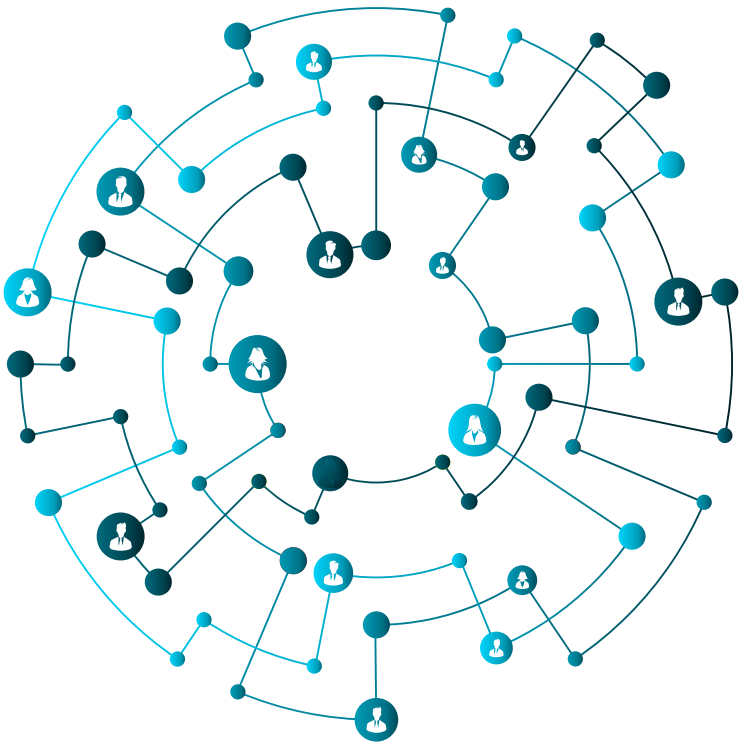
WHAT YOU DON'T KNOW ABOUT YOUR BUSINESS USERS, COULD DESTROY YOU!

IT'S TIME TO THINK ABOUT
MONITORING USER BEHAVIOUR
~ THE LAYER OF TRUST ~



Enjoy

CommsNet Group

THE CHALLENGE

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

But in reality, the greatest risk to any organisation today comes from within. Yes, the insider – your trusted user.

Whether it be that rogue employee who will go to great length to gain access to your sensitive data; Or perhaps that unhappy staff member that wants to take their revenge and divulge the information with the rest of the world; Maybe it's the unscrupulous user that uses your business for their personal gain; It could be a user who just doesn't want to confirm to organisation security and business policies - prefers running their own unauthorised applications, running a small venture scheme from within the corporate and copying sensitive data to the cloud. Or, perhaps it could be the ignorant user who unwittingly shared sensitive data with the wrong person.

All of the above may spell disaster for your organisation. Here are some examples:

- The Edward Snowden scandal highlighted a scenario where a disgruntled employee was determined to unearth highly sensitive and confidential information, yet it wasn't hard to do. Edward Snowden was an IT contractor who gained privilege access to information that he should not have been allowed.
- Financial services firm Morgan Stanley (one of the most reputable corporations in the world, operating in 42 countries, 1,300 offices and 60,000 employees) publicly admitted that it was the victim of an insider data breach. The breach included data on approximately 350,000 Morgan Stanley wealth management clients.

"Edward Snowden was an IT contractor who gained privilege access to information that he should not have been allowed."

INSIDER THREATS *ARE REAL*

An organisation is a "social invention" for accomplishing common goals. Organisations are made of people.

Every user who has or had access to corporate assets can be deemed as a Trusted User or an Insider. They are classified as insiders because, by virtue of their knowledge of, and access to, their employers' information systems.

Once a person has been selected to become an employee, that employee is then granted an "automatic" level of TRUST within the organisation.

Insider Threats are caused by a wide range of offenders who either maliciously, purposely or accidentally do things that put an organisation and its data at risk.

Malicious Insiders are those that have seriously breached the organisation trust.

According to Verizon Data Breach Report 2013, 69 % of reported security incidents involved an insider.

An insider has the potential to cause more damage to the organisation and has many advantages over an outside attacks.

Outsiders understand that humans by and large are vulnerable, exposed and easily prone to social engineering attacks. It has been demonstrated that a reward of $1 USD is enough to convince a large percentage of users to download and run potentially malicious software, while ignoring corporate policies.

Insiders have access to facilities and information. They have knowledge of the organisation and its processes and know the location of critical or valuable assets. Insiders will know how, when and where to attack and how to cover their tracks.

