

## Banking fraud on rise

**B**anking fraud using UK accounts in foreign countries has increased by 190% in the last three years. Figures from UK payments industry association APACS revealed that the cost of fraud committed on UK accounts abroad jumped to £121.2 million in the first half of this year from £41.8 million in the same period in 2005.

APACS attributes this to the lack of chip and pin technology abroad. "Criminals continue to target UK-issued cards, copying the magnetic stripe data and creating counterfeit magnetic stripe cards that can potentially be used fraudulently in countries that haven't

yet upgraded to chip and pin," it said in a statement. This year's figure represents an 11% increase on the same period last year.

Fraud committed on accounts by criminals in the UK still accounts for the largest share of bank fraud, however. Six in every ten compromised UK accounts were defrauded from within the country. And 17% more UK accounts were defrauded in the largely chip and pin-compliant UK than were compromised in the first half of 2007.

Overall, frauds on UK accounts grew by 14%. UK cash machine fraud jumped 22%, and fraud committed via face-to-face retailer transactions soared by a quarter.

## US toughens stance on cybercrime

**C**ongress brought legislation expanding the definition of cybercrime to the finish line last month when the US House of Representatives passed the Identity Theft Enforcement and Restitution Act (<http://tinyurl.com/4n2ajn>).

The legislation makes it possible for victims of identity theft to recoup the value of time and money spent recovering their identity, and also makes it possible for an identity theft felony to be prosecuted even

*Continued on page 2...*

## Featured this month:

### Lead me not into temptation

**T**he individual member of staff may be aware of the need for discretion in their work practices to protect the information they deal with on a routine basis. However, organisational demands, such as tight deadlines, which encourage working in public places, often make for a dynamic balancing act in which business will invariably win over security.

This article discusses some of the pressures and cites real life repercussions of badly designed and implemented security policy which can, in itself, have serious outcomes for both the business and the staff who become entangled. Be warned, your shocking conclusion may be that just making operational staff more security aware is not enough.

*Turn to page 6...*

## Contents

### NEWS

Banking fraud on rise	1
US toughens stance on cybercrime	1
Finjan uncovers new Javascript attacks	2

### FEATURES

#### It's a jungle out there:

#### Predators, prey and protection in the online wilderness

Steven Furnell and Jeremy Ward examine the similarity between the threats to users and organisations on the internet and the predator-prey relationships that exist in nature.	3
--	---

#### Lead me not into temptation

The Government is busy promoting the importance of security awareness of staff. This is entirely right and proper, says Wendy Goucher. However, the deeper expectations of senior management and other employees has proven to be the root of many security problems.	6
---	---

#### A practical approach to Government data handling recommendations

Mark Hocking of BeCrypt explores methods to support UK Government data handling requirements, and ways to design the IT systems that support them.	8
--	---

#### The rise of brandjacking against major brands

Margie Milam of brand protection expert MarkMonitor explores the evolution of brandjacking, and also discusses some of the legal issues surrounding the problem.	10
--	----

#### Are we being 'greenwashed' to the detriment of our organisations' security?

Mathieu Gorge explores ways to make your IT infrastructure greener without subverting security.	14
---	----

#### War and peace in cyberspace: Internal fraud – when system administrators leave

In this article, the authors write about their experiences in the world of ex-employee frauds.	19
--	----

### REGULARS

Editorial	2
Calendar	20

**Editorial Office:** Elsevier Ltd

The Boulevard, Langford Lane, Kidlington,  
Oxford, OX5 1GB, United Kingdom  
Tel: +44 (0)1865 843695, Fax: +44 (0)1865 843933  
Email: cfseditor@elsevier.com  
Web: www.computerfraudandsecurity.com

**Editor:** Danny Bradbury

**Editorial Advisors:**

**Silvano Ongetta**, Italy; **Chris Amery**, UK;  
**Jan Eloff**, South Africa; **Hans Gliss**, Germany;  
**David Herson**, UK; **P. Kraaibeek**, Germany;  
**Wayne Madsen**, Virginia, USA; **Belden Menkus**,  
Tennessee, USA; **Bill Murray**, Connecticut, USA;  
**Donn B. Parker**, California, USA; **Peter Sommer**, UK;  
**Mark Tantam**, UK; **Peter Thingsted**, Denmark;  
**Hank Wolfe**, New Zealand; **Charles Cresson Wood**,  
USA; **Bill J. Caelli**, Australia

**Production Editor:** Lin Lucas

**Subscription Information**

An annual subscription to Computer Fraud & Security includes 12 printed issues and online access for up to 5 users.

**Prices:**

€1017 for all European countries & Iran  
US\$1104 for all countries except Europe and Japan  
¥135 300 for Japan

(Prices valid until 31 December 2008)

To subscribe send payment to the address above.

Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971

Email: commsales@elsevier.com,

or via www.computerfraudandsecurity.com.

Subscriptions run for 12 months, from the date payment is received. Periodicals postage is paid at Rahway, NJ 07065, USA. Postmaster send all USA address corrections to: Computer Fraud & Security, 365 Blair Road, Avenel, NJ 07001, USA

Permissions may be sought directly from Elsevier Global Rights Department, PO Box 800, Oxford OX5 1DX, UK; phone: +44 1865 843830, fax: +44 1865 853333, email: permissions@elsevier.com. You may also contact Global Rights directly through Elsevier's home page (www.elsevier.com), selecting first 'Support & contact', then 'Copyright & permission'. In the USA, users may clear permissions and make payments through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA; phone: +1 978 750 8400, fax: +1 978 750 4744, and in the UK through the Copyright Licensing Agency Rapid Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P 0LP, UK; phone: +44 (0)20 7631 5555; fax: +44 (0)20 7631 5500. Other countries may have a local reprographic rights agency for payments.

**Derivative Works**

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution. Permission of the Publisher is required for all other derivative works, including compilations and translations.

**Electronic Storage or Usage**

Permission of the Publisher is required to store or use electronically any material contained in this journal, including any article or part of an article. Except as outlined above, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the Publisher. Address permissions requests to: Elsevier Science Global Rights Department, at the mail, fax and email addresses noted above.

**Notice**

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made. Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

02065

Printed by: Mayfield Press (Oxford) Limited

*Continued from page 1...*

when committed within a state. Previously, it had to be committed across state lines.

Other restrictions that the Act removes include the value of the damage caused. Under the new legislation, damage worth less than US\$5 000 can still be considered as a felony, rather than a misdemeanor, and it also makes it possible to prosecute the use of spyware on ten or more computers. This will make it easier to prosecute bot net operators.

Already passed by the Senate, provisions in the Act were included in a House bill that focused on providing secret service protection for former vice-presidents. It now awaits presidential approval.

## Finjan uncovers new Javascript attacks

**Security software vendor Finjan has highlighted a new technique used by criminals to hide malicious software in its latest report. The company warns that malware developers are now putting obfuscated code into files not traditionally used to deliver malicious code, such as PDF and Flash files.**

According to the company's *Malicious Page of the Month* report, issued in

September, criminals are exploiting applications' third party support for Javascript as a means of embedding malicious code.

"Since Javascript is the most-used scripting language for communication with web browsers, third-party applications such as Flash player, PDF readers and other multimedia applications add support for JS writing as part of their application," said the report.

Obfuscation of Javascript code, in which program code is disguised to fool malware detection tools, has been an ongoing practice for years. Coders used to use predefined functions to de-obfuscate and run code, and then switched to using private keys that would essentially decrypt obfuscated code embedded on a web site. Now, it has found PDFs that use obfuscated Javascript to execute malware on a victim's computer.

When PDF files are used in this way, the infection technique doesn't involve Javascript on web sites at all. However, the report also warns that when used in Flash, the attack could create a significant infection vector when used to display user-generated content on web 2.0 sites. Flash doesn't use Javascript directly (it uses Adobe's similar language, Actionscript). However, it is possible to write Javascript to a web page dynamically using Flash code.

## Editorial

One story that didn't make it into Computer Fraud & Security this month was the hacking of vice presidential candidate Sarah Palin's email account.

The method used to hijack it is particularly important. The hacker used Google to find answers to her 'secret questions' and change her password. One of the questions was where she met her husband, which the hacker said he was able to find out very quickly with a Google search.

This proves once again that in an age of freely available information, the concept of secret questions used to identify a password must be treated with extreme care. The chances are that the answers to most questions are available in the public domain, either through

Facebook or LinkedIn accounts, via public birth and death records or simply through search engines. Palin's relatively high public profile made the hacker's job even easier, but the dangers still remain, even for the ordinary Joe or Jane. In an age where social networking sites and memes encourage people to distribute private information about themselves online, insecure password questions are more dangerous than ever. The best answer to a mandatory secret question provided by a web site may simply be a long, random string designed never to be accessed or submitted again. Instead, storing the strong password in encrypted password management software might stop this kind of embarrassment from happening again.

*Danny Bradbury*

# It's a jungle out there: Predators, prey and protection in the online wilderness

Steven Furnell, head, Centre for Information Security & Network Research, University of Plymouth and Jeremy Ward, director of information security solution practice, Symantec (UK) Limited

It is no exaggeration that the internet is host to a range of threats, with problems afflicting individuals and organisations alike. For example, the 2008 Information Security Breaches Survey from the UK's Department for Business Enterprise & Regulatory Reform suggests that 76% of very large businesses suffered a serious security incident (with a significant proportion of the incident reporting categories being internet-related).<sup>1</sup> Meanwhile, domestic users (many of whom instinctively consider themselves unlikely targets) are frequently shown to be at considerable risk. Example findings from a 2007 study by McAfee/NCSA suggest that 54% of 378 respondents had experienced a virus, while 44% believed their system currently contained spyware.<sup>2</sup>

Such problems show the internet to be a far more dangerous environment than the real world we normally inhabit. A real world analogy for visiting the internet environment, with its risks and potential hostilities, could be a walk in the jungle. Both of these environments are largely unknown, contain myriad threats, and only offer relative safety if you stick to the established paths. Having suggested this analogy, we should consider how we think about ourselves and our potential attackers. This article considers the similarity between online attacker-victim relationships and predator-prey relationships found in nature. Having established that the drivers and advantages afforded to predators are quite similar in both contexts, we then consider how we (as the potential prey) could also follow some of nature's examples in our collective response.

