7SS Series

SEVEN SIMPLE STEPS

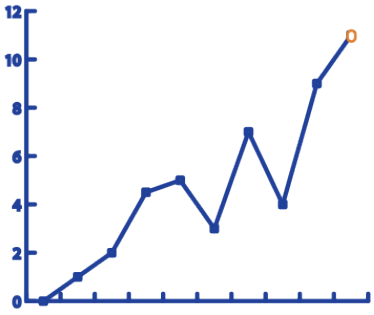
For Successfull Internal Threat Management

Almost everyday there is an article, or news item telling a sorry story of how someone, somewhere made a mistake that led to the loss of either a device or data. Or worse still a company has been compromised by a security breach which has led to the loss of thousands of customers' confidential details, addresses, contact details, bank or credit card accounts etc. In some cases these are caused through the accident of a user, in some the malicious attack from a dedicated external hacker and worst of all a disgruntled employee.

So what do you do? How does your organisation start the process of successfully protecting itself against all three? We've put together our 'Seven Simple Steps' for getting you started on the long-term management of your organisation's data.

1. What to Consider?

To begin you must consider 'why is monitoring important to your organisation?' Are you looking for something to improve key performance indicators (KPI)? Securing systems as part of a data loss prevention programme? Or maybe protecting staff from cyber bullying? Once you have identified why you want to monitor then it is a question of who you want to monitor. There are some organisations that once at a critical size will simply monitor everyone. In general terms we have always felt this is the fairest way; all staff treated equally.



Three key elements of what to consider are: Who? What? Why?

Who to monitor is a highly important consideration. Now, the most obvious choice would be "well, that's easy, my employees of course!". Yes, absolutely monitor the activity of your employees, however it is not just immediate employees whom have access to sensitive information and data regarding business operations. Consider third parties such as partners and suppliers – stakeholders as an entity in fact. Anybody with access to confidential information is to be monitored. Cover all grounds and do not allow your organisation to be exposed.

Written by: Ellen F Powles and Mike Q Hainsworh

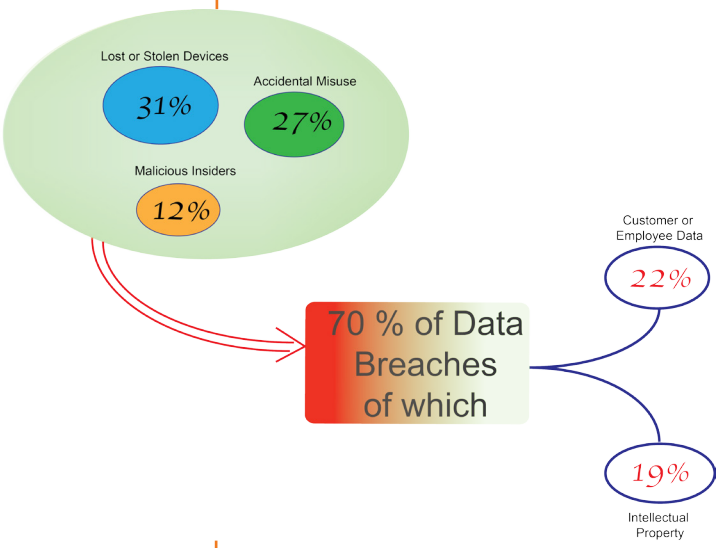
What to monitor may be slightly more complicated what with the modern 'flexible' working attitude that has been adopted by many. Yet, with solutions such as mobile device management and employee monitoring software it is simplistic to monitor employee behaviour, activity and productivity in real time focus. You should consider monitoring these three aspects as behaviour will provide you an insight into daily goings on, activity will grant you access to whether or not people are working and productivity analyses will allow you to understand how much of the activity is beneficial, efficient work and how much is idle screens or compulsive scrolls of the social media feeds.

