CYBERSEER

DETECTING INSIDER THREAT

WHITE PAPER

CYBERSEER

INSIDE THIS WHITE PAPER:

This document looks at the potential motives and impact of 'The Insider Threat', including trends and notable case studies. It discusses how existing traditional security measures are insufficient to combat this growing undetected threat actor. The paper introduces a new category of advanced threat detection that uses machine learning combined with human analytics to address this risk.

WHAT IS INSIDER THREAT?

The term "Insider Threat" is used to refer to the broad set of risks associated with an organisation's people and includes current and former employees, contractors and third party business associates. Essentially, an insider threat is any party trusted with non-public or "inside" knowledge and access to the IT infrastructure, applications and security systems of a business, and/or access to an organisation's valuable data.

An insider threat can come in a variety of forms ranging from a rogue employee leveraging their unique position to deliberately steal intellectual property and commercial secrets, to a contractor unknowingly plugging in an infected device to a corporate network under a BYOD scheme.

This white paper discusses the various threat types that are associated with insiders due to their trusted position, including high-profile examples, and approaches that can be taken to increase detection and reduce the risk of insider threats.

TRUSTING THE INSIDER

While companies have traditionally invested heavily in their perimeter to protect themselves from external threats such as hackers, competitors, state sponsored espionage and cyber-crime syndicates, it is fair to say that there has not been the same level of investment in addressing the unique risks posed by insiders.

Organisations have deployed large scale network security systems and controls which include data leak protection, firewalls, intrusion detection and prevention as well as ubiquitous desktop anti-virus solutions, but these are not designed to prevent insider-driven breaches. A large level of trust is placed upon employees, partners and contractors but it only takes one small abuse of this trust to cause a potentially catastrophic incident.

Sabotage, theft, fraud, and accidental leaks are often executed through a user's existing access rights or file permissions. Insiders do not always act alone and may even be unaware they are enabling a malicious party.

The National Security Agency (NSA), while investing heavily in external defences and running top secret operations, has been hugely damaged and embarrassed by one IT contractor. **Edward Snowden** was able to easily navigate through the internal systems and collect sensitive information, before exfiltrating the data via USB devices. At no point did he have to skirt security controls or hack devices to gain elevated privileges; he simply abused the access he had as a systems administrator to execute one of the most severe data compromises in history.

Another well publicised breach was the 2013 attack on US retailer **Target**. Attackers first gained access to the network using credentials stolen from a third party

refrigeration supplier to Target. Attackers were then able to leverage the trust and access Target gave to this supplier, to steal millions of credit cards.

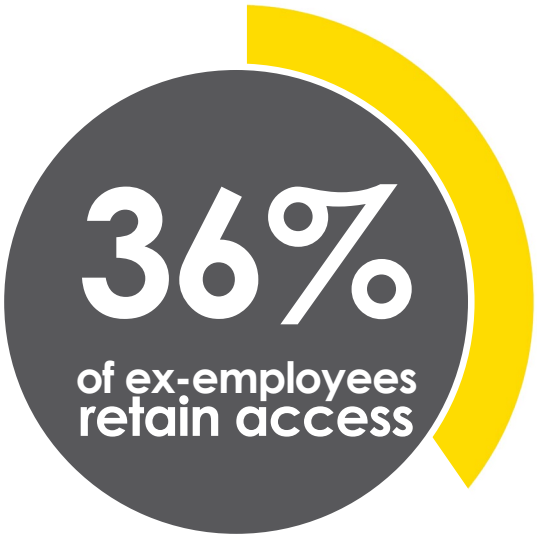
The threat from Insiders, whether acting unknowingly or with deliberate malice cannot be prevented or detected with traditional security measures designed to protect from the outside.

MOTIVES

There are numerous reasons for insiders to break their employers trust and abuse their position, predominately for personal gain. Selling valuable data, such as credit card or personal information to online fraudsters, can be an easy way for an employee to make some cash. There have been numerous reports of bank workers trying to sell account information on the black market or via the 'Dark Web'; unfortunately for them many of the buyers of such information have been members of law enforcement agencies, in particular, the FBI.

A new media story every week highlights the latest theft of online credit card data or user account information. Commercial secrets, intellectual property and proprietary information can also be readily sold on the Dark Web – finding its way into the hands of unscrupulous competitors or foreign governments, all of which are trying to gain an advantage whether it be informational, technical or economical.

One of the primary motives for many attacks is revenge, typically by a former employee trying to cause reputational and financial damage to their old employer. In 2002, a disaffected **UBS** systems administrator planted a logic bomb (a piece of code designed to detonate some time in the future and cause disruption), which took down 2,000 servers and impacted 400 branches. Interestingly in this case the rogue employee also bet $21,000 against UBS's share price, expecting a crash in its market value, combining his revenge with financial reward. Similarly, in 2008, a contract engineer working for **Fannie Mae** planted a logic bomb after his contract was terminated. According to court proceedings, had the attack been successful, it would have wiped data from 4,000 servers, causing millions of dollars of damage as well as shutting down operations at Fannie Mae for at least one week.