84%

of internal data breaches
come from regular business user accounts
with no administration privilege

[2014 IBM/Ponemon Cost of Data Breach Report]

LIMITATIONS OF TRADITIONAL IT SECURITY PROTECTION

Security controls such as next generation firewalls, intrusion protection systems, mail and web content filtering systems as well as the latest sandbox to detect zero-day attacks are all about adequately protecting from unauthorised access, misuse or fraudulent modifications or disclosure. Yet, these technologies are of little help when it comes to mitigating the insider threat.

Organisations have gone to great length to increase their security posture by adding additional tools such as Identity and Access Management Authentication. Unfortunately, these systems do nothing to directly protect data from misuse. They do have a key role to play in ensuring users are who they say they are.

Furthermore, organisations have adopted technology tools that gather and filter IT-event data for critical monitoring, analysis and auditing. It is interesting to note, that such logs were written by developers to debug applications and systems, but certainly not to understand user activity behaviour.

As a result, many applications lack sufficient visibility and clarity to provide security officers with the precise information necessary to determine what the user did and how they interacted. Should an incident require investigation, it may take the organisation weeks or months to try and piece the story of what actually happened.

Given these security gaps, it is not surprising that we hear many shocking security data breaches. There isn't a week that doesn't go by without a high profile case.

According to the Mandiant Threat Report (2014), attackers were able to compromise data in days or less 100% of the time. However, less than 25% of compromises were discovered in the equivalent time.
The average breach detection was 229 days.

40%

of Organisations Experience a Data Breach Or a Failed Compliance Audit

[2015 Vormetric Insider Threat Report]

UNDERSTANDING USER RISK

In striving to achieve corporate objectives, organisations develop strategies and seek evidence to support decisions that ideally lead to the best outcome. As such, organisations manage risks that could weaken them from achieving the most relevant and highest outcomes. Risks can often be described as "effect of uncertainty on objectives". If something were going to happen, what would be the impact?"

So how do organisations deal with the **biggest threat** to their mission? That is, dealing with trusted users that pose a huge amount of risk that they may not even be aware of?

Today, organisations invest heavily in 'infrastructure' to ensure their assets are protected. However, it is increasingly apparent, people (insiders) are "the weakest link in the chain".

The reason is not that employees are stupid, it's just that they may not care enough about security, they may have made an unintentional mistake; they may have intentionally disregarded organisation policies or were simply malicious. Either way, this could spell disaster for any organisation.

The current reality is that security technology measures are NOT enough to protect your organisation from an insider attack. Current approaches to IT security and risk management tend to underestimate and even ignore the human factor. Which is why we still see so many high profile data breaches.

Risk can therefore be broken down into two parts – ASSETS and PEOPLE. It is the interaction between People and Assets that creates risk.

For example:

- Place a child and a knife in the same room, you have a high risk. Take either of them away, then there is no risk.
- Take the people away from their computers, there is no risk. But also, there are no business activities.

Loss of proprietary information has increased 71% over the past three years

[2015 Security Report – Check Point]

USERS ARE THE GATEWAY TO RISK

In a recent *SANS 2015 Survey on Insider Threats* found while 74% of the 772 IT security professionals surveyed said they're concerned about insider threats from negligent or malicious employees, **32% said they have no ability to prevent an insider breach**.

The number and size of insider threat continues to rise year on year. The last 12 months have seen a continuous flow of high profile organisations reporting that their practice has been breached.

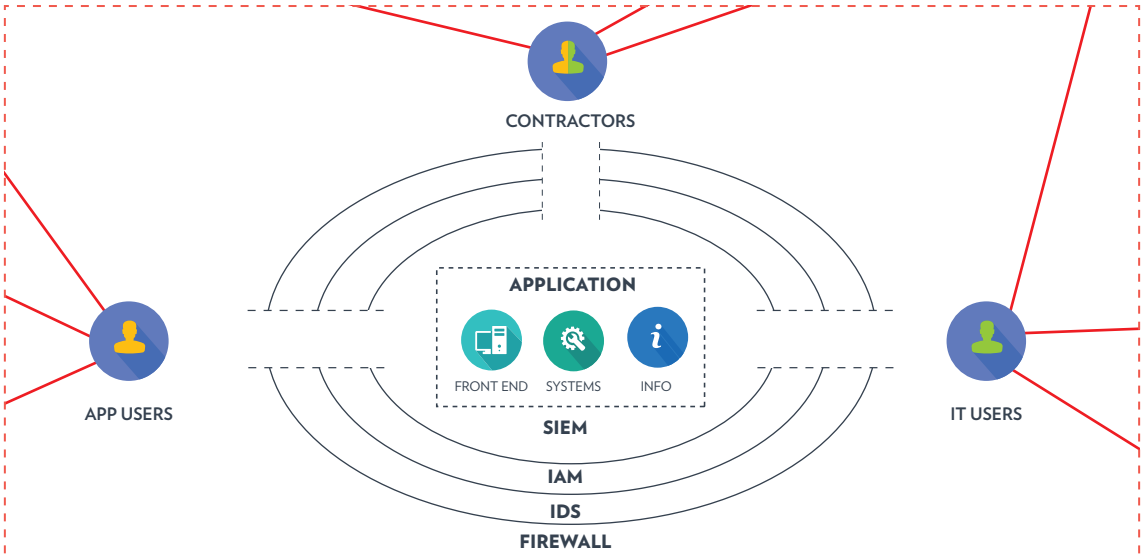
There has been a large push by industry and Government bodies worldwide to address security risk by ensuring organisations address their practices in ensuring their business practice remained security compliant.

