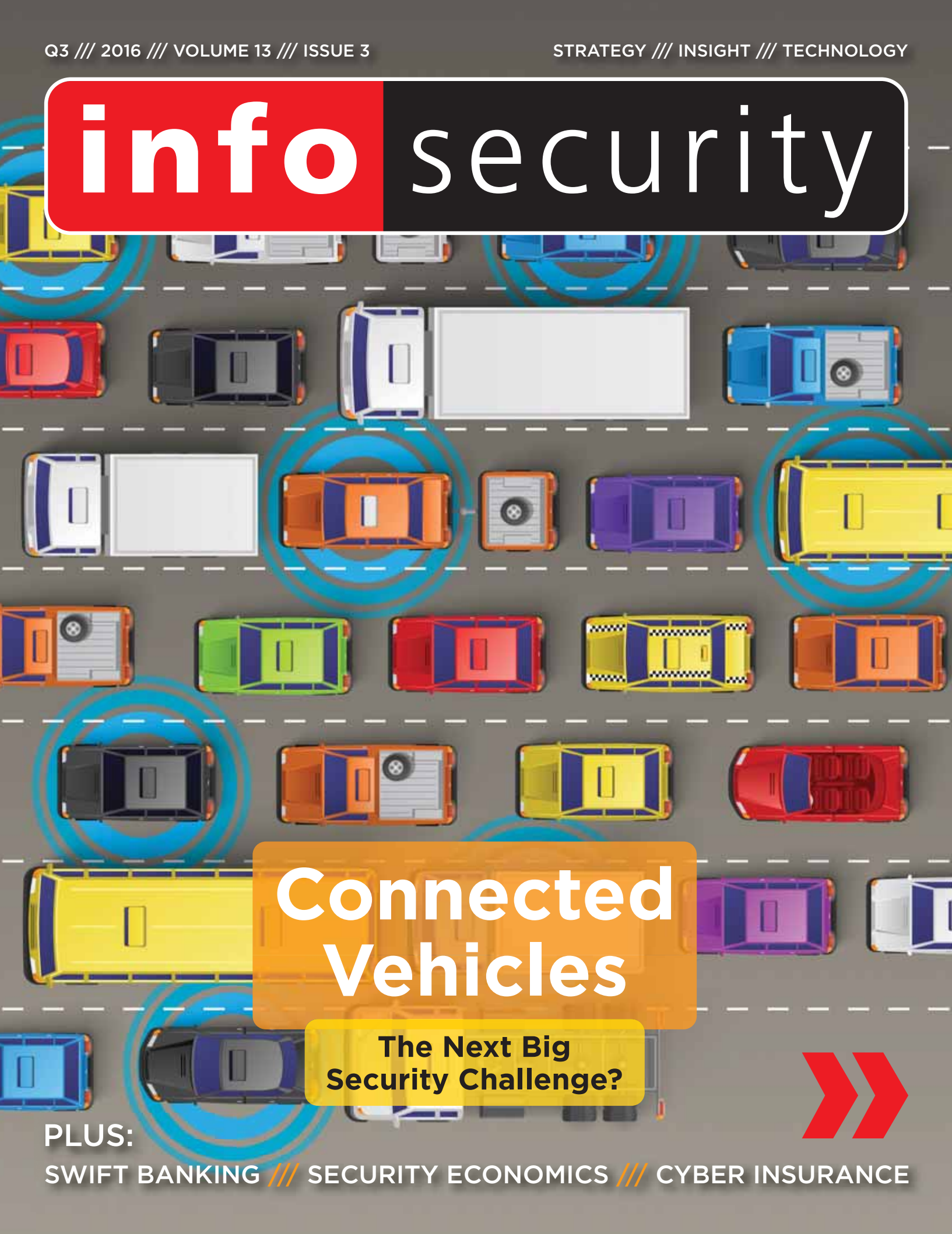
Q3 /// 2016 /// VOLUME 13 /// ISSUE 3

STRATEGY /// INSIGHT /// TECHNOLOGY

infosecurity



Connected Vehicles

The Next Big Security Challenge?

PLUS:

SWIFT BANKING /// SECURITY ECONOMICS /// CYBER INSURANCE

CyberSecurity Jobsite.com

Do you work in Cyber Security or want to?

Then join the UK's largest online job board for cyber security professionals...

- **Register**
  now to receive job alerts tailored to your particular skill set
- **Upload**
  your CV now and be seen by companies that are hiring right now
- **Relax**
  Sit back and let us do all the hard work for you...

INTELLIGENCE
INFORMATION ASSURANCE
COMPLIANCE
SOURCE CODE AUDITOR
LOSS PREVENTION
ETHICAL HACKER
IT SECURITY
MALWARE
VIRUS TECHNICIAN
CYBER THREAT
CISO
PENETRATION TESTING
FORENSICS
INFOSEC
SECURITY ARCHITECT
INTRUSION DETECTION
SECURITY ANALYST
CONSULTANT
RISK
CRYPTOGRAPHER
BIOMETRICS
VULNERABILITY
COMPUTER CRIME
FRAUD PREVENTION
CYBER SECURITY

Contents

July/August/September 2016

COVER FEATURE

FEATURES

OPINIONS

REGULARS

ISSN 1754-4548

ISRAEL AIRPORTS AUTHORITY BEN-GURION INTERNATIONAL AIRPORT | Ministry of Foreign Affairs | Prime Minister's Office National Cyber Bureau | ISRAEL EXPORT INSTITUTE | Ministry of Economy and Industry | Ministry of Public Security | ISRAEL MINISTRY OF DEFENSE SIBAT INTERNATIONAL DEFENSE COOPERATION

ISRAEL HLS & CYBER 2016

WHERE PHYSICAL & CYBER SECURITY MEET

The Israel Export Institute in cooperation with the Ministry of Economy and Industry, Ministry of Foreign Affairs, Ministry of Defense – SIBAT, Ministry of Public Security, The National Cyber Bureau and the Israel Airports Authority, invite you to meet with hundreds of decision makers and senior executives from HLS & Cyber industries worldwide at the 4th International Homeland Security & Cyber Conference

Conference Topics:

- INTELLIGENCE, CYBER CRIME & COUNTER-TERRORISM
- DEFENDING CRITICAL INFRASTRUCTURES
- A SMART GLOBAL WORLD
- MASS EVENTS - THE INTEGRATIVE APPROACH
- EMERGENCY READINESS

In addition to the conference, participants will also enjoy:

- EXHIBITION
- B2B MEETINGS
- ON SITE DEMONSTRATIONS
- PROFESSIONAL TOUR BEN-GURION INTERNATIONAL AIRPORT

NOVEMBER 14-17, 2016 | TEL AVIV CONVENTION CENTER

Secure your place now!

www.israelhlscyber.com | israelhlscyber@export.gov.il | +972-3-5142973

DIAMOND SPONSORS

Elbit Systems | IAI | MER Group

PLATINUM SPONSORS

Check Point | SuperCom

GOLD SPONSORS

IMI SYSTEMS | MAGAL S3 | PICSIX | RAFAEL | Rayzone Group

SILVER SPONSORS

GLOSEC Orad Control Solutions | MIGRAM SECURITY | ORAD | sesp

Don't Wanna Let EU Go

Another Infosecurity Europe has come and gone, and for me it was my ninth and the first as part of the team behind the show, and I was delighted not only by the high turnout of visitors, exhibitors and speakers, but also the general good vibe about the direction of the industry, which was plain to see.

