee turnover rates.\(^\text{42}\) It also leads to resentment and hostility towards the employer\(^\text{43}\). Such attitude towards the company may potentially lead to some of the insider attacks listed above because of dissatisfaction towards the company. If monitoring creates a morale issue, then the value of the monitoring would be greatly diminished because employees are critical to every business.

The key to balancing internal security and monitoring of employees is to create a policy that has clear expectations. It should also include the type of monitoring that will be executed within the organization.\(^\text{44}\) These policies should be properly defined, transparent and open. In fact, employers are encouraged to discuss these policies with employees before implementing them so that the employees have a clear understanding of the objectives of the controls in place. Employees should be educated on these policies, which includes explaining the reasons for why such policy exists and what actions would be taken to enforce those rules.\(^\text{45}\) If employees understand and agree with the rationale behind the monitoring system, employees will be more receptive to being monitored.

**Privacy issues in employee monitoring**

Tools used during the process of logging and monitoring employee behaviours and actions on the network may evade an employee’s privacy. Tools such as reading e-mails and instant messages, use of surveillance cameras to monitor behaviour and systematic key logging are highly intrusive tools which are only allowed under extreme circumstances where the organization suspects the employee of criminal


behaviour. Information captured during the process of monitoring employees may be confidential and private in nature. Therefore, organizations must exercise proper care in the use and storage of such information. In Canada, federally regulated employees have protection under PIEPDA as this law restricts employers to “collect, use and disclose personal information about their employees”. Other than Alberta, British Columbia and Quebec, who have their own personal privacy laws which apply to employees, employees in other jurisdictions do not have privacy rights under PIEPDA, but they do have some degree of privacy protection from the Charter, the collective agreement with the employer and the common law. Privacy needs to be balanced between employer’s legitimate business interest and the employee’s rights. Therefore, employers are allowed to monitor employees for security and productivity purposes. However, these controls must be considered “reasonable” and must not be intrusive unless under extreme circumstances. Firstly, employees need to have a “subjective expectation of privacy” which means that the employee must believe that his personal information will be kept from the employer. An example of this would be an employee expecting privacy on information that is encrypted with his/her own password. Secondly, employees must show that it was reasonable for them to believe that such information would be kept private. While both these terms are quite subjective, the best way to ensure that expectations are met and clear on both sides is to adopt a policy stating which type of information will be collected and if private, what the employer will do with the information. A general rule of thumb for employers is to meet the objective of the control by choosing the method that is least intrusive.

**Insider threat from trusted business partners**

As organizations increasingly outsource their non-core operations, a new type of insider has emerged. This type of insider is called a trusted business partner (TBP), which is an external organization which the company has contracted to perform a certain function of the company. Examples of these TBPs include payroll, IT and cloud computing service providers. These TBPs have authorized access to proprietary information, critical files and access to the company’s network. TBP insider cases have occurred in a variety of industries but a greater number occurred in the government and IT sectors.

The number of businesses utilizing cloud computing has increased and as mentioned, this type of computing platform has changed what constitutes an insider. There may be little visibility within the cloud and organizations that deploy the cloud may be unclear of how the service is controlled. While cloud


48 ibid.

computing offers significant benefits to companies, a new set of risks arise because of this lack of visibility. The cloud makes stealing information easier because employees with access to the cloud have access to large amounts of sensitive data from multiple organizations that use such service. Also, cloud computing service providers are typically focused on having controls from preventing attacks from outside the cloud but not within the cloud. The cloud also lacks transparency about hiring processes and background investigations which means that those with “ill intents” will be hired and gain access to valuable information. However, despite these new risks, organizations can mitigate them by requiring cloud service providers to use similar controls that are used to protect insider threats within the organizations. This can be done through a detailed service level agreement.

Growing insider threats in the financial institutions section

The current news on the internal breach of the Bank of America resulted in $10 million of losses and is an indication that organizations are not placing enough efforts to mitigate insider threats, specifically internal fraud risks. In the incident of the Bank of America, an employee with account information leaked personally identifiable information such as social insurance numbers, addresses, bank account numbers, drivers license numbers, PINs, etc, to a criminal group. Using that information, this group of criminals hijacked e-mail addresses and used the customers’ information to open new accounts. Bank officials have noted that there have been more and more incidents where organized crime groups have planted an employee within an organization to help get information with their authorized access. If proper controls were in place for segregation of duties, access management and to detect employee fraud, such incidents may be limited. However, for organizations such as banks, access to customer information is crucial in enhancing customer relationships. This tension between access management and security will continue to exist.

