

info security

A Breach Too Far?

What Ashley Madison says about security and privacy in 2015



PLUS:

WINDOWS 10 SECURITY /// START-UPS & FUNDING /// INSIDER THREATS



ADMIN ACCESS SECURED

RÂMNICU VÂLCEA, ROMANIA 04-23-2015 2AM



HE WILL GET IN.

YOUR FATE WILL BE DETERMINED BY YOUR SPEED OF DETECTION AND RESPONSE.

That's where we come in. LogRhythm's next-generation security intelligence platform identifies high-impact threats and neutralizes them before they can result in a material breach. It uniquely unifies SIEM and log management with network and endpoint forensics and advanced security analytics to provide comprehensive threat life cycle management and the ideal foundation for today's cyber security operations.

IMPROVE YOUR SECURITY INTELLIGENCE POSTURE AT LOGRHYTHM.COM/SIMM

 **LogRhythm**[®]
The Security Intelligence Company



Contents

October/November/December 2015

COVER FEATURE

24 **Hacking the Cheaters**

Phil Muncaster examines what the Ashley Madison incident says about security and privacy in 2015

FEATURES

12 **When Outsiders Become Insiders**

Abuse of privileged access to systems is a growing cyber-threat, Stephen Pritchard discovers



16 **Security's Ever-Growing, Ever-Moving Target**

As mobile becomes the norm, Joe O'Halloran asks how security is keeping up

20 **Penetrating the IT Dark Cloud**

Cloud apps are the revolution, but they pose security risks, say Aditya K Sood and Michael Rinehart



28 **Laying Down The Law**

Mike Hine speaks to leading privacy lawyer, Eduardo Ustaran, about the EU's General Data Protection Regulation

32 **More than Virtually Secure**

Virtualization has taken hold in the enterprise, and it can also enhance security, discovers Max Cooter

38 **Place Your Bets on Security Firms**

It's a golden age for investing in security companies. Joe O'Halloran asks how long the good times are set to roll

OPINIONS

22 **Awareness of GDPR is not Enough - Action is Needed**

How organizations can prepare for the EU General Data Protection Regulation

27 **Shining a Light on Shadow IT**

The journey from cloud skeptic to cloud enabler

31 **Security and ROI**

How security can be a business enabler, driving progress and return on investment

35 The Case for Better Threat Measurement

The security industry needs better intelligence, not more alarming statistics, writes Ian Trump

42 Cybersecurity Skills Crisis: A View from Academia

Professor Keith Martin examines if universities are doing their bit

CASE STUDY

36 Checking the NHS's Security Pulse

Infosecurity takes the security temperature at Sussex Health Informatics Service

REGULARS

6 Editorial

Joe O'Halloran reflects on a summer of security woes

8 News Feature

Microsoft launched Windows 10 this summer. Does it stack up as the most secure version of the OS? Davey Winder investigates



48 Book Review

Mike Hine turns the pages of *Obfuscation: A User's Guide for Privacy and Protest*

49 Slack Space

A round-up of tech's weirdest tales

50 Parting Shots

Recruitment and employee education are on Mike Hine's radar this issue

INFOSECURITY

EDITOR & PUBLISHER

Joseph O'Halloran
joseph.ohalloran@reedexpo.co.uk
+44 (0)208 4395648

DEPUTY EDITOR

Mike Hine
michael.hine@reedexpo.co.uk
+44 (0)208 4395643

ONLINE UK NEWS EDITOR

Phil Muncaster
phil@muncaster@gmail.com

ONLINE US NEWS EDITOR

Tara Seals
sealtara@gmail.com

PROOFREADER

Clanci Miller
clanci@nexusalliance.biz

CONTRIBUTING EDITOR

Stephen Pritchard
infosecurity@stephenpritchard.com

ONLINE ADVERTISING:

James Ingram
james.ingram@reedexpo.co.uk
+44 (0)20 89107029

PRINT ADVERTISING:

Melissa Winters
melissa@showtimemedia.com
+44 (0)1462 420009

Rosalia Lazzara

rosalia@showtimemedia.com
+44 (0)1462 420009

MARKETING MANAGER

Rebecca Harper
Rebecca.harper@reedexpo.co.uk
Tel: +44 (0)208 9107861

DIGITAL MARKETING CO-ORDINATOR

Karina Gomez
karina.gomez@reedexpo.co.uk
Tel: +44 (0)20 84395463

PRODUCTION SUPPORT MANAGER

Andy Milsom

ADVISORY EDITORIAL BOARD

John Colley: Managing director, (ISC)² EMEA

Marco Cremonini: Università degli Studi di Milano

Roger Halbheer: Chief security advisor, Microsoft

Hugh Penri-Williams: Owner, Glaniad 1865 EURL

Raj Samani: CTO, McAfee EMEA, chief innovation officer, Cloud Security Alliance

Howard Schmidt: Former White House Cybersecurity Coordinator

Sarb Sembhi: Past-president, ISACA London, editor of Virtually Informed

W. Hord Tipton: Executive director, (ISC)² Patricia Titus

ISSN 1754-4548

Copyright

Materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites are protected by copyright law. Copyright ©2015 Reed Exhibitions Limited. All rights reserved.

No part of the materials available in Reed Exhibitions Limited's *Infosecurity* magazine or websites may be copied, photocopied, reproduced, translated, reduced to any electronic medium or machine-readable form or stored in a retrieval system or transmitted in any form or by any means, in whole or in part, without the prior written consent of Reed Exhibitions Limited. Any reproduction in any form without the permission of Reed Exhibitions Limited is prohibited. Distribution for commercial purposes is prohibited.

Written requests for reprint or other permission should be mailed or faxed to:

Permissions Coordinator
Legal Administration
Reed Exhibitions Limited
Gateway House
28 The Quadrant
Richmond
TW9 1DN
Fax: +44 (0)20 8334 0548
Phone: +44 (0)20 8910 7972

Please do not phone or fax the above numbers with any queries other than those relating to copyright. If you have any questions not relating to copyright please telephone: +44 (0)20 8271 2130.

Disclaimer of warranties and limitation of liability

Reed Exhibitions Limited uses reasonable care in publishing materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites. However, Reed Exhibitions Limited does not guarantee their accuracy or completeness. Materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites are provided "as is" with no warranty, express or implied, and all such warranties are hereby disclaimed. The opinions expressed by authors in Reed Exhibitions Limited's *Infosecurity* magazine and websites do not necessarily reflect those of the Editor, the Editorial Board or the Publisher. Reed Exhibitions Limited's *Infosecurity* magazine websites may contain links to other external sites. Reed Exhibitions Limited is not responsible for and has no control over the

content of such sites. Reed Exhibitions Limited assumes no liability for any loss, damage or expense from errors or omissions in the materials or from any use or operation of any materials, products, instructions or ideas contained in the materials available in Reed Exhibitions Limited's *Infosecurity* magazine and websites, whether arising in contract, tort or otherwise. Inclusion in Reed Exhibitions Limited's *Infosecurity* magazine and websites of advertising materials 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.

Copyright © 2015 Reed Exhibitions Limited. All rights reserved

Ensure Secure Sharing & Protect your Revenue Streams

Locklizard's document security software prevents unauthorized document sharing and piracy. It controls access to and use of your information both inside and outside your organization, so you can securely, and cost effectively, distribute and manage your digital content.



1 Stop Unauthorized Access

Documents are locked to specific users and their devices and will not work if users distribute them to others. You can also enforce the location from where they can be used (e.g. office only).



2 Control Document Usage

Decide whether authorized users can print your documents and if so how many times. Stop screen grabbing, and change access controls even after distribution.



3 Expire & Revoke Documents

Set documents to automatically expire after a given no. of views, prints, days, or on a fixed date. Instantly revoke access to documents at any stage no matter where they reside.



4 Log Document Activity

See when users open and print your documents. Apply dynamic watermarks displaying user information to viewed and/or printed information to discourage sharing of printed copies.

Locklizard document security software is used worldwide by information publishers either selling content or ensuring compliance, corporates protecting trade secrets, or providing a controlled method to share their information, and government agencies concerned over potential misuse of their information.

So what do companies use **Locklizard** for?



Protection from piracy & revenue loss

The drivers that made us go to DRM for our electronic courses

NetMasterClass develops on-line training courses which cost thousands to produce. Two days after one course was released they found it offered for sale on e-bay. That blew away the costs of development and sales going forwards in one single hit. They had to take positive steps to protect their IPR in order to stay in business.

“The return on investment to our company has been immediately evident. We are now creating new products for our electronic portfolio without fear of seeing them being distributed through unauthorized channels.”



Cost and time savings

A greener and more cost effective means of document distribution

For 25 years TSD policy was to send out paper based manuals for its product lines to new customers. Manuals could take 7-10 business days from ordering to reach the customer, and could be copied and distributed outside of their control. They needed a solution so customers received instant gratification upon purchase and achieve a 'greener' result.

“Using Safeguard Enterprise PDF security has meant the elimination of many man hours, printing resources and postage. We currently estimate that costs have been cut by over 50%.”



Secure sharing & Trade secret protection

Preventing information leakage

CCS Companies needed to protect commercial proprietary documents which they have to share with clients but also keep secret. They often have to provide specific individuals with temporary copies of confidential documents for their review. It is essential that they are able to do this without them being copied or forwarded to unauthorized users.

“Proprietary documents are not misplaced, and cannot be forwarded to the wrong individuals. You cannot place a value on that.”

Start protecting your IPR now. Call us on 800 707 4492 (US) or +44 (0) 1292 430290 (UK & Europe) or visit www.locklizard.com to arrange a free 15 day evaluation and/or an online demo.



Locklizard



Ode to Autumn in Security

The season of mists and mellow fruitfulness approaches and with it comes this latest issue of *Infosecurity*. But what you'll find in this issue is not quite an ode to autumn in the style of Keats, but rather a nod to events over the summer that outline and hint at the shape of the industry to come.

For starters, we have a look at the security implications of Windows 10. Whatever you think about Microsoft and its products, it's a rare company indeed that doesn't either have a Windows product installed or deal with suppliers or partners which do. Quite simply this is an industry standard and Windows 10 is something that all businesses need to be aware of from a security perspective. The many security issues regarding the past versions of Windows are legion and frankly too drawn out to mention in full here.

One would think that, given the almost daily cycle of hits on businesses, the fundamental problems of access to admin rights and user data would be addressed in this new version. Some would argue not. The same dissenting voices also cast doubt upon the new version and its visualization capabilities, especially with regards to how they can improve security. Microsoft would clearly take issue – we present the pros and cons.

One of the other great issues of the summer surrounds privacy. First of all we'll look at the EU's General Data Protection Regulation which could finally be passed within a few months, after being in the works for half a decade. This is not just some impenetrable, prosaic, obscure piece of Euro law: the GDPR should at last clarify the terms that security and data privacy professionals have been anticipating for so long, and help the industry ascertain just

how far-reaching and radical its implications will be.

On a more personal note regarding privacy, we have Ashley Madison. (Stop sniggering now...) But jokes aside, losing 37 million personal records is something that should send shivers down the spine of anyone charged with protecting personal information in any business. What are the lessons, technological not moral, to be learned from the breach? Is it really a tipping point in how we treat digital privacy and the security of information shared with online service providers? Just consider the business ramifications of that. Can the quality of service and experience standards that other forms of business adhere to ever be applied strictly or feasibly to online services?

As we say in our feature: just as a car manufacturer can't afford to sell a vehicle with faulty brakes, a site dealing with super sensitive information cannot afford to have subpar privacy.

It begs the question: should we all work, and live our lives, under the assumption that if you can connect something to a network, it can be hacked? That seemed to be the leitmotif of this year's Black Hat event.

In between the incongruity of Las Vegas itself and the alarming demonstrations of real-time hacking of automotive computer systems – not for the faint-hearted – there was a genuine fatalism that hacks were just going to happen, as much as you'd eventually

lose a hand of cards in one of Sin City's many places to do so. And it's increasingly likely that the breach will be through mobile.

Let's just remind ourselves of recent events in mobile security. In August, Google announced that it felt compelled to beef up its patching and general mobile security by means of what it called the single largest unified software update the world has ever seen, pushing mass updates over the air to Nexus Android devices to address the Stagefright vulnerability. Rest assured, Google is under no illusion that security issues are going to diminish. Then only weeks later, security researchers discovered malicious apps on Apple's official App



Losing 37 million personal records should send shivers down the spine of anyone charged with protecting personal information



Store in China after developers of several well-known titles accidentally downloaded and used an infected version of a popular app-building tool. We'll give a lowdown on mobile security as well.

But coming back to the central point of if you can connect, you can be hacked, there comes the eternal balancing act between control and access. The harsh truth is that accessibility is a business fundamental. That genie is out of the bottle – now what do you do? We hope we can give you some answers in this issue.



Joe O'Halloran, Editor

Are Your Files Protected From The Cloud?



GoAnywhere™ is a **managed file transfer** solution that tightens data security, improves workflow efficiency, and increases administrative control across diverse platforms and various databases, with support for all popular protocols (SFTP, FTPS, HTTP/S, AS2, etc.) and encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption.

Visit GoAnywhere.com for a free trial.



**GO
ANYWHERE™**

GoAnywhere.com 800.949.4696

→ a managed file transfer solution by



**SAVES US A LOT OF
TIME AND HEADACHE**



Matt Booher
WIS:DOM Information Systems

*"It's helpful every single day
as the lifeline for communications
with our customers."*

Matt Booher
President
WIS:DOM Information Systems



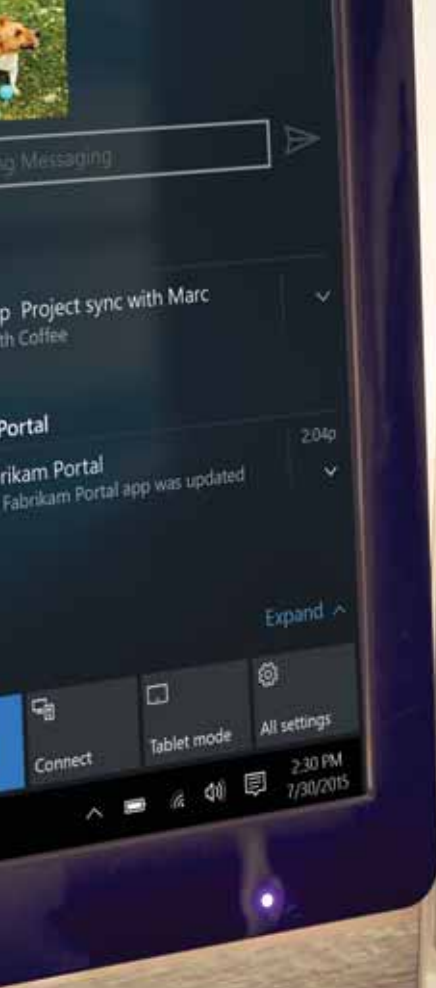


Cleaning

Windows



Microsoft launched Windows 10 this summer with great fanfare, providing the upgrade as a downloadable freebie to Windows 7 and 8 users. But does W10 stack up as the most secure version of the venerable OS? And what about the enterprise? **Davey Winder** investigates



Microsoft claims that Windows 10 is the 'most secure Windows ever' but that should be a given. Why would it develop, or anyone upgrade to, an equally or less secure operating system than Windows 7 or 8? The devil is always in the detail, and when it comes to security that detail can be hidden in the shadows. Insecurity can be introduced simply by the act of migration; security can be weakened through changes to patching strategy or an over-reliance on out-of-the-box defaults. So just how secure is Windows 10?

Enterprise Impact

The main concerns that need to be addressed are the security implications for enterprises that adopt Windows 10. While it goes without saying that any rollout of a new, or upgraded, operating system isn't going to be risk-free, that's not to say Windows 10 won't bring impactful changes to the organization from a security perspective; but maybe you should ask yourself how secure is secure enough.

That may sound overly simplistic, but Windows 8, for all the problems it may have had, is generally considered to be much more secure than previous versions. And

given that ransomware actors had Windows 10 exploit code within a week of launch (not to mention malicious code being able to exploit backwards compatibility of the platform) is Windows 10 actually secure enough to make a difference? Will it make life harder for hackers?

"Cybercrime is big business and evolves at such a rapid rate to combat detection and prevention solutions that I doubt Windows 10 will cause hackers to break stride," James Maude, senior security engineer at Avecto, told *Infosecurity*. "Many of the fundamental problems of access to admin rights and access to user data have not really been addressed in Windows 10," he warns, adding that "malware often follows Occam's Razor, whereby the simplest solution is usually the best, and there are plenty of simple ways to access or encrypt data already built into Windows."

