

The definition of Human Error is ‘a mistake made by a person rather than being caused by a poorly designed process or the malfunctioning of a machine such as a computer’. A simple, often unintentional, lapse in judgement can have detrimental repercussions and it’s no surprise that an organisation’s workforce has been identified as the weakest link. Yet undeniably the solution is to not to vote them off – with or without an Anne Robinson cheeky wink. So how can organisations protect themselves from these renegades?

Human error continues to be the primary cause of information technology (IT) security breaches. In fact, the UK Government has faced repeated embarrassments over lost data, with over 270 data breaches being reported over the past year alone. Prime Minister Gordon Brown recently stated that the government cannot promise the safety of personal data entrusted by the public, citing human error as the reason, so that’s okay then isn’t it? Of course it’s not.

Primarily the reason why security processes fail is that individuals are given the option to bypass them. If you take PA Consulting’s loss of a memory stick containing personal data on every one of the 84,000 prisoners in England and Wales as an example a single employee was in breach of its well-established information security processes. I’m sure he, or she, did not set out to intentionally destroy the reputation PA had built itself for handling sensitive government information securely for over 60 years, or to lose the £1.5 million contract, and potentially jeopardise the remaining £8 million contracts, yet that’s been the result. The salary of the individual involved has not been disclosed but even a lifetime of hard graft for gratis would never repay this deficit! In the individuals defence, although naivety is a fair charge, the fact remains that they were allowed to bypass the encryption software that would have saved PA its blushes. So in this case who really was the weakest link?

So who’s to blame

Let’s face it, anyone can make a mistake – the person who leaves a USB drive containing the latest (but not launched) advertising campaign behind at the coffee shop, the employee who forgets to lock their computer before going to lunch leaving sensitive data accessible, the commuter who, being efficient, uses their smartphone to review corporate documents on the train and then leaves it behind in the mad rush to the door, the consultant who places a CD with information on every employee at the company they are working for in an airline seatback while travelling and forgets to pick it up after a 12 hour flight, – everyone can have a momentary loss in concentration but it’s the cost of the mistake that’s the differential. So rather than pointing the finger of blame after the fact, organisations need to identify the potential risks and employ damage limitation tactics.

IT departments should never leave data security up to the end user, they don’t have the time or the knowledge, and it certainly wouldn’t be considered “reasonable and appropriate” (the underlying theme of data security regulation) if the device, and the data contained, was lost or stolen.

Likewise, everyone within an organisation must understand their responsibility for keeping sensitive information secure and how to use the available technology, such as encryption software, to do so. Often

if people understand why they need to do something, then they'll do it – the PA Consulting employee learned this lesson the hard way

So what's to be done

To ensure data protection in today's dynamic IT environment, leading analysts recommend that security protects what matters most: the data and not necessarily the device. Concerned about the damage and liabilities of lost and stolen data, enterprises are turning to encryption as a backstop to prevent corporate and customer information from ending up in the wrong hands. In fact, data security advice from the Information Commissioner's Office is to encrypt any personal information held electronically if it will cause damage or distress if it is lost or stolen.

Organisations need an intelligent, multilayered approach to encryption that automatically safeguards data without complicating essential IT and user operations – no back door, even for PA Consulting! A data-centric solution simultaneously meets security, IT operations and compliance needs. Encryption can take place whether data is on a desktop, laptop, PDA, or USB stick and it's granular, so administrators can set policies to determine which data is protected and against whom. A data-centric solution uniquely protects individual users' data, without interfering with the other operational processes (upgrades, patches, etc) that need to be done, it protects against the internal threat and provides lower TCO.

Corporate Governance requires organisations to not only have security, but be able to prove it is effective. When a device is lost or stolen then the company has to decide if a "breach notification" needs to be issued, along with all the expense and embarrassment that goes with it. However, if there is a reasonable belief

that the data was encrypted – and can be proved – then the affected individuals whose information has been lost do not need to be informed as it is not at risk. By using a solution that includes a central management console, every machine that is protected reports back to say that it has received the latest instruction and confirms that it has been carried out, keeping all the proof centrally. A tool that could have saved the blushes of Atos Origin, another Government contractor who lost track of a memory stick containing user names and passwords for its Gateway site, used by people for their tax, benefits and other Government services which had to be temporarily suspended while the loss was investigated. The stick was eventually found in the car park of a pub near Atos Origin's offices, and the fact that data on it was encrypted was discovered.

Every day employees are taking advantage of the latest must have gadget, even using personal devices in addition to company owned technology, to keep in touch whilst out of the office. Any organisation that not only embraces this trend, but actively encourages it, has a responsibility to empower its employees to do so securely thereby ensuring they never hear the immortal words – you are the weakest link, goodbye!