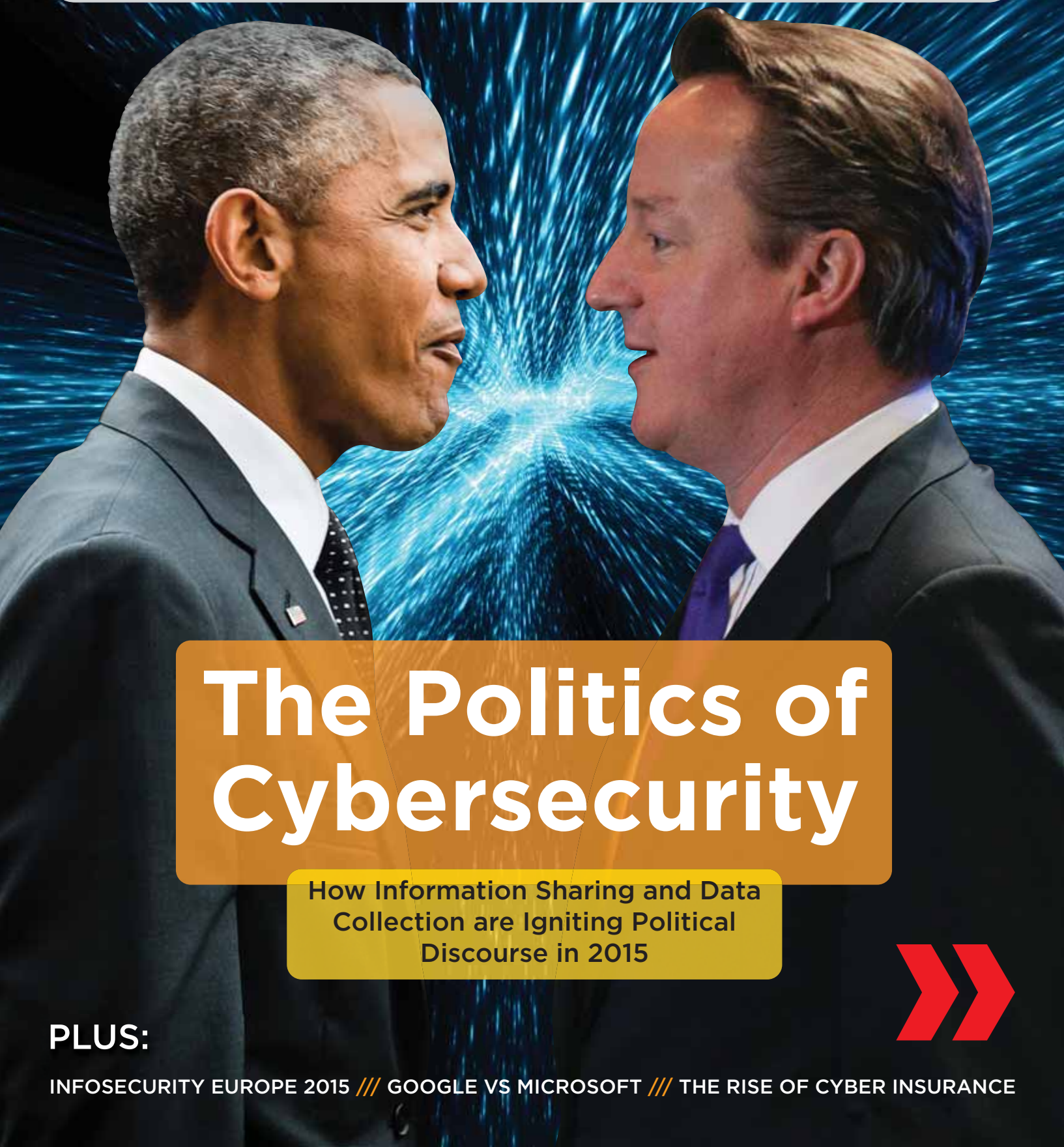


Q2 /// 2015 /// VOLUME 12 /// ISSUE 2

STRATEGY /// INSIGHT /// TECHNOLOGY

info security



The Politics of Cybersecurity

How Information Sharing and Data Collection are Igniting Political Discourse in 2015

PLUS:

INFOSECURITY EUROPE 2015 /// GOOGLE VS MICROSOFT /// THE RISE OF CYBER INSURANCE



THE NEXT GENERATION CLOUD SECURITY PLATFORM

Bringing Continuous Security to the Global Enterprise



FOR A FREE TRIAL
VISIT QUALYS.COM/CONTINUOUS



Contents

APRIL/MAY/JUNE 2015

INFOSECURITY EUROPE 2015

26 WELCOME



26 SHOW FACTS

30 KEYNOTE STAGE AGENDA

32 INTELLIGENT DEFENCE: EUROPEAN
TECHNICAL RESEARCH
CONFERENCE AGENDA

34 STRATEGY TALKS AGENDA

36 TECH TALKS AGENDA

38 INFORMATION SECURITY EXCHANGE,
TECHNOLOGY SHOWCASE & CYBER
INNOVATION SHOWCASE

39 NEW PRODUCTS & SERVICES GUIDE

40 SECURITY WORKSHOPS &
SECURITY TRAINING

42 NEW FEATURES

46 EXHIBITOR LIST

CELEBRATING 20 YEARS

02-04 JUNE 15
OLYMPIA LONDON UK

COVER FEATURE

14 Cybersecurity from Capitol Hill to Whitehall

Proclamations on cybersecurity and government surveillance have ignited political discourse in early 2015. Wendy M. Grossman cuts through the spin

FEATURES

18 The Rising Cost of Cyber-Insurance

You can insure yourself against cyber-attack, says Danny Bradbury, but be warned, prices are going up

22 Google vs Microsoft: Let the Patch Wars Commence

Phil Muncaster investigates whether an ongoing dispute between Google and Microsoft could change the way we fix security flaws in the future

49 Tales from the Crypt: Hardware vs Software

Encryption is never out of the spotlight in this industry, but the methods that businesses can deploy to encrypt their data are wide-ranging. Daniel Brecht examines the pros and cons of the various solutions on offer

POINT-COUNTERPOINT

52 People are the Most Important Piece of the Cybersecurity Puzzle

When it comes to strategic investment in security operations, KPMG's Stephen Bonner argues that people should take precedence over the latest, shiniest tools

53 In Re-assessing Security, Technology Holds the Key

Prioritizing investment in perimeter-agnostic and data-centric technologies is how companies can keep from being tomorrow's data breach headline, writes Watchful Software's Charles Foley

OPINION

58 Decoupling Encryption: Building Bridges Between CISO and CTO

Certes Networks' Paul German argues encryption's role must change

REGULARS

4 EDITORIAL

Eleanor Dallaway says farewell – for now – and looks back on some of her highlights from almost a decade in the industry

6 NEWS FEATURE

Whether meddling kids or a serious menace, Lizard Squad is part of a phenomenon that is here to stay, concludes Fahmida Rashid

10 INTERVIEW

Eleanor Dallaway interviews Intel Security's CTO, Raj Samani, a man so passionate about infosec that he turned a weekend at Legoland into an infosec lesson for some of the park's young visitors

54 MARKET ANNOUNCEMENTS

Product news from the vendor space

59 SLACK SPACE

Car-wash hacks; pay-by-selfie; and USB's turned computer-killer

60 PARTING SHOTS

Deputy Editor Mike Hine confronts the issue of information overload

INFOSECURITY

EDITOR & PUBLISHER

Eleanor Dallaway
eleanor.dallaway@reedexpo.co.uk
+44 (0)208 9107893

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:

Elex van Rensburg
elex.vanrensburg@reedexpo.co.uk
+44 (0)20 8910 7810

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
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



Goodbye For Now

As of June 4, I will be taking a break from the world of information security to bring my very own mini @InfosecEditor into the world.

As I get ready to send to press what will be the last issue of *Infosecurity* that I work on for a year, allow me to indulge in a trip down memory lane as I pick nine of my favourite memories from my nine years at the best information security magazine and news site there is.

9: Woman of Influence

When Microsoft nominated me for the 'women of influence' awards at the EWF event in 2013, I was humbled and honored. I flew out for the awards, entirely expecting to come home empty handed but content having spent a week at the incredible Gainey Ranch in Scottsdale Arizona with a couple of hundred inspiring women from the world of information security. Winning the accolade was just the icing on the cake.

8: Digital Evolution

When I joined *Infosecurity* in 2006, we had a static website, and a print magazine. In 2008, I launched our webinar series and virtual conferences. Seven years later, we run astoundingly popular weekly webinars and quarterly virtual conferences. More than 10,000 people attended our 2014 summer virtual conference, and our webinar channel reaches over 350,000 infosec professionals. That's a digital evolution to be proud of.

7: Gong After Gong

I first won my own BT journalism award back in 2008, but better still has been attending the awards every year and picking up award after award for *Infosecurity* features. We've never walked away empty-handed and usually scoop multiple gongs, testament to our diligent, cutting-edge reporting and editorial integrity and excellence.

6: Let the Show Commence!

I've survived nine Infosecurity Europes, but only four of them as an 'insider'. Infosec is a crazy week for anyone attending, but for the show team behind Europe's number one information security event, it's carnage. But nothing beats the buzz, or the intense work that brings the team together.

5: Interviewing Paul Judge

Writing the profile interviews for each issue of *Infosecurity* ranks pretty highly on my list of why I love my job. But my all-time favourite was Dr Paul Judge, a serial entrepreneur and noted scholar, whose passion for business and life left me completely in awe. I've enjoyed interviewing Judge on multiple occasions since, but more enjoyable still were the tens of bottles of incredible wine we've enjoyed – along with a limousine full of wonderful infosec people and friends – in Napa Valley after RSA finishes each year.

4: Relaunch, Revitalize

It took about two years from planning to live launch, but when we finally set our brand new website live last summer, I was as proud as punch. Huge kudos goes to Rebecca Harper, for leading this project through completion, and to Carlos Gomez-Rios, our then project co-ordinator, whose technical expertise and imagination contributed greatly to the success of the new site. Eight months on, it's still a shiny new toy that I can't get enough of.

3: Traveling the World

My very first overseas conference is special to me for many reasons. I was young, eager to travel, and couldn't believe my luck as I arrived in Orlando, eager to learn about an industry then alien to me. Since then, I've travelled to eight RSAs in San Francisco, five Black Hats in Vegas, and attended events in Miami, Seattle, Denver, Chicago, New York, Washington DC, Philadelphia, and Arizona. Closer to

home, I've been lucky enough to travel to Israel, Russia, and tens of other countries that column inches dictate I omit. Not only have I seen so much of the world, but the industry is no longer alien to me, and more importantly still, nor are the people in it. I've made friends that I know will last a lifetime.

2: Two Become One

In 2011, *Infosecurity Magazine* and Infosecurity Europe merged to create the Infosecurity portfolio, bringing together two power brands to create a one-stop-shop for industry, and a singularly authoritative source of information for the industry. I gained a whole new team of wonderful colleagues...and we've never looked back.

1: People, Wonderful People

And finally, there could be no highlight greater than all of the amazing people I've been lucky enough to work with over the past nine years, both colleagues and industry friends. These are the people that make saying goodbye – even if it is only for a year – very difficult.

I'll be at Infosecurity Europe for my last hurrah and would love to see as many of you as possible, so please do find me at the *Infosecurity Magazine* booth.

Now that I'm feeling appropriately nostalgic, all that's left to say is thank-you to all of our readers, and anyone who has contributed to the above nine memories. I'll see you in 2016.

Until then,
keep reading
and take care.



**Eleanor
Dallaway,**
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**



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

Matt Booher
President
WIS:DOM Information Systems



Lizard Squad: Original Pranksters



Whether meddling kids or a serious menace, Lizard Squad is part of a phenomenon that is here to stay, concludes **Fahmida Rashid**

Last year, over Christmas, millions of gaming fans were outraged when distributed denial of service (DDoS) attacks took down Xbox Live and Sony's PlayStation Network. A group going by the name Lizard Squad claimed responsibility. This was the same group behind the server outages for popular online games *League of Legends* and *Runescape* in August.

In 2015 alone, Lizard Squad has already claimed responsibility for hijacking the websites of Malaysia Airlines, Lenovo, and Google Vietnam.

The group's sole motivation for these attacks – based on its Twitter activity – appears quite simple: because they can. The group considered the Christmas attacks against Xbox Live and PlayStation Networks to be a “sort of a game” carried out for its own amusement, a self-proclaimed Lizard Squad member said in an interview with the UK's Sky News.

Lizard Squad is becoming a household name because it is prolific, but also because its activities are so visible, says Andrew Hay, director of security research at OpenDNS. The group has relied mainly on DDoS attacks to cause server outages at heavily-trafficked sites. It hasn't defaced actual company

websites, but rather redirected users to spoofed websites to make it seem like the pages are compromised.

“I hesitate to call Lizard Squad hackers,” Hay says, noting that hackers generally have a call-to-action, a reason for engaging in the attacks. ‘Pranksters’ is a better description, he suggests.

Cyber-attackers are generally categorized by their motivations. Nation-state attackers further the government's goals, whether that extends to espionage, sabotage, or theft. Cyber-criminals are financially motivated and typically focus on stealing money or valuable assets. Hacktivists are ideologically motivated, and their activities are typically designed to draw attention to something they care about, such as promoting free speech or protesting child pornography. Lizard Squad doesn't quite fit into any of these brackets.

For the Lulz

Lizard Squad's activities may evoke memories of LulzSec, an earlier hacking group which took on some high-profile organizations and websites in 2011. Even though LulzSec picked its targets based on ‘lulz’, or laughs, it clearly had hacker roots.



LulzSec was originally a disillusioned offshoot of the hacker collective Anonymous intent on exposing “just how bad things were” with security at some of the world's largest brands, Hay explains. Lizard Squad, in comparison, is “doing what it can for fun.”

Dismissing Lizard Squad just because it doesn't have an ideology or employ sophisticated attack methods would be a bad idea, says David Francis, a cybersecurity officer at Huawei UK. He adds that it doesn't matter that the group isn't using sophisticated tactics to disrupt operations and interfere with user experience, because the fact remains that Lizard Squad did succeed in its goals, and there was an impact on reputation and revenue.

“Whether you class Lizard Squad as pranksters or not is irrelevant; the bottom line is that all organizations, large or small, are subject to attacks,” Francis argues.

Tools of the Trade

Organizations operating online should be concerned about the methods the group



uses, says Steve Armstrong, a certified instructor at the SANS Institute. Lizard Squad launches its DDoS attacks using a botnet of compromised routers belonging to home users. Lizard Squad also put Lizard Stresser, a DDoS tool which uses the botnet to launch its own attacks, for sale on its website.

LizardStresser is an IRC Linux bot which attempts to connect to random IP addresses on the internet with default usernames and passwords. Users who may not have changed the default credentials on their routers may find their network devices hijacked into the botnet taking part in these attacks.

The source code was eventually leaked on GitHub, and some security experts who analyzed the code said it was unoriginal and impressive. It didn't have to be sophisticated – Lizard Squad was able to successfully launch its own attacks, and so were other people who bought the tool. Home routers

are notoriously insecure since device manufacturers may take a while to roll out security updates, and users may not know how to install the firmware, which means LizardStresser will continue to be effective.

A recent analysis by Recorded Future, a web intelligence and predictive analysis company, identified a Windows-based bot client linked to Lizard Squad which has not yet been used.

"It remains unclear what will come of this botnet, but it's related to Lizard Squad and is more capable than LizardStresser," the company said.

Organizations have to understand that DDoS attacks are serious because they impact service availability and inconvenience end-users. If the gamers can't get to the

servers to play, they can get annoyed and move on to other games, Hay says.

While many organizations may work with upstream providers to fight back and try to outlast the attack duration, there is the possibility that organizations may just pay a ransom to make the attackers go away.

This can be risky, because the money "could just encourage more attacks," Hay adds.



Cyber Vandalism

During the DDoS attacks against Xbox Live and PlayStation Network in December, Kim Dotcom offered 3000 free vouchers for Mega, his encrypted cloud storage service, to Lizard Squad to cease its activities. While the vouchers did stop the attacks, Hay was

concerned about the message this payoff gave to Lizard Squad and other hacker groups.

The vouchers were priced at \$99, and there were reports Lizard Squad sold them for \$50 each, netting the group at least \$150,000 in cash. Considering that DDoS attacks have been growing in volume and intensity over the past few years, a potential financial windfall may encourage more groups to launch attacks.

Vandalism and gaming remain the most popular reasons for DDoS attacks, but attacks acting as a smokescreen for data theft and extortion attempts are also on the rise, says Darren Anstee, director of solutions architects at Arbor Networks. These attacks are disruptive, can cause damage to brand reputation, and increase overall costs for the organization. "DDoS attacks cannot be considered pranks," says Anstee.

DDoS attacks aren't the only tricks up Lizard Squad's sleeve. Earlier this year, the group claimed responsibility for a series of website defacements, including the one for Malaysia Airlines. It didn't compromise the airline's site, but likely socially engineered the site's domain registrar to gain access to the airline's domain name system records.

Lizard Squad modified the records to point to a website under its control, but average users wouldn't realize they were on the wrong site. This is a tactic frequently used by other hacking groups, such as the Syrian Electronic Army.

Hijacking DNS records can result in considerable damage to the corporate brand because most users and customers will not realize the distinction and assume the company's servers have been compromised, Hay explains. And if the attackers modify the MX records for the mail server along with the DNS records, then the attackers have access to all the email messages being sent to the company. That has even more serious repercussions to the company's bottom line.

Organizations need to work with their domain registrars to put in mechanisms to protect themselves, such as two-factor authentication and domain locking to prevent unauthorized changes to DNS



Whether you class Lizard Squad as pranksters or not is irrelevant... all organizations, large or small, are subject to attacks

David Francis
Huawei UK

records, Hay says. Organizations should pick registrars which have implemented DNS security extensions (DNSSEC) which users can use to verify the site hasn't been hijacked.

Childish Antics

Whether or not Lizard Squad is just a group of kids with a questionable sense of humor doesn't matter, because it is not the only hacking group engaged in these activities.

CoreSec is another hacking group engaged in similar activities. The group launched a series of DDoS attacks against Finnish financial services group OP-Pohjola from New Year's Eve to 4 January. The group demanded ransom between 10 and 100 bitcoins to stop the DDoS attack. At least one member in the group is a Finn, said Mikko Hypponen, chief research officer of F-Secure. CoreSec's motives for the attack remain murky, but Twitter activity shows CoreSec and LizardSquad consider each other supporters, if not allies, in their cyber-pranking.

The earlier LulzSec is now defunct, with two of its leaders convicted. DerpTrolling has been active more recently, launching a string of DDoS attacks on multiple gaming companies and online gaming servers in early 2014. DerpTrolling was likely just trying to boost its collective ego and its "antics were often childish," security company CrowdStrike noted in its latest *Global Threat Report*.

"Despite their immaturity, the collective was able to consistently carry out DDoS

attacks on targets of their choosing, and these attacks had a real-world effect on the victims within the gaming community," wrote CrowdStrike.

The company also noted that Lizard Squad's antics had real-world consequences beyond the cyber-realm. The group successfully diverted an American Airlines flight carrying a Sony executive by posting on Twitter a rumor about explosives on board. The incident evokes memories of when the Syrian Electronic Army hijacked a media outlet's Twitter account to post a false report about an explosion at the White House in 2013.

"The threat [Lizard Squad] posed to gaming companies was still noteworthy, especially when combined with terrorist threats; although they were bluster, they still had considerable real-world consequences," CrowdStrike reported.

Analysis from Recorded Future attempted to identify members of the group by their interests, vernacular, and lifestyle to provide insight into how they operate. The company examined the group's social media activity for patterns in language and determined the leaders and key members are from the United Kingdom, Canada, or the United States.

Even though Lizard Squad is still seizing headlines, the group's activity has slowed since December, says Christopher Ahlberg, Recorded Future's CEO and co-founder. This may have been spurred by Finest Squad, another group which came to light in December and started reporting Lizard Squad accounts to Twitter for abuse, he says.

Lizard Squad's leaders and key members are most interested in guns, drugs, gaming, and hacking. The intersection of thug-life culture and pro-Nazi sentiments is perplexing, but the fact that one of the accounts associated with the group's leaders frequently expressed pro-Nazi sentiments may be an indicator of the direction Lizard Squad will be heading in, the company warned.

Instead of dismissing the group, it would "be prudent" to take Lizard Squad's warnings seriously in 2015, Ahlberg said.





SEE MORE. SECURE MORE.

**Can you see into even the darkest corners
of your network infrastructure?**

Are you sure?

Because right now, as you're reading this, someone is probably trying to find out. Learn how Gigamon and our extensive partner ecosystem can make sure your confidence isn't misplaced, shining a light across your whole network:

- Physical
- Virtual
- SDN/NFV Environments
- Private & Public Clouds

The Gigamon Visibility Fabric Architecture delivers simple, automated Pervasive Visibility that allows pro-active security and real-time decision making.