Microsoft hasn't been getting a smooth ride when it comes to the security functionality of Windows 10, at least from within the IT security pro community; many of the bumps have been external to the product itself. Take the end of Patch Tuesday, replaced with a rolling security update system. Continuous patching is great on paper, a much more secure way of doing things, until you consider whether it will break tried and trusted testing and deployment cycles, and by so doing introduce risk.

Guillaume Ross, senior security consultant with Rapid7, thinks that businesses should "evaluate each new feature of Windows 10, and see if the risk introduced by these features warrants the deactivation of that feature in the enterprise."

One example is the 'frictionless' approach to multi-device use adopted by Microsoft with Windows 10, and the privacy implications that come attached. Cortana can be disabled, if the collection of data such as contacts list, location info and searches is a concern.

"While the amount of data sent by Windows 10 might be significant," Ross says, "similar concerns exist on most platforms, especially as vendors try to make things like

searching and context-aware notifications more convenient for end-users, requiring more data access."

So What's New?

When it comes to security, Windows 10 brings with it some interesting new features. Jason Fossen, principal security consultant at Enclave Consulting and author

of the SANS Institute's *Securing Windows* course, points in the direction of a couple of things.

Fundamental problems of access to admin rights and user data have not really been addressed in Windows 10

James Maude
Avecto

Firstly there's what Fossen refers to as the most exciting security change in Windows 10: Virtual Secure Mode (VSM) for password hashes and other secrets in the enterprise edition of the OS. Virtualization-based security relies on various hardware features such as Second Level Address Translation (SLAT) and an input/output memory management unit (IOMMU) to help create a separate secure space in memory called 'Isolated User Mode.'

"Think of it as a tiny, hidden virtual machine into which secrets like encryption keys and password hashes can be squirreled away," Fossen says, continuing, "even if hackers have completely taken over the running Windows kernel, they should not be able to steal the secrets."

Well, that's the intention at least, and as the feature relies on security provided by hardware, it shouldn't matter if the

What's New at a Glance?

- **Azure Rights Management** – Taking data protection into the cloud
- **Device Guard** – Prevents unrecognized applications from running
- **Edge Browser** – Runs in app controller sandbox, limits extension support
- **Virtual Secure Mode** – Encrypted container credential protection
- **Windows Hello** – Biometric authentication using facial scans
- **Windows Passport** – Two-factor authentication using biometric equipped kit
- **Windows Update for Business** – Continuous rolling patches





Windows OS software is compromised, Fossen insists: "If Microsoft has done a good job of implementing it then virtualization-based security could finally provide a good defense against attacks like pass-the-hash, security token theft, and so-called Golden Kerberos Tickets."

So, has Microsoft done a good job? I guess we'll find out once the bad guys have had a chance to reverse engineer the source code.

The second security feature that Fossen flags is Windows Hello, a biometric login using facial recognition. This essentially builds a 3D map of your face using infrared, but is limited to those who have access to a 3D infrared scanner such as the Intel RealSense camera. Scott Rundle, a senior support consultant at Riverbank IT, isn't convinced on this last update: "Biometric logins aren't a new technology as such and have been around in laptops in the guise of thumb-print scanning since the days of Windows XP. The main reason they've never truly taken off is their poor reliability and buggy implementations." Whether Windows 10 changes all that (you guessed it) remains to be seen.

Maude is a fan of the Device Guard feature, aimed at blocking zero-day attacks by vetting applications accessing the machine and its attached network, in principle at least. However, he warns that it poses a number of challenges for the enterprise.

"At a hardware level Device Guard requires support for Unified Extensible Firmware Interface (UEFI), secure boot and a Trusted Platform Module

Picture credit: Stanislaw Mikulski / Shutterstock.com



(TPM)," he explains, "but these are not always widespread in an enterprise." Indeed, from a management perspective, application control is often considered an impossible task and in this case has to be administered via PowerShell, requiring a reboot to apply policy changes.

Then there's the end-user experience which, Maude warns, is "pretty inflexible because applications are either on or off, and will rely heavily on the ability of IT to audit and approve new applications being introduced into the environment."

Of course, even if the feature is deployed it can offer no defense against macros and JIT-based apps such as Java which will run unhindered as the parent application will likely be whitelisted anyway. Maude is also wary of the immediate security benefit of Windows Hello and Windows Passport as 'password killer' features. While he agrees everyone "wants a way to

make sure passwords are stronger and using two-factor authentications is a great step forward," Maude points out that "adoption of specific biometric sensors being built into hardware by OEM partners could take some time and slow the roll-out."

Another security upgrade, the introduction of Information Rights Management (IRM) with Azure Rights Management, is undoubtedly a step in the right direction towards securing data beyond the often under-utilized device encryption offered by

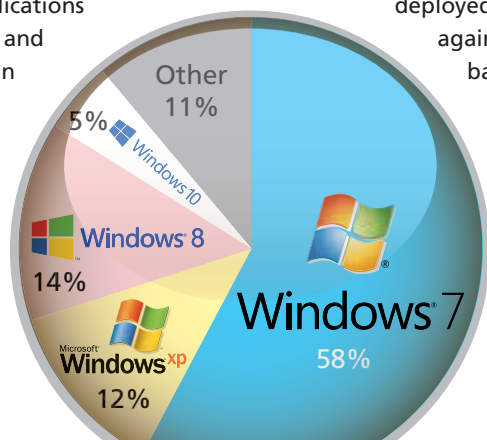
BitLocker. Once again though, Maude warns that, although potentially beneficial, "this does require a degree of configuration and management to work, so it will take time for the benefits to appear in the enterprise."

Good on Paper

Good on paper kind of sums up Windows 10, but is it really the most secure Windows ever? Ian Trump, security lead at LogicNow, thinks that claim is something of a moot point, arguing whatever Windows OS you run will do little to prevent exploitation when typically the first thing users and administrators do with a new OS is to disregard two key security features: User Account Control (UAC) is frequently turned off by administrators and local administrative rights are not removed.

"Also, analysis of exploit kit malware indicates a great deal more attacks are conducted against third-party applications, including Microsoft Office," Trump reminds us, continuing, "so again the 'most secure operating system ever' can quickly become just as vulnerable as any other operating system, almost through no fault of its own."

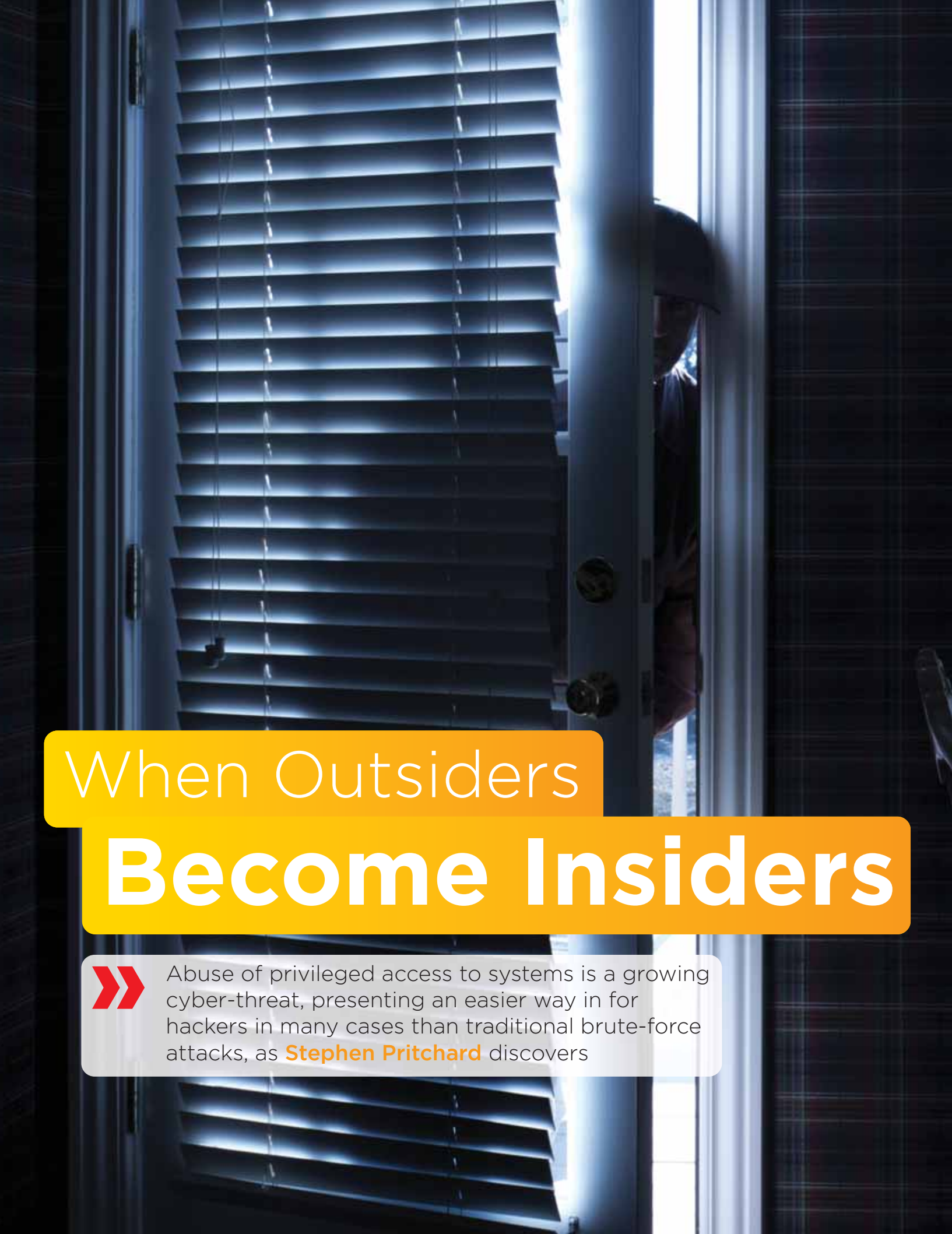
We'll leave the final word to Maude who agrees that the infosec community often rushes to poke holes in new things, advising that the smart money will "wait and see what state Windows 10 is in six months from now before considering a deployment."



Operating Systems Global Market Share

Source: Netmarketshare.com; data for 1 August to 3 September 2015



A person is seen from the chest up, peering through a window with closed horizontal blinds. The person's face is partially visible through the narrow gap between the blinds. The scene is dimly lit, with light coming from the window, creating a sense of secrecy and intrusion.

When Outsiders

Become Insiders



Abuse of privileged access to systems is a growing cyber-threat, presenting an easier way in for hackers in many cases than traditional brute-force attacks, as **Stephen Pritchard** discovers

As CIOs strengthen their organizations' perimeters, hackers will almost inevitably look for other ways in. And, like water dripping through a leaking roof, hackers and cyber-criminals always find the cracks.

One crack is the insider; another, the tools insiders use to manage their networks.

As brute-force technology attacks become harder to carry off, malicious groups are looking for people who can be bribed, cajoled, threatened or duped into letting them through the organization's defenses.

Once inside, hackers all too often find a trove of useful information: passwords stored insecurely, user accounts with unnecessarily high levels of access, or single passwords used on multiple systems.

Once the attacker gains access to these assets, the outsider effectively becomes an insider and, in too many organizations, they can disrupt systems and steal data almost at will.

The power of the insider attack lies in making the hacker look like a trusted user, staying below the radar of all but the most sophisticated security systems. It is this power that is forcing insider attacks higher up CISO, CIO and even board agendas.

Insiders on the Rise

Reliable statistics on insider attacks are hard to find, not least because companies often prefer not to report incidents. However, consulting firm KPMG found that insider attacks increased from 4% of

security incidents to 20% between 2007 and 2010. This largely coincides with improvements in companies' perimeter security controls.

The Ponemon Institute's *Annual Cost of Data Breach* report also ranks insider attacks, alongside criminal attacks, as the most costly form of breach.

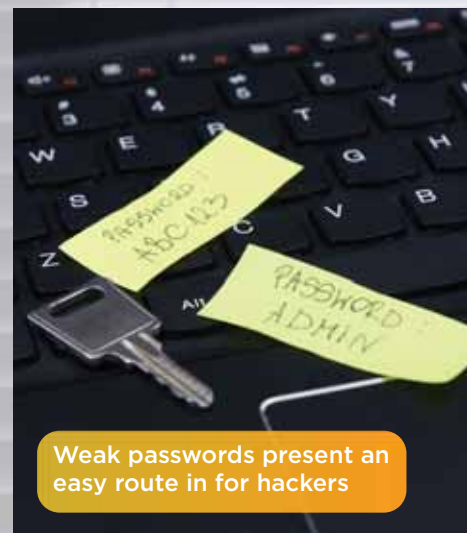
"Our experience shows a significant growth in blended attacks, where the outsider attacker takes advantage of insiders who can be manipulated or who have been careless. That is the greatest risk for organizations," says John Skipper, a cybersecurity expert at PA Consulting. "Deliberate malicious attacks are still rare, but very damaging."

Just how damaging is shown by some recent insider attacks, from Sony Pictures to Morgan Stanley. But hackers do not need a collaborator on the inside to wreak havoc or to steal data. The range of routes into an organization is broad, and not helped by weaknesses in businesses' security and IT administration controls.

"Insiders have been a soft target for a long time," says Adam Schoeman, senior intelligence analyst at security consultants SecureData.

He adds: "We've seen advanced attackers moving from external attacks on boundary devices and using tools available to trusted insiders. These are people who know what they are hitting. Advanced attackers say, 'I have access to this – what can I do with this access?'"

A lack of network monitoring by businesses also means that, once inside, attackers can go undetected for long periods of time.



Weak passwords present an easy route in for hackers

The causes of insider breaches, though, are hardly new. Most 'insider' incidents can be traced to employees who have left the organization, suggests Laurance Dine, managing principal in investigative response at Verizon's investigations unit: "People get disgruntled, you get misuse, people make mistakes."

"Then there is social engineering: duping people into giving out information that becomes the 'tip of the spear' for spear-phishing attacks, or people giving out their own credentials. Then there are incidents where people are threatened or coerced," he adds.

Notable Insider Incidents



South Carolina Department of Revenue
Data on 3.8m taxpayers lost following phishing attack

2012



Swiss Intelligence Service (NDB)
Employee downloaded sensitive files onto portable hard drives

2012

The right security systems, though, can pick up most attacks, Dine advises: "Have a good leavers' policy. It is quite common for accounts to still be active six months after someone leaves."

These 'hygiene factors' are increasingly important as hackers turn to insiders, and compromised privileged user accounts, rather than attempting to breach firewalls or other perimeter security systems.

Even relatively small weaknesses can leave a door open to attackers. At SecureData, Adam Schoeman warns that attackers have used OWA – Microsoft's webmail for corporations – to gain access to networks.

Hackers can then break into the organization and plant malware, use their access to attack other systems, or even to carry out social engineering attacks on other privileged users or key personnel, such as members of the board. "Once you are on the network, escalating privilege is not too difficult," Schoeman says.

This is not helped by poor security practices such as password sharing between users or systems, or keeping passwords unencrypted on the network in unprotected files.

"It is possible to take a primarily technological route and to hack in through the firewall and then capture credentials," says Skipper. "This is either because they're left in an insecure way, like passwords in Excel spreadsheets, or because of systems that are not properly configured and allow passwords to be captured."

Most organizations have now closed those gaps, he suggests, prompting users to turn to spear-phishing and other forms of social media manipulation to "take advantage of

unwitting behavior" and put a trojan or other malware onto the network.

But there is a further factor that works in the outsider's favor: organizations often rely too heavily on a single security measure or access control – again based on the

assumption that once someone is on the network, they are trusted.



Use the highest levels of security for things that really matter, such as two-factor authentication. Don't reuse admin passwords; don't share passwords

Laurence Dine
Verizon

"Insiders generally have too much access around a single control," says Phil Huggins, vice president of security science at security and risk consultancy Stroz Friedberg. "If the only thing that stops them breaching is a single control, even if that control is strong, that may not be enough."

Dine advises organizations to "use the highest levels of security for things that

really matter, such as two-factor authentication. Don't reuse admin passwords for each system; don't share passwords – we still see that a lot."

Keeping desktops and other IT systems up to date – including applying patches – is also vital; recent breaches such as Poodle rely largely on unpatched vulnerabilities to gain access.

