Insider Threats 101

"We have to start addressing the human element of information security, not just the technical. It's only then, we will stop being the punching bag!"

- Centre for Strategic Studies in the Crossfire:
Critical Infrastructure in the Age of Cyber War, 2009

IF I ask you what is the greatest information security challenge that your organisation face today in protecting your business from your next data breach, you will probably say a list of external threats such as hackers, malware, ransomware, phishing, social engineering attacks or even denial of service attacks.

But in reality, the greatest risk to your organisation today comes from within. Yes, the insider – your trusted user. The threat to your organisations is no longer the hacker attacking from beyond network walls. Now, it is the insiders already within those walls, and equipped with an all-access pass.

Yet organisations overwhelmingly continue to direct security funding to traditional network defences that fail to prevent damage from insiders. The growing impact of insider threats on business, governments and other organisations not only poses a risk to their assets, but also has a direct impact on the national and economic of everyone else.

The Challenge

Despite this known and expanding risk from insiders, there is little attention paid to this issue. Why? Because, we are dealing with people and not systems. We are dealing with people's behaviour, their emotions, their beliefs and values. How difficult is that to manage, let alone control.

In the face of it, the rising insider threat is made worse by the ever-increasing complexity of systems, access provided to users from anywhere and any device and the massive increase in connectivity between systems containing valuable data and global Internet infrastructure.

Let's admit it, insiders have knowledge, access to proprietary systems, allowing their actions to go undetected by security systems built to defend against breaches from the outside.

But not all insider incidents are malicious by nature. Recent headlines might make hackers seem like the bigger threat to organisation assets but according to CEB Study Research, shows that 60% of breaches has resulted from employee errors.

Why is that? The average employee today collaborates with more people than ever before, such as: clients, prospects, partners, vendors and 3rd party contractors. That means more data is changing hands and therefore more opportunities for the misuse or loss of sensitive information.

In addition, with the advent of cloud based technology and smart mobile device productivity, employees are more likely to send data to their personal devices and accounts, blurring the lines between personal and professional.

Most employees want to do the right thing, but stress is a major cause of insider negligence. Secondly, more than 90% of employees admit to violating policies designed to prevent breaches and non compliance – CEB Study Research

It's dangerous to assume that all employees are the same. It's dangerous to assume that employees are all willing to follow and comply with rules. The uncomfortable truth is that employees often know exactly what they are doing when they place the organisation sensitive assets at risk.

Which leads me to the most shocking statistics. In a recent Gallup Poll survey, found out that 87% of employees worldwide (142 countries) are not engaged at work. Now, countries like the US and Australia are not that bad, only around 71%

disengagement. Having said that, that's pathetic. But a more worrying figure that 24% are actively disengaged. What does this really mean? That means that they hate what they do, they hate the organisation and most likely they will actively work to disempower the environment.

Current Approach

Unfortunately, few corporate security strategies focus on this threat. Traditional network defences systems are reactive and intended to detect hacks through a firewall or other perimeter appliance. Some public and private sector security policies loosely address the insider threat by calling out the need to limit access to information required by a person's job–role-based access control–but few networks are adequately instrumented to detect unauthorised access by insiders or lateral movement within network segments.

Why? Because insider threat is not a technology problem!

Are Insiders Really A Threat?

The threat of attacks from insiders are substantial. Here are some of the more spectacular Insider Incidents examples:

- Terry Childs - The former network administrator for the City of San Francisco, held the city's systems hostage for a time. He refused to surrender passwords because he felt his supervisors were incompetent. Childs was convicted of violating California's computer crime laws in April 2010.
- Bradley Manning - Released sensitive military documents to WikiLeaks in 2009. Now known as Chelsea Manning who has just been released from prison
- Edward Snowden - Before fleeing the country, he released sensitive NSA documents that became a blow up about government surveillance.
- Morgan Stanley – In 2015, Galen Marsh had conducted 6,000 unauthorised searches of confidential data and uploaded 730,000 records to his home machine
- Target – A trusted third party contractor was responsible for the biggest data breach in its history. 40 million customer credit cards along with 70 million records of personal identifiable information.
- AT&T – In 2013 and 2014, three call centres employees were paid by 3rd parties to obtain customer information. The three call centres accessed more than 68,000 accounts without customer authorisation, whereby more than 293,803 handset unlock requests were made online.

A Preventive Approach

If the organisations hope to stay ahead of insider threats, they will have to start with a recognition of the significance of the risk presented by insiders and what risky activities they may place the organisations key assets. This is the first significant step. “Acknowledge the risk”.