This is not the first paper to consider a comparison between threats in cyberspace and the natural world. In earlier work we presented a comparison between malware and biological parasites, looking at how threats such as worms and viruses have become

increasingly more problematic as they have taken on more of the characteristics and behaviours of viruses in nature.<sup>3</sup> Taking a wider view of online threats, Carlsson and Davidsson present a comparison between information and biological ecosystems, referring to an 'arms race' between innocent and exploiter agents and concluding that the ecosystem as a whole becomes more robust as a consequence.<sup>4</sup> However, while the ultimate conclusion is likely to be valid, presenting the 'arms race' as equally balanced between the exploiter and victim gives no consideration to the varying pressures that each party faces. In addition, the discussion only seems to look at the one-to-one relationship that would exist between a single attacker and a single victim. It does not recognise the implications that arise if the would-be exploiters have a vastly larger population of potential victims to prey upon. As such, the aim in this two-part article is to consider the aspects of scale that currently work in favour of the predators and need to be similarly leveraged to the advantage of the prey.



Steven Furnell

## The internet as an ecosystem

We believe that it is valid and useful to view the internet as an ecosystem, in which a huge number of entities interact in varied and complex ways, for a variety of purposes. While the internet clearly offers advantages to those who use it for business or leisure, it also provides a good environment for cyber-predators – those who wish to exploit the 'legitimate' users. To appreciate why, we can consider the internet in terms of the traditional pre-requisites of means, motive, and opportunity that it affords a potential cyber-predator:

- **Means** in this context refers to a way for the cyber-predator to get at the cyber-prey. This is no challenge online, as a variety of channels used by the cyber-prey can easily be utilised by the cyber-predator as well. Examples include peer-to-peer networking sites, such as social networking and wargaming sites. These provide online predators with the cyber equivalent of waterholes, where prey species come to drink.

- **Motive** refers to there being an obvious gain for the cyber-predator. Everything online is visible from anywhere, so the cyber-predator can easily see the cyber-prey. In addition, there are associated gains to be made (either from the users directly or via the exploitation of their systems). Examples include online gambling and online banking, where money is transmitted online. Less obvious motives for the cyber-predator involve their ability to exploit online transactions to acquire new identities, although such interactions have more in common with parasitism than classic predation.
- **Opportunity** requires the obvious exposure of the cyber-prey, which typically poses no problem as many systems and users are effectively open to predation all day, every day (with the continued rise in broadband connectivity serving to increase the pool). Examples in this context include the tendency of internet users to neglect elementary security precautions, such as the use of firewalls and anti-virus; as well as basic naivety in continuing to succumb to social engineering ploys, such as phishing.

**“Everything online is visible from anywhere; so the cyber-predator can easily see the cyber-prey”**

In a biological ecosystem all the interacting entities strive to gain an advantage from the opportunities offered them by participation in the ecosystem. Advantage in the internet ecosystem may not be as simple and obvious. Internet gains are not only the acquisition of food or mates (although both are available), but may also be more complex and subtle, such as social and intellectual achievement. Like a biological ecosystem, the internet imposes selection pressure on participating entities – ensuring that those who gain the most advantage are able to intensify their participation, while those who fail to gain any advantage, or who find themselves at a disadvantage, are squeezed out and no longer participate. Like an ecosystem too, the internet offers interacting

entities the choice of gaining advantages from both competition and cooperation. Each of these characteristics is examined in this paper in terms of its implications for internet security.

**Predators versus prey – leveraging a natural advantage?**

In a biological ecosystem, selection pressure is an inherent result of the interaction between its entities. Selection pressure ensures the preferential survival of traits within individuals that enable them to maximise the number of their descendants. It therefore drives change and adaptation in individuals, populations, and ultimately the ecosystem as a whole. However, selection pressures that result from interactions between predators and prey act differently on individuals in each of these groups. As Figure 1 illustrates, in predator/prey interaction, predators face far greater selection pressure than prey. This is because the size of the prey population is large relative to the size of the predator population. As a result, the pressure on an individual member of a prey population is relatively small, since the chance of any one individual being preyed on is low. On the other hand, the pressure on an individual predator is relatively large, because failure in a predator/prey interaction has potentially catastrophic consequences for their survival.

The analogy between the biological ecosystem and the internet is clear. The majority of legitimate internet users (prey) thankfully do not suffer from the

actions of cyber-predators. However, this has created a situation in which prey tend to believe that predation is someone else’s problem, and that they themselves are unlikely to fall victim to it.

As a consequence of selection pressure, the predator will always need to improve faster than the prey. On this basis, we can take the analogy in the natural world a stage further and consider the theory of natural selection, as expressed by Charles Darwin in *The Origin of Species*, “... each new variety, and ultimately each new species, is produced and maintained by having some advantage over those with which it comes into competition; and the consequent extinction of less-favoured forms almost inevitably follows.”<sup>5</sup>

Cyber-predators have demonstrated their ability to take advantage of the user community through exploitation of popular services, showing that they are well attuned to the zeitgeist in online activity and can quickly adapt their techniques. This is seen in successive generations of attackers that have seized upon email, instant messaging, peer-to-peer, and most recently social networks as a means of targeting and exploiting the unwitting end-users.<sup>6</sup> Wherever prey can be found, the predators soon are too. In addition, the attackers’ responsiveness is shown by their ability to exploit current events. Anything from the arrival of the festive season to the start of the Olympic Games can quickly be harnessed to hook potential victims.<sup>7, 8</sup> The predators are agile and adaptable.

Although similarities exist, there are also some notable differences between

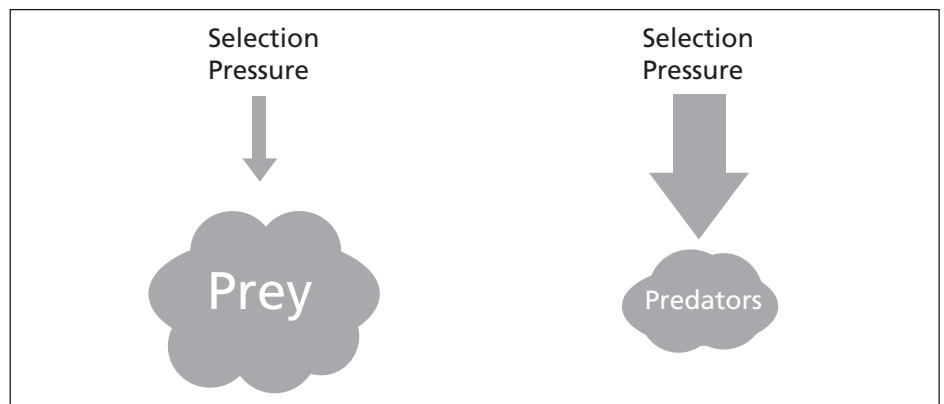


Figure 1: The different selection pressures on predators and prey.

predator/prey relationships in the natural world and those on the internet. Unfortunately, these differences only serve to amplify the risk to online prey:

- Online predators are able to hit multiple groups of prey with a single attack (best exemplified in contexts such as malware and phishing).
- The predator/prey interaction is not constrained by geography or time, so there is no limit to the number of predators that individual prey may face.
- Predators in the online context can easily learn from each other and assimilate successful techniques (for example, malware mechanisms originated by one attacker are quickly utilised by others – scripting of exploits makes them easily available to a large-scale population).

***“Anything from the arrival of the festive season to the start of the Olympic Games can quickly be harnessed to hook potential victims”***

Having established the validity of the predator/prey analogy, when considering interactions between legitimate users of the internet and those who seek to exploit them, it is worth looking at why the internet provides such an effective environment for predators and why it has not, as yet, been leveraged to the same extent by the prey. The success of online predators has not arisen through coincidence and happenstance. They have demonstrated their ability to respond to selection pressure by recognising ways to capitalise on the behaviour of potential prey, such as legitimate internet users’ propensity to adopt new services while not protecting themselves appropriately when doing so. In short, they are making use of the internet far more effectively for attack than the prey have managed to use it for defence. The reason for this can essentially be linked to the attitude of legitimate internet users, who are not well enough attuned

to their risk or are ill-prepared to devote time, money and effort to address it.

Another common characteristic of prey is that they are individualistic; not only do they consider themselves to have relatively little chance of becoming a victim, but they also fail to appreciate that their being hit would also have a potential impact upon others – particularly their direct contacts. A victim is most likely to put at risk those who are closest to him or her – family, friends, colleagues, and business contacts. For example, compare the spread of (some) replicating malware such as worms and viruses, and the behaviour of viruses in the natural world. In both cases when someone becomes infected, it increases the immediate risk to those closest to them. In the natural world, this would be those closest in proximity (in the same household or workplace), whereas in cyberspace it would be those with whom they communicate most frequently. A fundamental difference in cyberspace, though, is that direct contact is not constrained by time or location. As a consequence, a large-scale incident can develop very quickly, a good example being the infamous mass mailer I Love You worm, a classic malware technique. The primary means of propagation in this case was that the worm emailed itself to all the contacts in a victim’s Outlook address book. It also used an effective social engineering hook by pretending to be a love letter for the recipient. Both these characteristics helped to ensure that it rapidly became a worldwide problem.

Such cases not only exploit the technology of the internet, but also leverage the ‘small world’ phenomenon, in which networks of interpersonal relationships can very quickly expand to achieve world-wide coverage.<sup>9</sup> Recent research based upon internet communication has added further weight to the theory that social connectivity can lead to links between individuals who otherwise have no direct relationship.<sup>10</sup> A predator’s ability to exploit underlying mechanisms, such as email and instant messaging, can thus deliver rapid access to global prey.