But organizations also need to move away from the assumption that all users are trusted users, and plan for the chance that a trusted user might – unwittingly or deliberately – go rogue. This is likely to also mean more restrictions on who can access IT systems, when and where.

"Give access rights to people who need rights, give people access to what they need," says Dine. "If your security policy lets everyone down to reception have everything, you need to do that today."

When the Good Go Bad

For CISOs, this means moving beyond a purely technical approach to information security, to one that involves culture, policy and procedures, and even a measure of psychology.

Firstly, IT security teams need to be able to detect unusual or suspicious activity that might indicate an insider attack is taking place. But other parts of the organization, including legal and HR, need to develop techniques to spot changes in behavior and even pick up traits in employees that suggest they might turn to cybercrime.

By no means do all organizations have the real-time network monitoring tools which can detect unusual activity



Target
Network breached by using refrigeration vendors' credentials

2013



Edward Snowden
NSA contractor used his credentials to steal state secrets

2013



by employees or IT users, as well as attacks such as APTs. Nor do all organizations have data loss prevention (DLP) software, a tool which – though effective – experts say is expensive and can be difficult to deploy.

“Tracing what people are doing is more difficult [than detecting intrusions],” says Dine. “There are systems you can put in to monitor data usage – we recommend using those if you can afford to.”

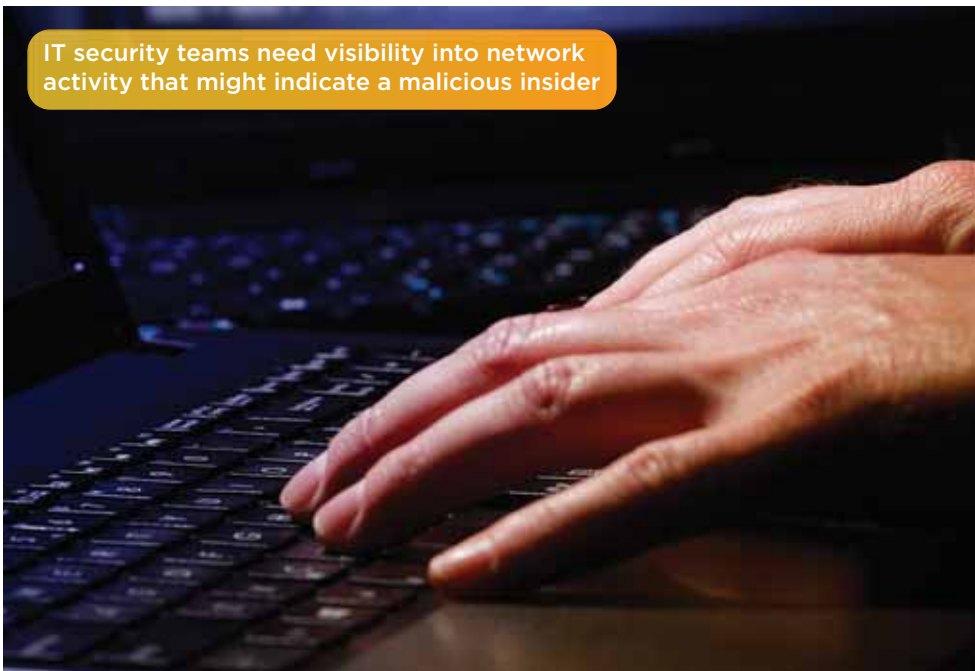
Huggins cautions that DLP is hard to deploy: “The idea that a computer understands what is a secret – and what is not – is laughable. What we are seeing is much more deployment of analytics – moving from setting off an alarm or something going red to pointing out individuals’ high risk activities.”

This, though, takes insider threat prevention squarely into the realm of the human factor. Often, the tell-tale signs are similar, whether someone’s behavior changes because they have been duped, threatened, or are looking for financial gain.

“Is someone downloading huge amounts of data, or changing their working hours, or undertaking activity out of sight of co-workers?” All these can be signs of an insider at work, he suggests.

Advanced organizations, including security agencies, are looking at behavioral analytics and psycho-linguistic analytics to pick up unusual patterns of activity. Whether all organizations can use these tools is open to question, however. Governments might be able to apply restrictive policies to computer use; a start-up may not.

IT security teams need visibility into network activity that might indicate a malicious insider



Companies also need to be aware of labor laws. In some countries, such as Germany, these place severe limits on employee monitoring. And businesses, says Schoeman, also need to lead from the top.

“The key thing is leadership behavior,” he says. “If the board can bypass access controls it devalues those controls for the rest of the business. You need a consistent policy.”

No policy, though, is foolproof. Edward Snowden – perhaps most high-profile insider of recent times – used legitimate access to NSA systems to download data. Organizations should bolster their protection against insiders by improving their incident response, so they are ready for when, not if, an insider breach occurs. As Schoeman points out,

organizations can “bank time” by having a well-prepared incident response plan.

This is likely to be increasingly important, as more hackers turn to the insider route to stealing information.

“Relatively few CIOs have their heads around this completely,” says Skipper. “They’re becoming aware that it’s a key area to think about.”

“The majority of CIOs we work with are reasonably confident in boundary security. But few can monitor what is going on in their networks. That’s where the focus is now. Most sophisticated organizations are making the assumption that some bad stuff will get in, and some already is in, and the ability to respond is at the top of the agenda.”



Sony Pictures Entertainment
Major breach of intellectual property and company data now attributed to hacking group including former employee

2014



Morgan Stanley
Customer data stolen; first blamed on an employee of the firm, but hacking is now also suspected

2015



Security's Ever-Growing, Ever-Moving Target



Portable platforms increasingly form the cornerstone of enterprises' long-term strategic aims to be more flexible and agile. But, asks **Joe O'Halloran**, as mobile becomes the norm, how is security developing to prevent more threat vectors from being introduced?



It would seem there is no airport, no train station, and no mode of transport that has not been used by mobile service providers to demonstrate the capabilities of their networks.

We've all seen the happy faces of sharp-suited mobile workers, head-down into their work wherever they are. Being agile. Being productive. Yet it's tempting to wonder how happy they would appear if they had an inkling of what they may be doing as regards security.

The Consequences of Corporate Flexibility

Mobile is a given for companies of all sizes. Moreover, a large number of enterprises worldwide have adopted the bring your own device (BYOD) trend to increase work productivity and reduce IT infrastructure costs. But there is a balancing act: the more flexibility and access anyone has to their corporate network, the more ways in which that network can be reached. The most secure network is one with no mobile access. It will also be the most unproductive.

Amrithesh Suman, an analyst with Allied Market Research, looked at how this circle is being squared: "Today, there is a growing acceptance for the use of mobile devices by employees at work. [Yet] as a consequence of the same, executives, managers and other corporate employees have to connect their mobile devices to corporate servers which involves a high data security risk of corporate data for the enterprises, thus increasing the need for data monitoring and security.

"In addition to enterprise users, individual users also demand cohesive, integrated mobile device protection and security solutions. Mobile security solution providers deliver security solutions for individual use that are able to restore and secure the data for any subsequent mobile device, regardless of the operating system."

The Mobile Threat Landscape

Here is the thing about mobile: demand is insatiable. The Apple iPhone 6s launch typified what the industry is all about. Faster processors, larger screens, enhanced access to richer applications. Such mobile platforms basically allow you to do more, much more, for your business. Sadly more should now really include security issues. Mobile malware is spiking, and is all too often pre-installed on a user's device.

In September 2015, researchers from security expert G DATA found that over 26 models from some well-known manufacturers including Huawei, Lenovo and Xiaomi have pre-installed spyware in the firmware. During the second quarter of 2015, researchers saw 6,100 new malware samples every day. By comparison, in the first quarter of 2015 they saw about 4,900 malware apps per day, representing an increase of almost 25% quarter over quarter.

Further, and maybe more alarmingly, the G DATA Q2 2015 *Mobile Malware Report* shows that there will be over two million new malware apps by the end of the year. Worse, the researchers suspect people are modifying the devices' software to steal user

data and inject their own advertising to earn money.

Says G DATA mobile solutions product manager Christian Geschkat: "Over the past year we have seen a significant increase in devices that are equipped with firmware-level spyware and malware out of the box which can take a wide range of unwanted and unknown actions including accessing the internet, read and send text messages, install apps, access contact lists, obtain location data and more – all which can do detrimental damage."

Considering the mobile threat environment, Check Point's global VP of products Gabi Reish suggests that the biggest risk to mobiles right now is large-scale vulnerabilities that affect mobile operating systems.

"Mobile device vendors are having to move so fast to add new features that innovation has raced ahead of security – when you develop quickly, some things get easily missed," he warns.

"The patch cycles for these flaws are slow, leaving millions of devices at risk – often without the users being aware... Check Point's 2015 *Security Report* found that in an organization with more than 2,000 devices on its network, there is a 50% chance that there will be at least six infected or targeted mobile devices on the network. That may not seem high, but in many cases the infections were sending traffic from mobile devices for weeks or months. What sensitive data could have been stealthily siphoned from just a single device during that time?"

New Platforms, New Threats

Mobile malware is very much a trend for 2015. Geschkat explains that “an estimated 2.5 billion people worldwide use a smartphone or tablet to go online. Chatting, surfing and shopping are possible anytime, anywhere thanks to smartphones and tablets. At the same time, the number of mobile malware apps has sharply increased in the past three years.”

The G DATA report also found that the first six months of 2015 has already broken all previous malware records – over a million new Android malware strains (1,000,938) were discovered within just six months. It’s fairly safe to say that the second half of 2015 will see more of the same and in a number of key places.

The G DATA security experts expect yet another significant increase in Android malware instances in particular. In those six months, the analysts have already discovered almost as many Android malware instances as in the whole of 2013. These include the recent Certifi-gate and StageFright flaws. Both affect hundreds of millions of Android devices, and the latter flaw makes all Android devices targets of remote take-over by simply receiving an MMS message, without even having to open or view it.

“Hacking Team, an IT company that develops a wide range of malware for intelligence services and governments, suffered a cyber-attack this year,” the report notes. “After this attack, corporate data and source code for an Android malware strain were published. G DATA security experts expect cyber-criminals to exploit this easily accessible knowledge base and publish large numbers of more mature Android malware.”

But before anyone thinks this is just an Android problem bear in mind that arch rival Apple has its own mobile security issues. August 2015 research from identity protection specialist Centrifry Corporation found that a lack of encryption and weak or shared passwords on Apple devices in the workplace were exposing sensitive corporate and customer information. It also found that businesses were simply not



Mobile device vendors are having to move so fast to add new features that innovation has raced ahead of security

Gabi Reish
Check Point

investing enough resources to secure or manage their devices with just over half (51%) of all products such as an iPhone or iPad secured by a password that is merely a single word or a series of numbers. Most devices (58%) did not have software installed to enforce strong passwords and only just over a third of Apple devices had encryption of stored data enforced by their company.

Flexible Solutions for Mobile Data

So how is the industry dealing with mobile security? By spending a lot of money it would seem. Allied Market Research calculates that the global mobile security market is estimated to reach \$34.9bn by 2020, growing at a CAGR of 40.8% during the forecast period 2014-2020. It added that enterprise end-user security solutions was the largest revenue generating end-user segment in the global market and accounted for \$2.86bn in 2013.

Allied Market Research’s Suman believes that there are a number of discernible trends emerging in the fields of mobile security, first among them authentication, mobile application management and mobile data protection. Drilling down he sees that two-factor authentication is the latest trend adopted by most of the service providers in their products, while he expects the mobile application management trend is likely to increase as more of such solutions are offered. Some of the prime reasons for the

development of application security solutions are the increasing dependency on applications and the frequency and length of usage.

The good news is that the mobile industries and device makers are making positive steps to improve mobile security. Even Android. In August 2015 Adrian Ludwig, head of Android Security at Google revealed just how much his company was pushing mass updates of patches over the air (OTA) to its Nexus Android devices, to address issues such as Stagefright.

For CheckPoint’s Reish, there was a basket of necessary solutions to remedy issues: “What’s needed to protect against these threats is a range of technologies including on-device sandboxing, static code analysis, mobile app reputation scoring, behavioral risk analysis and machine learning – ideally integrated with an organization’s existing MDM/EMM solution, and managed by a single dashboard for controlling supported devices and stopping mobile threats.”

Assessing the True Risk to Business

The mobile genie is completely out of the bottle and unless firms wish to hunker back into a bunker of limited access they will have to accept the fundamental risk of using mobile devices and services. But that is not to say that there are not ways in which such risks can be mitigated.

It’s not just a question of technology, but also a question of practice making, if not perfect, then increased protection. For example, under no circumstances should jail-broken devices be allowed to access the corporate network. Businesses should enforce rigorously standards and procedures for passwords and other forms of authentication.

And then there is the thorny issue of lost devices. Devices will get lost – that cannot be stopped. What can be stopped is lost devices automatically being a problem for the business. The technologies and services to do such things are readily available.

In fact, in this case, and in all others when it comes to mobile security, the answer is right in your hands.





WICK HILL

READ ALL ABOUT IT!!

The Wick Hill Guardian is a free publication available from Wick Hill in print or electronically. Aiming not to advertise, but to advise, the newspaper examines the key issues and concerns facing IT security professionals.

Featuring columns from some of the biggest names in IT security. You really don't want to miss out on your copy.

Get yours at www.wickhill.com/guardian



#becrypt



Penetrating the IT Dark Cloud



Cloud apps are revolutionizing enterprise IT, and their usage only continues to expand as businesses deploy them at a rapid pace. However, they also pose their own set of security risks. **Aditya K Sood** and **Michael Rinehart** of Elastic propose a solution

Cloud apps are becoming the preferred choice of enterprise IT because they offer universal access, reduced costs, and support a variety of apps, thereby enhancing business productivity. And as cloud apps become more accessible, powerful and flexible, employees will continue to adopt them, often without sanction, for their ability to enable collaboration with anyone, anywhere, and on any device.

However, as with all new technologies, cloud apps pose their own unique set of security risks, and IT professionals are rightly concerned that sensitive corporate data remains susceptible to malicious insiders, sophisticated attackers, and even naive users.

A significant problem facing enterprises is shadow IT: unauthorized apps and devices in-use but not sanctioned by IT. Shadow IT can significantly expand the attack surface of the enterprise. A potentially greater risk is shadow data: the unknown sensitive content that may be lurking in both sanctioned and unsanctioned apps. The inappropriate sharing or leakage of shadow data to unauthorized parties could have devastating consequences.

Shadow IT and shadow data create an increased attack surface and risk of data exfiltration, so we refer to them collectively as the 'dark cloud'.

The Rising Threat of the Dark Cloud

The main factor driving the rise of shadow IT is traditional IT's ineffectiveness in addressing different use models and vulnerabilities in newer cloud technologies. One extreme is the BYO (bring your own) culture whereby employees walk in with their own devices, networks, and tools. With such high variation, monitoring data transfer is a nearly impossible challenge, pushing data once secured within the enterprise network perimeter into the dark cloud.

New and unsanctioned cloud apps introduced by employees pose a serious risk to enterprise data from a security and compliance standpoint. For example, if a sensitive document (containing, say, credit card payment information) is shared through an unsanctioned cloud app, it creates a potential exposure, with possible legal ramifications. Having only a public folder, the unsanctioned apps may lack proper sharing controls or, worse, be indexable by search engines (via a publish option). If the public exposure is left unmanaged, it may be assumed that the document will be leaked and reside permanently outside the control of the enterprise.

The feathery edge of the dark cloud even makes its way into the realm of

sanctioned cloud apps and is a result of a lack of fine-grained visibility in the traditional security stack. For instance, consider a sanctioned file-sharing app that allows for public sharing. Next-generation firewalls can control access to specific apps on a device or user-by-user basis, and can provide insight into which apps a user accesses but not necessarily how they are using them.

Without fine-grained visibility into specific user actions, the only secure option to prevent public sharing is to block the app entirely, but the business value that cloud apps and services bring an organization increasingly precludes this option. This necessitates the development of new security technologies specifically designed for the cloud that are able to peer into specific user actions and set policies around them. Systems that can provide information about the data being accessed have the additional advantage of providing proactive protection against data exfiltration.

By comparison, traditional, on-premise software systems are either based around scanning traffic rooted in standards or signatures that are fixed or change slowly over time. Cloud apps, however, comprise a new class of systems capable of changing their traffic patterns, APIs, and feature sets



at frequent intervals – really, at the speed of software sprints.