Amusing to consider then, that this was in the face of the approved General Data Protection Regulation and the EU referendum, which was coined "Brexit" by the UK. As you will be all too aware, the referendum was in favor of leaving the EU by a majority of 52%, and in 2018 the Brexit will be complete. At the time of writing, the new UK Government is being formed and David Davis has been appointed as the minster responsible for delivering Brexit.

This is an interesting appointment; last year I had the opportunity to interview Davis and found him to be particularly interesting on the concepts of personal privacy and government surveillance, which he had discussed at industry events as a supporter of the right to privacy. Also, with Theresa May now the UK Prime Minister, having moved from the position of Home Secretary where she had been trying to push through the controversial Investigatory Powers Bill – which would have approved data collection and compelled service providers to collect and retain user information – it remains to be seen if the so-called "Snoopers Charter" will be approved by the new Home Secretary Amber Rudd, and with its creator now in the top job, I suspect it will continue its passage through the House of Lords.

That's UK politics though, and one thing I got a great understanding of whilst on holiday in Europe was how it was engaging many people outside of the UK. In a few weeks *Infosecurity* will be attending the annual "hacker summer camp" conferences in Las Vegas. I first attended Black Hat, Def Con and B-Sides Las Vegas in 2014 and as I chatted with other delegates and taxi drivers, it was clear that they felt that a change would be beneficial (to say the least) and with the US Presidential election only a matter of months away, the battle of Hillary versus Donald will be one that the world will be watching.

Speaking of the Las Vegas conferences, it is three years now since Chris Valasek and Charlie Miller had their car hacking talk rejected from Black Hat's call for papers, and subsequently picked up by Def Con 21. Since then, the subject of connected cars has become a key topic in security research with Jeep, Nissan, Fiat and Mitsubishi all finding themselves in the unusual position of the security headlines.

Following on from that initial research, this month we look at the issue of connected car security and ask the question of who will be responsible for fixing this in the first instance. If transport is about innovation, then surely the duty to build things securely is crucial, as otherwise you're driving around thousands of pounds worth of exploitative machinery.

In research presented at Infosecurity Europe and highlighted to the global media, Pen Test Partners' Ken Munro revealed such a scenario, and we talk to him in greater detail about the case for securing, and responsible disclosure to the car companies in an effort to fix the issues.

There has to be an appreciation of the reality of how dangerous a hacked car could be: it is about more than the discussions of "flying sideways" or SCADA-type disruption; if it is a common issue in many cars being driven around the world, then what is the likelihood of the manufacturer issuing a patch or recalling the vulnerable vehicle?

The skills and talent shortage has been well documented, but whether non-traditional technology industries start to hire the penetration testers that are apparently so desperately needed remains to be seen.

It remains to be seen if the so-called "Snoopers Charter" will be approved by the new Home Secretary Amber Rudd

To conclude this comment, this issue marks the end of my stint as editor of *Infosecurity* Magazine as we welcome Eleanor Dallaway back to the big chair after a year off creating her own future information security rockstar. It is far from the end though, as I'm delighted to be remaining with the magazine as contributing editor and working with the expanding conference division in what promises to be an exciting, prosperous and very busy future for this industry.

Dan Raywood, Editor

WHITE HAT RALLY

WHODUNNIT?

Travel along amazing roads, complete challenges, make friends and network over dinner

September 15-18

Register today!

Our three day navigation challenge guarantees a fun filled weekend for all participants. Everyone can join in! Form a team with your friends, families or work colleagues or talk to your employer about using it as your team building exercise.

This year the adventure takes place in France, with a murder mystery theme.

For more details please contact us via our website

www.whitehatrally.org

£52, 000 raised last year

Believe in children

Barnardo's

Connected Vehicles: the Next Big Security Challenge?

With the concept of the connected car invading our lives at what often seems like unprecedented speed, ensuring they are built securely at the manufacturing stage is emerging as one of the next big cybersecurity skills challenges. **Michael Hill** reports

We are entering a world of connectivity unlike the kind we have ever been exposed to before, with the concept of the Internet of Things (IoT) invading our physical lives at what often feels like unprecedented speed.

A prime example is the now commonplace use of internet-connected devices within the automotive industry, with most vehicles manufactured after 2010 having some form of internet access or wireless LAN, allowing for connectivity to appliances both inside as well as outside the car.

A plethora of on-board technologies that tap into this connection allow for a wide array of impressive features that make driving a smoother, more enjoyable experience for drivers and passengers alike. These include automatic notification of crashes, speeding and safety warnings, voice commands, contextual help/offers, parking apps, engine controls and car diagnosis, to list just a few.

However, whilst these represent how far technology is advancing and give us an exciting glimpse into what could be possible in the future of the automotive sector, the concept of the connected car is also unearthing a whole host of safety and security concerns, owing largely to the fact that the majority of the IoT devices being used are simply not manufactured with security in mind, and so are vulnerable to attack.

> We really have to start looking at who's designing and engineering these things
>
> David Shearer

Do you feel safe in a connected car?

What's more, there are significant concerns over whether there is the talent and know-how out there to cope with the sheer scope of tackling the issue, with many in the

Control your connected car from inside and outside

industry citing it as one of the next big skills challenges in security. It requires an ongoing understanding about the nature of threats and vulnerabilities in a rapidly changing landscape to build in strong security measures that effectively protect against these risks, something that is clearly currently lacking in automotive manufacturing.

Luckily, many of the instances we have seen recently where connected vehicles have been breached and tampered with have been orchestrated by honest hackers, seeking only to highlight their security issues and raise awareness of the problem. A prime example is when, last year, white hats from IOActive made the headlines by breaching a Jeep Cherokee on the highway.

"We spent a whole calendar year working specifically on the Jeep hack, so this isn't something that someone does in a weekend," Daniel Miessler, director of advisory services for IOActive, told *Infosecurity*. "At the same time, it is alarming what a single person can do from their sofa."

Miessler explained that once the engine control unit accepts commands over the control area network, a whole range of doors are open to an attacker, ranging from simply switching the radio station to completely overriding the engine control.

> Securing connected cars certainly is a challenge because these industries do not traditionally understand computer security
>
> Bruce Schneier

"It is also possible to access the power steering, parking brakes and electrical gear shift – more or less anything the driver in the car can control," he added.

"Since previous research had shown what could be done with physical access to a car, we were keen to demonstrate that remote attacks against unaltered vehicles are still possible and that we need to encourage everyone to take this threat seriously."

So, with vehicles only going to communicate even more in the future, it's surely just a matter of time before malicious hackers are not only able to lock down cars with ransomware or meddle with alarm functionality to make theft easier, but also truly endanger physical lives by remotely getting into the driving seat themselves, highlighting that very real security issues need to be addressed.

Bruce Schneier summed this up in typically astute style during his keynote presentation at Infosecurity Europe in London earlier this year, arguing that the physicality of today's IoT devices has the potential to create catastrophic risks of unprecedented scale should they be compromised, something the industry cannot afford to fail to recognize and respond to.

