Q3 /// 2014 /// VOLUME 11 /// ISSUE 3

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity

Heartbleed Beats On

The Diagnosis for the SSL Bug that Won't Stop Bleeding

PLUS:

XP APOCALYPSE /// PIRATED SOFTWARE /// CYBERCRIME & PUNISHMENT

INTRODUCING

CONTINUOUS MONITORING FOR THE PERIMETER

A New Paradigm for Security

FOR A FREE TRIAL VISIT
QUALYS.COM/**CONTINUOUS**

QUALYS®

The QualysGuard Cloud Platform and integrated suite of solutions helps businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Contents

July/August/September 2014

COVER FEATURE

FEATURES

POINT-COUNTERPOINT

INFOSECURITY

Editor & Publisher
Eleanor Dallaway
eleanor.dallaway@reedexpo.co.uk
+44 (0)208 910 7893

Deputy Editor
Drew Amorosi
drew.amorosi@reedexpo.co.uk
+1 203 722 4005

Online UK News Editor
Phil Muncaster
philmuncaster@gmail.com

Online US News Editor
Tara Seals
sealstara@gmail.com

Contributing Editor
Stephen Pritchard
infosecurity@stephenpritchard.com

ONLINE ADVERTISING:
Jem Duducu
jem.duducu@reedexpo.co.uk
+44 (0)20 8910 7093

Ben Race
ben.race@reedexpo.co.uk
+44 (0)208 9107991

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

Sophie Bottazzi
sophie@showtimemedia.com
+44 (0)1462 420009

MARKETING MANAGER
Rebecca Harper
Rebecca.harper@reedexpo.co.uk
Tel: +44 (0)208 910 7861

ONLINE MARKETING COORDINATOR
Rianna Ramkissoon
Rianna.Ramkissoon@reedexpo.co.uk
Tel: +44 (0)208 439 5463

PRODUCTION SUPPORT MANAGER
Andy Milsom

ISSN 1754-4548

LOSING REVENUE?

- Control who uses your content, what they can do with it, and how long they can use it for
- Stop unauthorized distribution, copying, printing, screen grabbing
- Expire content, and instantly revoke access to information
- Audit document usage, generate statistics and reports

Secure with Locklizard

Fight the Power

It was during an interview at Infosecurity Europe when my interviewee said to me "Every single vendor in this exhibition hall does exactly the same thing" when I realized that I'm actually quite protective about our industry's vendor community. The man, who I won't name (nor will I interview again) proceeded to tell me that his company was the exception to this 'rule'. I'm rolling my eyes even as I recount this conversation.

I'm not going to pretend I've never criticized the marketing methods of the industry's players, or that I believe each and every company to be doing something unique, because that would be a falsity. That aside, our vendor community is a concoction of some – perhaps most – of the best minds and talent in information security. The investment these companies are pouring into research and development is not only impressive, but it's the foundation on which much of our intelligence pivots upon.

Of the twenty interviews I conducted during the three-day spectacle that is Infosecurity Europe, the conversations that stand out in my mind as the most interesting and engaging were all ones with vendors. Take Jack Daniel (Tenable) for example, or James Lyne (Sophos), or Trey Ford (Rapid 7) or Kevin Mandia (Mandiant), or Rik Ferguson (Trend Micro)…I could go on, but I won't. Not only are the aforementioned all hugely respected and give a really good interview, but they're actually changing the shape of the industry. How often could you say the same of a CISO or an end-user?

It's absolutely no coincidence that when scouting for the *Infosecurity* magazine Summer Virtual Conference keynote interviewees that my search led me to James Lyne and Steven Chabinsky, chief risk officer of CrowdStrike. I invited Chabinsky to deliver the US event's keynote address hot on the heels of his company's release of the Putter Panda report, which alleges to uncover a second Shanghai-based PLA hacking group targeting US and European organizations.

Meet the team: The Infosecurity Group team at Infosecurity Europe 2014

And as for Lyne, I quizzed him on his latest research, the vulnerability he wished he'd have discovered and, quite frankly, what goes on in that brilliantly scientific brain of his. If you didn't catch it live, it's absolutely worth a listen on-demand.

But I digress. The vendor community employs many of the brightest minds and most innovative developers, researchers and coders. Sure, they are also responsible for a lot of FUD showered across the industry, and yes, their marketing messages are often questionable. But is there an industry that isn't guilty of dubious marketing? I could use L'Oréal shampoo every day for the rest of my life and my hair would no closer resemble Cheryl Cole's than it does today.

During my eight years in this industry, I've watched as the end-user superiority complex has grown. There's an absolute power imbalance, and this is completely logical: end-users hold the budget that the vendors are fighting for. But, I guess my plea is this: Let's not be dismissive of the vendor community. They have a lot to offer, and a lot that we need.

> Let's not be dismissive of the vendor community. They have a lot to offer, and a lot that we need

And to the man who I referenced at the beginning of this editorial – don't believe your own hype!

Before I sign off, let me share some exciting news with you: infosecurity-magazine.com will be re-launching in August and is looking absolutely amazing. The *Infosecurity* team (especially – and big shout out to – Rebecca Harper) have been working really hard to create a site that you, our loyal readers, can't live without. So you should look forward to that.

Thanks for reading and take care,

Eleanor Dallaway, Editor

Put Your File Transfers... Under LOCK & KEY

- SIMPLIFY
- AUTOMATE
- ENCRYPT

GoAnywhere™ is a **managed file transfer solution** that improves workflow efficiency, tightens data security, 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. Optional 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™ → a managed file transfer solution by LINOMA SOFTWARE

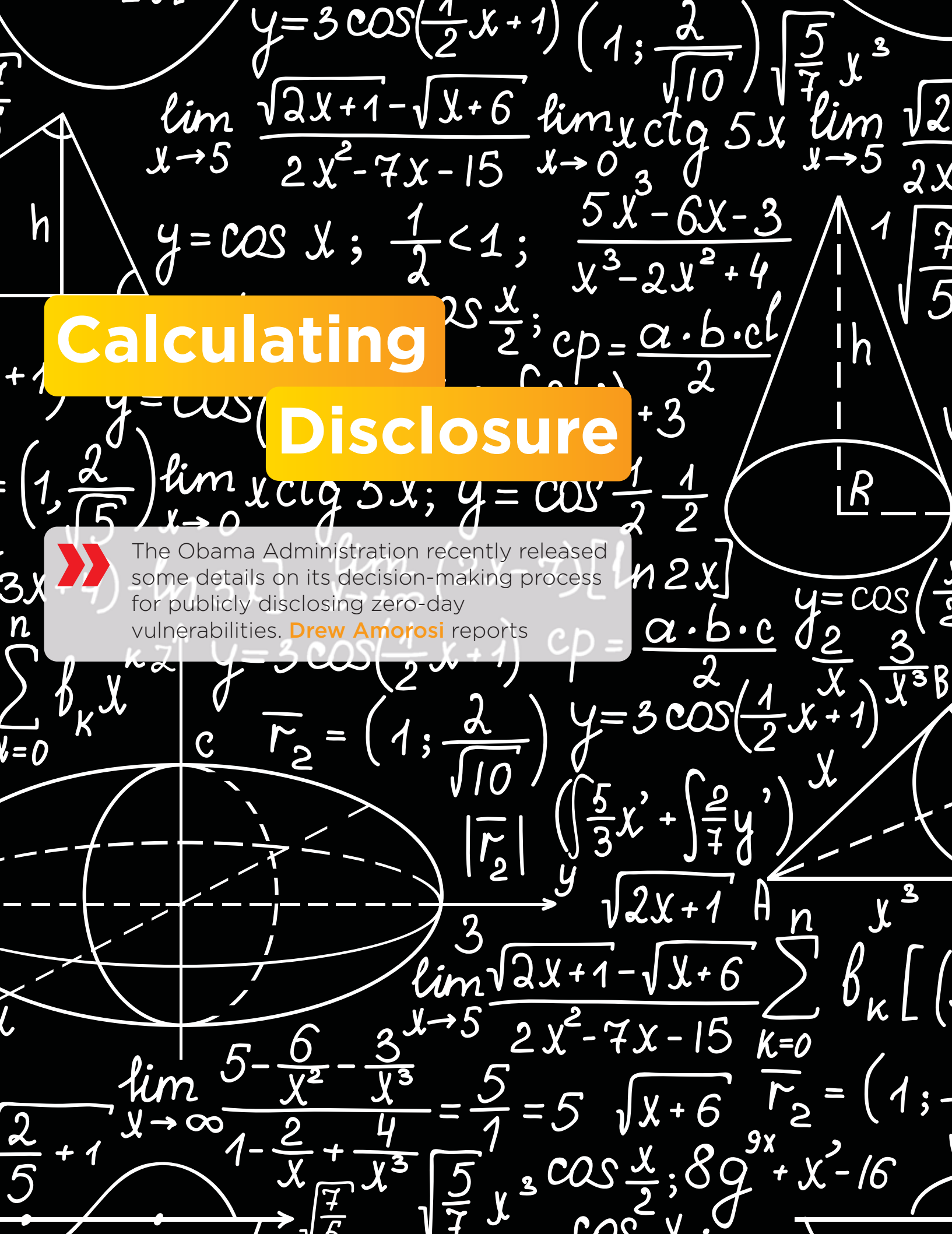
GoAnywhere.com 800.949.4696

OUR CUSTOMERS ARE SAVING TIME AND MONEY.

"We handle more than 33,000 transfers daily with GoAnywhere. It was very easy to implement and the best software value we've ever found."

Steve Tuscher
Director of IT, Grocery Outlet

Calculating Disclosure



The Obama Administration recently released some details on its decision-making process for publicly disclosing zero-day vulnerabilities. **Drew Amorosi** reports

Life is a series of choices. Should I get out of bed in the morning? Should I have pancakes or cereal for breakfast? Should I wear my grey sweater or my blue pinstriped shirt?

Choices like these, thankfully, are rather benign. The choice about whether or not to disclose a previously unknown software vulnerability, however, is anything but inconsequential. The Iranian nuclear program learned this lesson the hard way during the summer of 2010 when it was discovered that a piece of malware called Stuxnet was responsible for sabotaging uranium enrichment centrifuges, setting the process back by years.

Although the US and Israeli governments have never positively acknowledged their involvement in creating Stuxnet, security researchers examining the malware noted that it made use of no fewer than four zero-day software vulnerabilities. Someone, or something, conducted the research that discovered the vulnerabilities, pocketing the knowledge.

Fast-forward to April 2014, and the world of computer security was sent aflutter once again – this time by the Heartbleed bug affecting OpenSSL software. Immediately it was speculated that the US government and its much maligned National Security Agency were fully aware of the bug that went undetected for nearly two years. Documents disclosed by Edward Snowden, a former NSA contractor, show that the spy agency was seeking a way to circumvent web-based encryption in a similar manner that has been possible via the Heartbleed bug. Assumptions about a connection between the two seem almost obligatory.

It's no secret that governments are deeply involved in research to discover software vulnerabilities that make the type of cyber-espionage befitting our increasingly interconnected world possible. The governments of China, Russia, the US, the UK, and Israel are all guilty (depending on your perspective) of financing zero-day vulnerability research that will give them the upper-hand in the information gathering race. The big question here is, how long should governments hold onto this information before passing it along to the software's manufacturer for security patching?

Vulnerability Glasnost

Given the recent scrutiny being given to the NSA because of its mass surveillance programs, it should perhaps be no surprise that, as details on Heartbleed emerged, the Obama Administration felt compelled to provide unprecedented insight into its vulnerability disclosure process. A mid-April statement by Caitlin Hayden, spokesperson for the National Security Council, hinted at a revamped decision-making process concerning disclosure, based on a review of the recommendations handed down by a presidential advisory committee examining the NSA's bulk surveillance programs.

The advisory committee recommended the government make use of zero-day flaws on an extremely limited basis. The administration reviewed the committees' recommendations, resulting in a brief list of points to consider when determining how zero-days can be used, and whether they should be reported to the software or hardware manufacturer.

"The process is biased toward responsibly disclosing such vulnerabilities", Hayden relayed. As for the flaws the NSA discovers? President Obama's decision was that most of them, in a timely fashion, be passed along to the software vendor for patching. The president did make an exception for those flaws that have "a clear national security or law enforcement need."

Further details about a newly developed framework for disclosing vulnerabilities emerged via an April 28 White House blog by Michael Daniel, the president's cybersecurity coordinator. "Building up a huge stockpile of undisclosed vulnerabilities while leaving the internet vulnerable and the American people unprotected would not be in our national security interest", he wrote, adding "But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run."

White House Principles for Vulnerability Disclosure

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

What Daniel provided was insight into a newly developed balancing test the government would use to determine whether or not to disclose a security vulnerability, or if information about it should be withheld for a certain period of time. It comprises a series of questions that will help the administration evaluate the value of withholding information on a particular vulnerability (see box). Among the assessments is the consideration of the risk level should the vulnerability be withheld, and what damage could be done if the information about the flaw was obtained by adversaries or criminals.

TMI?

Did Daniel – and the Obama Administration – go too far in providing such unprecedented insight into its decision-making process regarding the nation's cyber-defense and approach to zero-day vulnerabilities? Or, was such a bold step

required from the US intelligence community in a post-Snowden world? Unsurprisingly, the reviews are mixed, even though most observers have praised the effort at transparency.

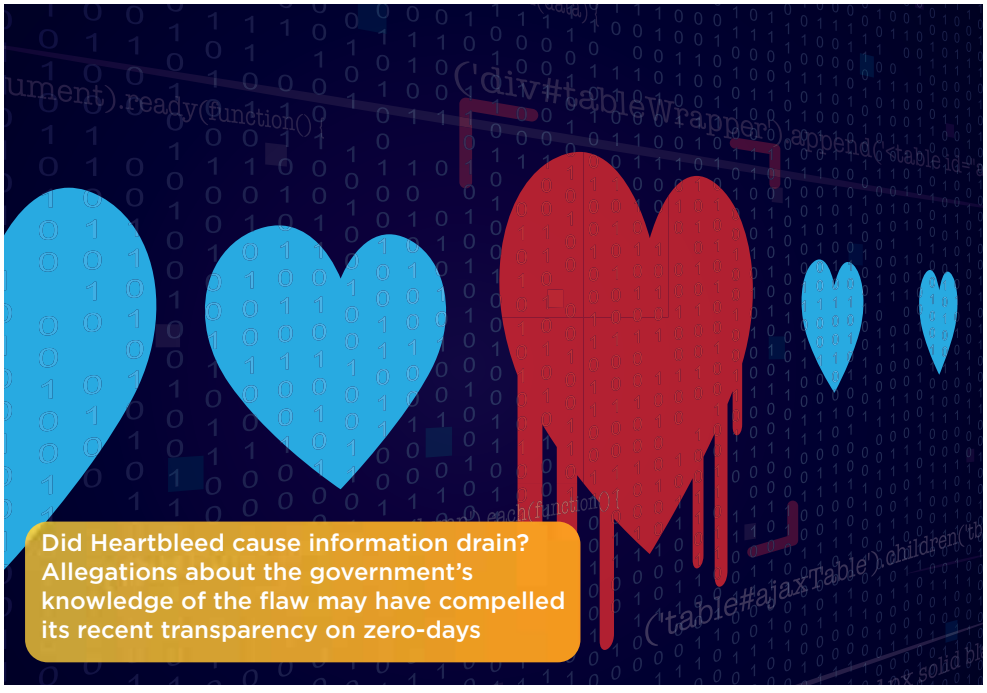
The statement delivered by the government's cybersecurity coordinator was described as "extraordinary for several reasons" according to Jack Goldsmith, a professor at Harvard Law School who specializes in national security law. "It implicitly reveals quite a lot about some dimensions of the US government's offensive capabilities, policies, and thinking", he noted. "Daniel makes clear that the US government takes defense of the internet, and disclosure of vulnerabilities, very seriously, and that it has gone to greater lengths than any other nation to make public its policy guidelines on the issue."

Whereas Goldsmith acknowledges the positive aspects of such unparalleled transparency, he also warns about a potential downside. "At some point – I am not sure we have reached it yet – more transparency will affirmatively harm intelligence collection in ways that outweigh the public confidence and related benefits of further disclosure.