Penetrating and Securing the Dark Cloud

Cloud Access Security Brokers (CASBs) are addressing the challenge of securing the dark cloud through a variety of technologies and services such as discovery of shadow IT, classification of sensitive content, granular policy enforcement, detection of suspicious account behavior and so on. The key to penetrating the dark cloud, though, is gaining visibility and control, and this is where specific CASB security technologies are critical.

Before you can detect threats related to any specific technology, it is imperative to first detect the existence of that technology in the environment. This holds true for shadow IT where cloud app discovery and risk assessment are essential to identify all of the sanctioned and unsanctioned apps running in the organization.

In the absence of such an assessment, organizations will simply remain in the dark with regard to the risks associated with these apps and their potential exposure. It is also critical to establish visibility and control points so that cloud apps can be monitored in the environment. Furthermore, you need to deploy security policies and next-

generation algorithms using data mining, machine learning, and natural language processing (NLP) techniques to detect and remediate data exposures when they occur.

The resultant next-generation security stack for cloud app security can identify malicious and anomalous behavior (analogous to what an IDS/IPS provides); detect undesirable content sharing (analogous to what a DLP solution provides); and apply behavior analytics and monitoring (analogous to what a network forensics tool provides).

Enterprise IT must educate employees to be aware of the potential dangers of the dark cloud and avoid the threats at the user level. In addition, policies such as a well-defined whitelist for sanctioned apps should be implemented to define the acceptable use policy for cloud apps.

Data should be secured via encryption while in motion or at rest as per requirements. Note, however, that encrypting data at rest might have unintended side effects of 'breaking' cloud apps and their integrations with other apps.

Finally, a mobile device management (MDM) solution should be adopted to implement strict control of the communication channels initiated through personal mobile devices. All the security measures discussed above provide a multi-

layered security approach to subvert the risks mounted by the dark cloud.

Comprehensive CASB solutions can provide all of these services in the cloud. Just as cloud apps have improved the productivity of business services with reduced IT maintenance effort, cloud-based security operations can arm infosec teams with the latest up-to-date security features with no additional maintenance on the part of the enterprise. It also provides an infrastructure solution to ever-changing enterprise cloud apps – as such cloud apps are updated, CASBs are able to adapt quickly and accordingly to maintain fine-grained visibility without any intervention.

Mitigating Risk

The dark cloud encompasses both IT-sanctioned and unsanctioned cloud apps and the data resident in them. With the rise of cloud technology, the dark cloud is gathering around cloud services and apps. There is no doubt that cloud apps are more prone to accidental or malicious leakage of business-critical data, and the risk becomes much higher when these cloud apps are unsanctioned.

Overall, a multi-dimensional security approach and new security stack for the cloud are needed to penetrate the dark cloud and mitigate the risks that it poses.



Awareness of GDPR is not Enough – Action is Needed



Tony Pepper, CEO of Egress Software Technologies, explains how organizations can prepare for the EU GDPR with the right balance of technology, process and education

As discussions over the EU General Data Protection Regulation (GDPR) rumble on, businesses risk complacency. As with any pan-European regulation, timescales are subject to bureaucratic negotiations, with legislators and politicians hammering out rules that will need to work effectively across 28 nations, risking the reform becoming 'old news' before it has even been passed.

Organizations could take the easy way out and do nothing until the changes are finalized (tentatively due early 2016) and then enforced two years later.

Yet preparation now will prevent organizations from later falling foul of stringent and far-reaching powers. Many of the fundamentals of the reform have already been agreed – and the savvy CIO and CISO will already be making changes both technologically and socially.

GDPR: What We Know So Far

The regulation calls for data protection 'by design and by default', meaning data controllers must take a positive approach to information security. Citizens will be at the heart of data protection with the right to know and the right to be forgotten. By granting widespread power to the people, the regulation will put organizations under scrutiny for their data collection and processing activities.

One factor that should focus minds at the highest level is the potential of fines levied for data breaches to amount to 2% of a company's annual worldwide turnover.

Improving Information Security

The first step in achieving GDPR compliance is to assess data protection risks by understanding how your organization processes and handles data. Without this knowledge, it will be impossible to implement effective policies and technologies. This internal review should canvass procedures at all levels, examining daily processes as they are actually carried out.

For example, even when information security measures are in place, unless they provide staff with a seamless experience, they are often bypassed in favor of convenience. Wherever security is perceived to be the enemy of productivity, an organization will be at risk of a data breach.

A continuation of this is end-user education. Employees must be made aware of the threat that data breaches pose to individuals and to the business. With major changes ahead, it is best to start educating employees now rather than ineffectively pleading ignorance later.

Support Employees with Technology

A recent freedom-of-information request to the ICO revealed that 93% of breaches can be

attributed to mistakes made by end-users. If organizations are to better protect the data they process, investment must be made in flexible, highly integrated information security solutions that are easy to use.

Today's increasingly complex IT environments do not lend themselves to a 'one-size-fits all' approach, so security solutions need to offer flexibility, be that offering email encryption, large file send or secure online collaboration.

Greater protection can also be applied by taking decision-making away from individual end-users. Rather than rely on a member of staff to decide when an email or file should be secured, by centralizing policy-based control, using the specific content of an email as a basis for security, decision-making is less open to error.

Organizations have ample time to familiarize themselves with the EU GDPR and the opportunity it presents to enhance data security procedures and systems. In the long run, this will better protect businesses, staff and customers. If not they could be forced to sit up and listen with a fine of up to 2% of global take over turnover.



» FOLLOW US ONLINE

AND STAY UP-TO-DATE WITH THE
LATEST DEVELOPMENTS IN THE
INFOSECURITY INDUSTRY



TWITTER: @INFOSECURITYMAG



LINKEDIN: INFOSECURITY MAGAZINE



FACEBOOK: INFOSECURITY MAGAZINE



GOOGLE+: INFOSECURITY MAGAZINE

WWW.INFOSECURITY-MAGAZINE.COM



Hacking the

Cheaters



Phil Muncaster examines what the Ashley Madison incident says about security and privacy in 2015

Thirty-seven million records is a pretty paltry number to qualify for entry into the Data Breach Hall of Shame. It has nothing on the 130 million of Heartland Payment Systems or the 110 million of Target, for example. But in years to come, the attack in July 2015 on Avid Life Media (ALM), owner of infidelity site Ashley Madison, may be seen

as a tipping point in how we treat digital privacy and the security of information shared with online service providers.

Many of the details have yet to emerge at the time of writing, but even at this early stage, it's clear that the incident should force security managers to re-examine their cyber-defense strategies. Netizens,

meanwhile, will want to take a fresh look at how much data they share online.

The Story So Far

On Sunday 19 July, Ashley Madison's homepage was briefly defaced with a message from a hacker or group calling itself The Impact Team, alongside a link to a small



sample of the hacked data. The hackers claimed to have obtained personal data on the firm's 40 million users – across Ashley Madison and sister sites Established Men and Cougar Life – including financial information and customers' sexual fantasies. Also stolen, according to Brian Krebs, were "maps of internal company servers, employee network account information, company bank account data and salary information."

The hackers' beef seems to have been ALM's 'full delete' privacy service, which gave users the option of spending \$19 to remove PII and account usage history. The Impact Team claimed this promise was a "complete lie" which had netted the firm \$1.7m in revenue in 2014. "Users almost always pay with credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important information the users want removed," they wrote.

The hackers continued: "Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online."

ALM responded a day later that it had closed "unauthorized access points" and invoked the Digital Millennium Copyright Act (DMCA) to take down any personal information already leaked online.

The site owner added that it was offering the full delete option to all customers for free, claiming it did work: "Contrary to current media reports, and based on accusations posted online by a cyber-criminal, the 'paid-delete' option offered by AshleyMadison.com does in fact remove all information related to a member's profile and communications activity. The process involves a hard-delete of a requesting user's profile, including the removal of posted pictures and all messages sent to other system users' email boxes. This option was developed due to specific member requests



Just as a car manufacturer can't afford to sell a vehicle with faulty brakes, a site dealing with super sensitive information cannot afford to have subpar privacy

Mac Macmillan
Hogan Lovells

for just such a service, and designed based on their feedback."

The Breach

At the time of writing it still isn't clear exactly how the hackers managed to infiltrate ALM's network and steal customer data, although signs point to an insider. For example, ALM CEO Noel Biderman is quoted by Krebs as claiming: "I've got their profile right in front of me, all their work credentials. It was definitely a person here that was not an employee but certainly had touched our technical services."

The attackers also apologized to director of security, Mark Steele, claiming: "You did everything you could, but nothing you could have done could have stopped this."

However it was caused, the incident should serve as a reminder to CISOs of the importance of understanding their respective businesses, according to Trey Ford, global security strategist at Rapid7.

"Over-leveraged security programs tend to focus their energy on protecting regulatory data centers of gravity – ask any executive where their PCI/PII/PHI data lives, and they'll have a pretty good idea," he tells *Infosecurity*.

"The Ashley Madison breach brings into focus the need for CISOs to understand the workings of their business, specifically what data is collected, where it resides, and how it is stored, accessed and logged. There is a

serious difference between understanding the sensitivity of information, and allocating budget and human resources to protecting it, especially for unregulated data sets."

The Implications

The potential impact on ALM and its customers is obviously pretty severe in this case. The Canadian firm was planning an IPO in London later this year which it was hoped would raise around \$200m, following bumper sales of \$115m in 2014. It can be reasonably expected that this will not happen. In fact, whatever the cause of the data breach, the future of the firm itself is now on a knife edge. For an industry where the privacy of user data is sacrosanct, an incident like this could be catastrophic in terms of brand reputation and customer trust.

The impact on customers of the site could also be grave. The personal information stolen included financial data which could be used to commit identity fraud. But unusually in a data breach case, the very fact of being identified as among those affected could ruin an individual's personal life. For that reason the data is a prime target for blackmailers, as well as those who could use the info to make follow-up spear-phishing attacks more effective.

Experts were divided over whether victims could claim compensation if they are 'outed' as part of the breach.

"In this context, merely being named as having been in the database, not to mention leakage of more intimate details and photos, can have grave implications for those involved. I am sure many individuals are already suffering grief and anxiety as they watch the events unfold," International Association of Privacy Professionals vice president of research and education, Omer Tene, tells *Infosecurity*.

"Courts have begun to recognize that this type of harm too can merit compensation."

Hogan Lovells counsel Mac Macmillan argues that, as it stands, UK Ashley Madison customers would not have legal remedy under the Data Protection Act, as ALM is a Canadian company without a major base in the United Kingdom. This might change

with the coming EU General Data Protection Regulation, although it would have to be proven that the firm didn't at the time have sufficient "technical and organizational security in place," she tells *Infosecurity*. The latter would include things like ensuring staff with access to customer data are properly vetted.

Lessons Learned

According to Ford, the incident should serve as a cautionary tale for security managers.

"CISOs tasked with protecting privileged, personal, and highly sensitive information should implement forced password rotations, customer notifications, a clear privacy statement, and immediately acknowledge an incident, with a statement of what specific data was impacted so users can work to protect themselves quickly," he argues.

For Tene, the incident is proof that firms "must treat individuals' data as a valuable but also potentially toxic asset."

He explains: "Even before legal implications, a data breach or misuse of personal information can seriously weigh down trust, reputation and brand, directly impacting the bottom line and subjecting senior management and the board to heightened risks. Between the FTC, FCC, state AGs and private litigants, including class action lawyers, enforcement risks are high and rising, as this area garners daily media attention."

"We recommend organizations institute comprehensive data governance programs accounting for both privacy and data security, and including vendor management, data retention, and responsiveness to individual rights."

According to Hogan Lovells' Macmillan, the case itself is unlikely to represent a tipping point in the way individuals or organizations regard data privacy and security as it simply isn't relevant to enough people – despite the large number of records breached. A senior internal auditor at UK

supermarket chain Morrison's was jailed for eight years in July after posting the personal and financial details of 100,000 employees online. However, this case received relatively little press attention because of it wasn't particularly salacious, she argues.

"Ashley Madison hit the headlines because of the subject matter, but equally a lot of people will disassociate themselves from it because it's not close enough to home," she adds. "Yet they're not thinking about the fact that every time they wear a fitness tracker they're sharing data without understanding the implications."

But Tene believes the case should force businesses and governments to look more closely at what safeguards they have in place to minimize privacy and security risks.

"This includes appointing dedicated officers to oversee data management, putting in place data governance programs, and using technological, administrative and legal safeguards to minimize risk," he argues.

"Businesses that fail to do so will sooner or later bear the costs. In particularly egregious cases, they'll be driven out of business. Just as a car manufacturer can't afford to sell a vehicle with faulty brakes, a site dealing with super sensitive information cannot afford to have subpar privacy and infosec safeguards."

KPMG cybersecurity practice senior manager Matt White agrees that online providers need to up their game, as incidents like this and the Adult FriendFinder attack in May become more widespread.

"It is alarming how relatively immature user awareness is when it comes to protecting their data. Users are yet to develop an almost 'hardwired' level of security that we see in other areas of their life. For example, most of us are brought up to always wear a seat belt or to lock our front doors to prevent burglaries," he tells *Infosecurity*.

"A certain level of awareness will come, but we are not at that stage yet, therefore companies need to ensure that they take every measure possible to protect their users and train their staff to protect the company's data assets against hackers."



Ashley Madison: What Happened When?

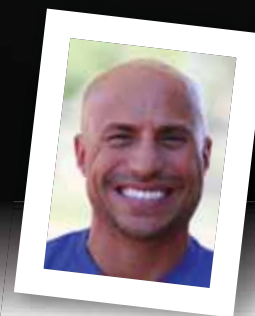
- July 19:** Brian Krebs reveals that The Impact Team published around 40MB of data stolen from Avid Life Media (ALM), including user card details and company documents. A statement from the group threatens to release data on all 37m users unless the site is closed.
- August 18:** The hackers post a 9.7GB file to the dark web including personal details of the site's users. A day after, the data spills online, while ALM tries to take it down by issuing copyright notices.
- August 20:** Second data dump appears, this time 19GB in size.
- August 21:** Canadian law firms launch \$578m class action against ALM on behalf of Canadians who signed up to the service, alleging their privacy was not properly protected by the firm.
- August 22:** Third trove of data released online including emails allegedly taken from ALM CEO Noel Biderman's personal account, appearing to show he cheated on his wife.
- August 24:** ALM announces \$378,000 reward for info leading to arrest of hackers behind The Impact Team.
- August 25:** It emerges that online scammers are using the news of the hack to extort and defraud ALM customers, or else trick them into downloading malware.
- August 26:** Brian Krebs claims hacker could be linked to Twitter user Thadeus Zu.
- August 28:** ALM reveals CEO Biderman has resigned, effective immediately.
- August 31:** ALM claims Ashley Madison is still attracting users, trying to quash speculation that it has grossly exaggerated the number of unique female users who actively use the site.



Shining a Light on Shadow IT



Sumo Logic's **George Gerchow** explains how organizations can go from cloud skeptics to cloud enablers



Enterprise perceptions of cloud applications have come a long way. Many no longer implement hard and fast policies that prohibit cloud apps or mandate that all data stays on site. Instead, organizations deploy a hybrid infrastructure and attempt to strike a balance between cloud and on-premise solutions.

But even organizations that regularly rely on cloud infrastructure are still cautious – and with good reason. While cloud adoption has become more established, strong and consistent security processes have yet to catch up.

The Dark Side of the Cloud

This disparity is evident in security-sensitive processes like off-boarding, when the process of removing outgoing employees' access may get forgotten in the shuffle. If not properly monitored and managed, Salesforce and other cloud platforms might still give ex-employees access, allowing them to log into sensitive systems. This opens the door for data tampering, potential data loss and theft, and non-compliance.

Similarly, rogue consumer cloud storage apps, such as Box, become shadow IT when used as business tools. Users may download these applications in good faith, but IT administrators have little, if any, visibility into them, which opens the door to malware, compliance violations and unauthorized access.

These issues influence organizations to lock down cloud platforms or impose stringent and

prohibitive security policies. But draconian rules may force users to find alternative (and sometimes more secretive) ways to access cloud tools that further mask their activities and put the organization at risk.

Cracking down on SaaS can also be counterproductive to business objectives and harm efficiency and productivity. This can dent an organization's agility or ability to offer competitive services.

The Shift to Cloud Enablement

Cloud doesn't have to be perceived as a business inhibitor. Instead, organizations can be progressive by changing processes to keep up with accelerating cloud adoption, as opposed to putting the brakes on.

For organizations, that means evaluating why and how employees are using these cloud services, and finding ways to secure and manage them that protects data while simultaneously meeting employees' ongoing work needs.