Finally, why? Why make the effort to monitor? In a word; protection. In two, prevention and protection. In deploying such monitoring methods, you will not only detect anomalies which will help you decide a plan of action, you will also gain an insight into every day activities of your team, your people, your organisation. By opening your eyes, in a sense, you will become more aware of what adaptations are required in order to protect your data and sensitive information likewise, discover threatening behaviour and whom it may be coming from.

2. *Internal Threat Management*

Perhaps it would be beneficial to reiterate just what is meant by internal threats. Simply put it is a threat originating within a company; the malicious hacker is in the form of an employee or internal stakeholder. Initially, three types of internal threat stand out:

1) Structured: individuals/groups competent in computer language
2) Unstructured: a hacker using easily available tools such as password crackers
3) Internal threats: authorised personnel accessing the network.



Internal threats generate serious damage to organisations; records are altered or destroyed, fraudulent behaviour occurs and disruptions to the network can force operations to cease. It takes the simplest of web searches to read a multitude of articles such as: *http://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell* which detail what can happen.

If you're hot on the tails of internal threats from the outset you will develop more and more expertise and become vigilantes in your own right. To start with, get the right people on the job, as mentioned in point 2, HR team members are perfect candidates for your virtual team. But shake it up a little, mix members of various departments in – do not only leave it to the Geeks. Often 90% of internal threats are non-technical, so, throw in a couple of stakeholders, add a legal representative in there and you'll be set. Fear not, however, this does not mean you have to invest more capital into hiring new bodies – select the best men (and women, of course) from your existing workforce and integrate the task into existing operations.

We know which are the best internal threat management solutions and it's important to acknowledge a couple of pointers. Ensure **you have** analysed and **identified** just what is requiring protection or attention. Ideally, you want to be ensuring **your data and intellectual property are** not **vulnerable to theft.**

Identify areas **exposed** to fraudulent attempts and ensure your **corporate resources** are encrypted, **lock them down!** Analysis will help you nip it in the bud early on. Start proactively making changes amongst the organisation; introduce policies such as prohibition of USB usage and either limit, or structure the protection of cloud file sharing. **Finally**, rather than using the scare factor **encourage** senior executives to **invest in** solutions which emphasise the benefits such as employee **protection**, **productivity** improvements and enhanced **security**.

Proactive methods can prevent your organisation coming under fire; **simple** actions such as network behaviour **monitoring** and productivity analysis **can detect** suspicious anomalies and encourage you to begin an investigation if a person's activity is **unusual** for their normal **behaviour**. A proven software solutions **allows** you to receive real time **focus** of what is going **on** over your corporate network, who is acting **productively** and who is spending a considerable amount of their working day in an idle position – physically and virtually, both are **concerning**. Internal threat management is one of our 7 Points because it's crucially important to **risk mitigation** and the protection of data in **the** organisation. Simple, yet **effective** methods can be the **difference** between exposure and breach, which can lead **to** loss of data and **market confidence**.

3. Productivity and Social Media

Let's start with statistics, after all who doesn't love a stat? So a few figures to acknowledge when considering productivity analysis as a means to mitigate internal threats are:

1) Google usage is the biggest cost of time at work with Facebook being a close second, given that most people use Google to search that makes sense, but Facebook?
2) 70% of all web traffic to the world's most trafficked free porn site occurs between 9am and 5pm, the typical working hours
3) The average employee wastes 2.75 hours of the working day on personal Internet use, this equates to 7% of the employees' salaries per annum

With regards to social media, it is expanding day by day and more and more platforms are becoming available for your employees to procrastinate on. However, workplace distractions can lead to internal threats, by cutting down on access to external sites you are proactively minimising the opportunity for insiders to harm the organisation. Unfortunately, social media can distort the boundaries between work and home which leaves the organisation vulnerable – you may not be fully aware of what sensitive information is being shared over the social media platforms or whether your organisation is under threat of malicious behaviour. The way to approach this?

