Protecting Data & People in the Digitally Connected Workplace

Executive Summary

Many things come to mind when you think about protecting your business, most business leaders would focus on certain specific and often obvious threats, for example; control overhead costs effectively, monitor profits closely, keep an eye on your competitors to ensure your business remains a viable option in the marketplace. There are then other aspects to business protection; you may think about types of disaster and how your business might survive during a power outage or a major event like a flood or fire. With risks like these a business would ensure it has got the correct liability and continuity insurance.

Most organisations are now reliant on the use of computers and digital information for their day to day operations and this practice introduces a completely different set of very serious risks and threats to their productivity, stability, and even their legality. Overlooking these threats can, even in a small business cost upwards of half a million pounds and not dealing with these threats can land you in court, with all of the costs that implies and many businesses simply do not survive the consequences. Ignoring these threats can wipe out your competitive advantages and literally hand your most important business assets to your competition. Once identified it is fairly obvious to see that many of these threats stem from one source; employees and in many cases most employees are not even creating these threats maliciously, they are simply not trained correctly or they don't stop to think about the consequences of what they are doing in their daily duties.

Collectively these risks are known as the "insider threat" and this document looks closely at the subject how to protect your organisation from the most serious and common of these risks in the digitally connected workplace.

Threat 1: Loss or Theft of Information

In today's competitive marketplace, every piece of digital information is critical. Your employees, of course, have access to a great deal of confidential and sensitive information. It is natural for employees to enjoy their work and hopefully be ambitious and excited about what they do for a living, additionally they are often excited about what the company does or is about to do. Sometimes however they just can't resist sharing a little, perhaps "leaking" a rumour to a supplier or customer about an upcoming product launch, or providing just a bit too much detail when sending an email, or even confessing (leaking) some delicate insider information over a chat message. Sometimes it isn't the information itself that is a problem, but the timing or context of the information leak, such as employees who discuss upcoming products before release or let slip about that large piece of business that hasn't quite been finalised and is under strict non-disclosure. In the end, of course, it's the employer that pays the price. Once the information is out there, it's out there and you will spend an immeasurable amount of time trying to track down who was responsible. That's especially true when employees use Internet email accounts. You simply don't have an audit trail for those activities, making it incredibly difficult to track down the perpetrator and deal with the problem. Once again, many breaches of this kind aren't intentionally malicious, employees just aren't always armed with good decision making skills, they get a little overexcited, and they let slip something that they shouldn't have.

There are, of course also incidents of data leakage that are deliberate. Electronic Information is extremely valuable and that value takes many different forms depending on the type of data concerned. For example; data is valuable to an outgoing employee who may be going to work for a competitor; copying or sending to their personal email accounts sensitive lists of information containing customer details and product and sales transactions would be very useful in the early days of their new employment. Similarly, data specific to a product or service would be valuable to a competitor and there are documented cases where employees have sold for financial gain specific types of intellectual property that resulted in the loss of their employer's competitive edge in the marketplace.

Whether accidental or deliberate, the loss of sensitive data for a business can be devastating. Investigation into such an event is massively time consuming and costly. Should the event become public knowledge the consequences from customer attrition through diminished confidence in your abilities can quickly present a situation that is irreparable and more recently governing bodies are frequently issuing fines for data breaches that would financially ruin many businesses or certainly wipe out profitability for months and even years.

Threat 2 – Misuse of Corporate Computers

Many employees knowingly use their company supplied computers in ways that undermine IT security and acceptable use policies. Many staff often change computer settings that alter security settings and expose the system to malicious programs such as viruses and phishing code that specifically target certain types of data to transmit back to the external perpetrator. Employees often share their work devices and therefore the information contained within with non-employees, often innocently such as allowing their children to use the device for internet access or computer gaming, there is no malice intended in these instances but again it unnecessarily exposes the company and its data. Many employees attempt and successfully bypass IT security settings to allow them access to external internet based services for downloading music or video, online banking and shopping.

There are also many cases where a company provided computer has been used to engage in online gambling and pornography access and download. Studies show that around 25% of employees surveyed admitted sharing sensitive information with friends, family, or even strangers and almost half of the employees surveyed share work devices with people outside the company without supervision. This behaviour can result in intellectual property leaking out of the company and reaching audiences that pose serious threats to corporate security and profitability.