To help organisation prepare for: Prevent, Detect and to Respond to Insider threats, I thought that the best way is to address the fundamentals – What is Insider Threats? And who are they?

Insider Threat 101

Insider

An Insider is any user whether they are a trusted employee, a contractor, a business partner or a former employee that has an authorised access to organisation assets. And the key aspect of such a user is that they still have access to organisation assets and applications including confidential data.

Malicious Insider

A malicious insider is a trusted insider who abuses his trust to disrupt operations, corrupt data, ex-filtrate sensitive information, or compromise an IT (information technology) system, causing loss or damage and negatively affecting the confidentiality, integrity or availability of the organisation information and systems.

There are three types of malicious insiders

1. IT Saboteurs

The usage of IT to harm critical assets being your information or your technology. These typically are disgruntled system administrator who want to cause damage, disruption or destruction to their organisation. Their motivation can be based on many different reasons, but primarily it could because of being fired; abusive or violent behaviour within the organisation; poor performance; drug use; demotion; unmet expectations; sexual harassment; revenge.

Impact & Loss:

Characteristically such sabotage affect the availability of that key piece of information or that key system that are up and running. Such a loss could be devastating to the organisation depending how quickly they are able to recover.

Case Study

An organisation that was responsible for managing the 911 emergency service, was disrupted for four major cities. This particular individual was a disgruntled former employee. He was an insider who worked in the IT department, which operated the computer and telecommunications systems throughout the United States.

He was asked to leave for an undisclosed reason without providing notification. As you can imagine, he was somewhat disgruntled. When he went home that particular night (he had retained access unbeknownst to the organisation), remotely accessed and shut down the components of the organisation's systems to include blocking some of the telecommunication services, including the 911 emergency look up services.

This particular individual affected obviously four major cities. As you can imagine an emergency look up service being available is certainly something that could cause more than just IT harm to organisation. Certainly the health and well-being of the citizens of these cities could be impacted as well.

2. Theft of Intellectual Property

A trusted insider who abuses the organisation trust to steal intellectual property. This category can also include espionage.

Case Study

A trusted US citizen was working for a chemical company that manufactured chemical products. This trusted employee was offered a position to go and work for an organisation unit outside of the United States that included incentives. He turned down that particular request as he didn't want to relocate his family.

The company then offered this trusted employee a reduced role and reduced responsibilities. As his role changed, he decided to find alternative employment with a possible competitor.

He went through the job interview, accepted a position with the new competitor organisation, but still worked for the chemical company for three months from the time he accepted a job.

During the three months period of time, he downloaded a significant amount of information from the chemical company – seventeen thousand PDF files; twenty-two thousand abstracts (around thirty-eight thousand documents in all). All these files were downloaded to the competitor provided laptop.

When the competitor company actually noticed that he was uploading information onto their networks, they started investigation. The new organisation then called the chemical company and provided details of what had happened.

This asset was valued about $40 million and is certainly something of significant.

3. Insider Fraud

A trusted insider that would steal money as the primary impact to the organisation. Furthermore, where an insider is incentivised for monetary gain to add or modify, use or delete data in a critical system, which causes some type of fraudulent activity to impact the organisation.

Case Study

The insider worked as an accountant for a certified public accounting firm. Due to her good performance, her employer decided to make her solely responsible for the accounts of two client companies, one of which was her supervisor's other business, a staffing agency.

The insider eventually created a fake employee on the payroll of her supervisor's business. Over the course of six years, the insider used this fake identity to pay herself money from the staffing agency. Several times she also issued fraudulent checks on be- half of the business and had them deposited to her personal accounts.

The insider was finally caught when her supervisor was preparing to buy a house and discovered a large amount of cash missing from one of the staffing agency's accounts. She confronted the insider about the situation, and the insider admitted to the crime. According to the insider, she stole the money for daily expenses and to pay her credit card debt. She had stolen more than $100,000.

Non Malicious - Unintentional Insider

Is an insider that through their actions/inactions without malicious intent caused harm or substantially increases the probability of future serious harm to the organisation information and systems.

Case Study

The personal details of world leaders at the G20 summit were accidentally disclosed by the Australian immigration department. Unfortunately, an employee of the agency inadvertently sent the passport numbers, visa details and other personal identifiers of all world leaders attending the summit to the organisers of the Asian Cup football tournament.

The cause of the breach was human error. The user failed to check that the autofill function in Microsoft Outlook which had entered the correct person's details into the email 'To' field. This led to the email being sent to the wrong person.