1) Apply acceptable use policies, as previously mentioned
2) Let employees know what you deem to be acceptable behaviour in the workplace; How an employee may utilise the Internet
3) Educating what can and cannot be shared regarding your organisation
4) Consulting with them should you desire to monitor their social media threads

However, should you wish to take this approach be cautious not to disgruntle your staff by displaying a negative attitude towards social media; instead it would be wise to promote a work-life balance, after all that crystal clear line between work and play is becoming blurred not helped by the utilisation of modern technology in the workplace.

To help understand the damage social media can have on an organisation, specifically internal threats: Estimates have been produced stating the misuse of the Internet and social media by workers costs the British economy £14bn every year. In addition, many employers are having to grapple issues such as time theft, defamation, cyber bullying and invasion of privacy. Now, whilst it is difficult for employers to keep on top of such issues what with switching between screens there are solutions to crack down on the compulsive tweeters or the cheeky time thief.

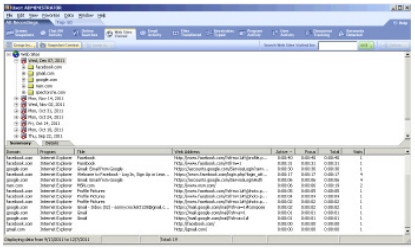
Productivity analysis methods allow you to access near video play back of screens with real time focus, therefore you can witness who is committing time theft at any given moment. Similarly, productivity analysis enables you to identify the high achievers and those that don't. So, rather than miss the tricksters pulling a fast one by updating their statuses, transferring files through social media via their mobiles yet adamant they are innocent claiming it was a crucial works email, deploy productivity analysis solutions and put yourself ahead of the game.

4. *Who to Work With*

Look at both internal and external options for this point. Internally your HR, ICT, Senior Management teams are the people you want to be concerned with Internal Threat investigation, externally from a supply chain point of view you'll want to be building a business relationship with IT experts who can provide you with the most suitable solutions at the best value for money.

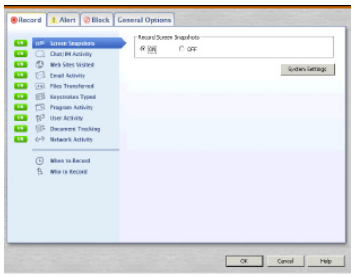
So, what you'll be requiring from HR and ICT is dedication to and support for the task. You will need the contribution and of trust your most analytical employees to manage your internal threat mitigation software, with the software ideally giving dashboard access to key information. Typically, with HR and ICT being so up to date and aware of the occurrences regarding personnel they will be savvy at monitoring data and combing through to discover only the most significant details. By working with appropriate software, dedicated and focused employees, you'll be able to decipher the detail to illustrate the facts and have accurately analysed and reliable reports and judgements of suspicious use.

Alternatively or, additionally you can venture outside the walls of your organisational environment and have monitoring and penetration testing undertaken; it would need to be done by experts in the industry whom will know every nook and cranny to explore. We always recommend careful consideration on who to work with ensuring the right people will be able to provide you with solid data loss protection techniques as well as the means to prepare your systems as a preventative solution should the worst be realised, sadly nothing in life is 100%.

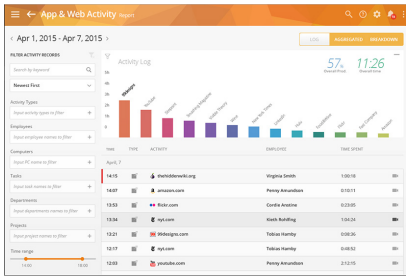


With internal threats becoming increasingly sophisticated it is crucial for everyone and you to build a bond with experts whom are able to provide you with real time focus and reports. The beauty of such feature is that you will receive reports constantly with detection of suspicious behaviour being highlighted as soon as it happens.

The best part? Such monitoring takes place in a passive manner therefore, allowing business managers to focus on critical operations for the organisation rather than investing time into monitoring internal threats. When finding an expert to work with it is vital you opt for the most adaptable team; not every business is the same, each organisation has it's own idiosyncrasies, ensure it is cared for with only the best tailored consideration which caters for your needs.