"This is a very tricky trade-off to manage", he continues. "The trade-off is tricky not just because transparency aids our adversaries. It is also tricky because disclosure invariably begets further disclosure, and because disclosures of the sort Daniel made – which reveal a lot about what the US government is up to – will diminish trust in the US government in many quarters, especially since no other country makes disclosures of this type."

Did Daniel provide too much information about the US government's approach? Regardless of whether this official administration statement provides a level of insight no other nation has been willing to provide, they are "reassuring noises" from the White House that are more superficial than substance, according to Jennifer Granick, who is the director of Civil Liberties at the Stanford Law School's Center for Internet and Society.

"While the questions he [Daniel] asks appear facially sensible, the answers are almost unknowable", Granick contends. "The Administration's decisions will rest on what are essentially guesses about what might happen with network insecurity. And those guesses take place within a secret interagency process governed by



Did Heartbleed cause information drain? Allegations about the government's knowledge of the flaw may have compelled its recent transparency on zero-days

The Administration's decisions will rest on what are essentially guesses about what might happen with network insecurity

Jennifer Granick
Stanford Center for Internet and Society

secret, internally crafted policies and norms. This is how our government is deciding one of the most important security, economic, and civil liberties issues of our time – how secure and reliable modern communications technologies are going to be allowed to become."

The last word, perhaps fittingly, goes to former presidential advisors Richard Clarke and Peter Swire. Both gentlemen were part of Obama's five-person Intelligence Review Panel, whose recommendations were a foundation of the new policy on disclosure. The two contend that a defense by default posture is superior to an offensive one, if for the only reason that it promotes the use of more security-hardened software across the entire computing ecosystem.

"The reality is that there will be very few cases where a strong argument could be made for keeping a software vulnerability secret", the two wrote in an op-ed for The Daily Beast. "Even then, the issue would be not whether to tell the American people about the cyberspace flaw, but how soon to tell.

"The Obama administration announced that, with very rare exceptions, when the US government learns of a software vulnerability, it will work with the software companies involved and users to patch the mistake as quickly as possible. That lean toward defense is, we believe, the right answer."

Follow us online

and stay up-to-date with the latest developments in the infosecurity industry

Twitter: @infosecuritymag

Linked In: Infosecurity Magazine

Facebook: Infosecurity Magazine

Google+: Infosecurity Magazine

info security

STRATEGY /// INSIGHT /// TECHNIQUE

infosecurity-magazine.com

Interview:
David Cass

In San Francisco, Elsevier's David Cass met **Eleanor Dallaway** to talk privacy, compliance, and what it takes to be a successful CISO in 2014...

Elsevier is a big user of cloud services, Cass admits, which means the disappearing perimeter has made his team shift focus to "how we protect the application and the data no matter where it is"

A biology major turned CISO, David Cass is the most softly spoken and unassuming security executive that I've had the pleasure of meeting. Surprisingly young in comparison with many of his peers, his experience and insight into the industry are notably impressive.

Now senior VP and CISO at Elsevier, a Reed Elsevier company, Cass took two hours out of his busy RSA Conference schedule to talk me through his career journey thus far.

Having grown up in New Jersey, Cass joined UPS as a network engineer, while he was still attending Lebanon Valley College in Pennsylvania. When the audit department advertised openings, Cass migrated and started working more heavily with computers – discarding his biology major. His next move was working for Max Blau & Sons in Newark, New Jersey, where he was essentially tasked with building their networks.

Security was only mildly on the agenda then, he tells me, with the focus on maintaining connectivity and basic passwords. "Not much was connected to the internet, just the email system, so there was a lower, less exposed surface area". Workflow and process, however, suffered as a result.

And Then There Was Data

In 2002, Cass took the position of senior manager and area IT leader at PricewaterhouseCoopers. His role was to aid internal IT operations, work with consulting groups, and support the desktop teams. It was at this point, he notes, that security was starting to be recognized as more of business issue. "Information was more sensitive, and all of a sudden it wasn't just our information, but our clients' information which we had to protect."

In 2002, Cass recalls, "you owned and ran your own data centers, so there was still a higher degree of control". Outsourcing was minimal and therefore you maintained responsibility for all of your end-to-end IT operations, "so it was easier to evangelize security when you were in control from end-to-end."

By the time Cass joined JP Morgan Chase as vice president of risk management for the technology group in the summer of 2006, "outsourcing was big, and indeed the whole operation was much bigger". By this stage, Cass had completed his first master's degree; an M.S.E. (Master of Science in engineering) from the University of Pennsylvania.

This qualification would serve Cass well within his present and future roles, giving him the knowledge and skills to understand the business leadership team's strategy and direction. "At the end of the day, the business needs to accomplish its goals and innovate, and it's my job to

figure out how to enable it to do that", Cass tells me. "If I don't understand what the business is trying to do, or the rationale, I can't engineer a strategy to help", he says.

One of the most important aspects of his current role, Cass considers, is as a translator. "The business doesn't want to hear that you have cross-scripting or SQL injection issues. The real risk to the business of something like that is losing the content of that database, or worst-case scenario, a breach. The business understands that aspect of it, so [it's my job] to convey that message, and work with them."

Fighting Fire with Strategy

Between his tenure at JP Morgan Chase and his current role at Elsevier, Cass served as senior director of infosec risk and governance at Freddie Mac, the US Federal Home Loan Mortgage Corporation. Cass joined Freddie Mac in 2009, when the company was being overseen by the Treasury Department in the wake of the housing crisis. He was tasked with "re-doing the entire information security practice and create the entire security strategy. There were literally hundreds of findings in the Congressional report that we were brought in to address", he recalls.

Cass describes the challenge as "a very good experience". When I ask what was the most significant lesson he took from the role, he considers the question before answering: "How to address problems from a tactical and strategic point of view...How to implement quick fixes, while ensuring they stay effective over the long term. At that point, after we came in, we had to fill the whole security strategy."

If that wasn't challenging enough, Cass also studied for his second master's qualification – an MBA from the Massachusetts Institute of Technology, Sloan School of Management. He later graduated a year into his Elsevier role in the summer of 2012.

Compliance has been a key component of Cass' various roles throughout his career, and as such, is a recurring topic in our interview.

The financial sector, he says, is "always the leader of the curve" when it comes to compliance because it has to deal with more severe regulators, fines and penalties "compared to a lot of the other industries where you don't have the same degree of regulatory scrutiny."

Surveying regulatory risk is key, Cass tells me. "Consider the regulatory risk in terms of what could possibly happen, and what's the customer impact? It's easy for a customer to switch banks, for example, causing a loss of revenue stream and a general loss of confidence."

The banking industry continues to experience an increase in scrutiny, Cass tells me, "but there's more and more regulation moving into other industries, having an impact on those that have traditionally been much less regulated", he says.

> You have to understand the business in order to know what to protect

As CISO at Elsevier, a large international media company, regulation needs to be considered in relation to each specific geography. This is especially poignant, he observes, when it comes to privacy.

Privacy by Design

"The EU has always taken a much stronger look at privacy, making sure that companies have more responsibility", Cass considers. "Traditionally in the US we've been more about the opt-out model versus the EU's opt-in model."

The increased regulations, he tells me, "are making sure that large companies are putting more scrutiny on what information they're collecting, what they're doing with it, and who has access to that information."

The increased regulations, of course, are partly thanks to Edward Snowden. "The Snowden revelations have put additional scrutiny on programs like Safe Harbor and the information that is being collected."

At Elsevier, Cass informs me, Snowden has encouraged additional scrutiny, although being an Anglo-Dutch publishing and information company, there has always been a focus on privacy practices as a true global organization. "We're trying to practice privacy and security by design, making sure we're transparent about whatever we're collecting." Further, he says, Elsevier is minimizing the data it gathers, "collecting only the personal information we need to, and ensuring transparency in our privacy statements."

"The biggest focus", he adds, "is on the different EU privacy directives and how we interact with the data protection authorities. You can't do privacy without security in a digital world."

Elsevier belongs to the Reed Elsevier group, which is also the parent company of Reed Exhibitions – *Infosecurity* magazine's publisher – Lexis Nexis, and RBI. "I have peers in each division, but there's no one CISO". Reed Elsevier does have a chief security officer, however, and the divisional CISOs (or equivalents) meet quarterly. "It's essentially an information security committee. In some ways, our companies are very different so it's not necessarily a 'one-size-fits-all' model", he reflects.

Spending a fairly significant amount of time on the road, Cass juggles a lot of speaking arrangements with his day job, and also finds time to guest lecture. "It's important to give back to the industry. Part of our job is bringing people up, discussing what we're seeing in the industry, and raising the visibility of the industry as a whole."

Cass reports to the Chief General Counsel at Elsevier, which he declares highly successful and "a very progressive and proactive approach". The reporting line gives him a seat at the table with the CIO, increasing his visibility.

Aligning Security with the Business

Having the CISO report to the Chief General

Cass received his higher education at some of the Keystone State's many fine colleges and universities, starting first at Lebanon Valley College, and then earning his first master's at the University of Pennsylvania

Counsel was one of the recommendations given to Elsevier in a PwC report they commissioned right before Cass was recruited. "The report made recommendations about what the information security team should look like and how it should be structured. There was a basic plan: get a CISO, start the staffing of the department". This, of course, was when Cass was hired.

"At this time, the company had begun its transformation into the digital world", and Cass was tasked with building an information security team and program from scratch. His first task on joining the organization was to learn all about the business, "because you have to understand the business in order to know what to protect."

Starting from the ground up meant that Cass' initial focus had to be on "tactical blocking", but three years later, armed with an excellent team and a stronger alignment with the CIO, the focus has switched to long-term strategy. "We're big cloud users, so that changes the way we have to do information security in general. The perimeter has gone, so we have to focus on how we protect the application and the data no matter where it is."

His biggest challenge, Cass explains, is ensuring that the information security team and policy are truly aligned with the business. "We have such a diverse application portfolio, because we have a mixture of legacy, things that are new, things that are very progressive, things that are out in the cloud, and out in mobile applications. The challenge is working out the right level of protection, and knowing what to protect, because you can't protect everything", he admits.

The nature and culture of Elsevier's business means that it is not acceptable to "lock people down" or ban social networking on instant messenger, for example. "In our industry, there's an expectation that you can access whatever you want. One of the biggest challenges for information security is understanding the way that people work has fundamentally changed, and adapting to that."

Beware of the Phish

Training and awareness, while one of the most important things you can do as a CISO, is also one of the hardest things to do effectively, Cass explains. "I can't stop them from clicking on things at home and releasing them onto the network". The key, says Cass, is to constantly train the users. He is planning an internal phishing program this year to "increase awareness among users. Nobody thinks they fall for that stuff, but so many people do". His planned phishing exercise will, he hopes, serve as a gentle reminder.

Another of Cass' ongoing challenges is to build security into the SDLC (secure development life cycle). "We're helping our developers to become better at secure coding", he explains. "When developers go to school, very few are taught secure coding."

Cass and his team are therefore launching an application security center of excellence to impart this knowledge on the development teams and "get them to take more ownership and accountability for the quality and security of the code that they develop."

Cass and I discuss the skills gap in the industry, and he admits that hiring people with the right skills is definitely a challenge. Nine of Cass' 11 hires at Elsevier have worked for him in the past and he refers to them as "a set of proven talent, highly skilled and highly experienced."

He has a mix of technical and business minds on his team, and Cass tells me that those in the more senior roles typically have a mix of both. "It's more important to have both skillsets the more senior you are", he says. "I want to make sure they're comfortable speaking to the business and just as comfortable speaking to the highly technical people."

During his career, Cass has witnessed the evolution of his role as CISO. Today, he tells me, it's all about enabling the business. "Information security has traditionally had the reputation as the people you don't want to go to because you know they're going to say no."

Once upon a time, he reflects, a breach would have ended your career as CISO. But now, he says with confidence, failing to help the business innovate will be the killer to your career. "Whoever thinks they haven't had a breach hasn't been in the industry for long enough or doesn't know better. It's not if when it comes to breaches, it's when. But not helping the business to innovate, that's to your detriment."

Despite this challenge, Cass insists that his current role is his dream job. And I, for one, am pleased to hear this, confident that our very own CISO is where he belongs, and that our organization

info security
STRATEGY | INSIGHT | TECHNOLOGY

INFOSECURITY WINTER VIRTUAL CONFERENCE

7TH - 8TH OCTOBER 2014

JOIN US AT THE LEADING VIRTUAL CONFERENCE EVENT FOR THE INFORMATION SECURITY INDUSTRY.

THE INFOSECURITY WINTER VIRTUAL CONFERENCE WILL PROVIDE THE OPPORTUNITY TO:

- EARN UP TO 10 CPE CREDITS TOWARDS YOUR SSCP®/CISSP® & ISACA CERTIFICATIONS
- ATTEND INFORMATIVE EDUCATION SESSIONS FEATURING HIGH CALIBRE INDUSTRY SPEAKERS
- WATCH VIDEO CONTENT EXPLORING THE LATEST IN INFORMATION SECURITY TECHNOLOGY, PRODUCTS & SERVICES
- DOWNLOAD WHITEPAPERS, PRESENTATIONS, PRODUCT INFORMATION SHEETS AND OTHER DATA
- NETWORK WITH COLLEAGUES IN REAL TIME

THE FULL EDUCATION PROGRAM AND SPEAKER LINE-UP WILL BE ANNOUNCED SHORTLY. RESERVE YOUR PLACE FOR FREE TODAY & JOIN THE LEADING INFORMATION SECURITY VIRTUAL EVENT.

WE LOOK FORWARD TO WELCOMING YOU.

WWW.INFOSECURITY-MAGAZINE/VIRTUALCONFERENCE

A Tale of Heartbleed

What some call the worst bug in history is only a few months old. **Danny Bradbury** asks: Do you really think Heartbleed is over?

April 1, 2014: There couldn't have been a more appropriate date for members of the OpenSSL team to learn that their code was giving away passwords and digital certificates all over the internet. That morning, an email arrived from Google, outlining details of what would become one of the most devastating computer bugs in history.

A flaw in the open-source code enabled attackers to use the service's 'heartbeat' feature. This allows one computer to request data from an SSL record held in the other computer's memory, to confirm that it's still active during a session. The computer receiving the request doesn't check the length of the requested payload, enabling the requester to ask for far more data than it really needs. This data – up to 64Kb of it – comes from memory close to the SSL record, which contains lots of sensitive information, including certificates and passwords.

This attack can be performed repeatedly, with no trace, enabling those in the know to devastate server security. What's more, it was in existence for two years before a research team from Google discovered it.

Mending a Bleeding Heart

The remediation process for Heartbleed was troublesome for the organizations it affected. Not only did they have to upgrade from the vulnerable versions of OpenSSL, but they also had to re-obtain digital certificates from their certificate authorities. Then, they had to ask (or make) their users log out, log on, and change their passwords again. For companies that rely on making their service as easy to use as possible, that's a big deal.

Still, at least it's all taken care of now, right?

Not so fast, warns Tom Brennan. Brennan left Trustwave to start his security firm, proactiveRISK, on April 30. It was timely – he received lots of calls in his first week from friends, colleagues, and family, asking about Heartbleed, so he ended up writing a Firefox plugin that would check every site that a user visited.

"200,000 of the most popular websites were still vulnerable as of May 2", he observes. Other estimates suggest that the number is even higher.

The Heartbleed vulnerability is a two-headed beast, Brennan warns. Even if a company fixes the bug, that won't be enough, he says, unless they renew the certificates that have been compromised. Those that haven't will still be at risk.

Many people have focused on the public facing services without taking a proper look at the internal aspects of their networks that may also be using OpenSSL, and could be similarly compromised.

"If I was to target an individual user, hooking his browser, at that point I'm able to pivot through that machine and go through to the internal network", Brennan says, suggesting that even VoIP phones could be vulnerable. "Call managers do login with service IDs. It's easy to get internal organization access by leveraging a vulnerability that was believed to be external and public facing."