Recent research has shown that around 36% of former employees still have access to company data or network systems after they have left an organisation.

By improving termination processes which are followed at the end of an employee's term of contract – simply locking accounts or changing passwords – businesses can reduce the risk from potential ex-employees who decide to act maliciously once they have left an organisation.

Insider threats also come in the form of employees acting without consideration of the security policy. Their actions may not be deliberately malicious but could have damaging consequences. For example, an employee copying sensitive files to a USB flash drive so they can work from home and then subsequently losing this device, which then ends up in the hands of a competitor. Another example could involve a system administrator opening a port on a firewall to allow easier remote administration of some critical hosts over a crucial deployment weekend and inadvertently opening up access to anyone on the Internet rather than a specific IP address. As you can appreciate, neither scenario was carried out with malicious intent. On the contrary, both were done with the best intentions, but the repercussions of either would not be pleasant for the individual or the organisation.

CYBERSEER

A 2013 study by Symantec identified that 62% of employees thought it was acceptable to transfer their work documents to their personal devices or to online file sharing applications. It was also found that the majority of these people never deleted the data they had moved and did not associate any risk in keeping it.

Unwitting employees could pose an insider threat by enabling external cyber attackers. For example, if an employee finds a USB flash drive in the company car park, their intentions may be to find its owner and return it; however, if it has been loaded with malware, plugging it in could give an attacker access to their machine. In this scenario, the insider threat is a critical part of the attack chain.

The infamous Stuxnet virus first found its way into top secret Iranian nuclear facilities through USB devices. Flash drives handed out at the 2013 G20 summit were "backdoored" with snooping software.

An employee with insufficient security training and poor decision-making can be as much of a threat from the inside as a rogue employee setting out to cause damage. External attackers can realise their goals by leveraging or manipulating the poor judgement of an insider.

Regardless of the motivation of the insider, the potential business impacts are universal: increased costs, fines, lawsuits and reputational damage from both a customer and market perspective, leading ultimately to impacted revenues and compromised shareholder confidence.

INSIDER THREATS ARE INCREASING

There are multiple factors that may account for the growth in insider threats. Organisations are increasingly outsourcing business operations: call centres, distribution processes, security and maintenance personnel and utilising cloud based IT infrastructure. Using third party services will increase the potential threat surface, and requires an inherent level of trust with the suppliers and their employees.

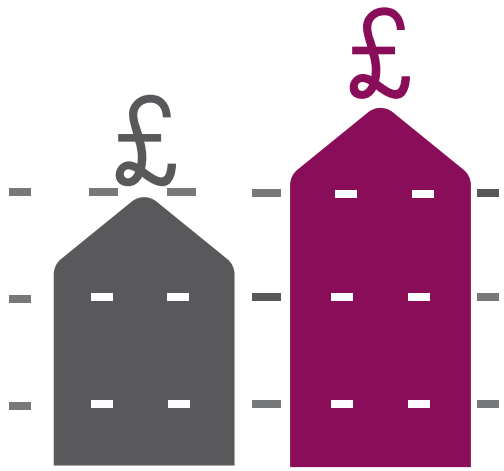
A notable example is **AT&T** who was recently a victim of a large insider breach by outsourced employees from overseas. Call centre workers in South America and the Philippines extracted proprietary network data and personal information from 68,000 customer accounts. The insiders sold this data to malicious third parties, primarily for unlocking stolen phones.

AT&T placed a large amount of trust in call centre suppliers, allowing them to access customer data. While this may have been necessary for normal business operations, insufficient controls and detection measures were in place to identify the suspicious behaviour of the malicious insiders. According to the National Cybersecurity Institute, this incident cost AT&T $25m as well as significant reputational damage.

Many organisations are now allowing employees and contractors to use their personal devices for work as part of BYOD schemes. While not intentionally acting maliciously, employees may be exposing their employers to external threat actors from within the corporate network. Smartphones and tablet computers have increasingly been targeted by malware developers. A recent report by Pulse Secure said that in 2014, approximately one million unique malicious mobile applications were produced; an increase of 391% since 2013.

