Mitigating Your Biggest Security Challenge: Your Insider Threat

Why User Behaviour and Machine Intelligence is The Key to Preventing Your Next Breach

User Behaviour plus Machine Intelligence IS THE KEY to Preventing INSIDER THREAT

Identifying Risky Users Mitigating Insider Threat

You do have the right to offer this report for free, offer it as a bonus or give it away to your clients, partners, suppliers, friends and business associates. You can also send this material as part of your sales and marketing strategies. You also have the right to pass these rights along to anyone who receives this report. You do not have the right to change the content in any way or quote it without giving credit to the author.

Enjoy
Boaz Fischer
© 2015
The Challenge

If I ask you what is the greatest challenge that you face today in protecting your business from your next security breach, most will probably say a list of external resources such as hackers, malware, denial of service and phishing.

But in reality, the greatest risk to any organisation today comes from within. Yes, the insider; that 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; Or perhaps it’s the unscrupulous user that uses your business for their personal gain; Or perhaps it was 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.
- AT&T one of the world’s largest telecommunication carriers warned its consumers about a data breach involving an insider who illegally accessed the personal information of an unspecified number of users. The compromised data includes Social Security numbers and driver’s license numbers.
- Barclays Bank, one of the 10 largest banks in the world lost control of 27,000 customer files containing everything from passport and national insurance numbers to information about earnings, savings, mortgages, health issues and insurance policies. This breach was potentially worth millions on the black market, as it would allow bad actors to use the stolen information to target unsuspecting individuals. The bank’s own employees were allegedly perpetrating the sale and distribution of the stolen information. To this day, no arrests have been documented.
- Target announced that a trusted third-party heating and air-conditioning contractor was responsible for the biggest data breach in its history. In this insider incident, 40 million customer credit and debit card numbers were breached, along with 70 million records containing names, addresses, email addresses and phone numbers of Target shoppers.
Let's define what an Inside Threat is: Inside Threats are caused by a wide range of offenders who either maliciously or accidentally do things that put an organisation and its data at risk.

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

Results from the 2015 Vormetric Insider Threat Report shows that Insider Threat awareness levels have increased. Only 11% of respondents felt that their organisation was not vulnerable to Insider Attack. That means that 89% feel at least somewhat vulnerable to an Insider Attack.

The most dangerous insiders have privilege access. Far too long system administrators with privilege access to the most sensitive corporate data have had open access with few controls placed. Management have realised this that a rogue employee with admin rights can do far reaching damage to their organisations.

Verizon 2013 Data Breach Investigation Report, which reported that 76% of all breaches originate from accounts with access to sensitive data.

Yet, what’s most alarming is that 84% of internal data breaches come from regular business users accounts with no administrator privilege according to the 2014 IBM/Ponemon Cost of Data Breach Report.

© 2015 – Intellectual Property Rights B. Fischer
The Risk Is Real

The Verizon 2014 Data Breach Investigation Report shows that not only is the risk to the organisation real, but the threat come from anywhere.

The trusted insider is anyone or anything that operates within the organisation using an unauthorised identity.

71% of employees say they are granted excessive access to company data they should not be able to see. They went on to say that when the access is not tracked or audited, an attack that gains access to employee accounts can have devastating consequences.

Organisations have a wide range of issues to worry about when it comes to IT Security – malware, phishing, hacking, denial of services attacks, BYOD, Cloud as well as adhering to security compliance are governance. Many security solutions are put in place to stop the illegitimate outsiders getting access to internal systems and sensitive information. However having visibility and control of what insiders are doing is now causing sleepless nights for the CEO.

Let's define what Risk is: Risk boils down to two things – Assets and People. It is the interaction of People and Assets that creates risk

- Assets without anyone accessing them – No Risk – but there is no business to be transacted either
- People without anything to access – No Risk – but nothing for them to do

In the world of Information Technology:

- Assets are represented by applications, systems and information
- People are represented by users
Identifying Activities and Intent

The 2014 IBM/Ponemon Cost of Data Breach Report shows that 29% of data breaches came from system glitches. This means that 71% of incidents have to be investigated and security must change its approach to better identify and track activities by user.