Taking Responsibility

One of the biggest worries about Heartbleed is that it's up to organizations to fix it. Technology journalists have an unwritten rule when a security flaw emerges: detail how it happened, and then make recommendations to ensure that it doesn't happen again.

When end-users are involved, this often means reiterating basic security best practices. Use strong passwords, change them often, don't give out credit card numbers, don't click on suspicious links, and so on. If nothing else, it makes end-users feel a little empowered.

Unfortunately, there are no such measures with Heartbleed. It attacked organizations, rather than individual users. Users could have demanded proof that organizations were not affected, but that's hardly helpful two years after the fact.

"There's a class of infrastructure software where, as an end user, you are essentially powerless", says Simon Phipps. He is the founder of open-source management consulting firm Meshed Insights, and vice chair at the Open Source Initiative, a California non-profit that focuses on building open-source communities.

Inevitably, when a security flaw of this magnitude occurs, people will ask who is to blame. The OpenSSL core development team consisted of four people, only one of whom is full time. It has a budget that ranged up to $1m per annum. Is it culpable for having not caught the bug?

If organizations focus too hard on any one particular bug, then they risk losing focus on the bigger picture

> It's easy to get internal organization access by leveraging a vulnerability that was believed to be external and public facing
>
> Tom Brennan
> OWASP Foundation & proactiveRISK

Not a chance, says Phipps, who points the finger squarely at the companies using the software. "For me, rather than raising questions about the open-source process, Heartbleed raises questions about the proprietary processes of the companies that are using OpenSSL", he says.

"If any of them spent a fraction of a second checking up on OpenSSL they would have realized that they needed to deploy staff into the community and maybe apply a backup process to ensure the integrity of the software themselves."

Companies are getting involved in open source, argues Phil Granof, chief marketing officer at Black Duck Software, which sells open-source management software and consulting services. The firm conducts a regular survey of open-source software users.

"Thirty percent of companies are making it easier for their employees to get involved in open source, and certainly, the percentage is higher if the products are relevant to the company", he argues.

That didn't stop Steve Marquess from complaining about the ones that didn't, though. Marquess is the co-founder and president of the OpenSSL Software Foundation, the commercial entity that supports the OpenSSL project with support contracts.

In a blog post called 'Of Money, Responsibility, and Pride', he called out Fortune 500 companies for not supporting open source more. "The ones who don't have to fund an in-house team of programmers to wrangle crypto code, and who then nag us for free consulting services when you can't figure out how to use it", he wrote. "The ones who have never lifted a finger to contribute to the open source community that gave you this gift. You know who you are."

It's all very well to criticize large companies for not catching the bugs, but this belies the fact that there are simply too many projects, says Art Gilliland, senior VP and general manager for enterprise security products at HP.

"There are hundreds and thousands of different open-source projects and so it's not realistic for any company to invest in any one of them", says Gilliland, pointing out that HP invests hundreds of engineers' time in protecting open source.

HP was one notable omission from the Core Infrastructure Initiative, a project organized by the Linux Foundation to support security efforts on large open-source software projects. The initiative includes Microsoft, despite the fact that the company's recently retired CEO, Steve Ballmer, once called open source a "cancer". How things have changed.

One of the questions in the initiative's FAQ asks why they hadn't done this before. "We're doing what we can now", begins the reply.

Better late than never, and never too soon, because this won't be the last time. "It's the last vulnerability of its type. There will never be another vulnerability capable of affecting more than a single percent of the internet", quips Gunter Ollman, CTO of security consulting firm IOActive. "Oh, and a unicorn gave birth to a flying pig yesterday."

He anticipates "close facsimiles" of this bug in other software.

Preparing for the Unknown

Given the difficulties of spotting even show-stopping bugs like Heartbleed, it's fair to say that there are still plenty of 'known unknowns' on the internet. We know that the vulnerabilities are out there, but we don't know where. Companies have to prepare themselves against an unknown enemy that could render any system vulnerable in unexpected ways. So, how do they accomplish that?

Stare too hard at any particular bug and you'll lose the bigger picture. HP's Gilliland points to the broader attack cycle, and says that organizations need to understand that if they are to protect their systems.

The Attack Cycle

He breaks that attack cycle down into five main areas. The attackers first research the target, and then infiltrate it. They map out its environment, and then they capture the data that they want. Finally, they exfiltrate the data. The dark market economy means that each of these activities gets a specialist, who is very good at it.

"So how does a company respond to the fact that they're competing against the best in the world at those steps?", he asks. "You don't rely on any one of those controls to protect your infrastructure. You build a capability in every one of those steps."

Gilliland is talking about defense in depth. The idea is that the next time there's a 'Heartbleed', and a company hasn't caught the flaw in the software it's using, it'll represent only one stage in an attack. The well-prepared company will have good protections built in to prevent the rest.

This is why in 2010, Debora Plunkett, then head of the NSA's Information Assurance Directorate, revealed the agency's policy of already assuming that its networks have been compromised.

Government spooks have the right idea, says the director of security at one well-known IT company affected by Heartbleed, who asked not to be named.

"We design systems so that we assume that they will fail", says the source, who confirms that he runs an entirely open-source stack. "We assume that bad guys will land in our environment. We are running file integrity monitoring, which is an integrated part of our Puppet process, so if a file is changed and it's not through puppet and the SHAs don't reconcile to the RPM database, then we have a problem."

It isn't about being rigid and ring-fencing your perimeter, says the source. It's about accepting that there is another Heartbleed. It's already out there, and waiting. "We tell everyone, 'you're going to get hacked'", he concludes. "It's going to happen. Just assume that you

If Pelé were a Network Security Solution He'd be ForeScout CounterACT™

Quick. Agile. Powerful.

Access and device diversity, dynamic exposures and advanced threats. No problem. Just as Pelé was a football game-changer, ForeScout has changed the game of network security. Leveraging our ControlFabric™ technology, ForeScout delivers the continuous monitoring and mitigation necessary to enable business agility without compromising defences. Be a game changer.

Complete Network Visibility and Control. Any Device. Anywhere.

Score a hat trick.
Learn more about capabilities and considerations for Next-Gen NAC with our Definitive Guide™ to Next Generation Network Access Control. Download the ebook at forescout.com/pele_infosec

Contact us: **ForeScout Technologies, Inc.** | Tel: 1-866-377-8771 (US) | www.forescout.com

ForeScout
BE A GAME CHANGER

Beware of the Software Pirates

Does pirated software still carry the same security risks that we have always been warned about? **Tom Brewster** examines the current state of the problem...

Legendary pirates of the seas were rather good at clandestine attacks. Take tricksy Welsh pirate Captain Howell Davis. According to one myth, he often duped people by using surreptitious methods. One saw Davis deceive the governor of the Royal Africa Company in Gambia to let him into the slave fort of the organization, disguising himself as a gentleman. He later took the governor as a hostage, demanding a ransom of thousands of pounds, which he duly received.

Digital pirates operate a little differently today, but similarities remain. Much like some of the famous swashbucklers of yore, they believe they're great economic levelers, modern-day Robin Hoods. But there are some particularly bad apples, ones who will carry out sneaky attacks, solely to fuel their own greed.

Fortunately for those individuals getting their hands on pirated software, films, music or other content, the danger of facing a legal threat is slim, says Steve Kuncewicz, intellectual property, media and social media lawyer at Bermans. He points to the recently announced UK scheme, the Voluntary Copyright Alert Programme (VCAP), which will see industry bodies sending offenders four letters of increasing severity, warning recipients about the illegality and impact of what they're doing. It's modelled on the 'six strikes and you're out' Copyright Alert System in the US, and seeks to fill the gap left by the failed implementation of the much-abhorred Digital Economy Act, except there will be no punitive measures mentioned in the letters.

Kuncewicz worries VCAP might not achieve its aim of stopping illegal downloads with a soft-touch approach. "The whole issue with VCAP is that given there are no punitive measures, it might become a bit of a joke", he says. "It's like telling your child: don't do it again, don't do it again, don't do it again."

Treasure with Nasty Hidden Surprises

Rather than going after individuals, the industry is now rapaciously chasing down

websites serving the pirated content, firstly by having ISPs blocking them. Law enforcement is also hoping to cut off such business' ad revenue. The City of London Police launched an Infringing Website List earlier this year, hoping it will encourage brands not to run ads on the implicated sites.

> I don't think that hacking pirated software is a major threat vector to the industry in general
>
> Amichai Schulman
> Imperva

Industry bodies and law enforcement are also taking a different tack to deter people from downloading pirated gear. They're educating users on the threat of malicious code, which is often found hidden inside or attached to knock-off kit, or on websites that serve it. As a prime example of the dangers facing those on the messy seas of the internet, Google warned in May that popular file sharing website Demonoid was carrying malware. Any user that tried to visit via the search engine or through the Chrome browser would have been greeted with a page detailing the danger of visiting the site. Seven of 78 pages scanned by Google resulted in malware being downloaded.

In April, researchers looking at 30 of the most frequently used illegal film and TV sites in the UK claimed nine in 10 contained malware or other "potentially unwanted programs designed to deceive or defraud unwitting viewers". They said that only one of the 30 sites monitored over a two-week period showed no signs of malware or attempts to defraud visitors in some way. The researchers, who were commissioned by Industry Trust, the anti-piracy UK film, TV and video industry's consumer education body, claimed one common tactic was to have the buttons that viewers clicked to view a film or TV show trigger downloads of malware or other programs.

A separate study commissioned by the same group found 17% of people who had unwittingly or unintentionally visited a piracy site had seen personal data lost or stolen, while 14% were exposed to material they said they didn't want to see, such as pornography or violence.

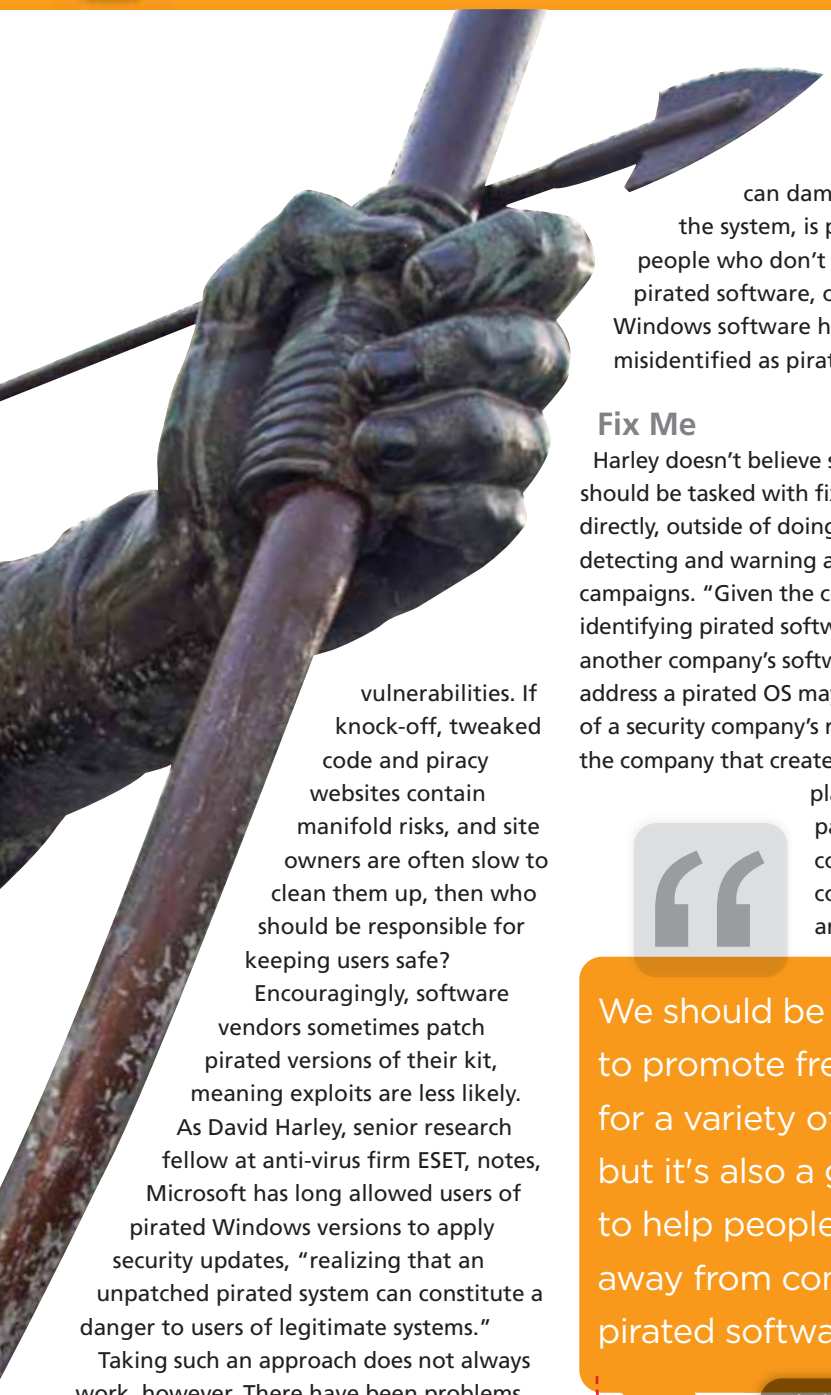
Are the Dangers Real?

Such figures might over-egg the threat level somewhat, says Amichai Schulman, chief technology officer at Imperva. "I don't think that hacking pirated software is a major threat vector to the industry in general", he asserts. "I know that it used to be a more prominent vector than it is now. Peer-to-peer networks were once a very convenient platform for spreading infected code. It is a less important platform today.

"For instance, you don't expect to directly compromise enterprise machines using pirated software because enterprises would not be using pirated software for legal reasons – and we all know that people have more fear and respect towards the legal department than towards infosec."

Schulman's doubts aside, it's clear many piracy sites do pose a risk to client security from a malware perspective, while cracked copies of software may not get the same level of support, leaving them riddled with

Digital pirates sometimes see themselves as great economic levelers, along the lines of a modern-day Robin Hood



vulnerabilities. If knock-off, tweaked code and piracy websites contain manifold risks, and site owners are often slow to clean them up, then who should be responsible for keeping users safe?

Encouragingly, software vendors sometimes patch pirated versions of their kit, meaning exploits are less likely. As David Harley, senior research fellow at anti-virus firm ESET, notes, Microsoft has long allowed users of pirated Windows versions to apply security updates, "realizing that an unpatched pirated system can constitute a danger to users of legitimate systems."

Taking such an approach does not always work, however. There have been problems with applying patches to Windows systems that may be pirated, as seen with the notorious KB2859537 update from 2013 that caused many programs not to work. Microsoft said problems could occur in Windows versions that contained an "instrumented version" of ntoskrnl.exe, a file in the Windows kernel, which the vendor didn't support. That was basically Microsoft's way of saying the update would negatively affect non-official versions of the OS.

"The combination of a pirated and therefore altered version of Windows ... and a patch that assumes legitimate system files can damage or even brick the system, is pretty hard on people who don't realize they're using pirated software, or whose legitimate Windows software has been misidentified as pirated", says Harley.

Fix Me

Harley doesn't believe security companies should be tasked with fixing the problem directly, outside of doing their day job of detecting and warning about malware campaigns. "Given the complexities of identifying pirated software – especially if it's another company's software – attempting to address a pirated OS may not be the best use of a security company's resources. Generally, the company that creates the software is best placed to implement patching. However, it's common for security companies to detect an attempt to exploit a vulnerability and take whatever remedial action is possible."

> We should be doing more to promote free software for a variety of reasons, but it's also a great way to help people move away from compromised pirated software
>
> Phil Hunt
> Pirate Party UK

Indeed, various security solutions verify that software deployed by an enterprise computer is properly signed and authorized. In such cases, pirated software – like any other unauthorized code – would be detected, notes Schulman.

Other technical solutions are proving useful in detecting legitimate code that has been given a malicious twist. "One promising development is for each program to run in its own sandbox, as with mobile phone operating systems or with Linux Containers (LXC)", says Phil Hunt, computer programmer and one of the founding members of the Pirate Party UK.