Visit Gigamon at infosecurity Europe Stand #D180

Interview:

Raj Samani



CTO. Author. Europol advisor. Information security enthusiast. Husband. Father. And not in that order. **Eleanor Dallaway** talks to Intel Security VP & CTO EMEA, Raj Samani, a man so passionate about his industry that he manages to turn a weekend at Legoland into an infosec lesson for some of the park's young visitors



When I meet with Raj Samani on a Monday morning at the Intel offices in Slough, he's 'fresh' from spending the weekend with his wife and three children on a "rock hard" bed at Legoland, where he indulged in reading up everything he could find on the Carbanak malware news that broke that weekend, and gave a technology career lesson to one of the park's unsuspecting young visitors.

But don't assume Samani has fallen into the trap of workaholic – the Carbanak news is to him what the latest episode of *Game of Thrones* is to some people, and educating children on not only the dangers

of cyber, but the opportunities, is his passion. "I know how to turn my phone off and have dinner with my family," he says. "Reading that news isn't work to me, it's what I'm interested in. If I wasn't doing this job, I would be reading that anyway."

To switch off, Samani is an avid gym-goer, and loves to box. "Mainly, I've learned to listen to my body. If my mind says to me, 'you can't read any more, just watch crappy TV', I'll do that. If my body says to me, 'hey listen – you really can't go to the gym this morning', I'll go back to sleep."

Wearing some pretty big shoes as VP & CTO EMEA of Intel Security, formerly McAfee, Samani could be forgiven for

finding it all a bit too much sometimes. But, he reassures me, he's "happy, really, really happy."

"It's not work to me, sometimes I have to pinch myself and think, 'people are paying me to do this', because I would do this for free."

Those big shoes allow him the ability to "help influence change right across the industry," and whilst Samani has worked at this with industry bodies like ISSA and CSA in previous roles, his current job allows him to "push things on faster and further."

"Would I ever have been able to help redevelop Bletchley Park when I was in the voluntary sector, or working as part of the



Sometimes I have to pinch myself and think, 'people are paying me to do this', because I would do this for free

industry forums and associations? No. Would I have had the ability to be able to stand and speak at some of the biggest conferences around the world? Probably not. Would the white papers I've written ever have got the same exposure? No. So that's why I came to McAfee," Samani explains to me. If those words sound arrogant in print, they didn't in person, and Samani's sincerity is always both refreshing and unmistakable.

I've known Samani for nine years, and when we first met he was working as a CISO in the public sector. I chose him as part of the working group that I was asked to assemble in order to present at the House of Commons to help advise the Conservative Party on their information security policy. Since then, I've always considered Samani an industry 'favorite' and have spent many interviews, lunches, and casual chats enjoying his honesty, sincerity, and passion for the industry. And these encounters are never short...the man can talk!

Just a Skinny Indian Boy from Slough

These are Samani's words, not mine. "I'm just a skinny little Indian boy from Slough, and now I couldn't even tell you which country I'm going to be in next week," Samani laughs, contemplating the path he took from his small home town in Wembley, North London, where he didn't even know the role of CTO existed, to his jet-setting senior position at one of the world's largest technology companies.

"I grew up in a time where technology wasn't ubiquitous. My dad ran a hotel and my mum was an accountant, and we didn't have a computer." That was, until Samani's dad presented him with a Pentium 75, which he taught himself how to use. "Technology allows anybody the ability to be able to explore the limit of their potential," he says. "Technology is agnostic – it's not good, or bad – if you have an appetite to learn, it enables that." And an ability to learn is one of the most powerful skills there is, adds Samani.

It's abundantly clear that beside his family, Samani's passion for learning is the only

thing that trumps his passion for information security. After earning a degree in economics, and a Masters in business information technology from Brunel University, Samani carried on studying whilst working in his first role as tech support at Roche Pharmaceuticals. "See, I've always been a techie," he smiles.

He took 35 professional exams in his 'free' time, and read "any piece of information I could get my hands on, day and night". This included *Applied Cryptography: The Second Edition* which he took on his honeymoon!

Samani even turned to textbooks to overcome his fear of public speaking. "I hated it, couldn't sleep for days knowing it was coming up, but knew I had to face my fear," he recalls. "I started to read about some of the best speakers in the world, their approaches, how they do it." The knowledge he gained, combined with his belief in the 'seven seconds of courage' mentality, allowed him to overcome his fear and accept his first speaking engagement at Infosecurity Europe.

"I always say to my kids, if there's something you're scared of, just be brave for seven seconds." And it worked for Samani, who now loves public speaking, but admits that he still gets butterflies and still gets scared.

These days, his passion for learning finds Samani writing books, not just reading them. "I use writing books as a vehicle to increase my technical understanding on topics where I want a deeper knowledge, like smart grids," he explains. "When I write

my books, my wife is sitting watching *EastEnders*, and I'm next to her searching for places to buy cheaper email addresses for spear-phishing."

His latest project is a co-authored book with Eric Knapp and Christopher Burgess called *The Unsocial Network*, which aims to straddle general interest with technical knowledge, and asks whether we're less social today than we were in the past. "Social networks have changed from being based on physical proximity to being based upon people with which you share common interests. Today, if somebody disagrees with you, you unfollow them. You disconnect them from your social network. So there isn't anybody that challenges our belief system, you only surround yourself with people that reinforce your belief system." Samani hopes that the book will appeal to his wife, "and absolutely everyone else."

No Such Thing as Too Busy

When I ask Samani how he finds time to pen books whilst balancing his day job, family life, and extra-curricular activities (Samani volunteers in schools educating children about cybersecurity, works with MPs on an all-party parliamentary group focused on technology, and acts as a member of the advisory group on internet security at Europol Cybercrime Centre), he answers simply: "You have to make time. There's no such thing as being too busy – it's just not prioritizing stuff." Samani uses his travel time – and there's a lot of that, as he travels weekly – to write, "and the fun part is, it's not even work, because I love doing this."

"This industry isn't just a job, it's a passion. What we do is really important. The industry can be quite depressing, dark, but we have an industry that is working collaboratively, both public and private sector, and many of us [partake in] voluntary efforts outside of normal working hours."

Could we be doing more on the collaboration side? "We could always be doing more, but the reality is that information exchanges and information sharing has been going on for more than

just a few years now. What we need is more real-time intelligence and information-sharing to be able to combat these issues."

Samani considers his job partly reactive and partly proactive, which is why, he explains, there is no such thing as a normal day for him. "It doesn't feel like a job, if that makes sense? It's just something I do." And he plans to do exactly that for the foreseeable future. "I'm certainly not consciously thinking about leaving, but then, never say never, right?"

As a technologist, Samani describes being acquired by Intel as "like Christmas. The breadth and the depth and the capability of the individuals here is just awesome," he gushes. And it's people that continue to inspire him both within and outside the Intel walls. "There are so many people in our industry that are just really good people. A huge part of my social friendship network is from industry – as I said earlier, you attract people similar to yourself." Indeed, it's the relationships and friendships that Samani has made and maintained that he is proudest of.

As for regrets, Samani is fairly philosophical. "Hindsight's a wonderful thing, but equally, mistakes help define who we are. You learn nothing from success, only from failure," he says. "So yes, I have failed on a number of occasions, but I don't see them as failures, I see them as learning opportunities, so I wouldn't change it." His mistakes have helped define who he is today, Samani continues, adding that the industry's lack of risk assessment framework to quantify security is one objective that he is yet to see fulfilled.

The Most Important Job of All

His most important job of all, Samani considers, is being a dad; helping his children navigate the rules of the new technical world that we're moving into is his upmost priority. "I kind of bear this burden of responsibility as a father, but also, as a CTO in this company, that I've got to not only help my kids, but as many people as I can.

"When we look at privacy in the 21st century, it's going to be completely different



Samani with Troels Oerting, signing the MoU with Europol's European Cybercrime Center (EC3)

to how privacy was in the 20th century. There are new rules being created, new societal norms, and we need to help preserve the foundations of trust that we need to operate in this world."

So will Samani be encouraging his children to embark on careers in technology? "I'd just like them to find their passion. I keep saying to my kids that they can do anything and be anything they want." Teaching them a real degree of technical competence is high on his agenda, however, "because that's important not only for their future careers, but generally in society."

Perhaps it's this "burden of responsibility" that is to thank for Samani's involvement in the Europol Cybercrime Centre advisory group. "My work and engagement with Europol is really because of Troels Oerting's vision. He recognized that cybercrime isn't something that the public sector can do alone, and so began this process of putting together this advisory council of special advisors.

Samani's admiration for Oerting is apparent, and he applauds the collaboration he has enabled between law enforcement agencies across the world, in addition to the private-public partnership. "The fruits of his vision and the fruits of his labor have been recognized in some of the takedowns and efforts we've seen over the last 12 months."

So what's next for Samani? "There used to be a time when I could almost map out my life. I'd tell you when I would be married, when I'd have kids, where I'd be working, and what sort of money I'd be earning," he says, pausing to reflect. "And now, actually the most exciting thing is that there isn't a path set out for me."

A self-confessed over-analyzer, and his own biggest critic, whatever does come next will undoubtedly be met with the same commitment and passion that Samani affords to everything else in his life. "My goals are always changing," he admits, with that mischievous grin that is synonymous with the Intel Security CTO. Not bad for a "skinny little Indian boy from Slough."





Protecting your enterprise from threats you can't see requires unified security intelligence.



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 today at logrhythm.com/simm

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



Cybersecurity from Capitol Hill to Whitehall



Proclamations on cybersecurity and government surveillance have ignited political discourse in early 2015.

Wendy M. Grossman cuts through the spin to find out what this means for technologists and citizens

Early 2015 saw multiple announcements on cybersecurity from US president Barack Obama and British prime minister David Cameron. Both were responding to recent events, primarily the Sony hack (which is estimated to have cost the company \$15m) and the shooting in France of 11 staff at the satirical magazine *Charlie Hebdo*. The two countries also announced joint 'cyber wargames', whereby teams from each country will attack the other to test critical infrastructure.

Obama proposed improving cybersecurity information-sharing between government and the private sector; criminalizing the overseas sale of stolen US financial information; extending the RICO laws to include cybercrime; and requiring national data breach reporting.

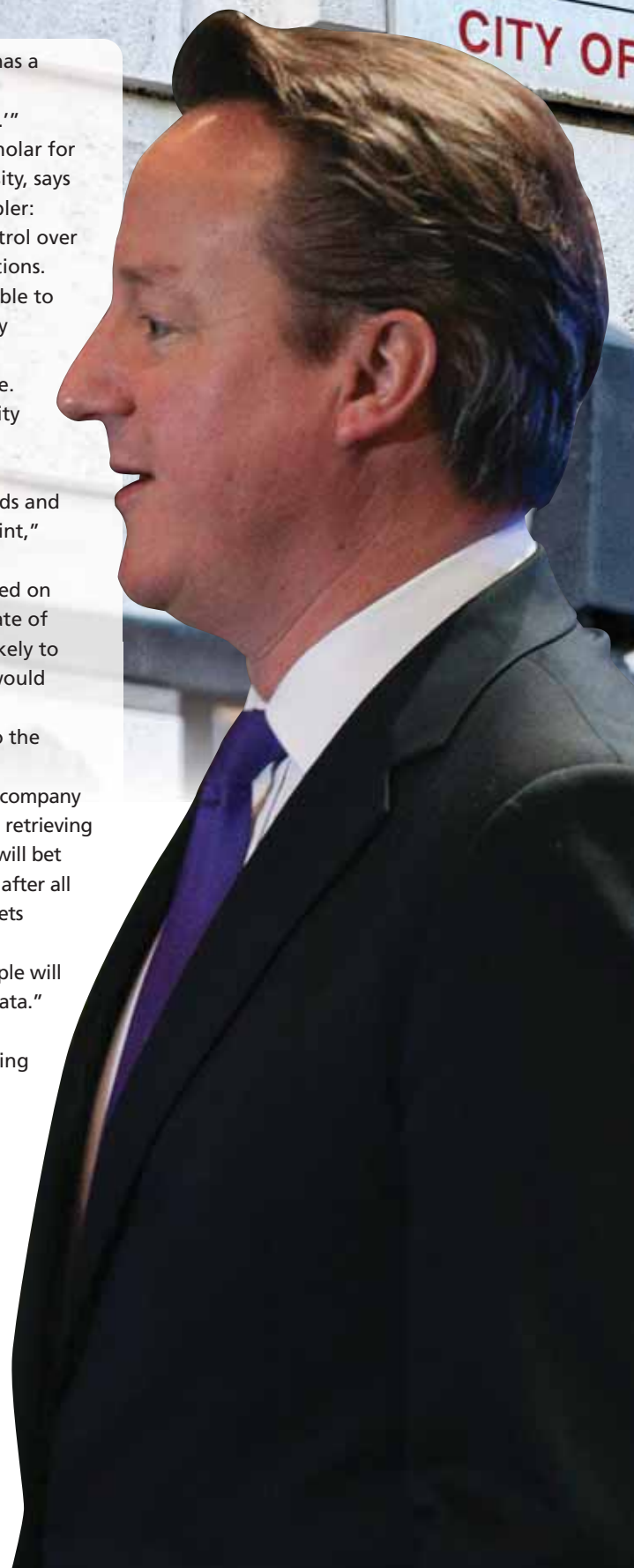
The Electronic Frontier Foundation has described the resulting Cybersecurity Information Sharing Act (CISA) introduced in March as a "terrible surveillance bill" because it would allow companies to launch countermeasures against attackers.

EFF and the Center for Democracy and Technology also complain that the bill bypasses current privacy protections for private-sector information.

In the run up to the UK's May general election, Cameron and the home secretary, Theresa May, proposed reviving long-contentious policies: the principle that government must be able to read all communications, and the Communications Data Bill, which opponents have dubbed the 'Snooper's Charter'.

These policies would add to an already substantial framework for communications surveillance established in multiple pieces of legislation stretching back to 2001. In March, in the first of a series of planned reviews, the Intelligence and Security Committee (ISC) declared GCHQ's activities as leaked by Edward Snowden to be legal, but said the law lacks transparency and accountability and could be interpreted as a 'blank cheque' for the security services.

Britain's data protection regulator, information commissioner Christopher



Graham, criticized the report for a basic misunderstanding: "At one point in the report they say specifically that if citizens are relatively OK about the security services reading letters and tapping phones with appropriate authorization, then why is the internet any different?"

"I thought that represented a very naïve view of what the internet actually is, because it isn't just another communications channel, it's the universe through which we are transacting, doing business, [running] our companies, our work, our personal life, and so on. And the idea that that has got to be left open to be inspected by the authorities, whether good or bad, just seems to me to be ludicrous."

Meanwhile, he adds, the same politicians speak regularly about cybersecurity, but there is an incompatibility in advocating securing communications and infrastructure against myriad threats while ensuring the authorities have access. "I thought it was naïve of the committee to assume that the bad actors wouldn't take advantage of the vulnerabilities that might be left," Graham said.

Content: Return of the Crypto Wars

Cameron is not alone in wanting access to encrypted communications. In March 2015, FBI director James Comey asked Congress to enact legislation requiring technology companies such as Apple and Google to include back doors in any encryption built into their products. Around the same time, the FBI removed from its website advice that consumers should protect their data by using encryption.

There are two kinds of objections to key escrow: ideological and technical. Susan Landau, professor of cybersecurity policy at Worcester Polytechnic Institute Department of Social Science and Policy Studies, describes the technical objection.

"Communications tools built with law-enforcement access to the keys will not be secure against skilled opponents. But the use of encryption where the end-users – and not Apple or Google, for example – hold the keys, means, as the president observed,

'Even though the government has a legitimate request [to wiretap], technologically we cannot do it.'"

Herb Lin, a senior research scholar for cyber-policy at Stanford University, says the ideological objection is simpler: individuals should have full control over access to their own communications.

However, Lin says, it's impossible to make a mechanism that will stay locked down forever, because computing continues to advance. But 1000 (or 100) years of security is long enough. Meanwhile, 10 seconds is clearly inadequate. "Somewhere between 10 seconds and 100 years there's a crossover point," he says.

Performing a risk analysis based on specific proposals and an estimate of how long the cryptography is likely to be secure in that application "would at least get the debate off the theological argument and on to the technical argument."

Lin also raises a practical issue: company helpdesks are overwhelmed with retrieving and resetting user passwords. "I will bet anything that two to three years after all this unimpeachable encryption gets deployed, they will start offering recovery features," he says. "People will not want to lose access to their data."

Likely true, though privacy advocates will argue that choosing a (possibly third-party) key recovery scheme isn't the same as having one forced upon you.

With six years of communications intelligence in his background, John Walker, visiting professor at the School of Science and Technology at Nottingham Trent University, takes a view more in line with law enforcement concerns about 'going dark'.

"I respect privacy and I would like to have privacy," he says, "but what we have



Once encryption keys are handed over to a third party, whether 'benign' or not, security is irrevocably weakened

to look at with a liberal attitude is whether we can allow insurgents – we're talking about a global insider threat of which we have to be aware. If the price I have to pay to keep my legs attached to my torso is privacy, then so be it." The key, he says, is ensuring that the use and exercise of such powers is proportionate and appropriately limited.

Metadata: Bulk Collection

The requirement for ISPs to retain communications traffic data for up to two years was implemented in the EU Data Retention Directive in 2006, a response to the July 7 2005 London bombing attacks. The UK had long favored data retention; a giant centralized database to store the flow was mooted as early as 2000. The 2012 version of this, the Communications Data Bill, would have required communications service providers to collect many forms of data that they currently do not, and disclose it to a substantial range of actors with oversight that opponents such as the Open Rights Group argued was insufficient. The bill failed politically.

In April 2014, the European Court of Justice ruled that the Data Retention Directive conflicted with the European Charter of Human Rights, thereby invalidating the supporting national legislation. In July, Parliament hastily enacted the Data Retention and Investigatory Powers Act (DRIPA) to ensure

that ISPs did not begin deleting the stored data during the summer recess.

A key element of the Communications Data Bill as proposed in 2012 was 'black boxes' to be installed on ISPs' networks and through which traffic would pass; these would extract the metadata for retention. The Internet Service Providers Association complained about the likely loss of speed; advocacy organizations such as the Open Rights Group compared the idea to a man-in-the-middle attack.



If the price I have to pay to keep my legs attached to my torso is privacy, then so be it

John Walker
Nottingham Trent University

Retention practices such as this raise further questions as to whether the principles of necessity and proportionality are being used in the filtering of data – 'filtering' being a term used in early versions of the CDB, though never clearly explained in satisfactory detail.

There is a grey area here around intelligence demands for data that isn't necessarily used in legal proceedings. This is problematic, as is the general opacity of the law.

That opacity is one piece that everyone can agree on. "They already had Tempora," says Privacy International researcher Richard Tynan. "The police and security agencies said 'we want this, so make it lawful for us to do what we're already doing'. To have that as the mindset is the opposite to me of any legal course I've done on the rule of law. They will say they can't do it without authorization, but we don't know what cannot be authorized by Theresa May. To me, that is an unconstrained system."

Will Semple, vice-president of security operations for Houston-based Alert Logic and a veteran of both intelligence and financial services, has seen both sides, yet does not think that Cameron's proposals are "a balanced approach, especially from a military intelligence background and understanding the risks I experienced day in and day out."

Simon Crosby, co-founder and CTO of the security company Bromium, also calls the government's policies poorly conceived: "Once [technology companies] start to engineer for security, the ability to provide arbitrary back doors to arbitrary interested parties is just not going to happen – or at the very least Theresa May will have to answer the question of, 'should Yahoo! provide a back door to China?'"

More bluntly, he says, "The 'Snooper's Charter' is techno-babble. It's nonsense."

Crosby, too, agrees that today's genuine threats require access to data in some circumstances, but he's scathing about the methods proposed. "They've only come out with two so far. One: break everything and be a bad guy, really terrible. Two: they're going to pass stupid laws for technologies that are literally impossible to develop."

What's needed instead, he says, "is a rational debate about how one could legitimately achieve and deliver data in the national interest – and not just the UK and US. The internet is a big place; it's an international problem."



The Web App Security Puzzle



In today's increasingly digital world, web applications are the new battleground for attackers and defenders, argues **Wolfgang Kandek**, CTO, Qualys

The attackers are looking to gain access to corporate or personal data and control web servers for secondary infections.

The recent *Verizon Data Breach Investigation Report 2015* reported that up to 61% of breaches involve attacks against web applications. In fact, vulnerabilities in web apps are now one of the most common cyber-threats, accounting for 55% of all server vulnerability disclosures.

Custom-developed apps are another story altogether, but in general, vulnerability numbers are estimated to be much higher in that area.

The goal of a web app security program is to prevent an attacker from gaining control of an app and obtaining easy access to the server, database and other back-end IT resources. However, as hackers find new ways to exploit web apps, it's important for the security industry to outmaneuver them by quickly finding and fixing the vulnerabilities before an incident occurs.