"I think this is going to hit a tipping point," he said on the day. "This is the 'too big to scale problem', where our systems are getting so big that we can't afford a single failure, and it's going to happen soon."

Speaking to *Infosecurity* after the event, Schneier divulged further by explaining that vehicles today are essentially mobile computers, thus everything that is true about computer security, including vulnerabilities, becomes true about cars.

"Securing connected cars certainly is a challenge because these industries do not traditionally understand computer security, so all of the things that Microsoft and Apple [for example] had to learn with regards to how to secure computers, now everyone else has to learn."

"The car manufacturer doesn't know any better, so there's going to be a huge learning curve just like we had in the computer industry in the 1990s as all of these other industries try to figure it out."

However, unlike computer security, which has an agile ethic whereby patches and automatic updates can be quickly implemented to fix new vulnerabilities, cars come from the world of "get it right the first time," otherwise the ramifications can be far more severe, added Schneier.


Bruce Schneier

"The automobile industry needs to learn that they need security in their IoT products and they need to hire the right people to do it."

Therefore, with the IoT invading our physical lives to such an extent through the connected devices in our vehicles and the possible risks having the potential to be so high, it's clear that a greater focus on ensuring they are made more secure at the manufacturing stage is of paramount importance. This is an area where, according to David Shearer, CEO at (ISC)², the industry is failing on an international scale to attract enough talented individuals with the skills and knowledge to deal with the problem.

With imbedded, connected systems now in everything that we buy, successfully securing them requires the coming together of every engineering discipline on the planet, Shearer told *Infosecurity*.

"Consider what engineering goes into the manufacturing of a car", he said. "It's mechanical, electrical, software, chemical; so you really have a convergence of every engineering discipline in the manufacture of consumer products that have life and safety issues. We need to have engineering disciplines that understand that at the design and engineering phase they need to be thinking about security."

"You have a great degree of people that are educated in the engineering disciplines, in the science and mathematics technologies, but still the numbers [in cybersecurity] are not where they need to be," he added.

As a result, it is becoming all too common for vehicle manufacturers to overlook security at the conception phase of their IoT products and implement the far riskier technique of trying to reverse security further down the line if required, with car firewall add-ons a prime example.

"We really have to start looking at who's designing and engineering these things, and we have to start pulling people (engineers in any discipline) out of colleges and universities; somehow we have to reach them and also have curriculums that teach them that throughout the lifecycle of developing a product, whether it's software, hardware, or engineering, they need to be thinking about the implications of cybersecurity. That's a bigger call to action for (ISC)² and the community at large."

These were sentiments echoed by Stephanie Daman, CEO at Cyber Security Challenge, the government's collaboration with UK industry and academia to find and nurture cybersecurity talent across the country. Speaking to *Infosecurity*, Daman explained that with a huge industry skills gap already in relation to cybersecurity, we now need to take account of the effect that the proliferation of the IoT in our vehicles is having on the skills required across the industry to ensure the safety of consumers.

> It is alarming what a single person can do from their sofa
>
> Daniel Miessler

"The skills required to tackle this wide array of cybersecurity threats are continuous and ever-changing, so in order to have any chance at sustainability, we have to engage with those who will be the cyber experts of the future. A fantastic way to encourage young people into the sector is through problem-based interactive challenges, and these are what we use in our events in order to develop the talented cyber professionals of tomorrow."

It's always been perfectly clear in the cyber industry that as technology advances, there will be a lag in the amount of professionals that are trained adequately to deal with the security issues that inevitably arise, and connected cars are no different.

However, it's an issue that vehicle manufacturers need to be taking seriously because, after all, they are the ones who will be found accountable for any breaches that their devices suffer.

Automakers need to be employing or training people who are able to build security in from the beginning, rather than simply adding it on top. At the same time, education and government bodies need to be just as mindful, recognizing their responsibility to dedicate time and resources into nurturing the next generation of cybersecurity talent in this area in order to mitigate the risks of cybercrime within the automotive industry so that people's vehicles, personal data and lives are kept safe.

Outlandish Claims? Car Hacking

Connected cars hit the headlines recently, with the Mitsubishi Outlander's security failings detailed to the world. **Dan Raywood** looked at the research

Many electric and connected cars have proved to be hackable, and visitors to this year's Infosecurity Europe got to see another example – the Mitsubishi Outlander; a plug-in hybrid electric vehicle with a mobile app, usually used for locating the car, flashing the headlights and locking it remotely, which is enabled by a Wi-Fi access point on the vehicle.

Research by Pen Test Partners found that in order to connect to the car functions, you have to disconnect from any other Wi-Fi networks and explicitly connect to the car AP and from there, you have control over various functions of the car.

"This has a massive disadvantage to the user in that we can only communicate with the car when in Wi-Fi range," said partner Ken Munro. "I assume that it's been designed like this to be much cheaper for Mitsubishi than a GSM/web service/mobile app based solution. There's no GSM contract fees, no hosting fees, minimal development cost."

The research found that the system had not been implemented securely: the Wi-Fi pre-shared key was cracked on a 4 x GPU cracking rig in fewer than four days. By de-authing the mobile from the home Wi-Fi router continuously, there was a fair chance of it then connecting to the nearby car, at which point the handshake could be captured.

Tinkering with the mobile app, Munro and Pen Test Partners were able to successfully turn the lights on and off, alter the charging program, disable the alarm and turn the air conditioning or heating on/off, draining the battery.

Munro said that some of the design mistakes in this case "defy common sense," and called on Mitsubishi to re-engineer the AP. Speaking to *Infosecurity*, Munro explained that the most significant problem for vehicle manufacturers is the long development time required for a car.

> More and more car manufacturers are taking a 'connected-first' approach
>
> Matthias Maier

"It can take years for a design to get to market," he said. "Retro-fitting security late into a development cycle can be very difficult. Whilst auto manufacturers are taking security seriously, there will be a lag for showroom models to reflect their progress in security for the above reason."

He added that there is also the question of auto manufacturers dealing with security researchers. It's a new arena for them as well. For instance, attempts to disclose the issue privately to Mitsubishi were greeted with disinterest initially – but, after disclosure, the automaker is now working on new firmware.

In a statement, Mitsubishi claimed this is the first time one of its vehicles has been hacked and that it is working "diligently" to investigate the problem. "The subject hacking has no effect on the ability of the consumer to safely start and drive the vehicle. Further, the vehicle's immobilizer is unaffected. Accordingly, while the vehicle alarm could be turned off, the vehicle would remain locked and the car could not be started without the smart key remote control device."

"More and more car manufacturers are taking a 'connected-first' approach," Matthias Maier, security evangelist at Splunk said. "For example, increasingly updates can be installed 'over-air', providing the customer with the

Live hacking at Infosec

opportunity to regularly improve their car's performance and software, as well as monitoring the operation of those vehicles. [But] if those networks aren't totally secure or isolated, an opportunity exists that hackers could exploit."