Conclusion

Insider threat has always existed in every organization, but organizations never managed it properly because of the perceived infrequency of these insiders attacking. However, as the workplace environment changes into one that is more mobile and where information, including sensitive information, is available in many places, the opportunities for such attacks substantially increases. Organizations are advised to evaluate their current plans to mitigate insider threats and to focus more efforts on improving the plans that are considered inadequate using the key controls described above. C-suite executives

should also beware of the potential loss of employee morale and privacy issues due to the increase in internal security. Executives are required to find a good balance between the three aspects.
Appendix I: CERT’s model of insider IT sabotage

Source: Slide 18 of “Combat IT Sabotage: Technical Solutions from the CERT Insider Threat Lab”
Appendix IIA: CERT’s model of the Entitled Independent (Part I)

Appendix IIB: CERT’s model of the Entitled Independent (Part II)

**Source:** Page 6 and 7 of "A Preliminary Model of Insider Theft of Intellectual Property."
Appendix III: CERT’s model of the Ambitious Leader

### Appendix IV: Controls relating to specific types of insider attacks

<table>
<thead>
<tr>
<th>Controls</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of IP</th>
<th>National Security Espionage</th>
<th>Unintentional Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know your assets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Document policies and controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Monitor suspicious behaviour</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Be extra cautious with system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>administrators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log and monitor employee access</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Insider incident response plan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>


Hanley, Michael. "Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-

<http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=2333847241&sid=1&Fmt=3&clientld=1
6746&RQT=309&VName=PQD>.

<http://web.ebscohost.com.proxy.lib.uwaterloo.ca/ehost/pdfviewer/pdfviewer?sid=3fd5ae79-a749-
4a74-a007-2ab5337f09f5%40sessionmgr13&vid=1&hid=24#>.


Julia, Allen, and Hanley, Michael. "Indicators and Controls for Mitigating Insider Threat." CERT Podcast

Kaplan, Dan. "WikiLeaks Fallout: The Data Breach Heard around the World - SC Magazine US." SC
data-breach-heard-around-the-world/article/193219/>.

<http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=2280481101&sid=1&Fmt=3&clientld=1
6746&RQT=309&VName=PQD>.


youre-missing-real-threat-894?page=0,0&source=IFWNLE_nlt_daily_2010-03-10>.


<http://www.cio.com/article/164552/Survey_Says_Insider_Threat_Remains_a_Serious_Security_Pro-
blem>.

<http://web.ebscohost.com.proxy.lib.uwaterloo.ca/ehost/pdfviewer/pdfviewer?sid=89804277-00f2-
4fd9-bc7f-3b6dd29f96d0%40sessionmgr11&vid=1&hid=21>.

<http://web.ebscohost.com.proxy.lib.uwaterloo.ca/ehost/pdfviewer/pdfviewer?sid=09728972-f7b4-
475c-b412-e7577806bfa4%40sessionmgr10&vid=19&hid=21>. 


## Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

There are many challenges to managing a company’s security along with maintaining employee privacy. Some threats that can affect companies are IP theft, computer and email misuse, bullying/harassment/discrimination/misconduct, fraud and theft, and contractual disputes. With more storage types available out in the market, such as USB sticks, and SD cards, it’s difficult for a company to maintain its security. On one of these devices, an employee can steal an enormous amount of data. A mistake companies make is to investigate employees by taking a look at an employee’s computer, which could alter the reputation of the company on the basis of bullying/harassment/discrimination, if the company accuses the incorrect person. Also, when turning on a suspect’s computer, it could tamper with date stamps and other important metadata which can be used as proof of an employee who has wronged. Instead, there should be a proper plan in place to deal with these possible threats and a properly trained team to deal with these issues. Preventative measures should include having policies in place. For example, the policy might include details on the use of personal USB sticks in the workplace. Other preventative measures include using encryption and only allowing approved USB devices to connect to the computers.

Survey conducted by Cyber-Ark Software shows that:
- Nearly 1/5 C-level executives surveyed admitted that there was sabotage by an insider threat in their workplace
- 16% of C-level executives surveyed believe competitors received sensitive information or intellectual property from an insider, including customer lists, product information and marketing plans
- 1/4 of IT staff surveyed believed their privileged accounts were not being monitored
- 48% of sample surveyed believed that the IT department had the most likelihood to snoop around a company’s network, 10% believed that managers were most likely to do that, and 7% believed that human resources had the highest likelihood for such actions

In addition to these numbers from the survey, a Cyber-Ark representative indicated that privileged accounts are important to both external and internal employees, for retrieving a company’s sensitive information.
Annotation

Three cases are studied regarding IT personnel abusing their privileges. The first case relates to pirating software. In this case, an employee had access to all computer systems that the company used. The employee was paying himself, through a company that he owned, for pirated software. Microsoft notified the CFO of the company that they believed that the company had fake copies of Microsoft software. The company was able to change all the passwords, and fire the employee. In total, the situation cost the company $250,000 to $300,000. To avoid this situation, the company could have: segregated the employee’s duties, perform proper background checks on employees, and avoid hiring arrogant staff.

In the second case, a company decided to outsource most of its IT. An employee with high privilege levels planted logic bombs in the computer systems. After the employee left, many of the servers the company had crashed, and the company was initially uncertain had happened. The company later found out who had caused all of the damage and made an agreement with the employee to fix the servers (and in return, the employee would not be prosecuted). The company suffered estimated costs of $7 million. Preventative measures that could have stopped this situation are: to avoid privilege escalation, segregate duties and have IT oversight, and be more proactive in overseeing angry employees.