A Hacker's Attraction to Web Apps

The simple architecture of web apps – including connectivity and hosting via browser-controlled environments – has made it possible for organizations and individuals to easily adopt them to transact business, conduct research, store information and collaborate online. Likewise, for IT teams, web apps can dramatically reduce resource requirements for endpoint devices, as the bulk of processing occurs on servers located at remote sites.

Yet the simplicity driving the adoption of web apps is often the same reason why hackers are inclined to attack them. Part of the reason is that the ability to quickly spin up a web app has contributed to an

increased number of vulnerabilities, as testing and quality assurance can often be an afterthought.

Another reason is that web apps are usually connected to valuable data, including databases containing banking information and consumers' personal identity data. Once a web app is compromised, an attacker can use that data to reap bigger rewards on the black market or in phishing scams to attack larger networks.

Protecting Data with Integrated Data

The good news is that the most prevalent web app vulnerabilities can be easily detected with regular, automated scanning. Automated web app scanning enables IT teams to discover and catalog all web apps within an organization, lower the total cost of operations by automating repeatable testing processes, ensure accuracy by effectively reducing false positives, and identify vulnerabilities early.

But what should you do when you detect a web app vulnerability? And how should you react to actual vulnerabilities and potential exploits?

That's where web application firewalls (WAFs) have become a critical piece of the web app security puzzle. WAFs are capable of detecting, alerting and blocking known attacks on web apps. However, traditional WAFs are often thought to be too complex to set up and too difficult to manage.

Another piece of good news is that WAFs are evolving and new solutions coming into the market are providing more simplicity, flexibility and automation than ever before to protect the data and IT resources behind web apps. The industry is now seeing WAFs capable of automatically integrating scanning data to take on the mitigation of vulnerabilities.

Particularly advanced WAFs also have virtual patching capabilities, enabling IT teams to fine-tune security policies, remove false positives and customize rules leveraging vulnerability data from automated scanners. This data provides insight into common web app vulnerabilities, like those outlined by the OWASP Top 10, as well as critical zero-day exploits where customized patches are not readily available.

Overall, the skeleton key for achieving the best security posture lies within the data – whether it's as broad as threat data shared within the industry, or as narrow as automated vulnerability data shared between a web application scanner and a web application firewall. For the latter, finding a WAF that leverages and integrates data automatically will put you ahead of the curve for web app security.



AUTHOR PROFILE



As the CTO for Qualys, Wolfgang is responsible for product direction and all operational aspects of the QualysGuard platform and its infrastructure. Wolfgang has over 20 years of experience in developing and managing information systems. His focus has been on Unix-based server architectures and application delivery through the internet. Wolfgang earned master's and bachelor's degrees in computer science from the Technical University of Darmstadt, Germany. Wolfgang is a frequent speaker at security events and forums including Black Hat, RSA Conference, Infosecurity Europe and The Open Group. Wolfgang is the main contributor to the Laws of Vulnerabilities blog.



The Rising
Cost of

Cyber-Insurance



You can insure yourself
against cyber-attack, says
Danny Bradbury, but be
warned, prices are going up



Information security is all about mitigating risk. Savvy CISOs spend their time asking what threats their organizations face, how deeply these threats would sink the company, and how likely they are. In that sense, CISOs are suitable customers for another industry that's also about risk management: insurance. So why haven't the two overlapped more?

A Young Industry

At its heart, insurance is about the paid transfer of risk. Companies have been happily transferring their risk to insurance firms since the late 1600s, when economists created insurance services in response to the Great Fire of London.

Traditional risks, such as fire, flood, theft and injury, are well understood. On the other hand, the insurance industry is just getting to grips with cyber-risk.

"When we started looking for the first time at the issue of cyber-attacks and determining whether it would make sense to have a cyber-insurance policy, it was all green space," says Ty Sagalow, former COO for AIG e-Business Risk Solutions, now running Innovation Insurance, a consulting firm and brokerage based in New York.

"It was new. There was no actuarial data on frequency or severity. We had to figure out how to create insurance for a risk that we knew very little about," Sagalow adds.

How do companies manage that risk? Fifteen years is a heartbeat in the insurance business, and so cyber-insurance is still a relatively unknown quantity. The way that insurance companies assess risk involves analyzing past claims. But in a sector with such a short track record and quickly changing characteristics, that isn't always easy. As such, the market is segmented from the general insurance pool, and covered by special policies.

Insurance companies identify and quantify the exposure, pinpoint the threats, and then make a model of how likely those threats are to occur.

"You have a lot less certainty about that frequency than for more established classes like life insurance or auto insurance, but that isn't to say that there isn't any

information in the insurance industry," says Tom Regan, the cyber practice leader for insurance broker Marsh. "We spend a lot of time and money looking to assess the probability of events."

In any case, insurers have an appetite for risk. After all, that's what makes them money.

"You don't go into a new piece of business or a new product because you fear losses. You go in because you hope you'll be

able to make money.

If there's no risk, there's no reward," says Sagalow.



The insurance industry can deal with risks that grow significantly if they can be appropriately compensated

Tom Regan
Marsh

Insurers can mitigate their risk in cyber-insurance as they do in other industries, by splitting risk with other insurers, and by using re-insurance, where the insurers are themselves insured by other companies. They can also impose high deductibles.

What Policies Look Like

Typically, cyber-insurance coverage falls into two broad areas: first party and third party. The first party coverage focuses on the internal costs incurred by the company. It covers expenses such as hiring an attorney to deal with the legal ramifications of a breach, and taking on a PR firm to help get out in front of the problem and minimize reputational damage.

Savvy companies will bring in an external data forensics team to find out where the breach occurred, and remediate it. A first party component will also cover the cost of

notifying individuals, and potentially even setting up contact centers to field calls from worried customers.

In addition, first party coverage typically covers the restoration of lost data, and it will usually compensate companies for lost business, says Michelle Lopilato, director of the cyber-risk solutions practice at North American insurance brokerage Hub International.

"If your network was breached and goes down, and you're no longer able to transact business for a certain amount of time, that loss can be replaced," she says.

Lost business protection won't kick in as soon as a disruption occurs. The most aggressive contracts start around six hours after the disruption, but can go as late as 18 hours for companies with poor business continuity operations, she said.

Third party coverage handles the fallout from cybersecurity events that affect other companies and individuals. Typical coverage here includes network maturity liability (if your network is used to infect another company's systems, for example). It will also cover financial harm to other individuals from a company's privacy breach, along with the cost of post-breach regulatory investigations and fines.

Rising Prices

Insurance companies are getting better at assessing clients' cybersecurity readiness, according to Sagalow.

"The industry has matured," he says. "We have determined that, at least for now, we can continue to underwrite the severity and frequency of cyber-risks, despite the mass attacks that we read about almost every day, whether that be Target, Home Depot, Sony, or others."



Strong security controls, including PoS encryption, are often prerequisites for companies seeking cyber-insurance

But for how much longer? There are signs that cyber-insurance companies, which have blossomed in number over the last decade, are reacting to industry events.

"The industry is continuing to change and expand, and in certain areas of the business, we see some prices going up," says Regan. "The insurance industry can deal with risks that grow significantly if they can be appropriately compensated for them. As long as they can get an adequate premium, they'll be OK."

Where are those prices likely to hit hardest? Look to retail, says Lopilato.

"We are seeing some tightening of the reins as far as underwriting goes. The insurers are looking for best-in-class controls and securities, and if they don't have them, then they are getting declinations," she says.

These controls include encryption at the point of swipe for credit card collection, along with point-of-sale network monitoring, up-to-date security patching, and PCI compliance. "If you can satisfy those four bullet points first, then you do have several carriers still willing to write this business," she adds.

Companies that take advantage of these policies may even find themselves battling to get coverage. Such was the case with Atlantis National Services, a New York state-based title insurance agency licensed in 32 states. It obtained a cyber-insurance policy through Lloyds of London, after the Department of Homeland Security mandated a data center controls standard, SSAE 16, for title insurers. Atlantis co-

“
Insurers are looking for best-in-class controls and securities, and if [clients] don't have them, they are getting declinations

Michelle Lopilato
Hub International

founder Radni Davoodi began looking for cyber-insurance not long afterwards.

"It gives banks further comfort using us versus our competitors," says Davoodi, but he adds that it wasn't easy to obtain. The industry is still so new that choices are limited, he warns.

"It took us a while to get a quote, and the only broker who was able to provide us with one gave us a cookie cutter and said 'take it or leave it'," he says, recalling that there was no option on the deductible or the protection offered. "We're hoping that in the coming years it will be a little more selective on our end."

Do customers want insurers to take on their business, though? The Corporate Executive Programme, which monitors corporate security threats, surveyed 40 of its members for a January 2015 report on cyber-

insurance. Only one in five companies had dedicated cyber-insurance, it found, and this was among a base of large companies, half of which measured revenues in the billions.

Cyber-insurance adoption also differed dramatically between the US (where 40% of companies had it) and the UK (where just 13% of firms did).

Regan says that regulation makes a big difference in adoption on either side of the Atlantic. In the US, where data breach notification is mandated in 47 states, more companies will be driven to adopt cyber-insurance because of the potential fallout should a breach occur.

Dr Claudia Natanson, chair of the CEP, suggests another factor.

"There was a point given by one of our legal members, stating that it wasn't so much that the US had breach notification that promoted greater take up, but that unlike Europe, US [companies] could suffer class action suits," she says.

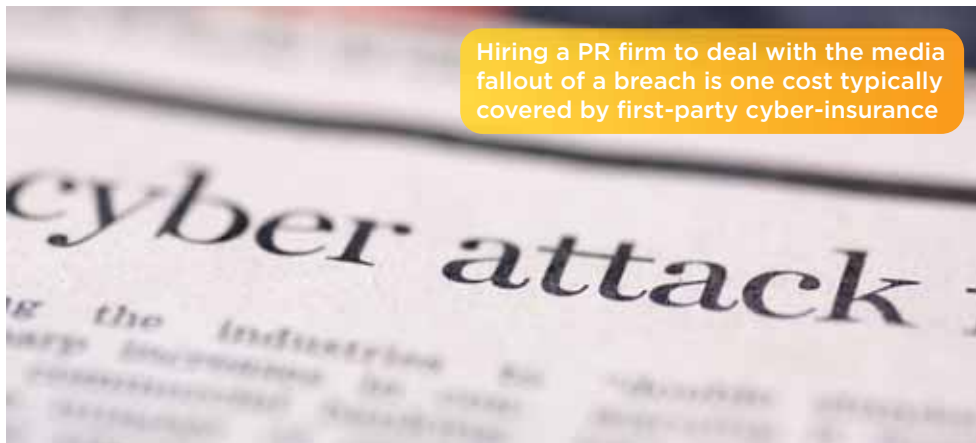
European adoption will likely rise, adds Natanson. But with an average of four in five companies still not adopting dedicated cyber-risk insurance, there is a lot of potential headroom in this young industry.

Sagalow, who first took steps into cyber-insurance 15 years ago, is already expanding into something new: bitcoin. The cryptocurrency, which is slowly disrupting traditional financial markets, has been beset with security problems. Now, secure bitcoin storage companies are offering peace of mind to users who might hold thousands of dollars-worth in a software wallet. He is working with them to insure their customers against losses incurred in this strange new electronic asset.

"Bitcoin is the new cyber," Sagalow says, recalling how the internet represented a fundamental shift in how business was done in 2000. "Fast forward 15 years later, and the same thing is happening again."

Wherever you find uncertainty and risk, you'll find a forward-thinking insurer exploring ways to underwrite it. The customers may take a little while to come, but if they're aware of the dangers they're facing, they'll arrive eventually.

Hiring a PR firm to deal with the media fallout of a breach is one cost typically covered by first-party cyber-insurance



infosecurity

EUROPE

02 June - 04 June 2015
Olympia, London, UK

**WE HAVE THE SOLUTIONS
TO MATCH ALL YOUR NEED:**

macmon[®]
nac ■ smartly simple

Intelligent Network
Access Control



Flexible Unified
Threat Management



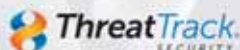
Industry Leader in Digital
Investigative Solutions



Industry Leading Protection
from Viruses and Malicious Code



Award winning Authentication
and Encryption solutions



Simple and Fast IT
Management and Antivirus



Accelerate, Optimise
and Secure



Continuous
Network Monitoring



On-demand Security
Awareness Training



Security, Networking
and Storage Solutions



Market Leading,
Proven Internet Security



WICK HILL

**Visit
Wick Hill
on stand
E100**



**WIN A
SONOS PLAYBAR**



**Telephone: 01483 227600
email: info@wickhill.com**

© 2015 Wick Hill Ltd. All rights reserved. Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other brand and product names are trademarks of their respective owners.





Google vs Microsoft: Let the Patch Wars Commence



Phil Muncaster investigates whether an ongoing dispute between Google and Microsoft could change the way we fix security flaws in the future

At the start of the year, Microsoft and Google became embroiled in a very public spat over vulnerability disclosure. The two computing giants, never the best of friends, became more animated than we've seen them for some time, exchanging barbed comments via blog posts and social channels. The reason? Google's Project Zero initiative, announced last July, and its strict rule of revealing vendors' software bugs publicly after 90 days if they have not been patched.

So who exactly is the bad guy in all of this? Microsoft, for failing to patch as quickly as Google would like, or the Mountain View giant, for disclosing flaws before security fixes were ready? And is the ongoing dispute likely to change how the industry deals with vulnerability disclosure?

A Bit of History

It all kicked off when Google decided to release details of a Windows flaw just two days before it was due to be fixed in

January's Patch Tuesday. The bug itself was not particularly critical, needing a victim machine to have already been compromised in order to work. However, plenty of commenters let their feelings be known on the related Google Security Research forum post.

"Automatically disclosing this vulnerability when a deadline is reached with absolutely zero context strikes me as incredibly irresponsible and I'd have expected a greater degree of care and



maturity from a company like Google," wrote one user.

Microsoft then waded in with a strongly worded blog post from Chris Betz, senior director of the Microsoft Security Response Center.

"Although following through keeps to Google's announced timeline for disclosure, the decision feels less like principles and more like a 'gotcha', with customers the ones who may suffer as a result. What's right for Google is not always right for customers," Betz wrote in that post. "We urge Google to make protection of customers our [combined] primary goal."

This didn't seem to deter Google, which released details of several additional Microsoft product flaws in the weeks that followed. Here's the twist though. One batch of disclosures came about before the 90-day deadline, after Microsoft effectively told the web giant that the flaws were so small they were not worth patching. This is despite several of them – including an elevation of privilege issue and an information disclosure bug – being marked as 'high severity' by the Project Zero researcher in question.

The waters have been further muddled by Microsoft's somewhat controversial decision in January to effectively make its Advanced Notification Service (ANS) private. Redmond claims the decision was taken to meet customers' evolving needs – in other words, that most firms have automatic updates or proper patching regimes which render the public blog posts and notices irrelevant. However, experts argue it was a retrograde step that could at best be viewed as an attempt to hamper transparency into product flaws, and at worse a cynical move designed to make money by forcing customers to upgrade to 'premier' status.

Who's Right?

Google relented recently and allowed vendors a further 14-day grace period on top of the mandatory 90 if a patch is already slated for release, as well as promising not to disclose flaws on US public holidays or at the weekend. But there's still a fair bit of

The definition of 'responsible' disclosure is something the research and vendor communities often disagree on



bad blood about how it has handled the whole affair.

So is this a dispute we should really take sides on? For Nigel Stanley, cybersecurity practice director at consultancy OpenSky, neither firm has covered itself in glory.



Instead of throwing stones, those that live in glass houses need to give their neighbors support

Nigel Stanley
OpenSky

"Both Microsoft and Google need to grow up and understand that great care needs to be taken in disclosing vulnerabilities in a calm, controlled way," he tells *Infosecurity*. "This will reduce the opportunities for exploits to be developed and give over-worked sysadmins a chance to test and then

patch their systems. Instead of throwing stones, those that live in glass houses need to give their neighbors support for the benefit of the broader industry."

For Ed Skoudis, SANS Institute fellow, Google needs to be a bit more aware of the sheer complexity involved and the huge resources that are needed to create and test fixes for certain vulnerabilities.

"As [Google's] systems are in the cloud with code they control, there are few hurdles to them throwing resources at a problem and getting fixes out in 90 days or less. Project Zero is a way of Google draining a swamp very quickly," he tells *Infosecurity*.

"However, they don't have the extended enterprise customer base with lots of on-premise software and legacy systems along with strict controls around applying patches," Skoudis adds. "In some cases, 90 days is just not reasonable and a rushed fix might actually lead to more problems than it solves."

In fact, that exact scenario has occurred several times of late, most notably in August 2014 after an August Patch Tuesday fix locked computers with the dreaded Blue Screen of Death.

Responsible Disclosure

Most commentators, software vendors, and security researchers agree that responsible

disclosure is the best way forward. The problem is, they don't agree on exactly what 'responsible' means.

Some take the extreme view that unless a flaw is made public immediately, the vendor will procrastinate, downplay its importance and possibly even use legal means to silence the researcher – while the bad guys are working on crafting attacks in the meantime. Others say the vendor should be informed privately and given a decent amount of time to fix the flaw.

However, once again the debate rages as to how much time should be allowed and for which kind of flaws, according to Secunia director of research and security, Kasper Lindgaard.

Infosecurity asked Lindgaard what represents 'a timely fashion' when it comes to giving vendors a chance to fix a vulnerability, before disclosing it.

"Our policy is to give vendors six months to fix the vulnerability and issue a patch, and for a huge majority of the vendors that is plenty of time," he says. "But it is also necessary to be flexible and adapt to circumstances: you have to look at the individual vulnerability – at how critical it is, how complex it is to fix, and how widespread the vulnerable product is."

Jim Fox, director in KPMG's cyber team, is actively involved in pen-testing and vulnerability identification. He argues that the most important thing from the vendor's point of view is to be transparent with its customers.

Even if there's not a patch immediately available, he explains, the vendor could produce a way to mitigate the problem which would quickly keep customers secure in the meantime – or their customers could

The most important thing to do in the vulnerability management dimension, from a vendor perspective, is communication

Ramsés Gallego
ISACA

come up with their own temporary solutions. Either way, Fox believes the Common Vulnerability Scoring System (CVSS) provides a ready-made, commonly understood framework which could help them prioritize newly discovered flaws.

This is essential given the sheer volume of black hats out there researching flaws, he tells *Infosecurity*.

"People are taking a methodical approach to identifying and exploiting vulnerabilities in widespread systems. To think only one person will find them is crazy," Fox adds. "You don't need to put out a press release each time you find a flaw – that's irresponsible. But at the same time, if you alert a vendor, say they have a week or 10 days to tell their customers and announce a patch or at least mitigation, that's fair. The vendors don't move faster because it's disruptive for them, so you need to make it in their best interests to do it."

ISACA international vice president, Ramsés Gallego, agrees that greater transparency is the way forward.

"The most important thing to do in the vulnerability management dimension, from a vendor perspective, is communication," he tells *Infosecurity*. Gallego believes that in the cyber era, threats will always exist – it's not a matter of if a company faces a vulnerability, it's when and how quickly they'll then recognize and mend it.

A Troubled Future?

Yet for Fox, Microsoft is moving not towards greater transparency, but away from it, as witnessed by its decision in January to end its Advance Notification Service. He argues that failing to inform all customers through notifications means many won't even be aware of vulnerabilities which malware writers are actively developing exploits for.

"The only people to get hurt will be those who need to defend themselves. Less transparency is a mistake; I rarely learn of a vulnerability through a press release," he adds.

So what of the future for vulnerability disclosure? Can the vendor community afford to pour more resources into developing timely patches or will the quality of security fixes suffer, and patching times inevitably get longer as the sheer volume of flaws identified mounts?

Skoudis thinks Google's gung-ho approach could yet have negative consequences.

"Unfortunately, there is a risk that Google may incite copycats that are maybe less wedded to a 'don't be evil' philosophy," he argues. "In future, we could have others pushing out zero days into the public forums that are incredibly dangerous without warning. And then what started out as a positive approach could turn into a major issue for everybody."

In the meantime, it's the sysadmins – the "poor bloody infantry" – who will be forced to pick up the pieces, according to Stanley.

"Some vendors forget that there is a world outside of their products and that sysadmins are having to test and apply patches from multiple vendors, often at the same time," he says.

It's difficult to foresee a time when this will ever change.



Before broadcasting their findings to the world, researchers should consider the impact on vendors and end-users

20TH INFOSECURITY EUROPE CONFERENCE & EXHIBITION EVENT PREVIEW

Intelligent Security

Protect. Detect. Respond. Recover.

CELEBRATING 20 YEARS

02-04 JUNE 15
OLYMPIA LONDON UK

Featuring:

- Conference Programme
- Infosecurity Intelligent Defence
- Security Workshops and Training
- New Features
- Floor Plan
- Exhibitor List

New location

See you at
Olympia
Kensington,
London

Organised by:



infosecurity[™]
GROUP

Intelligent Security: Protect. Detect. Respond. Recover.