Threat 3 – Accidental Error & Negligence

An Employees ability to use the business assets provided to them is often not as good as it could be. It is simply impossible to watch over what every employee is doing all of the time, they often have gaps in their knowledge of how to perform a certain task or experience difficulty undertaking an activity and they often do not request any help or raise their hand to declare their issue. It is often the case that the employee isn't aware there is an issue because they do something the way that they have always done it, or have been shown incorrectly in the past on how to do it, therefore they don't know any better. It is easy to see how some seemingly inadvertent activity could lead to a massively damaging situation. We have all at some time or another heard about the email containing sensitive information that was accidentally sent to hundreds of incorrect recipients because the sender simply did not understand how to use their email program correctly.

Training appears to be the answer here, however; even if you have good training practices for staff, over time how do you know if it was effective and that they now know how to use their computer to an adequate level of competency. There is a very obvious aspect to further this challenge; time. In today's business world, time is a scarce commodity and it is very unlikely that you will have the time to accurately and regularly assess members of staff to ensure they carrying out their duties in-line with the requirements of their training and the wider needs of the business.

Research indicates that over 50% of all business leaders polled quote accidental or negligent actions by an employee as a significant issue in the exposure of their critical and sensitive data.

Key Points – Identification & Context

In all of the scenarios imaginable, there are two key aspects requiring immediate and absolute attention when considering damage to your business from the insider threat;

- Timely identification of a breach is paramount and this is probably the biggest challenge presented; but how do you know you have a problem or breach if you are not actively looking. Simply hoping somebody notices and informs you of an issue is not a solution and by the very nature is also “after the fact” which means you are already in a position where remedial action is the only available course to take and as discussed previously this approach is both costly and potentially crippling for a business. Having some method for a pre-empting a potential breach event is really the only viable solution to this central aspect of protecting the organisation.

- The other essential consideration to these issues is identifying the perspective or context in which a security problem or breach has occurred. As already identified, there are many differing and sometimes mitigating circumstances where an organisation has been exposed to a damaging situation concerning employee actions or data leakage. It is absolutely key to resolving a situation after an event that you understand how the event originally came about and under what conditions. Again, the investigation process here can be lengthy and costly and often not produce any real facts or tangible evidence to draw a satisfactory conclusion. Ideally, a system that recorded computer activity and user actions would be invaluable in the investigation process and could provide evidential material to irrefutably pinpoint context and even intent.

The Solution – User Activity Monitoring

User Activity Monitoring (UAM) can help solve these very serious issues presented by the Insider Threat and also provides an organisation or business with a viable solution to increased levels of computer security data protection.

It is possible to monitor and record every aspect of computer usage, thereby providing you with valuable information about how your organisations computers are being used and delivering an unrivalled insight into computer user behaviour of your workforce. The technology aspect to this solution is relatively simple; a small software agent is installed on your employee computers to capture key usage information and transmit that data back to a centralised server where it can be processed and analysed to provide alerts in real time to inform the business of potential security issues or breaches and also be collated into reports to illustrate factual information on computer usage across the organisation.

UAM software literally records your all computer activity including keystrokes and potentially even including screen snapshots every so often which can capture the all-important context of a user's actions.

By deploying a UAM solution and letting your employees know that their activities in the workplace do matter and are being monitored, they will think before engaging in potentially harmful activity. Knowing that personal consequences are possible they will generally avoid the problems in the first place, simply because they will make better decisions which primarily helps them but ultimately benefits the business as a whole.

Once a UAM system is operational and If your organisation experiences a security breach, the system will generate and instantly transmit an alert to key personnel to highlight the threat the moment it happens. The alert details exactly what user action(s) are considered suspicious, the user that it relates to, and information relevant to the context of the user action.

Some Employee Activity Monitoring solutions now have the capability to baseline user activity and therefore identify abnormal or unusual user actions, with this level of intelligence an organisation is given not only data on each user and what activities are being engaged in, but also invaluable insight into teams, departments and the organisation as a whole to detect and prevent issues before they arise.

Choosing a Monitoring Solution

When selecting a monitoring solution, you must determine whether you will deploy and manage a solution in-house or consider a "Managed Service" from a specialist technology partner who has the capability to implement and manage a solution for you.