The way to do this? Find a consultancy who understands threshold setting, do not settle for a generic product provider, but look for multiple options. Finally, ensure they come up with the goods and are willing to demonstrate their fit within your environment.



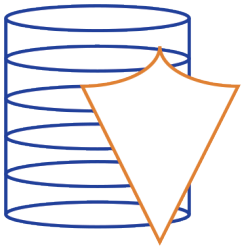
Its key to work with people with a 'finger on the pulse' approach and do not allow your organisation, of which you have trusted them with, to fall victim to preventable attacks.

5. HR and Human Rights

The challenge of the modern HR professional today is finding a balance between a motivated staff, provision of policy to secure the organisational data and the legal implications of each. The challenges that we see HR facing in this context are:

- How do we keep staff motivated?
- Is this policy up to date?
- What are the legal impacts of a policy?

One might argue that if an organisation has to I worry about motivation then it really ought to look at hiring practice and line management. Yet once a policy is implemented its delivery will have an impact on morale. Often we see Acceptable Use Policy (AUP) sitting as part of the company handbook, yet the practical delivery of measurement and monitoring activity is left to the ICT team to worry about, with HR only getting involved if they consider the delivery of monitoring too Draconian. So there must be some balance?

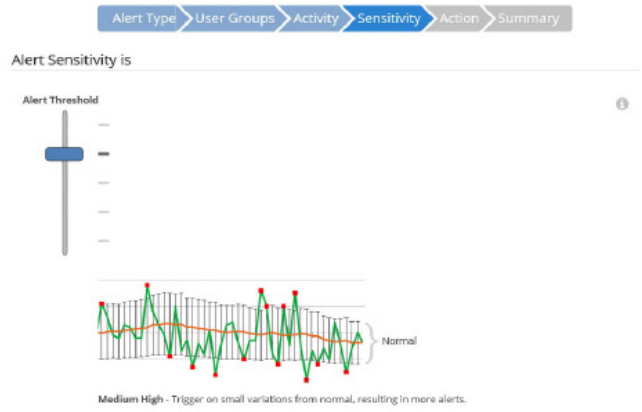


Unfortunately, internal threats have become all too common. They are encouraged by the increased access granted to sensitive organisational information and data. With technology continuously evolving the methods of extracting information and generating a cyber attack internally are becoming ever more sophisticated.

These movements are not to be ignored, internal attacks cause significant damage to an organisation and are capable of forcing closure, impacting on stock and customer confidence. The type of internal threat that we have seen are not exclusively initiated by an employee, although a disgruntled or demotivated staff member may initiate just as easily as an innocent mistake by an unwitting one, as happened with Coca-Cola a breach via a targeted executive in 2009.

However, having a solid and skillful HR team working in tandem with their ICT team such dilemmas can be managed effectively. HR can use systems to log the behaviour of your employees, making them the eyes and ears you need to detect any suspicious behaviour, likewise monitoring software as previously mentioned can be deployed with seamless integration into the current IT infrastructure.

Managing your people effectively will deter internal threats as potential attackers will acknowledge your awareness of potential crises. It is not all one sided however, monitoring internal threats can be a team game, HR should command the support of employees and encourage their participation in the reduction of internal threats and malicious behaviours.



By instilling a security culture into your workforce internal threat management will become an everyday norm for your organisational team.

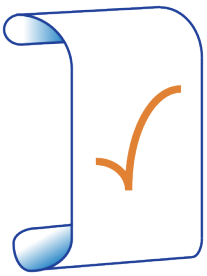
Three key elements for HR to consider with regards to internal threat management are:

1) **Manage:** assets (employees, intellectual property), identity (know who employees, partners + suppliers are, time management) and the volume of transactions
2) **Behavioural Anomalies:** crucially important for when real time focus is adopted, these will highlight main areas of focus
3) **Integration of Business Functions:** ensure there are no blind spots amongst functional areas

With HR and internal threat management, context is key. This informs the workforce of sensible yet insightful rules and generates meaningful alerts for HR to analyse.