Having established some of the characteristics of predators and prey in an

internet environment, we will move on in the second part of this article to evaluate response mechanisms that prey can use to protect themselves. This will be published in the November edition of *Computer Fraud & Security*.

### About the authors

*Prof. Steven Furnell is the head of the Centre for Information Security & Network Research at the University of Plymouth in the United Kingdom, and an Adjunct Professor with Edith Cowan University in Western Australia. His interests include security management, computer crime, user authentication, and security usability. Prof. Furnell is a UK representative in International Federation for Information Processing (IFIP) working groups relating to Information Security Management (of which he is the current chair) and Information Security Education. He is the author of over 190 papers in refereed international journals and conference proceedings, as well as the books Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). Further details can be found at [www.plymouth.ac.uk/cisnr](http://www.plymouth.ac.uk/cisnr).*

*Dr Jeremy Ward is director of information security solution practice for Symantec in Europe, Middle East and Africa. His interests include information security risk assessment and management, information security governance in business, information security risk metrics and the development of standards for information security risk assessment and management. Dr Ward is chairman of the European Network and Information Security Agency’s working party on information security risk assessment and management. He is an expert adviser on information security to a number of international and national bodies, such as the UK CBI and the OECD. He started working life as a research entomologist and has retained an interest in the interaction between IT and biological systems.*

### References

1. BERR. 2008. 2008 Information Security Breaches Survey – Technical Report. Department for Business

- Enterprise & Regulatory Reform. April 2008. URN 08/788.
2. McAfee-NCSA. 2007. McAfee-NCSA Online Safety Study – Newsworthy Analysis, October 2007 <[http://staysafeonline.org/pdf/McAfee\\_NCSA\\_analysis.pdf](http://staysafeonline.org/pdf/McAfee_NCSA_analysis.pdf)>.
  3. Furnell, S. and J. Ward. 2004. “Malware Comes of Age: The arrival of the true computer parasite.” Network Security October 2004 : 11-15.
  4. Carlsson, B. and Paul Davidsson. 2001. “A Biological View on Information Ecosystems”, in Proceedings of the Second International Conference on Intelligent Agent Technology, World Scientific.
  5. Darwin, C. On the origin of species by means of natural selection. Chapter 10, “on extinction”. 1st ed.
  6. Persaud, J. 2008. “Facebook and MySpace attacked by new worms.” SC Magazine. 1 October 2008. <<http://www.scmagazineuk.com/Facebook-and-MySpace-attacked-by-new-worms/article/113250/>>.
  7. Sophos. 2007. “Santa’s virus striptease goes down a Storm, warns Sophos.” Press release. Sophos. 24 December 2007. <<http://www.sophos.com/pressoffice/news/articles/2007/12/santa-storm.html>>.
  8. BBC. 2008. “Hi-tech thieves target Olympics.” BBC News Online. 9 October 2008. <<http://news.bbc.co.uk/1/hi/technology/7548870.stm>>.
  9. Travers, J. and S. Milgram. 1969. “An Experimental Study of the Small World Problem.” Sociometry 32.4 : 425-443.
  10. BBC. 2008. “Study revives six degrees theory.” BBC News Online. 6 October 2008. <<http://news.bbc.co.uk/1/hi/technology/7539329.stm>>.

# Lead me not into temptation

Wendy Goucher, Idrach Limited

**When my primary school aged son returned home yesterday in his new uniform (we live in Scotland so he has been back a while), I noticed that the knees of his trousers are already showing signs of wear. The problem here is the tension between the desire I have for him to be smart through the day and the (arguably more important) desire to have him playing active games in the breaks and therefore keep fit and healthy. In business there is a tension between the desire to keep information secure and it actually staying secure in practice. There are a number of reasons for this. Suffice to say at the outset that security awareness programs often focus on what staff must and must not do. In many cases, however, it is the demands of the business itself that bring about insecure practice.**



Wendy Goucher

## The privacy of passwords in practice

I work for a small consultancy and when I am out talking to clients there is a good chance there is nobody around to mind the office. To this end, a month or so ago I became part of the iPhone gang. Therefore, I can now take calls and deal with my e-mail on the train so people can get a quick reply to urgent questions. If I also have my laptop with me, there is very little business I can't do during the journey, and I am not alone. Of course this can lead to indiscretion on the phone and plenty of opportunities for the bored traveler to indulge in a spot of shoulder surfing, both of which are significant problems that I have discussed at length in this publication before.

With mobile indiscretion it is easy to put the lion's share of the blame on the person working in public places. However, as with a good puppet show, that is to miss the strings of control. Much of this work is done because of the perception of travelling time as wasteful. When your staff member comes off a customer site, do you expect them to 'check in' with you and give you information as soon as they can? This may be necessary, especially if there is a tight deadline, but not always. However, it has become part of the expectation or culture of many businesses. Likewise in the office, there are expectations which mean that the required behaviour is against the spirit of good information security.

An example that has happened across the land during the summer is the sharing of passwords. Speaking to office administra-

tors I find they often have a note of their colleague or boss's passwords to keep an eye on things while they are on holiday. I realise that the sharing of passwords is expressly prohibited in just about all acceptable use policies, but it does still happen. After all, if I trust my colleague, and I have no non-work email going to the account, it seems harmless. Nobody wants to come back to an overflowing in-tray. But the password system is important to the business because as well as access, it allows for accountability, traceability as well as protection for the user. If there is fraud or other discipline issues such as harassment using the email system then it is necessary to be able to see where the suspicious activity does, and does not, originate. If the person designated to that login has shared it, then it can be very hard for them to prove their innocence.

Let me give you a real life example. A few years ago a friend of mine found themselves suspended from their job because someone from within the business had spoofed his email account and sent inappropriate mail to senior managers using it. Fortunately, my friend was at a social event, with no computer access at the time of the incident (it was pre-Blackberry) and had a number of witnesses who could attest to his attendance. Even so it took several weeks to fully untangle the story and identify the perpetrator. If my friend had shared his password with a colleague, or colleagues, then it may well have proved harder, or even impossible, to demonstrate the innocence of all concerned and that would certainly have had a big impact on his career, which I suspect was the perpetrator's intent.

## Policy meets the real world

Another incident I heard about a few years ago again also arose partly because of the perception of passwords as simply a key to access. However, a more important factor in this case was the mismatch between a good idea and the implementation. This situation happened in a London hospital about five years ago. The patient records were all kept on a database that was reasonably (for its time) protected from outside intrusion.

They were protected internally by giving each member of the nursing staff their own personal login password. Clearly this is a good idea. Then there came the problem. Somebody thought that it was a really good idea if the passwords were not given to a member of staff until they had attended a security awareness briefing. In many organisations, this would be a straightforward matter, but there are real problems when you try to fit this generalised plan to a hospital where there is a high dependency on agency staff or short-term workers. This is especially so because at the same time the budget for training was being tightly controlled and it was felt that the security awareness briefing should only be delivered in normal

business hours to reduce any overtime claim for training staff.

This meant, in practice, that many staff members on the night shift did not have passwords. This was a particular problem amongst agency staff who were unwilling, or unable, to attend a class in the day. In the event the problem was not immediately obvious as staff just passed on their password (or the one they knew) to the incoming colleague. While it is true, I am sure, that nurses are professional and discrete and would not allow anyone who should not be authorised to have access, they themselves were left vulnerable should a mistake happen. If there had been a problem from the entering of incorrect data, or the using of the data incorrectly, the person at fault was unlikely to be identified and many innocent staff members would have suffered upset and stress due not to their fault, but to the lack of operational knowledge of the person designing the system.

## Information in transit

The final way in which the organisation leads its staff into the ways of unsafe practice is by expecting work done at home. Where the business is cautious about the use of laptops due to the risk of theft, this leads to work being transferred using USB keys, sticks thumb drives or whatever you want to call them. When common external data storage was on 3½" discs many of my colleagues had boxes of them on their desk. Some even neatly categorised and labelled. Now we carry one or maybe two USB keys which hold information from a variety of sources. So if a few documents travel home to be worked on the chances are that there are many more along with it. This key could be lost, but it can also be borrowed amongst members of the family.

When I visit my local college I often see students accessing work on sticks that contain work that appears to be from local businesses and organisations. For the most part no harm comes of it but the business information is away from the place it is meant to be and that should always be a matter of concern.

Security awareness should be addressing more than basic business activity. It should look to the culture of the business and the expectations it has of staff, and then be aware of the operational limitations that might mean that staff gangplank security measures in order to get work done. It is like the problems that the smoking ban brought to the physical security of buildings. The need to swipe or pin in every smoking break often leads to staff propping fire doors open with fire extinguishers so as to ease their way. It is simple to simply prohibit such activities. It is harder, but arguably more effective in many cases, to look for an alternative such as secured areas that can be reached without security devices, but that still prevents casual entry with a gate.

There are many ways in which lack of security awareness amongst the staff leads to information security incidents. For this reason, time and effort needs to be skillfully applied to keeping awareness sharp. However, this is less than entirely effective if the organisation applies pressure. Such pressure could call for contact that leads to indiscrete communication, for deadlines leading to information traveling between home and work in an insecure manner, and for the following of security ideas that are incompatible with normal operations is stronger than the culture of security.

## About the author

*With a background in psychology and economics, Wendy Goucher is unusual in the information security arena. She began to focus her interest in the human contribution to business security about 10 years ago and for a long time she conducted the research as an antidote to the tedium of routine work. Now working for Idrach Ltd, a small consultancy, much of her effort is directed at persuading businesses to delegate real responsibility for information security from the sticky grasp of IT onto everyone's desk. Wendy is a member of the British Computer Society and an Associate Member of the Institute of Information Security Professionals. She can be contacted at [wendy@idrach.com](mailto:wendy@idrach.com)*

# A practical approach to Government data handling recommendations

Marc Hocking, chief technology officer, BeCrypt Limited

**Three reports have recently been published about data handling in the Government and public sector space:**

- *Data Handling Procedures in Government: Final Report*, undertaken by the Cabinet Office<sup>1</sup>
- *Loss of MOD Personal Data for the Permanent Under Secretary Ministry of Defence*, by Sir Edmund Burton<sup>2</sup>
- *Review of information security at HM Revenue and Customs: Final Report*, by Kieran Poynter<sup>3</sup>

Each report makes a different set of recommendations that will impact widely on the public sector, third-party organisations that work with the public sector, and the wider business community.