The Sony Pictures breach in December 2014 made headlines around the world. Whatever the truth around who was responsible, the breach highlighted yet again that no organisation is immune to cyber-attack.

Consequently, information security is no longer just about protecting the network against attacks – it's about building cyber-resilience to minimise business impact in the event of a breach. Despite that, only 35% of respondents to the Infosecurity Europe Industry Survey 2015 are seeing a significant change in focus from a purely prevention-based security strategy to one that balances prevention with detection, response and recovery.

Information security professionals face a multitude of conflicting, complex risks and priorities, as enterprises become increasingly connected and collaborative, with extended network perimeters, and the adoption of new business practices. Against this backdrop, security practitioners are working to develop intelligent security strategies that are aligned with the individual organisation's risk profile and business priorities.

Knowing their business and understanding the context of the cybersecurity risks they face is fundamental to aligning security strategy with the business. Yet communicating risk to senior management, speaking the language of the business and developing an enterprise-wide security culture continue to be a challenge, and ineffective communication consistently stands in the way of intelligent security.

Recent incidents suggest that it is taking too long for organisations to detect breaches, as demonstrated by the JP Morgan breach in August 2014. But how do organisations even know they've been breached? Most organisations don't have the resources to continually monitor and detect incidents, and if an organisation doesn't know it has been breached, it can't respond appropriately.

With potentially catastrophic repercussions for a business, the ability to respond to and recover from an attack rapidly and efficiently is critical to building cyber-resilience and an intelligent security strategy. Infosecurity Europe Industry Survey 2015 respondents revealed that in the event of a security incident, minimising the impact

on the customer is the biggest priority, closely followed by business continuity. Enabling the business to function is crucial to intelligent security strategy.

Against this backdrop, Infosecurity Europe provides you with the opportunity to gain the tools, techniques and strategies you need to develop an intelligent security strategy, centred around the business requirements of your enterprise and balancing prevention, detection, response and recovery. Featuring an extensive conference and seminar programme, and showcasing the latest innovations in information security, Infosecurity Europe is the meeting point for the information security community.

We look forward to welcoming you to Olympia London in June.



Kerry Prince
Infosecurity Portfolio Director

Key Facts About the 20th Infosecurity Europe

Intelligent Security:

Protect. Detect. Respond. Recover.

Infosecurity Europe is the largest European information security event that enables industry professionals to gather vital information about the latest trends and developments in information security all under one roof. Come along to exchange ideas, make new contacts and shop for products and services to secure the future of your business assets where it matters.

A Highly Satisfied and Influential Audience - What You Missed in 2014

- 15,253 information security professionals travelled from 73 countries
- 346 exhibiting companies from 24 countries

- 160+ international thought-leaders and expert speakers were featured
- 3,000+ information security professionals collected CPD/CPE credits with our certified content
- 98.1% satisfied visitors, 97.2% satisfied exhibitors
- 96.6% of visitors are likely to return for Infosecurity Europe 2015 (81% are extremely or very likely)
- 100+ influential industry and mainstream press in attendance reporting about Infosecurity Europe globally

When and Where

09.30 - 17.30 - Tue 2nd June 2015
09.30 - 17.30 - Wed 3rd June 2015
09.30 - 16.00 - Thu 4th June 2015

Introducing CSX Skills-Based Cybersecurity Training and Certifications.



More and more cybersecurity professionals are turning to Cybersecurity Nexus™ [CSX] for the knowledge, tools and guidance they need to be successful in their jobs. CSX is your premier source for education, training, research, industry events and community — and now, for cutting-edge certifications and training courses. Our new, skills-based programs are designed to help you build, test and showcase your skills in critical areas of cybersecurity. Because it's not enough anymore to show you have the knowledge, it's about proving you have the technical skill and ability to do the job from day one.

**Visit us on
Stand H60**

Visit www.isaca.org/cyberEU for more information.



TOP 5 Reasons to Attend



1 Join the Community

Be part of the information security discussion that drives your industry forward. Come and network with a group of the leading voices in the information security world and participate in a premium conference programme designed to deliver the biggest learning and knowledge sharing opportunity in Europe.

Find solutions for tomorrow's threats and challenges.

80% of visitors new to Infosecurity Europe were highly satisfied with their visit in 2014 and 96% are very likely to return in 2015!

"Infosecurity Europe is the best forum for all security professionals to get access to IS and IA vendors, products, experts, peers under one roof."
Paul Ryan, Senior InfoTech Security Officer, Lincolnshire Police

4 Learn From the Experts

Take home proven strategies, save money and improve your businesses' security posture

200+ expert speakers 150+ hours of conference programming in a variety of delivery formats+

85% of Infosecurity Europe 2014 visitors rated the educational sessions as high quality

2 Accelerate Your Career

Collect up to 5½ CPD / CPE credits per day and choose from 200+ hours of seminars and workshops.

16½ CPD / CPE to be gained!

Harvest expert advice and gain insight that is relevant to your needs! The conference includes:

- Keynote Stage
- Strategy Talks
- Tech Talks
- Information Security Exchange
- Security Workshops
- Technology Showcase
- Security Training
- Cyber Innovation Showcase
- DevOps Connect
- RANT Forum – Infosecurity Special



Join **15,000+** information security peers

3 Find Out What's New

Select from 345+ global and leading information security vendors and service providers to help you solve your burning information security problems. Our comprehensive and diverse range of exhibitors have been brought together under one roof to allow you to keep abreast of new companies entering the market, see what's new from the vendor names you know and respect, and find out about new developments in your industry.

94.8% of visitors attending in 2014, were looking for inspiration and to see what's new

"The best networking event in security!"
Steen Larsen, CEO, Cloud Bastion

5 Grow Your Business Network

Our event attracts over 15,000 industry professionals, from the who's who of the information security world. Over the course of the three days, you can reconnect with your existing peer group and meet new contacts to share knowledge, experiences and common objectives.

"I have made many useful contacts via Infosecurity Europe over the years, a very worthwhile meeting place."
Sean Marks, Senior Consultant, Serco Group plc

Register Once, Benefit Twice



SITS15 – The IT Service Management Show – is the UK's Leading Exhibition and Conference for ITSM Professionals. Discover the latest solutions and gain expert advice from some of the world's leading suppliers. Get inspired and gain insight into the latest issues and trends in the practical seminars and keynotes, plus network with thousands of your industry peers.

New Venue: SITS15 will be located at Olympia, London on the 3-4 June and will be collocated with Infosecurity Europe.

The UK's leading exhibition and conference for ITSM professionals looks set to celebrate its milestone 21th anniversary in great company, with a host of big name vendors, consultancies and service providers now confirmed as exhibitors, view the full exhibitor list online.



Highly sensitive becomes highly secure. With secunet in CRITIS.

Critical infrastructures (CRITIS) like water and energy supply are vitally important for society. At the same time, they depend now more than ever on the flawless functioning of information and communication technology. secunet protects these infrastructures sustainably and comprehensively against cyber attacks with professional IT security strategies and products like SINA. So that critical does not become dramatic!

Sounds impossible? Put us to the test!

www.secunet.com/critis

secunet

IT security partner of the Federal Republic of Germany



KEYNOTE STAGE



Intelligent Security: Protect. Detect. Respond. Recover.

As the threat landscape becomes more complex, and organisations become increasingly connected, information and cybersecurity professionals face a multitude of conflicting risks, priorities and challenges. Utilising a deluge of threat intelligence, they need to ensure they implement an intelligent security strategy that identifies the key risks to their business, driving protection strategies, whilst building cyber-resilience. The Keynote Stage will look at these challenges and provide strategic and practical advice on how to address them.

Created for the Industry by the Industry

Created for the industry by the industry, following extensive research with the information security end-user community and consultation with an advisory council of senior industry practitioners, the Keynote Stage is the vibrant hub of the Infosecurity Europe seminar programme.

Insight, Ideas and Inspiration

The Keynote Stage provides attendees with direct access to information security knowledge and expertise presented by some of the industry's leading end-user practitioners, policy-makers, analysts and thought-leaders. Delegates will gain new ideas, insight, and actionable intelligence to enable them to streamline their information security strategy, accelerate the effectiveness of their security tactics, and reinforce the critical position of the information security function.

Key Themes to be Addressed in the 2015 Keynote Stage Agenda Include:

- **Intelligent security:** Risk-based information security strategies to address prevention and response and align information security to the specific needs of your organisation

- **Building cyber-resilience:** Effective tactics and techniques to detect and respond to security incidents
- **Next generation information security:** Keeping pace with the evolving, connected business and adapting to new technologies and working practices
- **Threat analysis:** Evaluation of the latest threats and attack vectors and insight into how to address them

Don't forget to build the Keynote Stage sessions into your Infosecurity Europe agenda!

www.infosecurityeurope.com/keynotes

Day One: Tuesday 2 June

10.00-10.40	Keynote Presentation Security and Privacy <i>Ciaran Martin, Director General, Cyber Security, GCHQ</i>
10.55-11.55	The 2015 Cyber Security Breaches Survey: Official Launch, Key Findings and Analysis Details of the 2015 security breaches survey results will be discussed and reviewed. <i>Richard Horne, Partner, Cyber Security, PwC</i> <i>Andrew Miller, Cyber Security Lead for Government and Public Sector, PwC</i> <i>Chris Potter, Partner, PwC</i>
12.10-12.50	Infosecurity Perspectives Mitigating the Human Risk <i>Jenny Radcliffe, Social Engineer</i>
13.05-14.10	Infosecurity Strategy Panel Discussion Establishing an Enterprise-Wide Cybersecurity Culture This session will include the White Hat events charity cheque presentations. Panellists: <i>John Meakin, CSO, Richemont International</i> <i>Lee Barney, Head of Information Security, Home Retail Group</i> <i>David Jones, Head of Information Security, BBC</i> <i>Andrew Rose, CISO and Head of Cyber Security, NATS</i>

	<i>Bruce Hallas, Founder, The Analogies Project</i> Moderator: <i>Stephen Bonner, Partner, KPMG, Infosecurity Europe Hall of Fame Alumni</i>
14.25-15.05	Keynote Presentation Solving Security Challenges: How Google does Information Security <i>Eran Feigenbaum, Director of Security, Google Apps</i>
15.20-16.15	Secure Development Panel Discussion From DevOps to DevSec: Securing Application Development Panellists: <i>Pawel Krawczyk, Application Security Manager, Open Web Application Security Project (OWASP)</i> <i>Bryan Littlefair, Global CISO, Aviva</i> <i>James Lyne, Security Researcher</i> <i>Richard Rushing, CISO, Motorola Mobility</i>
16.30-17.30	Cloud Focus Panel Discussion Solving the Cloud Conundrum: Privacy, Trust and Accountability Panellists: <i>Quentyn Taylor, Director of Information Security, EMEA, Canon</i> <i>Eran Feigenbaum, Director of Security, Google Apps</i> <i>Justin Somaini, Chief Trust Officer, Box</i> <i>Daniele Catteddu, Managing Director, EMEA, Cloud Security Alliance</i> Moderator: <i>Adrian Davis, Managing Director, (ISC)²</i>



Day Two: Wednesday 3 June

10.00-10.40	Keynote Presentation Cracking the Cipher Challenge <i>Simon Singh, Science Writer</i>
10.55-11.35	Keynote Presentation How to Hack an Enterprise: Exploitation for Beginners <i>James Lyne, Security Researcher</i>
11.50-13.00	Infosecurity Intelligence Keynote Panel Discussion Know Your Adversary: Who is the Cyber-criminal? Panellists: <i>Andy Archibald, Deputy Director, National Cybercrime Unit, National Crime Agency</i> <i>Professor Alan Woodward, Visiting Professor, Surrey Centre of Cyber Security, University of Surrey</i> <i>Wil van Gemert, Deputy Director Operations and Acting Head of EC3, Europol</i> <i>Michael Driscoll, Assistant Legal Attaché, FBI</i> Moderator: <i>Brian Honan, Founder & CEO, BH Consulting</i>
13.15-13.55	Breach Detection and Response How Do You Know You've Been Breached? Rapid Breach Detection and Effective Response To Minimise Incident Impact <i>Bruce Schneier, Infosecurity Europe Hall of Fame Alumnus</i>

14.10-15.00	Infosecurity Strategy Panel Discussion Articulating Risk to Senior Management: Enabling Informed Decision-Making Panellists: <i>David Cass, Senior Vice President & CISO, Elsevier</i> <i>Mike Pitman, CISO, Head of Information Security, John Lewis</i> <i>James Mckinlay, Head of Information Security UK&I, Worldline</i> Moderator: <i>Peter Wood, Security Advisory Group, ISACA London Chapter</i>
15.15-16.15	Infosecurity Intelligence Panel Discussion Vulnerabilities, Risks And Threats: Actionable Intelligence for Robust Cyber Defence Panellists: <i>Gianluca D'Antonio, CISO, FCC Group, Chair of ISMS Forum</i> <i>Burim Bivolaku, CISO, The Noble Group</i> <i>Dr Eduardo Solana, Senior Lecturer, Computer Science Department University of Geneva</i> Moderator: <i>Wendy Nather, Research Director, Information Security, 451 Research</i>
16.30-17.30	Regulation and Compliance Panel Discussion Smart Strategies to Address Increasing Global Regulatory Oversight Panellists: <i>Richard R. Starnes, CISO, Kentucky Health</i> <i>Bridget Treacy, Partner, Hunton & Williams</i> <i>Steve Wright, Chief Privacy Officer, Unilever</i> <i>Jonathan Bamford, Head of Strategic Liaison, Information Commissioner's Office</i> Moderator: <i>Stewart Room, Partner, PwC</i>

Day Three: Thursday 4 June

10.00-10.40	Keynote Interview Infosecurity Europe Hall of Fame During this session the 2015 Hall of Fame inductee/s will discuss a timely development in information security, be it a post-incident review of a recent breach, the threat landscape or a presentation on a new technological development.
10.55-11.45	Risk Insight Panel Discussion Prevention to Response: Intelligent Risk Management to Bolster Security Posture Panellists: <i>Shan Lee, Head of Information Security, JUST EAT</i> <i>Jonathan Kidd, CISO, Met Office</i> <i>Mark N Jones, CISO and Director IT Compliance & Governance, Heathrow Airports</i> <i>Vicki Gavin Compliance Director, Head of Business Continuity and Information Security, The Economist Group</i> Moderator: <i>Jean Noel Georges, Global Programme Director, Research Manager, Frost & Sullivan</i>
12.00-12.50	Incident Response Panel Discussion You're Under Cyber-Attack. Now What? Panellists: <i>Chris Gibson, Director, CERT-UK</i> <i>Tom Mullen, Head of Cyber Response & IT Security, Telefónica UK</i> <i>Jon Townsend, Head of Cyber Intelligence and Response, Department for Work and Pensions</i> Moderator: <i>Dave Clemente, Senior Research Analyst, Information Security Forum</i>

13.05-13.55	CNI Panel Discussion Securing Critical National Infrastructure: Managing Cyber Risk in a Hyper-Connected, Physical World Panellists: <i>Don Randall, Cyber Ambassador, Bank of England</i> <i>Peter Gibbons, Head of Cyber Security, National Rail</i> Additional speakers to be confirmed Moderator: <i>Andrew Kellett, Principal Analyst, Ovum</i>
14.10-14.55	UK's Most Innovative Small Cybersecurity Company of the Year: Competition Final During this session the four finalists from the national competition launched through the Cyber Growth Partnership, with the support of BIS and techUK, will pitch their technology/service to a judging panel which will select the winner and award the title of 'Most Innovative Small Cyber Security Company of the Year'. Judges: <i>Nazo Moosa, Managing Partner, C5 Capital</i> <i>David Cass, Senior Vice President & CISO, Elsevier</i> <i>Wendy Nather, Research Director, Information Security, 451 Research</i>
15.10-16.00	Infosecurity Strategy Panel Discussion Keeping Pace with the Evolving Business: Building a Next-Generation Cybersecurity Roadmap Panellists: <i>Michael Colao, Head of Security, Group Technology and Operations, AXA UK</i> <i>José A. S. Alegria, Director, CyberSecurity, Privacy and Business Continuity, Portugal Telecom</i> <i>Becky Pinkard, Director, Security Operations, Pearson</i> Moderator: <i>Bob Tarzey, Analyst and Director, Quocirca</i>



Smart defence to detect,
contain and respond

02-03 June 2015, Olympia London



Register Online: www.infosecurity-intelligent-defence.com

Day One: Tuesday 2 June

08.30-09.00	Registration and coffee	12.30-13.30	Smart Home Invasion <i>Craig Young, Security Researcher, Tripwire</i>
09.00-09.10	Welcome from Chair Opening remarks from the conference chair.	13.30-14.45	Lunch
09.10-10.10	Keynote Presentation <i>Adam Laurie, Security Researcher, Director, Aperture Labs</i>	14.45-15.45	The Researcher's Guide to the IoT Galaxy <i>Andrew Hay, Head of Research, OpenDNS</i>
10.10-11.10	POS Attacker Toolkits: Frontline Analysis of POS Attack Toolkits <i>Kyle Wilhoit, Senior Threat Researcher, Trend Micro</i>	15.45-16.45	Keynote Presentation Regulating Your Nose to Spite Your Face <i>Sergey Bratus, Research Associate Professor, Dartmouth's Institute for Security, Technology, and Society</i>
11.10-11.30	Morning refreshments	16.45-17.00	Closing comments from the Chair The conference chair will review the day's sessions and key conclusions.
11.30-12.30	Detecting and Responding to Advanced Threats: Exposing the Skeleton in Your Closet <i>Lee Lawson, CTU Special Operations, Dell SecureWorks</i>		

Day Two: Wednesday 3 June

08.30-09.00	Registration and coffee	11.30-12.30	Wolf in Sheep's Clothing: Your Next APT is Already Whitelisted <i>Juan Andres Guerrero-Saade, Senior Security Researcher, Global Research and Analysis Team (GReAT), Kaspersky Lab</i> <i>Fabio Assolini, Senior Security Researcher, Global Research and Analysis Team (GReAT), Kaspersky Lab</i>
09.00-09.10	Welcome from Chair Opening remarks from the conference chair.	12.30-13.45	Lunch
09.10-10.10	Keynote presentation Details to be announced	13.45-14.45	Data Sanitization: Effective Protection or Latest Buzzword? <i>Szilard Stange, Director of Product Management, OPSWAT</i>
10.10-11.10	Detecting Malicious Typosquatting Domains <i>Gerben Broenink, Security Specialist, TNO</i> <i>Harm Schotanus, Information Security Specialist, TNO</i>	14.45-15.45	The Fault In Our Clouds <i>Yonatan Most, Head of Adallom Labs, Adallom</i>
11.10-11.30	Morning refreshments	15.45-16.00	Closing comments from the Chair Final review and summing up by the conference chair.

ARE YOU SMARTER THAN THE ATTACKERS?

Intelligent defence against cyber attacks

- Gain in-depth understanding of the latest vulnerabilities, exploits and threats
- Hear from leading security experts who are at the sharp end of technical research
- Access best practice advice on how to mitigate the effects of new vulnerabilities and exploits

Meet the Advisory Council

Dr Eric Cole, Jack Daniel
James Lyne , Trey Ford , Rik Ferguson



Find out more at:
www.infosecurity-intelligent-defence.com

02 – 03 June 2015

**REGISTER
ONLINE NOW**

www.infosecurity-intelligent-defence.com

Olympia. London.





STRATEGY TALKS



Intelligent Security: Strategic Insight to Optimise Security Posture

Acquire strategic insight into how to develop a resilient information security strategy to support enterprise growth, innovation and transformation.