Unfortunately, organisations that "tick all compliance boxes", still leave their business vulnerable, as it does not prevent abuse from Insider Threats. Sony, Target and Vodafone were all compliant at the time they suffered a data breach.

User based threat is an ever increasing major risk and requires a new approach.

Not only do users have access to your network, your users also access to other networks whether it is from home or even using their mobile iPhone. This means outsiders can use your employees or contractors as a gateway to access those assets you protected so well. Here are a few other scenarios:

- A person who has continued access to the organisation extranet event though this person no longer works there.
- Employees emailing personal data to the wrong recipient. Who hasn't sent an email to the wrong person?



"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]

THE TRUSTED USER

Every organisation wants to believe that their employees are above reproach. Every organisation also wants to believe that their employees are trustworthy. But that's not reality!

Do you know every employee of your organisation personally? Would you know whether any of these users are risky? After all, they are all trusted people. However, it's very difficult to identify whether they pose risk to your organisation. It's not as if they are wearing red jackets and saying "I'm a risky user".

An organisation is a "social invention" for accomplishing common goals. As such, organisations have people who present both opportunities and challenges.

Once a person has been selected to become an employee, that employee is then granted an "automatic" level of trust within the organisation.

This is where the risks start to escalate.

Here are some examples of failure in Trust:

- **Does trusting your boss leave you vulnerable?**

The Enron scandal, revealed in October 2001, eventually led to the bankruptcy of the Enron Corporation. It came about because Enron executives with the use of accounting loopholes, special purpose entities, and poor financial reporting, were able to hide billions of dollars in debt from failed deals and projects.

- **How much do you trust your co-workers or employees?**

Would you bet $400,000 on that? In a true story, a former employee at a bank in Queenstown, New Zealand was recently convicted and imprisoned after being found guilty of stealing more than $400,000 from her then-employer. Investigators found that the she began committing her inside-attack against the bank in 2010 and continued until 2013. Creating sixteen fictitious accounts with loans and overdrafts ranging from $12,000 to $120,000. Altogether, the amount totalled $402,386.

No matter how much you trust someone, it's always a good idea to trust and verify. Your most trusted employees are the ones with the most opportunity to steal, defraud, bend the rules or unintentionally divulged information accidentally.

> *"We're all digital. We're all vulnerable and everything is instant – so instant. Instant success and instant failure"*
>
> *[Madonna, pop star on the digital theft and leaking of her unfinished album "Rebel Heart" before it was released]*

THE CASE FOR USER BEHAVIOUR MONITORING

The risk of user-based threats has never been higher. Identifying who or what is driving a data breach is crucial for successful remediation and recovery at multiple levels.

Protecting organisation data is proving to be a daunting challenge for IT Security teams. The threat and potential for data to fall (or to be replaced) into the wrong hands is considerably high.

Organisations can't function without extending trust to their employees. It is this critical need which is the heart of the problem. Whether employees work independently or in teams, they still require to access to information assets to satisfy their work objectives. Given that users are provided with trusted and unchallenged access, enterprises have no visibility of what their employees are doing.

For this reason, organisations need to consider **User Behaviour Monitoring** which will address this critical gap. By monitoring, recording and analysing what users are doing, enterprises can now start to understand the direct relationship and the interactivity between the user, the application and data.

If someone has keys to the door, user behaviour monitoring will tell you exactly what he or she did once inside.

Knowing what users are doing is the missing key element in the risk equation.

When behaviour monitoring is focused on the user, actions taken by that user from the time of login to logout provides the security teams with clear picture of the user behaviour as well as the ability to quickly investigate suspicious, exception or abnormal activities.

With proper user based behaviour monitoring, the system will be able to deter and prevent data breaches scenarios from completing.

Users are a gateway of risk. It's time that organisations monitor user's behaviour and not assume that they have the enterprise at heart just because they are 'trusted'.