Justin Harvey, chief security officer at Fidelis Cybersecurity, said: "It's not the first time we've seen hackers gain access to a car system; it's reminiscent of the security vulnerabilities found by researchers in the Jeep Cherokee last year. The problem is that any time you connect physical devices, objects or machines to the internet, you are taking the risk that these could one day be compromised due to vulnerabilities."

If connected cars are to be a part of the future, then this example shows that security has to be part of the equation. Munro said: "In the long-term, I think Mitsubishi should be taking this a lot more seriously than they have, it's a very popular vehicle and there are loads on the roads in the UK and around the world and I really don't think that this approach to security is acceptable."

I asked Munro if he felt that the number of connected car hacking stories show a general failure of security to be part of the connected automotive process, and what could solve that. He said that car manufacturers are starting to get to grips with security (with some exceptions), but the issue is that of retro-fitting to existing vehicles on the road, plus those already past the design phase.

"It's one thing starting on a brand new car design and building in security. That's relatively straightforward," he said. "Changing a design that is already getting close to production is hard work. How much of the system, wiring loom, interfaces, gateways etc. do you change? How much do you delay the vehicle launch by? Or do you try to 'bolt on' additional modules to offer extra security and deal with the cost increase?"

Munro said that for cars in the field, it's a whole different ballgame, as manufacturers would have to decide whether to do an over the air fix, or a product recall, and could the car even support a fix?

"It's a similar challenge to that with SCADA: old technology, it has worked fine for years, but now new attacks have emerged. Do you engage in a program of slow improvement, waiting for kit (cars) to end of life? Or do you tackle it head on and rip out (replace?) perfectly functional but rather insecure technologies?"

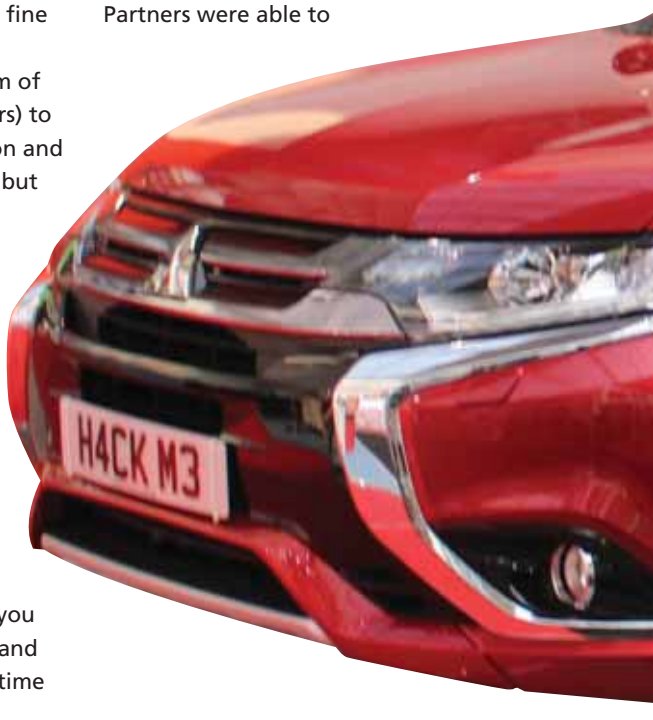
Later, Ken talked to me about some of the details that Pen Test Partners were still working on, and what had not been disclosed back in June. He said this was primarily in the way that the packets were intercepted, and the Service Set Identifier (SSID) which can be changed, but the pre-shared key cannot be changed. "This is the wrong way around", he said. "It is something you don't care about that you cannot change. The PSK is factory set and cannot be changed. We have got the time spent cracking the PSK down to two and a half days and we can sniff the handshake but do not need to be by the car."

He said that the next stage of research was around gaining full control of the car, and he said that you do still need to be near the car to capture the handshake, but once you have got the car's vehicle identification number (VIN), you are in.

Munro said that despite the media coverage of how insecure the connection between the mobile app and the car was, he had found that very few Outlander owners had switched the car's Wi-Fi off. "You only need to be within range of the car's Wi-Fi and if you can find a vehicle, either by using a national database or locate a parked car via Google Streetview, you should be able to connect to it," he said.

"The terms and conditions state that you are not able to remotely connect to the Wi-Fi, but it also states that you shouldn't be able to disable the theft alarm."

The act of stealing and cracking the Wi-Fi key allows an attacker to intercept and modify data and send Wi-Fi traffic without the mobile app. I asked him further about the packet capture, and he said that the commands had not been disclosed, nor had the content of the scripts used. Pen Test Partners were able to



> It's one thing starting on a brand new car design and building in security
>
> Ken Munro

reverse engineer packets over the air, replayed it and reduced the findings over and over in order to find out which packets were causing that to happen.

"For example, a function to retrieve the door status was not displayed within the mobile app, and also a function to unlock the doors from within the car, but the capability is there, as is a lot of functionality that doesn't appear to be used by the mobile app," he said. "We are trying to make this succeed so we have full ownership of the vehicle."

He said that current work on this project was in looking at fixes and further control of the car, and the next step was in looking at the Controller Area Network (CAN), and there was a plan to unmount the body network control module and review further.

Speaking at the Steelcon conference in Sheffield in July, security researcher Chris Ratcliff said that "CAN is on its last legs and will be replaced by Ethernet." He made a very valid point that car manufacturers are not going to go back and retro-fit everything that is on the road and when the hack on the Chrysler Jeep was publicised, they sent out a USB to every registered owner.

The reality is that fixing a car with an over-the-air patch is not easy, and apart from Tesla, which Ratcliff described as "a technology company that makes cars," automotive companies will want users to buy a new car to fix a security issue.

Another researcher, Scott Helme, who looked at similar flaws in the Nissan Leaf along with Australian researcher Troy Hunt where Hunt was able to access the air conditioning and heating in Helme's car from the other side of the world, said that in the case of automotive security research he doesn't consider it to be hacking "as security is not built as one of the design roles."

Is car hacking going to continue? Undoubtedly. Will car manufacturers take this seriously? I think it depends on whether a second model from Mitsubishi, Jeep or Nissan is researched. Is this going to change the way connected-device research and hacking is done? I think this is just the beginning.

Will the **GDPR** Help the **CISO?**

The General Data Protection Regulation will be the biggest shake up of data protection measures in almost 20 years, so what does it mean for your average security type? Dan Raywood talked to **Quentyn Taylor** for his two-year predictions

The statement made on the regulation panel at this year's Infosecurity Europe was "GDPR affects you if you are alive and on planet Earth."

That panel was chaired by PwC's Stewart Room, and appearing on that panel was Quentyn Taylor, director of information security at Canon for the EMEA region. I recently caught up with Quentyn to talk about how the GDPR will affect businesses and ask him the big questions: are companies going to be ready for this in May 2018 and is it actually going to help?

"I think it largely depends, as businesses are becoming more ready for it, but the problem with having a law with a two-year sunrise period is that it is very easy to put off and put off and then you realize [the deadline] is in six months," he said.

Taylor likened it to a university dissertation, as you put off writing it until you realize it is due in a matter of days and have to work on it overnight – he said that is what he worries about, as GDPR is not something that can be done overnight, because rather than a change of law it is a change of mindset and attitude.