Her Majesty's Government (HMG) is not alone in having well documented instances of breaches of confidentiality of personally identifiable data; large commercial organisations have them too.

HMG has rigorous controls in place to securely manage departmental data – protective levels are assigned to rank data in impact levels one to six. Yet these controls are not necessarily applied to citizens' data. To date there have been few guidelines as to how and when citizens' data is managed with respect to internal access and availability, or to where and with whom that data is shared.

While the Cabinet Office report makes recommendations to redress this situation it also clearly states that each Government department is responsible for assessing and managing its own data handling requirements and that, where appropriate, individual departments may go beyond the minimum recommendations to secure information.

All of the reports accept that personal data is required in order to provide better and more personalised services

and that this data must be stored.

However, all state that data should be properly safeguarded because the government, rather than the owner, is the custodian of the data. A new concept of 'protected personal information' has been introduced.

Another common theme is that end users, i.e. staff members, must be given clear guidance, including regular training, on the treatment and handling of data and that data security measures must be quantifiable, transparent, and easily open to scrutiny.

So how do organisations comply with three different sets of data handling recommendations? How do they ensure that staff understand and adhere to data security policies, and how can they prove that policies are followed? On top of this, given the ever increasing drives to push down costs, provide more flexible working for staff, and share data with third parties to provide better services, how can they implement stronger data security systems?

All of the reports call for a change in culture to one in which personal data is treated with the utmost respect. This will happen slowly through re-educating staff to understand the implications of safe data handling procedures. Yet, how do

they impose another set of policies on an already beleaguered workforce? It can be done by computer systems that underpin set policies and procedures, with which people will comply, because their behaviour is either controlled or monitored.

Monitoring may be achieved by the implementation of data security systems. These systems should be transparent to the end users and therefore not impact the way they work. They should also be centrally managed so procedures can be monitored and enforced. Audit trails would prove compliance and highlight any irregularities.

As the reports note, there are challenges to managing data; namely how and where it should be stored, as well as how much is required and for how long. The reports also suggest that there is no need to store more data than is required, or for longer than is necessary. Data should also not be sent to places where it is not required.

The issues of data aggregation and lifecycle management require policies in place and procedures for ensuring compliance and auditing the policy adherence.

A third area of vulnerability is data access: who is accessing the data, and what specifically do they have access to? For an organisation this means putting policies in place to monitor the back end (where the data is stored) and the front end (where users access the data).

## Sharing information securely

Breaches of the security and confidentiality of protected personal information show that Government departments need to develop policies and procedures to handle

citizens' data more sensitively, particularly when sharing information with third parties, which is seen as the biggest risk area.

It is important to enable shared services. Therefore data should be protected in such a way that authorised recipients can still easily access it. Information that leaves direct control must be protected by clear processes which ensure that the right person is authorised to receive and access it. These issues have driven a number of initiatives, including the Whole of Life Assurance Model from CESG, which have resulted in new products that allow the secure export of data, as well as the control of the data by the authorised recipient.<sup>4</sup>

**“Breaches of the security and confidentiality of protected personal information show that Government departments need to develop policies and procedures to handle citizens’ data more sensitively....”**

CESG believes that the Assurance Model will help address some of the challenges the Government community (and its partners) face in developing ICT systems in today’s complex and joined-up world. The model has been created to provide a consistent language and framework for people managing information risks to government business.

The Assurance Model may be used by anyone who manages technical risks to information assets or data, whether they are a departmental ICT system accreditor, product manufacturer, or an ICT user. The model helps to identify alternative ways of mitigating the impact or likelihood of a risk. It comprises four elements. They are considerations associated with:

- The concept, origin and development of an ICT solution (*intrinsic*)
- The independent testing of an ICT solution outside the development environment (*extrinsic*)
- The architecture of the ICT solution and its integration with the business (*implementation*)

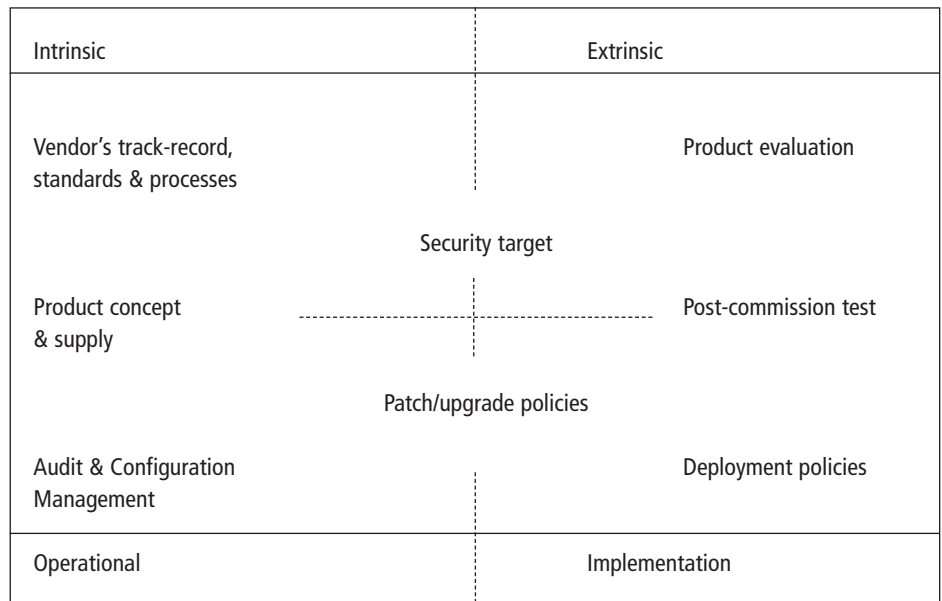


Figure 1: The Assurance Model.

- An ICT solution that handles ‘live’ information or that is used by or relied upon by a business (*operation*).

By considering the mitigations for a risk across all of these elements, risk managers or owners can build up a whole-life risk management plan. They can choose the most appropriate approach to managing an information risk and balancing the needs of the business for functionality, with the need to manage the risks to the integrity, availability, and confidentiality of its data.

An example of this framework might be used with a firewall. A firewall controls access across an IT network boundary and its policies must reflect the needs of the business. A risk assessment of a network connection might determine that an assured product is needed.

Risk managers who use the Assurance Model should also ask the following questions:

- How much trust will be needed in the supply chain, now and later? (*intrinsic, operational*)
- How will upgrades or patching be performed? (*intrinsic, operational*)
- Does the hardware or software need to be evaluated to mitigate the risks, or would regular penetration testing be more appropriate? (*extrinsic, operational*)
- Will the firewall be integrated into the

- business so that its security functions aren’t degraded? (*implementation*)
- Can the firewall be configured to support the access policies that the business needs? (*intrinsic, implementation*)
- How will illicit access attempts be identified and what will be done if they occur? (*implementation, operational*).

Such questions may be asked at any point in the solution life-cycle, but are most powerful when asked continuously.

**Examples of risk management by category**

Although the aim is to phase out the use of removable media for the transfer of data or the sharing of data with third parties, in the short term many departments must still use this removable media. To solve this problem, government-approved products are now available with a ‘zero footprint’ encryption option in which data files are protected by encryption and automatically decrypted when the authorised recipient authenticates. In addition, these encryption options can define how data is handled once received at the destination, providing controls and an audit trail to track what information has been sent, what has been received,

and ensure that it has not been tampered with in transit.

An even better solution is to allow data to be accessed on its home server so that it never leaves its safe and protected environment. This can be achieved by providing cost-effective secure access via a virtual private network, which is ideal for staff members who need to work away from secured headquarters; for example, from a third party's premises, on the road, or at home. This solution can also be used to grant other organisations access to data without the overhead of having to set up permanent network access. Users are issued with a low-cost USB device that carries a secure, encrypted operating system. With this device, they can boot from any machine and access defined areas and files on the home network. The device is totally isolated from the host machine so there is no possibility of cross-contamination by viruses and other malware, or of data leakage. If lost, no data can be accessed by unauthorised users because the USB device is totally encrypted.

Using this kind of device, staff may work in any location, including at home. This supports the Government's move to

provide more flexible working conditions for its staff, and enables staff to be more productive, while maintaining a better work-life balance.

With the deployment of such solutions, citizens and employees can be assured that the integrity and confidentiality of their personally identifiable data is appropriately managed. And in time, Government departments should gain a reputation for being safe custodians of other people's information.

### About the author

*Marc Hocking is a leading proponent of information assurance, with Government and global cross-border data security experience. Before joining BeCrypt, Marc worked for the UK Government Cabinet Office where he worked closely with HMG CTO and CIO councils to deliver solutions to support the delivery of the HMG Transformational Government Implementation Plan. Mark also spent ten years in a variety of roles within global financial institutions, working on systems that included PKI, authentication, authorisation, and privilege-management infrastructure.*

### References

1. Cabinet Office. "Data Handling Procedures in Government." June 2008. Cabinet Office. 14 September 2008 [http://www.cabinetoffice.gov.uk/reports/data\\_handling.aspx](http://www.cabinetoffice.gov.uk/reports/data_handling.aspx)
2. Burton, Sir Edmund. "Report into the Loss of MOD Personal Data. For Permanent Under Secretary Ministry of Defence." UK Ministry of Defence. 30 April 2008. 14 September 2008 <[http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton\\_review\\_rpt20080430.pdf](http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton_review_rpt20080430.pdf)>.
3. Poynter, K. "Review of information security at HM Revenue and Customs. Final Report." HM Treasury. June 2008. 14 September 2008 <[http://www.hm-treasury.gov.uk/media/0/1/poynter\\_review250608.pdf](http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf)>.
4. "CESG Assurance Model." CESG The National Technical Authority for Information Assurance. 14 September 2008 <[http://www.cesg.gov.uk/policy\\_technologies/assurance/index.shtml](http://www.cesg.gov.uk/policy_technologies/assurance/index.shtml)>.