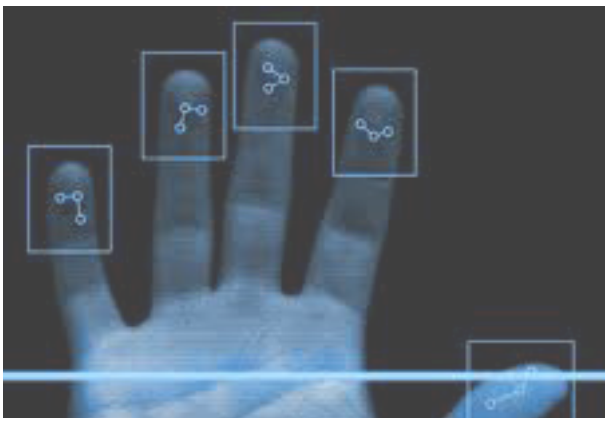
Written by: Ellen F Powles and Mike Q Hainsworh

Commonly, the most valuable rules and regulations are the least obvious; therefore, it is of great responsibility to your HR team to ensure all stakeholders are appropriately aware to prevent any human errors or mistakes from occurring which may be interpreted as attempted internal attacks.



In relation to this, it is important to consider human rights when discussing the role of HR in monitoring internal threats. It is vitally important to make every member of your workforce aware that monitoring is in place. Similarly, the monitoring methods deployed must comply with regulatory frameworks, being both legal and ethical. There is never any need to neglect human rights when utilising such monitoring methods. Publicise the information internally, ensure your employees are aware of the happenings yet remain unpredictable to prevent circumvention. A simple pop up window at login, or an elective sign-in to monitoring are easy ways to overcome this.

Human rights are to be greatly respected. It must be known that it is rarely legal to monitor your workforce without consent or awareness; a simple statement in the Employee Handbook, or Contract, or AUP comply with these two. Guidance given by the data protection law states: secret monitoring is not allowed in private areas, such as toilets…so is the company laptop, desktop, phone, desk a 'private area'; are the emails an employee sends, or the web activity they have during the time they are contracted to work for you on your organisation's infrastructure 'private'? One might argue that banking/credit card details are private and any decent monitoring software will keep it private. Therefore, codes of conduct and policies should be in place to inform your employees of the monitoring and what is expected of them with regards to acceptable behaviour. By covering all areas from the initial point of employment you prevent your organisation becoming vulnerable.



So, its simple. Justify your use of logging emails, recording screen activity and receiving alerts and Bob's your uncle! There will be no excuse for disgruntled employees crying about Big Brother watching them. Failing to educate your employees on what monitoring methods you are using can lead to employment tribunals or complaints to the Information Commissioners. So make it crystal clear, explain your policies! The only time you are able to monitor without the knowledge of your stakeholders is: if you believe the law is being broken or you have reason to believe the investigation will be impacted if it was shared.

6. Communication

Now, a crucial element to internal threat mitigation is transparency. You must ensure the communication throughout the organisation is clear and maintained. According to the Huffington Post (*www.huffingtonpost.com/robert-siciliano/data-breaches-how-to-pro-t_b_5357354.html*) the more transparent the network and security policies the more effective each department will be in the communication of requirements, needs and wants.

Encouraging transparency in the work place and combining this with stakeholder management aids the discovery of risks. It is important to identify both obvious and more discrete stakeholders and analyse their authority and interest. From here you can then develop a communication plan accordingly and divulge only the most important and relevant information to each party. By deploying such communication strategy not only will you build positive relationships (the foundation of any effective communication) but you'll also find the problems before they find you. What's not to like? However, it is beneficial to develop two or more mediums of communication per stakeholder, whether this be a combination of email and documentation or a personal one-to-one and a telephone conversation.