In the third case, a company’s human resource staff informed an employee to stay put, and indirectly alerted the employee that the company knew about his actions. The employee was using the company’s website (that was hidden) to sell pirated electronic equipment. With the alert by the human resource staff, the employee quickly deleted the only copy of some encryption keys. Therefore, some data was lost forever. This cost the company approximately 18 person years of work. This situation could have been prevented if they shut down the employees’ access immediately after they found out about his activities, and by keeping a backup of this sensitive information.

Annotation

Many studies have come to the conclusion that security professionals are more afraid of insider threats than external threats. The 2010 Verizon Data Breach Investigation Report stated that 48% of cases studied were from users that abused their access privileges to sensitive corporate information. The study also notes that insider threat is generally more costly to fix when compared to external threats. One type of insider attack is when employees intentionally attack IT systems – these employees are usually disgruntled, are technically competent and are usually system administrators. These types of employees need to be monitored carefully, especially if the human resource department knows that they are disgruntled (i.e. if they were fired, or resigned). Another type of insider attack has to do with taking away sensitive information (such as intellectual property). Usually, these employees can be distinguished into two groups: (1) the employee that believes that the work that they have been doing is their own personal intellectual property (i.e. an engineer may have designed an item and believe they own the design of the item), or (2) those that have the intention of just stealing the intellectual property for the purposes of another organization. In addition to these types of insiders, an
employee who places morality over all else can be an insider. The example used in this article is WikiLeaks, where a soldier released sensitive government information. While having morality is generally considered good, morality can mean different things to each individual or organization. One general suggestion to prevent insider threat is to have policies and procedures with severe punishments.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oleksak, Joe</td>
<td>Cybercrime: How to Protect Your Financial Institution</td>
<td>Hoosier Banker</td>
<td>Vol 95, Iss.1</td>
<td>2011</td>
<td>34-35</td>
<td>May 28, 2011</td>
<td>ABI Inform</td>
</tr>
</tbody>
</table>


Annotation
In the first three months of 2010, there were 173 breaches reported, where 12 percent of these breaches related to financial institutions. Insider threat can be posed by loan officers, bank tellers, computer technical, mailroom supervisors, basically anyone within the organization Examples of insider threat within financial institutions:
- A member of the IT team of a large bank dispensed cash (more than $5,000) without any record of a transaction because he was able to deploy malicious computer code into the program
- A former switchboard operator, now with another institution, took customer information which resulted in more than $200,000 stolen from 13 of the banks' customers

Ways to control these threats:
- Conduct background checks for everyone including contractors, temporary staff — criminal, credit, employment check. These checks should be repeated on a periodic basis for employees holding a highly sensitive position. If employee is from a different country/state, conduct background checks for all the states that he/she lived/worked in.
- Raise employee awareness through training
- Employ strong access controls (i.e. on a “need-to-know” basis); have unique IDs for everyone
- Employ strict segregation of duties, restrict remote file-sharing systems, block external e-mail websites, scan outgoing e-mails, monitor audit trails, use surveillance cameras, restrict access during non-business hours

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blades, Marleah</td>
<td>The Insider Threat</td>
<td>Security Technology Executive</td>
<td>Vol. 20, Iss.9</td>
<td>2010</td>
<td>32-36</td>
<td>May 28, 2010</td>
<td>ABI Inform</td>
</tr>
</tbody>
</table>

http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?index=37&did=2233949191&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306635364&clientId=16746

Annotation
While cyber-attacks are fairly common since even non-technical employees can do it, focusing protection on only cyber controls is not enough. The threat is the individual employee, and not the method they used to attack the company. According to e-crime Survey and Ponemon Institute’s Cost of Cyber Crime Study 2010, insider incidents cause more monetary damages than external breaches because insiders know what
information to target and how to get to the information. The problem is that while many organizations think that insider threat is very costly, and creates a large impact, they feel that the frequency of the incident happening is very low. To organizations, managing this threat becomes a lower priority because of its low frequency. Other companies feel that it is important to protect against insider threat, but they feel incapable of preventing it from happening.

Anyone within the organization can pose threats to the company, not just disgruntled IT workers. Examples of damages include: espionage, fraud, misuse of information, or theft of intellectual property. Typically, the employee tends to pursue his/her plan for an extended period of time and the intent to harm is often a result of personal life problems. Several traits that provide hints to potential employees that pose security threats include: self-centredness, feeling neglected, passive aggressive behaviour and intolerance of criticism.

Since the threat is complex and may be hard to detect, the best way to guard against it would be have a layered approach, incorporating processes and policies, technology and cultural change. It is important for the company to have an understanding of the assets (including IP, proprietary data) that are valuable to the company.

