



# computer

# FRAUD & SECURITY

ISSN 1361-3723 June 2011

www.computerfraudandsecurity.com

## Featured this issue:

### Building solid foundations: the case in favour of data classification

**A**lthough data classification is considered by many professionals to be the foundation of any information security activity, few organisations outside of defence and the security services have done much about it. The discipline is a crucial one, however – not least because, in an ideal world, it should drive the rules that determine what users are permitted to do, or not do, with corporate information.

In fact, information security professionals are increasingly starting to view data classification as the core of all other information security activity. Cath Everett explores why it is so important, what benefits it offers and why, despite this, it has not been more widely adopted to date. She also puts forward suggestions for constructing a business case for data classification and looks at what steps organisations need to take to ensure that these complex change projects succeed.

*Full story on page 5...*

### Going beyond the boundaries of compliance

**A**dhering to compliance standards is critical for most organisations, and as a result these standards often have a heavy influence in information security decision-making. There are numerous reasons for this, but most importantly IT professionals are looking for guidance and direction, and where better to look than industry standards?

However, regulations often lag behind the real-world threats being faced by organisations: compliance does not guarantee security. And recent research has shown

a very mixed picture when it comes to the use of encryption, particularly as it relates to compliance. One of the critical issues is key management, but Jon Geater of Thales believes that the message is starting to get out – that everyone knows about key management and that simply encrypting data is no longer sufficient. Over the coming years, the quality of key storage, access control and management will come under increasing scrutiny in all areas of the information society.

*Full story on page 8...*

### Mergers and acquisitions: security under stress

**W**henver two organisations come together due to mergers or acquisitions it is always stressful for both organisations. But one issue that is not commonly considered during a merger or acquisition is information security.

In effect, you are taking two completely separate organisations and merging some or all of the back-office functions, which means there will be important security issues to think about, says James Rees of Razor Thorn Security.

*Full story on page 12...*

## Contents

### NEWS

- Sony hacked repeatedly as new hacker group emerges 3  
Mapping European cyber-security 20

### FEATURES

#### **Building solid data foundations: the case for data classification** 5

Although data classification is considered by many professionals to be the foundation of any information security activity, few organisations outside of defence and the security services have done much about it. Information security professionals are increasingly starting to view data classification as the core of all other information security activity. Cath Everett explores why it is so important and what benefits it offers.

#### **Going beyond the boundaries of compliance** 8

Adhering to compliance standards is critical for most organisations, but regulations often lag behind the real-world threats being faced by organisations: compliance does not guarantee security. One of the critical issues is key management, says Jon Geater of Thales.

#### **IT security needs a new perspective** 12

More than 30 billion pieces of content are shared on Facebook each month. Meanwhile, on Twitter more than a billion tweets are sent every week. With such growth in the use of social media that can be accessed anywhere, the management of potential threat and data loss sources becomes ever-more challenging, says Bob Pritchard of Clearswift.

#### **The evolving threat of social media** 14

The proliferation of social networking sites has opened up numerous new communication methods for individuals and organisations. However, accompanying these new avenues is a dramatic increase in the volume and speed at which cyber-threats are being created, says Catalin Cosoi.

#### **Mergers and acquisitions: security under stress** 17

In the past few years the business world has seen a dramatic change in almost every sector; companies have risen and fallen, others have had a complete reverse in fortunes and some have been actively merging or being bought outright by other organisations. This situation is likely to continue for some time yet in the West, and it has important security connotations, says James Rees of Razor Thorn.

- Editorial 2  
News in brief 4  
Calendar 20

#### Photocopying

Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.

# Building solid foundations: the case for data classification

Cath Everett, freelance journalist

**Although data classification is considered by many professionals to be the foundation of any information security activity, few organisations outside of defence and the security services have done much about it. The discipline is a crucial one, however – not least because, in an ideal world, it should drive the rules that determine what users are permitted to do, or not do, with corporate information.**

However, Mike Gillespie, director at information security consultancy Advent-IM, puts it another way: “If you don’t understand how sensitive different elements of your information are, how can you do any form of risk assessment on it? If you don’t understand the potential impact of a breach in terms of confidentiality, integrity or availability, how can you know how best to protect it?”