Rather perversely, use of digital rights management (DRM) tools designed to protect against copyright theft actually open up security problems, Hunt adds. "What security vendors should not do is become a part of the problem. Companies have used rootkits to build DRM systems and to monitor the users of their software. This is irresponsible and opens the door to further abuses."

One answer for those who want good, cheap software instead of getting bogged down in the world of licenses, or risking using pirated kit, is to find free tools that do a more than adequate job. "We should be doing more to promote free software for a variety of reasons, but it's also a great way to help people move away from compromised pirated software", says Hunt. "Obviously, in the long term, making legally obtained software more accessible by limiting copyright will make it less likely that people would access software from dubious sources, and that is what it comes down to."

Users could also deploy open-source alternatives to popular software, says Sarb Sembhi, director at security consultancy IncomingThought. As with free tools, it's all about ensuring the source hosting the kit is trustworthy. "Open source is good and I trust it, but it depends on which source you get it from", Sembhi relays. "The problem is where you're getting it from and whether the source is cleaning its site to ensure you don't get malware."

Even Google struggles to keep malware off its own software platform, so guaranteeing the legitimacy of the source is no simple task. Businesses and individuals have to decide whether they either pay out for official licenses, or go down the riskier but cheaper route of open source and free software. Each option carries its own risks.

infosecurity EUROPE

29 Apr - 01 May 2014 | EARLS COURT | LONDON

Security as a business enabler

'Security as a business enabler' was the theme of Infosecurity Europe 2014 and a host of engaging, informative information security end-user practitioners, analysts, policy-makers and thought-leaders shared insight into the evolution of information security as a business discipline. The various education theatres hosted sessions addressing a range of business-critical issues and challenges related to this overall theme. Attendess left with new understanding on the current challenges facing the sector and how to streamline security strategy and reinforce the position of the information security function as a business enabler.

TOP TEN KEY TAKEAWAYS

1. As the attack surface grows rapidly, organisations need to work with their third-party partners to reduce risk
2. 'Protect the castle' model is dead – protect the application and data no matter where they lie
3. Data classification has never been so important in the risk conversation, and is the primary driver when establishing controls
4. Speak the language of the business – risk is the language of the C-Suite
5. Translate threat data into meaningful intelligence that can be understood by the business
6. Invest in the right people, and train, support and retain those people
7. Information security needs to put users in a safe environment – make it easier to do the right thing, harder to do the wrong thing and easier to recover if they do something wrong
8. Engage Generation Y users through brevity, being personal in all communications, and try to understand their motivations
9. Engage stakeholders, align security incident response with maximize and organizational strategies and effectiveness for effective incident response
10. Develop an action plan to do more to help the business achieve goals and reduce challenges

WHO ATTENDS?

41%	22.3%	19.33%	10.2%	20.5%	13.7%
of visitors represented companies of 1,000+ employees	were Director Level and above	were IS/IT Management	were General Management	were Technical Specialists	were female
					86.3% were male

These statistics refer to the Infosecurity Europe 2014 attendees.

Find out more: www.infosec.co.uk

At the Show

Egress Market Survey Results

One-third of those surveyed were not aware that upcoming EU DPA reforms would impact the way they or their organization handles and protects data

Throughout the three days at Infosecurity Europe 2014, Egress Software Technologies carried out a market survey – *'2014: The Year of Encryption'*. Tony Pepper, CEO, Egress Software Technologies explains: "The information security market has changed radically over the last 12 months. Edward Snowden's revelations about the scale of international data surveillance and the increasing media coverage that now surrounds data breaches and losses have shaken industry confidence in cloud-based communication solutions. Already reflected in the change in emphasis that organizations consequently place on data security when selecting cloud-based third-party services, it came as no surprise that many delegates also voiced such views at Infosecurity Europe 2014."

Pepper continues: "One-in-two delegates, who took part in the survey, now perceive the cloud to be less secure as a result of Snowden, with 78% suggesting that the story will influence future provisioning. However, the 'Snowden effect' has the potential to make the information security industry stronger. In fact, the *'2014: The Year of Encryption'* survey also showed the emphasis that delegates place on Government certification and industry recognition when procuring a solution. Those surveyed felt that the UK Government's Certified Product Assurance (CPA) program (led by CESG) is helping to simplify the procurement decision-making process, with over two-thirds stating that Government certification combined with ease of use would be deciding factors when selecting a data security solution."

Linoma Software Improves User Experience and Security

Linoma Software has recently announced the addition of SSO (Single Sign-On) support in its secure FTP server software, GoAnywhere Services, with the release of version 3.5. The new feature is specifically designed to simplify the user experience without sacrificing security. Enhancements include:

- **Single Sign-On** – GoAnywhere Services now offers improved security and simplicity with Single Sign-On support for the HTTPS Web Client. Implementing SSO offers time and cost savings for a company. The addition of SAML v2.0 support, using the OpenSAML API, allows GoAnywhere Services to improve productivity, increase adoption, centralize user access control and add a uniform security layer. SAML (Security Assertion Mark-Up Language) is an XML-based open standard for authorization and authentication between an Identity Provider and a Service Provider.
- **Expanded Language Support** – Following customer feedback, version 3.5 adds support for two new languages, Portuguese and Bahasa. This release also improves language support by accommodating custom disclaimers for each language.
- **Virtual Folder Commands** – GACMD (GoAnywhere Command) received an update that improves the ability to create, update, and delete virtual files and folders across a range of web user and group profiles in GoAnywhere Services.

Complete Visibility Across the Entire IT Infrastructure with Netwrix Auditor 6.0

Netwrix Corporation, the leader in providing change and configuration auditing software, announced the release of Netwrix Auditor 6.0, a unified platform that streamlines compliance, strengthens security, and simplifies root cause analysis by delivering complete visibility into who did what, when and where across the entire IT infrastructure.

The new Netwrix Auditor 6.0 includes two major features and over 25 enhancements. The first major feature is Enterprise Overview dashboards that provide a high-level view into what is happening on a network. It does not matter where changes are made – in Active Directory, Exchange, File Servers, or other systems – the Enterprise Overview will notify the user and make them available for future analysis.

Users can quickly get a bird's-eye view of their IT changes and dive into the most suspicious areas with just a click. Detailed information is also available about a particular person's changes across the entire network in one easy report.

The second major feature is SharePoint auditing. Netwrix Auditor 6.0 tracks changes to farm configuration, user content, and security settings, including modifications of permissions and permission inheritance, SharePoint group membership, and security policies.

Exclusively focusing on delivering complete visibility into what is happening across IT infrastructures, Netwrix aims to become the de facto standard for change and configuration auditing, leaving all the competition far behind. The Netwrix Auditor 6.0 release is a major step towards achieving this goal.

At the Show

Encryption in the Cloud Report

At Infosecurity Europe 2014, Thales e-Security released its annual Encryption in the Cloud Report. This report gathers insight from over 4,000 organizations across the world on the security implications of moving to the cloud, the transparency of cloud providers, and how organizations are treading the line between trust and control with regard to encryption and how encryption keys should be managed.

Richard Moulds, VP Strategy at Thales e-Security says, "Given that encryption has recently been topping the international news agenda, it was interesting to see that whilst using encryption to protect highly sensitive data is increasing, the cloud could be losing its 'scare factor' for businesses, as over half continue to store data that is 'cleartext', meaning that anyone who gets their hands on it can read it.

But the universal pain point remains key management. Key management is a critical control issue for respondents, who are increasingly focused on retaining ownership of keys as a way to control access to data. Deployed correctly, encryption can help organizations to migrate sensitive data to the cloud, allowing them to safely unlock the full potential for economic benefit the cloud can deliver. Knowing where your data resides and the level of protection it requires will be a key element in ensuring that valuable business assets are not put at risk."

Qualys Continuous Monitoring Helps Prevent Perimeter Breaches

Qualys has recently updated its QualysGuard Continuous Monitoring (CM) cloud solution, which helps customers efficiently monitor their entire global perimeter and discover threats and unexpected changes before hackers do. Continuous Monitoring allows organizations to continuously scan their entire perimeter, set triggers to detect exceptional occurrences from their baseline perimeter state, and only receive alerts related to those unexpected changes. For example, rather than receiving redundant notifications for low-priority vulnerabilities, IT staff can restrict alerts to events that create new risks, such as newly discovered hosts, expiring SSL certificates, or the appearance of prohibited ports, protocols or applications.

This latest release includes enhancements that simplify the creation, sorting and prioritization of alerts, including a new wizard for creating alerting rules and tying them to specific assets. The alerts generated by these rules are communicated by email and via a dashboard. To identify new problem patterns, customers can now filter the dashboard by alert type – for instance, to view only certificate issues – and can specify a date range. The emails summarizing alerts now break out events by category, allowing for simpler drill down.

These new enhancements for QualysGuard CM are available to all customers immediately without added cost or deployment effort.

ISACA Launches Cybersecurity Nexus (CSX) Program

ISACA's Cybersecurity Nexus (CSX) program addresses the growing worldwide cybersecurity skills crisis. CSX emphasizes expertise in business strategy and communication, in addition to technology.

CSX, developed in collaboration with global chief information security officers and cybersecurity experts, fills the need for a single, central location where security professionals can find cybersecurity research, guidance, certificates and certifications, education, mentoring and communities.

Robert E Stroud, CGEIT, CRISC, ISACA international president and vice president of strategy and innovation at CA Technologies, said: "Unless the industry moves now to address the cybersecurity skills crisis, threats like major retail data breaches and the Heartbleed bug will continue to outpace the ability of organizations to defend against them. ISACA is proud to help close this gap with a program that provides expert-level cybersecurity resources for each stage in a cybersecurity professional's career."

CSX includes career development resources, frameworks, community, research and guidance designed to provide vital security-related information within the larger business context.

CSX reflects ISACA's ongoing collaboration with other global cybersecurity organizations, such as NIST (U.S. National Institute of Standards and Technology) and ENISA (European Union Agency for Network and Information Security).

More information is available at www.isaca.org/cyber.

At the Show

Libraesva International Development Begins at Infosecurity Europe 2014

Libraesva, the Italian leading provider of advanced email security solutions, attended Infosecurity Europe for the first time this year. Libraesva showcased the 64-bit version of the Virus Bulletin award-winning Libra ESVA email security gateway, which has been developed to increase performance, flexibility and control.

Paolo Frizzi, CEO & Founder of Libraesva, says: "We are extremely satisfied with the results of our first participation at Infosecurity Europe 2014. It has been the best choice for us to showcase the latest offerings from our security-solutions portfolio and to develop close connections with international contacts."

At the show, Libraesva closed an important contract with a distributor to cover Austria, Germany, Switzerland and Russia with its unique offer of anti-spam solutions. Frizzi adds: "The interest we received at the Show confirmed the validity of our vision and strategy, aimed at developing our presence outside the Italian region through partnerships with new distributors."

Document Templates for ISO/IEC 27001 Enhanced

Public IT, creators of the document template set for ISO/IEC 27001, announced that is has a licensing agreement with the British Standards Institution to allow the use of BSI copyright information within their products.

"This is great news for our customers because we are now able to offer more detailed content in documents such as our gap assessment, which will make the process of implementing the ISO/IEC 27001 standard using our document templates even faster", said Ken Holmes, CEO of Public IT.

The document template set is available for download at www.iso27001templates.com

VASCO to Expand its Authentication Technology Portfolio

VASCO Data Security International, Inc. recently announced that it has executed a definitive agreement to acquire Risk IDS, Ltd., a provider of risk-based authentication solutions to the global banking community. Risk IDS provides online transaction risk management and intelligent authentication decision solutions. The core technology is a Dynamic Challenge Platform that is optimized for stability and high volume. The platform is designed to evaluate the profile of the user requesting access to the system to determine the risk profile associated with the transaction. It features a real-time analysis engine that uses rules and statistical techniques to improve real-time fraud detection. VASCO, a global leader in authentication, digital signatures, and identity management, will integrate Risk IDS' risk-based authentication technology into future product offerings.

T. Kendall Hunt, VASCO's Chairman and CEO, says that the acquisition will enhance VASCO's leadership position in the authentication segment and extend the company's broad product portfolio: "Our clients face increasingly sophisticated attacks from well-organized criminal hacking organizations that create new attack vectors every day. Our focus is to always keep our clients one step ahead of an ever-expanding threat horizon and this is an important move in support of that mission."

Good News for iOS/Android Security From LockLizard

While reviewing their press releases, LockLizard recently found an entry in the following blog: www.mesuva.com.au/blog/recent-work/australian-college-of-operating-room-nurses-acorn/. Not a blog written by LockLizard, it reports on a successful DRM security development using the LockLizard system primarily for iOS/Android devices, and a satisfied customer.

It doesn't mention, however, that they found there was no need to go and develop an app to display the pdf documents on those platforms. The LockLizard Viewer app was able to display the medical standards documents on both devices without any altering or tweaking, saving time and cost and enabling the project to be brought in much more efficiently than was initially expected.

To find out how LockLizard products can quickly, easily and effectively add security to the pdf's you want to distribute securely, visit www.locklizard.com or give LockLizard a call on +1 800 707 4492.

Expanded Support from SSH Communications Security

In light of several advanced threats and security breaches making headlines over the past year alone, SSH Communications Security recently announced that its CryptoAuditor solution now supports SSL/TLS decryption, monitoring and DLP integration, representing encrypted channel monitoring support for all major data-in-transit encryption protocols.

CryptoAuditor is an identity and access intelligence (IAI) solution that enables organizations to continuously monitor traffic on encrypted networks, delivering critical context to network and information access. As a minimally invasive, inline solution, CryptoAuditor is invisible to the end user, requires no staff training or IT help desk support, and does not impact administrator work flow. This expanded support enables organizations to monitor and control SSL/TLS, Secure Shell, SFTP and RDP connections, closing security gaps and reducing the risk posed by advanced external threats.

A holistic approach to encrypted channel monitoring can have a profound impact on preventing critical, widespread security disasters and keep an organization's critical assets safe and secure.

New Release of API Gateway From SOA Software

SOA Software, a leading provider of API Management and SOA Governance products, recently announced a major new release of its API Gateway, with significantly upgraded security and threat protection capabilities to provide a comprehensive, hardened, and integrated API security solution. This release establishes a new standard for an integrated solution that combines security, integration, and mediation capabilities delivered both in the cloud and on-premise.

SOA Software's API Gateway provides a comprehensive security and threat protection solution for enterprise APIs. It covers a wide range of use cases, including threats related to identity and access, message encryption, and compliance.

The API Gateway streamlines development, management, and operation of APIs; enhancing security and regulatory compliance through authentication, authorization and audit capabilities. It is available in the cloud, on-premise, or as a virtual appliance for ease of installation and configuration.

The new release includes many new capabilities, including support for Hardware Security Module (HSM), enhanced support for Kerberos (including SPNEGO policies) and support for Virtual Host Configuration, empowering users to centrally manage and configure all their virtual services. Find out more at www.soa.com.

Security Specialist Wick Hill Doubles Training Capacity

Wick Hill, a specialist in IT security, has doubled its training capacity with the opening of a new custom training center at its Woking HQ. Wick Hill is one of the UK's major security trainers, running courses for leading security vendors, including WatchGuard, Check Point, Kasperksy Lab and SafeNet.

The opening of the new center has been prompted by increased demand for courses, which has been growing strongly year on year.

Wick Hill provides a range of training courses, both at Wick Hill and on customer sites. It is an accredited training center for most of its suppliers, with the majority of courses being vendor accreditation courses, open to both value-added resellers and end-users (through the channel). Courses are designed to improve product knowledge and fulfill vendor certification requirements.

The company has also appointed Barry Davies, an experienced IT and Education Manager, to the new role of Professional Services Manager. Davies' responsibilities in the role will include developing and growing the training business.

Demand for courses has also been high at Wick Hill's German division in Hamburg, where there has been a similar increase in the space made available for training.

Integrity Solutions to Open Third UK Office

Integrity Solutions, the UK's fastest growing IT security consultancy, has announced that it will open its third UK office within the next month. Along with its current UK offices in London and Glasgow, the company plans to open an office in Birmingham following a successful year during which the company has grown by over 300%. At least six new technical roles will be created as a result of the expansion.