"If you break it down into the 12 points that the ICO rather helpfully broke it down into, you have bits in there that are essential and you should start with now – privacy by design, privacy impact assessments – you should start thinking about that as your system could be going live in two years' time, but you've got to do the preparation work now and there are not a lot of people doing critical path analysis to work out if they work backwards from 25 May 2018, and need to know what they need to have done now."

Taylor said that what you need to have done now is to have a strategy, an idea of what you need to do and an idea of what you need to do that. "Also a lot depends on your geographical scope; which leads on to whether this will help companies – absolutely it will help companies. I think if you are a large multi-national, or a company who is considering binding corporate rules, or is dealing with multiple data regulators, or are a company who is having to wrestle with multiple sets of data laws, or are a company dealing with all kinds of data in all different places, then this will absolutely help you as the concept of 'one stop shop' is in there," he said.

"The concept of picking a lead regulator, and the ability to register once and not with lots of different places, and the ability to have one set of laws and one set of rules will apply. These are really interesting bits and hopefully this will also avoid on the regulatory standpoint, the death of a thousand cuts where you end up with multiple regulators wanting to talk to you about a major incident."

So it is all positive then, and Quentyn said that it is "something that has been a long time in coming and I am really happy it is finally here," but it's important to begin taking it seriously, as if you treat it like a project and not as a lifestyle change, then it will be back to hurt you.

The regulation addresses several key areas of modern data protection, including data ownership, data breach notification and it addresses export of personal data outside the EU and after its formal adoption on 27 April 2016, it replaces the 1984 legislation and 1995 Data Protection Directive, which the 1998 UK Act was based upon.

"The EU could have done a directive relatively easily, as a directive would go through as the changes could have been made locally without changing a huge amount," Taylor said.

The initial steps were made in early 2012 when Viviane Reding, vice-president of the European Commission in charge of justice, fundamental rights and citizenship,

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

1. Awareness
You should make sure that decision makers and key people in your organization are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Legal basis for processing personal data
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7. Consent
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8. Children
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11. Data Protection Officers
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arragements.

12. International
If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Courtesy of the Information Commissioner's Office

announced the changes. After a lengthy process of approval, it suddenly came back to life in December 2015 and was approved this year.

Taylor said that when it came through, people were a bit shell-shocked after the planning had taken place and the event was suddenly upon us. "That's the thing with GDPR, we spent so long talking about it and agonizing over what it might be and thinking about it that within a few short weeks, it was through."

Moving on to how it will help businesses, Taylor said that he believed it will achieve two levels of help: for some companies it will make some processes easier as it will achieve one centralized process; and it will also help the information security industry "dramatically" as its factors will give the canny information security person a place at the table.

"I'm lucky and do have a place at the table, but I talk to colleagues and they say that they don't have a place and now by law, the data protection people have to be there at the beginning," he said. "If you make your privacy impact assessment and wrap them all together, you get a place at the table in the beginning. So this will help the industry dramatically and I say to people to get out there, learn about it as you can be useful and helpful and the sky is not falling in, there is a huge world of opportunity and you have just got to work out how to utilize it."

In our last issue, we talked to the National Association of Data Protection Officers (NADPO) about the impact and creation of the DPO role in the era of the GDPR, and Taylor said that it is good practice to have someone in that position as if you want to play in the space of handling large amounts of personal data, you have got to determine where your data is.

So is one of the early problems of the GDPR responsibility, and is the next challenge to make sure someone takes a lead on this, whether they be in IT, security, compliance or even legal? Quentyn said that this is the key point, as step one of becoming ready is to have a strategy and sit down and say "what are we looking to do."

"It is the old story of someone saying 'our database vendor is our strategy,' and I say 'no, a product is not a strategy, a strategy is a strategy and the product supports the strategy.' It is the same thing, compliance is the end goal but it is a big word so what are we going to change and make different to what the current processes are and what do we do with cross-border transfer, is it going to change the areas of business that you are going into and what areas does it open up? My opinion is not what is this going to stop, but what is it going to enable you to do?"

He believed that in information security, a lot of people are 'glass half empty' types, and GDPR is a bit of a mixed bag as there are good things and bad things, and if you go in thinking it is a bad thing, then it will be a bad thing.

"Go in with positivity. Privacy by design, privacy impact assessments and data mapping are the three biggest things – 'where is my data' is a big question and it is a question information security people need to understand," he said.

"The correct way is to sit down and say 'what are we trying to achieve' and then risk assess the different areas of your business and say 'what are the areas that are most and least sensitive.' I recommend looking at the ICO's 12 step plan (see left) and working through it, as being ready is not just about getting a data protection course of policies, but how we are changing the culture of the company."

"The GDPR is very prescriptive on the way to do this, and you must have documented processes; and the standards are down to one way of doing things and we will receive guidance on that."

In conclusion, Quentyn left me with an analogy: "If data is the soil of the new economy, then risk and risk management is the fertilizer that helps it grow. Too much or the wrong type, and the plant dies. Just the right amount and it flourishes."
Let's wait and see if GDPR will over-feed the security industry.

Seconomics

Money continues to be spent on security solutions and services, but is there a return on investment? **Wendy M. Grossman** looks at the case for security economics and whether spending to defend really adds up

"Money spent on security is like life insurance," says Steve Bellovin, a Columbian professor and author of the recent book *Thinking Security: Stopping Next Year's Hackers*. Then, mimicking a frustrated buyer: "I spent all this money on it and I didn't die even once."

Estimating the cost of cybercrime is always tricky. In 2014, the Center for Strategic and International Studies put it at $445 billion globally and called it a "growth industry." In June 2016, the Ponemon Institute found that the average cost of a data breach for the 363 companies it surveyed was $4 million, a 29% rise since 2013. Ponemon also estimated the chance of a data breach involving 10,000 or more records at 26%, a likelihood that declines sharply as the size of the breach increases.

In the years that it has conducted this type of research, Ponemon notes that the costs of data breaches have not changed significantly and the report therefore concludes they are a permanent cost of doing business.

Estimates of how much we spend on security are more clear-cut. Cybersecurity Ventures expects worldwide spending to reach $1 trillion for the five years between 2017 and 2021, though even that number doesn't include consumer costs like post-breach recovery and personal identity theft protection services.

It doesn't help the case for security spending to see that many companies – LinkedIn, Sony, Target – that have been the targets of large, highly publicized breaches have survived reasonably well. Eldar Tuvey, whose company, Wandera, uses the cloud to block attacks on mobile in real time, has been observing the impact of beaches on companies for more than 15 years.

Despite some companies' survival rate, he says: "The secondary costs of a breach – reputational cost, credibility, brand – are sometimes existential for a corporate." According to Tuvey, a key problem for most businesses is the increasing complexity of networks and supply chains: "I don't think any one player can be an expert in all these areas."

Complexity is also the biggest issue for Ottavio Camponeschi, VP for EMEA for the security vendor FireMon. "The environment right now is so complex it's almost impossible to manage," he says. He believes that it's essential to simplify and smooth workflows to make it easier to correlate and analyze different data streams.

"Every time customers add something – an application, a company – they're building workflows that are carrying security holes," he says. "Firewalls are carrying rules and policies that are ten years old. How effective can those be?" Sometimes, he adds, "They're built for a specific application which is no longer used inside the infrastructure – and the people that built it have maybe left the company."

