The role of user-driven security in data loss prevention

Typically, some 90% of data loss incidents are accidental, not malicious. They continue to happen despite the use of Data Loss Prevention (DLP) technology by the organisations affected. However, out of all the IT security solutions deployed, DLP is arguably the most suitable for a user-driven approach.

Many current DLP solutions rely entirely on automation at a central computer system to determine whether information may or may not be sent outside the organisation. While it may seem at first counterintuitive, involving end users in the process can dramatically improve the effectiveness of DLP schemes. At the same time it helps engender security awareness among staff and educates them in security policies, explains Stephane Charbonneau of Titus.

External pressure for internal information security controls

Organisations wishing to win new business through tenders and bids are under pressure to give clear information on how they deal with information governance and security. This has become so important that an organisation issuing a tender might choose one supplier over another based solely on its compliance with applicable regulations or the fact it holds the ISO 27001 certification.

Companies are therefore wondering if they should get certified, what compliance entails and what the implications of these ‘bureaucratic complications’ are. In any case, an information security review or internal audit can be a vital tool to enable a firm to understand its current maturity level and possible improvements as well as to answer lengthy and detailed security questionnaires, explains David Cowan of Plan-Net.

Point to own: the problem with hacking tools

The controversy over weaponisable software tools is escalating. Software designed to footprint, enumerate or internal audit can be a vital tool to enable a firm to understand its current maturity level.

Looking behind you: the dangers of shoulder surfing

The situation where travellers or restaurant users find themselves privy to credit card details, business plans and other data is a fairly common experience. You might, for example, simply hear someone giving out their credit card details over a cellphone. Why does this leakage occur — or, to put it another way, ‘why are people so stupid’, asks Wendy Goucher of Idrach.
markings are defined by the organisation, and can be placed in the document header, footer and/or watermark, or in the email message body and/or subject line, as shown in Figures 2 and 3.

A significant benefit of visual markings is that the security instructions are visible to all recipients, including those outside the organisation. The visual markings become part of the email and document, and the recipient does not need any special software to see them. For example, a large organisation may work with several sub-contractors on a confidential project. The sub-contractors need to follow the same regulations as the prime contractor, but may not be as well versed in security policies. A user-driven security solution enables the originator to automatically include handling instructions, such as 'export controlled' or 'confidential', at the top and bottom of the email or document. This makes the recipient accountable for handling the information appropriately.

**Enhancing DLP strategies**

In addition to visual markings, a user-driven security solution also creates metadata within an email or document. This step is automatic and is triggered by the user's selection of a classification category for the email or document. For example, if a user selects 'confidential', this value will be stored as metadata in the document or email properties.

This user-driven metadata helps DLP solutions make more intelligent policy decisions. Most DLP solutions can read metadata in documents and email, and then make policy decisions based on the metadata values. For example:

- Stopping users copying documents to USB drives when the document contains the metadata value 'secret'.
- Automatically encrypting email at the gateway when the email has the metadata value 'personally identifiable information'.
- Preventing the upload of documents to external websites where the document contains the metadata 'internal only'.

By adding metadata to emails and documents, user-driven security augments automated DLP solutions to provide the best of both worlds – automated scanning combined with users' own knowledge of sensitive content.

A user-driven security solution can, therefore, provide several critical components for an effective DLP strategy. Most importantly, users become key partners in identifying sensitive content, raising security awareness, and remediating policy violations. When combined with a DLP solution, the result is a dramatic reduction in the risk of inadvertent data leaks from authorised users within the organisation – all without compromising business productivity.

The last word goes to Graham Titterington. “User-driven security is an example of how technology can be turned to advantage in enabling businesses to operate more efficiently, by enhancing security without obstructing the work people are trying to do.”

**About the author**

Stephane Charbonneau is chief technology officer at Titus (www.titus.com). He has 15 years experience working with international organisations in the public and private sectors. He worked as senior security architect at a major US financial institution and in several Canadian federal government departments. He graduated from Canada’s University of Waterloo with an honours degree in computer science.

---

**External pressure for internal information security controls**

David Cowan, Plan-Net

The amount of information and the collective effort required for a company to win new business opportunities through formal tenders and bids has always been quite high. However, with a stronger focus nowadays on the protection of personal and sensitive data belonging to organisations and their clients, bidders are being pressurised to give even more information about their internal processes and procedures. At the same time, they need to provide clear answers and tangible evidence on how they deal with information governance and information security.

The increased emphasis in this area has become so important that an organisation looking to acquire services from a third party through a tender process might select one bidder over another based solely on its compliance with applicable regulations or the fact that it holds the ISO 27001 certification.
Tenderers are therefore increasing their attention towards information security. Recent research shows a growth in the percentage of companies that identify ‘client requirement’ as a factor to justify the implementation of information security controls within an organisation to protect its information assets. Indeed, the ‘2011 Global State of Information Security Survey’ by PriceWaterhouseCoopers (PwC) revealed that in the past three years, the ratio has gone up from 34% in 2007, to 41% last year – a growth of 21%.