Country Manager, Mark Evans, said: "We are really excited about our growth plans and delighted to be hiring very experienced security professionals across a range of security disciplines to cater for the huge demand we are seeing for our Managed Security Services."

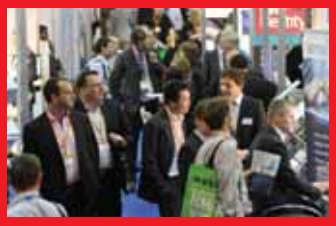
Integrity Solutions was founded in 2005 with its head office based in Dublin. In 2011 it established itself in the UK market and has since gone from strength to strength. As one of the most prominent new exhibitors at Infosecurity Europe, Integrity Solutions has well and truly announced its presence and intentions in the UK market.

For information regarding available positions, please visit: www.integritysolutions.co.uk/careers

Eoin Goulding, Managing Director and Mark Evans, UK Country Manager

At the Show

Advanced Cloud-based Management Console From Webroot



Webroot announced an advanced cloud-based management console at Infosecurity Europe 2014: Global Site Manager. For use with its SecureAnywhere Business-Endpoint Protection solution, the new management tool is aimed at Managed Service Providers (MSP) and developed as a no-cost alternative to the Webroot standard console. It allows customers to administer more complex SecureAnywhere deployments easily and efficiently.

The new tool addresses many of the challenges that MSPs often struggle with, it can protect multiple sites and provides a hierarchical view of the endpoints under protection, allowing MSPs to have a global view of their customers and drill down to group and individual user views in real-time.

The solution is also highly scalable, allowing for hundreds of customers and thousands of endpoints to be managed via a single console. For more information go to www.webroot.com

Security Can Be a Business Enabler

Security can be an enabler for a more efficient, and more profitable business. But making security work for the business takes skill.

This was the message from the Security as an Enabler panel at Infosecurity Europe 2014, chaired by Peter Wood, CEO of First Base Technologies and of member of ISACA's London Chapter security advisory group.

This does, though, require a culture change among both security professionals, and the business. Security professionals can no longer say no, but they also need to advise the business on acceptable levels of risk.

"With the move to the cloud, you have to move away from protecting the castle. You have to protect the data and the applications, and that changes the process", said David Cass, SVP and CISO at Elsevier. "You have to help the business to make money", said Lee Barney, head of information security at the Home Retail Group.

But, said Peter Wood, helping the business means finding security professionals who have business acumen. "It is up to us to find, and nurture, people who want to help the business", he said.

This means engaging with the business, said Michael Colao, head of security, chief technology organisation at AXA UK, even if that is a battle the security sector has been fighting for some time. "It means having security professionals prepared to engage with the business", he said.

"They need to answer the questions the business wished it had asked, rather than the questions it actually asked." Non-security professionals will think in terms of easier access to an online account, rather than biometric or token-based security."

Although the panel remained skeptical about how far information security can go in driving profits, it is clear that poor security, and poorly-implemented security, can drive away customers.

"In retail, if people don't like what you do, they vote with their feet", said Barney. "Our margins are very tight. We absolutely have to keep our customers, and we care about the customer journey, and customer security."

World's Most Advanced Hackers are in Russia and Eastern Europe

Photo credit: Gustavo Molina

As MD for international markets, LogRhythm's Ross Brewer is well versed in the latest geographical trends and targets. "Germany is a big target at the moment", he told *Infosecurity* during an interview with Eleanor Dallaway at Infosecurity Europe 2014. "It is a manufacturing country with amazing IP. It's a country conscious of monitoring its population too much with a focus on employee privacy, and this is not lost on the hacking community." German IP is therefore a target and tends to end up in Asia, according to Brewer.

As an emerging market, the Middle East positioning itself as 'the destination' is also a target, Brewer said. "The biggest threat to Europe comes from Eastern countries where the most experienced, most capable hackers are. The most advanced hackers on the planet reside in Russia and Eastern Europe." Threats from Asia tend to be less stealthy, however, Brewer declared. "So whilst the most obvious threat comes from Asia, the most real threat comes from East Europe."

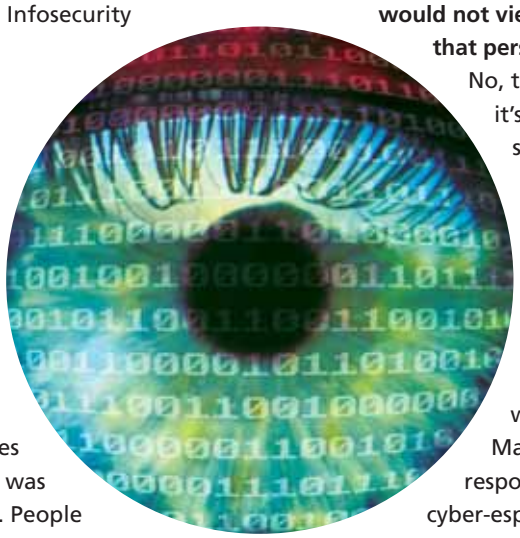
LogRhythm's Brewer also flagged the French market as vulnerable, notably "because they buy all their technology from within France, but forget they're plugged into a global internet which leaves them exposed."

Brewer also addressed Africa. "As technologies become more pervasive and wireless more common in Africa, there will be increased threat activity. At the moment, the African infrastructure is not on the same level as the rest of the world, with power and technology intermittent, but as that increases, so too will the threat".

"Critical infrastructure is the target now, in every country", Brewer told *Infosecurity*.

Cyber-espionage is the "New Normal"

Infosecurity's Drew Amorosi jokingly asked Kevin Mandia, CEO of Mandiant, if his company specialized in investigating the Chinese government. "We just go where the intrusions are, and it just happens to be them", Mandia replied, whose company focuses on security incident response and management. Following are some highlights from that conversation, which took place at the recent Infosecurity Europe 2014 in London:



What makes Mandiant unique among its competitors?
I've always believed that you can't secure everything all of the time, and that security breaches are inevitable. In 2004, we actually had on our website 'security breaches are inevitable', and that was a little ahead of its time. People thought it was pessimistic. Responding to data breaches is the best job in information technology. It's fun – there's an adversary, a defender, and we have mutual respect. In the end you are looking to answer two questions: What happened, and what to do about it? It's the only way to make better security products. We get to see how everything else fails, not just the people and the processes, but also the technologies. Mandiant is on the front lines, responding to every breach that matters.

You called breach response fun. I'm assuming most of your customers would not view it from that perspective?
No, they wouldn't, but it's the reason that security exists. Security doesn't exist because of compliance; it exists because if you don't do it, bad guys will break in. In 2004, when I started Mandiant, I had been responding to Chinese cyber-espionage as a government guy for a while, and we had started seeing that capability hitting the private sector – and I knew we were sitting ducks. You can't expect the private sector to withstand a nation-state's capabilities.

Last year Mandiant made headlines with its Comment Crew report about Chinese cyber-espionage. What type of information are these cyber-intrusions seeking?
It's all over the map really. It's a lot – anything from IP, to communications and emails, things about processes. I'm not a mind reader; I can only tell you what they are taking. Sometimes it's a lot, where you can't see a focus. Other times it is focused on specific programs.

Can we blame the Chinese for cyber-espionage in a world where attribution of attacks is so difficult?
Every once in a while there is a slip up or two that gives us a tremendous amount of insight. We wanted to be careful, so we actually took a lot of the evidence out of the report. If you ever watch the video we posted about it, you will see one of their attackers create a Gmail account, and that guy sent about 1000 emails. We read them all, and from that we knew a lot about him – what he did, where he worked, what his job was…you get the idea.

What has caused you to focus on Chinese government involvement in cyber-espionage?
We absolutely don't focus on anything. We go where the attacks are – we don't go to where the Chinese or Russian governments are. They just so happens that the most prominent threat actors today are about 10 military units out of China that are executing intrusions. Our customers bring us this; the evidence keeps going back to China. We don't focus on the Chinese nation-state, it just happens to be very prominent, and that's what we are being hired to respond to.

How do you respond to spokespeople from the Chinese government that have called reports like Mandiant's "groundless and baseless"?
That response is to be expected – it's the new normal. It doesn't bother me in the least bit.

At the Show

ServerChoice Offer Free PCI DSS Health Check for V3.0

As announced at Infosecurity Europe 2014, ServerChoice's PCI-compliant cloud platforms and colocation infrastructure all conform to the new version 3.0 of the PCI DSS standard. To celebrate this, ServerChoice are offering a free PCI Health Check to organizations who are worried they may not meet the new requirements added in V3.0, and the offer has recently been extended to companies who just want to find out more about their PCI status in general.

Infosecurity Europe 2014 offered ServerChoice the chance to swap ideas and generate discussion points and the information security officers spent much time on-stand discussing differences between V2.0 and V3.0 of the PCI DSS standard and reviewing security requirements with business owners and IT Managers.

Being a Level 1 Service Provider, ServerChoice have the technologies and experience to help with gaining or maintaining PCI compliance with minimum hassle and cost.

Infosec Training in Tallinn

SANS will be offering three popular information security courses in Estonia this September. The Sokos Hotel Viru in Tallinn will welcome students from September 1–6 for the six-day sessions run by a trio of world class instructors.

SEC401: Security Essentials Bootcamp Style taught by Bryce Galbraith aims to help individuals learn the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems.

SEC504: Hacker Techniques, Exploits & Incident Handling with George Bakos is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

With web applications identified as a major point of vulnerability in organizations, SEC542: Web App Penetration Testing and Ethical Hacking with Dave Shackleford helps Infosec professionals understand the context behind the attacks and assess an organization's web applications to find some of the most common and damaging vulnerabilities. For more information and to benefit from early registration discounts, go to www.sans.org/event/tallinn-2014/.

ElcomSoft Revamps Phone Password Breaker

ElcomSoft recently revamped Phone Password Breaker, allowing access to valuable information in popular mobile devices such as: iPhone, iPod, iPad, BlackBerry, or Windows Phone. The tool also offers unique features such as cloud acquisition as an alternative way of retrieving information stored in mobile backups produced by Apple iOS, and the only method to explore Windows Phone 8 devices. Improvements include: Backup decryption of BlackBerry 10 devices, data extraction from Windows Live! cloud service available for all Windows Phone 8 users, iTunes backup data decryption with data categorization, and all-new Qt-based user interface for more convenience. The new look and feel is more intuitive and quickly adjustable for new market demands. For more information go to www.elcomsoft.com/eppb.html

NCP engineering's Remote Access Solution Recognized with Top Award Wins

NCP engineering recently announced that it has garnered recognition for three awards for its Secure Enterprise Solution, a robust VPN system that provides a single point of remote access administration for enterprises. NCP engineering has won a Government Security Award and an American Business Award for the second year in a row, and has been designated a finalist by Network Products Guide three out of the last five years. The award recognition underscores the company's continuing leadership in remote access amidst a rapidly changing threat landscape.

NCP's award-winning Secure Enterprise Solution is designed with the Bring Your Own Device (BYOD) trend in mind and offers a flexible and secure approach to remote access security by integrating with existing infrastructure and supporting all major operating systems, including Windows 8/7/Vista/XP, OS X Mavericks/Mountain Lion, Linux, Android and Windows CE.

Security Products' GOVIES 2014 Government Security Awards

Cybercrime and Punishment

We all know the fight against cybercrime is an uphill battle, as **Kevin Townsend** explains. In the end, he finds, the solution may be a change in both legal and social policies

Cybercrime is increasing and something needs to be done about it. Everybody can agree with this statement, but that's just about all that is agreed upon. Nevertheless, most people look first to the Law for protection.

In response, legislation is taking two separate routes in its attempts to reduce cybercrime. The first is to define the crime and attack the criminal with anti-hacking legislation. The purpose of this anti-hacking legislation is deterrence – to dissuade the criminal through fear of the punishment.

The second route is to make hacking more difficult by requiring companies to improve their security and better protect their data with anti-breach and data protection legislation. The purpose of anti-breach and data protection legislation is persuasion – to persuade companies to better secure their data through fear of the punishment.

In both cases it is believed that only severe sanctions – long prison sentences and/or heavy monetary fines – will make the legislation effective. That in turn leads to legislation's biggest difficulty: because the law cannot define all eventualities, there will always be collateral damage; that is, severe sanctions levied on relatively minor infringements. The problem here is that if exceptions are or can be made, the deterrent effect is reduced and the effectiveness of the legislation is diminished.

There are two further problems in using legislation to defeat hacking: hackers need to be caught, while business frequently ignores regulations (even legal requirements).

The Uphill Battle

To prosecute hackers, they must first be identified, apprehended, and then presented to a court. This is easier said than done – the international and multi-jurisdictional nature of the internet makes it an uphill battle. One example will suffice: the Russian constitution forbids the extradition of Russian nationals. Because of

this, any Russian hacker within Russia cannot be extradited to the US, irrespective of the weight of evidence against him or her.

Business' failure to adequately secure data is more complex, and is probably influenced by senior management's subconscious subjection to the 'optimism bias' – that is, the common belief that bad things only happen to other people. Data protection legislation tends to punish only those that have been breached; and if that is not going to happen to you, then there is little incentive to spend money complying with the law.

Guy Bunker, a senior vice president at Clearswift, suggests what he calls a 'company-killer' sanction would be needed – that is, a fine so heavy that the company is forced into liquidation – before other companies take proper notice of data breach legislation. Company-killer fines could become a reality if the EU's proposed changes to European data protection become law.

The Legislative Problem

In the past, Europe has primarily relied on its data protection laws (based on the EU's data protection directive) to persuade businesses to protect data. But the sanctions are miniscule, with little deterrent effect. The EC commissioner for justice, Viviane Reding, recently pointed out that despite fining Google the maximum possible for breaching the French data protection law, it amounted to "0.0003% of [Google's] global turnover", which she described as pocket money. In contrast, the proposed replacement for these laws, the general data protection regulation, can impose fines of up to 2% of global turnover. In Google's case, that could amount to a fine of up to $1 billion, which Reding describes as, "a sum much harder to brush off."

In the US, the most used anti-hacking legislation is the Computer Fraud and Abuse Act (CFAA), which already includes severe sanctions. Here, criticism is levied less on its content and more on its enforcement; with some very high-profile examples of severe prosecution for minor offenses. Rather than face decades in jail for downloading academic papers that he believed should be free for anyone, Aaron Swartz committed suicide. In a separate case, Andrew Auernheimer (aka, 'weev') was sentenced to 41 months for downloading – not for hacking – personal information from AT&T. Auernheimer was released from a federal correctional facility earlier this year when a US court of appeals decided to reverse and vacate his conviction after he served just 14 months of the sentence.

These and others are examples of the inevitable collateral damage from legislation that cannot keep up with technology. Chris Pogue, a director at Trustwave SpiderLabs and a former criminal investigator with the US Army, believes we should not blame the law. "Like motor vehicles or firearms or anything else, it's not the gun that kills people, it's the person holding the gun. The problem is inappropriate use – not the law itself."

> Although it is difficult, we must somehow differentiate between the cybercriminal and the white hat researcher, even though both are initially doing the same thing
>
> Eric Chiu
> HyTrust

The danger with inappropriate application of legislation, perhaps such as its use against Auernheimer and Swartz, is that it could have a chilling effect against the independent white hat hackers who patrol the internet, find vulnerabilities and report them to the software vendors. Pogue recognizes their importance. "As long as there is something to take, there will be someone to take it", he explains, "and it's been that way since Cain slew Abel. We have to have the proactive security researchers and ethical hackers that can help us to identify the security vulnerabilities before the bad guys find them."