While it may seem like a monumental task, it's important to recognize that organizations simply can't prevent the use of cloud apps. Workers are using them for a reason, and won't stop if those apps make their jobs easier.

Organizations need to find ways to create visibility into these services with dedicated security solutions. If these apps prohibit visibility or management, administrators need to offer corresponding services that meet the same specific business needs, but which they can secure and manage.

Meanwhile, authentication and other security issues created inadvertently by cloud tools may present a few more challenges. To address these issues, organizations need to conduct comprehensive assessments to identify security gaps and determine where and how they can better manage their cloud-based tools. That means examining and improving access management processes and policies across all platforms, and particularly scrutinizing those policies that apply to departing or terminated employees.

In addition, administrators need to evaluate and improve key management and encryption in order to protect critical but potentially unsecured data. To do this, they need to determine who manages the keys and oversees best practices, dual controls and other functions. Organizations also need to implement robust and effective data leak prevention technologies, to ensure that cloud services don't accidentally open full visibility to sensitive data.

Above all, organizations need to prioritize visibility in all areas of the network, ensuring they have access and the ability to monitor, manage and control all network functions. By not operating in the dark, organizations can avoid many of the pitfalls and challenges created by the cloud. By overcoming its limitations, businesses can become cloud enablers, and truly leverage its potential.



Laying Down the Law



The EU's General Data Protection Regulation has been in the works for half a decade, but it could finally be passed within a few months. **Mike Hine** speaks to leading privacy lawyer, Eduardo Ustaran, about its background and impact



There's been a storm brewing in the world of privacy and data security legislation for several years. But despite a few ominous rumblings, the thunderheads have yet to break, always hovering somewhere on the horizon.

That, finally, could be set to change, with the EU General Data Protection Regulation (GDPR) due, finally, to pass by early 2016, with a two-year transition period to follow. It's been a long time coming, and the final agreement should at last clarify the terms that security and data privacy professionals have been anticipating for so long, and help the industry ascertain just how far-reaching and radical its implications will be.

The Story So Far

The legislative reform process behind the GDPR started back in 2008, when a number of EU data protection regulators, including the ICO, began to publicly question the relevance of the EU Data Protection Directive of 1995. Renewing a framework like this would be a substantial undertaking, and the EU Commission was initially not keen, but in 2010 it produced a white paper which outlined the need to modernize the legislative framework, heralding the official beginning of the GDPR wrangling.

It is perhaps unsurprising that the 1995 Directive was reaching the end of its application by the second decade post-Millennium. The speed with which technology has developed and proliferated across workplaces and homes has vastly expanded the data collection and analysis capabilities open to businesses and

government bodies. Policy-makers didn't have to reach too far for examples of how the 1995 law did not really match the technological possibilities of the day.

Eduardo Ustaran, a leading privacy lawyer and partner with Hogan Lovells, was very actively involved in the early stages with stating the case for a legislative overhaul. He told *Infosecurity* about the background to the reform from the perspective of a legal practitioner actively involved in the world of privacy and data protection.

"In the 90s, we didn't have smartphones or the internet as we know it," he begins. "Our interaction with technology has radically changed. The amount of data being collected, the sophistication [in technology], and the value of information is completely different. The framework that was created in the 90s is not geared to protecting data in the way in which it is used today."

That premise is clear, and has been for at least five years. The tortuous period that followed is exactly what the skeptics point to when they question the applicability of legislation like the GDPR to the world of technology: law-making is a grindingly slow process; tech moves at light speed. How can the two be effectively reconciled? And what's taken so long?

"It's a very political process," Ustaran says, "and, at the same time, the stakes in terms of getting it right are very high. There is a sense that technology is changing everything and now is the time we either protect the data right or we will lose data protection and privacy forever."

Indeed, as the process behind the GDPR has rumbled on, it has become clear that issues of data privacy are so entwined with a range of political and civil rights issues that navigating it appropriately has become exceedingly complex. In Europe, Ustaran explains, information about an individual is perceived to belong to that individual, which means legislating to allow for the responsible, commercial exploitation of that information becomes a headache. This tension between the political drive to protect personal data and create a system that allows for responsible exploitation is, in Ustaran's view, "almost swimming against the current."

It's not hard to see why, given the dependency of our digital economy on personal data. Companies and technology are set up to obtain as much data as possible. Removing the right to collect data en masse would cut the essence of what fuels that economy.

Ustaran explains: "Data minimization, theoretically, is wonderful, but in a practical way it is not going to work. It's too late to stop phones, websites and apps collecting data about us. They are designed in such a way that digital information by default is retained. The success of Facebook, Google and others depends on the fact that that data has been generated by the mere users. We cannot stop that now."

What the Future Holds

This whole concept has meant that the GDPR's potentially more radical possibilities have not been fully realized. However, it is

The Google right to be forgotten case was landmark in the history of EU privacy law



Picture credit: Maglara / Shutterstock.com

set to enact a number of significant changes, many of which focus on the responsibility of organizations that collect and use information to be transparent, reasonable and avoid harming individuals.

One of the most impactful will be mandatory breach notification across the EU. It's still in the process of being decided, Ustaran explains, what will trigger the breach notification, but across industry sectors there will be an obligation to announce the breach to a regulator or the victims, and there is likely to be a set-in-stone time limit of hours.

"It's going to expose security weaknesses, as has happened in the UK," Ustaran says. "Since the UK has introduced mandatory breach notification we have had greater visibility of breaches taking place in this sector."

But perhaps the biggest headline-grabber when the GDPR does finally pass will be monetary penalties, whereby organizations that suffer a data breach, and are found to have been non-compliant with the regulation, could face fines of 5% annual turnover.

Explaining the rationale behind this, Ustaran says: "Part of the reason non-compliance is so widespread is that enforcement has been very weak. From a policy-making point of view the

Commission was very keen to ensure that in some serious cases regulators had the power to enforce the law through very large fines. The percentage of global turnover is something that has worked for years in the area of competition law; it is obvious in some respects."

Another major change that is set to come in with the GDPR is the extra-territorial effect of the law, whereby organizations outside the EU will be treated as data-handlers under the regulation if they are processing data of EU citizens.

"That is in line with the fact that information is global," Ustaran explains. "European data is collected on a global basis and therefore should be protected on a global basis."

The practical difficulty is going to be enforcing that part of the law against organizations that have no presence in the EU, but that is probably not going to be a priority of regulators, who will instead try to enforce the law against global organizations that have a physical presence in Europe, Ustaran clarifies.

Data protection authorities, meanwhile, are almost certainly going to acquire increased powers under the GDPR and take on a bigger role. Their resources, however, are not likely to increase substantially, meaning increased pressures in the quest to deal with the monumental task of enforcement in a world where data breaches are becoming a daily occurrence.

"What we have today," Ustaran says, "and what we are likely to have in the future, is a drop of enforcement in a sea of non-compliance. Regulators are smart people and they will go after the big fish. That will continue to be the case and they will try to use one case to drive change across a whole sector."

The regulation will also require the appointment of data protection officers within organizations that process data about 5000 or more subjects, or possibly those with 500 or more employees (subject to confirmation). Either way, this will affect a very large amount of EU companies. The role of DPOs, Ustaran explains, will be to

establish a level of compliance and to monitor that level of compliance.

"It will be a relatively independent role, to raise the awareness of data protection within an organization. The most successful data protection officers will be the ones that are able to align data protection with the objectives of the organization.

"Data protection officers in isolation are not going to achieve everything. I think there will be a general effort to emphasize the importance of issues and companies themselves finding a way to raise awareness. We've talked about that with clients recently – making an incident response policy available globally and making it work within an organization. That's a real challenge and will continue to be."

Brace for Impact

It is the intention that the GDPR will improve transparency. But to be transparent and to be clear about how data is used is increasingly difficult, because citizens' interaction with technology has increased exponentially and will continue to increase. It's become almost impossible for us to know when our data is being used.

So what will be the impact of the GDPR? Ustaran argues that the regulation will be "slightly out-of-date" before it is even passed: "There will be elements of that law that will be ineffective from day one in terms of protecting information and that is a reality. It is disappointing that it has not been radical enough in changing some of the perceived 'rules that cannot be changed', like reliance on consent or the limits on international data transfers. These are concepts that worked many years ago but don't anymore."

Ustaran is more positive about the introduction of privacy thinking in the way in which products are developed, organizations are run, and services are provided.

"On the whole Europe is rather conservative in this area and I would have probably gone for something that takes into account the relentless evolution of technology and the globalization of data and I'm not sure that has been taken into account."





Security and ROI



Vormetric CSO **Sol Cates** looks at how security can be a business enabler, driving progress and ROI



Are you seeing a return on your security investments? It's a difficult question. Although the answer is almost certainly yes, it can be difficult to measure with any precision and often requires a shift in mindset.

Data security used to be seen as a business burden, like tax, but that is changing. Recent incidents have shown the damage a data breach can cause – it can shut a business down entirely or cost someone senior their job. The pressure is on for businesses to allocate security spend on technology as wisely and strategically as possible.

Fortunately, for those within the business who must justify security spending, improvements to security are now enabling organizations to adopt technologies traditionally seen as 'risky' (cloud computing, mobility etc) at a much faster rate, giving a considerable competitive advantage and drastically improving ROI.

The Times They Are A-Changin'

During the past five years, the business operating landscape has been transformed. With an intricate latticework of data centers, cloud services, contractors and various other data handlers, businesses must hedge their exposure to risk from a multitude of sources and increasingly find a way of protecting data. Allocating security resource efficiently today is also different – perimeters and end-

points still need protection, but the attack surface is so much broader than before. Today, businesses must also find a way of limiting data access to those who truly need it to perform their work.

Recent insider threat research by Ovum showed that over 50% of European organizations now classify 'privileged users' as the highest risk to data. These types of user accounts must be treated with far greater care, but this brings a variety of technical challenges – not least because such accounts are used to perform essential network maintenance and administration procedures.

In addition, the insider threat does not stop there: contractors, development teams, data scientists, system administrators, network administrators and other third parties often have access to data without a real need for it.

Cloud, big data and IoT technologies have unsurprisingly exacerbated things – often expanding the internal pool of privileged users, and adding the potential for service providers to see information. As a result, today's businesses can either block access to new, productivity-boosting and business-enabling services, or risk the exposure of sensitive data through their use.

Security as an Enabler

Fortunately, awareness of security's merits as a business enabler is growing. Take a trend like cloud computing – the cost, efficiency and

scale benefits are undisputed, but the security concerns remain (think of the iCloud hack).

Ovum research found that almost half (46%) of global respondents are using the cloud because of 'market pressures'. However, the same report reaffirms that security remains a major stumbling block: though 80% of enterprises are already using cloud environments, only 54% reported keeping sensitive information in the cloud, highlighting perceptions of insecurity.

What if you could better address those concerns? What if you could make greater assurances that cloud data will remain defended even in the event of a breach? Establishing a means of securing data as it enters into – and is accessed while contained within – cloud environments is fundamental to propping up the long-term operations of a company. In this light, security goes beyond the defense of data, becoming fundamental to business progression.

Adopting data security measures that are designed to protect the data itself and, in turn, monitor, track and control how that data is accessed, will go a long way to addressing anxiety among businesses concerned about making data security investments. Ultimately, business leaders need to know they are getting as much value as possible for the money spent.





More than

Virtually Secure



There's little doubt that virtualization has taken hold in the enterprise. As well as reducing costs, cutting floor space, and improving performance, it can also enhance security. **Max Cooter** finds out just how



In some ways it's misguided to say that virtualization is a new technology: sandboxes, which have been part of the IT armory for some years, also employ virtual technologies, albeit with some differences (of which more later).

But what really kick-started the latest interest in virtualization as a security technique was Microsoft's adoption of the technology in VBS (virtualization-based system) as part of the recently-launched Windows 10 operating system. Formerly known as virtual secure mode (VSM), Microsoft claims that it offers a new way for customers to protect data, reducing the need for antivirus products.

It sounds a revolutionary approach. Microsoft is drawing on a technique that has also been fostered by start-up Bromium. Headquartered in California, Bromium does much of its research work in a laboratory in Cambridge, England and claims to have pioneered what it calls micro-virtualization as a way to isolate viruses and other forms of malware.

It's a welcome thing for the corporate world. According to Gartner's latest *Magic Quadrant* for endpoint protection, "The rise of the targeted attack is shredding what is left of the anti-malware market's stubborn commitment to reactive protection techniques. It is clear that the industry is failing in its primary goal of keeping malicious code off PCs."

The Art of Xen

Micro-virtualization technology is based on the Bromium microvisor, which, in turn is based on Xen technology. The hypervisor creates micro virtual machines for every task that the PC is processing; this has the effect of isolating user tasks for each other and from the connected network.

Among the people behind Bromium are Simon Crosby and Ian Pratt, both of whom were behind the Xen Source hypervisor (both also went to Citrix when it acquired Xen).

CTO Crosby says that Bromium has built its business on companies who have a lot to lose: "people who lose more than money."

However, the Bromium message is penetrating more than high profile customers. The emergence of Microsoft's virtualization-based security has shaken the market up even more.

For Crosby, the adoption by Microsoft of virtualization as a security technology has been an endorsement of the basic technological approach but takes care to point out that the two systems fit well together. "What they do is absolutely complementary to us."

He likens the two approaches to a medieval castle where Microsoft has hidden the jewels deep in a tower: "We're on the ramparts, isolating anything that comes to the system using virtualization." He stresses that Bromium is an important Microsoft partner.

A statement from Microsoft endorses this view: "Microsoft is applying hardware-enforced isolation to critical components of the core Windows operating system...VSM will ensure that attackers will not be able to steal the system's credentials even if the Windows operating system is compromised by an attacker."

However, Microsoft says, "VSM will not protect user files and other sensitive information stored on, or accessible by, the endpoint running VSM; nor does it prevent malware from accessing the corporate network."

Bromium is designed to isolate the unknown or 'untrusted' external information a user interacts with in a hardware-enforced micro-VM. This is claimed to be able to ensure that nothing downloaded from the web, or opened from an email message, can attack the protected system.

Bromium adds that it can provide protection not only for the Windows operating system, but for non-Windows programs like Adobe Acrobat or Google Chrome. That means eliminating attack vectors on the endpoint, and Microsoft hardens the OS – both through the use of virtualization technology on the endpoint CPU.

What Microsoft does that's different, says Crosby, is to focus very much on the device: "With DeviceGuard, Microsoft is moving



The rise of the targeted attack is shredding what is left of the anti-malware market's stubborn commitment to reactive protection techniques

Gartner Magic Quadrant report

towards device-based security. It is releasing a whole bunch of technologies all of which allow the device to become more secure."

DeviceGuard pulls together aspects of hardware and software to enable a device to run only trusted applications. But it goes further, using the new virtualization-based security in Windows 10 Enterprise to isolate the Code Integrity service from the Microsoft Windows kernel itself, enabling pre-defined signatures to determine what is trustworthy. This is a shift from the traditional anti-malware process where all apps are trusted unless they're blocked by antivirus software to where apps have to be authorized to work within the enterprise.

For Crosby, this approach is a step in the right direction: "DeviceGuard depends substantially on VBS." He highlights two key areas in particular that are offering enhanced protection. These are the way that credentials are moved away from LSASS (Local Security Authority Subsystem Service), where they had been previously stored and the use of the hypervisor as a barrier to LSASS.

The Microsoft approach now is to use a new process called LSALso, part of VSM but separate from the operating system itself – it sends credential requests through what Microsoft calls a trustlet. This will approve requests but not reveal any confidential information that lies deeper in the operating system – hiding the crown jewels.

What does this approach mean for traditional antivirus products? There are commentators who believe that the emergence of virtualization as process would mean that antivirus software's days are numbered. Microsoft plays this down a bit: "Virtual Secure Mode offers increased security to the user, and has no impact to traditional antivirus products."

Drawing a Line In the Sandbox

One of the traditional security vendors is happy to give the thumbs-up to Microsoft's approach. David Emm, principal security researcher at Kaspersky Lab, says, "Microsoft's aim here is to prevent an attacker from accessing identity information that would allow them to impersonate the authorized user of the computer. The user's access tokens are held in a secure container that is separated from the operating system. Whilst there's no such thing as 100% security, I believe that this will make it much harder for an attacker to obtain this information."