“Companies wishing to tender for business are asking themselves: is it worth obtaining ISO 27001 certification or is alignment enough?”

Furthermore, in the ‘Information Security Breaches Survey 2010’, also by PwC, 68% of large organisations stated that they had been asked by their customers to demonstrate their compliance with information security standards, while 61% ensure that their contracts with third-party providers include security provisions.

It is apparent that information security is gaining more and more importance in business activities. However, there are still some uncertainties regarding the actions to take in order to have an efficient Information Security Management System (ISMS). Companies wishing to tender for business are asking themselves: is it worth obtaining ISO 27001 certification or is alignment enough? Although it depends on the company that issues the tender, both solutions might have the same effectiveness – and it could be said that it is the journey rather than the destination that is important in this case. It is through an information security review or internal audits – performed for the purpose of certification or simply following best practice which leads to potential corrective or preventative action – that you can identify how an organisation handles and stores information, deals with possible breaches of the Data Protection Act and trains its staff accordingly (or not). This can help enormously in understanding and then answering the lengthy and complex questionnaires used in tender processes, and possibly increasing organisations’ chances of winning the potentially lucrative contract.

The questionnaire

A standard information security questionnaire might have around 100 questions, consist of an Excel spreadsheet or online portal and will rarely require simple yes/no answers. The process has changed to a point where the typical questionnaire will now ask for details of processes, procedures and policies in all areas – and possibly require proof or evidence to support any statement. It could typically take half a day to complete the document or, in some cases, even longer, mainly because it can be very difficult to understand the questions and what kind of information and detail is required – ie, there is a question within a question: what are they really asking? Even the most experienced IT director or account director struggles to understand the level of detail required. Furthermore, the questionnaire cannot be completed without having relevant knowledge of how other departments or business units, such as HR, finance, marketing, risk and audit, and facilities handle and dispose of information assets. In fact, to give all the relevant details, examples and evidence that the client is asking for, the work of one person is simply not enough – a collaborative approach is required.

“Questionnaires also enquire about third parties … how they ensure that security requirements are included in third-party agreements and contracts, and whether they implement effective information security controls”

A typical question could be: ‘Who within your organisation has been formally mandated to own and manage information security and business continuity?’ This requires the names and positions of all those who have responsibilities in these areas, as well as details of how information security and business continuity are structured. Another typical question concerns how your policies are communicated to staff members and contractors, not only upon induction to the business but also when they leave or change roles. Today, questionnaires also enquire about third parties the tenderer might deal with: how they ensure that security requirements are included in third-party agreements and contracts, and whether they implement effective information security controls. This must be followed by examples of information security clauses included in contracts, copies of any third-party assurance/risk programmes and
examples of third-party assessments with findings and remediation plans.

Questions that might require greater collaboration with other departments that deal with information include: how is sensitive information removed from any assets before they are disposed of or sent out for repairs? Non-IT departments should provide details about how they deal with the information contained on decommissioned or broken computers and reprographic hardware, out-of-date CV databases, CRM systems and so on. Not only does the process have to be explained, but a copy of the formal procedures should be included as well.

It is obvious that having the right information to hand and understanding what the clients are asking before completing this type of document can make the process much more efficient and cost effective. The same goes for having the assurance of a level of maturity within the implemented controls equal to or superior to the one deemed acceptable by the potential client – all things that can be achieved through a standard internal audit programme or external information security review.

**To be or not to be certified?**

It may be difficult for a company to understand the complex questions even in the situation where it already has a mature ISMS in place and all the relevant documentation and procedures. Perhaps obtaining the ISO 27001 certification can help diminish the volume of questions in a tender, as some organisations issuing the tender accept the certificate as an assurance that the bidding company is following best practice related to information security and that it is therefore a safe partner. However, the certificate is not exactly mandatory – alignment with the ISO 27001 standard might be enough to satisfy a company.

Often it is not necessary to hold the certification before bidding for the tender. Some clients are happy with assurances that the bidder is working towards the certification or is aligned with its standards. If the bidder is able to show them the relevant project or management plan highlighting that corrective action is being taken towards an efficient ISMS, it might be enough for the partnership to be accepted. So you have to be very clear and specific with your management plan if the ISMS is not in place. Of greater importance is that senior management has committed to the plan and has allocated the necessary resources and time to achieve it. The company tendering for business will most likely keep track of progress throughout the due diligence and contract term.