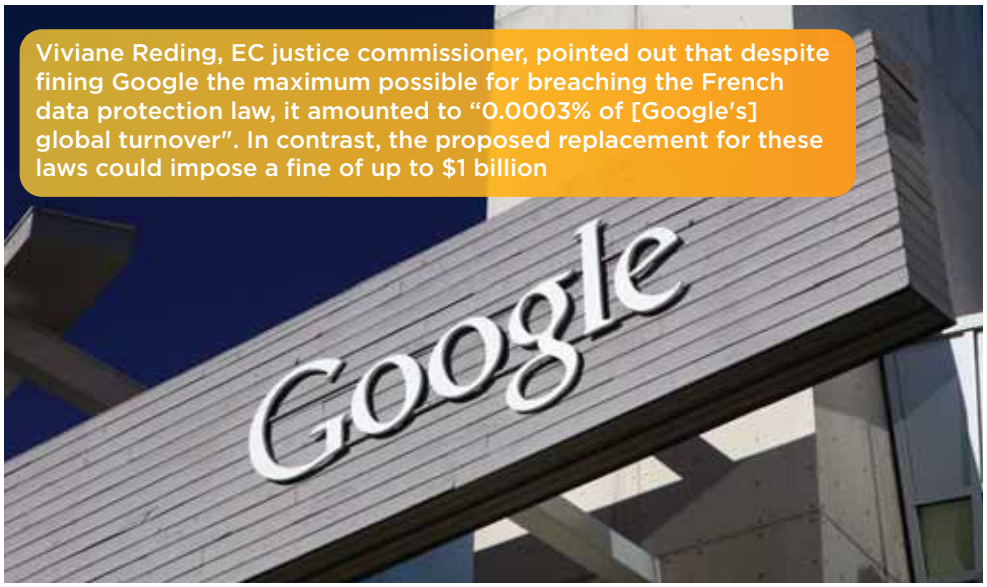
The need to nurture the white hat hackers or security researchers has been recognized by legislators on both sides of the Atlantic. In the US, senators Zoe Lofgren (D-Calif.), Jim Sensenbrenner (R-Wisc.), and Ron Wyden (D-Ore.) introduced 'Aaron's Law,' a bill designed to amend the Computer Fraud and Abuse Act. The problem with the CFAA is that it criminalizes 'unauthorized access to a computer', a phrase that can be given many interpretations. At its worst, it criminalizes even the most innocuous breaches of either a company's or website's terms of use.

Judge Alex Kozinski of the US Ninth Circuit Court of Appeals explained the potential for abuse in 2012. "Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com."

Aaron's Law is designed to remedy this issue by removing the term "exceeds authorized access" and replacing it with "to obtain information on a computer that the accesser lacks authorization to obtain, by knowingly circumventing technological or physical measures designed to prevent unauthorized individuals from obtaining that information."

At the time of writing, however, the website govtrack.us gives Aaron's Law only a 55% chance of getting past the committee stage, and only an 8% chance of becoming law.

There has been more success at reform in Europe. The initial draft of Europe's new anti-hacking law took an approach similar to the CFAA in the US. It was opposed by the Green justice spokesperson Jan Philipp Albrecht, who explained, "the legislation fails to recognize the important role played by 'white hat hackers' in identifying weaknesses in the internet's immune system, with a view to strengthening security. This



Viviane Reding, EC justice commissioner, pointed out that despite fining Google the maximum possible for breaching the French data protection law, it amounted to "0.0003% of [Google's] global turnover". In contrast, the proposed replacement for these laws could impose a fine of up to $1 billion

Photo credit: Ken Wolter/Shutterstock.com

will result in cases against these individuals, who pose no real security threat and play an important role in strengthening the internet, whilst failing to properly deal with real cyber criminals. The result will leave hardware and software manufacturers wholly responsible for product defects and security threats, with no incentive to invest in safer systems."

Albrecht's opposition paid off, and the draft was amended. Commenting for this article earlier this year, he said, "European cybercrime law was updated in 2013 and now includes harsher penalties if you, for example, run a botnet and not just hack into one computer. But we also have ensured that legitimate security testing is not criminalized, because this would undermine the internet's immune system."

What Should the Law Do to Prevent Hacking?

Drafting laws is difficult because legislators are continually subject to conflicting arguments. For anti-hacking laws, civil rights groups seek to protect personal freedoms while vested interests (such as intelligence agencies and the content industries) seek the maximum possible sanctions and the tightest possible terms. For data protection laws the roles are reversed: civil rights groups seek greater controls and higher sanctions while vested interests argue that light-touch legislation is necessary to foster investment and innovation.

However, because the most effective lobbying will always come from those with greater resources, it is reasonable to predict that anti-hacking legislation will, in general, be strict, whereas data protection legislation will be relaxed.

This leads many in the security industry to suggest that security researchers will need to find alternative ways to protect themselves if they wish to continue probing the internet's weaknesses. "The legal sanction against hackers has to be very strong", explains Eric Chiu, president and co-founder of HyTrust. "Although it is difficult, we must somehow differentiate between the cybercriminal and the white hat researcher, even though both are initially doing the same thing."

Bunker suggests that licensing might be the answer. "Licensing pen-testers would close the door to random 'hacking by researching' but would also keep people above the law – but perhaps there should also be another system, for example, via the NSA or FBI, around how an individual could disclose something without going public". Another suggestion is that ethical hackers can protect themselves by limiting research to those companies that offer a bug bounty – the invitation of a bug bounty implies an invite to probe that would be difficult to prosecute.

But it should also be said that there are those who do not believe a solution can be found in legislation. The problem, they contend, is a social one, and only a social solution can solve it. One of these is Ilia Kolochenko, founder and CEO of High-Tech Bridge, a penetration testing and computer forensics company located in Switzerland. For Kolochenko, the base problem is the wealth gap between the rich and the poor. "Young people today", he says, "know that they are smart and skilled, but have no money and no future. But they see other people with no skills and no brain, but money and fast cars. They see that they can make many thousands of dollars every month by cybercrime; so that's what they do."

Kolochenko does not believe that legislation will change this – and he has some support from the Obama administration's application of the US espionage laws. Obama's administration has prosecuted more whistleblowers than any other president, and used the very strict espionage laws to do so. Whistleblowing, however, is on the increase rather than decrease, driven more by social pressures than it is limited by legal pressures.

This social argument should not be dismissed out of hand. In January 2013, George Friedman, founder and CEO of intelligence firm Stratfor, described the potential for civil war in Europe driven directly by the EU's ability to save the banks, but not the people. "It is difficult to see", he wrote, "how continued stagnation and unemployment at these levels can last another year without starting to generate significant political opposition that will create governments, or force existing governments, to tear at the fabric of Europe."

In January 2014, the World Economic Forum declared 'severe income disparity' to be the world's fourth most serious risk, while 'structurally high unemployment / underemployment' is at number two, and 'profound political and social instability' comes in at number ten. By comparison, 'cyber risk' is not mentioned at all in the top ten global risks.

Agility and the 360° Information Security Awareness Program

By **Keith Ducatel**, director, Article 10 Information Security Awareness and Education

In an agile environment, adhering to information security policy isn't always as black and white as it should be. In addition to driving a greater focus on communicating the value of information to employees, some organizations are now using their awareness program to root out conflicts between policy and practicality.

Logically, we might say that rigid application of information security policy is paramount. Practically, however, we all know it's not always so. What happens when mission-critical business imperatives clash with information security directives?

For example, let's say your client needs a vital report within 24 hours. The only way to achieve that is to pull in more team members to work on it. However, these particular employees don't have the required access to work on the system, and the process of awarding it takes two working days. As the client account manager, what do you do? Do you tell the client you have to let them down? Or do you break company policy and share your system user ID and password (cue flash of lightning and deafening clap of thunder!).

Unfortunately, the question here isn't what's right or wrong. The question is, what does the client account manager feel compelled to do? After all, an angry customer and line manager may be more of a concern than a rap on the knuckles from IT.

Agile Information Security

Frustrating the issue is our modern agile working environment. We've all witnessed the radical shift in the way we do business over the last ten years, and most organizations have had to adapt to some degree. Traditionally, smaller organizations and those heavily embedded in the online sector tended to be the most agile. This is no longer the case. For instance, one of our largest clients recently moved offices and introduced a full hot-desk environment throughout most of the business. Similarly, BYOD has become a standard in many organizations, with some also relaxing their policy on home-working.

The move to agility has, of course, required a similar shift in our approach to information security. No longer can policies contain shackling edicts that keep employees hard-wired to desktops. They must be defined and delivered as enablers across the business.

Effective agile information security requires a very specific employee mindset for success – one that is built on clear subjective and objective understanding of the scenarios that could play out. In other words, you need to get employees to the point where they can accurately extrapolate the potential outcomes of their decisions.

Employees must appreciate that information security helps to protect their hard work and the hard work of colleagues. It protects the business too, and ensures it stays healthy. Most employees will already recognize that a healthy business is good for them personally. Naturally, this message is particularly potent in organizations with profit-sharing schemes!

These positive scenarios are subtly reinforced with the negative. Employees must equally understand what might happen if the business was to lose profitability due to a breach caused by their carelessness.

The 360° Perspective

Some organizations are going one step further and using their employee awareness program to improve information security efficiency.

Benchmarking employees at the outset of an awareness program is a way to determine the existing culture of information security in an organization. But it can also be used to determine how those policies are adhered to, and where areas of conflict exist. This enables the information security function to tweak policies or practices in order to optimize the practical situations that employees face.

Benchmarking doesn't detect all the possible areas of risk, which is why an ongoing approach is essential. For example, deploying campaigns that focus on specific topics helps to drill down into the fine detail of the policies. Many of our campaigns provide team leaders with a 'toolkit' – a set of communications assets that help them to educate their teams about the subject. Within the toolkit is a team presentation with speaker notes and suggested questions. This helps team leaders to generate a discussion about areas of the policy that are impractical for their team, which can be communicated back to the information security function.

The 360° approach shows how incredibly valuable information security awareness has become. Bespoke programs tailored to an organization are now being used to drive the wider success of the business, and are starting to make a key contribution to the bottom line.

To learn more visit www.article10.com or call +44 (0)20 7749 4450.

Navigating the Potential

Windows XP Apocalypse

To upgrade, or not to upgrade? It's a question that each organization must grapple with. Yet, not all environments lend themselves to a move away from Windows XP. **Wendy M. Grossman** surveys the peril

Thirteen years ago, in 2001, AOL and Time-Warner merged, marking the peak of the dot-com boom and sparking the dot-com bust. Wikipedia and the iPod hit the market. People bought 'candy bar' feature phones. New computers had Pentium chips. And, in October of that year, Microsoft released Windows XP.

That was then, and this is now. Microsoft officially ended support for most versions of XP on April 8, 2014. There was a brief moment of reprieve when, on May 1, Microsoft included the aging operating system in the patch for a newly found zero-day vulnerability in Internet Explorer version 6 and above. But no more, the company said at the time. The exceptions are the several versions of embedded Windows XP, such as those for ATMs and point-of-sale systems; they will be supported until 2016 for ATMs, and through 2019 for POS systems.

Qualys estimated in April that although the number of XP systems is steadily dropping, 13% of its scans still found Windows XP in use as of the first quarter of 2014. Reports from other sources vary.

Sergio Galindo, general manager of the infrastructure business unit for GFI Software and former head of IT at a large financial services company, says he's seeing closer to 20%. Karl Sigler, manager of SpiderLabs Threat Intelligence at Trustwave, predicts it may even be as high as 25%. Lamar Bailey, the leader of the Vulnerability and Exposures Research Team for Tripwire, says his large-organization customers report closer to 10%. Whatever the percentage, it's clearly substantial.

Sigler isn't particularly sympathetic. "[XP] is getting creakier and older, and it's going to be obvious that it's not working relatively soon", he says.

Resisting Change

The reasons for not upgrading vary. In smaller businesses, Galindo says, "they don't see the benefits, only the cost." Larger businesses see the risk in staying, but, "many still have applications running on XP."

Often, Bailey observes, these are applications that can't be upgraded: the original vendor has not issued an updated version or has gone out of business; the specialist software's coders are no longer available and no one else understands the code; the cost of updating is wildly disproportionate; or the source code is lost. Or, as Fred Touchette, a senior security analyst at AppRiver says, in some cases – such as expensive medical equipment – trying to update the underlying operating system may break the proprietary software that runs it.


Ninety-five percent of ATMs may still run Windows XP, and thus support for their version will continue until April 2016

"I still see Windows NT in environments sometimes", Bailey notes. Occasionally, adds Guillaume Lovet, manager of threat response EMEA for Fortinet, the cost and hassle of replacing the underlying hardware also figure into the decision. Plus, while every customer sees the effort involved in learning a new interface, many don't see the better security built in under the hood. "Exploiting Windows 7 is a hell of a lot more difficult than exploiting XP", Lovet contends.

Something like the expense argument applies to the 95% of ATMs that still run XP. Support for their version will continue until April 2016, but even so, sending someone to each individual ATM to update its software and – probably – hardware, is labor-intensive. In the US, the move to adopt anti-fraud chip and PIN, already a decade old in Europe, might be an opportunity.

"A lot of companies are already in the process of upgrading point-of-sale systems and ATMs for chip and PIN", says Sigler. However: "They have this whole plan in place with budget and finances and they're ready to go – but they never put in place, in seven years, a plan to upgrade the operating systems. The two projects really weren't merged. It's really indicative of the type of priorities that organizations set."

The Bigger Picture

Ruth Anderson, a senior manager in KPMG's cybersecurity team, takes a broader view. "End-of-life and end-of-support is not just about XP, but about how companies do this more broadly and manage the risks they face as a result", she says. However, organizations should view the decision about whether and how to upgrade as part of a broader vulnerability assessment. "Companies should absolutely be looking at where their end-of-life software is, including XP. If they're not going to upgrade, then they have to decide what they're going to do, but they should look at it in the context of all the vulnerabilities they face as an organization."

Assessing that risk isn't easy. The obvious first question is whether the system in question is connected to the internet or is easily accessible from other parts of the network. Galindo says that most companies are smart enough to have isolated those systems to lessen the chances of a successful attack (see box).

What seems certain is that the risk will increase as known but unpatched vulnerabilities pile up. Many believe the coming months will see attacks based on Windows XP vulnerabilities that have been found and saved up over the last six or more months, awaiting the end of support. Another possibility, suggested by Galindo, is that attackers will reverse-engineer upcoming patches for Windows 7 and 8 to deduce where there may be similar holes in XP.

An equally important question surrounds the threat model. It's one thing if the asset being protected is revocable information such as credit card numbers; worse if the asset is more sensitive and permanent, such as medical and financial records, that cannot be recalled once it has escaped.

Finally, it's important to assess the assets that the continued use of Windows XP puts at risk.

Stationary Risks

For Tim Keanini, CTO of Lancope, the constancy and speed of change are risk factors. "The internet has caused an evolution in information systems to change faster, and anybody who can't change is going to be fragile in this dynamic world."

This is one reason that Matt Palmer, chair of the Channel Islands Security Forum, believes the entire software industry may have to rethink its approach.

"Very few organizations, small or large, can afford to turn over their entire software estate on a three-to-five-year basis", he says. Y2K upgrades were the result of programmers' basing coding decisions on the assumption that their software would not still be in use 50 years later. "There is this assumption that software is temporary – and it really isn't temporary", Palmer reflects. Even in his relatively short career so far (he entered the industry at the turn of the 21st Century), Palmer has come across companies running software written in the 1980s. "Nobody really expected that stuff to be in use today, but it is. It's foolish to think that the stuff we're writing now will be obsolescent in a few years' time."

This will especially apply to the developing Internet of Things: people will expect software to last as long as the expensive items they're used to replacing only a few times during their lives, such as refrigerators, cars, high-end medical equipment, and the industrial control systems they are embedded in. "If something is doing the job it's meant to do, you don't want to have to throw it away", he adds. Many software companies have benefited handsomely from software that needs regular replacement. But, as Palmer says, "from the customer's point of view, the last thing I want is everything written for me every few years, but we are very bad at writing software that hands over seamlessly to its successor."

While not going quite as far as Palmer, Tripwire's Lamar Bailey at least partially agrees. "There needs to be an easier way to migrate cost-effectively", he asserts. "If we can make it so the test cycle is not so long and updates can be rolled out easier, then we won't get stuck in this place anymore."

That's a hope for the future. For the present, says Fred Touchette: "The best advice is to upgrade immediately."