In the outmost layer of protection, the company should prevent potential insider threats from becoming a part of the organization. To do this, the company should ensure mandatory background checks and use the interview and hiring process to reject those candidates that possess the certain traits mentioned above. The company should also foster a team culture because a popular reason for insiders to act against the company is when they feel left out by their peers and supervisors. Training employees to report suspicious behaviour and promoting a culture where employees will feel comfortable reporting what they know is essential to mitigating insider threat. The last layer of protection would be to have technology tools and controls to monitor suspicious behaviour, audit the logs and to maintain proper access controls and tracking of employee access.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>


**Annotation**

As the public sector workforce decides to cut employees by 500,000 by 2014/2015, employee morale and motivation will decrease. This increases the likelihood of insider threat. Therefore, the public sector needs to protect itself from exposure to information risk and security. Organizations should try to focus on improving not only process efficiency, but also risk culture. The leaders should actively encourage the staff to improve the organization and provide them with opportunities to foster a stronger sense of loyalty. The public sector needs to focus on increasing staff motivation and morale despite the need to increase process efficiency by letting go so many employees. At the same time, there needs to be proper controls in place to monitor and track key assets and to reduce the risk of loss, leakage or corruption.
New technologies such as ERP and B2B processes enhance data availability but they also increase the risk of insider threat. These insiders can steal IP and consumer and employee data. While companies can require their employees to follow their security policies such as encrypting sensitive data within e-mail messages, these policies may not be sufficient enough to prevent such threat. Below are recommended ways for organizations to manage security risks for insiders:

- Implement centralized and automated identity and access management controls to monitor employee and third-party access and use of sensitive information:
  - 1. Gather management and stakeholders to determine which information needs to be protected
  - 2. Agree on what is considered sensitive information
  - 3. This data should be tagged and consolidated with central services that are encrypted and have sufficient physical security controls
  - Digital rights management technology can then be used to control the use of the information. However, there needs to be proper balancing between the mitigation of security risks with legitimate users’ access to fulfil their jobs

- Automating processes and related controls:
  - Providing new user access based on the job’s requirement and the user’s responsibilities. Ensure that whenever there is a promotion, the access management is changed in a short period of time.
  - Reduce delays in termination accounts of those employees that leave the organization. Also monitor activity of those employees who plan on leaving the company – may find users trying to frequently access important files
  - With response to third-party access to information, the company should set up a separate area, away from the internal network, for which these parties may enter. The corporation should use identity and access management controls to ensure that tagged sensitive data are not uploaded to the demilitarized zone where third parties are allowed to enter.

---

**Annotation**

80% of security breaches are perpetrated by insiders, but recent research (in 2008) indicated that the majority of the attackers are external. However, the removal of botnet command significantly reduced the amount of spam and players in external breaches. Outsider attacks such as...
A mass mailing of a virus may be used to gain access to the server, or destroy a website; however insider attacks are much more targeted as they know where the information is located. These attacks are more likely to succeed and also have a greater impact. It is also easier to guard against outsiders because you can use off-the-shelf firewalls, IPS, e-mail anti-virus spams etc. However, it is harder to prevent the targeted attack, specifically when the employees know how to access the company’s system. Therefore, companies should spend more time preventing insider threat, specifically in cost-cutting situations, e.g. when they plan to lay-off employees because of the recession as employees will become unhappy and may plan an attack against the company.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messmer, Ellen</td>
<td>Sys admin gone rogue is biggest insider threat</td>
<td>Network World</td>
<td>September 2010</td>
<td>2010</td>
<td>11-13</td>
<td>May 29, 2011</td>
<td>Business Source Complete</td>
</tr>
</tbody>
</table>

Annotation

The biggest insider threats are those who are part of the IT department, the ones who put the system together, specifically those who have privileged access to the network. When these system administrators go rogue, they will become a significant threat to the organization as they can potentially steal data, set up secret access, plant logical bombs, etc. within the system and without anyone finding out.

Some statistics relating to insider threat include:
- Insider participates in 48% of all data breaches
- 275 data breach cases occurred in 2009, and went up by 29% in 2010
- 90% of all reported insider cases are deliberate and malicious, and involve the misuse of privileges
- 24% of the crimes are done by those that were undergoing a job change

Security experts recommend companies to monitor those with special network privileges. Some companies rely on software (such as ArcSight Enterprise Security Manager) to monitor the employees, while others, such as Computershare, uses a more periodic manual process for "entitlement review" to ensure that access to the systems matches the functions of the employees. These experts also recommend that corporations should have segregations of duties so that there would be a way to monitor and prevent excessive power from being placed on just one person. Cox, an analyst at System-Experts recommends that companies ensure role-based access is current. There also needs to be a balance between the amount of controls set up and the efficiency of the workers. Employees also need to be informed that they are being monitored for privacy reasons.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

Annotation

Insider threat has grown because the value of data has increased significantly – personal records such as credit cards, insurance numbers, bank account information, can be sold for 4-8 pounds per record. This gives insiders more motivation to steal data because of these organized crime
groups that are willing to buy the information. Motivation for hacking has changed from pride to financial. Each stolen record costs the organization around 75-150 pounds in remediation expenses.