The secret to a well structured, comprehensive communications strategy is ensuring your employees are made aware that cyber security and data privacy is an element of each member's job role and that the entire workforce is expected to proactively prevent internal threats and mitigate risks. This can be instilled through the rewarding of employees whom actively take a lead in this expectation. Rewards could be given to those who turn in any phishing emails, proactively change their passwords frequently or identify potential threats throughout the network.

Clear communication will deter internal threats as those with the intention to harm the organisation will acknowledge that the culture is such that each individual makes an effort to mitigate risk, this will minimise their chances of a successful attack.

Communication is key in preventing initial internal threats, but how important is it following an attack? Just as important, if not more so, remember the Blackberry outage of 2011, how after four days of issues finally there was some feedback from senior management? With immediate communications could they have stemmed the exodus of customers? How you communicate with your stakeholders is vital, suppose there is a breach you would need to consider if there was a lack of communication? Thus your strategies would require a revisit; whatever the reason it is vitally important to communicate any past breaches along with instructions on how to react or prevent such undesired circumstances. Again, transparency here plays a role, explain everything you know – do not hide details, the last thing you want is more disgruntled employees on your tail because you did not provide information with clarity. Not only will honesty and openness provide reassurance but it will deter future, potential threats by unsuspected insiders.

A common flaw in communication is the lack of seniors in contact with employees across the organisation; empowering seniors to communicate is a form of threat mitigation in its own right. Trust and respect will be developed across all levels of the workforce hierarchy and with general employees feeling acknowledged and respected by their superiors, temptation to attack the organisation through frustration will be mitigated. Two-way communication creates a platform for employees to voice their concerns, questions and requirements freely in a less daunting environment. Freedom of speech and the encouragement of communication creates harmony amongst the work place and as a result deters internal threats.

7. What You Can Do

And so we're brought onto the final point of our **'7 Simple Steps to Internal Threat Management'**. This step allows us to put everything into a nutshell for you and simplify what has been said throughout. There are a number of actions to be taken in order to protect your organisation effectively and mitigate internal threats.

The one we should start with and place considerable emphasis on is employee training. Educate your employees from the initial recruitment stages on what an internal threat is, how they are devised, who carries them out and the implications they have on the business – not forgetting the consequences they have on the instigator. Investing in effective training and education will benefit your organisation substantially; often internal threats and attacks are devised unintentionally by employee errors occurring due to lack of awareness and education in the relevant areas.

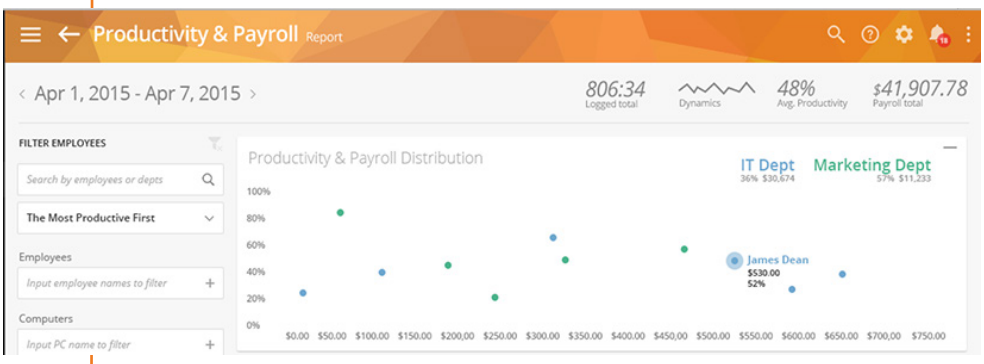
In relation to devising and applying **A**cceptable **U**se **P**olicies (AUP) within your organisation will also manage internal threats and improve productivity. The policy should clarify what is deemed acceptable with regards to behaviour in the work place, Internet usage (personal, social media access) and access to corporate resources at any given time, being able to monitor the AUP validates having it in place, otherwise it is like having CCTV but not turning the camera on. Likewise, disciplinary action for breaching the code of conduct should be communicated.