The View From Microsoft

Tim Rains, director of Microsoft's Trustworthy Computing Group, recently gave his company's take on Windows XP end-of-life and the associated security risks. To read his opinions and recommendations, visit: infosecurity-magazine.com/view/37844/windows-xps-time-has-comeand-gone

Managing Legacy Systems

As previously noted, in some situations, organizations have little choice but to continue running Windows XP. In these cases, limit the attack vectors as much as possible. Treat such machines as a high-risk presence on your network, and ring-fence them as much as you can. Here is a list of some of the finer points as outlined by the experts we consulted:

- Don't use Windows XP machines for email or web surfing, says Sergio Galindo; keep it away from virus-laden websites, rogue links, and other dangers.
- Isolate them on a separate network and protect them with a firewall and as many security controls as you can, says Lamar Bailey.
- If you can keep the box disconnected from the internet, your chances for safety go way up, notes Guillaume Lovet. Fred Touchette adds that this is doubly true if you can lock it down so the box only sends information but doesn't receive it, as might be possible with some medical equipment, for example.
- Shut down unnecessary functions to shrink the attack surface, says Karl Sigler, and pentest regularly.
- Make sure you know exactly where your end-of-life software is and that you thoroughly understand both the risk you're taking and the protections you have in place in the context of all the vulnerabilities the organization faces, says Ruth Anderson.
- Ensure you are able to spot attacks as soon as they arise; today's attackers can be highly patient and persistent, hiding out in the network for months or even years, says Tim Keanini.
- Bear in mind that attackers will be studying your network looking for the easiest points of entry and locations where they can hide out, awaiting their chance to escalate the attack. Windows XP will be high up on the list of vulnerabilities they're looking for – and, as Galindo warns, "You can only be as secure as that weakest link."

Sizing Up the Tools of the Trade

The **(ISC)² US Government Advisory Board Executive Writers Bureau (EWB)** looks to help CISOs and their counterparts identify cost-effective approaches amidst the soaring price of cybersecurity tools

The compounded annual growth rate of the worldwide cybersecurity market is around 9%. US demand for cybersecurity jobs has expanded 3.5 times faster over the past five years and 12 times faster than the labor market as a whole, according to a 2013 analysis by the *Wall Street Journal*. For the chief information security officer (CISO), this typically means increasing budgets.

That being said, adding cybersecurity tools, year-after-year, to an organization's budget is like buying underwear; no one wants the expense, but everyone realizes it's a necessity. For most CISOs, it's a nightmare to convince decision-makers that an expensive IT security tool is actually a necessary cost-saving measure that will provide a return on investment, instead of a revenue-generating measure.

To make matters worse, if the CISO has succeeded in his/her job, prior breaches or other enterprise vulnerabilities in dire need of fixing may not be identifiable. For this reason, you might hear a CISO muttering under their breath, "I just wish a *little* something would happen", knowing that even the smallest security incident ensures a stream of resources into the security budget.

In 2012, a survey of technology managers in the US conducted by the Ponemon Institute and Bloomberg found organizations that wanted to achieve the highest possible level of IT security (capable of repelling 95% of attacks) would have to boost spending from the current $5.3 billion (combined) to $46.6 billion, nearly a seven-fold increase. Even an ability to stop just 84% of attacks would require an approximate doubling in their investments.

While 95% establishes a high standard, professor Lawrence Gordon of the University of Maryland's Robert H. Smith School of Business proffered that a 100% level of security is neither attainable nor particularly desirable, as it would not offer a good return on investment. The key is finding the "optimal level" of investment, he asserts, keeping in mind that costs are rising. Once new common vulnerabilities and exposures are publicly acknowledged, we can expect even shorter times for hackers to develop rootkit-based exploits with widespread release. Just as there are automation tools for rapid software development, those tools and technologies will be applied more frequently to malware.

Larry Ponemon, chairman of the Ponemon Institute, attributed the rising costs we see today to the fact that attacks are much more difficult to identify, resolve, and remediate. "Some of these pieces of malware are just brilliant and they cause a lot of damage", he said in an October 2013 comment to FierceITSecurity. "These attacks are often targeted attacks that can continue for months if not years. This drives costs up substantially". According to an April 2014 report by security firm Mandiant (owned by FireEye), hackers spend an average of 229 days on a victim's network before they are even identified.

Thus, with the gamut of cybersecurity tools on the market, a CISO's recommendations must be well-thought-out and justifiable to address the soaring costs. Following is some 'food for thought' when preparing your budget and considering your specific security program(s).

Security Intelligence Tools

Before investing in additional security tools, it is highly suggested that security intelligence tools be integrated into your program to gain a better understanding of what you need. Because the value of intelligence can decline in a matter of days or hours, more organizations are implementing an in-house threat intelligence program, including dedicating staff, tools, and other resources to network baselines, anomaly detection, deep packet inspection, and correlation of network and application data activity.

> Cyber insurance is becoming less of an option and more of an automatic purchase
>
> Dave Navetta
> InfoLawGroup

The rise of threat intelligence services is helping enterprises gain greater insight into global and industry-specific threats. The CISO's job is to figure out how to make that information actionable and to implement countermeasures in a timely manner. The key benefit of leveraging threat intelligence with analytics is that it produces predictive threat warnings and mitigation advice by monitoring security events from a wide and diverse variety of sources. By analyzing and correlating millions of global events, organizations can uncover malicious activities that may have otherwise gone unseen.

In-house threat intelligence programs can be as simple as IT staff being trained to pay closer attention to data or developing a team of people to perform deep packet inspection and forensics on a full-time basis. For those organizations that opt to purchase intelligence tools, Chuck McGann, (ISC)² U.S. Government Advisory Board Co-Chair warns, "It is important that the tool vendor invest in the success of its tools. Defining realistic outcomes and requiring an onsite technical support resource who will be held accountable for delivering such outcomes will help to minimize false expectations often presented in an initial sales pitch."

Security Suites vs Stand-alone Programs

Internet security suites include three essential software components – anti-virus, anti-spyware, and firewalls – usually with optional plug-in features for a sizable fee. Some companies bundle additional components to include identity theft prevention, anti-phishing software, and online backup.

An internet security software suite is usually cheaper than buying separate stand-alone programs, and it also reduces the likelihood that security programs will be incompatible. All of the components of an internet security software suite, however, may not be useful. A firewall is essential to protect your computer from intrusion threats, but there may already have been a firewall included on your wireless router, which experts say is more effective than software. The internet service provider or email program may already have taken care of filtering spam. Therefore, choosing between buying an internet security suite or stand-alone security software is partly a matter of weighing the strengths and weaknesses of each package against your own security priorities.

Cloud Security

Despite the convenience and economic benefits, cloud computing may not be for all organizations (i.e., those with highly classified missions and/or extremely sensitive data). However, for most, the security advantages of cloud computing, coupled with the ability to create private clouds, should offer the security assurances needed to satisfy a good number of organizations.

Those who choose to move data from physical to virtual environments should

consider the need to update their security. For instance, you can't install a traditional firewall or anti-virus software in a cloud-based virtual environment. Hypervisor security is critical when using clouds and is often overlooked. If an intruder gains control of a virtual server, they may be able to gain control of the hypervisor. And, by the way, a whole new set of security issues comes into play if enterprises allow employees to access corporate data with smartphones and tablets.

Cyber Insurance

As a supplement to security tools, insurance should be considered as a means of mitigating risk, but be advised that insurance companies are also launching new cyber products, and premiums are rising. Cyber insurance premiums can range widely based on the size of a company and the extent of its perceived exposure.

Ken Goldstein, VP & Worldwide Cyber Security and Media Liability manager at Chubb Insurance says, "small and mid-size companies may have a $2,000 to $15,000 price per $1 million limits of liability of coverage, compared with $17,500 to $50,000 or more for larger-size companies. It is something to think about." Dave Navetta, founding partner of the InfoLawGroup who helped develop cyber insurance products at AIG at the start of last decade, adds: "Cyber insurance is becoming less of an option and more of an automatic purchase."

Taking a Formulaic Approach

To compare the cost of a malware attack to the value of security tools, a formula of some type may prove useful. Following is an example:

- **Assign values** to your organization's data by determining how much it would cost to restore lost information.
- **Estimate the losses of a single incident** in recovering from a malware attack (lost employee time, lost revenue due to compromised systems, fines and penalties relating to disclosure of sensitive/privacy information, etc.).
- **Previous attacks:** Estimate how many significant malware attacks your business has suffered in previous years. This will provide you with a loss expectancy number for the years to follow and – by combining the previously determined losses – reflect the dollar amount that malware is costing your business each year.
- **Assess internal and external users:** While, in general, people don't like their actions to be tracked, businesses can use employee behavior as a tool for threat identification. If need be, place a subjective value on your security teams' level of proficiency, as well as employees' overall attitude and compliance toward security practices. If the value is high then the risk may be lower and, in turn, offset the expenditure on unnecessary tools.
- **Plan your budget.** The estimated losses will give you a rough idea of the maximum amount you should spend on malware countermeasures. Many companies may wish to spend far less, however. That's because there are situations in which businesses are willing to accept a higher malware risk, either because the likelihood of an attack is so low or the cost of mitigating the risk is so high. A rule of thumb suggests that cybersecurity expenses should be between 30% to 40% of potential losses.

Costs come in a variety of forms that include direct disruption of operations, payment transactions, and theft of sensitive data, such as trade secrets and credit card information. They also generate indirect losses such as legal liability and long-lasting harm to a business's brand. There is no one solution for all organizations. The compilation of intelligence tools with stand-alone programs, including intelligence tools plus cyber insurance, may be best for one organization, whereas a security suite is the answer for another.

Because businesses continue to become more dependent on the internet, cybersecurity budgets will continue to increase – as well as the cost of the technology solutions. Hopefully this article has provided you with some options. As the old adage goes, 'If man built it…man can defeat it!'

This article was written by the (ISC)² U.S. Government Advisory Board Executive Writers Bureau (EWB). Members of the Bureau include federal IT security experts from government and industry. Lou Magnotti, EWB member, was lead author of this peer-reviewed article. Visit the (ISC)² website for a full list of Bureau members.

The CISSP Companion You Can't Do Without

Reviewed by Shan Lee, head of information security, Just Eat

Title:	*The CISSP Companion Handbook*
Author:	Javvad Malik
Publisher:	Self-published e-book, available on Amazon
Price:	$1.29

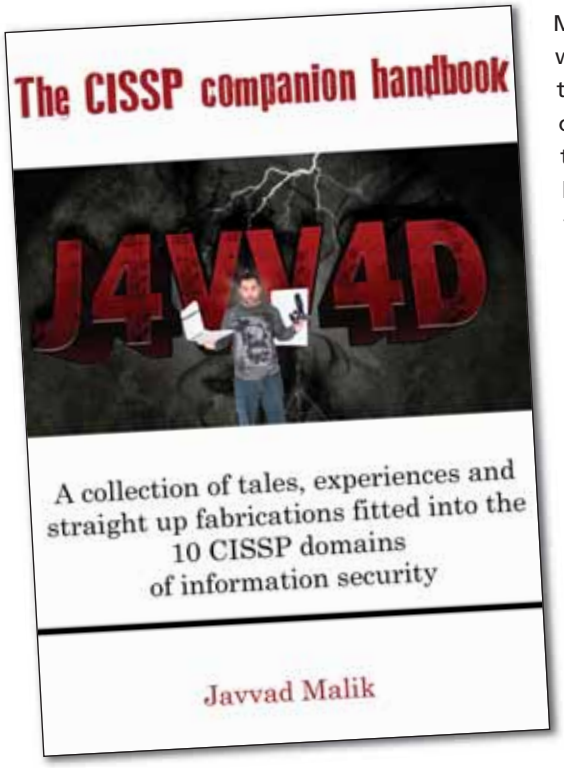
Love it or hate it, the CISSP certification is arguably essential for anyone serious about a career in information security. Many heated debates have raged far and wide as to how good, bad or ugly it is, but the simple truth of the matter is that if your CV hits the average recruiter's inbox without those five magic letters on it, then that's as far as it will go.

For most, the path to CISSP certification is a bootcamp-style course, a copy of the official CBK guide and/or many long nights in the company of Shon Harris, whose weighty tome is the go-to resource for anyone preparing for the marathon exam.

It's no criticism of the works of Shon Harris, Hord Tipton et al to call them weighty or dry; they have to be to convey the sheer amount of information they cover, but they are a daunting prospect for someone just getting into the world of information security. This is where Javvad Malik's new book *The CISSP Companion Handbook: A Collection of Tales, Experiences and Straight Up Fabrications Fitted into the 10 CISSP Domains of Information Security* comes in handy.

Malik is well known in the information security world for bringing the various concepts and issues discussed in lofty infosec circles down to earth with a bump. By combining a great sense of humor with multimedia presentations (including an excellent video blog, ably assisted by his young daughter 'Girl Cynic'), Malik has a knack for explaining those concepts in entertaining and unexpected ways. This book is no different.

Opening with a comparison between authentication controls and nightclub bouncers, the reader is taken briskly



through the basics (and some not-so-basics) of the 10 domains of the CISSP Core Body of Knowledge. Malik introduces us to the TCP/IP 'rock band', complete with FTP and SMTP 'groupies', deals with the 'supermodel wives' and 'mixed up blood groups' of the confidentiality / integrity / availability triad, and warns us of the 'evil stepmother' that is compliance.

Cryptography, possibly the most feared domain, is handled masterfully. Beginning with a fictitious email exchange that is both comedic and worryingly realistic, Malik illustrates the fundamental problem we have in information security: the fact that information security professionals often speak an entirely different language to the 'normal' people that run the businesses we work for. Without putting too many spoilers out there, it involves princes, princesses, witches and frogs in a fairytale story of asymmetric cryptography and public key infrastructure. Oh, and there's a hobbit in there somewhere too.

If, as with me, your CISSP exam is now a hazy memory, you'll find this book an easy and incredibly entertaining refresher. You'll be amazed how much you learned back then that returns to the front of your mind.

If you are teetering on the edge of whether or not you want to go down the path of studying for your CISSP, read this book before you reach for the more traditional texts. It will be the best $1.29 you've spent in a long time. You'll get a great overview of the subject matter in an easily digested format, you'll giggle at the analogies, and when you start on the big formal learning program, you'll remember them with a grin, making the whole process a lot more bearable.

info security

STRATEGY /// INSIGHT /// TECHNIQUE

Dedicated to **serving the information security industry;** in person, in print and online

- **Virtual Conferences** – All the benefits of a normal conference from the comfort of your own home. Qualify for CPE credits on attendance.
- **Webinars** – Keep up-to-date on new technologies, best practices, hot topics & issues impacting the industry. Follow a webinar and earn CPE credits.
- **White Papers** - Download free technical articles giving you in-depth insight into specific industry issues.
- **E-Newletter** – All the news, reviews and industry developments from the Infosecurity team direct to your inbox!

infosecurity-magazine.com

Should Governments Immediately Disclose Vulnerabilities?

...Point...

Sooner, Rather than Later

In the business of information security (now often called cybersecurity) there are many things that cause deep divisions among those in the profession. The role of government versus private industry, the cause of intrusions and how they can be stopped are primary examples. There is, however, one area that has caused continuous debate for more than 20 years: disclosure of vulnerabilities in software.

Many of us remember when there was no such thing as a disclosure debate – simply stated, the default was 'security by obscurity'. The concept was applied broadly to information security, but more than anything else it applied to vulnerabilities. I look back and think how flawed this concept was, but the justification for non-disclosure seemed to make sense at the time. If no one talked about a vulnerability, then no one would know about it, and therefore it would never be exploited.

The first argument in favor of non-disclosure was that no one else had the ability to find the vulnerability, therefore it would not be discovered. That rationale seemed reasonable because there were not many people doing research in finding vulnerabilities, and those that were found were rarely disclosed outside of a small community.

Second, there was the fear that disclosure would shut down critical infrastructure systems. There is no shortage of bad actors who would look to use a vulnerability to disrupt power, financial or telecommunications systems.

Third is the likelihood that disclosure would result in intrusion into government, corporate or academic systems and conduct massive exfiltration of personal data. This could result in credit card fraud, identify theft, theft of intellectual property and getting a foothold for long-term access into a system.