In fact, Gillespie believes that risk management and data classification exercises should go hand-in-hand – although in the real world, they rarely do – as the success of one is intrinsic to the success of the other. The idea is that, if an organisation is handling information risk

properly, it should likewise be classifying its data assets properly – by employing an agreed, standardised classification system across the enterprise.

## The problem

While such views make sense, a key challenge is that data classification is seen as distinctly unsexy, particularly when contrasted against the latest shiny new boxes with flashing lights. Kevin Curran, a reader in computer science at the University of Ulster and senior member of the IEEE, compares it to Search Engine Optimisation (SEO) in terms of its glamour factor.

***“Even if a technology fix were enough, tools that can automatically classify information based on key words and phrases without the need for manual intervention are not available”***

“SEO is crucial if you’re online, but to do it properly is very tedious,” he says. “You build up links, let people know they’re genuine and add suitable content to the website. It’s boring and everyone hates doing it, but it’s really

important. And it’s the same with data classification.”

There are other inhibitors to adoption, too. One is that, although it may seem like the easiest thing to do, simply throwing technology at the problem will not work because data classification is very much a people and process problem. Even if a technology fix were enough, tools that can automatically classify information based on key words and phrases without the need for manual intervention are not available anyway.

A third block, meanwhile, is that, outside of the defence realm, data classification – like risk management – is still a comparatively young discipline. Advent-IM’s Gillespie explains: “As with many of the softer aspects of information security, it’s taken a long time to realise the importance of doing it properly and so it’s taken longer to drive it up the management agenda.”



Catherine Everett



Mike Gillespie, Advent-IM.



Kevin Curran, IEEE.

## Adoption levels

This statement is nowhere more true than in the private sector, where classifying data is an almost non-existent activity and the concept is poorly understood. While central government and its agencies have used the mandatory Government Protective Marking Scheme (GPMS) for years to positive effect in relation to the physical world of paper, many public authorities have struggled to translate it adequately into the electronic domain. Among other public organisations – with the exception of the police – adoption rates are much lower than their central government counterparts, not least because using the GPMS is a recommended requirement but is not compulsory.

***“If you have five pieces of information and none has been given a classification, how do you know how important any of them are and which ones you could be fined for?”***

However, things are slowly starting to change. The WikiLeaks’ scandal, which saw the release of thousands of secret or sensitive US documents, led to the data classification issue being raised explicitly in the press by the information security industry for the first time. Moreover, in the UK, the fact that the Information Commissioner’s Office (ICO) is now subjecting organisations to fines of £100,000 or more following data breach incidents has also served to focus minds.

“When managers see there are significant fines being imposed for losing personal data, they start to ask, how do we know what sensitive data we’ve got so that we don’t have a breach too?” explains Gillespie. “The question is, if you have five pieces of information and none has been given a classification, how do you know how important any of them are and which ones you could be fined for?”

## Key drivers for future uptake

As a result, the use of such schemes is expected to become much more widespread over the next three to five years, not least because of an increasing tendency among central government bodies and the police to insist that contractors use the GPMS or equivalent when doing business with them. As adoption starts to rise in other organisations, such as the National Health Service and local authorities, they are likewise expected to demand compliance, thereby creating a trickle-down effect in the wider market.

Growing interest in the ISO 27001 information security management standard, which specifically mentions data classification as a core requirement, is also likely to spark demand, as is the continuing move to cloud computing. The significance of the cloud in information security terms is that it serves to both create new challenges and heighten existing ones. In a data classification context, this means that, if organisations fail to assign a value or level of sensitivity to their information assets, the danger is that they could end up migrating highly confidential data out into the cloud without realising how sensitive it is. They are also unlikely to have a clear idea of what information should be kept in-house no matter what the circumstances or what levels of encryption should be demanded to protect the varying categories of data being stored by third-party cloud providers.