Yet it may be that it is not just antivirus products that look somewhat isolated: where does emphasis on virtualization leave sandboxes? As mentioned earlier, this is a security technique that bears some resemblance to virtualization, even if it's not quite the same: the sandbox works by wrapping a virtual container around an application, while a VM acts like an entire separate computer, isolated from all other virtual machines.

According to Orlando Scott-Cowley, cybersecurity strategist at Mimecast, traditional sandboxes are reaching the end

“Viruses have become so good at detecting sandboxes. More malware is going to bypass sandboxes and start attacking the operating system”

Orlando Scott-Cowley
Mimecast

of the road: "The issue has moved on because viruses have become so good at detecting sandboxes," he says. "More malware, such as Dyre and Kimber, is going to bypass sandboxes and start attacking the operating system."

Scott-Cowley believes that Microsoft is on the right track but warns there is another issue to contend with, connected with the way in which malware deals with virtual instances.

"A lot of malware makes the distinction between physical and virtual machines. They look for things like mouse movement or what other applications are on that machine: if they can't find them, then that malware isn't going to run," he adds.

That's all well and good, but that doesn't mean the malware won't run at all and, he says, solving that problem takes a lot of code,

meaning many more additional lines of code on top of the millions of lines of code that already make up Windows. "And we know that the more lines of code there are, the more likely there is to be a flaw," he adds.

Even though virtualization has been widely adopted across organizations, the security aspect has been somewhat neglected. According to a recent survey from Kaspersky Lab, the cost of recovering from breach in a virtualized environment is twice as expensive as that of a breach in a physical system.

"It's mainly because companies don't understand that they are vulnerable. The risk to virtual and physical systems is essentially the same, but there is sometimes a perception that in a virtual system, protection is somehow built-in because it's not a physical device," warns Emm.

One of the surprising elements of the move to virtualization as security is the non-appearance of VMware among the players. After all, this is the company that is leading the virtualization market and would normally be expected to look to using the technology for security. According to Crosby, the company was investigating the possibility in what was known as Project Fargo, with the goal of making VDI VMs boot quicker.

451 Research chief analyst Eric Hanselman is also aware of VMware's work in this field: "I know that VMware has been looking to build a route of trust around their environment but, so far, has not released anything."

A Question of Time

Despite the absence of the market leader in virtualization, it's clear that Microsoft and Bromium are on to something. Virtualization as a security technique offers plenty of opportunities for new levels of security but, as Scott-Cowley warns, time is limited.

"We know that at some point, the attackers get ahead of you," he says, pointing out that the good guys are fighting to keep the cyber-criminals at arm's length.

Virtualization works for now: but how much longer before that's breached too?



Virtualization may not be new but it's certainly shaking up traditional approaches to security



The Case for Better Threat Measurement



The security industry needs better intelligence, not more alarming statistics, writes LogicNow's **Ian Trump**



Frederick the Great wasn't talking specifically about IT security when he said, "He who defends everything, defends nothing." But nonetheless, it would be prudent to heed these words.

No organization has limitless resources, so it's important to allocate them intelligently to tackle the most dangerous and prevalent threats. If, for example, 99% of phishing attacks don't make it to the intended recipient, does it make more sense to try to block the 1%, or invest in user education?

It's accepted that cybercrime is the main driver behind the rise of malware, but we don't really know how large the increase has been. Attempts to measure malware use have had limited success because there is no industry-accepted standard. The numbers put forward by vendors, industry bodies and the media all vary widely.

Numbers Don't Lie?

Alcatel Lucent claimed that in 2014 malware infections in mobile devices increased 25%. McAfee, meanwhile, reported that 2014 saw a total mobile malware growth of 167%, and Sophos Labs reported an increase in Android malware by nearly 600%. However, the Verizon 2015 *Data Breach Investigations Report* argued that mobile security threats were "overblown" and "negligible".

So who is right? The disparity in numbers is partly down to different ways of

measurement, a different focus, or simply analyzing a different data set. But does this mean that a serious attempt to establish the scale, the cost or the impact of such attacks is doomed to failure?

The approach to measuring malware needs to change. Simply grouping everything together as an 'attack' regardless of the activity that occurred is not useful. This means that a bot-driven vulnerability probe, a politically-motivated site defacement, and the theft of financial data are all treated equally, despite the different impact they could have. By lumping everything together, it limits the clarity.

Focusing on global trends tells us little about the impact and costs to business. We know that malware is increasing worldwide, and whether that's 60% or 600% doesn't tell us anything of interest. Instead, by collecting and analyzing specific local data, and then comparing national and regional successes and failures (against a score card of controls across specific industry groups), we could generate specific mitigation responses to identified threats, and help customize the response.

Share and Share Alike

The biggest potential issue is the sharing of data. Business leaders will likely recoil at the thought of sharing information with competitors. But there are precedents. High-

risk sectors such as financial services share threat intelligence, even though they are among the most protective of proprietary information. Formal collaborative services such as the RSA eFraudNetwork allow for secure intelligence sharing – preventing those who have perpetrated a successful attack on one organization from repeating the same trick. This kind of threat-sharing framework does not have to be expensive or complex to implement, and can be replicated across industries.

At the heart of all of this is the need for responsible and open disclosure. If we continue to go down the road of never disclosing or identifying the security components that failed, or the components that were not in place when a breach happened, we will never make any progress against the most elusive of enemies.

The data used by security vendors to make a big splash may be effective in sowing fear and uncertainty, but these are ultimately the tools of those we are working to stop – the ransomware developer that makes people pay for fear of losing their data, or the phisher that uses uncertainty to steal login credentials. The security industry needs better intelligence about where to focus its efforts more than it needs big, but ultimately empty, headline-grabbing numbers.





Checking the NHS's

Security Pulse



Managing 40,000 devices across 500 sites is a huge challenge for any organization. But in the health sector added, mandatory security concerns make this even harder. **Infosecurity** takes the security temperature at Sussex Health Informatics Service

Security managers in all sectors probably lose a bit of sleep from time to time over the fear of a breach. In healthcare, the idea of being hit results in whole nights lost rather than the odd hour or so. The theft of healthcare records simply does not bear thinking about.

The Pressures of Provision in Healthcare

The UK health sector is under unprecedented pressure to manage increasing workloads with diminishing

budgets. Doing more with less is a way of life. In security, this means protecting better against bigger threats with fewer resources. Despite the South-East's relative prosperity, in August 2015 a parliamentary and health service ombudsman singled out the region for its poor record on health service failures: the South-East is attributable for 14% of complaints to NHS England and UK government departments.

Now part of the NHS South-East Commissioning Support Unit (CSU), this is where Sussex Health Informatics Service

(HIS) operates, supporting 40,000 users spread across 11 NHS member organizations. The organization provides a full suite of IT services as well as governance, project management, training, change management and strategy for all NHS trusts in Sussex. Protecting the integrity of the data and its patients is paramount.

Setting Out a New Security Infrastructure

Sussex HIS found that it needed a proactive, network-based approach for access and



endpoint compliance. Initially, however, it had to cope with an ageing intrusion prevention system (IPS) that only provided reactive security and whose alerts were at least a day old and clouded by false alarms. A real-time network security solution was needed to deliver complete visibility and policy-based control of all devices connecting to the Sussex Community of Interest Network (COIN).

A secure network, with no disruption to users or service, was deemed essential due to the time-critical nature of healthcare. In addition, the solution had to support a variety of IT staff, device types and network member sites with different operating environments. Key factors were ease of deployment, flexible administration and low total cost of ownership.

The IT services team determined that network access control (NAC) would address security challenges. To fund the NAC project, Sussex HIS replaced its ageing IPS. The project success criteria focused on deployment ease, management flexibility and low TCO. In the process of getting the appropriate NAC, the Sussex HIS team weighted each supplier against two initial requirements: the solution had to be agentless to support more rapid deployment and reduce overhead; and it must be capable of supporting multiple sites with varying operating infrastructure.

"Some NAC suppliers never made it past this first stage, as they didn't grasp the technical and cost implications of these two basic requirements," recalls Peter Ward, senior security engineer, NHS South-East CSU.

Next, the team created a requirements matrix incorporating more stringent test criteria that included: agentless capability; integration with existing systems; ability to identify and manage unknown devices and users; multiple operating system support for Windows, Linux and Mac; support for machine compliancy checks, AV, encryption, domain membership, and more.

Once each NAC appliance was tested against the core criteria, Ward wanted to ensure the final selection could be customized, run custom scripts and create



If the organization incorrectly identifies an A&E patient monitoring system as a rogue device, that is potentially life threatening

Peter Ward
NHS South-East CSU

custom actions. Additionally, he was looking for an enhanced level of data regarding endpoints and users.

Working Smarter and More Profitably

After assessing each NAC product in a test environment and considering performance in context with cost, Sussex HIS selected ForeScout CounterACT.

Ward explains: "CounterACT was agentless and flexible enough to meet the needs of our diverse healthcare infrastructure and customers. The management console allows us to provide our healthcare members with tremendous visibility and more automated control."

The first appliance was deployed in July 2012. The NAC platform roll-out did not require agents and it could be set to monitor-only mode, making it quick with no user disruption. The ability to centrally manage the system and enforce policy across multiple NAC appliances, regardless of network infrastructure diversity, further reduces typical NAC implementation challenges. Within two weeks, the network teams had installed all appliances and they were up and working.

Sussex HIS found that CounterACT removed the need to place appliances in the data path, reducing implementation costs, making routing reconfiguration unnecessary, and not generating additional

points of failure. As such, Sussex HIS could deploy and centrally manage seven physical appliances located at five strategic nodes around the COIN network, covering all NHS member organizations and third-party IT suppliers operating on the COIN.

"We run an extensive network where support of our healthcare provider's ability to deliver efficient and effective patient care is a top priority. Within any healthcare environment, there is an incredibly diverse range of hardware and users that change daily," Ward observes.

CounterACT provided NHS South East CSU with visibility of devices connecting to the internal network in real-time. The resulting information was used to make informed access and endpoint configuration and security management decisions in order to more rapidly address, mediate or block any IP device or person highlighted as a risk to NHS data, infrastructure and hardware.

Looking Forward

Due to the scale of Sussex COIN, Sussex HIS could not monitor what devices were connecting in real-time, let alone classify, segment and assess endpoints appropriately. CounterACT enabled this, and allowed for the automatic assessment of all devices and users previously and currently on the network, checking their compliance and remediating any problems without disruption.

Accurate device classification was essential, Ward stresses: "In healthcare, everything from sterile washers, MRI scanners, medical kiosks, patient monitoring systems through to the chief executive's iPad all need to be classified correctly and monitored. If the organization incorrectly identifies an A&E patient monitoring system as a rogue device and subsequently blocks it, that is potentially life threatening."

By replacing the ageing IPS, Sussex HIS made significant cost savings by removing the high management overhead. The new network security platform provides a better use of funds and adds value across the IT organizations. In today's NHS, this combination of peace of mind and cost savings is quite the tonic.





Place Your Bets on **Security Firms**



The City and the Street say that this is a golden age for investing in security companies. **Joe O'Halloran** sees just how long the good times are set to roll



Ultimately, the success of companies such as his, says Jason du Preez, CEO and founder of Privitar, all comes down to finding money and finding the right people to make the business work while you go looking for that funding. It all sounds so simple. And in an industry such as security, where the need for the fundamental product gets ever more important, how hard can it be to find funding?

Well therein lies the problem. It's not just a case of funding per se, but the type of funding and the timing. Subjecting the investment community to as much scrutiny as it puts on security firms that represent a potential investment, some interesting dynamics emerge. It certainly isn't a case of simply putting money on anything security based and waiting to collect on the bet. Not at all.

At the Bleeding Edge

Being part of a startup is a heady thing. There's the excitement of creating something based on your vision. For du Preez, the vision is to facilitate the use, collaboration and trade of data while adopting an "uncompromising" approach to protecting private personal information. He believes that there is a growing realization that, unless companies incorporate privacy into every aspect of the data supply chain, they run the risk of impeding innovation and exposing customers to harm.

Privitar was set up to provide its customers with the tools to tackle these issues, offering security that the firm claims goes way

beyond traditional methods. Prior to founding Privitar, du Preez co-founded and led the growth of UK-based m35 (enterprise data management software) up to a successful exit through sale to Thomson Reuters in 2009. While there he first met his co-founder Gerard Buggy, an adviser and investor with 20 years' experience within information technology encompassing real-time enterprise software and data architectures. Buggy brought with him John Taysom who started the Reuters Venture Capital Fund in Palo Alto in the early 1990s.

In early 2009, Taysom conceived the original concept that data was going to be a problem, believing that the mere act of companies collecting, generating and assimilating information sets on people could tip a power balance. Patents were awarded in 2014 and then Taysom approached Buggy and du Preez to get more structure around their idea.

Investment Procurement: An Art Not a Science

But how easy was it to go through the first cycle of investment necessary to gain a foothold? Not very, du Preez says, despite working in what he calls an ostensibly "frothy" market with phenomenal valuations.

"Many people say that it is easy to get seed funding and there are a lot of high worth individuals in the market who are looking to place bets that you'll deliver a better return than the mainstream market," he says. "But finding the right seed money and taking a long-term view in how your

business is funded is critical. It's a long journey. The strategy for developing this story is important. It's not just about going to investors and saying 'here is our plan'; you shop around and market that idea. And that is hard work."

For du Preez this process involves bringing in a variety of individual investors who are attracted not just by the concept of the technology or purpose but also by how the company is going to execute on this vision. Here, says du Preez, is where a bit of art comes into play: "At each stage of funding you have something that you need to build and something that you need to sell and you need financing at every juncture. So when you start out with a really good idea and have a plan and then [build] a large amount of hope and value, how do you price that? It's intricate and challenging. It's an art not a science."

Security is a good place to be at the moment. But, stresses du Preez, companies should not take for granted that they will be inundated with investment offers. There is a lot of work to be done: "We have a huge opportunity. We have traction in a segment of this market that is very deep. And it adds up to a great valuation. And how do you access these people? That is a lot of leg work. We tapped into various angel networks and once you have convinced them that you have a good idea they will assemble a group of people to listen to your pitch."

Du Preez is also keen to add that, when picking investors and partners, you should

bear in mind what their input can do for you as a company. A prime example is attracting talent, of which there is a dearth, for a variety of reasons, he insists.

"If you hire a guy who is really good he could charge a fortune. Unless you appeal to the cause or lifestyle or the strategy, you can't win. More fundamentally than security is that there is just a very large industry that is extremely lucrative: that is the black hat side of the fence. There is a talent challenge. Having investors and the right profile makes it easier to hire and smooth the way to the next round of investment. Recruitment is so important in the first hires. Get that wrong then you have completely set yourself up for failure."

For Privitar, such steps have been taken and the company is on a trajectory that will see it raising its next round of funding as growth capital. It is now working with tier 1 clients in the financial and telco markets, gaining capital to grow. "The winner is the first to scale, not first to market" du Preez notes. "So this will put us into a situation to look to raise the growth capital sometime in 2016."

Ultimately, it does come down to the ongoing battle to dash for cash, but only once a solid foundation has been built: "Every aspect of the business is you living that on a daily basis. Good investors will

never close the purse strings on failure if you have solid fundamentals."

The Non-VC Route

All businesses start with an idea. But not many successful companies have been told by their own government that they had totally the wrong idea. But that is how ExactTrak began life in 2008, reminisces CEO and founder Norman Shaw.

"We started off with an idea and then the UK Home Office told us we had the wrong idea. And then they said, 'Lovely idea but why don't you track data? That's where the money is.'" After taking on board this constructive criticism for a week, Shaw and his team got down to turning the company on its head.

Still working with the UK government (and others), and now in the mainstream corporate sector, ExactTrak is a specialist in mobile data security and has developed a number of patented mobile data protection products that meet the growing need for mobile data security and asset recovery for remote and mobile users.

Shaw reveals that he started off his company right in the middle of the credit crunch in the UK without any VC at all. He already had 'quite a lot' of money, about £700,000. He then looked at who was around to build on this foundation. That's when he

met now CTO John Pragnell who was key to getting the business off the ground.

"There was no point in following the [VC] trend, so I went to this company which was to build the first prototypes of what would be our first product and quickly realized that I was soon going to run out of cash because of all of the developers' fees. Fortunately John Pragnell convinced me that we were onto a winner, but he said 'give me some equity.'" The parties agreed on 10% and Pragnell made his crucial investment.