"A lot of the people holding the reins don't always know what the shrewd investments are," says Trustwave's EMEA director, Lawrence Munro. "Technology is only as good as the people who operate it, and tuning is very important." If, he adds, the technology is sending out thousands of alerts, it will get turned off very quickly. This is one area where researchers such as Miranda Mowbray at HP Labs in Bristol hope that machine learning can play a part by vastly cutting down the numbers of false positives.

Munro offers practical advice: fix things as early as possible and embed security as early in development as you can; spend the money you need on the right people for the job; and evangelize security at all levels of the business. "Security is everyone's responsibility," he says.

All of these approaches tackle the practical aspects of how you allocate your available resources so they're not wasted. Business managers and security practitioners wrangle over this every day: what money needs to be spent on which technologies and practices, to defend against what threats?

Bellovin argues that what's crucial is understanding who might be targeting you and why. If your attacker is a nation-state, "the more you're going to spend and the less you're going to get for the money". If you really are such a target, he suggests strategies such as pulling a machine at random and taking it apart down to the bits to see what you find.

The deeper aspects of what Bellovin is saying, however, are more theoretical: applying the discipline of economics in order to understand how misplaced incentives make security fail in unexpected ways.

> Outrunning the other guy is still a good thing
>
> Steve Bellovin

Because: if spending money on security doesn't make you safe, why do it? How do you make the case if you never really know what your money bought you?

"You can point to specific attacks and specific defenses and say 'this defense will stop that attack', but attackers are adaptive, and if they want to get you [specifically] they will move on to the next attack," Says Bellovin.

However, it's also easy to err in deciding whether or not you're a target. Bellovin's example: a threat intelligence company determined that computers in a small Wisconsin welding shop had been penetrated by Chinese hackers and used as a stepping stone. There are three likely scenarios. First, the attacker chose this specific company because of its relationship with a certain, larger target. Second, the attacker thought the company might have interesting customers, and then chose one that looked worthwhile. Third, the attacker operated randomly, and then explored the possibilities.

Determining which might apply to your specific case requires the engagement between security, technology, and business people to assess the industry and the competition, as well as the technology landscape.

The theoretical aspect of security economics has been growing quietly in the research community ever since Cambridge University professor Ross Anderson and Google's chief economist, Hal Varian, co-chaired the first Workshop on the Economics of Information Security in 2001.

"As techies, we were trying to figure out why the stuff we were doing wasn't working the way we thought," says Bruce Schneier, a WEIS co-founder. "It turned out there were economic reasons." The reasons why money is misspent varies, but "There are a bunch of examples of security failures which are not technology failures but economic failures." Incentives may be in the wrong place, or network externalities mean that the people who shoulder the costs are not the ones who suffer when security fails.

As an example, Schneier cites the length of time we had to wait for viable solutions to spam email. Although it was a persistently growing problem for both ISPs and individual users, workable solutions that could have been installed in the backbone carriers were never adopted: "They don't have any economic interest in seeing that you don't get a virus." It wasn't until Gmail and Hotmail aggregated large numbers of users that these backbone solutions were deployed and users' inboxes became manageable again.

There are many examples like this. One reason – to answer the question we began with – it's important for everyone to pay attention to security as that with today's complex, interconnected partners and supply chains anyone may provide the vulnerability that makes someone else suffer. The 2013 Target hack is a perfect example: the attacker's entry point was stolen credentials from a heating and air conditioning contractor.

The earliest work in this field is usually dated to Angela Sasse's 1999 paper "Users Are Not the Enemy." BT had asked Sasse to study the question of why its staff was so incapable of remembering their passwords. Sasse's resulting study became the first research to consider the role of usability in effective security – people couldn't remember their passwords because there were too many, they were too complicated, and they had to change them too often, all problems that persist today because "best practice" has not changed.

Further, economics also featured: Sasse's commission was a response to pressure from the accounting department to do something about the fact that the cost of the help desk was tripling every year with no end in sight.

There are a bunch of examples of security failures which are not technology failures but economic failures

Bruce Schneier

"They said, 'Figure out what's going on – and stop it'," she says.

More recently, Sasse has headed the RISCS Institute, a collaboration among five universities with the goal of putting a solid scientific evidence base under information security. Her particular project, Productive Security, sought to establish "how to" device security practices and policies that make it easier, not harder, for users to do their real jobs.

Most of the papers presented at WEIS every year are too descriptive to provide practical advice to practitioners in the field, but their influence is spreading into projects – such as RISCS – that do produce practical advice and usable tools.

The usefulness of economics in understanding and predicting security behavior stretches beyond simple cost-benefit analysis, though that's important, too. As Sasse says, based on her years of research inside companies, because many security people spend their time in their own silo, "They feel like because security is important they don't have to think about the costs."

In the end, Bellovin says, we keep spending because, "It does provide benefit – not as much as we'd like, but outrunning the other guy is still a good thing."

Divided We Stand:

Will Brexit Weaken the UK's Cybersecurity Industry?

After the historic EU referendum result in June, **Phil Muncaster** takes a look at what the next steps are

Well, it happened. It may have been a slim 52:48 majority but the country has spoken, albeit in a referendum many have argued should never have been called. The result is that the UK's politicians will most likely feel obliged to act according to the "will of the people" and negotiate their way out of Europe. Few in the technology industry wanted this outcome: a pre-referendum poll of techUK members had 70% in favor of remain, but now we all have to deal with it.

The question remains though: deal with what exactly? The truth is that at the time of writing, Article 50 – the part of the EU Treaty which allows a member state to notify of its intention to leave the bloc – has yet to be triggered. In fact, it might not be triggered for some time to come, as political parties elect leaders, decide whether they need another general election, or even work out a way for parliament to veto the result of what was a non-legally binding referendum. In the meantime, there is uncertainty, and uncertainty isn't good for any industry.

So what exactly will happen to the information security industry if or when the UK formally requests to leave the world's biggest single market? What impact could a prolonged period of uncertainty have on us? After all, these are uncharted waters. Once Article 50 is triggered there is a maximum two-year process of exit talks before we leave. This cannot be extended.

The status quo will be welcomed by some, as it means current agreements continue. The UK is still in the EU, and although this means it is still making those pesky financial contributions, it also brings rewards in the opposite direction. For example, the European Commission recently announced a €450 million ($500m) fund to encourage the development of innovative new cybersecurity products.

For one thing, we're still sharing threat intelligence across borders. A CERT UK spokesman tells *Infosecurity*: "It is very much business as usual for us. As for the future, it is too early to speculate how things may change, but we are all agreed that information sharing is key, so no reason to think that will change."

BH Consulting founder Brian Honan, special advisor to Europol, agrees. "I would hope that once the UK decides to formally leave the European Union that the appropriate agreements will be negotiated and put in place to ensure the minimal disruption to how UK law enforcement agencies will work with their counterparts within the EU and also with bodies such as Europol," he tells *Infosecurity*.

> Implementing an arrangement with the UK would not be a new departure for them
>
> Brian Honan

"It should be noted that Europol does cooperate with law enforcement agencies outside the EU already and therefore implementing an arrangement with the UK would not be a new departure for them."