Users who maliciously don’t generally perform a single malicious act in a “vacuum” with no indications. They precipitate malicious actions with other identifiable signs. These signs can be activities like exploration of systems and data stores that they don’t normally operate in or performing uncharacteristic data collection and or movements, operating outside of their normal access times and any other indicators.

In fact, Patrick Reidy, the FBI’s CSO, reported in Dark Reading. “We look at how people operate on the system, how they look contextually, and try to build baselines and look for those anomalies.”

If security can detect such precursors and alert such suspicious activities in real time, this is a huge step forwards in proactively battling the insider threat.

Patrick Reidy outlined his recommendations in a paper called The 5 best practices for combating the insider threat in your business. This is a summary of the key points from Forbes:

1. **Focus on deterrence not detection.** In other words, create a culture that deters any aberrant behaviour, so that those who continue with it will stand out from the ‘noise’ of normal business and can be more easily found and investigated.

2. **Know your people.** Know who your weak links are and who are most likely to be a threat. Use your HR data to narrow down threats, rather than looking for a needle in stack of needles.

3. **Identify information** that is most likely to be **valuable** to someone else and **protect it** to a greater degree than the rest of your information.

4. **Monitor ingress and egress points** for information (USB ports, printers, network boundaries).

5. **Baseline normal activity** and look for anomalies.15

It’s interesting that Behaviour Anomaly Detection technology has been doing precisely this for over a decade.
Machine Behaviour Anomaly Detection (BAD)

BAD an advanced approach to enterprise security. BAD was based on a new premise - rather than applying behavioural thresholds or industry-based patterns, or relying on endless on-site scripting updates, BAD used algorithms to ‘learn’ the normal behaviour and usage of your ICT systems. In summary, it includes the following key points:

- Establish a baseline of normal behaviour - and pinpoint exceptions
- Adapt to authorised network changes & usage spikes - yet distinguish the risky anomalies
- Connect seemingly unrelated events that pose a threat - which are otherwise invisible
- Monitor the whole enterprise for non-compliant events – continuously and in real time
- Assess unusual events in the context of their risk to the enterprise
- Take protective actions to minimize loss instantly – not hours, days or weeks after the damage is done.

As one recent commentator noted, the FBI’s baseline methodology means that ‘If a Bradley Manning starts to exfiltrate hundreds of thousands of documents that aren’t really in his area of study, then alarms go off and these things would be caught sooner, according to FBI training video on new Insider Threat to Intelligence Agencies, CBS – July 2013
What Infrastructure Monitoring Doesn’t See!

When it comes to the risks associated with our Assets, we have done a pretty good job:

- We have a firm understanding of the critical assets that are most valuable to our company – Employee/Customer data, etc…
- And we have put in infrastructure to manage them

But what we are missing is that our users are exposing us to a huge amount of risk that we not aware of and if we not aware of the risk, how can we protect ourselves from it.

So what have we done to date? We have taken what has worked for protecting our assets and attempted to use them to protect our users by guessing what they are doing and attempting to control their access.

Log collection and analysis is the typical security team will look to for infrastructure monitoring. Machine Behaviour Anomaly Detection is an excellent technology to understand machine intelligence but not user behaviour.

It is interesting to understand that logs were originally written by developers to debug applications and systems, not for security and certainly NOT to understand user behaviour.

Identifying suspicious activities often require searching through multiple logs across the environment to try and piece a story together. In many cases of breach, logging did not log the entire event such as moved, deleted, copied files.

Further, many applications lack sufficient activities and change logging to notify administrators of malicious actors. Secondly and more alarming, there are many applications that just don’t generate any system event or logs. So how does a log analysis application see the whole picture? It doesn't!

No wonder, the average time between breach and detection was 229 days – 2014 Mandiant Threat report.

As such infrastructure based detection and alerting is insufficient in identifying critical compromises.
Identifying and Mitigating the Insider Threat

User Activity Monitoring

Given the examples of the shortcoming commonly experienced with traditional security logging and analysis solutions, it is clearly evident that we need to understand and monitor user based activities.

So what is the first step to protecting our organisations assets? Understanding our User-Risk profile. It is the key to identifying behaviour that leads to data breaches.