# The rise of brandjacking against major brands

Margie Milam, corporate secretary and general counsel, MarkMonitor

**By all measures, web 2.0 has been universally successful in bringing users of all ages, demographics, and interests to the internet. This global reach, coupled with the low cost of entry, has attracted both legitimate and unsavoury elements determined to profit from the trust and naiveté of this online community.**

As a brand protection company, MarkMonitor suspected that major brands were experiencing unprecedented levels of online abuse. These suspicions fuelled the genesis of its

Brandjacking Index, a quarterly report that highlights the systematic analysis of the world's largest brands and contains trends of threats targeting these famous brands.<sup>1</sup>

## Methodology

The Brandjacking Index is produced quarterly and explores numerical trends and statistics of brand abuse, targeting



Margie Milam

30 of the most popular brands as ranked by Interbrand. It contains anecdotal information about the business and technical methods used by brandjackers, along with analysis and discussion of the business and social implications of brand abuse. The Brandjacking Index tracks millions of emails and billions of web pages, including listings of online auctions and B2B exchanges. The conclusions are based upon a weekly sampling of potential brand abuse incidents conducted throughout the period from the first quarter of 2007 until the end of the first quarter of 2008.

## Global brands under attack on multiple fronts

The results surprised MarkMonitor. It was common knowledge among brand professionals that cybersquatting had been a problem since the 1990s. However, no one anticipated the exponential growth of cybersquatting and the various derivative forms of abuse such as domain kiting, pay-per-click (PPC) abuse, and false association. In the first quarter of 2008, MarkMonitor observed an average of 402 882 instances of cybersquatting per week targeting 30 major brands. This represented an increase of approximately 40% over the same period in 2007. The obvious question is: what accounts for this dramatic increase?

## Evolution of cybersquatting

The cybersquatters of the 1990s profited by misdirecting consumer traffic to web sites that could generate revenue with offensive content such as pornography, gambling and other illicit activities. By 2004, most memorable dictionary words were registered as .coms, leaving no quality names available for registration. A secondary market then emerged for trading or reselling domain names, which generated additional revenue for registrants of domain names. Portfolios of domain names were registered en

masse as part of a perceived land grab by speculators eager to participate in this new market.

With these enlarged portfolios, domain speculators, or 'domainers' as they prefer to be called, sought ways of monetising their portfolios while they waited for offers to purchase their domain names. By pointing their domain names to pay-per-click search pages, they could generate revenue from internet traffic associated with those domain names. But since all good traffic-generating domain names were already registered; registering variations and misspellings of famous brands became their modus operandi.

## Domainers abuse ICANN policies

Before long, domainers developed more lucrative schemes for abusing famous names, such as domain tasting and kiting. Taking advantage of a loop-hole in ICANN policy, domain name registrars allowed domainers to register a domain name for a brief period to test the amount of pay-per-click revenue generated. If the domain name was deleted within five days, the domainer would not be required to pay for the domain name and could actually keep the revenues earned during that five-day period. This practice, known as domain tasting, gained quick acceptance among the domainer community. Domainers would then re-register the same domain name a few days later, for another five-day period. This cycle became known as domain kiting.

Domain kiting became advantageous because companies did not have the resources necessary to pursue each kiting incident. Unable to keep up with the paper trail of registrations, deletions, and re-registrations, abusing brands was virtually risk free. The good news is that domain kiting and the related abuse, PPC activity, have levelled off. This is attributable to the increased scrutiny on domain kiting by ICANN, as well as a wave of high profile litigation by major brand holders against certain domainers and complicit registrars.

## Phishing and online fraud continue as insidious threats against brands

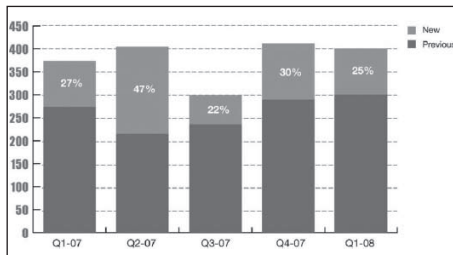
Phishing for financial credentials continues to be a widespread problem, confounding businesses and governments in the search for an easy solution, as criminals such as the Rock Phish gang adapt their technology and targets to maximise their ill-gotten gains. These international gangsters misuse domain name servers to launch thousands of phishing URLs to avoid the anti-phishing countermeasures adopted by browsers and other security companies, such as blacklists.

***"The Brandjacking Index reveals that a total of 14 companies account for 90% of all phish targets"***

Phishing has become a specialised scheme, with phishers carefully picking their most desirable targets. The Brandjacking Index reveals that a total of 14 companies account for 90% of all phish targets, based on phished URLs. During the first quarter of 2008, there was a decrease in the number of new organisations targeted by phishers. 102 companies were observed for the first time as attack subjects, versus 122 in the fourth quarter of 2007. There is also a seasonal shift in the types of target industries as well as increasing sophistication in the types of exploits used by phishers to obtain individual user account information.

Overall, 406 different organisations were targets of phishing attacks last quarter, which represents an increase of 8% over the number observed from the first quarter of 2007. MarkMonitor observed a slight decrease in attacks from last quarter, consistent with a seasonal drop as post-holiday shopping declines. Banks and financial services firms continue to be the most-phished business, having 12 out of the 14 most-phished

brands. The emphasis of phishing is on the English language; seven out of the 14 most-phished companies are based in the United States, and the remaining seven in the United Kingdom.



**Figure 1: New vs. previously attacked organisations.**

## How much is the dark economy of brandjacking worth?

Estimating the value of the brandjacking economy is difficult, due to the lack of publicised information. By combining some known segments, MarkMonitor estimates its value at over US\$141 billion globally.

Losses associated with phishing are fuelled by a growing demand for personal credentials in the underground economy. Symantec reports that bank account credentials are advertised on underground economy servers at prices ranging from US\$10-US\$1000, depending upon the amount of information available.

The amount of domain-related PPC revenue was estimated to be approximately US\$1 billion during the first

quarter of 2007, which projects to US\$4 billion annually. However, these numbers include legitimate PPC activities as well as brandjacking. The dirty little secret among domainers is that PPC targeting of major brands is incredibly lucrative. Leaders in the domainer community openly boast that the registration of trademarks and typo-squats is a “brilliant business model.” Domainers have developed domain name valuation models based upon the PPC revenue generated that include a ‘risk’ discount for infringing trademarks that are actively enforced. Thus, MarkMonitor conservatively estimates that 25% or US\$1 billion of domain-based PPC activity is attributable to brandjacking, as well as 25% of the secondary market sales of US\$70 million, or US\$17.5 million.

## Legal resources available

For domain-related abuse involving generic top-level domains (gTLDs), such as .com, and .net, the primary legal resource available is the Uniform Dispute Resolution Policy (UDRP).<sup>2</sup> The UDRP is a mandatory arbitration proceeding applicable to each gTLD registrant arising from the registration agreement entered with its registrar. The UDRP applies to any gTLD registrant, regardless of location, and is considered a relatively cost-effective solution when compared to traditional

litigation. UDRP filing fees range from US\$1 500 to US\$5 000.

Under the UDRP, a complainant must prove that: (1) a registered domain name is identical or confusingly similar to a trademark or service mark for which the complainant has rights, (2) the registrant has no legitimate interests in the domain name, and (3) the domain name was registered and used in bad faith.

According to the World Intellectual Property Organisation (WIPO), a record 2 156 UDRP complaints were filed in 2007, representing an 18% increase from 2006. The top three countries of UDRP complainants were the United States (45%), France (10%), and the United Kingdom (8%). The case outcomes are generally favourable to brand holders, with 85% resulting in the transfer of the domain name.

Most country code top-level domain disputes, such as .uk, and .de, adopt policies similar to the UDRP. For example, Nominet, the .uk registry, has adopted the Dispute Resolution Policy (DRS) applicable to .uk names, containing requirements similar to the UDRP. Specifically, the complainant must prove that it has rights in the name, and that the registration, in the hands of the registrant, is an abusive registration. The policy also includes a mediation process, to mediate the dispute before fees are paid to the independent panellist. Approximately 60% of DRS cases settle during mediation. The remainder is forwarded to an independent panellist with a filing fee of £750 plus vat.

Under the UDRP and the DRS, the remedy is limited to a transfer or deletion of the domain name. Companies seeking additional remedies, such as injunctions or monetary damages related to abusive domain registrations, instead rely on the laws of their respective countries. In the United States, the Anti-cybersquatting Consumer Protection Act provides brand holders with the ability to seek statutory damages of up to US\$100 000, as well as attorney’s fees and injunctive relief.<sup>3</sup>

Value of the global underground brandjacking economy	
Type of Abuse	Globally, in US\$
Phishing	US\$3 266 500 000
Domain PPC	US\$1 000 000 000
Secondary Domain Market	US\$17 500 000
Online Counterfeits	US\$137 000 000 000
<b>Total</b>	<b>US\$141 284 000 000</b>

**Table 1: Value of the global underground brandjacking economy.**

In the United Kingdom, companies look to the Trademarks Act of 1994 to obtain relief for domain-name-related infringement.<sup>4</sup> In addition, the courts have recognised that using trademarks as domain names can constitute an illegal passing off. Passing off is a common law tort that benefits trademark holders and is applied when a party misrepresents its goods to be that of another company or otherwise associated with another party. Damages, injunctive relief, and attorneys' fees are generally recoverable in the UK for trademark infringement.