***“Assigning a classification to data makes it more obvious how long it should be retained for in order to both comply with internal policies and external regulations”***

A similar theory applies to information lifecycle management. Assigning a classification to data makes it more obvious how long it should be retained for in order to comply with both internal poli-

cies and external regulations such as the Data Protection Act. Knowing when to destroy information, rather than simply keep everything just in case, also has the added benefit of minimising the cost of storing and processing large amounts of unnecessary data.

While such considerations are not at the forefront of most people’s minds today, as cloud adoption begins to seriously heat up and security breaches start to hit headlines, they will inevitably gain credence.

## The need for a business case

In the meantime, the lack of awareness of data classification as an issue, combined with the fact that it effectively comprises a change management programme, will require the development of a business case in order to win high-level sponsorship and funding – both of which will be crucial in order to push the initiative through.

The IEEE’s Curran believes that it is possible to make just such a case based on two key premises. These are that data classification can either be used to “protect the organisation’s information assets from harm or misuse” or it can provide access to those assets “in a manner that supports the organisation’s business objectives”.

In the first instance, it may be possible to justify investment by communicating potential information security risks and setting them off against the hypothetical costs of any data loss incidents. A more upbeat approach, however, is to emphasise the positive benefits of programmes of this type.

First, because classification is likely to entail the tagging of data, it should mean that business users can routinely find the information they require, more quickly and easily, Curran says.

Second – and often more important – in order to win the argument, tagging data in this way can also help organisations in meeting legal and regulatory

requirements that require them to retrieve specific information within set timeframes.

Third, because the process of tagging helps to identify duplicated information for subsequent removal, data classification can help to cut down significantly on storage and backup costs.

## Playing tag

There is a downside to the tagging argument, warns Richard Walters, director and co-founder of information security consultancy Invictis. He believes that writing classifications into the metadata of a given file can end up having unintended operational consequences in terms of blocking people from doing their job.

“So you have to have clearly defined business processes and only apply blocks to clearly defined workflows,” he says. “Otherwise if the CEO can’t access a critical document at 10 o’clock at night using webmail as he has no access to his corporate email, you’re going to get pretty unpopular very quickly.”

***“Assets are likely to comprise HR, financial or intellectual property-related information, but prioritising in which order they should be tackled is important”***

Once funding has been obtained, the next step is to undertake a risk-assessment exercise in order to understand what the organisation’s most sensitive and confidential data assets are. Such assets are likely to comprise HR, financial or intellectual property-related information, but prioritising in which order they should be tackled is important because of the sheer amount of both structured and unstructured information that most organisations possess.

The next step is to identify both who owns the data in each key functional area and other interested stakeholders, including senior managers. The idea then is to

co-opt them into helping define high-level classification categories, while also working out which kinds of documents will fall into each grouping, who should be allowed to access them, who will be responsible for them and so on.

## Deciding on classifications

Although most large companies tend to go for five broad classifications such as Top Secret, Highly Confidential, Proprietary, Internal Use Only and Public, three may suffice for smaller organisations with less information to manage.

A vital consideration when choosing workshop participants is to include only senior personnel, as their decisions will carry most weight, and to limit numbers in order to prevent decision-making by committee. It is also important to set fairly tight deadlines in order to focus minds and guard against discussions disappearing down rabbit holes.

***“More than half of the data in most organisations does not need to be classified at all, as it falls into the default ‘public’ category”***

On a positive note, however, Pete Wood, a member of the London chapter of ISACA’s security advisory group and chief executive of security consultancy First Base Technologies, indicates that the classification task is not quite as onerous as it may appear at first glance. This is because more than half of the data in most organisations does not need to be classified at all, as it falls into the default ‘public’ category. To work out where everything else fits in, he advises asking stakeholders to assess the importance of confidentiality, integrity and availability in relation to each type of document under review.