Patently Obvious

The now partners carried on with development to get the product to its first commercial stage. Shaw's accountants had started putting out details of ExactTrak to its clients, advertising the firm as a good prospect for private investment. Shaw had one key criterion for the ideal partner, even though it limited the field in terms of potential investment sources: "I wasn't just interested in money, they had to bring brains and they had to make a contribution with their expertise. And I don't regret that for one single minute."

Shaw had a basic pitch for the investors: "This is what we are making, this is the market need, and [the product is] scalable and identifiable. And I think the majority of investors looked at that and agreed." Eventually, investor Simon Thorp put in around £50,000 and then he brought in others. In the space of a few months Shaw had accumulated around £300,000.

As well as the usual expenditure on development and marketing, a lot of money was put into patents, a decision that brought huge reward. "That really is your lifeblood," Shaw says. "We had some unique stuff and the government gives you the opportunity to meet patent boards. So we came up with a patent portfolio that is expandable. Small companies don't realize the importance of patents and what they can do. It's the best £75,000 I have ever spent."

For the third funding round, Shaw approached the shareholders to explain the need of further investment. They quickly





came up with the goods. They also had new shareholders following working with AMD.

"The combination of the market sector and scalability and the opportunity that AMD would give encouraged more people to come on board," Shaw recalls. "We got more investment and this time from the US in the form of a personal friend of our chairman."

Shaw describes the latter as a breakthrough in that it brought first a US service provider and distributor and then opened up funding channels within US-based groups. And it enabled the company to address the American market, something Shaw says can only really be done from inside the country.

ExactTrak now has a mixture of larger investors who have put in over £100,000 and a number of small investors whose stake is under £10,000 each. The latter tend to be slightly more concerned with monthly sales figures but none will accept anything that isn't tangible evidence of progression. Looking to the future, Shaw assures that the company won't start snatching at any deal on the table. For example, crowdfunding is one option that won't be explored: "It will open us up to the market unnecessarily. It's difficult enough to try to run a business with 15 shareholders – I really don't want to do it with 1500."

Challenges and Culture

Assessing the road ahead, Shaw is clear and blunt as to what he believes will be the company's biggest challenge to procuring more investment: the British mentality.



Jason du Preez, Privitar CCEO



What makes a business a success are people who are passionate. If your end game is cash in your back pocket you won't win

Jason du Preez
Privitar

"[British investors] all think short term and they always like to see a revenue stream. That is a difficult thing to do when you are right at the bleeding edge of technology. You go to America and they want a growing user base; they are not too fussed about a revenue stream, though they want to see the opportunity for one, and they are very good at structuring the amount of money that they put in according to progression through the KPIs. Whereas the UK funding KPIs are typically just, what's your turnover?"

Du Preez also says that there is an interesting and continuous contrast between the way things work in the UK and the way things work in the US: "Looking at the level of funding of our competitors and the rounds and how the mechanics work and the how they work here, it's a very different market."

By different does he mean better? "The jury is out. Most people would say that the [funding market] is better in the US and that it is easier to secure capital but the counter to that is that the European investor is more discerning. In the US there is more investment and a deeper appetite for risk. In the UK people want to see more of the fundamentals in place before talking the same degree of risk. Here we have to prove solid fundamentals which is a good discipline. If you can't provide these fundamentals, what are you doing anyway?"

Seeing More than The Exit Door

There's a saying that all businesses should start thinking about an exit strategy exit on the day they're created. And for start-ups and those in mid-life, like Privitar and ExactTrak, talk of what would happen if somebody waved a big check in your direction is not fanciful. Though for du Preez, thinking about the end of the road when you've barely started the journey says a lot about the intrinsic nature of a company and its direction.

"Everyone will ask [this question] eventually and this is where it gets interesting," he remarks. "What makes a business a success are people who are passionate about the product. If your end game is cash in your back pocket you won't win. In these early days it's not glamorous. It's about washing the coffee cups and doing everything because you are excited and enjoy it. Recognizing this is the mark of a good investor."

For his part Shaw has no worries about a big check from a supplier or customer. Indeed he can't really see why his company would accept such an offer. But is this just the optimism of being in the right place at the right time with the right product? What would happen if the security industry changed and became less of a desirable place for investors, or if indeed another segment started to capture all of the smart money? It's an issue that affects not only companies such as Privitar and ExactTrak but also the bug guns such as Norse.

Speaking to *Infosecurity*, Sam Glines, CEO of Norse, agreed that security is indeed hot at the moment and is most certainly not overhyped. While pleased with his company's performance, and believing that it is where it needs to be in terms of investment, he warned that the good times will not roll on forever and that firms needed to get the basics done now.

"[Security company] valuations are at an extreme level [now] and will be pulled back sometime within the next 18-24 months. There is still a lot of money in the deal flows but the music will stop. Those who aren't set up right are in for a shake up."



Cybersecurity Skills Crisis: A View from Academia



Universities' role is only part of the bigger picture, writes
Professor Keith Martin of Royal Holloway, University of London

We hear much about a so-called cybersecurity skills crisis, mainly from employers struggling to fill vacancies: "Where are the required cybersecurity experts? Shouldn't universities be supplying more? We need them now!"

There is a chronic cybersecurity skills crisis at a societal level. We all genetically understand physical security but intuitively lack common-sense cybersecurity principles. Technology has been adopted at a greater rate than our ability to securely develop and engage with it. At a more fundamental level, perhaps it's more of a cybersecurity awareness crisis than a skills crisis.

We really need to improve cybersecurity awareness and skills at all levels in society, from the schoolroom to the boardroom. We, as information security professionals, all have responsibilities to engage with this process. This will take time and energy, especially since the target is evolving. However, I am optimistic that society will eventually develop an understanding of 'cyber health' sufficient to alleviate most day-to-day cybersecurity issues that arise from ignorance and naivety.

Universities, undoubtedly, have their role to play, particularly in developing cybersecurity skills. There are two major ways in which I believe universities should be contributing.

The first is to provide courses for the development of cybersecurity specialists. This is, I suspect, the role expected of academia by many who decry the production rate of new professionals. UK academia has engaged with this and there

are a number of excellent cybersecurity courses on offer. Sure, there are also less outstanding offerings, but the UK Government has initiated the Certified Masters Degrees in Cybersecurity program to help applicants and employers identify quality. A government initiative to more broadly identify Academic Centres of Excellence in Cybersecurity Education is eagerly anticipated.

So is this component of the solution to the skills crisis sorted? Well, seemingly not. Coming from Royal Holloway, the university which offered the first dedicated cybersecurity program and now with over 3000 graduates around the world, you would think that we were fully doing our bit. But, somewhat surprisingly given the apparent skills crisis, we have retained some capacity in recent years on our programs. The skills crisis issue perceived by some employers is not necessarily down to a lack of supply channels. At least with respect to UK students, there is also an apparent lack of demand for such skills. Put more brutally, universities cannot supply cybersecurity experts if students don't wish to become them.

One organization that has long recognised the above issue is the Cybersecurity Challenge UK, which has worked hard to raise the profile of cybersecurity careers through its imaginative suite of competitions. We are enthusiastic supporters of the Challenge for this reason. I accept that universities have a role to play in trying to entice students into cybersecurity careers. We, for example, also run a cybersecurity residential program for the

Smallpiece Trust, which is dedicated to attracting schoolchildren to consider science and engineering careers.

However, I strongly believe that the main promoters of careers in cybersecurity should be those who wish to employ cybersecurity experts. If the cybersecurity profession can create the demand for cybersecurity skills amongst potential new entrants to the profession, rather than bemoaning the lack of supply, then universities can comfortably deliver those skills.

The second role that universities can play is long term and relates to the much more fundamental societal cybersecurity skills crisis. While there will always be a need for specialist cybersecurity courses, our need to establish a future notion of societal cyber health requires that cybersecurity skills be embedded in all forms of training, including those provided by higher education. While this is beginning to happen with computer science programs thanks to efforts by organizations such as the BCS, every student, whether on a business administration or a medical program, needs to be equipped with relevant cybersecurity skills in order to be fit for the modern workplace. Indeed cybersecurity skills should probably feature in the list of high-demand transferable skills that currently includes topics such as presentation and writing proficiency.

The UK Cybersecurity Strategy has one thing absolutely right. No sector can address cybersecurity issues without help from the others. UK academia is able and more than willing to play its part.





infosecurity

MIDDLE EAST

15-17 MARCH 2016

ADNEC, ABU DHABI, U.A.E

www.infosecurityme.com

SECURING YOUR WORLD AGAINST CYBER THREATS

Infosecurity Middle East is the launch event from Infosecurity Europe, a pioneering information security exhibition and conference with 20 years of successful history. Following the success of the information security pavilion at ISNR 2014, this leading international event will debut at the ISNR Abu Dhabi 2016, and host an exhibition, expert workshops and specialised trainings, that ensure the security of vital data and IT infrastructure.

Infosecurity Middle East brings together government organisations, major public institutions and corporate buyers, making it the ideal place to showcase your leading-edge innovations, best practice solutions and world-class technologies in the Middle East.

**SHOWCASE YOUR BUSINESS TO A GOVERNMENT
AND PRIVATE SECTOR BUYING AUDIENCE!**

BOOK YOUR STAND TODAY!

NEHME SHEHAB - Group Sales Director ■ Tel.: +971 2 409 0346 ■ E-mail: nehme.shehab@reedexpo.ae

Platinum sponsor



Organised by



abudhabipolice
@abudhabipolice
theabudhabipolice
moiaue

» MARKET ANNOUNCEMENTS

Cloud-based Services Adoption on the Rise – but Challenges Lie Ahead

Digital Guardian and Quocirca's latest report shows the challenge for many UK organizations will be not whether to accept cloud-based services, but how well prepared they are for their adoption.

The report found that the number of businesses identifying as "enthusiasts" of cloud-based services has doubled in two years, whereas those actively avoiding them has dropped by almost two thirds.

As interest in cloud-based solutions grows, confidence in data security is incredibly varied. The report highlighted that only 41% of enthusiasts were confident about their data security, showing that whilst cloud popularity increases, there is still a long way to go before businesses feel their data is secure.

Whilst enthusiasts view IT security as a key enabler, avoiders of the cloud consider it a key reason to minimize use of cloud-based services.

Luke Brown, vice president and general manager of EMEA services commented: "The business case for the use of many of the cloud services is now so strong that it's pretty much irreversible. What's important is that organizations ensure that in today's modern hybrid IT environment, data remains protected at all times."

Bringing Data and Memories Back to Life

Cardwave's new data recovery service, Data Resus, is launching this autumn. The new service by Cardwave Services Ltd will recover all types of digital media including USB drives, memory cards and hard drives.

The move to offering a data recovery service is a natural choice for Cardwave given its experience in flash memory over the last 10 years. Together with its research partner, Cardwave has developed the latest generation software packages and hardware tools for recovering data from all types of media.

Recover data from:

- Hardware failure
- Human error
- Power related problems
- Flood / water damage
- Fire / heat / smoke damage
- Vandalism and sabotage



A new website will be launched in the autumn at www.dataresus.co.uk

edgescan Features in Two Gartner Categories

edgescan, a leading provider of web application and server risk management solutions recently announced that it has been added to Gartner's *Magic Quadrant for Managed Security Services 2015*.

The Gartner *Magic Quadrant* is the go-to resource for an objective perspective on technology and service markets. In Europe alone, Gartner is aware of more than 80 managed security service providers. Selections are based on analyst opinion and references that validate IT provider claims.

edgescan has also been listed as a "sample vendor" in the Gartner *Hype Cycle for Application Security, 2015*.

Rahim Jina, director with BCC Risk Advisory, edgescan's parent company, explained: "This validates our approach to vulnerability management. After providing Gartner with numerous vendor briefings, our approach to combining both Layer-7 (Web Applications) and hosting infrastructure vulnerability management as one service is proving positive."

Japanese Banks Deploy VASCO Solutions to Tackle Cyber-fraud

With the Japanese market experiencing an increase in losses from fraud due to phishing and man-in-the-middle attacks, VASCO's secure authentication solutions proved popular in Japan this summer with both Sumitomo Mitsui Banking Corporation (SMBC) and Jibun Bank choosing to deploy VASCO's DIGIPASS for Apps.

In the case of SMBC, it has expanded its use of VASCO Authentication Solutions through the use of DIGIPASS for Apps with Mobile OTP. The solutions form part of a bid to reduce fraud, while also enhancing convenience for its online retail banking customers, offering them a highly-secure mobile banking solution that has been developed with VASCO's DIGIPASS for Apps for their Smartphones. This is the bank's third major implementation of an authentication solution.

Meanwhile, Jibun Bank Corporation implemented VASCO's DIGIPASS for Apps and VACMAN Controller in an effort to enhance security for online and mobile banking customers. The bank claims that DIGIPASS for Apps was the only solution that met all of its requirements. The bank opted to embed an additional authentication feature into its self-developed mobile banking application using the DIGIPASS for Apps Software Developer Kit. Jibun bank believes this the first implementation of electronic transaction signing in a mobile banking application.



Security Apps Top Business Agenda in Latest Good Technology Report

With organizations adopting an increasing number of apps to secure corporate information, Good Technology's latest quarterly *Mobility Index Report* states that 67% of businesses now deploy two or more apps beyond email to mobilize content and strengthen cyber-resilience. This is a result of accumulating pressure from employees for secure access to corporate information behind the firewall on mobile devices, resulting in secure browsers being the most frequently used apps in the workplace, representing 21% of all apps deployed.

The desire for security through mobility is also spread widely across industries. The report found that secure browsers had double digit adoption in all but one case. After high tech, insurance and manufacturing sectors are the most frequent adopters of secure browsing apps, indicating that remote access to corporate data is a key business need across the board.

In response to the report's findings, chairman and CEO at Good Technology, Christy Wyatt, said: "We continue to see security at the heart of every enterprise conversation, coupled with end user privacy concerns. Now more than ever, organizations require a platform that enables them to deploy secure-based apps while protecting end user privacy with containerization."

Advanced Modular Console Manager

Lantronix has announced the worldwide availability of the USB I/O module for the Lantronix SLC 8000 – the industry's first modular console manager. The USB I/O module leverages the modular design of the Lantronix SLC 8000, allowing IT professionals to easily support a variety of interface combinations including RS-232 and USB for secure out-of-band management.

With 91% of data centers experiencing unplanned outages in 2013-2014 costing an average of £577,156 per outage, an optional dial-up modem or cellular gateway is available to provide out-of-band access if the network is down. This reduces downtime and increases response efficiency so that IT incidents are resolved quickly and with minimal or zero network disruption.

The SLC 8000 provides IT managers with future-proof critical infrastructure management capabilities and robust encryption suitable in finance, healthcare and other commercial applications where protection of privacy is critical.

The SLC 8000 Advanced Console Manager also:

- Simplifies service deployments and balances CAPEX and OPEX with its modular design
- Enables custom 'mix-and-match' configurations with USB and RS-232 (RJ45) device port modules
- Minimizes cable clutter with software-reversible device port pins
- Protects management interfaces with authentication and FIPS 140-2 compliant security
- Simplifies service deployments with quick expansion and customization



Best Overall Value

Info-Tech Research Group, an IT research and analysis company, recently released a report naming Linoma Software's GoAnywhere managed file transfer (MFT) solution as having the highest Value Score of the MFT vendor group in Server-to-Server and Ad Hoc Enterprise use cases.

Info-Tech Research Group defines a Value Score as an index of "each vendor's product offering and business strength relative to its price point. Vendors that score high offer more bang-for-the-buck (eg, features, usability, stability) than the average vendor."

The findings were released in Info-Tech Research Group's report, entitled *Select and Implement a Managed File Transfer Solution*, which lays out numerous criteria for designating MFT products and evaluating products in that market niche.

According to the report, "With enterprise-level controls and rigorous audit logs, GoAnywhere ensures strict security policies and compliance regulations are met, regardless of industry. The product is FIPS 140-2 certified and is compliant with PCI DSS, HIPAA, HITECH, SOX, and GLBA. Its ability to connect and interface with multiple technologies provides a versatile solution in disparate environments."

Further details on Info-Tech Research Group's Managed File Transfer Vendor Landscape are available at <http://go.linomasoftware.com/infotech2015>.



Latest Study from Barracuda Networks

Barracuda Networks recently commissioned analyst firm, Freeform Dynamics, to conduct a study on the impact of new business practices on existing IT infrastructure and security in the European mid-market. The study of over 600 IT and business professionals identified a number of emerging trends that are placing a strain on existing IT infrastructures, as well as significant confidence gaps amongst those tasked with adapting these infrastructures to meet new demands.