When monitoring is focused and captured on the user and the action taken by that user from the time they log on to logout in the way in which it was performed (like a movie), the organisation has a key understanding and visibility.

So when the question rises “who did what, when and how and from where?” We can quickly identify and answer this question. No finger pointing and no time wasting!

Now here is a solution that focuses on human behaviour with the ability in real time detect abnormal suspicious user activity and appropriately alert these threatening actions and activities to the appropriate people.

Gartner has predicted that by 2018, User Activity Monitoring will be part of 80% of enterprise security solutions.

*USER-BASED SECURITY*

"Securing Enterprises will require a shift to User Activity Monitoring"

Source: Prevention is Futile in 2020, Gartner
The Best of Both Worlds

Infrastructure monitoring is a very important management tool that is useful for security in understanding Machine Intelligence. Organisation need to bring the Human intelligence to address user activities. By combining both the Machine Intelligence and Human Intelligence working together, organisations can start in identifying and mitigating the Insider Threat.

How it works?

Security incident involve a combination of users and system devices (application, network, servers). By collecting Observe IT data into Huntsman, Analyst can now monitor the security risk of users in addition to risk from devices. ObserveIT metadata is integrated with Huntsman and will automatically collect, match and correlate all user activity data with data collected from other devices. Additionally when an incident is generated in Huntsman, all user information surrounding that incident can be automatically added from Observe IT.

The following diagram, illustrates that “user behaviour” is about the various “touch points” the user has interacted with their applications and data. And these applications are built on infrastructure and systems.

User Activity Monitoring must monitor the top two layers of user activities. The last two layers require to be monitored by infrastructure monitoring. Together, these activities require to be correlated to provide a complete picture of organisation risk.
The Key Benefits

- **Gain Visibility of Insider Threat** - Identify risky users by monitoring user activities anomaly behaviour as well as breaching organisation policies

- **Understand Insider Threat** – Correlate User Anomaly behaviour with machine behaviour anomaly detection.

- **Recognise Insider Threat** - Analyses and correlates events to pinpoint unusual events which are also risky and understand what User Activities may have instigated them

- **Identify Insider Threat** - Triages User and Machine alerts so you can focus on the genuine threats and take immediate action.

- **Detect Insider Threat in Real-Time** - Know precisely what users did, how and from where - Including applications launched, files accessed and URLs viewed

- **Alert Of An Insider Threat** – Allow instant response to suspicious user actions. Identify user actions that breach organisation policies. Identify user behaviour anomaly and correlate to the exact machine and occurrence.

- **Root Cause of Insider Threat** - Discover the root cause of system configuration changes within minutes

- **Identify Privilege Account Users With Insider Threat** - Monitor privileged account users, including shared administer users with 2nd level authentication,
Conclusion

Without a doubt organisations are facing increasing security threats. Every organisation wants to believe that their users, consultants, contractors, vendors and partners are all trust worthy but the truth is not so. Ins[12]ider Threat is the biggest threat that any organisation is now facing!

That is because, a disgruntled employee, a rogue administrator or a careless business user have access to the most sensitive data.

Unless properly controlled all of these groups have the opportunity to expose the organisation to massive business exposure, massive costs and severe damages.

To keep an organisation safe from Insider Threat a unified solution is absolutely necessary, because it incorporates two sides of intelligence behaviour gathering - machine monitoring and user monitoring activities in real time.

The result is a complete solution for identifying and managing all forms of user and machine based risk and most importantly, mitigating your next breach.

- How well does your organisation manage it’s Insider Threat risk?
- How much visibility of your users do you have?
- What applications are they accessing and why?
- How well do you understand the user behaviour in real time?
- How vulnerable are you to Insider Threat?

Complete the Checklist below to assess your ability to Identify and Mitigate your Insider Threat.
Are you able to Identify and Mitigate against the Insider Threat?

This paper emphasises why it is essential that organisations like you take a proactive approach that appropriate focus and tools in investing a balance of technical controls and procedures that take into account human as well as machine behaviour factors.

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

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

To mitigate your biggest security challenge - your insider threat, email or call Commsnet today and arrange for a Discovery and Audit of your Privilege Accounts.

To find out more, visit


For more information, please email us at info@commsnet.com.au or call 02 6282 5554 today.