“So if you’ve got a proposal or quote, you ask them ‘what would it mean in confidentiality terms if this got out?’ and



Richard Walters, Invictis.

to give the document an impact rating of between one and three on that basis,” says Wood. “For availability, it would be ‘what happens if you can’t read it?’ and for integrity ‘what happens if it’s not accurate?’. But you always go with the highest value among the categories and assign it that.”

When handing out such classifications, it is also worth bearing in mind that regular review dates should be included as part of the process to ensure that categories remain valid at different points in time. Such reviews are best carried out by information asset owners from the business who have been assigned responsibility for looking after the overall welfare of their data.

## Ensuring ongoing compliance

Invictis’ Walters explains the rationale: “When an annual report is being worked on internally, it may be classed as ‘highly confidential’. But when it goes out for review it could become ‘proprietary’, and be reduced still further to ‘public’ when it’s published. So it’s best practice to have processes in place to ensure that these classifications are regularly reassessed and reviewed.”

The next stage is to come up with a simple, enforceable policy statement that can be easily understood and employed by users. This statement is intended to outline in broad but well-defined terms

what each category means and which kinds of document fit into it.

Also valuable to include here is a read-at-a-glance table of ticks and crosses, the aim being to show users in a very visual fashion whether, for example, various document types have to be shredded or can just be thrown in the wastepaper bin after use. Another simple way of ensuring that personnel stick to the brief is to design Microsoft Word and Excel templates for a whole range of documents, from proposals to corporate presentations, which include the relevant protective marking in the footer.

“If someone writes a proposal, they start by opening the relevant template and, because everything’s embedded, they know right away if the document is confidential or not,” says Wood.

## The value of education

Ensuring that users keep to requirements is a matter of ongoing awareness training and education campaigns, both of which

will be key to the success of the scheme. “It’s not just a case of having half an hour in a lecture room and saying ‘this is the new scheme, so use it,’” explains Gillespie. “You have to explain why it’s there, why it’s important and how they need to apply it and you have to tell them that on an ongoing basis.”

***“It’s not rocket science. It’s just about using common sense and taking the time and effort to do it properly”***

While marketing departments can be co-opted to help with such campaigns, workers must also be provided with a conduit for obtaining answers to any queries. Possible mechanisms here range from a FAQ on the corporate intranet to email addresses or telephone helplines that are routed directly to information security personnel.

Document management systems can be used to both embed classifications into files and enforce them. And there

are useful tools, such as those from Titus Labs. This software provides users with a pop-up dialogue box that includes classification options when saving an email message for the first time.

Once the programme is finally up and running, the final step is to create effective governance procedures, which include regular audits and spot checks, in order to ensure that things continue to remain on track.

“The whole organisation has to stick to the classification scheme or there’s no point,” says Gillespie. “But it’s not rocket science. It’s just about using common sense and taking the time and effort to do it properly.”

## About the author

*Cath Everett is a freelance journalist who has been writing about business and technology issues since 1992. Her special areas of focus include information security, HR/management and skills issues, marketing and high-end software.*

# Going beyond the boundaries of compliance

Jon Geater, Thales

**Adherence to compliance standards is critical for most organisations, and as a result these standards often have a heavy influence in information security decision-making. There are numerous reasons for this, but most importantly, IT professionals are looking for guidance and direction, and where better to look than industry standards?**

From many perspectives this is not an unreasonable approach: organisations could spend a lot of money buying all of the security products they can find and still not be bulletproof. And even if they achieve a high level of security, the economics of such actions simply do not make sense. Complying with recognised

standards is a necessary step and in doing so, CIOs effectively ensure that they keep up with best practice. Or do they?

In a recent research report commissioned by Thales and conducted by the Ponemon Institute, more than 500 auditors were surveyed, with roughly half representing internal IT security audit

teams and half representing independent external audit companies and consultancies.<sup>1</sup> One of the initial findings was that only 32% said that the organisations they audit are proactive in managing privacy and data protection risks. The danger, however, is that this reactive, compliance-driven approach can leave organisations under-protected and constantly running to keep up.

Despite the agreement among auditors that organisations are mostly focused on compliance, 60% of respondents agreed



Jon Geater