



So Many CCTV Cameras:

Have you ever wondered why we have so many CCTV cameras hanging from lamp posts and attached to buildings? They say it's for security right? But the majority of people are not doing illegal things, so why have so many cameras?

Then when some terrible crime is committed there is always an appeal 'do you know this man?' and a still image taken from a CCTV camera is presented.

Data Breaches: Insider Threats to Board Room Execs:

ICS As we write this article Three Mobile are releasing updates on their most recent breach, which indicates an Insider Threat.

ICS Talk Talk's data breach of 157,000 customer records in 2015, cost them a record fine by the ICO of £400,000 and they are still reeling from it.

ICS Coca Cola was infiltrated at the exec level in 2008 for a month.

ICS In 2014 the same company warned 74,000 people that personal information concerning them had been compromised, the threat was internal.

How important are your organisation's reputation and data to you in your responsibility to protect it? What would someone's violation of trust cost you?

Head of IT:

I first met this guy who was working on an IT service desk in 2005. We became friends, now skip forward some years later and in 2015 after learning his trade, he has his own office, is the head of IT for a large UK charity, he has people working within his team, he is ten minutes walk from the train station and his home is a fifteen minute journey away.



He can work flexible hours and from home some days per week. Life is good and he has the ideal work scenario many of us wish for. Wouldn't you?



Unbeknown to my friend one of his juniors had some strange ideas of their own. They falsified information and made some false accusations about my friend's behaviour towards her, such that his employers had to take immediate action. A long story short he lost his job.

Why Monitor? Is it not too Big Brother?

The problem my friend had was there was no quick means of proving his innocence, a number of times prior to this I had recommended he consider implementing monitoring software, which would have been able to log who was doing what, where and when, but for one reason or another he was reluctant to.



For many the main reason is 'Why should I? We trust everyone we employ here. Monitoring is a bit Big Brother, isn't it?' There are a lot of organisations both public and private that feel this same way and will sympathise with employees who object to being monitored.

The notion that monitoring activity is somehow wrong within the modern workplace is a common distraction and delays action. There are numerous examples of monitoring taking place everyday. The most obvious is start and finish times of work, or logging the number of sick days or holidays someone has had, filtering email or web activity, setting acceptable use policies, performance reviews, management by objectives, the list goes on. Your organisation will have one or more of these, you may have others that have not been mentioned.

What Breaks the Status Quo?

It is quite often the case that something alters within an organisation that means the management team cannot continue with the status quo. So, something has to change.



We have often seen this moment occur when management has to deal with an unwelcome challenge that is likely to lead to a tribunal, or they have to deal with something after the event and wish to ensure they are secure moving forward.

For example, this might be a leaving member of staff who takes the company database with them, or prior to handing in their notice a member of staff forwards key information to themselves via a webmail account. These are not isolated or infrequent actions but happen on a regular basis regardless of the size of organisation. So what can be done to prevent it?

Insight from Loss:

So what changes a manager from indecision into action, when it comes to monitoring?



Fundamentally the moment of insight comes when the manager or the management team realise that something has been lost through not looking, or letting things be as they were. Yet this realisation often comes after the event. Which reminds us of two classic quotes from industry experts:

“Security is always excessive until it’s not enough.” - Robbie Sinclair and

“The anguish of low quality lingers long after the sweetness of low cost is forgotten” - Peter Gregory.

We have to find the right solutions that work well, quickly, simply and better than before and deliver it.



Accountable for Loss:

Installing monitoring is an easy decision once the management team realise it will be held accountable for all loss of data, company information, and customer records. The management team are accountable if there is no form of audit to illustrate compliance to acceptable norms, or they've not provided staff with learning points to prevent future leakages. Monitoring is the only way to mitigate against the loss of data. It is after all why cars have to be insured when driven on UK roads. Not because the government thinks we are all going to have accidents but to protect everyone, just in case.



What Other People Say:

Sadly one person's great idea may be the scourge of another. Often in organisations the internal politics prevent things from happening. How often have we seen this?

So when a senior manager decides that the right thing to do is set in process the extension of existing monitoring systems they often face the resistance of others, be it their peers or those who they work with.

But when one knows something is right it is not a problem to continue on a course of action that takes you there. Inaction can often have far worse consequences. Ultimately if you had a chance of securing your organisation's data, or not, what would you do?



The question that really should be asked by management teams is “**what will happen if we don't do this?**” Or a better question is “**can we do this better?**”

In the case of monitoring, learning from other businesses examples is always a great place to start. Talking to an IT director they were explaining how monitoring was an essential part of their security and no question about keeping it in place. Earlier that year a trusted member of their company had decided to start out on their own, this employee had secured funding from a large European competitor on the basis of setting up with the knowledge, contacts, customer records and supplier details from their existing workplace. The management team had no idea this person was even considering leaving, let alone setting up in direct competition, using intellectual property of the company and backing from a competitor. So what happened?



Protection Through Knowledge:

By having simple monitoring in place, activity reporting and behaviour analytics the management team were made aware of what was happening through the individual's abnormal actions, all just in the nick of time to protect the company, the staff's jobs and their livelihoods.

Protection Through Action:

If you had the opportunity to protect your livelihood and those of your colleagues wouldn't you? Between the choice of monitoring and keeping your company safe, or not monitoring and living with the uncertainty of someone's actions leading to a crisis, what would you do? In numerous examples we have seen time and again customer's implementing monitoring for security and data loss protection concerns; then seeing how productivity levels, best practice, workflow, key Application usage and rewarding non-sales activity through measurement of objective achievement can all be achieved in addition to this.

Protection of Time and Money:

When my friend the Head of IT was told he was being investigated due to gross misconduct, he knew he was innocent, but without the facts in front of him he had difficulty proving this. Gradually as things unfurled he proved his case. However, as he is one of the good guys, and whilst he could illustrate his employer had made a number of mistakes, he didn't want to cause any ill will so left the charity anyway. He now works for a larger charity, with a bigger team to manage, a better salary and still works from home for part of the week. What he realises now, is if he had had the monitoring of activity in place then a simple report illustrating the particular individuals activities would have saved a lot of time and embarrassment.

CCTV cameras are not in place to watch us, but there as a security to protect us should something bad happen.

We hear this and similar in many of the large and small organisations in both the Public and Private sectors we service. And because we've learnt so much more about security monitoring ourselves we wanted to share our 7 Simple Steps to Internal Threat Management. <http://incommsec.com/articles>. We are happy to answer any questions that this article may raise.



+44 (0)20 3368 6301



www.incommsec.com

enquiries@incommsec.com



[@incommsec.com](https://www.facebook.com/incommsec)

www.facebook.com/incommsec