It is important for C-level security executives to use three broad categories to determine who has access to data, their access policies and what route they take to get that data within the organization:

- Unauthorized and malicious – those who have to mask themselves to steal information
- Authorized and intelligent – those with privileged access and use IT resources appropriately within the defined policies
- Authorized and dangerous – those with privileged access but make unintentional mistakes that appear to be malicious and fraudulent

Recommendations by CERT include: monitoring network access, monitoring database for unusual activity, set thresholds of access for different classes of users, use automated account auditing and real-time activity monitoring.

**Author**

<table>
<thead>
<tr>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A: debate between CEO of Prism Microsystems and Senior analyst at Forrester Research</td>
<td>Debate: The model of ‘trust but verify’ is effective at mitigating the insider threat.</td>
<td>SC Magazine</td>
<td>February 2011</td>
<td>2011</td>
<td>N/A</td>
<td>May 29, 2011</td>
</tr>
</tbody>
</table>


**Annotation**

**Arguments to “Trust but Verify”**

- It is inefficient to completely disallow certain features that help employees increase productivity; such as hardening; it is inefficient and non-competitive
- Responsible organizations should trust that employees are going to do the right thing, but at the same time, verify information is handled properly
- Controlling insider threats should also be balanced by the organization’s information needs
  - Identify critical assets, establish assess control, publically display acceptable-use policies, inform and enforce the policies with continuous monitoring

**Arguments against “Trust but Verify”**

- The profession has only implemented the trust, but forgot to verifying, which explains the increase in insider breaches
- Trust should not be relied upon, instead, companies should start verifying
One type of insider threat is those that are malicious, intentional, and cost organizations a fortune to fix. Another type of insider/security threat is called “Lifestyle Hackers”. Lifestyle hackers are new hires in the twenties, who have grown up with the internet and web 2.0. These insider hackers do not have the intention to cause problems with the company’s information, but they just want to use social networking sites and to multitask. While this may seem unproductive to the corporate owners who set rules on blocking access to social networks, these lifestyle hackers, also known as the Net Generation, increase productivity through multitasking and Facebooking.

An example given in this article was that an intern working in the technology department had the role of server administrator. The corporate security staff found that there was a large volume of data transfer from his workstation and investigated whether or not there was a potential security breach. It was found that the employee had connected his workstation to his computer at home, so that he could stream music from sites that were blocked by the company’s proxy. However, at the same time, the employee was also modifying a sensitive report. While this employee did not have the intention of exploiting the company’s data to the public, he was fired from the company because of his actions and potential exposure of sensitive information to the public. This employee’s act was not malicious and did not break of the company’s policies. He was motivated by his desire to multitask, which did not hinder his productivity. Corporations should consider solving the Net Generation productivity problem and finding the right balance for the company.

Many companies have been taking action to monitor their employees’ e-mail usage and the messages that they are sending. These companies read and analyze outgoing e-mails to scan for leaking of confidential information:
- More than 50% of companies that monitor e-mails found suspected leak of information
- 20% of employee e-mails contain information that poses risk (legal, financial or regulatory)
- 1/3 of companies fired at least one employee for the improper use of e-mail

The law requires companies to explain the monitoring procedures to employees, and should be included in a written policy. Employers need to strike a balance between over-monitoring and damaging staff morale. Employees who feel that they are excessively monitored tend to have a negative attitude to their workplace, which potentially leads to a reduction in productivity. Employers should first weigh the benefits of monitoring and the potential impact on morale before implementing the monitoring strategy.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaplan, Dan</td>
<td>WikiLeaks fallout: The data breach heard around the world</td>
<td>SC Magazine</td>
<td>January 2011 Issue</td>
<td>2011</td>
<td>N/A</td>
<td>May 29, 2011</td>
<td>SC Magazine</td>
</tr>
</tbody>
</table>

**Annotation**

After WikiLeaks published secret U.S. government information, the government was questioned as to how such information could possibly be leaked. It is difficult to identify and prevent data leakage in organizations as big as government agencies because access and sharing of information is essential to one’s job. If the organization employs too many restrictive controls, it may decrease employee performance, morale and cause employee backlash. According to Verizon’s 2010 data breach report, most organizations have been slow to react to data breach incidents. While there are many technologies (i.e. database activity monitoring, digital rights management, access control) available, not all of these can be deployed. Security needs to be balanced with the demand and requirement to access information in one’s job.

**Annotation**

Technological advancements have increase workers' productivity but have also opened the doors to unauthorized access of data by employees. Corporations need to re-examine the balance of corporate security needs against employees’ privacy in the changing environment. Security response tools can be categorized into 5 groups, ranging from least intrusive to very intrusive to employee privacy:

1. Passive: establish policies, implement procedures
2. Active, but not intrusive: block unapproved websites, filter internet and e-mail
3. Active off-line intrusion: internet monitoring, scanning e-mail
4. Active real-time intrusion: reading e-mails, instant messages; surveillance cameras
5. Active forensic intrusion: computer and network forensics