Strategy Talks Sponsor:

BLUE COAT[®]

For the latest programme and speaker updates visit www.infosecurityeurope.com/strategytalks

Day One: Tuesday 2 June

10.00-10.25	Overcoming Insider Threats to Intellectual Property <i>Laurent Porracchia, Chief Information Officer, Safran Morpho</i> <i>Stephane Charbonneau, Chief Technology Officer, Titus</i>
10.40-11.05	The Flaws in the Onion: What does Context-Aware Next-Next Generation Security Look Like? <i>Gary Newe, Technical Director, F5</i>
11.20-11.45	Rethinking Enterprise Security: Lifecycle Defence <i>Felix Leder, Director Advanced Malware Defence, Blue Coat Systems</i>
12.00-12.25	Dear Executives, Parlez-Vous Security? <i>Dwayne Melancon, Chief Technology Officer, Tripwire</i> <i>Brian Honan, CEO, BH Consulting</i> <i>Thom Langford, Director of Global Security, Sapient</i>
12.40-13.05	Trouble in Paradise: End Island Hopping by Embracing the Tactical Shifts of the Underground <i>Rik Ferguson, Global VP Security Research, Trend Micro</i>
13.20-13.45	FUD or Fact: The Role of the News Media in Security <i>Anthony Freed, Senior Editor of Publications, Norse Corporation</i> <i>Thomas Brewster, Journalist, Freelance</i> <i>Brian Honan, CEO, BH Consulting</i> <i>Raphael Satter, Investigative Journalist, Associated Press</i>

14.00-14.25	UK Public Sector and Healthcare Industry Panel Debate: Managing Security Risks and Protecting Information Assets <i>Bruce Wright, Connectivity Technician Consultant, South East CSU (NHS)</i> <i>Bob Tarzey, Analyst and Director, Quocirca</i> <i>Phil Gibson, Chair, PSN Industry Association, Director, Avoca Associates (Speaking on behalf of Forescout)</i>
14.40-15.05	ProTips for Tackling Incidents Involving Advanced Attack Techniques <i>Steve Armstrong, Technical Security Director, Logically Secure</i>
15.20-15.45	Method for Assessing Risk in a Business: It's Not Just About Vulnerabilities <i>Matt Alderman, VP Strategy, Tenable Network Security</i>
16.00-16.25	How Think Money is Utilising Continuous Monitoring to Mitigate Today's Threats, and to Meet Regulatory and Contractual Obligations <i>Neil Dawson, Senior Information Security Analyst, Think Money Group</i> <i>Ross Brewer, Vice President & Managing Director of International Markets, LogRhythm</i>
16.40-17.05	It's About the Data, Stupid <i>Salo Fajer, CTO, Digital Guardian</i>

Day Two: Wednesday 3 June

10.00-10.25	Where Flow Charts Don't Go: An Examination of Web Applications Security Process Management <i>Gabriel Gumbs, Managing Director, Research and Products, WhiteHat Security</i> <i>Matt Johansen, Senior Manager, Threat Research Centre, WhiteHat Security</i>
10.40-11.05	Are You Seeing a Return on Your Security Investments? Security as a Business Enabler <i>Sol Cates, CSO, Vormetric</i>
11.20-11.45	The Plateau Effect: Why Security is Being Reinvented <i>Hugh Thompson, Chief Technology Officer, Blue Coat Systems</i>
12.00-12.25	Fridge FUD: Freezing Out IoT Myths <i>Carl Leonard, Principal Security Analyst, Websense</i>
12.40-13.05	Automated Security Reviews in a Continuous Integration Environment <i>Richard Fry, Information Security Manager, Swinton Insurance (Speaking on behalf of Quotium)</i>

13.20-13.45	The Hunted Becomes the Hunter <i>Darren Anstee, Director of Solutions Architects, Arbor Networks</i>
14.00-14.25	Beyond Risk Avoidance: Demonstrating the True ROI of your Application Security Programme <i>Gearoid O'Connor, Senior Security Programme Manager, Veracode</i>
14.40-15.05	Innovation and The European Cybersecurity Research Landscape: From Academia to Business <i>Tom Ilube, CEO, Crossword CyberSecurity</i>
15.20-15.45	Technology is not Enough: Full Security Relies on Processes and People <i>Terry Greer-King, Director, Cyber Security, Cisco</i>
16.00-16.25	Hey You, Want To Come onto My Cloud? <i>Robin King, CEO, DeepSecure</i> <i>John Godwin, Head of IA and Compliance, Skyscape Cloud Services</i>
16.40-17.05	Why Women in Security are Being Paid More <i>Karla Jobling, Operations Director, BeecherMadden</i> <i>Gemma Mahoney, Delivery Director, BeecherMadden</i>

Day Three: Thursday 4 June

10.00-10.25	Defining Moments in the History of Cybersecurity Which Have Led to the Rise of Incident Response <i>Paul Ayers, General Manager, EMEA, Resilient Systems</i>
10.40-11.05	Threat Intelligence – Marketing Hype or Innovation? Discuss <i>James Chappell, CTO, Digital Shadows</i>
11.20-11.45	The Inception Framework: The Strategic Implications of the Modern Threat Landscape <i>Christophe Birkeland, CTO, Malware Analysis, Blue Coat Systems</i>
12.00-12.25	Finding Fortune on the Web via Exposed Fortune 500 Employee Credentials <i>Staffan Truvé, CTO and Co-Founder, Recorded Future</i>
12.40-13.05	Distraction in Depth: Evolving from Defence in Depth to a More Coordinated Strategy <i>Chester Wisniewski, Senior Security Advisor, Sophos</i>

13.20-13.45	Threat Information Sharing in Retail: One Year On. Is it Working? <i>Barmak Meftah, CEO, AlienVault</i>
14.00-14.25	Simplifying the Adoption of Cloud Applications: Identifying, Classifying and Protecting your Organisation's Sensitive Information <i>Gil Zimmermann, CEO/Co-Founder, CloudLock</i> <i>Russell MacDonald, Head of Digital Solutions, PA Consulting</i>
14.40-15.05	Mobile has Changed your Business. Now What about Security? <i>Chris Taylor, Senior Product Manager, Entrust Datacard</i>
15.20-15.45	Using Threat Intelligence to Improve Security Response <i>Piers Wilson, Head of Product Management, Tier-3 Huntsman</i>

Manage security events and cyber threats in real time

- ▲ Automated threat detection and resolution in seconds
- ▲ Real-time security and compliance monitoring
- ▲ Unified Console to consolidate and modernise legacy SIEMs
- ▲ True Behavioural Anomaly Detection



www.huntsmansecurity.com

T: 0845 222 2010 **E:** info@huntsmansecurity.com



TECH TALKS



Intelligent Security: Technical
Approaches to Resilient Security

Gain up-to-the-minute technical tools, techniques and skills to successfully combat today's sophisticated security adversary.

Tech Talks Sponsor:



For the latest programme and speaker updates visit www.infosecurityeurope.com/techtalks

Day One: Tuesday 2 June

10.00-	Opening Misfortune Cookie:
10.25	The Hole in 12 Million Internet Gateways Worldwide <i>Shahar Tal, Vulnerability and Security Research Manager, Check Point Software Technologies</i>
10.40-	People are the Weak Link in Data Security not Technology:
11.05	What Technical Steps can be Taken to Mitigate This? <i>Neil Larkins, Chief Operations Officer, Egress Software Technologies</i>
11.20-	Presentation by Cisco
11.45	<i>Details to be announced</i>
12.00-	Strategic Attack Surface Management: Involving the Business
12.25	<i>Wim Remes, Manager, EMEA Strategic Services, Rapid7</i>
12.40-	Protecting Applications on Amazon Web Services
13.05	<i>Chris Gove, Enterprise Architect, Imperva</i>
13.20-	The Challenge Spectrum
13.45	<i>Ziv Gadod, Senior Security Analyst, Radware Werner Thalmeier, Director Security Solutions, Radware</i>

14.00-	Tracking Malware in Criminal Internet Neighbourhoods
14.25	<i>Dhia Mahjoub, Senior Security Researcher, OpenDNS</i>
14.40-	Optimising the Mobile Cloud Era Through Agility and Automation
15.05	<i>Ian Evans, Vice President and Managing Director, EMEA, AirWatch by VMware</i>
15.20-	A Call to Arms: Using a Working Model of the Attack Surface to Improve Incident Response
15.45	<i>Gidi Cohen, CEO and Founder, Skybox Security</i>
16.00-	Securing the Internet of Things Without Boiling the Ocean
16.25	<i>Tim (TK) Keanini, CTO, Lancope</i>
16.40-	Android Live Hacking Demo: How Common Coding Flaws, Overly-Permissive Permissions and DIY Certificates can Compromise Android Security
17.05	<i>Ken Munro, Senior Partner, Pen Test Partners</i>

Day Two: Wednesday 3 June

10.00-	From Fiction to Facts: Examining Real-World Exposure to Credentials Abuse
10.25	<i>Andrew Dulkan, Senior Director of Cyber Innovation, CyberArk</i>
10.40-	Prepare for Cyber War with the Right Intelligence
11.05	<i>Dave Merkel, CTO, FireEye</i>
11.20-	Presentation by Cisco
11.45	<i>Details to be announced</i>
12.00-	Uncloning Advanced Malware: How to Spot and Stop an Evasion
12.25	<i>Marco Cova, Senior Security Researcher, Lastline</i>
12.40-	How Forensics and Cybersecurity Must Co-exist
13.05	<i>Graham Thornburrow-Dobson, Information Security Consultant and Official Instructor, (ISC)²</i>
13.20-	Windows Server 2003 End of Life: Your Problem and My Problem
13.45	<i>Ian Trump, Security Lead, ControlNow</i>

14.00-	Understanding the Data Breaches of 2014: Did it Have to be this Way?
14.25	<i>Patrick Grillo, Senior Director, Product Strategy, Fortinet</i>
14.40-	Office 365 and its Implications for Networking, Security and Compliance
15.05	<i>Klaus Gheri, Vice President Network Security, Barracuda Networks</i>
15.20-	Hacking without Hacking: An Expose into Infrastructure Hacking due to Poor Configuration and Design
15.45	<i>John Stock, Technology Director, Outpost24</i>
16.00-	Swimming with Sharks: The Importance of Hardware for Security
16.25	<i>Ian Pratt, Co-Founder, Bromium</i>
16.40-	DDoS Attacks: What You Can't See Can Hurt You
17.05	<i>Dave Larsen, Chief Technology Officer, Corero Network Security</i>

Day Three: Thursday 4 June

10.00-	Ensuring Your Botnet Takedown Results in a Knockout
10.25	<i>Brian Foster, CTO, Damballa</i>
10.40-	The Virtual World Exposed: Hacking the Cloud
11.05	<i>Jason Hart, Vice President of Cloud Solutions, Safenet</i>
11.20-	Presentation by Cisco
11.45	<i>Details to be announced</i>
12.00-	Achieving Governance via your Software Development Life Cycle
12.25	<i>David Juitt, Chief Security Architect, Ipswitch</i>
12.40-	The Node.js Highway: Attacks are at Full Throttle
13.05	<i>Maty Siman, Founder and CTO, Checkmarx Helen Bravo, Head of Product Management, Checkmarx</i>

13.20-	Turning Security Against You: How Hackers Take Over Your Secure Shell Environment
13.45	<i>Kalle Jääskeläinen, VP, Solutions and Services, SSH Communications Security</i>
14.00-	The Evolution of Malware
14.25	<i>Mark James, Security Specialist, ESET</i>
14.40-	Overcoming Challenges in Deploying NAC Solutions in Highly Distributed Networks with 100.000+ End Points: A Case Study
15.05	<i>Necati Ertugrul, CTO, NATEK</i>
15.20-	Resilient Security Architectures
15.45	<i>Paddy Francis, CTO, Cyber Security, Airbus Defence and Space</i>

WE MAKE YOUR SECURITY AWARENESS CAMPAIGN EFFECTIVE



- SHORT & INSPIRING SECURITY AWARENESS VIDEOS
- EDUCATE YOUR USERS WITH MAXIMUM RESULTS
- READY TO DEPLOY ON YOUR SOFTWARE AND SYSTEMS



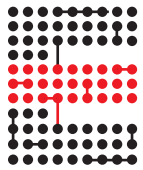
AwareGO produces high quality videos to maximize the impact of security awareness campaigns. Our videos improve employee's security with minimal effect on their productivity. Ultimately enhancing overall security of businesses and organizations.

AwareGO's key differentiators include:

- We think of security awareness as a marketing campaign.
- Our customers help us make our products better and more relevant.
- We can customise the videos to fit your branding and security policies.
- Dynamic culture of innovation, creativity and security make our videos unique.
- Our videos can easily be translated into any language.

Some of our customers





INFORMATION SECURITY EXCHANGE



Next-generation Information Security Methodologies and Tactics

Benefit from the chance to discuss how to tackle the latest challenges in information security and gain fresh perspectives on the latest technologies and research. Featuring in-depth presentations, panel discussions and case studies, the Information Security Exchange brings together end-users and vendors to engage in open dialogue and exchange technical and strategic expertise in a range of formats.

Leave the sessions equipped with new approaches and techniques to enable you to enhance your organisation's information security strategy and tactics.

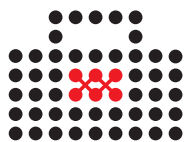
Hear expert opinions from leading organisations including **BSI, MobileIron, Bitdefender, L-3 TRL Technology, Radware, Pulse Secure, LRQA, AVG Business, Atos** and **Level 3 Communications**

Topics to be addressed include:

- **Moving the Attack Surface: A Coherent Strategy for Protecting Interconnected Information and Operational Systems**
L-3 TRL Technology
- **The Next Cyber War: Geo-Political Events and Cyber-Attacks** Radware
- **The Benefits of the 3 C's of BYOD: Connectivity, Compliance & Containerisation** Pulse Secure

- **Can Technology Save us from Evolving Cybersecurity Threats?** Level 3 Communications
- **What Security Pros Can Learn from Shadow IT: Lessons from the Infrastructure and Operations Playbook** Bitdefender
- **Say Goodbye to Enterprise IT: Welcome to the Mobile First World** MobileIron

To view the full agenda and the latest speaker and session updates, please visit www.infosecurityeurope.com/ise



TECHNOLOGY SHOWCASE



Innovative Technologies to Address the Latest Information Security Risks

- Hear about new and existing products, services and solutions as exhibitors take to the stage to demonstrate the capabilities of their information security technologies.
- Pose your questions directly to the solution providers and find the answers you've been looking for.
- Take this opportunity to gain the insight you need to maximise ROI on your solution purchases.

Hear from leading organisations including **Box, Cryptzone, CyberArk, ExtraHop, GB&Smith, Jenrick IT, Lumension, Pulse Secure, BackBox, Secure Islands Technologies, TrapX Security, VMWare, Wallix** and **Zscaler**

To view the full agenda and the latest speaker and session updates, please visit www.infosecurityeurope.com/techshowcase



CYBER INNOVATION SHOWCASE



Showcasing the Latest Innovations in Cybersecurity

The cyber innovation showcase gives you the opportunity to stay abreast of new innovations in information security technologies. This newly added theatre includes presentations from the 11 shortlisted companies from the UK nationwide competition launched through the Cyber Growth Partnership, with the support of BIS and techUK to find the **UK's Most Innovative Small Cyber Security Company of the Year**. This showcase will give you deeper insight into the products these and other companies have designed, developed and brought to market.

Presenting organisations include **Abatis, Cambridge Intelligence, Crypta Labs, Geolang, Minded Security, Purelifi, Sedicii, Westgate Cyber Security, ZoneFox, Cyberlytic, Pervade Software, BAE Systems** and **SSH Communications Security**.

To view the full agenda and the latest speaker and session updates, please visit www.infosecurityeurope.com/cyberinnovationshowcase



NEW PRODUCTS AND SERVICES

Acuity Risk Management



Stand F123

www.acuityrm.com

info@acuityrm.com

+44 20 7297 2086

At Infosecurity Europe 2015, Acuity will showcase its new STREAM Version 4 GRC software, which scales seamlessly from a free single-user edition to an unlimited enterprise edition.

The configurable, scalable and easy to use software has been improved and extended in Version 4 with a range of new features including a Custom Report Builder, a new API for third party interfaces and exciting new 'risk delta' functionality for identifying and prioritizing control improvements with the greatest risk return on investment.

STREAM is used world-wide for automation of risk registers; risk and control self-assessments; and integrated cybersecurity management systems, including ISO 27001, ISF and the NIST Cyber Security Framework. STREAM integrates data from third party tools with self-assessments and audits to provide a business risk perspective for senior business managers.

A free single-user edition of STREAM Version 4 is available from <http://www.acuityrm.com/> together with access to Acuity's on-line STREAM Training Portal.

Infosecurity Magazine



Stand M60

www.infosecurity-magazine.com

Infosecurity.magazine@reedexpo.co.uk

Infosecurity Magazine has over 10 years of experience providing knowledge and insight into the information security industry. Its multiple award-winning editorial content provides compelling features both online and in print that focus on hot topics and trends, in-depth news analysis and opinion columns from industry experts.

Infosecurity Magazine also provides free educational content, including webinars, virtual conferences and training opportunities endorsed by all major industry accreditation bodies, which are therefore considered a key learning resource for industry professionals.

Stop by *Infosecurity Magazine's* stand at Infosecurity Europe and try your hand at protecting your network from malware and insider threats in our brand new and exclusive computer game – challenge your colleagues and take on the bad guys for a chance to win prizes and be crowned 2015 Infosecurity Chief Protection Officer.

Spikes Security



Stand G100

www.spikes.com

contact@spikes.com

+1-408-755-5713

Spikes Security, founded in 2012, is a ventured-backed network security start-up based in Los Gatos, California. The company is focused on preventing all web malware from targeting web browsers and infecting endpoint devices. This is critically important because web browsers are highly vulnerable and have become a primary attack vector used by cyber-criminals to gain access to enterprise networks. Spikes Security prevents all web malware through the use of innovative, patent-pending isolation technology, which ensures that all web content is rendered on a specialised appliance outside the network, then transformed into a benign, malware-free format and delivered safely to end-users inside the corporate network. Discover how you can make the web safe for your organisation. Visit Spikes Security at stand #G100.



SECURITY WORKSHOPS



Intelligent Security: Practical Techniques and Strategies to Protect Information Assets

- Take advantage of the opportunity to build your skills during in-depth, extended workshop sessions covering a range of business-critical topics in a practical and interactive format.
- Develop your skills whilst engaging with your peers and learning from leading security experts.
- Leave the sessions with practical know-how and learning that can be applied directly to your business.

Organisations offering workshops include (ISC)², cybX, VMWare, Cloud Security Alliance, NextSec and the IISP.

Topics to be addressed include:

Professionalising Information Security BCS
Have You Got What it Takes to be a Crisis Leader?

Infosecurity Magazine

- **CISSP Preview: Security and Risk Management (ISC)²**
- **CISSP Preview: Security Assessment and Testing (ISC)²**
- **Developing Organisational Cyber Resilience, cybX**
- **European Privacy Compliance and Security SLA: CSA Addressing the Challenges, CSA**

To view the full agenda and the latest speaker and session updates, please visit www.infosecurityeurope.com/securityworkshops



SECURITY TRAINING

Certificate of Cloud Security Knowledge (CCSK)



Discover how to optimise cloud security within your organisation

- Access the strategic and tactical know-how to overcome cloud security challenges.
- Discover how to protect and control sensitive data in the cloud.
- Understand how to implement robust security controls to optimise cloud security.

Date: Thursday 4th June: 9.00-17.00

Price: £649+VAT

Register and find out more at www.infosecurityeurope.com/ccsk

Cybersecurity Fundamentals



- Develop a solid understanding of the principles of cybersecurity including information security architecture, application security, risks and vulnerabilities and incident response.
- Evaluate the security implications of evolving technologies.
- Access insight into the importance of cybersecurity, and the integral role of cybersecurity.

Date: Tuesday 2nd and Wednesday 3rd June

Standard Rate: £599 +VAT

ISACA member rate: £499 + VAT

Register and find out more at www.infosecurityeurope.com/isaca

DevOps Foundation Certification Course



Understand how to utilise DevOps to optimise workflow and maximise business agility

Date: Two-day training course -

Day 1: Live, instructor lead, virtual session: Monday 1st June, 8.30-18.00 BST

Day 2: Face-to-face training course at Infosecurity Europe, Olympia London: Wednesday 3rd June, 8.30-18.00 BST

Price: £749 +VAT

Register and find out more at www.infosecurityeurope.com/devops

How to Turn the Human Firewall On



Discover how to create a robust enterprise security culture by effectively engaging the employee

- Understand how to secure employee engagement and increase the likelihood of a positive security choice.
- Gain insight into how behaviours are formed and influenced and learn how to integrate them into security strategy and day-to-day operations.
- Find out how to implement effective training and awareness programmes to positively impact security behaviours.

Date: Thursday 4th June, 9.00-17.00

Price: £649 +VAT

Register and find out more at www.infosecurityeurope.com/analogies



» PROVIDING CONTENT & CONTACTS IN PERSON, IN PRINT & ONLINE

WHATEVER YOUR MARKETING NEEDS -
WHETHER BRANDING, THOUGHT LEADERSHIP OR
LEAD GENERATION - WE HAVE THE PLATFORM TO SUIT YOU:



VIRTUAL CONFERENCES



WEBINARS



WHITE PAPERS



E-NEWSLETTERS



RSS FEED

TO DISCUSS THESE & OTHER BESPOKE OPPORTUNITIES CONTACT
MALCOLM WELLS - +44 20 8910 7718
MALCOLM.WELLS@REEDEXPO.CO.UK

Introducing New Features



UK CYBER INNOVATION ZONE

tech^{UK}



The Cyber Growth Partnership, in association with The Department for Business, Innovation & Skills and techUK, is supporting a new UK Cyber Innovation Zone at Infosecurity Europe 2015. The zone is being used to showcase 11 small innovative UK cybersecurity businesses. The magnificent 11, exhibiting their innovation at Infosecurity Europe this year, are:

- Abatis (UK) Ltd
- Cambridge Intelligence
- Crypta Labs
- Cyberlytic
- Geolang
- Minded Security UK Ltd.
- Pervade Software Ltd.
- Purelifi
- Sedicii Ltd.
- Westgate Cyber Security Limited
- ZoneFox



NEW EXHIBITOR ZONE

The New Exhibitor Zone will be making its fifth appearance at Infosecurity Europe this year. This highly popular area for visitors is filled by over 50 new exhibitors to the

event, from around the world, showcasing and demonstrating their innovative products and services never before seen at Infosecurity Europe – the ideal place to identify and learn about the information and cybersecurity solutions of the future.



