cnme
computer news middle east

Ticking time bomb

by **Tom Paye** - June 11th, 2013

The last year has shown more than ever how careful businesses need to be with their data. However, recent reports suggest that only a fraction of Middle Eastern enterprises have data loss prevention policies in place. Does this make the region a ticking time bomb about to explode with data breaches? ***Tom Paye*** *investigates.*

Remember the premise of the latest James Bond movie, *Skyfall*? The British Secret Service’s boss, M, loses a hard drive containing the names of every undercover NATO operative working around the world. The main antagonist, Raoul Silva — a former MI6 operative and self-proclaimed computer genius — then goes about using the list to reap havoc in an attempt to ultimately kill M.

Skyfall might have been the most successful Bond movie of all time, but there’s not an IT pro in the world who would say that the technology-related parts of the premise were anything like reality.

Apart from the ease with which baddie Silva is able to hack one of the most technologically advanced government entities on the planet, there’s little chance that MI6 would have allowed the data on that hard drive to be lost, even if the drive itself was. In real life, any spy agency worth its salt would have implemented some kind of data loss prevention (DLP) solution — just as any organisation intent on keeping its data secure would.

DLP differs from traditional security in the sense that it focuses entirely on protecting information as an asset, according to Rob McMillan, Research Director, Gartner.

“Without DLP, there are few options to protect information as a discrete asset; most technical security controls are focused on the protection of infrastructure, rather than information," he says. "It provides organisations the opportunity to control the release of information in real time using a policy-based approach, with control decisions based on both the business rules (i.e. the policies) and the actual content of the information.

"It also provides an ability to give staff real-time tutorial on the decision that they make with regard to an organisation's information, thus providing a new and effective form of user awareness."

However, Paul Wright, Managing Director of Professional Services and Investigation Team for the Middle East, India and Africa, AccessData, says that DLP is not such a clear-cut term.

"In the eyes of some, data loss prevention is purely and simply a marketing tool. They say that there is no such thing. The reason being, other than switching off all computers and networks, it is impossible to guarantee that you have prevented data loss. The best that can be aimed for and achieved is data loss detection or deterrence," he says.

"Many DLP users only have selective features switched on. To turn on all the features would completely disrupt an organisation's business and networks and is why it is exceptional to find organisations running DLP in full-blown mode. It should be noted that, even then, it will not guarantee preventing data loss."

If you really want to keep your data secure, then, there are differing views on how effective a DLP solution will be. Perhaps this is why the Middle East has been slow to jump on the DLP bandwagon, as a recent report from the InfoWatch group suggests.

"Let's take KSA [the Kingdom of Saudi Arabia] as an example," says Natalya Kaspersky, CEO, InfoWatch. "Joint research conducted with our local and regional partners suggests that 80 percent of companies in the Kingdom operate without internal data security systems in place. That's the bad news."

But why is this such bad news? Do traditional methods of securing data and networks simply not suffice anymore? And does this mean that the Middle East is soon to witness huge numbers of data breaches? According to Kaspersky, the risks associated with not having any DLP solutions in place are substantial, particularly when talking about government organisations or financial institutions.

“On a global scale, 2012 was the year of leaks from government organisations. There has been a noticeable increase in the proportion of leaks which emanated from government sources, demonstrating that the public sector is not paying sufficient attention to the issue,” Kaspersky says. “Other areas of impact include the financial sector (more specifically banks). Data loss resulted in over $2 billion in direct losses globally in 2012 as a result of over 2 million records being compromised. And that’s only what was reported in public.”

Indeed, the InfoWatch report said that, given companies in many Middle Eastern countries are not forced to disclose data leaks, the region could have lost much more as a result. One expert suspected that the Middle East could have lost billions all on its own, all because proper procedures were not put in place to ensure the safekeeping of data. But if companies really are losing so much due to data leakage, why are they not doing something about it?

“Businesses are lax because legislation is lax,” says Miguel Braojos, Vice President of Sales for Southern Europe, the Middle East and Africa, SafeNet. “And although most of them are aware of the dangers of not protecting their data, few of them are actually implementing DLP. Their approach is more reactive than proactive.”

That said, the high-profile attack on Saudi Aramco last year has jolted the region into action. Braojos says that some government and financial institutions in the region are beginning to adopt DLP solutions, as the consequences of data loss are more serious in these sectors. Kaspersky, meanwhile, says that Saudi Arabia is expected to invest $400 million in DLP over the next five years, and that InfoWatch’s research shows similar interest in the technology across the region.

So if we take it as a given that CIOs need to begin investing in DLP solutions, what should they be looking out for from vendors? In other words, what should a decent DLP solution be made up of?

“There are a number of components which are important. The first, and probably the most important, is setting some parameters for how data is classified,” says Nicolai Solling, Director of Technology Services, help AG. “The other requirements are more technical and deal with how well classification of data is performed, and then finally how well data is enforced.”

Muhammed Mayet, CTO, Security, Dimension Data MEA, says that a good solution begins with identifying and prioritising data within the business.

“Once this has been done, the business has a better understanding of the level of sensitivity and confidentiality of the data that lives within the business,” he explains. “The choice of technology needs to be appropriate for the business, taking into account network DLP (data in motion), endpoint DLP (data in use), and file or storage DLP (data at rest). Also key is the integration between the DLP technology and the existing ICT infrastructure.”

Another thing to ask vendors is whether or not their solutions cater for BYOD, a trend sweeping the IT world that shows no signs of going away. Of course, having company data on a personal mobile device is a risk in itself, so can DLP solutions return an element of control to network managers?

“The questions of where mobility fits into a DLP policy is a great one,” asserts Gartner’s McMillan. “Some DLP platforms now support mobile devices, but this is still relatively new. However, it is certainly an emerging space and many vendors are developing solutions.”

Of course, even once a CIO finds a good DLP solution, and decides that it would fit perfectly into the company’s infrastructure, there’s always the matter of justifying the expense to the CEO and CFO. Mayet says, “It is critical that any proposed DLP solution has the support of key stakeholders that own the affected data.”

But according to Haroon Iqbal, Sales Manager, WatchGuard MEA, it shouldn’t be a problem convincing these stakeholders, as the costs of implementing a DLP solution should be justifiable.

“The costs for a good DLP solution depends on the amount of security needed, which can vary according to the amount of sensitive data a business needs to secure, the critical nature of that data, the size of an organisation, number of employees, and the specific work style of that organisation,” he says. “The question to ask is not the cost of DLP, but the cost of data loss, and that will help put the investment in perspective.”

But what if the CIO simply can’t find the budget to invest in a DLP solution? What other ways are there for him to protect his data? Dimension Data’s Mayet says that this is unlikely: “In a perfect world, educating your end users and increasing their awareness of the impact of data loss or leakage would be sufficient. However, in reality, every policy and procedure requires a monitoring mechanism and an enforcement tool. Without a DLP solution, businesses cannot effectively track and secure their data."

However, Braojos, from SafeNet, believes that encryption can offer just as much protection for an organisation's data in lieu of a DLP solution.

"Organisations have sensitive data everywhere, and with cloud and virtualisation, there are many vulnerable spots," he explains.

"But by using data encryption, it doesn't matter who has it. Encryption is like the anti-DLP. You don't care who sends it out or steals it because they would not be able to read anything."

Traditional security solutions also have their part to play, but however a CIO decides to proceed, the consensus among many experts is this: company data in any format is a hugely valuable asset, and it needs to be protected. Indeed, it's something that M should have realised in *Skyfall*. With so many data protection options now available to organisations, she had no excuse for losing the names of those undercover NATO agents.

Source