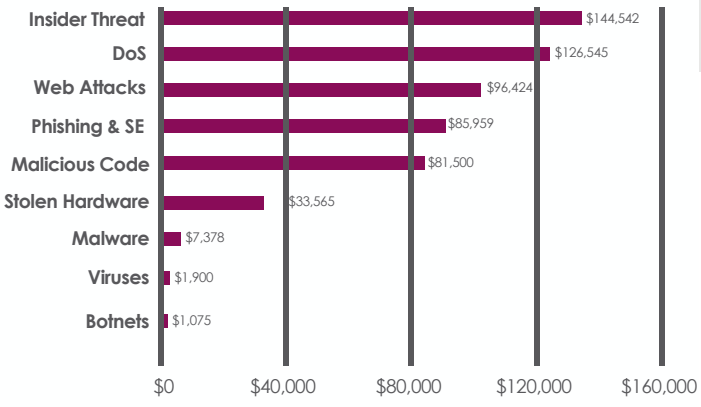
The rise of insider cyber attacks is attributable to employees' increased use of social media. Personnel can therefore be targeted as a means to compromise security. Through popular platforms such as Facebook and LinkedIn, attackers can identify employees that are likely to have a high degree of access, and begin to profile and recruit them, knowingly or unknowingly. Attackers can pay insiders for information, target their

devices to gain access to the network or use more complex schemes such as blackmail or 'romance scams' on dating websites, which involves scammers taking advantage of people looking for romantic partners via dating websites, apps or social media. They will gain their affection, and then use that goodwill to commit fraud.



THE INCREASING COSTS OF INSIDER THREATS

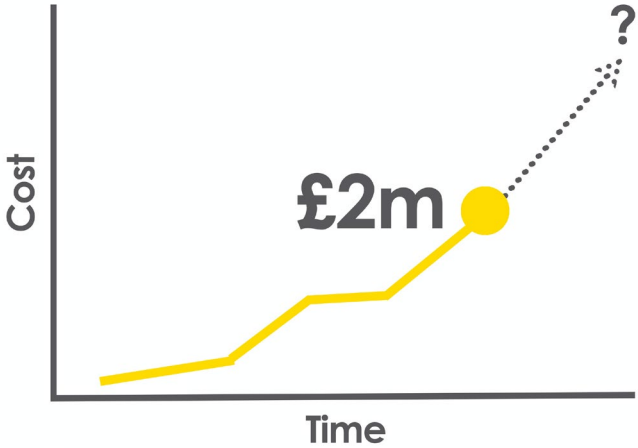
According to recent report from Securinux, last year malicious insiders were not necessarily the most common source of an incident, however they were the costliest. On average an insider incident cost each organisation approximately $144,000, as shown in the graph below:



(Data sourced from Securonix, 2015)

It is also likely that the cost of insider incidents is actually greater than this number, as organisations may not detect an issue for months, or costs may not manifest themselves until years later.

In March 2014, a disgruntled employee working for UK supermarket **Morrison's** stole and leaked the details of over 100,000 members of staff, in an attack driven by revenge. The insider, working as an auditor, compromised information including salaries, National Insurance numbers, dates of birth and bank details, which he uploaded to a file-sharing website and sent copies to multiple media outlets.



At the time of the incident Morrison's had costs of over £2m. However, 18 months later, a group of more than 2,000 current and ex-employees are preparing to sue the supermarket, which will likely see further costs in legal fees and potential damage settlements.

Detecting insider threats as early is possible is the only way to mitigate the impact to business operations or reputation. Without real time detection and analysis, it is not possible to take preventative measures or identify individuals.

Sources: http://www.securonix.com/insider-attacks-were-the-most-costly-breaches-of-2015/

CYBERSEER

PERIMETER DEFENCES FOCUS ON EXTERNAL THREATS

By the nature of their positions, insider threats already have access to part of an organisation's data and a higher level of knowledge of the security systems than an external attacker. While perimeter defences are designed to stop external threats gaining this access or knowledge, they offer limited protection against the actions of internal employees accessing data and systems they are trusted to access.

