

Fraud Intelligence

For the prevention, detection and control of fraud in all its guises

Under the mattress – the safest place for your digital secrets?

As we move increasingly towards an intangible world of 1s and 0s stored on data servers in the Cloud or virtualised across continents, have we liberated or lost control of the data most critical to our businesses and lives? Vijay Rathour of Stroz Friedberg ponders.

Who can you trust?

The chances are that if you log into an office network from home or abroad, you probably use an RSA token, generating an endless string of meaningless numbers, to help secure your login. RSA's SecureID token technology is used by an estimated 100 million people, in the form of hardware and software code generators, and many of us use this fairly innocuous technology to help secure our work and property online. The recent news that RSA's SecureID technology had been compromised by outside hackers using a form of highly sophisticated, but increasingly common, advanced persistent threat, led many to question just how secure any form of digital security is if one of its flag-bearers can fall.

It has become almost regular reading to learn that another brand-name website has been hacked and compromised, spewing unfathomable quantities of sensitive information into the hands of wrongdoers. The number and sophistication of these attacks is growing. While the goal for many hackers, targeting relatively low-hanging fruit like retailers' websites, may be financial information such as credit card numbers, a more focused group of intruders has learnt to identify the value of the intellectual capital that businesses and individuals hold dear. The even loftier goal of elite cyber-criminals, often with a state-sponsored backer, appears to be to tear through the fragile fabric of trust that underpins security in our online world.

With the power to issue themselves digital certificates that assure Internet users of the authenticity of the website they are browsing, digital terrorists have gained the power to bless fake phishing websites with the credentials of their more wholesome doppelgangers. The motivation here does not appear to

be mere financial gain, but for the hackers to gain an insight into our digital lives in a way they almost never could in the physical world. Email addresses, bank details, intimate or illegitimate relationships, trade secrets, legal documents, social security numbers and every other bit and byte of digital miscellany that we let loose into the online sphere comes up for grabs.

Layers and lies

The Secure Sockets Layer (SSL) is an almost ubiquitous encryption protocol built into most modern browsers to help them establish a relatively secure communication channel between a web server and browser. The industry standard protocol, typically signified by a padlock icon in the browser, is used to provide relative security to millions of transactions every day, and relies on the underlying web server, which may be a bank, Facebook, or your office email server, being issued with a SSL certificate to authenticate its credentials to its users.

Very few bodies are able to issue SSL certificates and they are rightly prized for the confidence they lend to sensitive online communications. However, fraudsters have continued to demonstrate their ingenuity by penetrating the security of one of these issuing bodies and issuing illegitimate certificates to themselves, permitting them to pose as Google, Microsoft, Skype and others. Although it is suspected that these attacks emanated from Iran, unravelling the intentions and origins of such hacks, as with the Google and Adobe hacks from 2010, will typically require the assistance of seasoned experts.

Coffee cup hijacks

"Session hijacking" is a form of hacking which, whilst in common use for some time in the darker reaches of the Internet, has only fairly recently become known as a risk to the mobile activities of the general public. The longstanding vulnerability was recently leveraged in a proof-of-concept tool called "Firesheep", giving the nefarious user the ability to easily and

immediately masquerade as a legitimate user of Facebook, Amazon, Twitter or many other websites. With a simple click the hacker can inherit the credentials and passwords of legitimate users sharing the same Wi-Fi network, going on to make purchases, steal credit cards numbers and intercept passwords, all while carrying the online appearance and liability of the unsuspecting “sheep”.

Many of the sites at risk to this vulnerability quickly advised users to switch to SSL encrypted pages, where they were available, to prevent such exploits. Unfortunately, most popular social networks and websites are still scrambling to make SSL encrypted communications the default means of access, and as demonstrated by the SSL certificate hacks, security in a digital age is only as strong as its weakest link.

The Californian State Bar has recently issued an opinion recognising the risks of legal professionals using potentially insecure technologies and networks, such as their local coffee shop Internet connection. The opinion requires the user to weigh up the risks to their clients, the degree of sensitivity of the information they are accessing and the legal ramifications of it being intercepted, amongst others, when using such technologies. As states and governments scramble to regulate and legislate the technologies of yesterday, there will always be a lacuna in what is permissible and what is possible. Managing these technological risks requires more than computing skills, it calls for the ability to examine the digital fingerprints left behind and the human nature of those who covet and control your information.

The human factor

Social networks have proven to be a boon for many businesses, and the ability to stay in touch with those you work and deal with can help to increase knowledge about your market and improve your brand awareness. However, while companies have had to deal with espionage, insider trading and a multitude of internal threats for generations, a disgruntled Generation Z employee can do more damage in a single 140 character outburst than a succession of philandering and extorting executives might have managed.