Key aspects for consideration in a monitoring Solution;

- **Threat & Incident Management**
  The sheer amount of information captured can be overwhelming and you must have the time and experience to identify what is and what is not a threat to your organisation. You would also need the capability to filter this information down into meaningful data that you can understand and then use in the course of managing the security events and threats identified.

- **Sensitive Information**
  Some of the information captured will be sensitive, either commercially or from a people perspective. It is sensible to keep this information secure and within the business' network security perimeter, however this may present an issue for internal IT staff or external IT contractors who should be denied access to sensitive information.

- **Private Cloud, Not Public Cloud**
  As the information is sensitive, it is not suitable to be stored within the public cloud nor do you want it transmitted across the internet using insecure means.

- **Employee Privacy**
  Some employees might be concerned about what is being monitored. Setting out expectations via an Acceptable Use Policy is a first step and then monitoring against that policy ensures employees understand what is acceptable. Furthermore, monitoring can be customised to specific times of day - for example, if you allow any personal use at lunchtime or for organisations that allow employees to use their own device it is possible to enable monitoring purely within office hours when that device is being used for work.

Choosing a Managed Service

If you're not in the business of computer usage monitoring and computer security then any time you spend on implementing, maintaining and managing a UAM solution is time not spent on your core business activities.

The best solution may be to pick a technology partner who will implement and manage the monitoring solution for you according to best practice but also with an understanding of your needs as a business. The service provider would effectively become your "eyes and ears" in terms of monitoring user activity. This would mean that security event alerting is primarily intercepted by the technology partner, then evaluated and measured against a predefined and agreed set of procedures that set out the correct actions to undertake. Secondary alerting and reporting is then passed to you in a more managed and controlled manner and tailored to suit your needs, thereby not taking up any more of your time than is necessary and equipping you with the information you need to take any necessary actions to improve the security of your business.

The partner should bring efficiencies and best practice gained through the experience of doing this as its core business, this not only saves you money compared to having an in-house solution but also provides a better quality service overall.

The optimum solution would be to have the solution hosted in a private cloud data centre where the data is encrypted and a secure Virtual Private Network connection back to your office network. This means the communications are secure and also means that the computer equipment and any data collected is still within your overall network security perimeter, thereby giving you the benefits that a cloud service brings without any security compromises or data storage concerns.

Having regular service reviews with your partner to run through alerts and reports to help you understand what is going on, proactive support and guidance for the alerts and security events whilst benchmarking against KPIs specifically defined for your business will ensure that the solution has continuous improvement built in from the start, meaning you should always be deriving best value and ensuring a return on investment for the business.

Conclusions

Implementing a User Activity Monitoring solution shouldn't be seen as negative and there is a very valid view point that it is somewhat careless to operate a computer and digital data dependent business without one. There are many benefits to the deployment of a monitoring solution and those discussed within this document are simply the most commonplace currently, history has shown that the threat to computers progresses and broadens at an alarming rate and as such it is surely a matter of time before UAM is deployed in every business in much the same manner as Antivirus software is today.

It is unrealistic to rely on Managers to oversee or IT staff to track every act or activity within a computer user workforce. Business leaders must acknowledge the risk presented by the insider threat and lead the initiatives to deliver the tools to provide adequate methods to reduce the risk, without a monitoring solution there appears to be no efficient and comprehensive alternative method, indeed without a business-wide approach it is almost impossible to address these issues and improve the overall security and effectiveness of the business.

Summary Points

- Insider threats exist, are commonplace and have the potential to cripple business.
- Prevention is easier to achieve and far less costly than a reactive post breach approach.
- Fines for data breaches are getting more frequent and rising in value.
- Deploying a business-wide User Activity Monitoring solution can help to address and even prevent most Insider Threats.
- User Monitoring as a Managed Service is an easy to deploy, low overhead and effective solution to the Insider Threat.

Seccura: Data Intelligence & Security

About Seccura

Seccura is a privately held IT Security company dedicated to protecting critical data assets and enhancing corporate and personal productivity. Our aim is to provide peace of mind for our customers so they remain focussed on managing and growing their business.

For further detail and contact information please visit the Seccura Website at www.seccura.co.uk