There are Four Patterns of negligence

1. Disclosure – accidental disclosure of sensitive information by an insider. For example: Sensitive information posted public on a website, mishandled, sent to the wrong email, fax or mail
2. Malicious Hack – An outsider who has managed to gain entry into the Insiders network and planted malware or spyware software. This could have been done via a phishing attack, drive-by download or unauthorised USB drive. For example, the insider becomes a victim by clicking a link or opening a malicious attachment which then allows the attacker to infiltrate the organisation through malicious malware.
3. Physical – Improper or accidental disposal of physical records. For example, computers that have been thrown out without destroying the contents of the disk drives. Other examples, lost or stolen electronic records such as paper documents.
4. Portability – The insider portable equipment no longer in possession. Lost, discarded or stolen data storage devices such as laptops, smartphones portable memory devices, CD, hard disk drives or data tape. An example could be a user accidentally leaving their smartphone in the taxi, bus or plane.

Non Malicious – Rule Bender

Is an insider that through their action without malicious intent caused harm or substantially increases the probability of future serious harm to the organisation.

The best way to describe such insiders are those people who circumvent organisation policies because it suits them, they want to cut corners, they need to circumvent corporate policies because they have urgent deliverables or because corporate policies are just too difficult to understand or follow. And majority of the time, insiders believe that nothing bad will come out of it.

Case Study

A mid level employee copied millions of personal records to a USB as well as to his laptop unbeknown to the organisation in order to finish a project after hours. The insider doesn’t have the intent to harm the organisation but through their actions, intellectual property leaves the organisations.

Important Lessons

The most important lesson from the above Insider cases are that the seemingly least-threatening employees with little technical knowledge or privileged access to organisational systems can still use organisational systems to cause significant damage.

In many of the studied cases, the insiders did not require technical knowledge to commit their crimes. They easily bypassed security controls or concealed their actions with non-technical actions and exploited insufficient access controls that were put in place by their organisation.

Organisations should assume that ill-intentioned employees will leverage the most easily exploitable vulnerabilities first. Often, such vulnerabilities are within the reach of most non-technical personnel. No amount of intrusion detection systems, database triggers, or host system hardening procedures will defend against an insider with authorised access to data. Therefore, an organisation can only begin to minimise or prevent costly insider attacks if it continually builds and develops its Insider Threat Program.

What Can You Do About It?

The insider threat is ever evolving and changing. But, can it be stopped? Well, you can certainly reduce the risk significantly but unfortunately, not eradicate it. After all, you are dealing with people.

The best approach is to build an effective Insider Threat Program. The goal of the Insider Threat Program, should be to protect the organisation critical assets from the threats that originate from within the organisation, both malicious and non-malicious.

How can CommsNet Group Help?

CommsNet Group is the only specialised Insider Threat focused organisation in Australasia. CommsNet Group helps organisation to identify and mitigate the threat from within.

CommsNet Group uses tested and proven methodologies from Carnegie Mellon University (which is part of CERT – Software Engineering Institute.

For nearly 30 years, CERT division of the Software Engineering Institute has been a trusted an authoritative research organisation in Insider Threats. No other organisation has the corpus of insider threat incidents that the CERT Insider Threat Centre has, nor has any other organisation done the amount of analytics on that type of corpus, that the CERT Insider Threat Centre has.

If you want to tap into the rich knowledge and understanding of how to effectively mitigate the Insider Threat, you can tap into CommsNet Group expertise in either of the following ways.

1. **Attend an Insider Threat Workshop** - This Workshop is an interactive presentation with practical exercises to assist you in gaining a better understanding of what constitutes insider risk and how to deal with it.
2. **Conduct an Insider Threat Vulnerability Assessment** - Based upon CERT Carnegie Mellon University methodology helps you determine how well prepared you are to prevent, detect, and respond to insider threats, should they appear in your organisation
3. **Schedule a meeting to discuss how to build an effective Insider Threat Program** – Contact details below
4. **Download a free eBook** – "*Protecting Your Business From Insider Threats In Sever Effective Steps"*, visit CommsNet Group website www.commsnet.com.au
5. **You can visit CERT - Carnegie Mellon University - Software Engineering Institute** regarding Insider Threat best practices, visit the following site - http://www.cert.org/insider-threat/

Of course, you can seek out more information available on our website – www.commsnet.com.au

For more information, reach out to CommsNet Group by the following

Email: sales@commsnet.com.au

Phone: +61 2 6282 5554