See a list of all new companies exhibiting at Infosecurity Europe:
www.infosecurityeurope.com/nez



DevOps Connect: Rugged DevOps at Infosecurity Europe is a full day of learning, networking and thought leadership focused on DevOps and security's role in the software development lifecycle. Bringing together the DevOps and the information security communities the day will include panel discussions, presentations, and industry case studies on the integration of security and DevOps.

Thursday, 4th June 2015, 09:00 - 17:00

www.infosecurityeurope.com/ruggedDevOps



The Risk and Network Threat (RANT) Forum is a unique community of information security professionals who work within end-user organisations. This ever-popular event is created for industry by industry and allows you to voice your concerns and opinions on all of the pertinent topics and issues that you deal with every day as an information security professional. RANT is proud to be working together with Infosecurity Europe and their brilliant partner Zscaler to host a RANT Special within the exhibition in the Henley Suite 1 on the first day of Infosecurity Europe.

Tuesday, 2 June 2015, 15:00 - 17:30

www.infosecurityeurope.com/rant



Impressions from Infosecurity Europe 2014



Security Made in...

As a global information security hub, Infosecurity Europe addresses international information security challenges and brings together international vendors and service providers to

share their latest industry solutions and technologies. Infosecurity Europe's country pavilions showcase country-specific technology and innovations. www.infosecurityeurope.com/countrypavilions

USA



- Opswat
- Cyphort Inc
- Recorded Future
- Security Innovation
- Adallom
- CO3 Sysytems
- AccellOps Inc
- Observe IT
- whiteCryption
- Threatstream
- Authentify
- Firemon
- Arxan
- Emerging Threats, a Proofpoint Company
- Tanium
- Sonatype
- US Commercial Services

France



- Bertin IT
- Cybelangel
- DenyAll
- GB&Smith
- Hexatrust
- ILEX International
- OpenTrust
- Oveliane
- Pradeo Security Systems
- Qosmos
- Wallix

Germany



- Giegerich & Partner GmbH
- Pyramid Computer GmbH
- Sirrix AG
- Virtual Solution AG

Israel



- Secure Island Technologies
- Kaymera Technologies
- TrapX Security

Northern Ireland



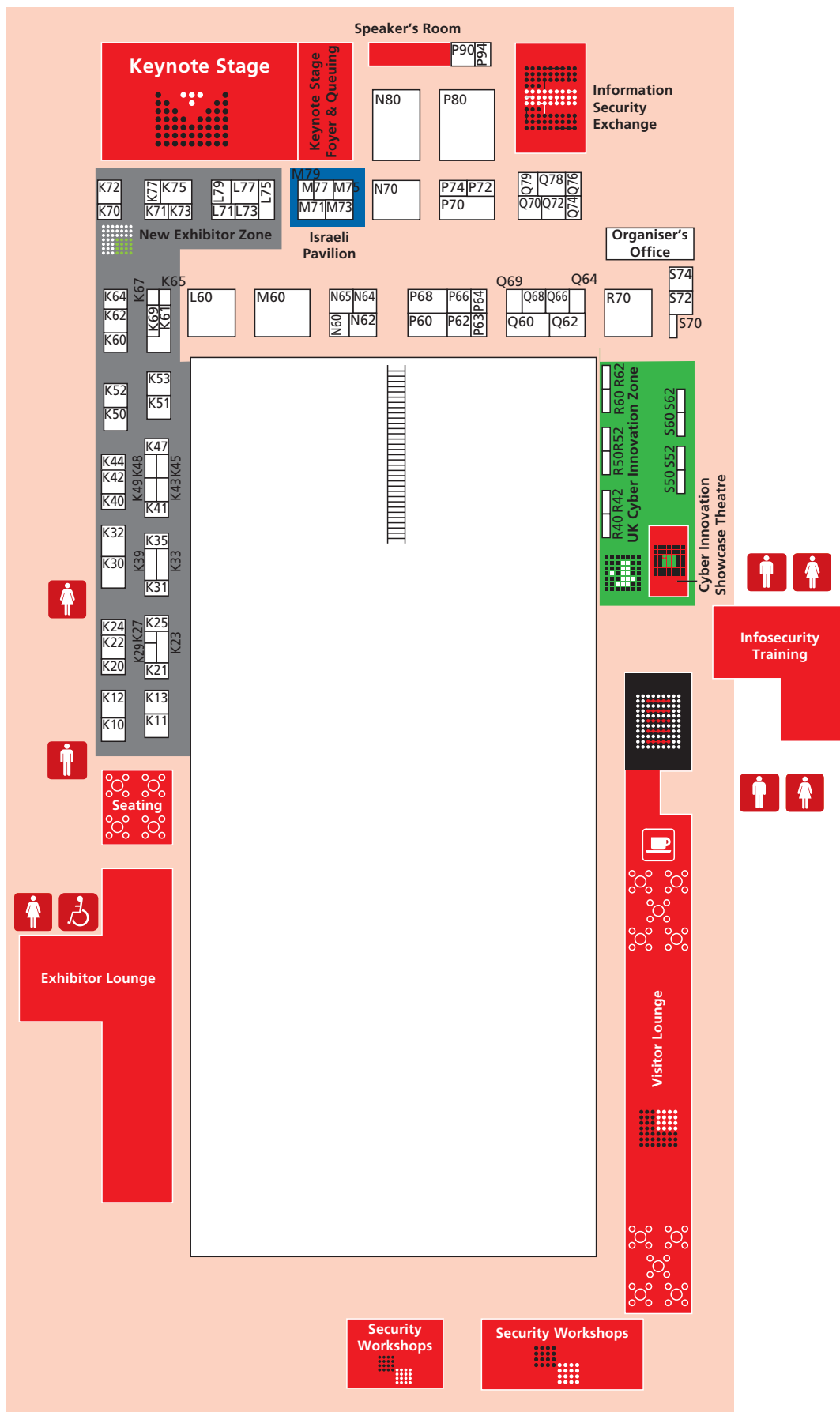
- CSIT
- Sabsa Courses
- DiskShred
- Titan IC Systems Ltd.

Ground floor





Level 1



A-Z Exhibitor List

(ISC) ² UK Ltd	A32	C		Encode UK Ltd	B222
3M (UK) Plc	E204	Cambridge Intelligence	R40B	Endace Europe Ltd	B40
A		Centrify	C265	Enforcive Systems Ltd.	A100
Abatis UK Ltd	R40A	Certes Networks	A110	Entrust (Europe) Ltd	E40
Accellion, Inc.	D235	CertiVox UK Ltd	K73	E-Recycling Limited t/a Euro-Recycling	A40
AccelOps, Inc.	F182	CESG	C142	eSentire Inc	A70
AccessData	E185	Check Point Software Technologies	C60	Eset spol.sr.o	D40
activereach Ltd	F45	Checkmarx	B45	European Reseller	M61
Acuity Risk Management	F123	Chemring Technology Solutions	D222	Evolution Recruitment Solutions Ltd	P64
Acumin Consulting Ltd.	F80	Cigital	A170	Exclusive Networks	G124
Adallom	F180	CipherCloud	G60	ExtraHop	C262
Aerohive Networks	C200	Cisco International Limited CIL	F120	F	
Agileise Ltd	N60	Citrix Systems (UK) Ltd	F100	F5 Networks	B240
Airbus DS limited	D45	City University London	G164	Feitian Technologies Co., Ltd.	Q60
AirWatch	C100	CloudLock, Inc.	B210	FireEye UK Ltd	C120
Akamai Technologies Ltd.	D25	Codenomicon	A50	FireMon	F170
AlgoSec	B60	Commissum	G104	ForeScout Technologies, Inc.	G20
Alienvault	F65	ControlNow	K75	Fortinet Inc	E140
APM Group	C144	Corero Network Security	E269		
APM Group	Smart Space	CoSoSys Ltd.	E183	G	
ARBOR NETWORKS UK LIMITED	B125	CREST	K48	GB&Smith	F200
Arxan	G175	Crossword Cybersecurity	K77	GB&Smith	F200
Authentify	G184	Crypta Labs	R40C	Geolang Ltd	R40D
Avecto Ltd	H50	Cryptzone UK Ltd	F290	Giegerich & Partner GmbH	G160
AVG Technologies UK Ltd.	F85	CWT Meetings & Events on behalf of Gemalto	G120	Gigamon UK Limited	D180
B		CYBELANGEL	F200	H	
BAE Systems	B160	Cyber-Ark Software (UK) Ltd.	E60	HEXATRUST	F200
BalaBit IT Security	G70	Cyberlytic	R40J	Hitachi ID Systems	G142
baramundi software AG	D184	Cyberoam Technologies Pvt. Ltd.	G140		
Barclay Simpson	B62	Cybertinel	B200	I	
Barracuda Networks	D140	Cyphort	G193	Iasme Consortium Ltd	P63
BCC Risk Advisory	L74	D		iboss Network Security Ltd	E45
BCS	A115	Damballa, Inc.	C80	Identiv	F48
BeCrypt Ltd	E85	Darktrace Limited	N80	Idax Software	K25
BeecherMadden	A105	Deep-Secure Ltd.	F104	ILEX INTERNATIONAL	F200
Bertin IT	F200	Dell Corporation Limited	D270	Imperva UK Ltd	C20
BeyondTrust	F145	DenyAll	F200	Imprivata UK Limited	G65
Bit9	D238	DeviceLock, Inc.	P11	Infinigate UK	E280
bitdefender	C180	Digital Guardian Inc	B181	Infosecurity Magazine	M60
Black Duck Software	E83	Digital Shadows Limited	H160	Information Security Forum Ltd.	C204
Blanco UK	C15	DOSarrest Internet Security LTD	F142	Institute of Information Security Professionals	A65
Blue Coat Systems Limited	D220	Druva Europe Ltd	Q68	Invest NI	N70
Bob's Business Ltd.	A55	E		Ipswitch File Transfer	F140
Bomgar	F220	e92plus	F25	ISACA	H60
Bournemouth University	L77	eco- Association of the		ISMG, Corp.	P18
Box.com (UK) Ltd	C190	German Internet Industry	G160	ISSA UK	Q69
Bromium	D240	ECSC	E160	iStorage Limited	B260
BSI	Q79	Egress Software Technologies Ltd	C160	ITSA	A60
Bull S.A.S.	F78	Emerging Threats	G178	Ixia	B120
BusinessFrance	F200				



J		Pervade Software	R40K	Association Germany	G160
Jenrick:IT	A180	PhishMe Inc	F165	Tenable Network Security Limited	E260
K		Ping Identity	E250	The Open University	K65
Kaymera Technologies	M79	Plixer	E224	Threat Finder Ltd	P66
L		Pradeo Security Systems	F200	ThreatStream	G182
L-3 TRL Technology	B80	Protection Group International	B220	Thycotic Software Ltd	H90
LampKicking Ltd	L71	Pulse Secure	F280	Tier-3 Security Ltd	D160
Lancope Inc	F20	Purelifi	R40F	Titania	F40
Lastline, Inc	K53	Pyramid Computer GmbH	G160	TITUS Inc	E262
Level 3	C45	Q		TrapX Security	M75
LibraEsva Srl	G10	Qosmos	F200	Trend Micro EMEA (GB) Ltd	D60
Link11 GmbH	C162	Qualys	E20	Tripwire	D20
Lloyds Register Quality Assurance	D15	Quotium Technologies	F102	Tufin Software Technologies Ltd	F125
Logically Secure Ltd	F15	R		Turnkey Consulting	K67
LogRhythm Ltd	E25	Radware	E180	U	
M		RandomStorm Ltd	E43	University Of Oxford	Q70
ManageEngine	B180	RAPID7	E242	Utimaco IS GmbH	H95
Metacompliance Ltd	G40	Recorded Future	G190	V	
Minded Security UK Ltd	R40E	Red Island Consulting Ltd	B185	Varonis UK Ltd	E80
Mobile Iron International	H110	Resilient Systems Europe Limited	F184	Vasco Data Security SA	F160
Mozy	H45	Restricted Intelligence	F290	Veracode, Inc	F10
MWR InfoSecurity	A20	Royal Holloway, University of London	N62	Verisec LTD.	P70
My1login	B225	S		VERISIGN	E200
N		S2S Electronics Ltd	D210	VÍNTEGRIS SL	N65
Natek A.S.	C19	Safeway Solutions LTD	D230	Virtual Solution AG	G160
NetSupport Ltd	B65	SC Magazine	A140	VMware International Limited	F98
NETWORK TECHNOLOGY		Secunet	C164	Voltage Security, Inc.	F60
SOLUTIONS (UK) LIMITED	C200	Secure Islands Technologies Ltd	M73	Vormetric	C140
Network Utilities (Systems) Ltd	P60	Security Cleared Jobs	M20	W	
Netwrix Corporation	C260	Security Innovation	G191	Wallix	F200
Neustar Inc	H150	Sedicii Ltd	R40G	Watchful Software Inc	E206
Nippon Control Systems	K54	Serbus Limited	P72	WatchGuard Technologies	D280
Norse Group	E202	Serco cybX	P68	Webroot International Limited	B100
NQA	G162	ServerChoice	E240	WebSense UK Ltd	D200
NSFOCUS Information		Sirrix AG	G160	Westgate Cyber Security Ltd	R40H
Technology Co., Ltd.	D85	Skybox Security Inc.	C40	whiteCryption	G185
O		Skyhigh Networks	D182	WhiteHat Security	G80
Observe IT	G186	SmoothWall	B140	Wick Hill Ltd	E100
OpenDNS	G68	Sonatype, Inc	G172	Y	
OpenTrust	F200	Sophos Limited	D260	Yoh Solutions Limited	K70
OPSWAT	G196	Spikes Security, Inc.	G100	Z	
Origin Storage	L11	Splunk Services UK Ltd	B20	Zonefox	R40I
Outpost24 UK	E65	SSH Communications		Zscaler Inc	K61
Oveliane	F200	Security Corporation	D83		
P		SSL247	C210		
Palo Alto Networks (UK) Ltd	D100	SureCloud	D48		
Pen Test Partners	D80	Swivel Secure Ltd.	F82		
Pentese Limited	A150	T			
Pentest Limited	P74	Tabernus Europe Ltd	B182		
Pentura Limited	D225	Tanium	G170		
Perforce Software	K50	Tatius	K27		
Perspecsys Corp.	G144	TeleTrusT – IT Security			
		Association Germany	G160		
		TeleTrusT – IT Security			

This information was correct at the time of going to print. For the latest exhibitor list, please visit:
www.infosecurityeurope.com/exhibitors

This information was correct at the time of going to print. For the latest exhibitor list, please visit:
www.infosecurityeurope.com/exhibitors

20TH INFOSECURITY EUROPE CONFERENCE & EXHIBITION

SEE YOU THERE

Intelligent security

Protect. Detect. Respond. Recover.

CELEBRATING 20 YEARS

02-04 JUNE 15
OLYMPIA LONDON UK

Download
the
Infosecurity
Europe
Mobile App

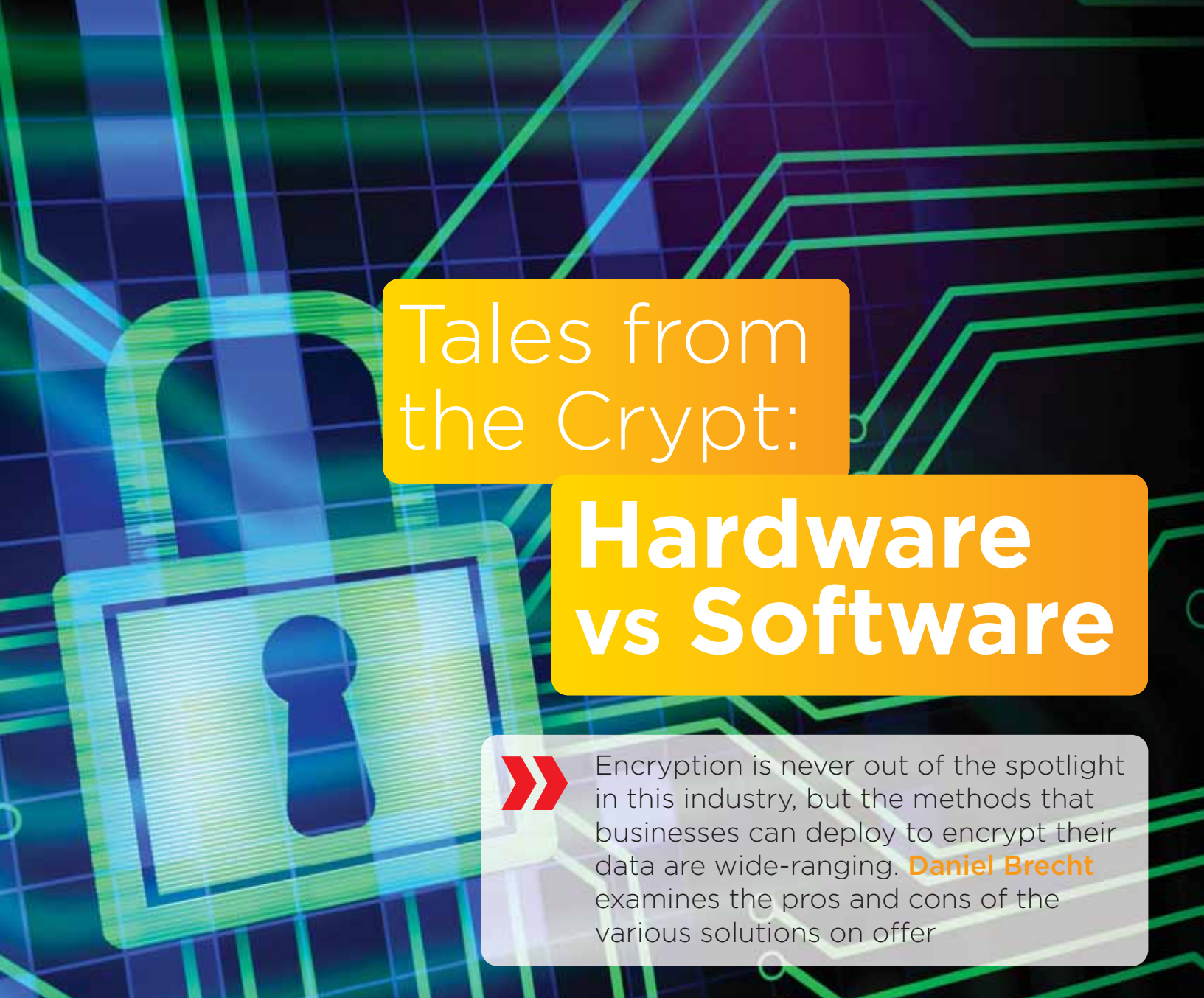


New Features Include:
Networking Live Feed,
Conference Programme,
Exhibitor Directory,
My Agenda, Interactive Floor
Plan, Product Directory,
Polls & Surveys

Organised by:



infosecurity[™]
GROUP



Tales from the Crypt:

Hardware vs Software



Encryption is never out of the spotlight in this industry, but the methods that businesses can deploy to encrypt their data are wide-ranging. **Daniel Brecht** examines the pros and cons of the various solutions on offer

With the use of mobile devices booming, and attacks against government networks and business databases escalating, data security has become a hot topic for IT system managers and users alike. Today's technology advances have spurred a number of solutions to meet the requirements and the pockets of everybody who needs to secure a machine, from a simple home computer, to the most sophisticated networks. Sorting through so many different solutions, however, can be overwhelming.

Whether to opt for software-based or hardware-based solutions is the first decision users are faced with, and it's not an easy choice. Although both technologies

combat unauthorized access to data, they do have different features and must be evaluated carefully before implementation.

Software-Based Encryption

Software encryption programs are more prevalent than hardware solutions today. As they can be used to protect all devices within an organization, these solutions can be cost effective as well as easy to use, upgrade and update. Software encryption is readily available for all major operating systems and can protect data at rest, in transit, and stored on different devices. Software-based encryption often includes additional security features that complement encryption, which cannot come directly from the hardware.

The protection granted by these solutions, however, is as strong as the level of security of the operating system of the device. A security flaw in the OS can easily compromise the security provided by the encryption code. Encryption software can also be complicated to configure for advanced use and, potentially, could be turned off by users. Performance degradation is a notable problem with this type of encryption.

Hardware-Based Encryption

Hardware-based encryption uses a device's on-board security to perform encryption and decryption. It is self-contained and does not require the help of any additional software. Therefore, it is essentially free



Hardware encryption is most advisable when protecting data on portable devices

from the possibility of contamination, malicious code infection, or vulnerability.

When a device is used on a host computer, a good hardware-based solution requires no drivers to be loaded, so no interaction with the processes of the host system is required. It also requires minimum configuration and user interaction and does not cause performance degradation.