**“Enforcement measures are readily available to companies seeking to enforce their intellectual property rights against brandjackers”**

## How easy are punitive measures to enforce?

These enforcement measures are readily available to companies seeking to enforce their intellectual property rights against brandjackers. The problem is not the lack of legislation, but the lack of resources to deal with the volume of abuse. Multinational corporations do not have the resources necessary to initiate enforcement actions or UDRP proceedings against the thousands of incidents harming their brands.

Today, many companies adopt a pragmatic approach towards fighting online brand abuse. Working with brand protection specialists, companies tackle the brandjacking problem through a three-pronged approach:

- Defensive domain name registrations to register obvious variations and typos of major brands
- Monitoring the internet for instances of abuse in new domain registrations and on web site content such as auction sites
- The systematic sending of cease and desist, and take down notices by e-mail to abusers, ISPs, and auction houses hosting infringing content.

Utilising an automated case management system to calendar, send, and track the results of these email notifications, companies can be successful in dealing with online abuse through an in-house program staffed by paralegals instead of turning to costly outside counsel.

Financial institutions targeted by phishing and other forms of online fraud need to take a more aggressive approach to protect their customers from identity theft. Because law enforcement agencies do not have the time or resources necessary to investigate and prosecute phishers, companies have the burden of fighting phishing independent of any government assistance. Anti-phishing solution providers have filled this void, operating around the clock to offer detection and administrative services designed to take down phishing sites hosted throughout the world as quickly as possible, sometimes in only a few hours.

Unfortunately, the financial incentives associated with brandjacking will encourage abusers to develop more innovative and insidious schemes for the internet. By adopting a comprehensive online brand management program designed to detect and monitor these new schemes, companies should be

well-positioned to respond in a meaningful way to these new threats on their famous brands.

## About the author

*Margie Milam is the corporate secretary and general counsel of MarkMonitor. Margie supervises all legal aspects related to MarkMonitor's business, including its intellectual property, corporate acquisitions, and strategic initiatives. An expert on licensing, internet and domain name issues, Margie is a frequent speaker at ICANN and other industry conferences. Previously a partner with the global law firm of Pillsbury Winthrop Shaw Pittman, she practiced in the areas of intellectual property, corporate securities, mergers and acquisitions.*

## References

1. MarkMonitor. “MarkMonitor Brandjacking Index”. brandchannel.com. April 2007. 3 September 2008 [http://www.brandchannel.com/images/papers/329\\_brandjacking-report-april-2007.pdf](http://www.brandchannel.com/images/papers/329_brandjacking-report-april-2007.pdf)
2. ICANN. “Uniform Domain Name Dispute Resolution Policy”. Internet Corporation for Assigned Names and Numbers (ICANN). 3 September 2008 <<http://www.icann.org/en/udrp/udrp-policy-24oct99.htm>>.
3. “REPORT TO CONGRESS: The Anticybersquatting Consumer Protection Act of 1999, section 3006 concerning the abusive registration of domain names.” United States Patent and Trademark Office. 3 September 2008 <<http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf>>.
4. “Trade Marks Act 1994”. UK Intellectual Property Office. 3 September 2008 <<http://www.ipo.gov.uk/tmact94.pdf>>.



## A SUBSCRIPTION INCLUDES:

- 12 printed issues
- Online access for 5 users
- A three-year archive of back issues
- Free delivery

[www.computerfraudandsecurity.com](http://www.computerfraudandsecurity.com)

# Are we being 'greenwashed' to the detriment of our organisations' security?

Mathieu Gorge, CEO, VigiTrust

**When we think about green IT, a number of topics come to mind: hardware equipment recycling, computer paper recycling, business phone recycling, power, and cost-effective data centres. We even include environmentally friendly home-based staff or teleworkers who save the planet by not travelling to work every day.**

However, the definition of green IT is not universal and while intelligence available from the public domain is growing, the vastness of subject matter under the heading of green IT gives rise to concerns about how genuine green IT organisations are. Moreover, since getting greener often means virtualising, recycling equipment which may contain sensitive data, or even re-organising data centres' physical and logical infrastructures, green IT does raise a number of concerns from a security perspective.

In order to discuss these concerns we should first attempt to define in more detail what green IT is and what solutions the market offers for getting greener. This will show us what security threats may need to be mitigated when engaging in a green IT strategy and what constitutes green IT security best practices for organisations that are already engaged in or about to engage in a 'get greener' exercise.

## Trying to define what green IT encompasses – what market intelligence is telling us

Research into the links between green computing equipment, greener use of IT resources, and the concept of green IT, reveals a number of trends that have emerged in the last few years. There appears to be more intelligence in terms of industry

and government reports about green IT, but there is still some confusion as to what it means and how it can be applied.

To start with, green IT – also referred to as green computing – can roughly be defined as the process by which organisations procure, use, maintain, and dispose of computing equipment in an environmentally friendly framework.

***“There appears to be more intelligence in terms of industry and government reports about green IT, but there is still some confusion as to what it means and how it can be applied”***

The last decade and especially the last three years, have seen a huge increase in the take up of green IT. A simple Google search for 'green IT' shows results including information on green strategies from giants such as HP and Microsoft, listings of organisations offering green computer equipment recycling, as well as a myriad of consulting firms offering green IT strategic advice. One common trend is the clear link between green IT and virtualisation technology which will be discussed further in this paper.

Another trend is that IT teams are being blamed for not using cost-effective and environmentally friendly solutions,

and CxOs are being blamed for not complying with corporate social responsibility (CSR) mandates.

Governments have started not only to regulate around green IT but also to enforce regulations. In the US, the Environment Protection Agency ([www.epa.gov](http://www.epa.gov)) regularly produces figures showing the impact of non-green computing on the environment, stating that 1.5 % of total US power consumption comes from data centres and that, at this rate, it will increase to between 2.5% and 5% in next five years.<sup>1</sup> The EPA also covers all the various acts and bills that are enacted in the US and covers recycling laws, not just related to IT.

In the EU, the Waste Electrical and Electronic Equipment (WEEE) directive – the European Community directive 2002/96/EC on waste electrical and electronic equipment – together with the RoHS Directive 2002/95/EC became European Law in February 2003.<sup>2, 3</sup> The WEEE directive sets targets for collection, recycling, and recovery for all types of electrical goods and it is being promoted by each of the EU states who take their own green IT initiatives to promote green IT awareness. An example is the promotion of the “Code of Good Practise for EEE Retailers” by WEEE Ireland.<sup>4</sup>

## Are there figures available to demonstrate the need for and impact of green IT?

Concerns about green IT and its links to security and IT management are mentioned in a survey from Techtarget, published in

July 2008, which was aimed at discovering how green IT aware their readers were. The survey asked questions such as “How many pages per year does the average worker print?” followed by “What percentage of office documents are thrown out within a day?” and “Within a week?” The answers were respectively 10 000 pages a year, 50% of printouts thrown away within a day, and up to 75% within a week.

The survey also looked at issues such as using virtualisation as a way to get green and determined that only 36% of US data centres had engaged in a virtualisation process. It also stated that while 60% of organisations in Asia Pacific and Japan, and 55% of European countries were reported to have green policies, only more than one third of their US counterparts did. The report did not confirm in detail what green policies were.

During 2007, Gartner, McKinsey and Forrester all produced separate reports on green IT, respectively entitled *Green IT: The New Industry Shock Wave*, *Reducing US Greenhouse Gas Emissions: How Much at What Cost*, and *Green Progress in Enterprise IT*.<sup>5,6,7</sup> An impressive number of sessions on 24 January 2008 at the Davos (Swiss-based) World Economic Forum were dedicated to environmental issues, including green IT. As part of this initiative, CxOs from leading organisations including Microsoft, Dell, Cisco and Intel started to explore ways in which they might be able to co-ordinate their efforts towards green IT.

A number of company announcements followed, stating that green IT strategies are being put in place. The most significant public press release was made by Hewlett-Packard which announced it had already overachieved on its goals for recycling e-waste and that it would improve again in the next two fiscal years.

## The drivers behind green IT & green IT policies: Have you ever been greenwashed?

It would seem that software and hardware vendors are riding the green IT wave.

Some detractors argue that this is a marketing stunt; that vendors do not worry about the environment, but rather try to lure the market into buying what are labelled ‘green solutions’. This is debatable, especially given that there is no worldwide benchmark on how to measure green IT initiatives rolled out by vendors. However, public requests for tender do include certain criteria for green IT strategies deployed by tendering organisations. These organisations are now asked to detail how their proposed solution lines up with legal and industry frameworks in terms of environmental waste, recycling, and even power consumption. Consequently, main vendors have had to outline their plans for helping the planet. They do so by promoting plans to build more power-efficient hardware solutions, use recyclable material, or develop virtualisation-friendly software to name but a few examples.

Businesses are also urged to set up green IT strategies from an end-user perspective. These range from initiatives to comply with the likes of WEEE or the EPA, to including tele-commuting roll-out plans, to video-conferencing solutions that cut down on the amount of travel done by employees. Comprehensive green IT strategies cover much more, including disposal and recycling policies for equipment as well as clear links to corporate security policies, which will be discussed further in this document.

Cost reduction is often cited as a driver for green strategies. We have established that green IT can be linked to financial aspects of the organisation’s infrastructure at the procurement stage (e.g. as a criterion for tenders). It can also be linked to total cost of ownership (TCO) of equipment which covers not only the initial capital expenditure and the cost of implementing and maintaining the solution, but also running costs such as power and costs of disposing of the equipment in a green way – hence the link with green IT.

The cost of powering the IT infrastructure we rely on should also be considered. Traditionally power costs have been calculated by adding the costs of running desktop

and laptop computing and associated equipment. Now, the running costs of server equipment running mission-critical applications (in other words applications which were in an active state) should be added.