While security measures are important and effective to protect the organization against internal threats, they can also lead to potential privacy violations. Three areas to consider are: legal, ethical and practical constraints. In Canada, computer monitoring is considered unacceptable unless it is used under extreme cases where an employee is a suspect to some criminal behaviour. Ethically, monitoring may mean a lack of trust and respect granted to employees. Also, organization may accidentally gather personal identifiable information during the process of monitoring, in which the organization must properly deal with this information. Excess monitoring will create hostility towards the employer, resulting in decrease employee morale, a “poisoned” organizational culture and low retention of employees.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friedman, Barry A. &amp; Reed, Lisa J.</td>
<td>Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail use</td>
<td>Employee Responsibilities &amp; Rights Journal</td>
<td>Vol.19, Issue 2</td>
<td>2007</td>
<td>75-83</td>
<td>May 29, 2011</td>
<td>Business Source Complete</td>
</tr>
</tbody>
</table>

**Annotation**
There is a trade-off between workplace privacy and morale, and employers’ need to protect its assets. The cost of electronic monitoring and surveillance is decreased employee satisfaction and morale. Some of the reasons why employers want to monitor employees’ e-mail use include productivity concerns and protecting against potential loss of intellectual property such as trade secrets, customer information and proprietary information. An employer can legally intercept and monitor e-mails in the U.S. when it is for legitimate business purposes, such as guarding against financial losses from loss of valuable data. Employees can protect their privacy, if they feel that they have been invaded and out of the scope of the company’s policies, through common law claims. There have been studies that claim that computer monitoring increases stress level, anxiety and anger, and promote a “Big Brother” organizational culture. Increased electronic surveillance leads to violation of privacy, infringement on human dignity. It also decreases employee morale, increases stress levels which decreases productivity. Employees generally accept monitoring if they feel that there are proper policies and procedures in place to guarantee privacy.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**
Training on insider threat awareness; the following are examples of research well underway to combat insider threat
- Pacific Northwest National Laboratory: focused on training in a variety of domain, analytical modeling for insider threat detection
- Carnegie Mello University/Software Engineering Institute CERT program: examine insider cybercrimes and focus on technical and behavioural areas
- US Air Force Research Laboratory: Examined different ways to train cognitive skills
CERT has a MERIT interactive approach which is a simulation used to educate and train organizations to combat insider threat. This approach is a role-playing exercise, simulating different aspects and positions of insider threat within the organization and challenges players to solve realistic organization problems. Ultimately, an organization needs to balance the 3 components in its plan to respond to insider threats – “IT tools for predictive defence, organization policies and practices, management/staff training”.

http://web.ebscohost.com.proxy.lib.uwaterloo.ca/ehost/detail?vid=20&hid=21&sid=09728972-f7b4-475c-b412-e7577806bfa4%40sessionmgr10&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRI#db=bth&AN=25277468

http://www.cert.org/archive/pdf/combatthreat0408.pdf
Podcast featuring Michael Hanley and Julia Allen

Indicators and Controls for Mitigating Insider Threat

Cert

N/A

2011

N/A

May 30, 2011

Cert.org

Podcast: http://www.cert.org/podcast/show/20110125hanley.html

Annotation
Mike Hanley, the interviewee is the leader of CERT’s Insider Threat Team for laboratory work. Mike is currently researching on how to design effective controls to prevent, detect, and respond to insider threat indicators and those that will help organizations guard their IP against these insider threats. One of the key findings from this type of research for their theft of IP Model is that 65% of insiders steal data within 30 days of their resignation. From Mike’s case studies, of over 500 candidates, the team tries to profile behaviours and attach indicators and controls to them. Most controls/indicators fall into 3 categories: prevention, detection and controls to help with response. Prevention would be more of an active defence that would prevent an employee from accessing sensitive information or downloading a large volume of data. Detection is not just about using technical tools after the fact that something happened, but also looking at employee behaviours to intervene with the act. Organizations often do not realize that they already have a lot of tools in place to detect the threat: packet capture, firewall, intrusion detection systems. These tools can help recognize things like whether employees are sending off a large volume of data in an attachment to a foreign firm’s server, which can all tie together to help prevent the employee from committing a malicious act. The last type of controls and indicators are to help firms, who realize after the fact that an incident happened, to gather information to piece the puzzle together and report these incidents. They found that a lot of organizations cannot prosecute the insiders because they simply don’t have enough information to confidently prosecute someone. These controls will help gather information to support the prosecution.