A hardware-based solution is most advisable when protecting sensitive data on a portable device such as a laptop or a USB flash drive; it is also effective when protecting data at rest. Drives containing sensitive data like that pertaining to financial, healthcare or government fields are better protected through hardware keys that can be effective even if drives are stolen and installed in other computers.

Self-encrypted drives (SEDs) are an excellent option for high-security environments. With SEDs, the encryption is on the drive media where the disk encryption key (DEK) used to encrypt and decrypt is securely stored. The DEK relies on a drive controller to automatically encrypt all data to the drive and decrypt it as it leaves the drive. Nothing, from the encryption keys to the authentication of the user, is exposed in the memory or processor of the host computer, making the system less vulnerable to attacks aimed at the encryption key.

Hardware-based encryption offers stronger resilience against some common, not-so-sophisticated attacks. In general, malicious hackers won't be able to apply brute-force attacks to a hardware-encrypted system as the crypto module will shut down the system and possibly compromise data after a certain number of password-cracking attempts. With software-based solutions, however, hackers might be able to locate and possibly reset the counters as well as copy the encrypted file to different systems for parallel cracking attempts.

Hardware solutions, however, might be impractical due to cost. Hardware encryption is also tied to a particular device and one solution cannot be applied to the entire system and all its parts. Updates are also possible only through device substitution.

The Debate

There is no single answer to companies' encryption needs, stresses Bruce Schneier, CTO of Resilient Systems and creator of the blog Schneier on Security.

"Software is easier because it is more flexible," he says, "and hardware is faster when that is needed. My preference is software, because I tend to use general purpose hardware and specific software. So my email encryption, web encryption, IM encryption is all software. But the software

might use the hardware-specific instructions in the Intel chip for encryption."

Nico de Corato, telecommunication engineer and founder of DubaiBlog, has a similar approach when it comes to choosing encryption solutions: "Each device requires software in order to operate, and a device is nothing else than hardware. You could not really choose between hardware and software; there is a total interdependence."

The solutions used depend on the needs of the individual, he adds: "In some cases you can choose, and often I'm the one preferring software solutions. For example, if you need to buy a new GPS, the best solution is probably to download the application on your existing devices (eg a smartphone). This way, you are always going to have the GPS with you; you are going to pay much less than buying a new GPS-device. The same goes for encryption software solutions."

Companies need to consider factors like impact on performance, backup, security and available resources to decide on proper encryption implementation. Businesses should consider the risks involved in losing the data they handle, but also how long they need to keep data encrypted and how well they would be able to manage encrypting keys with each solution.

It is also important, in light of the strict regulations that have been issued for data protection (such as HIPAA and PCI), that businesses choose the solution that allows them to be fully compliant.

Different considerations guide the choice. According to Tom Brennan, managing partner of cybersecurity consulting company ProactiveRISK, "In the commercial space it is mostly about price. With .GOV clients, it is more about data classification right."

When budget is a concern, the choice is often to steer away from hardware-based solutions in favor of software solutions that can be implemented across the board. In addition, "rather than deal with the expense and inconvenience of being locked into upgrading one proprietary hardware platform every few years, some prefer to use software," Brennan adds.



Industry Models

"Recent security breaches in multiple industries – including entertainment, retail, and healthcare – tell us that large enterprises are not paying enough attention to security best practices," says Dan Timpson, CTO at certificate authority DigiCert.

"In addition, many of these companies lack basic security measures. According to the Online Trust Alliance, 90% of data breaches in 2014 could have been prevented."

The potential consequence of a data, privacy, or network security breach is very significant. According to the Ponemon Institute's *2014 Cost of a Data Breach Study*, data breaches now cost \$3.5m on average, and the cost per lost or stolen record is \$145. In a previous report, the Ponemon Institute reported that the average value of a lost laptop is \$49,246, with only 2% accounting for the hardware replacement costs. Encryption could abate this sum by \$20,000 as it prevents criminals from accessing and using data contained within.

Sometimes the size of a company makes for a different approach. Larger companies with massive security departments and large budgets probably already have a valid security posture, but smaller businesses might not be treating the issue with the importance it deserves. Many SMB managers believe that only larger companies are the target of malicious hackers. That couldn't be further from the truth.

Symantec's *2014 Internet Security Threat Report* showed that companies with less

Software is easier because it is more flexible and hardware is faster when that is needed

Bruce Schneier
Resilient Systems

than 250 employees accounted for more than half of all targeted attacks (61%) in 2013, an 11% increase from the previous year. A study by the National Cyber Security Alliance reported that 20% of small businesses fall victim to cybercrime each year.

Timpson comments that "using software-based encryption is straightforward and may be more approachable for a smaller business that does not have an on-site IT admin dedicated to data security measures."

However, this is a valid solution only if companies realize that "the need to outsource this work brings the responsibility to find companies that are trustworthy and vet their products and services to ensure a good fit," he adds.

Timpson believes that "introducing a third party increases the potential for vulnerability." Although hardware encryption is perceived as more costly due to the upfront investments that are needed to

supply an entire organization, Timpson believes that "in the long run, hardware can reduce costs with IT labor, user productivity, and licensing fees."

So, what is the best solution to protect data? It depends on where you are trying to protect it.

When data is at rest, especially on removable devices,

hardware-based encryption is often best. By encrypting entire disks or USB drives, everything is secure, from directories to file systems to content. Authentication should be done prior to booting so that not even the OS is started if the user is unauthorized. However, smaller companies might find it hard to justify the expense even for the added security and better systems performance.

If data is in transit, however, file level encryption is more appropriate: files and folders are singularly encrypted and stay encrypted regardless of how and where they are transferred. Possibly less expensive, these solutions are prone to a number of drawbacks from performance degradation to less-than-perfect protection due to hackers exploiting OS and memory vulnerabilities that expose encryption keys.

New theories and technology advances could eventually change that. As Andrew Avanesian, executive vice-president of consultancy and technology services at endpoint security software firm Avecto, explains, "AES instruction sets, which are included in some modern processors, allow software encryption to be more efficient and perform better without relying on dedicated hardware but applications need to be optimized to take advantage of this."

Choosing carefully is paramount, but there is no place for indecision. Avanesian believes the real problem is that "some organizations can get hung up about encrypting devices and end up delaying implementations. With the increasing portability of devices and BYOD, it is important to get some level of encryption setup as soon as possible."

Encryption is necessary and is the best mechanism to protect data confidentiality, integrity and genuineness. It minimizes the chance of security breaches and adds layers of protection to secure data. Costs related to data loss and requirements dictated by law should be incentive enough for all businesses to adopt solutions, regardless of whether they are hardware-based or software-based.



Mobile working practices necessitate a considered approach to encryption for organizations

Should Companies Invest More in Skills or Tools?

Point..

People are the Most Important Piece of the Cybersecurity Puzzle

In IT, there is a common belief that a good programmer is 10 times more valuable and productive than a mediocre one. But developers are working in a relatively static environment. Their goals are constant – once you've written code that works really well, the environment doesn't adapt to break it. There is business change, but the underlying approach is still optimal for that environment.

Cyber is another world – once we solve a problem, the environment and the attackers in it evolve to attempt to invalidate our solution. We must refresh our knowledge, and continually update our work, just to stay in the same place.

If we give a mediocre programmer a value of one, and the rock star equivalent 10, we might find that a mediocre security professional, even after all their tools are factored in, is still a one. The rock star equivalent, with the addition of tools, will become a 100.

Tools are a force multiplier, but multiples of zero are still zero. In the worst case, an incompetent security professional, given powerful tools, may actually become dangerous. For example, it is easy to block legitimate business emails with a poorly configured data loss prevention system, while still allowing essential information to be stolen.

A poor-quality security professional doesn't just fail to implement good security – they can cause a security breach. Social engineering and phishing succeed because of a failure on the part of staff – a failure that cannot be prevented with technology.

There are plenty of people selling tools to solve your problems and superficially this can seem tempting. But default

configurations are for default organizations, and your organization isn't default.

In the right hands, tools can be useful, but in the wrong hands, tools can also be turned against us. Attackers will often attempt to gain access to security control systems and exploit these to extend their footprint within organizations.

Because tools are predictable, attackers train against them until they can defeat them, then they launch attacks – only a swift response by skilled people can outwit attackers.

In my years of cybersecurity work, I've found the key ingredients to successful cybersecurity are context, creativity and communication.

You need to look at the context of a situation to understand whether a particular behavior is cause for concern, or perfectly normal. Tools are beset with false alarms – they don't understand context, and hence they over-alarm or miss subtle cues that a skilled human would pick up.

In order to respond to an incident and outwit the attackers, you need creativity. Attackers become familiar with responses, so new ones are more likely to trip them up. Although cybersecurity is a higher priority in many organizations than it once was, it is still rarely a high priority for a development team – you need creativity to help them meet your goals without missing their own.

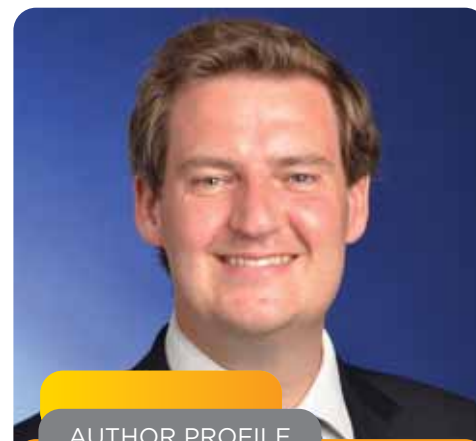
Communication, within and beyond your organization, is key to cybersecurity success. Approachable, friendly members of staff with strong people skills get better information from all directions and convince the entire organization to do the right thing. When was the last time a robot convinced you of anything?

When users are given automated responses that do not convey the logic behind them,

they focus their creativity on circumventing your controls, not embracing them.

Context, creativity and communication are all things that tools are unfortunately terrible at. Pop-up browser warnings are laughably ineffective – most users click 'Yes' without even reading the associated text, but an informed discussion by a passionate security professional can swiftly strengthen a user's online behavior.

I concede that tools are essential to deal with low-level repeated attacks. They automate much of the growing workload that we all face. The shortage of skilled people elevates their importance, but only when properly configured, managed and maintained. Tools without craftspeople give a false sense of security, while they rust in the corner.



AUTHOR PROFILE

Stephen Bonner is a partner in the cybersecurity team at KPMG, where he leads a team focused on financial services. Before KPMG he was group head of information risk management at Barclays. Bonner was inducted into the Infosecurity Europe Hall of Fame in 2010.



.....Counterpoint.....

In Re-assessing Security, Technology Holds the Key

We're now facing the next phase of cybersecurity attacks, with new 'bad guys' and attack vectors. As with any paradigm shift, pundits are up in arms, asking 'How is this happening? Why don't our defenses hold up?' This has ballooned into one of the stronger debates occurring in IT meetings – and even boardrooms – globally.

It raises a key dilemma: budget is finite, so do we hire more security experts, or spend on advanced technology to keep us safe?

Unfortunately, that's a flawed decision process from the start, with either road leading to failure. Simply hiring more IT security experts won't necessarily enhance competency; you may simply find yourself with a greater number of uninformed people.

Likewise, throwing money at an ever-escalating array of firewalls and network appliances is not guaranteed to pay off either. You could find yourself broke and exposed (with lots of iron). So does this mean you're damned if you do, and damned if you don't?

Not necessarily. The fact is that, to fight the current (and future) onslaught of cyber-criminals, organizations must revitalize three core areas: strategies, competencies, and technologies. Start by revisiting your core strategy of defense.

The starting line in the post-Snowden, Target-sensitized, Sony-aware era is one fundamental question: 'Do we have the right strategy to secure data in today's world?'

Most experts agree that the IT industry needs to enact a rapid shift from 'network-centric' to 'data-centric' strategies. With the tidal wave of BYOD and wholesale defection to the cloud, legacy strategies built on a secure-the-perimeter mind-set are no longer adequate; there simply is no network perimeter to secure any longer.

Incredibly sensitive communications – such as confidential emails – are done on BYOD smartphones. Users tap ubiquitous cloud storage for housing product plans, IP, and financials with no idea of the security parameters. Board presentations are delivered to Wi-Fi tablets in coffee shops around the world. Hence, the strategy focus must shift from 'protect the perimeter' to 'protect the data'.

Only a move from 'castle walls' to 'bodyguards' can ensure that information is safe regardless of where it's created, where it's sent, where it's stored, or who finds a way to get their hands on it.

And you can't scale enough to do this with just people – it must be done with technology.

This doesn't mean you should stop investing in intellectual capital. But don't rely on acquiring more so-called experts. Today, every single corporate user is a potential breach point; you can't assign an IT expert to each employee and stay in business.

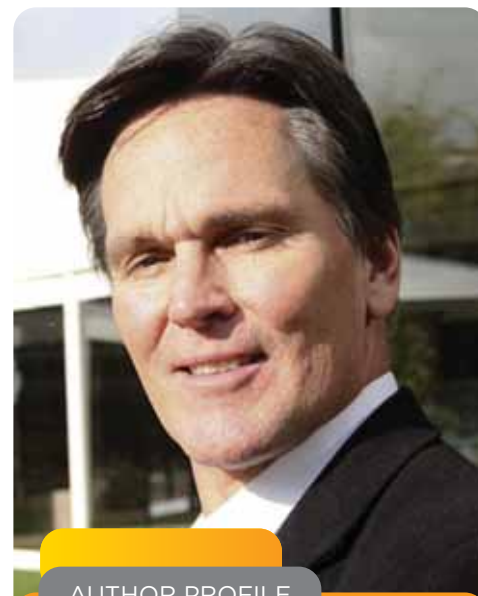
It's simple math: when all users were in a single network perimeter (circa 2000), you could invest in a stronger perimeter, with a few 'guards' patrolling. But now that there is no perimeter (circa 2015), you must realize that the only path to safety is to assign a 'bodyguard' to each user, in essence making sure each user has a mini-CISO riding shotgun at all times. To scale, these mini-CISOs can't be people, they must be technology instances.

This thinking should drive your new technology investment strategies.

Technology to protect today's mobile, cloud-based information has to be ubiquitous, all-encompassing, and smart. It should be ubiquitous in that it protects data on any device users employ; all-encompassing in that it analyzes any kind of data to see if it's sensitive and potentially

toxic; and smart in that it identifies and encrypts sensitive information the moment it's created, staying with it regardless of where it's sent, stored, or used, even if the user doesn't know this is going on.

Prioritize your IT investment strategy to increase and re-validate the competency of your team (~10%); fill 'gaps' that might exist on the team (~10%); and invest in technologies (~80%) that are perimeter-agnostic, and data-centric. That's how you keep from being tomorrow's data breach story of the day.



AUTHOR PROFILE

Charles Foley is chairman and CEO of Watchful Software. He has over 20 years of experience leading both private and public company teams to success. Prior to Watchful Software, he was the chairman and CEO of TimeSight Systems. He has also held senior positions at IBM and Memorex-Telex, and sits on the board of directors as chairman for Critical Links and Phuture Concepts, LLC, while holding advisory positions with RackWare and myPlanit.

» MARKET ANNOUNCEMENTS

Mizuho Bank Deploys VASCO's DIGIPASS 275 to Protect Customers' Online Banking Transactions

Mizuho Bank, the core institution of Mizuho Financial Group and one of Japan's three major banks, has selected VASCO's DIGIPASS 275 authenticator with electronic transaction signing to secure its online retail banking services. The bank wanted to be the first to implement electronic signatures in the Japanese retail banking segment.

The solution from VASCO Data Security International helps secure the bank's online and mobile services, called Mizuho Direct, against fraudulent transactions initiated by hackers. It provides superior

protection against the latest fraud activities such as man-in-the-middle and man-in-the-browser attacks.

The one-time password function in DIGIPASS 275 is used for both authentication at account sign-in and for an electronic signature during transactions such as bank account transfers and payment settlement services.

In March 2008, Mizuho Bank initiated a program of security enhancement for its online banking service, using the VASCO's DIGIPASS GO6 and its VACMAN Controller. This latest upgrade provides further protection against the latest attacks online banking customers may be exposed to.



Good Technology Extends Partnership With Microsoft

Good Technology recently announced a range of innovations that extend Good Work's secure mobility capabilities for Microsoft customers. Good Work now integrates with Microsoft OneDrive for Business for easier document storage and a new Good Dynamics SDK simplifies development of Windows 8.1 and Windows Phone 8.1 apps.

Good also announced the ability to host Good Work in the cloud, on-premise, or in hybrid environments, continuing the company's efforts to deliver maximum flexibility in deployment options. Organizations can confidently and securely support a heterogeneous environment, extending its applications on both Microsoft and non-Microsoft devices with strong security on a unified management platform.

Microsoft and Good Technology have also collaborated for Microsoft Dynamics CRM for Good, which brings Good's secure containerization and government certified security to Microsoft's CRM solution.

As organizations move beyond MDM to mobile apps that drive productivity, CRM apps are in demand by sales organizations. As customer data is highly sensitive and often regulated, IT may be unwilling or unable to offer more CRM access without providing more stringent security controls. Microsoft Dynamics CRM with Good's secure container technology helps to meet the needs of both sales and IT, delivering high value integration for enterprises wanting to accelerate CRM deployments to iPads.



Acunetix Clamps Down on Costly Website Security With Online Solution

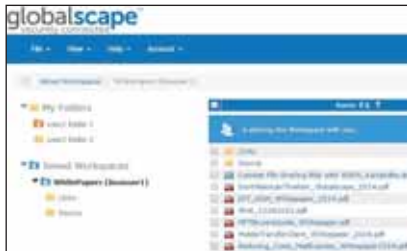
As cybersecurity continues to hit the headlines, even smaller companies can expect to be subject to scrutiny, and securing a website is more important than ever. In response to this, Acunetix is offering the online edition of its vulnerability scanner at a new lower entry price. This new option allows consumers to opt for the ability to scan just one target or website at just \$345.

A vulnerability scanner allows the user to identify any weaknesses in its website architecture which might aid a hacker. They are then given the full details of the problem in order to fix it. While the scanner might previously have been a niche product used by penetration testers, security experts and large corporations, Acunetix has recognized that such products need to be made available to a wider market. To address this, its product and pricing has become more flexible and tailored to multiple types of user. Use of the network scanning element of the product is also currently being offered completely free.

Users can sign up for a trial at:
www.acunetix.com/vulnerability-scanner/register-online-vulnerability-scanner/

Workspaces Provides End User Choice and Ease-of-Use

Globalscape recently announced the release of Workspaces, the latest addition to its managed file transfer solution suite, Enhanced File Transfer.



Workspaces allows users to share folders and files with other users without sacrificing governance, visibility or control. The new offering is an on-premises solution that eliminates the risk of shared-infrastructure or cloud-based services, utilizes multiple secure protocols including HTTPS, FTP, FTPS and SFTP, includes workforce automation to support compliance, and provides for a flexible authentication and encryption. Workspaces also allows IT administrators to retain full control and visibility of the file transfer infrastructure, ensuring the highest levels of security and compliance.

On-premise Cloud Storage and Sharing Alternative from Linoma Software

Linoma Software recently released GoDrive by GoAnywhere, a secure on-premise Enterprise File Sync and Sharing (EFSS) solution that takes document storage out of the cloud and puts IT administrators back in control.

With GoDrive, files and folders can be easily shared between authorized employees and partners with advanced collaboration features including file revision tracking, commenting, a trash bin, media viewing and synchronization with computers running Windows and OS X.

End-to-end encryption protects sensitive files and, since no data is stored in the cloud, organizations maintain local control to meet compliance requirements. GoDrive combines:

- Familiar tools like drag-n-drop and image previews, allowing employees to quickly and easily adopt GoDrive
- Detailed audit logs giving management and compliance officers the peace of mind that all activity is well documented
- Proven security features of the GoAnywhere Services administrative tools, with the addition of device authorization and remote wipe capabilities

GoDrive has no subscription fees, so organizations currently using traditional private or public cloud services could see considerable cost savings.

The multi-platform software can be installed using an on-site or hosted server and allows for unlimited scalability of storage. Find out more at www.GoAnywhere.com

Cleo Wins Xerox Partner of the Year Award

Cleo, provider of secure enterprise data integration solutions, recently announced that it has been awarded the Xerox Outstanding Customer First / Service Support Partner of the Year Award for 2014.

Presented for excellence in customer and service support, this award recognizes the significant contribution of partners to the success of Xerox Corporation and its customers. Xerox has awarded a Partner of the Year award to Cleo for the past five years.

"Cleo is extremely honored to again receive this prestigious partner service award from Xerox Corporation," said Mahesh Rajasekharan, PhD, CEO of Cleo. "This award underscores the depth of Cleo Stream integration with Xerox multi-function products, providing our customers with highly productive solutions for their network fax and dynamic interactive messaging and communication engagement needs. The strategic partnership between Cleo and Xerox for more than a decade demonstrates a continued commitment to providing outstanding value to our joint customers."