***“Whether green IT is a goal or a sub-objective, organisations need to understand the wider technical, financial, social, and security challenges associated with it and look at what solutions the market has to offer”***

Still further elements need to be taken into account. Globally, businesses as well as governments are reaching the point where data proliferation and data duplication are leading them toward a new era in which storage solutions host terabytes or even petabytes of data. This means that solutions hosting such data need to be robust and fully redundant. In this instance, it is not uncommon for the initial cost of storage equipment to be higher than the cost of active mission-critical applications. Considering that data storage is very rarely optimised and that most storage solutions are under-utilised or used the wrong way (i.e. for storing obsolete or duplicated data), it is easy to see why environmentalists question the effectiveness of business green IT strategies. Storage solutions may end up using more power than active mission-critical solutions, which makes storage capacity planning also key to green IT.

Additional green IT issues include all those linked to recycling and the custody chain within the recycling process. There is indeed very little merit in using IT recycling providers who boast green strategies but who end up using sub-suppliers who do not. An example would be a US-based corporation that outsources recycling to another US-based business, providing it with all the relevant documentation on how it has disposed of the equipment, only for that equipment to end up being sent to a sub-contractor in a developing country where green laws either do not exist or are not enforced.

Whether green IT is a goal or a sub-objective, organisations need to understand the wider technical, financial, social, and security challenges associated with it and look at what solutions the market has to offer.

## Security considerations of green IT and how to mitigate threats

On a positive note, IT vendors are now offering technical solutions which consume less power, allow virtualisation of applications, and foster collaborative communication channels; thus reducing travel and related side effects on the environment. Although this adds value on the one hand, green IT may also have side effects of its own regarding the security of the organisation's infrastructure and data.

The industry might be asking businesses to rush into virtualisation, which may end up being detrimental to security altogether. Virtualising can help reduce the number of physical machines required to run applications but there are distinct documented risks if virtualising is done in an unsecured way. Before virtualising, organisations should fully understand what applications they have and which are mission critical. Virtualisation allows multiple applications to reside on separate software – to be virtualised and co-located on the same physical server with logical partitions. One obvious downside for security is that if a physical machine hosting four solutions instead of one goes down, then four potentially mission-critical solutions are out of service. There is a business continuity issue as well as a disaster recovery consideration.

Furthermore, a virtualisation project should also include de-duplication of data, otherwise the storage implications of the virtualised solution will not help the environment since the same amount of storage for live and backed up information will still be required. Organisations should re-examine their data classification and retention policy as part of a virtualisation project.

In the end, virtualisation software is not inherently more secure than

standard software. In fact, if configured badly, virtualised solutions may leave applications more open to attacks. For instance, if a physical server that is hosting multiple applications instead of one is stolen, the impact of the theft will be greater.

***“As your organisation increasingly relies on the data centre to host sensitive data within a virtualised infrastructure, the data centre is in a position to provide appropriate security controls and reporting mechanisms”***

It is also important to consider the effect of restructuring hardware infrastructures since it may impact on the overall physical and logical security of the organisation. When data centres are consolidated, the physical space available in racks to host virtualised applications that are currently hosted on single servers within the corporate environment into the data centre must be considered. It is necessary to establish if there will be enough space and how the space will impact the security of the data during the virtualisation process; while the data is in transit either logically through file transfer (which is not recommended in any case) or physically, as new hardware hosting the virtualised application is being transferred to the data centre. Organisations should investigate tools that can be used in energy efficiency planning.

Increased security at the data centre also needs to be taken into account as next-generation data centres become a high potential physical and logical attack area for the virtualised organisation. If you embark on such a project, it may be a good time to perform a security audit on your data centre. You would need to ensure that as your organisation increasingly relies on the data centre to host sensitive data within a virtualised infrastructure, the data centre is in a position to provide appropriate security controls and reporting mechanisms.

Traffic between virtualised applications should be restricted and controlled. Security audits of virtualised environments show, however, that this is not always the case. As with any software environment, the OS as well as the applications must be secured for access, management, and logging. You should also secure the hypervisor, which is the software that allocates the physical hardware and logical resources such as CPU, memory, and partitioning between the virtualised applications. Depending on the software solution used to virtualise applications, the hypervisor size may range from a few hundred KB to a few GB, thus making its attack surface more vulnerable. This is a major risk since it has control of and access to the virtualised applications.

It is also important to understand the virtualisation architecture of the chosen virtualisation software. Things to watch out for are separation between the kernel and user mode; global partitioning as well as application partitioning; access rights; and virtualised application process management. Finally, the virtualised solution should be configured with a security policy that will incorporate alert mechanisms for security non-compliance, focusing not only on external attacks but also on cross-application traffic behaviour to monitor for unusual activity.

Another key element of green IT strategies is to push for teleworking solutions that allow staff to work on the go, or from home, thus reducing the carbon footprint on our planet. The merits of such initiatives are rarely questioned as they make perfect sense and are measurable. However, organisations should remain vigilant and follow best practices during teleworking. Communication between remote workers and the back office must be done over secure channels using VPNs or SSL connections, whether it is initiated from a mobile phone, internet kiosk, or laptop. Remote hardware must be encrypted and access to such equipment must be provided using strong authentication mechanisms. At a policy level, workers must be trained to secure their mobile environment

and how to behave when using corporate IT resources and data outside the corporate environment.

One big mistake organisations can make is to forget to cover the social behaviour of staff outside corporate environments. Most organisations will cover AV, spyware, and firewalling technologies and the most advanced will also cover remote backup and remote wipe technologies for lost or stolen equipment. Few, however, include lost/stolen items procedures and thorough interviews of staff whose equipment goes missing. Some do not even account for mobile IT equipment. As an integral part of the green IT strategy, organisations should not only roll out technical solutions that protect mobile resources and data hosted on these devices but should also implement strong security policies and procedures. In addition, they should give awareness training on how to securely use corporate resources outside the corporate environment.

Security consideration should also be given to the printing and document capture environment. While a lot of care is taken to reduce the use of toners, cartridges and paper in order to reduce cost; very little care is given to the security aspects of the printing environment, especially where multi-function devices are concerned. Such devices enable organisations to rationalise their printing fleet and increase the ratio of users per machine, thus reducing the overall number of devices in use, incidentals costs, and paper and ink usage. They also allow users not only to print and copy (paper to paper) but also to scan documents to e-mail or FTP and fax. This functionality makes it possible for organisations to control who can print and ensure users authenticate at the device before they do so (typically through the use of third party authentication solutions). In this way, the printer can save paper and become a tool towards a greener environment.

***“Power consumption, paper consumption, non-recyclable hardware coupled with poor recycling policies, and non-optimised power-hungry storage solutions are all proof of that”***

When deploying such devices, however, organisations should be aware that these devices may become a backdoor in terms of security, as this environment tends not to be controlled for usage. A policy governing acceptable usage of multi-function device functionality should be promoted to ensure that access and reporting security controls are put in place, which in turn ensures that users are not abusing the printing and document capture environment. At an IT level, these devices must be thought of as servers. Most of the newer generation multi-function devices have an embedded web server and a hard drive. They can be addressed via an IP address and are therefore subject to DOS and hacking attacks similar to those of servers. Therefore, in the same way as servers used in virtualisation solutions are, multi-function devices must be part of the security policy and incorporated within the network in a secure fashion. The European Network and Information Security Agency (ENISA), published a white paper on secure printing which sets out how to address threats posed by multi-function and document capture devices.<sup>8</sup> Following these guidelines can help your organisation not only get greener but also more secure.

## Summary and final thoughts

Governments and industry alike agree that we all play a role in keeping our planet a healthy and enjoyable place to live in, and most of us will recognise the impact of IT on the environment. Power consumption, paper consumption, non-recyclable hardware coupled with poor recycling policies, and non-optimised power-hungry storage solutions are all proof of that. The idea of green IT is noble in itself and is begin-

ning to be pushed by major vendors and monitored by governments. However, it is primarily driven by cost-reduction objectives and does not necessarily incorporate secure answers to the challenges it is trying to address. Green IT incorporates new solutions such as virtualisation, teleworking, rationalised printing environments, and next-generation data centres, all of which come with their own sets of implementation and security challenges.

The key to a successful green IT roll out seems to be to go back to basics. Green IT best practice should definitely include a mix of policies and procedures, technical solutions, and raising of awareness within the organisation. Know your environment through regular assessments, in order to identify and ensure where and how your organisation can get greener. Then decide how to engage in data classification projects, virtualisation solutions, and secure printing deployment by following best practice security. This will enable your organisation to deliver a greener strategy for the use of corporate resources and will help increase the overall security levels of your environment. Green IT aspects should be incorporated in the security strategy and the security strategy should facilitate the implementation of green IT initiatives moving forward.

## Resources

Waste Electrical and Electronic Equipment Directive page, Wikipedia, accessed Sept 2008. <[http://en.wikipedia.org/wiki/Waste\\_Electrical\\_and\\_Electronic\\_Equipment\\_Directive](http://en.wikipedia.org/wiki/Waste_Electrical_and_Electronic_Equipment_Directive)>  
Green IT Corporate Strategies, BusinessWeek, February 11 2008. <[http://www.businessweek.com/innovate/content/feb2008/id20080211\\_204672.htm](http://www.businessweek.com/innovate/content/feb2008/id20080211_204672.htm)>

## References

1. Laws, Regulations, Guidance and Dockets. US Environmental Protection Agency. 17 July 2008 <<http://www.epa.gov/lawsregs/>>
2. Directive 2002/96/EC of the European Parliament and of the Council

- of 27 January 2003 on waste electrical and electronic equipment (WEEE). Official Journal of the European Union, 13.2.2003, L 37/24. 16 July 08 <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:037:0024:0038:EN:PDF>>.
3. Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment. Official Journal of the European Union, 13.2.2003, L 37/19. 16 July 08 <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:037:0019:0023:EN:PDF>>.
  4. Code of Good Practise for EEE Retailers. WEEE Ireland. 17 July 2008 <<http://www.weeeireland.ie/retailers-codeOfPractice.htm>>.
  5. Simon Mingay, Green IT: The New Industry Shock Wave, Gartner, December 2007.
  6. Reducing US Greenhouse Gas Emissions: How Much at What Cost, McKinsey, accessed Sept 2008. <[http://www.mckinsey.com/client\\_service/ccsi/greenhousegas.asp](http://www.mckinsey.com/client_service/ccsi/greenhousegas.asp)>
  7. Christopher Mines, Green Progress in Enterprise IT, Forrester Research, December 2007.
  8. "Secure Printing". The European Network and Security Agency. April 2008 <[www.enisa.europa.eu/doc/pdf/ENISA\\_secure\\_printing.pdf](http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf)>.