Make your employees aware of the ethos amongst the organisation, ensure they are kept up to date on all policies throughout the network and emphasise the severity of failing to comply – this could be as simple as an employee calling in sick yet colleagues report seeing pictures being uploaded on their social media sites. At the end of the day, your organisation needs protecting from all angles; do not allow a preventable blind spot to tear down the entity. Internet usage policies also create the same protection and allow your business to enjoy the benefits of the Internet whilst reducing pitfalls. By deploying the policy, you are ensuring effective use of the Internet through the use of firewalls and security software, restricting access to settings changes and applying rules and regulations to the connection of personal devices to the network. Internet usage policies are productive as limits are applied to personal use, website visits are restricted, downloads are controlled and guidelines on social networking use are given.

Understandably, every organisation has budgets they must adhere to, however it can be highly rewarding to invest time and capital into monitoring solutions. Monitoring solutions as already briefly touched upon throughout the other steps provide real time focus into every day happenings throughout the business. With more and more employees being given the option to work remotely – away from the organisation's main base – monitoring solutions are increasingly becoming an essential to risk mitigation strategy.

Remote working poses unique challenges for performance management. Now, most managers providing remote working opportunities are focusing on end-products as opposed to time management however, monitoring solutions enable both aspects to be considered which is highly valuable in internal threat management scenarios.

The solutions will allow you to gain an insight into how productive your staff are when away from the work environment and how they are utilising the corporate resources from a third party destination. This agreement ties in with the communication element as it is crucially important to maintain on going dialogue with the staff working remotely as well as those present in the workplace.



Productivity analysis is an advantageous element of monitoring solutions as it allows HR or seniors to understand how corporate time is being consumed and to what extent of it is being invested into completing tasks. Productivity analysis solutions generate alerts when behavioural anomalies are detected – so any suspicions you have regarding idle workers, those who will need motivating, will be either confirmed or reduced.

Now, it may seem unnecessary to clamp down on every period of idle time however it could be that a potential internal attacker has opened up the corporate resource with the intention to lead the analyser into a false sense of security, allowing them to believe they are working whilst actually plotting how to hack or steal sensitive information from the organisation. Therefore, the beauty of monitoring solutions combined with productivity analysis is the simplistic notion of being informed of alerts and having the real time evidence to justify approaching the situation from a defensive angle.

7SS

To conclude the 7th step of our guidance another security action you should consider is a departing employee policy. How will you protect your business once a member has left the organisation? Simple. Initiate a departing employee policy from the point of recruitment and ensure employees are aware of this as soon as they are employed by the business.

The policy should be focused on securing the IT infrastructure of the organisation through the suspension of access to systems and compulsory requirement of password changes prior to contract termination.

To emphasise the policy employers should request the employee to sign a confidentiality agreement and outline the terms and conditions as well as the consequences should the agreement be breached.

So, there it is Incommsec's '**7 Simple Steps to Internal Threat Management**'. By educating your team and the relevant stakeholders within your organisation on the advice provided in our 7 steps you will increase the protection of the organisation substantially whilst deterring internal threat risks as a result. It is vitally important to ensure all areas are covered, as much as we'd like to assure you that all your employees are trustworthy angels without any bad intentions that isn't always reality. Our aim is to help educate on how to prevent an organisation coming under fire from preventable attacks as well as providing the solutions to create more harmony amongst a workforce.

If you want to find out more information or follow us throughout business please feel free to visit our website www.incommsec.com, follow us on twitter: @incommsec, connect with us on LinkedIn: Incommsec Limited, or even pick up the old fashioned telephone as we're happy to talk: 020 3369 6301

Written by: Ellen F Powles and Mike Q Hainsworh