> *"The most effective way to prevent and detect insider crimes is to make it an enterprise-wide effort to master both the technical and behavioural aspect of the problem"*
>
> *[Carnegie Mellon Study, December 2012]*

THE FOUR ESSENTIAL COMPONENTS OF USER BEHAVIOUR MONITORING

RECORD AND MONITOR

The foundation of user behaviour monitoring is the ability to capture all user activity no matter where they log in from and no matter what application they may be using.

They say a picture is worth a thousand words. If a physical break-in to a retail shop occurs where money has been stolen, you can either get the forensic team to identify finger prints and other evidence of the break in or you can simply watch the CCTV to gain an understanding of how the break-in took place. Obviously both have an important place in such investigation. However, CCTV can provide you with the visibility and understanding of what took place much easier.

User Behaviour Monitoring is like the CCTV. It monitors the activities of what users do once logged in.

ANALYSE & DETECT

But the most crucial aspect of User Behaviour Monitoring is the analysis and context of the user activity. It must be able to transcribe captured on-screen user activities into meaningful user logs. Without these user logs, you can spend hours and hours looking for suspicious behaviour and activities.

USER PROFILING

With these user behaviour activity logs, you can now start to piece an "insider" story. The analytics of these user activities can provide you with a rich understanding of their behaviour.

- Recognise the interactivity and relationship between a user and associated applications
- Recognise the interactivity and relationship between a group of user and associated applications
- Understand whether abnormal activities are taking place by any user.
- Gain visibility in real time whether users are breaking corporate policies.
- Gain an understanding of whether users have the capability and skills to follow workflow processes.
- Gain real time visibility whether users are abusing, sabotaging or leaking corporate data.

SECURITY ECOSYSTEM INTEGRATION

And finally, these user behaviour logs can help and support the whole security Ecosystem integration. User Behaviour Monitoring paired with SIEM and Log tools provides organisations with a significantly more powerful security framework and efficient security force.

Pairing User Behaviour Monitoring with other security controls such as Identity Management, Access Management or Privilege Management tools will empower enterprises to enforce policies and governance more effectively.

"Don't expect what you don't inspect"
[The Success System That Never Fails. W.Clement Stone]

CONCLUSION

Your people are your greatest asset and the greatest threat to your business. It's time to protect your critical assets. Start to understand what your people are doing!

Infrastructure security and monitoring are important tools that can be useful for security but it falls short of addressing user-based threats.

If you want better security of your data and assets, then you will need to urgently start to address this Insider Threat security risk and include it as part of your overall security risk management strategy.

By fully preparing your organisation with the level of comprehension that we have discussed here, you will integrate the human dynamic with your entire security and risk management practice.

Only when you adopt user behaviour monitoring as part of your security practice, will you "see" and "hear" user behaviour activity with unprecedented awareness. And you will understand everything with a new sense of clarity.

Only then, when a user with the very intent of launching an attack against your organisation, they will quickly realise the futility of this activity.

DO YOU KNOW WHO YOUR RISKY USERS ARE?

This paper emphasises why it is essential that organisations like you take a proactive approach to identify and mitigate your risky users.

To assess your business risk and impact, you should be able to answer the following questions in the following checklist.

IDENTIFYING AND MITIGATING THE INSIDER THREAT	YES	NO	NOT SURE
1/ Do you consolidate all your logs into a central repository system?			
2/ Can you provide a single view across you whole security environment?			
3/ Are you able to analyse and correlate to pinpoint unusual events which may be risky?			
4/ Are you able to monitor system changes in real time?			
5/ Are you able to gain immediate visibility of compromised IT assets or the exfiltration of valuable intellectual property?			
6/ Are you able to precisely identify security breaches with root cause analysis and validation (including false positive identification)?			
7/ Are you able to monitor your compliance processes and procedures?			
8/ Do you know exactly who is accessing your data, what they're doing and whether it's legitimate or not, in real time?			
9/ Are you able to monitor and audit every action your trusted partner (vendors, contractors) are doing when the remotely access to your system?			
10/ Are you able to capture whether users are performing unusual operations or running rarely used commands?			
11/ Are you able to tell whether any of your users are running unusual applications?			
12/ Are you able to monitor and audit the activity of privileged users (system administrators, help desk users, DBAs, programmers, etc.) on critical systems?			
13/ Are you able to analyse user activity and generate real-time alerts about any suspicious or out-of-policy behaviors?			

For those questions that you are "Not Sure" or answered "No", we suggest you seek advice by contacting CommsNet Group either by writing to **insider-threat@commsnet.com.au** or calling **02 6282 5554** today.