# War & Peace in Cyberspace: Internal fraud – when system administrators leave

Dario Forte, CFE, CISM, founder and CEO of DFLabs and Richard Power, author and journalist

It is true that we live in a strange world, but the recurrence of some security incidents borders on the incredible. Naturally, employees who are fired from their jobs tend to be unhappy. But a recent survey of 300 Australian IT administrators found that a whopping majority would go so far as to steal company data if they were fired.<sup>1</sup> According to the survey, 88% of IT administrators said openly that they would take company secrets with them on departure.



## Okay, but what data?

There are two categories of people who would be able to engage in this kind of behaviour: so-called 'power users', whose job descriptions grant them access to confidential data, and people with advanced skills who are able to escalate privileges. While the latter are usually blocked or intercepted before any malfeasance, the former are pretty difficult to recognise, especially during the short period before the event.

According to the survey, the target information includes CEO passwords, the CEO mailbox, the customer database, R&D plans, financial reports, M&A plans and so forth. The survey also revealed that perhaps the most important target would be the company's list of privileged passwords. This

treasure chest would be of interest to over a third of the interviewees.

One of us recently spoke at Eurosec France, one of Europe's most important information security events, and gave a practical example of how such things could happen. A southern European company had fallen victim to internal fraud. Several sales people had been discovered (by chance) padding out their expense reports with the help of a system administrator. The monthly damage was about €28 000 and the employees were fired. An inspection of the administrator's PC revealed several top management documents in its memory.

Unfortunately, a lack of forensic soundness in the investigation methodology, specifically in how data were preserved, meant that the evidence may not have been accepted in court and the company

could have risked a lawsuit. This situation demonstrates the extensive risks a company faces if the controllers are not controlled. We will touch on this again later in this article.

Part of the information we have been discussing comes from Cyber-Ark, an identity management firm, which released these findings in its annual review titled, *Trust, Security & Passwords*. Udi Mokady, CEO of Cyber-Ark, stated, "Most company directors are blissfully unaware of the administrative or privileged passwords that their IT guys have access to and which allow them to see everything that is going on within the company. These privileged identities, which lie on hundreds of servers and applications, very rarely get changed as it's often considered too much hassle."

## Not just disgruntled employees

There are several sides to the problem and many associated issues. Let's imagine, for example, that segregation of duty has been implemented and supported by technological countermeasures. Unfortunately, the survey also demonstrated that, regardless of measures to prevent disgruntled former system administrators and employees in general from causing damage, it appears that some system administrators still display insecure behaviour.

The survey found that more than a third of respondents admitted to writing down passwords on Post-It notes and leaving them stuck to computer monitors. As if that wasn't enough, they also sent confidential or classified information via unencrypted email.

IT administrators are often guardians of sensitive information storage and their actions are not monitored at all. At least 30% of the administrators interviewed for the survey admitted to snooping around the network, looking for confidential data such as employee salaries, and prying into personal emails. In addition, many IT administrators are also careless when making online purchases, with 12% of them admitting to having sent cash through the mail.

***"The survey found that more than a third of respondents admitted to writing down passwords on Post-It notes and leaving them stuck to computer monitors"***

### So what?

So these IT administrators look like doctors who don't listen to their own advice. Let's analyse the problems. We think that at least the following points should be evaluated.

Is segregation of duties applied in your company? It is important to separate some system administration duties, for example, the ability to control entire portions of the network. The side effects are also important. Many companies use the iden-

tity management paradigm to implement duty segregation. The complexity of such a project is great, however, and it increases in proportion to the size of the organisation. It is a big mistake to believe that identity management can be fully implemented merely by obtaining a product and some consulting services from a vendor. To be successful, a project should also bring in a certain amount of third party and independent work.

If the company accepts the risk, is it ready to investigate both proactively and reactively? Although crucial, this question has been left unanswered in 90% of the cases we have investigated. A company should be prepared for a digital investigation. This means that forensic readiness should be implemented before a potential event has a chance to occur.

As we write, the benchmark requires the tracking of all actions performed by administrators plus policies and procedures for forensic examination. Tracking (we are basically speaking about log management) is usually managed by the security people, who work under the segregation-of-duties paradigm themselves. It is also important to track all actions performed during an investigation or incident response task. The taxonomy of the management process laid out in the literature covers two points: follow-up and trace-back. In this context, follow-up refers to the actions taken in response to the initial notification of an incident or an investigation, whether reported by an automated process (e.g., an alarm) or by a user. Follow-up generally addresses both the process line and the originator. The requirement for completeness of information is pertinent in both cases, a requisite that cannot be achieved without proper operation tracing. It is thus clear that the solutions currently available (very few) are also oriented in this direction. In both incident management and digital forensics this need is satisfied via the generation of an automatic timeline of incident-related events and

the possibility of adding events manually. This should allow supervisors and higher management levels to check and review at any time any operation that has been performed. Those who are familiar with and have had practical experience of this field know how important it is to keep accurate track of everything. While this is always possible in theory, if it is not done correctly it is very difficult to trace a set of tasks after three years (the average recall period following, for example, the intervention of judicial authorities).

***"Whatever else is done, further secure information custody measures should be put in place to prevent or limit unauthorised information access"***

Is the human resources (HR) department really involved in those processes? Cases such as the southern European company mentioned above and portions of the complex Société Générale case happened because of a lack of coordination inside of the HR department. According to the *New York Times*, preliminary investigations revealed that Kerviel (the man who has been charged for the fraud), worked almost five years in the risk management department before working at the trading desk, and was thus familiar with all the control mechanisms (including the ones related to the Eliot system) that are supposed to work at closing time. This is further evidence that a security process should be in place, not only when a person leaves the company, but also when he or she is moved internally to another department.

Is sensitive information hidden in a digital vault? Whatever else is done, further secure information custody measures should be put in place to prevent or limit unauthorised information access. 'Digital vault' refers to cryptography applied to the protection of files and folders. This should be done *a priori*. The good news is that current technologies are able to interact with the identity management solutions we mentioned above.

1.	Is segregation of duties applied in your company? Many companies use the identity management paradigm to implement duty segregation. The complexity of such a project is great, however, and it increases in proportion to the size of the organisation.
2.	If the company accepts the risk, is it ready to investigate both proactively and reactively? A company should be prepared for a digital investigation. This means that forensic readiness should be implemented before a potential event has a chance to occur.
3.	Is the human resources department really involved in those processes? A security process should be in place, not only when a person leaves the company but also when he or she is moved internally to another department. The human resources department should be involved in this process.
4.	Is sensitive information hidden in a digital vault? Whatever else is done, further secure information custody measures should be in place to prevent or limit unauthorised information access.

Table 1: Four priority questions to ask information security management and company directors.

## Conclusions

At the moment, high-level managers are concentrating on preventing litigation risks associated with employee discharge decisions. This means that they are concentrating – rightly or wrongly – on legal matters and paying little attention to information security. Many high-level managers prefer to prevent or promptly correct any unlawful behavior by supervisors or co-workers. However, we are reaching a point where information technology workers are becoming dangerous gatekeepers. Control, tracking, prevention, and security are factors that must be kept under consideration. If not, non-compliance will be automatic.

## About the authors

**Dario Forte**, CFE, CISM, Is adj faculty at University of Milano at Crema, where he teaches incident management. Former police detective and founder of DFLabs, Forte has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the World Bank, RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the US Department of Defense Cybercrime Conference, and the US Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las

Vegas in 2003. Forte has published over 100 papers worldwide, working for editors such as: Elsevier, Wiley, AP. He provides security consulting, incident response and forensics services to several government, law enforcement agencies and private companies worldwide. [www.dflabs.com](http://www.dflabs.com)

**Richard Power** is an internationally recognised author and journalist, and a trusted adviser to the executive leadership of government, industry, academia and the humanitarian community. He champions a bold approach to the unprecedented challenges of the 21st century, based on the principle that security, sustainability and spirit are interdependent issues. Richard provides insightful analysis and practical recommendations on travel security, crisis management, business continuity, awareness and education, cyber security and counterintelligence, and assists organisations in implementing such programs. Power has delivered executive briefings and led professional training in over thirty countries. He has also published five books.

## References

1. Cyber-Ark. "Security Survey Reveals Exiting Employees Have The Power." Press release. August 27, 2008. 16 September 2008 < [http://www.cyberark.com/news-events/pr\\_20080827.asp](http://www.cyberark.com/news-events/pr_20080827.asp)>.

# Calendar

## 27–31 October 2008 15th ACM Conference on Computer and Communications Security

Location: Alexandria, VA, USA  
Website: <http://www.sigsac.org/ccs/CCS2008/>

## 31 October 2008 Second Computer Security Architecture Workshop

Location: Fairfax, VA, USA  
Website: <http://www.rites.uic.edu/csaw/>

## 13 November 2008 The Payments Card & E-payment Solutions Conference 2008

Location: Old Trafford, Manchester, UK  
Website: <http://www.purchasingcardnews.co.uk/conference/>

## 15–21 November 2008 CSI Annual Conference

Location: Washington, DC, USA  
Website: <http://www.csiannual.com>

## 18–20 November 2008 TrustCom 2008

Location: Zhang Jia Jie, Hunan, China  
Website: <http://trust.csu.edu.cn/conference/trustcom2008/>

## 25–27 November 2008 International Workshop on Security

Location: Kagawa, Japan  
Website: <http://www.iwsec.org/>

## 1–9 December 2008 SANS London

Location: London, UK  
Website: <http://www.sans.org>