That said, for some companies it might be easier and more cost effective to gain the certification than to continue to answer wave after wave of time-consuming questionnaires – or at least they feel it would make them more comfortable with their answers as they would have already gained the relevant knowledge required to answer the questionnaire.

Alignment or compliance leading to certification is also important for a company if it wants to grow its business by not only keeping existing clients but taking on even larger, more profitable customers. It will allow the business to maintain its reputation, which is easy to lose when a breach of information security occurs. Lose your own or your client’s information and not only will you potentially have to pay a fine, you will also incur reputational damage that is not at all easy to repair. As a consequence you will lose clients, in particular those dealing with personal or sensitive information, such as a public sector organisation with medical records, family or income details. These types of organisation have always asked for more assurance compared to the private sector; however, the latter is following in their steps and information security is rapidly becoming one of the top priorities during bids and tenders across all sectors, encouraging bidders to have an efficient and best practice-aligned ISMS. It is common practice to mitigate the risk of bringing on a new supplier by performing ‘due diligence’ to check who you are working with; but in the coming months and years this process will become even more comprehensive, with dozens, perhaps hundreds, of very detailed and specific questions, sub-questions and

---

“Lose your own or your client’s information and not only will you potentially have to pay a fine, you will also incur reputational damage that is not at all easy to repair”

---

**Figure 2: Increases in security incidents between 2008 and 2010. Source: ‘Information Security Breaches Survey 2010’, PwC.**
requests to upload relevant documents as proof that a company can be trusted with personal and sensitive information.

**It’s not all about documents and processes**

Having stated their significance, it is important to note that having all the relevant processes, controls and policies in place is not enough. Other elements are necessary in order to reduce the risk of data leakage or business outages through malicious activities or unforeseen circumstances – for example, staff awareness, training and education, and so on. If the reporting process is not clear to members of staff, or they are not aware that what they have done is a breach of the DPA (for example, if they take data home with them on a removable device and then misplace or lose it) then it is also difficult to calculate the number or severity of security incidents that occur within an organisation, and then analyse the results and trends to improve security and prevent the incident recurring in the future.

“A relationship with a client built on trust and good governance will most likely result in an improved reputation – and consequently more clients and more revenue”

It is clear from the PwC survey that 92% of large organisations and 83% of small ones have experienced a security incident in the past year, compared to 72% and 45% respectively the previous year. This does not necessarily mean that breaches are occurring more often – it might instead be that organisations are more aware of what constitutes a security incident and that reporting processes are improving, making it easier for companies to gather more data and use it to improve their ISMS. The PwC survey shows, in fact, that 90% of respondents from large organisations have a formally documented information security policy, up from 88% the year before, and 68% (up from 65%) have partially or fully implemented ISO 27001.

However, only 30% of staff said that they believed responsibilities for information ownership and data protection were very clear. This is a huge problem as security roles and responsibilities have to be very clear in order for staff within the organisation to understand what an incident is and then, once it has been reported, how to deal with it. Fortunately, there are some positive signs towards improved efficiency. The data collected reveals that organisations are increasingly recognising that staff education is a vital element in the achievement of an efficient ISMS – the percentage of respondents providing staff with on-going security education doubled from 26% in 2009 to 52% the following year, evidently growing very quickly.

**Positive progress**

It is clear that organisations are becoming increasingly conscious of how processes and procedures alone are not enough. Management commitment, educating staff and making all parties aware of security-related responsibilities is vital and is becoming an important requirement for clients and potential clients. With organisations today using an increasing number of third parties, the pressure on their suitability with regards to information security is intensifying. The pressure on service providers can be eased with a thorough internal or external information security assessment aimed at identifying the information assets of the business and recommending corrective action to mitigate those risks. This makes it easier to have a clearer vision of the current maturity levels of an ISMS, highlighting any opportunities for improvement and remedial work and, ultimately, completing the lengthy information security questionnaires during tenders/bids to assure companies that they are a safe and reputable partner.

With this newly acquired awareness, organisations large and small wishing to win new business through tenders and bids will have not only streamlined the questionnaire and due diligence phase, reducing the time and effort, but also created more potential to be selected as providers and therefore grow the business in a sustainable fashion. An investment in information security can therefore yield that all-important yardstick, ROI, since a relationship with a client built on trust and good governance will most likely result in an improved reputation – and consequently more clients and more revenue.

**About the author**

David Cowan is head of consulting services at IT service provider Plan-Net (www.plan-net.co.uk). An IT professional with over 12 years’ experience in the industry, he has worked with some of Plan-Net’s biggest clients to deliver technically complex projects and manage change in major businesses and public sector organisations. Cowan works across all aspects of the IT spectrum with a detailed understanding of ITIL, ISO/IEC 20000, ISO27001 and PRINCE2.

**References**