The three emerging business trends cited as having the greatest impact were: the growing use of cloud for business critical functions (69%); the increase in remote and mobile access to business networks (62%); the general increase in volume and density of network traffic (58%). The three areas anticipated to cause the most problems in the future were: new and changing compliance regulations (34%); use of cloud-based infrastructure (34%); M2M connectivity and IoT (32%). The areas identified as being most affected by increasing network demand were: network performance (74%); network reliability (66%) and security (66%).

"The effects of rapidly evolving business practices in existing infrastructure are clearly highlighted in the findings of this research," said Tony Lock, IT industry analyst, Freeform Dynamics. "With almost everyone we spoke to having concerns, it is clear that a large proportion of mid-level businesses have significant work to do to improve their capabilities and prepare for the future."



Publication Helps IT Security Managers Understand Current Security Issues

The fifth issue of the *Wick Hill Guardian* is now available on-line from Wick Hill – or as a mailed-out printed version. With its aim 'To Advise, Not Advertise', the Wick Hill Guardian is a great read for IT security managers looking to understand more about existing and future security issues, as well as suggesting the type of solution best suited to deal with them.

Barry Mattacott, marketing director at Wick Hill, commented: "The *Guardian* features authoritative articles from some of the world's leading experts in IT security. It's an informative and entertaining read, which will help IT security managers navigate their way through today's rapidly changing IT landscape."

Leading companies who have contributed features include: WatchGuard, Kaspersky Lab, Check Point Software Technologies, Tenable Network Security, BeCrypt, Threat Track Security and of course, Wick Hill.

The wide range of security topics covered includes the growing problem of mobile malware; how to handle encryption; and the growing prevalence of DDoS as an attack vector.

To view the Wick Hill Guardian online, or request a mailed-out hard copy, please visit: www.wickhill.com/guardian



Manage, Visualize and Control Security Policies

Tufin recently announced the launch of the latest release of the award-winning Tufin Orchestration Suite R15-2, which reduces the attack surface and increases security controls across heterogeneous networks. R15-2 enables organizations to efficiently manage, visualize and control security policies across their entire physical network and hybrid cloud platforms through automation and analytics.

Tufin Orchestration Suite R15-2 offers improved security through automated application connectivity decommissioning and adds additional controls for compliance needs such as NERC and PCI DSS 3.0. New visibility and control capabilities are also available for OpenStack private and public clouds.

This new release also introduces a raft of other enhancements including

new capabilities to improve workflow automation, scalability, reporting, topology analysis, policy browsing and authentication, as well as support for a wider range of third-party products and services.

Ofer Or, VP products at Tufin, said: "The *Verizon Data Breach Investigation Report 2015* estimated that \$400m is lost from compromised records and 60% of incidents can be attributed to errors made by administrators. Only through effective security orchestration can organizations hope to guard effectively against the growing threats we face from ever-more sophisticated and determined hackers. That's why we've focused on security as well as agility to make it simpler and quicker than ever for our customers to ensure policy compliance and minimise the risks to their organizations."

LockLizard's PDF DRM Browser Viewer Gets Updated for Windows 10

LockLizard Web Viewer, which enables DRM protected PDF files to be viewed in a browser



without requiring installation of any software, has been updated to include support for Microsoft Edge, multiple simultaneous user logins (so more than 1 user can share the same login credentials), own branding and customization options, and the ability to categorize documents.

LockLizard Web Viewer delivers a flexible, granular and secure document DRM solution for PDF documents that enables document publishers to control who can view documents, for how long, where and when.

LockLizard PDF Security is used worldwide by fortune 1000 companies, governments, small and large publishers, training companies and research institutes, preventing unauthorized use and misuse of their information. www.locklizard.com

DiskShred Awarded Coveted Distinction With Honors ADISA Certification

Following a recent audit, DiskShred, a market leader in on-site secure hard drive destruction, has been awarded the ADISA certification, achieving the highest level of the accreditation; a Distinction with Honors. This achievement is held by just four other members in the UK.

Philip McMichael, MD at DiskShred, commented: "This is the fourth year that we have received the level of distinction and due to the ongoing commitment of our staff we have further improved to achieve the Distinction with Honors. This reiterates the commitment DiskShred have to retaining the highest level of security and compliance throughout our business processes. We've worked hard to ensure that we maintain first class standards, reinforcing to our clients that the security of their data is our top priority."

Launched in 2010, the ADISA IT Asset Disposal Security Standard was started to improve the quality and security of service offered by data and IT disposal providers. By adhering to ADISA's regulations, DiskShred continues to assure customers that data-bearing IT assets are being disposed of securely, responsibly and in accordance with Data Protection legislation to the highest industry standards.

Book Review: Obfuscation, Helen Nissenbaum & Finn Brunton

Reviewed by
Mike Hine

Title:	<i>Obfuscation: A User's Guide for Privacy and Protest</i>
Author:	Helen Nissenbaum, Finn Brunton
Pages:	144
Publisher:	The MIT Press
Price:	\$19.95/£13.95

There's a growing canon of literature both academic and generalist that confronts digital surveillance. Such texts typically set out to examine the myriad ways in which every facet of our lives, on and offline, can and is being recorded by technology; assess the alleged purpose of this surveillance; and explain what we, as a society, could or should seek to do to challenge such activity.

Obfuscation, A User's Guide for Privacy and Protest is a work of academia, but is nonetheless readable and engaging. Indeed, it begins with a rousing call to arms: "We mean to start a revolution with this book."

However, its authors are not inviting readers to take up physical weapons, but rather a repertoire of digital, obfuscatory techniques designed to tackle spying mechanisms of all types. As the authors demonstrate, the reasons that someone might want to obfuscate are many (to prevent profiling, hide identities, as an act of protest etc.) as are the methods and likelihood of success. The odds are stacked heavily, the authors state, against the individual in power relationships whereby providers of essential services hold all the cards, and

unfortunately whole banks of our usage and behavioral data.

The first section of the book chronicles obfuscation through the ages, and explores how individuals have been seeking to fool surveillance mechanisms both human and automated. The potential applicability of obfuscation to each and every one of us nowadays is self-evident, and whether you see such fears as an

indicator of paranoia or common sense, there's little doubt that this short book is a handy user's manual-cum-manifesto for anyone who wants to stick two fingers up to search engines, face recognition cameras on our streets, advertisers, and so on.

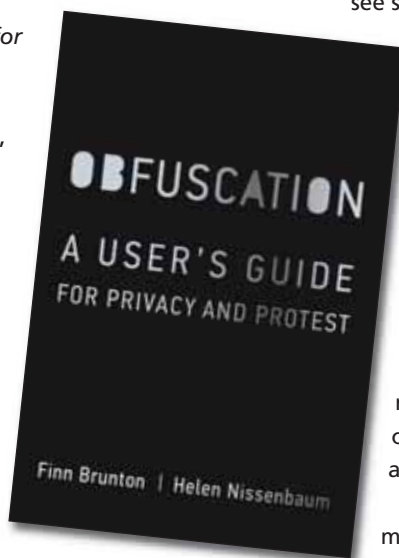
One of the book's main strengths – and where it strays farthest in academic territory – is in its examination of the ethics of obfuscation. After all, by poisoning data sets or committing acts of obfuscation against consumer services, the obfuscator could, inadvertently, be disadvantaging other users of the systems.

One example would be databases used by law enforcement to identify terror suspects. To what extent should individuals seek to trick and obfuscate against systems of this kind?

The philosophical and moral implications of obfuscation are examined in detail by the authors, here, and they offer a range of compelling arguments setting when and where obfuscation is ethical, just and fair. Such decisions rely heavily on both the means and ends of the surveillance system in question, and the nature of the power asymmetry in evidence.

Helen Nissenbaum, one of the book's authors, is a developer behind the TrackMeNot software which generates and bombards false search engine queries for the user, counteracting the effect to which location data and other types of profiling can be carried out with a user's search history. Her credentials in this arena are proven, and both her and co-author Finn Brunton's knowledge and understanding of both the technological and philosophical facets of privacy and security are unimpeachable.

Even though it is by no means a light read (what would one expect from MIT Press), *Obfuscation* is an invaluable resource for anyone interested in wresting back some control over the privacy of their actions in a world where it's never quite clear who is listening, watching and tracking each and every one of us.





Slack Space

Kicking Against the Man

Who needs DDoS when you can take down technology the old-fashioned way?

That was the rationale of Long Island, NY resident Stephen Ruth, who used a painter's pole to tilt red-light cameras at four different stoplights up and away from traffic. He also recorded the stunts with a selfie stick and posted them on Facebook, saying that he just saved taxpayers \$10,000 in traffic tickets. His other rationale? To keep the big, snooping government from taking advantage of its citizens.

"To all the people thinking 'why would he do that? Didn't he think he was going to get arrested?' of course I knew I would be arrested," he said in his Facebook post. "I did it for the people who come back from war and get abused by these cameras. I did it because senior citizens are getting these, the same ones that went to war for us. These same seniors live in New York's high-cost environment and are being forced out of New York because of its high taxes."

Ruth was taken into custody charged with four counts of criminal tampering.

Giant Waterslides Invade the UK

Who doesn't love a giant slip-n-slide? No one, that's who!

And armed with this knowledge, someone made a big splash, as it were, on Facebook, in time for the UK's end-of-summer bank holiday on 29 August.

No less than 50 Facebook pages appeared in August purporting to represent a range of cities and towns in England, promising "the most exhilarating water event to ever hit" the community. The pages spoke of riding on an overgrown, giant version of the popular garden-hose-powered backyard waterslide, with free admission, and visitors were told to "be ready for the ride of your life!" They were also encouraged to "JOIN, SHARE the Event & INVITE your friends!"

Irresistible. From Bristol to Manchester, thousands joined, shared and invited... but (downer alert) none of the municipalities had any such plans for such a summer-tastic event. Which, given the generally tropical, warm nature of English summers, and the multiplicity of large outdoor swimming pools throughout the country, especially in the north, should be surprising... oh, wait.

"How can this be happening in Hull? There are no public open air pools," commented one killjoy Facebooker.

So did the hoaxer simply have a deep, deep love of water-sliding? Unlikely. Instead, it seems a brilliant way to collect personal information to sell. Who needs spam when you can splash?

Not a Bundle of Joy

File under gross: someone has been trolling expectant mother groups online, stealing 'baby bump' photos and posting them on so-called 'preggophilia' sites.

The Australian Multiple Birth Association (AMBU), New Zealand Multiple Birth Association, and Multiple Births Canada, all of which cater to parents with twins, triplets or more, said that people were signing up under fake names, and then going on to ask for photos of pregnant bellies.

"We have been informed of a bogus person joining Facebook groups and our administrators are on high alert," Ali Mountifield, AMBA communications director, told the Australian Broadcasting Company. "Pregnancy is a sacred time. Photos should be shared with whom you choose, in the way that you wish, not stolen for the gratification of others. We wanted to raise the alert as it's an international problem and it's not just related to those expecting twins, triplets or more."

Some preggophilia websites offer explicit sexual content, while others are just galleries of 'bump' pics. Either way... eww.

Hacking in the Sun

Nearly 90% of Brits throw cybersecurity out the window when they go on holiday.

Whether all-inclusive in Mallorca or renting



An open air water slide in Hull... too good to be true?

a caravan in Cornwall, going on holiday apparently means taking a break from cyber-protection too. According to research from Intel Security, the majority access open, public Wi-Fi while traveling, without a security product installed on their device.

The 18 to 24-year-old set are the most reckless – in-between mojitos and tanning, over a third (38%) said they'd connect to open Wi-Fi while on holiday, with just 6% claiming to have a security solution installed.

By comparison, the over-55s were much more risk averse, with just 5% claiming they'd use Wi-Fi abroad in the same way as they do in a secure environment at home.

Public Wi-Fi is of course a fertile field for cyber-criminals looking to intercept log-in credentials for valuable online accounts, lift credit card information, mine personal information and more; and even if one is, say, lounging by a pool in the Mediterranean sun, it's worth keeping that in mind.



Anyone who wants to share their grumbles, groans, tip-offs and gossip with the author of Slack Space should contact infosecurity.press@reedexpo.co.uk



Parting Shots

On the 'softer' side of the security debate, there are three issues that crop up repeatedly: recruitment, skills, and employee education. In each case, problems arise due to a perceived shortage of some kind.

Recruiting in security is hard because finding and keeping skilled personnel is made difficult by a low ratio of jobs to candidates. The skills shortage is so hard to combat because of a historic lack of programs to nurture young talent into cybersecurity from an early age, and also to convert computer science and IT graduates into pure play security professionals. And employee education is hindered by both a lack of general awareness around security hygiene, and a lack of effective means through which to deliver training that really works.

But it is not through want of trying that these issues keep cropping up. There are a number of organizations dedicated to training the next generation of cybersecurity talent and fill the job market. Think of the SANS Institute, or the UK's government-backed Cyber Security Challenge. On the employee education side, there are companies dedicated to providing cyber-awareness among employees, such as PhishMe or Wombat Security, and (ISC)² is reaching out to youngsters in classrooms through its Safe and Secure Online program.

There are initiatives and lots of passionate security professionals out there working tirelessly to spread the word. It is often argued that, as information security, or data privacy, or cybersecurity – whatever your preferred term – is such a relatively new concern for businesses and citizens, it will take time for behaviors to change across society to meet the demands that threats to our data place on each of us. It will take

time, too, for schools, colleges and universities to catch up and integrate proper education about security – everything from cyber-bullying to the technology skills required for proper security.

So, is it safe to assume that, with time, and the continued dedication of non-profit

groups and businesses which aim to promote security training and awareness, that the recruitment gaps, skills shortfall and lack of employee education will be mitigated? Not necessarily.

Education needs to be effective for it to sink in – in many cases more effective than what is currently offered within organizations. Indeed, it's clear from a number of studies that employee behavior around data is not getting any more security savvy, despite the constant wave of breaches in the media.

A report from Intercede in August found that, of a sample of 2000 UK and US 16 to 35-year-olds, just 5% had full trust in existing safeguards to protect against data loss online. Only 6% believed their own password use practices adequately protected them from fraud. There also seems to be a disconnect between the low faith that youngsters and young adults have in the security of their information, and their willingness or ability to take proper action to step up their security. Around half of those surveyed by Intercede never change passwords unless forced to.

Research from Intel Security, meanwhile, discovered that 90% of Brits aged 16 to 24 don't have a security product installed on their mobile devices. Nearly four in 10 would connect to open Wi-Fi when holidaying abroad.

It would also seem that it's not just the younger generation. According to a recent

Accenture study, nearly two-thirds (63%) of C-suite executives say that their companies experience significant cyber-attacks daily or weekly, but just a quarter say their organization always incorporates measures into the design of their company's technology and operating models to make them more resilient.

Is this down to a lack of both willingness to act or education about how to act? It's most likely a blend of both. Clearly, cybersecurity's profile is rising, and as it does so people's awareness of the issues is growing. It's not considered esoteric knowledge that poor password hygiene and low privacy settings on social media put users at risk. Turning awareness of these basics into action is the conundrum – and it's one that isn't being answered satisfactorily.

Much of the answer lies in getting to youngsters early in their and starting education as soon as kids' hands are strong enough to grip a phone or tablet. There may also have to be a subtle rethink about messaging. When I recall my own school days – road safety was a big one. The message was most effective when it combined shock tactics with emotional



Employee behavior around data is not getting any more security savvy, despite the constant wave of breaches in the media



impact. A case study or speech from someone who's been personally affected would never fail to capture attention and make us think twice. Could the same work for cyber? I'm not one to advocate scare tactics, but given that it's still very much a case of 'once bitten twice shy' with cyber, there needs to be a rethink before proactivity and security become easy bedfellows.



Mike Hine, Deputy Editor

SECURITY AT YOUR FINGERTIPS - FREE

-  Asset Inventory Service
-  Website Security Audit
-  OWASP Top 10 Scan
-  Patch Tuesday PC Audit

-  SSL Secure Website Test
-  BrowserCheck
-  Top 4 Security Controls
-  SCAP Computer Audit

[QUALYS.COM/SECURE](https://qualys.com/secure)



QUALYS®

ADVANCE YOUR CYBER SKILLS AND CAREER

Train for the new performance-based CSX Practitioner Certification. Acquire hands-on instruction in a cyber-lab environment—available through CSX certification training partners. Embrace skills aligned with globally recognized NIST Cyber Security Framework domains. Gain the certification that affirms your readiness to be an in-demand first responder in the global cyber security workforce.

Start now at: www.isaca.org/CSXCert