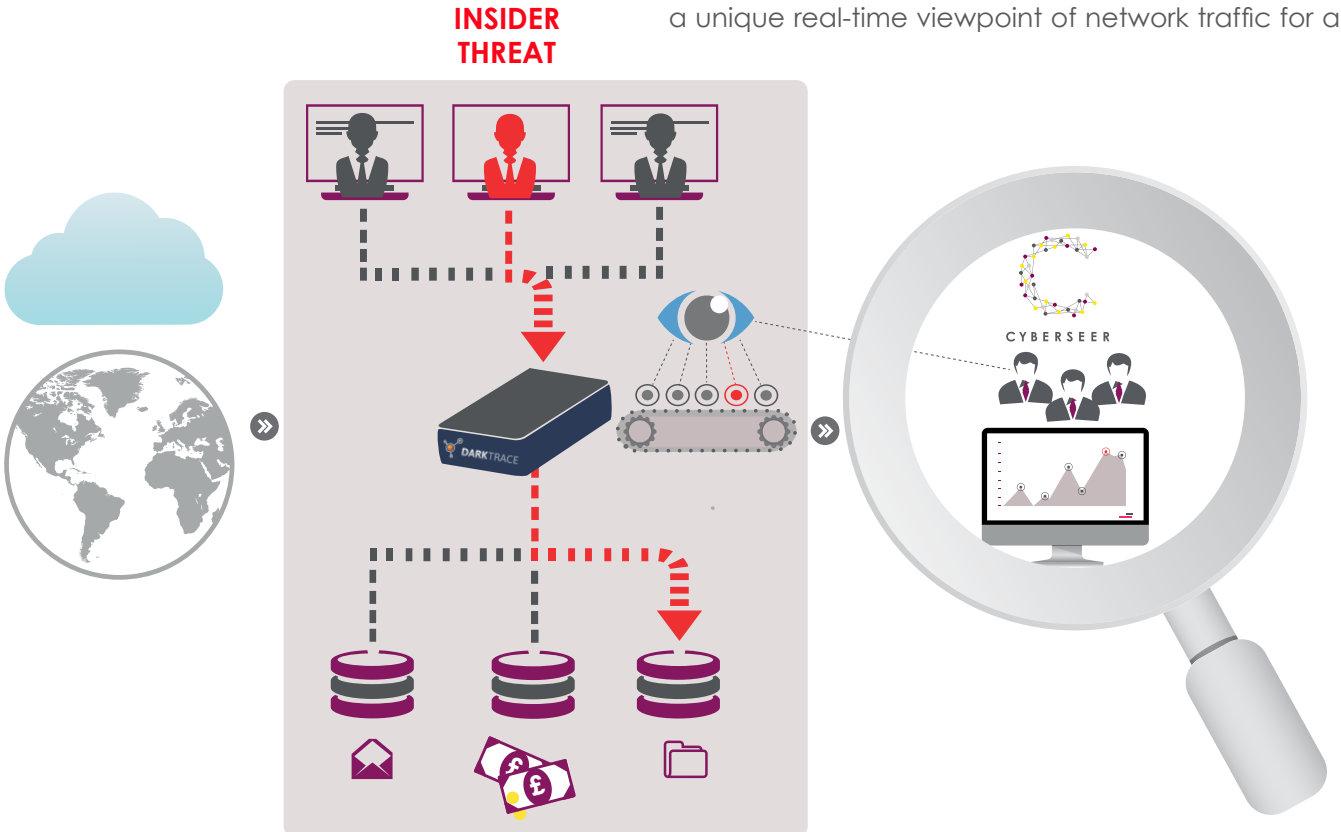
A major problem is that the majority of network security solutions are only designed to identify known threats, through the use of signatures for example. Insider threats typically do not use tools or techniques that will set off signature based security products. An authenticated user will have firewall access, bypassing the Intrusion Detection System (IDS). An employer's security against insider threats is equivalent to the trust they place in their staff.

THE CYBERSEER APPROACH ADVANCED THREAT DETECTION WITH MACHINE GENERATED INTELLIGENCE

While implementing a strong security education and awareness programme for staff is essential to significantly reduce the risk of insiders unknowingly aiding an attack, these will be of little benefit to an organisation against a properly motivated individual determined to exploit their unique position to steal data or sabotage systems.

Cyberseer's advanced threat intelligence service leverages behavioural analysis and anomaly detection technology to identify both external and insider threats. By combining research, data-science and the Darktrace anomaly-driven threat detection platform, Cyberseer can provide alerts into potential insider threats. Real-time investigations, by experienced cyber security Analysts can uncover targeted and opportunistic insider attack movements.

The diagram below, details the deployment of the Darktrace technology on the internal network, behind existing perimeter controls, providing Cyberseer with a unique real-time viewpoint of network traffic for all



devices in an environment. Based on the captured network packets, behavioural analysis can be performed to build a picture of normal activity for devices, users and networks. Events that do not fit into this model of learnt normal behaviour are classed as unusual. Whether the unusual events, connections or data transfers are caused by external threats or malicious insiders, Cyberseer will capture and track them.

Perimeter defences are imperative to help mitigate the majority of external threats. However, as these controls are outward looking, organisations need to consider the increased threat from the inside of their environment and take a combined and integrated approach to address the issue.

Insider threats are inevitable. It is important to take stock of the magnitude of the problem as we continue to face threats of ever-increasing size and regularity. Organisations should avoid over-dependence on traditional security systems and signature-based tools. As seen in this white paper, insider threats can be the most damaging, with one small breach of trust leading to severe and costly consequences.

CYBERSEER

CONTACT US

+44 (0)203 823 9030

If you would like to discuss any element of this white paper or find out about how the Cyberseer team can make difference within your organisation with regards to advanced threat detection, contact us today.

This white paper has been prepared by Cyberseer Ltd and contains information from a variety of sources.

info@cyberseer.net | **www.cyberseer.net**

Talk to us about customer use cases.

Demo both the Darktrace technology & the Cyberseer service.

Cyberseer have not sought to establish the reliability of these sources or verified information provided.