It is important for organizations to train and educate their technical operators to look for the types of alerts that they monitor on a daily basis, to recognize the potential threat of an insider’s malicious acts.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

IDC believes that managing insider threat should be a top priority for the C-level suite executives. There is no one solution that can be used to respond to all the risks that internal security poses. While there are many ways for employees to perform malicious acts, it is found that one of the most common ways that insiders can inflict large financial damages in corporations is through out-of-date and excessive privilege access to steal information. It was founded that 60% of the system’s accounts are expired accounts and that employees use these accounts to commit illegal acts against the firm, leading to multiple failed audits. This paper is a study by IDS and RSA analyzing an in-depth survey that the two organizations have conducted. Below are some of the findings in this paper:

- While insider threats encompasses those “bad people” in the firm who perform intentional malicious acts, a large majority of insider threats are from unintentional acts of “good people” due to their negligence
- There is an issue with operational integrity – not enough internal risk guards against USBs, encryption of sensitive data, etc.; not enough controls for access management
- Contractors and temporary staff are the greatest insider threat to organizations, which is then followed by IT technicians and administrators
  - Contractors and temporary staff have a casual understanding of the company’s policies; IT technicians and administrators have privileged access to the IT system
- Potential future risk regarding outsourcers and “cloud-based” service providers threatening to expose data

As of the time of the survey (2009), 43% of the organizations have a specific budget allocated to internal security risk and 40% of the surveyed organizations wish to increase spending in this area, confirming that internal security is now a top priority for top executives. An eleven-step risk mitigation strategy was proposed in the study. IDC believes that a framework, such as the one proposed, would help organizations the risks mentioned in the study.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

According to research from Carnegie Mellon University, 86% of perpetrators hold technical positions in the company, of which 57% attack after
their termination. These insider attacks result in loss business, costly damages and failed audits. Privileged passwords are the main provider of opportunities for insider attacks to happen. These passwords are also the biggest concern for auditors and enterprises. Privileged password is defined as one that is non-personal shared and that exist virtually in every device. Below are ways that the author suggests to lessen this concern:

- Create an inventory of privileged passwords: they exist in a lot of places within the company, such as the "Administrator Account"
- Define the role of Identity and Access Management: the system for privileged password management should tie individual identities to shared accounts, and this information should be securely stored
- Apply change policy to privileged passwords: research shows that 20% of workstations never change their passwords from default; this is dangerous because if the laptop was lost, someone can go online and search for the default Administrator password for that laptop. Each company should have a policy for changing passwords and the criteria of the password
- Make sure privileged passwords are securely stored
- Create a staged approach to deployment
- Remember that computers are humans too, i.e. the passwords need to be changed: studies show that up to 42% of companies never change hard-coded embedded passwords
- Ensure reporting structures: if possible, get audit reports for privileged passwords

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1350000/1346328/a7-martinez-moyano.pdf?ip=129.97.58.73&CFID=27045950&CFTOKEN=83942253%3E_acm__=1307072587_2be154ba7267fd89e97f43282c03a19b

**Annotation**

Most companies prevent insider threat through the implementation of technological controls. However, research indicates that successful defence against these threats are based on both technical and behavioural solutions. Organizations should implement policies that acknowledge the role of cognitive behaviour traits of the organization's workers, and identify those traits that are common in potential inside attackers. An effective way to manage insider threat is to implement technological tools as well as understand the behaviours of these people, even though this part of the plan is usually neglected.

The purpose of this article is to describe the behavioural side of insider-threat. The authors have developed a case study using data from previous security violations and “constructed a system dynamics model of a theory of the development of insider-threat risks.” In this study, the authors also performed numerical simulations with different parameters in the model. There are three primary types of insider attacks that organizations face today: long-term fraud, sabotage and espionage (information theft). The study focuses on long-term fraud and uses data to examine the motives and trade-off within an organization with regards to the decisions made in their internal security systems.
### Annotation

Insider threats have ranged from low-tech to high-tech sophisticated crimes, causing damages that are not only financial, but also damaging to the company’s reputation. Companies are more vulnerable to insiders than outsiders because insiders can bypass many physical and technical measures designed specifically to prevent outsiders from gaining unauthorized access. These controls to prevent external threat, such as firewalls and intrusion-detection systems do not prevent insiders from performing malicious acts. Insiders are not only aware of policies, procedures, and technology used in the organizations, but they also know where the weaker and flawed parts of the networks. The article/study provides 13 best practices that can help mitigate the risks of malicious insiders by preventing or early detecting such attacks:

- Institute periodic enterprise-wide risk assessments – determine critical assets and define risk management strategy to protect them
- Institute periodic security awareness training for all employees – employees should be aware of the policies, as well as their consequences if found guilty of them
- Enforce segregation of duties
- Implement strict password and account-management policies
- Log, monitor, and audit employee online actions
- Be extra careful with system administrators and privileged users
- Actively defend against malicious code – have practices that can be implemented for early detection
- Use layered defense against remote attacks – some employees may feel more comfortable attacking the system away from their co-workers so they may choose to attack from a remote area
- Monitor and respond to suspicious behavior
- Deactivate computer access following termination
- Collect and save data for use in investigations
- Implement secure back up and recovery processes – in the unfortunate event that insider does attack, the company has something to recover from
- Clearly document insider threat controls

---

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cappelli, Dawn; Moore, Andrew P. &amp; Shimeall, Timothy J.</td>
<td>Protecting Against Insider Threat</td>
<td>Software Engineering Institute – Carnegie Melon</td>
<td>N/A</td>
<td>2007</td>
<td>N/A</td>
<td>June 2, 2011</td>
<td>Google</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choudhury, Amit Roy</td>
<td>Insider threat likely to grow in 2011, says CA; Identity and access management will be key security focus</td>
<td>The Business Times Singapore</td>
<td>Monday, December 26, 2010; section: FBZIT</td>
<td>2010</td>
<td>N/A</td>
<td>June 2, 2011</td>
<td>Lexis Nexis</td>
</tr>
</tbody>
</table>