As the disclosure debate continued, disclosure was viewed as a way to protest software companies that were not responsive to reports of vulnerabilities. The view of many in the information security community was that large software companies did not care about vulnerabilities and they just wanted to pump out software without any regard to security.

The forward movement came in agreements that now constitute what we call 'responsible disclosure'. Not everyone subscribes to the concept, but it brings some structure to the disclosure process.

I have never subscribed to the 'security by obscurity' method, nor do I subscribe to notions of immediate disclosure, which puts everyone at risk when there is no fix for the vulnerability. In my experience, the vast majority of disclosures should be released within 24 hours of discovery. Over the past few years, the number of those with the expertise to evaluate and publish vulnerabilities has increased significantly. It is no longer a small group that can do this. It further supports the argument to disclose as soon as possible, because any vulnerability will be disclosed anyway.

In a perfect world, all vulnerabilities would be vetted and disclosed according to the threat they pose, but we live in a cyber-world where openness and freedom of expression are of paramount importance. More than once companies have had to scramble to respond to a zero-day vulnerability, but through it all the components of our cyber world still work.

So when it comes to disclosure, the sooner the better is what I believe works best. The absolute best is not to have to deal with vulnerabilities by doing better, more secure coding to develop more secure software.

AUTHOR PROFILE

Prof. Howard A Schmidt currently serves as a partner in the strategic advisory firm, Ridge-Schmidt Cyber, an executive services firm that helps leaders in business and government navigate the increasing demands of cybersecurity. He also serves as executive director of the Software Assurance Forum for Excellence in Code (SAFECode). Schmidt brings together expertise in business, defense, intelligence, law enforcement, privacy, academia and international relations, gained from a distinguished career spanning 40 years. He most recently served as Special Assistant to the President and the Cybersecurity Coordinator for the US. In this role he was responsible for coordinating interagency cybersecurity policy development and implementation and for coordinating engagement with federal, state, local, international, and private sector cybersecurity partners. His former White House appointments include Cyber Advisor to Presidents Barack Obama and George W. Bush.

.....Counterpoint....

Let the Vendors Do their Part

The recent Heartbleed vulnerability in OpenSSL raised the issue of whether or not the NSA was already aware of the vulnerability and indeed actively exploiting it. This was subsequently strongly denied by the US government, with President Obama stating that if a US government agency discovers a major vulnerability it should disclose it to the vendor. However, Obama also noted that an exception to that policy would be if the vulnerability could be used for a "clear national security or law enforcement need."

So this leaves us with the dilemma as to how and when governments should reveal any vulnerabilities they discover. Disclosing discovered vulnerabilities will mean any advantage governments may have gained over their adversaries will be lost. It also means that vendors now have a low-cost means of getting vulnerabilities identified and reported. Low cost, that is, for the vendors themselves.

We are then faced with the issue of how do governments determine which vulnerabilities to disclose and which ones provide a "clear national security or law enforcement need"? It seems logical to conclude that the most effective vulnerabilities will be the ones the government will not want to disclose, while they may be happier to reveal other, less severe vulnerabilities.

Of course the aforementioned policy is what the US government has said it will now use to manage and disclose vulnerabilities. There are many other countries that conduct vulnerability research for their own interests. Will they comply with some type of international treaty based on this process so that all users of the internet can benefit? Should all countries agree to such a treaty? Will they rate and determine which vulnerabilities can be disclosed and which ones should be kept for a "clear national security or law enforcement need"? Without some transparent means to manage this type of process, it will soon be abused. We can see how other similar treaties to limit research, development, and the proliferation of chemical, biological and nuclear weapons have had limitations in the past.

Using such a treaty that forces governments to reveal any discovered zero-day vulnerabilities will result in vendors gaining from that research – the type of research that, arguably, the vendors should be conducting themselves, thereby ensuring their products are developed securely from the start. There is also the challenge in identifying which vendors a government should divulge that information to. Should it be vendors from that government's own country? Should it be vendors that are part of that country's critical network infrastructure, no matter which country the vendor keeps its headquarters? Or should disclosure be to vendors from other friendly countries?

The alternatives to these are that governments continue to conduct their vulnerability research but not disclose it to anyone; governments conduct their vulnerability research and disclose all their findings; or that we ban governments from conducting any vulnerability research. Given the nature of the internet, the diversity of systems we use, and the numerous nation-states involved, none of these proposed alternatives are workable.

If we insist on governments revealing all vulnerabilities they discover, then we – in effect – simply provide vendors with a cost-effective way of testing their own software. In addition, an outright ban on vulnerability research by governments, or indeed by anyone else, will not be enforceable and would result in our systems being more insecure.

In an ideal world, all vulnerabilities should be disclosed to vendors in a responsible manner. We do not live in an ideal world, however, and forcing governments to disclose vulnerabilities is not a suitable solution. Instead, we need to focus on the vendors and demand from them higher-quality standards in how they secure our systems. We need to look at ways to push more responsibility and, indeed, liability onto vendors for vulnerabilities discovered in their products. As an industry, if we continue allowing manufacturers to avoid responsibility and liability for faults in their products, then we will continuously struggle to secure those products, our systems, and ultimately our nations.

AUTHOR PROFILE

Brian Honan is an independent security consultant (BH Consulting) based in Dublin, Ireland, and is recognized as an industry expert on information security. He is COO of the Common Assurance Maturity Model and founder and head of IRISSCERT. Honan also sits on the Technical Advisory Board for a number of innovative information security companies and is on the board of the UK and Irish Chapter of the Cloud Security Alliance (CSA).

CELEBRATING 20 YEARS

Join Europe's biggest free-to-attend information security conference & exhibition

infosecurity EUROPE

02-04 JUNE 2015 | OLYMPIA | LONDON | UK

Securing the connected enterprise

Collect **CPE/CPD** credits

WHY YOU CANNOT MISS INFOSECURITY EUROPE 2015

98.1% of visitors attending Infosecurity Europe in 2014, were satisfied to completely satisfied

96.6% of visitors are likely, or more than likely to attend in 2015, of which 81% are more than likely to return

84.1% of visitors are very likely to recommend participating in Infosecurity Europe to a colleague

97.2% of exhibitors were satisfied in 2014 and 80% have already rebooked to participate in 2015

ROI £447,528,560 of future orders expected to be placed with exhibitors as a direct result of Infosecurity Europe 2014

REGISTER YOUR INTEREST NOW
www.infosec.co.uk

Part of infosecurity GROUP

Organised by Reed Exhibitions

Slack Space

Hooters Blames the Hacker

After someone posted an offensive visual rape 'joke' on the official Facebook page of the Hooters restaurant chain, the organization blamed a hacker for the incident. Needless to say, the posting provoked outcry – and a curious situation in which Hooters had to portray itself as having standards when it comes to treating women as sex objects.

The image, of a woman pointing at her nether regions, has a headline of "Girls these days!!!" and carries the caption, "EXHIBIT A: The proof that she was asking for it your Honor." Clearly all kinds of wrong, and in the resulting furor, Hooters was swift to issue an apology, claiming that Facebook took its administrative rights away. "We apologize for the unauthorized posts made and are distressed by the insensitive material that was posted out of our control", the company said. "Hooters does not share these opinions. As of 7 p.m. EST, we have regained admin rights to our page and are working closely with Facebook to investigate the matter."

Not everyone was buying the excuse, however, considering the chain is best known for its scantily clad, prodigiously endowed waitresses – it's not exactly a feminist bastion. The comments section for the May 21 apology post has become a forum on sexism, objectification, free will and male hormones. Hooters itself has had to post several "we're sorry you feel that way" replies.

Nobody makes a cannoli like grandma, but as for her malware? Nonna still needs a bit more practice before she is ready to roll that out with the Sunday sauce

Others have applied hacker logic to the excuse. "If I was a hacker and had access to a corporate brand's Facebook page with over 2.6 million fans, I'm not sure that I would post something as tepid (albeit highly offensive) as that rape joke", Graham Cluley, independent security researcher, noted. "Wouldn't it be more worth my while posting a malicious link to a webpage that was hosting spyware that could make me money, or attempt to phish login credentials from unsuspecting users? Why would I just post a tasteless joke?"

It's far more likely that one of the page's administrators made an error of judgment, though Cluley acknowledged that the waters are a bit murky. "Admittedly, it's harder to tell than normal what's going on in this case because scrolling back through the Hooters Facebook page, its normal activity does seem to consist of regular servings of bosomy…waitresses wearing tight-fitting Hooters T-shirts", he observed. "Hardly the most classy part of Facebook at the best of times."

Cybercrime *Cosa Nostra*

Let's face it, "Leave the malware. Take the cannoli" doesn't have quite the same caché as the original quote from the *Godfather* about leaving guns behind after a hit, but the fact of the matter is, organized crime is increasingly a virtual enterprise. And it comes with some of the same trappings for the 'made men' of the bunch.

Look no farther than the offer from a global cybercrime syndicate to give a Ferrari to the hacker who came up with the best scam. Earlier a video surfaced from the Dark Web featuring a presenter in a car showroom alongside a Porsche, a Ferrari and glamorous female assistants, explaining that all of this could be reality for one lucky fraudster, as long as they can net millions of Euros for the boss.

Apparently, this is a fairly common practice. "A kingpin will offer a Porsche or a Ferrari to sub-groups who earn the most money", said Troels Oerting, head of the European Cybercrime Centre (EC3), who told the UK's *Independent* newspaper that his agency was seeing 85% of cybercrime activity coming from Russian-speaking territories, which international law enforcement has a difficult time reaching.

'TRO LL' of Corporate America

Andrew 'weev' Auernheimer, the hacker responsible for the 2010 heist of email addys from Apple iPad users, has been relieved of his 41-month prison sentence following a decision to vacate his conviction. Now, Auernheimer said that he's launching a company devoted to internet trollism.

Dubbed TRO LLC (get it?), the company will be devoted to short-selling the stock of companies with security vulnerabilities. Auernheimer told the *Washington Post* that investors will benefit in this way: security researchers will be tasked with identifying vulnerabilities in large-scale corporate wares; TRO LLC will then bet against these companies in the stock market before going public with the flaws, presumably driving down stock prices and netting its clients an engineered windfall. Naturally, Auernheimer will only accept Bitcoin payments.

As for whether or not the legal framework of the nation likes his tactics, Auernheimer also declared that he's committed to the endeavor and that he "will place [his] body on the altar of liberty 10 more times if it will help overturn the CFAA [Computer Fraud and Abuse Act]."

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

Every discipline has its basics – whether it is a science, a sport or, yes, information security. As with any field, failure to learn and master the fundamentals is a sure-fire route to failure. So, in the realm of information security, what is the fundamental knowledge or practice that is the dividing line between success and failure?

Having spoken with numerous information security and risk management professionals, it seems to me that the logical first step in responding to any situation is to take a personal inventory. This inventory applies to the individual as much as the organization, and often reaches beyond the realm of infosec and IT security.

Basic data protection in today's perimeterless enterprise demands a data-centric approach to security – after all, this must be true, because I can't find an analyst, consultant, or practitioner who would champion an alternative method. Taking inventory in this sense involves the categorization of data, and making risk-based decisions on the level of protection each requires. You can't build a moat around everything, so the exercise of categorizing data – through assessing inventory – is a necessity. It seems like basic, routine advice that is constantly imparted on information security practitioners, yet time after time we see organizations fail at the fundamentals, whether it is a lack of resources, oversight, or anything else.

Take, for example, data breach and security incident response. Once again, the advice of some of the industry's best experts starts with taking inventory. I recently spoke with security guru and SANS instructor, Eric Cole, as we discussed last year's Target breach and incident response in general. Effectively responding to breach scenarios, he says, starts with mapping your network. In fact, Cole noted, such a map should be undertaken before any incident occurs, so when the issue arises, those investigating can see what went wrong and where.

Cyber resiliency is a term I have heard often used by Steve Durbin, managing director of the Information Security Forum. In short, it speaks of agility when it comes to data protection, and adopting a posture that identifies critical assets requiring the highest level of protection, while also leaving your approach flexible enough to respond to the eventual mishaps and changes in technology. Again, without a proper inventory of what data your organization maintains and how it is used, employing a cyber-resiliency approach is near-impossible.

So what's the point of all this infosec 101 redux? Allow me to draw a straight line to the recent Heartbleed vulnerability affecting OpenSSL and reportedly up to two-thirds of websites – the subject of our cover feature. If a rather unscientific poll during our recent webinar on SSL attack methods is any indicator, there is an uncomfortably large number (10%) of enterprises out there that have not yet evaluated their website's potential risk exposure to the Heartbleed bug. Once again, say those in the know, a slash-and-burn response is hardly the answer. Instead, taking inventory is your best first step.

I don't want to minimize the impact of Heartbleed, or its significance in the pantheon of information security milestones. The simple fact, however, is that not all organizations that use OpenSSL software are affected by this vulnerability. By assessing your inventory and determining which versions of OpenSSL are being deployed by your organization, you can then determine the likely risk associated with this latest headline grabber. Mark Brown, director of information security at EY, recently explained to *Infosecurity* that companies using older versions of OpenSSL may actually be unaffected by the bug. In this case, it seems, being behind the curve may prove beneficial – but I wouldn't recommend it as a matter of practice.

Executing fundamentals like inventory assessment, Brown added, can actually save money in the case of Heartbleed. If proper documentation of what versions of OpenSSL are being used are actively maintained, or quickly evaluated, those tasked with responding to this and other security incidents can avoid unnecessary wholesale security reviews that waste time and money. To do so is a lot like making a patient endure an MRI to confirm a hangnail diagnosis.

Information security and incident response are hardly elementary disciplines, but what I have learned in my years covering this industry is that a significant proportion of security incidents have at their root-cause a level of neglect for industry-accepted best practices. It's less often the case that a hacker will breach your walls through ingenuity, and more likely because someone forgot to lock the metaphorical front door. No matter how sophisticated the world of information technology may become, remember that revisiting the basics can be that loyal best friend who never lets you down.

> It's less often the case that a hacker will breach your walls through ingenuity, and more likely because someone forgot to lock the metaphorical front door

Drew Amorosi, Deputy Editor

ISACA®

Trust in, and value from, information systems

"I WORK IN A **FAST-CHANGING ENVIRONMENT.**

WHEN CHANGE HAPPENS, **ISACA IS THE FIRST TO TALK ABOUT IT."**

— **ROSEMARY AMATO, CISA**
DIRECTOR, DELOITTE
AMSTERDAM, THE NETHERLANDS
ISACA MEMBER SINCE 1998

As a global association with local connections, ISACA defines the roles of information systems, governance, security, audit and assurance professionals worldwide.

Learn more at ***www.isaca.org***

MORE CONNECTED

CISA® Certified Information Systems Auditor®

CISM® Certified Information Security Manager®

CGEIT® Certified in the Governance of Enterprise IT®

CRISC™ Certified in Risk and Information Systems Control™

6-day courses

- Advanced Exploit Development for Pen Testers
- Advanced Network Forensics and Analysis
- Security Essentials
- Intrusion Detection
- Hacker techniques, Exploits and Incident handling
- Securing Windows with the Critical Security Controls
- Cloud Security Fundamentals
- Web App Pen Testing and Ethical Hacking
- Network Pen Testing and Ethical Hacking
- Mobile Device Security and Ethical Hacking
- Virtualization and Private Cloud Security
- Advanced Pen Testing, Exploit Writing and Ethical Hacking
- Advanced Computer Forensics, Analysis and Incident Response

5-day course

- ICS/SCADA Security Essentials

2-day course

- Securing the Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Includes NetWars Tournament and @Night Talks

SANS EMEA

EUROPE'S LARGEST INFORMATION SECURITY TRAINING AND NETWORKING EVENT

SANS LONDON

15th - 24th November 2014

Fifteen SANS Information Security Training Courses

Further information and online registration

www.sans.org/event/london-2014

SANS World-Class Instructors

Stephen Sims, Steve Armstrong, Matthew Luallen, Dr. Eric Cole, John Strand, Eric Conrad, Pieter Danhieux, Jess Garcia, Rob Lee, James Lyne, James Tarala, Dave Shackleford, Raul Siles, Tim Harwood.