Online technologies continue to move forward at a feverish pace, and while Twitter passes its fifth birthday the majority of businesses and brands remain unconscious of the risks such social networking technologies might pose to their reputation. Most are

equally unprepared to control or deal with the 100+ million tweets per day pouring out of every pore of business, divulging uncensored, sensitive, secret and scandalous information every second of the day. Every employee and individual is a possible point of weakness, and the failure of a single unwitting or complicit accomplice can lead to the destruction of your defences from the inside. As companies increasingly choose to host their data abroad, or in virtual environments scattered across continents, the potential attack surface grows and risks become almost impossible to manage.

Monitoring employees' use of communication systems in the workplace can be a divisive issue, although most would agree that an expectation of privacy might be reasonable for legitimately personal and private communications. The difficult area beyond, where an employee might be using work computers to post commercial secrets to a personal email account, or the world at large, brings both technological and legal issues into play.

Justifying the reasons and level of monitoring of potentially private communications requires careful legal and practical considerations. As an employer can easily be accused of unlawful monitoring, leading to potential criminal liability under various laws and regulations, it is always prudent to seek expert advice prior to taking such steps. A detailed “Electronic Communications” policy is normally required to ensure compliance with the *Regulation of Investigatory Powers Act 2000* (RIPA), the *Data Protection Act 1998* (DPA) and the *Telecommunication Regulations 2000*, among other relevant legislation. However, many firms have failed to supplement this with a specific “Social Media” policy, extending the employer's rights and employee requirements in the use of the new generation of communication platforms.

Informed consent

Social media networks provide new opportunities to steal sensitive, costly and private information from employers and other employees. In most instances, putting digital cats back in the bag is nearly impossible in an age of ubiquitous search engines and Internet archives. Technical measures can be put into place to filter various forms of communication, although again, ensuring that this is not an illegal form of communication interception requires expert guidance. Employment policies should ensure that legitimate use of these forms of media is professional, legal, appropriate and in compliance with other employment responsibilities owed by the employee.

To the greatest technical and legal extent possible, employers should ensure that employees give free and informed consent to appropriate monitoring of their activities.

The underlying technical simplicity of most social networks belies the complex human interactions that typically take place on them. The use of sophisticated technical tools to discern psychological and emotional themes in online postings can help to predict and isolate instances of cyber-bullying, irresponsible or inappropriate content and potentially illegal activities.

Those intent on stealing valuable intellectual property, or causing reputational damage through potentially libellous or illegal postings online, will often ignore the policies in place to prevent this. A marriage of technological and legal safety nets can

permit an employer to put in place appropriate information access controls and rights to limit the scope of these attack vectors and to trace back the digital breadcrumbs to help identify the source of potential leaks.

Keeping digital secrets safe is not an easy task, but leveraging expert advice and technology can help ensure that you enjoy the benefits of the modern age without becoming another hacker headline.

Vijay Rathour (+44 (0) 20 7448 0481, vrathour@strozfriedberg.co.uk) is a solicitor and vice president of Stroz Friedberg (www.strozfriedberg.com) in the UK. The company specialises in digital forensics, data breach and cybercrime response, electronic disclosure, and business intelligence and investigations. Working at the crossroads of technology, law and behavioural science, the company provides technical assistance and strategic advice to help manage the inherent risks and responsibilities of doing business in a digital era.

Editor: Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • Email: timon.molloy@informa.com

Editorial board: John Baker – Director, Risk Management – Fraud Solutions, RSM Tenon • Neill Blundell – Head of Fraud Group, Eversheds • Andrew Durant – Senior Managing Director, FTI Forensic Accounting • Chris Osborne – Director, Dispute Analysis and Forensics, Alvarez & Marsal

Production Editor: Frida Fischer • Tel: 020 7017 5501 • Email: frida.fischer@informa.com

Marketing: Naeemah Khan • Tel: +44 (0) 20 3377 3847 • Email: naeemah.khan@informa.com

Sales: Nicola Helfet • Tel: +44 (0) 20 3377 3123 • Email: nicola.helfet@informa.com

Renewals: Helen James • Tel: +44 (0) 20 7017 5268 • Email: helen.james@informa.com

Subscription orders and back issues: Please contact us on 020 7017 5540 or fax 020 7017 4614.

For further information on other finance titles produced by Informa Law & Finance, please phone 020 7017 5540.

Printed by: Premier Print Group • This newsletter is printed on paper sourced from sustainable forests.

ISSN 0953-9239 © 2011 Informa UK Ltd

Published 6 times a year by Informa Professional, Telephone House, 69–77 Paul Street, London EC2A 4LQ. Tel 020 7017 4600. Fax 020 7017 4601. www.informa.com

Copyright While we want you to make the best use of *Fraud Intelligence*, we also need to protect our copyright. We would remind you that copying is illegal.

However, please contact us directly should you have any special requirements.

While all reasonable care has been taken in the preparation of this publication, no liability is accepted by the publishers nor by any of the authors of the contents of the publication, for any loss or damage caused to any person relying on any statement or omission in the publication. All rights reserved; no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electrical, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.

Informa UK Ltd, Registered Office: Mortimer House, 37/41 Mortimer Street, London, W1T 3JH.

Registered in England and Wales No 1072954.

informa
law
an informa business