**Annotation**

According to CA Technologies, an IT management and software solutions firm, the rise of insider threats will continue to surge, as insider breaches have more than doubled compared to the previous years. They say that IT security professionals will need to be prepared to protect the organization from insider threats through improving their identity and access management (IAM) tools. The article also mentions that organizations are beginning to use behavioural analysis to predict insider threat, examining psychological traits that may help them prevent the incident from happening. Mr. Brown, CA Technologies’ Vice President, noted that organizations will need to use programs such as “access and information use policy that are identity-based.” This is called “IAM content-aware”. IAM content-aware will not only help control identities but also control what they can do with the information based on their identity.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAlearney, Shawna</td>
<td>Survey Says Insider Threat Remains a Serious Security Problem</td>
<td>CIO</td>
<td>N/A</td>
<td>2007</td>
<td>N/A</td>
<td>June 2, 2011</td>
<td>CIO.com</td>
</tr>
</tbody>
</table>

**Annotation**

Malicious insiders are a factor in organizations, but even those well-meaning, trusted employees can expose sensitive information to the public, without intentionally doing so. It is normal for employees to be in contact with sensitive information on a daily basis. However, these trusted insiders may accidentally expose data because of their carelessness, the company’s lack of security controls or inadequate following of procedures. 63% of respondents to RSA’s survey stated that they will send work documents home via their personal e-mail so that they can work on it at home. The problem with this is that sensitive information can be vulnerable during the transmission of the e-mail. Also, more than half of the people surveyed use public hot-spot wireless to access their work e-mail via a public computer. Furthermore, mobile devices, such as laptops, USB drives and smartphones are becoming more and more popular, and much of these devices hold sensitive information that relate to the employees’ job. Once these devices are lost, the information contained within these devices will also be vulnerable. Lastly, apparently common courtesy also plays a role in insider threats because many friendly and polite employees will hold open the door for people, even those whom they
have never seen before – according to the RSA’s survey, 34% of the people have held a secure door for someone who they do not recognize.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper</td>
<td>Defending Against Insider Threat</td>
<td>Juniper</td>
<td>N/A</td>
<td>2009</td>
<td>N/A</td>
<td>June 2, 2011</td>
<td>Google</td>
</tr>
</tbody>
</table>

**Annotation**

Technological tools such as antivirus tools, intrusion detection systems and network access controls alone will not be sufficient to prevent insider threat. The tools combined with proper process and procedures, along with employee education/awareness will help prevent against such risks. There are two types of insider threats: 1) those who explicitly perform illegal acts such as stealing data for financial gain and more commonly 2) those employees who make unintentional mistakes by losing laptops, USBs, which contain sensitive information. Another form of insider threat is “social engineering” which is when insiders are tricked into giving up sensitive information. As mentioned, technological tools are important, but tools must not only protect the perimeter of the network, but also the interior, to guard resources and specifically sensitive databases. A good tool to have is a system that detects behaviour abnormality from a user; i.e. if someone tries to download a large amount of sensitive data during after hours, it should raise a red-flag and the person in charge should investigate on this matter. Another tool is the network access control (NAC), which not only ensure security of the company’s customer’s connection to the company’s network but also to help verify employees before allowing access to them. Corporations should consider an open and scalable security network. CERT’s research found that insiders using autonomous agents can delete or corrupt files within the system and this can be prevented in a dual sign-off requirement in a configuration management system. Another way to detect unauthorized access is to track the access control system for who can access what system and under what circumstances. Lastly, employees should be informed of their role to not only be educated about security but also their role to report and prevent potential harmful actions by insider threats.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

This article provides pointers and answers to frequently asked questions for organizations to effectively use these technological tools to monitor their employees. Proper use is important as if these monitoring devices are implemented poorly, surveillance would be expensive, ineffective, and can create employee morale problems. 4 simple rules to follow with respect to having a corporate policy is: have a written policy that’s fair and clear, include the policy in the employee handbook and require an employee signature, periodically remind people that are being monitored of what the policy says, and enforce the policy in a consistent and fair way. To prevent employee morale from declining to a strict policy, organizations should provide reasoning behind the policies and practices. Use of fake cameras, deactivated cameras or hidden cameras are strategies to physically monitor employees or at least deter them from performing any malicious acts within the premise. However, all these strategies create different types of risks. A tip to successfully install video surveillance is to have the security team and the information systems
team work closely together. To prevent insider threat, organizations should keep watch over what employees are doing with their sensitive corporate data, such as monitoring how they interact with the data to ensure that they abide to the policy set by the company. While some companies choose not to let employees know that they are being monitored, the Massachusetts Department of Revenue says that it is essential to let employees know. Companies should also remember to deprovision access of contracts that no longer work for the organization.