Cleo is a member of the Xerox Business Innovation Program. Cleo Stream helps automate and centralize workflows from Xerox multifunction printers, allowing customers to send, receive, store, and track communications securely. For more information visit www.cleo.com

Acuity Adds the NIST Cyber Security Framework to Its STREAM GRC Tool

Last year, The US National Institute of Standards and Technology (NIST) released a framework for 'Improving Critical Infrastructure Cybersecurity'.

Acuity Risk Management, the governance risk and compliance (GRC) specialist, and provider of the popular STREAM Integrated Risk Manager software solution, recently released this framework as the latest addition to its library of pre-configured content. This new addition is a scalable framework originally developed for use by organizations of all sizes.

Use of the NIST framework will raise awareness and communication levels with stakeholders; this can be further enhanced by making use of the STREAM action management, workflow and report builder functionality, to produce board level and other stakeholder reports.

Implementation of the NIST framework will help prioritize critical activities that relate to cybersecurity helping to promote cost-effective cyber security risk management within organizations.

The NIST Cyber Security Framework content for STREAM is available as a free download from the Acuity website for users of any of its STREAM subscriber editions which start at just £295 per year: www.acuityrm.com/store

Centrify Delivers Industry's First Privileged Identity Management Solution for Big Data

Centrify recently announced the industry's first privileged identity management solution for Apache Hadoop-based big data infrastructures, as well as partnerships with big data vendors Cloudera, Hortonworks and MapR Technologies. With Centrify Server Suite 2015, organizations can now leverage its existing Active Directory infrastructure to control access, manage privilege, address auditing requirements and secure machine-to-machine communication with, and across, its Hadoop clusters, nodes and services.

The global Hadoop market, powered by the rise in demand for big data analytics, is forecast to grow from \$2 billion in 2013 to \$50.2 billion by 2020, according to Allied Market Research. Hadoop clusters often contain sensitive personally identifiable information (PII) and other highly regulated data, so auditing and controlling user and administrator access to Hadoop and its underlying server infrastructure is critical to address both security and compliance requirements for regulations such as SOX, PCI and HIPAA.

Centrify has built new features and compatibility enhancements, including Kerberos network authentication, service account management and Active Directory and Hadoop interoperability into Centrify Server Suite 2015. These features address these concerns and extend the security capabilities provided by the Hadoop platform vendors to now offer robust privilege management for Hadoop environments.

CipherCloud Unveils New Global Cloud Data Security Report

CipherCloud recently unveiled its inaugural edition of its Global Cloud Data Security Report, the industry's first global study on cloud data protection challenges and strategies.

The report examines the kinds of data security challenges facing Global 2000 companies and the steps being taken by organizations to mitigate these risks in the cloud. North American organizations represent 65% of the companies. Approximately 23% of the organizations are European. Asia Pacific (APAC) and Latin American (LATAM) organizations comprise the remaining 12%.

Security needs include a combination of technology, legal, financial and political factors at play. In Q1 2015, 64% of organizations identify audit / compliance / privacy as a top challenge, 32% name unprotected data in the cloud as a primary concern, 2% cited malware protection for documents, and 2% cited lack of enough secure cloud file sharing solutions.

Key Findings on the State of Cloud Data Protection include:

- Across geographies, data encryption (81%) led tokenization (19%) at enterprises with a cloud security deployment
- Of the 12 vertical industries profiled, healthcare (38%) topped finance (25%) as the leading sector adopting cloud data protection
- Healthcare and finance respectively protected 100% of all electronic protected health information (ePHI) and personally identifiable information (PII)
- Of the top four sectors, only Government (9%) favored the use of tokenization over encryption



LockLizard Adds Document Watermarking to Its DRM browser

Locklizard's 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 dynamic text and image watermarks. User information is applied when viewing and printing protected PDF documents as an additional security measure to discourage users sharing printed documents.

Locklizard's Web Viewer delivers a highly 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 is used worldwide by fortune 1000 companies, governments, small & large publishers, training companies and research institutes, to help prevent unauthorized use and misuse of information. To learn more visit www.locklizard.com

Thycotic Secret Server 8.8 Enhances Privileged Account Security

Thycotic's newest privileged account management solution, Secret Server 8.8, includes improved support for Secure Shell (SSH) keys, allowing customers with large Linux or UNIX environments or network equipment to more easily control and audit the usage of all of its organization's privileged account passwords regardless of the platform each user is running. Thycotic Secret Server 8.8 also features revamped support for security-conscious customers using hardware security modules (HSM) to protect encryption keys.

"Thycotic is a reliable and agile partner in identity management," said Peter Koch, system administrator for Thycotic customer Dataport. "With the latest release of Secret Server, Thycotic supports one of the best ways of storing your key material – a network HSM. The smart interface allows configuration in a matter of minutes." For more information visit www.thycotic.com

New Barracuda Security Suite Now Shipping From Wick Hill

Now available from Wick Hill is the Barracuda Security Suite, which allows customers to purchase and deploy proven protection across three common threat vectors – email, web browsing, and network perimeters – and independently scale these functions with a purpose-built virtualized platform.

This latest solution is part of Barracuda's Total Threat Protection initiative, which is aimed at providing powerful, robust protection across multiple threat vectors with simplified management. The Barracuda Security Suite integrates next-generation network and content security – including individual virtual instances of the award-winning Barracuda Firewall, Barracuda Web Filter and Barracuda Spam Firewall – on a single appliance.

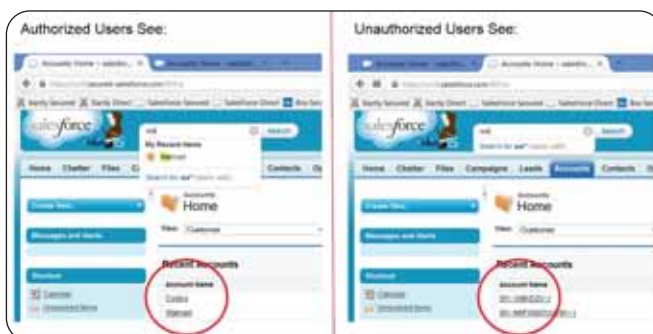
Ian Kipatrick, chairman of Wick Hill Group, commented: "Many early generation UTM's have not been able to scale to defend against today's threat landscape, neither in capacity nor in throughput. The Barracuda Security suite delivers a market-leading solution for users looking to upgrade to a cost-effective, high-performance, high-security solution. We have seen considerable interest in the security suite from our channel partners."

Protect Sensitive Information Before It Gets to the Cloud

Protegrity recently announced the availability of the Protegrity Cloud Gateway to help enterprises adopt software-as-a-service offerings such as Salesforce.com, Box, Gmail, Office365 and Xactly without risking data exposure, impacting business processes or sacrificing SaaS functionality.

Protegrity Cloud Gateway sits between cloud applications and users, replacing sensitive data with flexible, format-preserving tokens or encrypted values before being sent to the cloud. A gateway server cluster handles the traffic to and from the cloud, while the Protegrity Enterprise Security Administrator (ESA) provides client security teams with central control of policy, protection methods, automated key management, security event alerting, reporting, and auditing.

Protegrity Cloud Gateway offers customization via configuration, stateless architecture, continuous discovery and monitoring, and Protegrity vaultless tokenization. Marty Weiss, Director of Protegrity's Cloud Security business commented: "During proof-of-concept tests performed by a client, Protegrity Cloud Gateway was proven to have flexible, empowering performance, be more cost efficient, and able to accomplish many things that the competition was simply not able to do at all or as fast as the Protegrity solution." For more information go to www.protegrity.com/products-services/protegrity-cloud-gateway



PowerBroker Password Safe 5.5: Advanced Threat Analytics and Simplified SSH Key Management

BeyondTrust, a cybersecurity company dedicated to proactively eliminating data breaches from insider privilege abuse and external hacking attacks, recently released version 5.5 of PowerBroker Password Safe.

PowerBroker Password Safe 5.5 is a solution for automating privileged password and privileged session management.

This new release features:

- **Clarity Threat Analytics:** Clarity Threat Analytics correlates data from Retina CS Enterprise Vulnerability Management and other third-party vulnerability management solutions, privileged user and account data from PowerBroker for Windows and PowerBroker for UNIX and Linux, and threat data from the PowerBroker Endpoint Protection Platform. With version 5.5, BeyondTrust now supports data feeds from PowerBroker Password Safe, which enables the patent-pending Clarity Threat Analytics engine to analyze privileged password, user and account behavior.
- **Simplified SSH Key Management:** Between the lack of rotation and the sharing of SSH keys, organizations can lose accountability over its systems which could lead to those systems being vulnerable to exploits. Version 5.5, PowerBroker Password Safe can simplify this process by automatically rotating keys according to a defined schedule and enforcing granular access control and workflow to access SSH keys. For companies with few or no tools or processes in place to protect against privilege misuse on tier 1 UNIX and Linux systems, this capability can greatly simplify the management and secures the use of SSH keys for better control, accountability and security.

BeyondTrust is hosting daily demos at Infosecurity Europe 2015, Stand F145.

Decoupling Encryption: Building Bridges Between CISO and CTO

Opinion..

Data encryption is ever more important; indeed, it is demanded by regulators. As Certes Networks' Paul German explains, it is only by decoupling encryption from its current 'add-on' role that the needs of both CTO and CISO can, finally, be addressed

Data encryption is the gold standard for corporate security. Yet for most organizations, data in motion remains the big corporate conundrum. With the rise of mobile devices and changing working practices, more data than ever is flowing within and outside organizations, and unencrypted data is becoming a major security concern.

The problem, however, is not one of understanding; 51% of organizations want to use encryption to secure sensitive data traffic, but can't, according to Spiceworks' *Global IT Manager Survey*. The problem is that the industry continues to ask businesses to make a compromise by bundling encryption into other parts of the security or networking infrastructure.

For the CISO, under huge pressure from standards bodies such as PCI and ISO, the key requirement is to lock down the network and encrypt all data in motion. For the CTO, tasked with implementing this strategy, while the need to improve security and avoid any breach makes perfect sense, the priority is to deliver a high-performance network and application infrastructure. These two mandates are in direct opposition and lead to conflict that is thorny to resolve.

Escalating Risk

Facing the reality of a potential 75% drop in network performance as a result of turning on encryption within the firewall, router or switch, most CTOs have no option but to renege on the encryption commitment, leaving the CISO powerless and the organization at risk of serious breach.

However committed to the concept of a secure infrastructure, as soon as any user complains about slow throughput or application access problems, the IT team's immediate response is to switch off encryption and deliver a hike in performance. Furthermore, the problem with traditional data-in-motion security is not only the impact on the performance of network devices and applications. The CTO also faces a big resource drain – it can take hours to configure a new site and device level encryption is both easy to misconfigure and hard to monitor and audit.

The issue for both CISO and CTO is being compounded by the rise in BYOD, remote access and cloud-based applications. The use of personal devices and access to externally hosted applications continues to grow – yet the CTO cannot deliver the security required in line with the CISO's requirements. The result is shadow IT.

Flawed Model

This whole problem is due to the security industry's persistence in expecting network devices such as firewalls and routers to double up and deliver encryption. For a firewall, encryption is a hobby, not its main purpose; this approach is simply not adequate for today's threat landscape. For the defense-in-depth model to truly work effectively, organizations need to decouple encryption and deploy dedicated devices designed specifically for this purpose. In addition to avoiding any degradation in network performance, dedicated data-in-motion solutions offer a single point of control, removing the

complex, time-consuming configuration and management overhead.

With one central point of control, responsibility for encryption no longer lies with the IT team but can be handled by the CISO. The process is not only transparent to the essential network equipment, but with user-specific encryption, control is, finally, back in the hands of the person with a mandate to protect the business.

Today, the fact CISOs have the responsibility for protecting sensitive data in motion but no control over the implementation of those controls is clearly flawed. But the need for truly effective encryption has never been greater. It is only by decoupling encryption that an organization can maintain network performance and, critically, enable the CISO to realize the gold standard security vision.



AUTHOR PROFILE

Paul German is VP EMEA of Certes Networks. He has spent more than 18 years in the industry, gaining a broad experience from roles at Sipera Systems, Cisco, Siemens Network Systems and Lehman Brothers.



Slack Space

Car Washes LOVE Facebook

The internet of things (IoT) has gotten buzzier and buzzier as hundreds of heretofore deaf and dumb consumer devices start to come online. But connected things expand the attack surface to entirely new concerns – insecure refrigerators that spy, watches that track, cars that can murder and, drumroll... automated car wash equipment that can post to Facebook.

Independent researcher Billy Rios (formerly of the Google security team) has found that running your car through the wash after a fill-up at the gas station can have consequences.

In the course of an IoT analysis, he found car wash equipment out there running a version of Windows CE on an ARM processor (just like a smartphone), with Telnet enabled and a default five-character password and default username.

"If you know that default username and default password you can do a lot of interesting things," Rios said during the Kaspersky Lab Security Analyst Summit. "Your car wash can send you emails and yes, your car wash is on Facebook, too."

Car washes can freak out their patrons with social media shout-outs including license plate pics, let's say. Or, taken over by the wrong people, car washes could be used to wreak basic prank-related mischief, like changing the type of wash being given or offering a double dose of Turtle Wax. Will #RainyDaysSuck become a trending topic?

However, Rios noted that hackers can carry out more serious damage. For instance, an attacker could disable the safety sensors on the back and front doors of the wash bay, which prevent them from coming down on a person or vehicle.

For the car wash industry though, cybersecurity isn't a main focus.

"Remote access changes your threat model. But to be honest, I don't think we

can trust the makers," Rios said. "The people who made that car wash won't understand any of things we just talked about, like SQL injection or buffer overflows. We're going to see this in other IoT places as well."

Pay-by-Selfie: It's a Thing

Alibaba has a mobile payments idea for the Kardashian age: why not use selfies for payment processing?

Jack Ma, the founder and executive chairman of the Chinese e-commerce behemoth, debuted the idea at CeBIT. Onstage, he demonstrated the function by scanning his face and, via mobile facial recognition, using the scan as a digital signature to purchase a German stamp online.

The service, called 'Smile to Pay', is currently in beta mode, and will be incorporated into the company's Alipay Wallet NFC service in China, with other markets likely to follow. For now, Apple Pay and Google with Google Wallet – both of which use tap-and-pay mechanisms – dominate the mobile payments arena in the West, which has been projected to reach \$16.25bn by 2022.

It's unclear whether it would be used as an extra layer of security or as a standalone authentication mechanism – if it's the latter, there are of course, serious security concerns. Facial recognition has been fooled in the past by simply holding up photographs of the user, or with animated gifs.

But, arguably, it's more secure than simply requiring the verification code on the back of a credit card when buying stuff online or a signature in-store. But, a PIN may still be the safest way to go.

Kill-switch, Engage

USB drives are notorious for acting as modern-day Trojan horses for malware and viruses. But a Russian blogger known as

Selfies may now have a purpose beyond vanity



Dark Purple has created a different kind of doomsday weapon – a thumb drive that will literally fry a computer's circuit board with a high-voltage surge.

"The device is designed to pull in power from USB ports using a DC-to-DC converter until it reaches negative 100 volts, at which point the power is pushed back into the computer to overload its components," reported ESET researcher Kyle Ellison. "This process is run on a loop so that everything possible is broken down."

Goodbye forever, CPU.

ESET noted that Dark Purple is said to have come up with the idea after reading about a case where someone stole a USB drive from a friend's backpack, only to have half of his laptop 'burnt down' when he inserted the device.

Feeling entrepreneurial, the blogger then developed the idea himself, ordered the circuit boards in China, and made a prototype.

The takers for this kind of thing are myriad, from disgruntled employees to sociopathic high school kids, to spies out there in the field. Obviously, to avoid a meltdown, know your thumb drive before you use it, and try to avoid sharing them.



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

Events and conferences come thick and fast in the security industry, and it's sometimes hard to find time to sit and reflect on each one. Add white papers, webinars, and roundtables to the equation, and it's easy to end up with a head-spinning amount of security information, daily.

Many people in this field get used to life on the road, or in the air, traveling far and wide on the speaking circuit to spread the security gospel, and meet with like-minded professionals all over the globe. Then there are the infosec practitioners, who take time out of pressured schedules to join the congregation, attending conferences and virtual events in a bid to expand their understanding and industry knowledge, with the aim of making their organizations – and the world at large – a safer place to conduct online activity.

But with many events offering a slew of different conference sessions and tracks, sometimes it's easy to come away feeling bludgeoned by knowledge. There are so many dedicated and impassioned speakers delivering razor-sharp insight into all facets of this diverse industry, that the glut of quality information can feel overwhelming. The question is: How to step back and focus on the key actionables for you, the individual, who attends events with the hope of bolstering your security intel arsenal?

In a sense this is analogous with some of the concepts of 'threat intelligence' – eradicating the noise on your network to help you establish the security incidents and events that matter: hearing the vital message amid the cacophony, or, to use the old cliché, finding the needle in the haystack.

A theme across security is that incident responders and network defenders don't have enough time to deal with everything; they have to prioritize. If you can identify

sophisticated actors carrying out attacks and spend time firefighting that, and not spend your day tackling nuisance and untargeted malware, you'll be running a more effective security operation.

Prioritizing intelligence is also integral if you're going to keep up-to-date with the

constantly mutating landscape of threats – both to your organization and those facing the world at large. Just as security professionals seek to spend less time sifting through false alarms and get to the nugget of information that will help them stop a catastrophic event on the network, they also need to cut through the noise that the industry generates to make sure that they're getting the right insight in their ongoing quest to become the best security practitioners possible.

Identifying what information is worth taking the time to assimilate is hard. There are innumerable magazine articles, white papers, independent and vendor blogs, research reports, government bills, intel-sharing forums, conference speaker sessions, webinars and more. Each of these could provide the epiphany you need to drive forward your security ambitions.

An additional challenge in keeping track of the security industry's direction is that all too often its various components seem to operate in silos. Government, private sector and the security community all have a role to play and a message to communicate, but trust between each isn't always optimal. So when a government makes an announcement, like the recent Protecting Cyber Networks and National Cybersecurity Protection Advancement acts in the US, the instinctive response from much of the security industry is skeptical at best – and this drives a whole debate that can be both engrossing and distracting.

Consider too the 'white noise' that sellers of security products produce. Many technologies are marketed as the miracle pill to cure all ailments, and practitioners are confronted with a number of buzzwords and passing trends that can be misleading. Endpoint security is the holy writ one year; then it's incident response; once it was the perimeter. All these things have their place, but the promotion of one above the other through noisy marketing and pitching can often distract from the fact that so many security incidents are easily avoidable. It's education and a sound understanding of infrastructure that forms the bedrock of security.

So if you're reading this at Infosecurity Europe or another event, and you're wondering how to make the most of all the intel and information being served up, consider what really matters to you. What do you need to know to become a better security professional? The conversations that will make a difference are the ones that buck the silo mentality trend. A discussion that takes place in an echo chamber – security crowing to security about a certain product



Many technologies are marketed as the miracle pill to cure all ailments, and practitioners are confronted with buzzwords that can be misleading



or technique to prioritize – won't deliver long-term action points.

Find the conversations that look outwards, that aspire to push the industry in a new, more open direction, and that build bridges between sectors. Then, when the dust settles, you may have that nugget of information you need to drive your security practice to the next level.



Mike Hine, Deputy Editor

You can't put a price on high-quality education

REGISTER for the world's biggest free Infosecurity Education Programme!
www.infosecurityeurope.com

CELEBRATING 20 YEARS

02-04 JUNE 15
OLYMPIA LONDON UK

**REGISTER
FREE NOW**

- Access to the experts and industry leaders
- Learn from inspirational speakers
- Network, share, collaborate and build relationships
- Discover new and innovative security solutions
- Earn CPD and CPE credits by attending the free education programme



Managed by:

infosecurity[™]
GROUP

Part of:

 Reed Exhibitions[®]



Engage with Infosecurity Europe on Twitter: @infosecurity #infosec15



NOVEMBER 16TH TO 21ST 2015 • GRAND CONNAUGHT ROOMS, LONDON, WC2

SANS LONDON

THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING

12 SANS INSTITUTE TRAINING COURSES AT ONE EVENT

Immersive Training ★ World Class Instructors ★ GIAC Certification ★ SANS@Night evening talks and networking ★ Social Functions

SEC542

Web App Penetration Testing
and Ethical Hacking

SEC401

Security Essentials
Bootcamp Style

SEC501

Advanced Security Essentials -
Enterprise Defender

SEC503

Intrusion Detection
In-Depth

SEC504

Hacker Tools, Techniques,
Exploits and Incident Handling

SEC511

Continuous Monitoring
and Security Operations

SEC560

Network Penetration Testing
and Ethical Hacking

SEC575

Mobile Device Security
and Ethical Hacking

SEC579

Virtualization and Private
Cloud Security

SEC660

Advanced Penetration Testing,
Exploit Writing, & Ethical Hacking

FOR408

Windows Forensic
Analysis

ICS410

ICS/SCADA
Security Essentials

Register online and see full course descriptions at www.sans.org/event/london-2015

Register and pay before September 30th and **save €375 on course fees**