People Power

When it comes to recruitment, things aren't looking so rosy, however. MediVisas partner Victoria Sharkey is an immigration lawyer who sees the referendum decision as having a largely negative impact on the cybersecurity industry.

"The UK has just become a less attractive place for people to come and work, and this, tied in with the likely visa regulations, will deter EU nationals from coming here," she says. "If you are a German infosec specialist, you may have taken a job in the UK because you can just come here without the need for a visa. If you now need a visa, you may as well go to the US. I feel that when we do leave that it is going to become significantly harder for UK employers to encourage the best in their industry to come and work in the UK."

It may also force UK nationals – especially those lucky enough to have secondary European citizenship – to move abroad, further reducing the talent pool, she says.

The prospect of Silicon Roundabout dissembling might please some people, but there is a genuine risk that the UK could undo all the good work it has put in over the past decade or so in encouraging a new generation of innovative start-ups to drive the digital economy onwards and upwards. London has fought hard to become the start-up capital of Europe, but already rival cities are lining up to replace it. Germany's Freie Demokraten (FDP) Party even hired a van recently to drive through the capital displaying the message: "Dear start-ups, Keep calm and move to Berlin."

Uncertainty Creeps

Philip Letts, CEO of global enterprise services platform blur Group, has led both Silicon Valley and UK tech businesses. His assessment of the situation? "It's bad news for investment, start-ups and tech focused purely on growth and the UK market."

Letts predicts that, although the big US multi-nationals will want to stay in both the UK and EU, over time they could shift the

majority of operations to the more lucrative mainland. "Business confidence is low and many will hunker down, try to avoid risk and wait for this to play out," he adds.

"Of course, attracting the right talent is already challenging, but it's probably just got that bit harder. For me, the UK tech sector needs to focus on what it can control – customers, cost reduction and profitability – and continue to do what it does best – innovate – whilst making sure the world knows that the UK and its businesses absolutely remain global in their outlook."

Chatham House associate fellow, Emily Taylor, is also concerned that a prolonged period of uncertainty could lead to various multi-national companies pulling data out of the UK and transferring it to European outposts. A potential clash between the coming Investigatory Powers Bill, or Snoopers' Charter, and the European General Data Protection Regulation over bulk surveillance may also cause problems if the UK wants to stay in the single market, she adds.

"At stake is the legality of data flows between the UK and the EU. We've seen in response to the Safe Harbor decision that data can move offshore very quickly. There's uncertainty over whether planned data center build-outs will be stalled by Brexit," she tells *Infosecurity*.

"Either way, it's a good idea for businesses, during this period of uncertainty, to continue to comply with data protection legislation. For now, these are still our laws, and in the future it may protect EU-UK data flows to be able to show compliance."

That's also the advice from the Information Commissioner's Office (ICO) which, even if we were to leave the EU and not follow the Norway model, appears to favor harmonizing the UK's data protection laws with those of Europe. Its statement soon after the referendum result had the following:

"With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organizations and to consumers and citizens. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the UK law remains necessary."

Doom and Gloom?

All told, it's pretty tricky to find optimists in the cybersecurity space at the moment, but KPMG UK's head of technology, Tudor Aw, thinks the industry is resilient enough to thrive outside the EU, referencing the tech sector's positive response to the financial crisis.

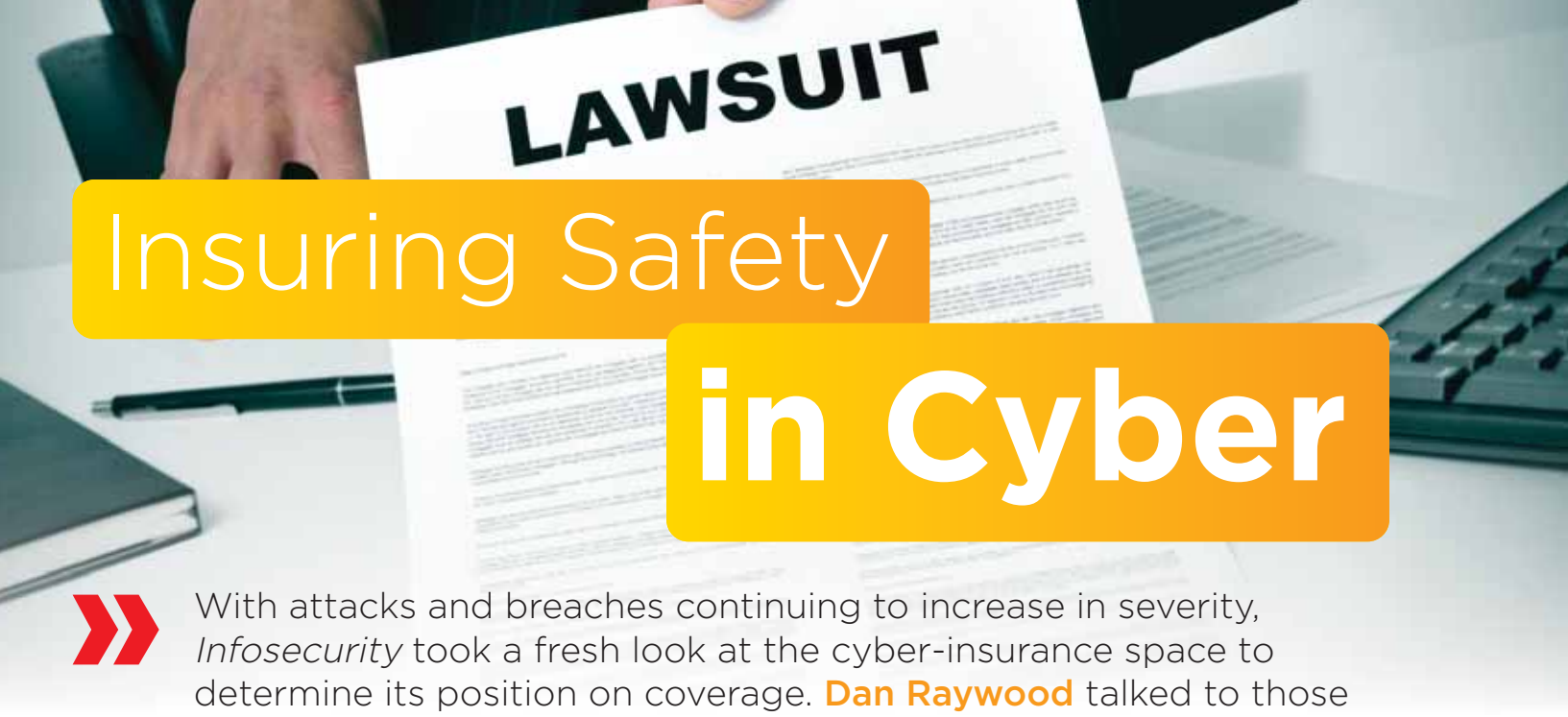
He adds that as technology is "a key sector that underpins all other sectors," it will continue to receive growing levels of investment, in or out of Europe, as organizations seek to drive efficiencies and strategic growth.

