



# computer FRAUD & SECURITY

ISSN 1361-3723 October 2008

www.computerfraudandsecurity.com

## 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?

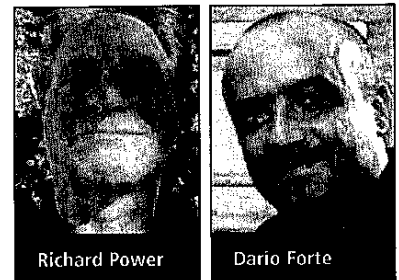
There are two categories of people who would be able to engage in this kind of behaviour: so-called 'power users', whose job descriptions grant them access to confidential data, and people with advanced skills who are able to escalate privileges. While the latter are usually blocked or intercepted before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



Richard Power

Dario Forte

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 unsecure 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>