"There are of course challenges ahead and the biggest of these is immigration. Even before Brexit, tech companies were commenting on the difficulties of recruiting tech talent. If we are to move to a points system, I would like to see the tech sector prioritized so that we can attract and recruit the very best tech entrepreneurs, investors and talent," he tells *Infosecurity*.

"[But] the core attributes that have made the UK tech sector so strong and attractive remain in place, including an amazing talent base that has a long track record of creativity; great infrastructure and facilities; first class universities, a stable legal system; appropriate fiscal incentives; timezone advantages; and an ecosystem of advisors that support the needs of tech companies."

> When we do leave it is going to become significantly harder for UK employers to encourage the best in their industry to work in the UK
>
> Victoria Sharkey

Time will determine the impact of the referendum on the UK cybersecurity industry and the UK economy, but one thing is assured: with the GDPR and Brexit both set to be delivered in 2018, we're all going to be pretty busy over the next few years.



Insuring Safety in Cyber

With attacks and breaches continuing to increase in severity, *Infosecurity* took a fresh look at the cyber-insurance space to determine its position on coverage. **Dan Raywood** talked to those involved to understand if this is in a better place in 2016

The last time that *Infosecurity* looked at the cyber-insurance market, the hype machine was in overdrive about taking it out, what it covers and how much coverage you could get. However, the big question remains on whether or not it's really worthwhile having insurance to protect you from an unknown threat.

After all, Target had at least $100 million of cyber-insurance to cover its 2013 breach, and typically cyber-insurance covers first and third party cases with the first party covering internal costs incurred by the company, and third party coverage handling the fallout from cybersecurity events that affect other companies and individuals.

According to research released in June by Mimecast, firms are unsure about how their cyber-insurance policies are affected by evolving email attacks. Its survey of 436 IT experts found that 45% of firms with cyber-insurance are unsure if their policy is up-to-date for covering new social engineering attacks, and only 10% believe it is completely up-to-date. Just 43% of firms with cyber-insurance are confident that their policies would pay out for whaling financial transactions. Nearly two-thirds (64%) of firms don't have any cyber-insurance at all.

"Cyber-insurance uptake is growing quickly, but a lack of employee training on the latest email attacks is leaving organizations at great risk of breaking policy terms," said Steven Malone, director of security product management at Mimecast.

"While insurers often pay for clean-up fees after a breach, it is important that organizations check that their policies protect them if an employee is tricked into sending a large amount of money to a fraudulent account. Attacks where employees are tricked into sending personal data or intellectual property are even less likely to be fully covered."

"With the cybersecurity landscape constantly evolving, cyber-insurers will have great difficulty keeping their coverage up-to-date. A comprehensive cyber resilience strategy is only effective alongside regular employee training on the latest threats combined with appropriate technology fail-safes."

Mimecast are not alone in highlighting this issue – PwC's Global State of Information Security Survey for 2016 found that 59% of businesses were implementing cyber-insurance to improve their posture, while the survey of attendees to the 2015 Black Hat USA conference found that 37% of respondents said it was either "highly likely" or that they "have no doubt" that they would face a major breach in the next 12 months; in 2016, that figure has risen to 40%.

One solution to the problem could be a central database of cyber-incidents, which would help tackle the lack of data to enable insurers to properly price the cyber-risk and help the cyber-insurance market to grow and provide more choice for businesses.

This was proposed by the Association of British Insurers (ABI), which it said would be a not-for-profit database to contain details of incidents including business interruption losses, ransom demands, loss of confidential data, and damage to IT systems.

The anonymized data would be made accessible to insurers who could then use it to improve pricing, and potentially put the UK at the forefront of the global market. Brunella Flackett, client partner for Financial Services and Private Equity with Armstrong Craven, believes the database can be of benefit in other ways too. "We have completed an insight project for an insurance client which wanted to understand the optimal organizational structure for a number of different areas including digital; they wanted to know what best practice looked like in other sectors as well as their own and this included how others were addressing the cyber issue," she said.

"Because cyber is a fast emerging area, the talent is scarce and therefore in high demand. Organizations are moving fast to map and pipeline the best talent in this very specialized field. to ensure they have the best possible strategy in place in the event of attack."

In this section we will look at the cyber-insurance sector, with opinions on coverage, underwriting and how information security, attacks and insurance are coming together.

Reducing the Exposure of a Breach

Dan Trueman, underwriter at Lloyd's

Catastrophic losses from data breaches can affect any business, of any size or industry. Even for those covered by insurance policies, many will be unaware of the specifics and whether a cyber-attack is included in their cover or not (known as "silent cyber"). According to research from Mimecast, an alarming number of businesses have little or no idea whether they are covered against particular threats – a worrying prospect.

Without expert insight, it is quite challenging for many businesses to quantify their exposure to a cyber-attack. As such, it is vital for businesses to increase levels of insurance for better risk management.

Understanding Cyber-Insurance

Traditionally, cyber-insurance covers the losses relating to damage to, or loss of information from, IT systems and networks, but today, it does much more than that. It covers both the liability of holding large amounts of data, whilst also covering a business' resilience.

In today's threat landscape, insurers are capable of covering various types of risk, from cyber-extortion and ransomware to liability for holding payment data. Working with underwriters who understand this risk from the beginning will benefit a company's security strategy enormously, as this will allow businesses and insurers to identify their risks from the off-set.

This also means better value, cheaper premiums and more accurately aligned tools in place to protect the organization – working with the C-suite, security teams can protect the business from the perils based on vulnerabilities, not just ones they think they need protection from. It's all about building cyber-insurance in alongside tools that protect the business from the inside out from the beginning – not bolting it on when a new threat appears.

> It's no longer an "us vs them" when it comes to insurance and security teams
>
> Dan Trueman

Data is the New Oil

Hand-in-hand with a good cyber-insurance policy is the implementation of security software and hardware that can help protect an organization's most valuable commodity – data. It's vital that this asset is kept safe and insured for extra protection. Shareholders and customers are already judging businesses by how they handle a breach.

With data now nicknamed the 'new oil,' it is a high risk commodity and because of this there is a huge requirement for better expertise and importance around consolidating and best practice.

Because the cyber-insurance industry has been dealing with notification for many years, it understands where the risks lie and also the possible exposure of a data breach. Having cyber-insurance implemented from the beginning can ensure any notification is effective, risks are reduced and any communication is accurate.

Protecting the Balance Sheet, Together

Huge hacks such as those on TalkTalk and Ashley Madison have highlighted how it's now a matter of "when, not if" a company suffers a cyber-attack or breach, but they shouldn't be company-ending events. This is where the expertise from the security industry and insurers can work together to combat the growing threat.

It's no longer an "us vs them" when it comes to insurance and security teams. Insurers deal with thousands of organizations a year and it's important for these teams to work together to minimize the risks of cyber-events.

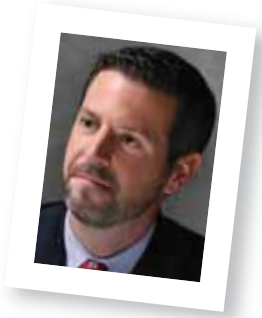
Insurers are not there to tell businesses that they are not doing enough, but instead to help them understand what effective and efficient best practice is. By doing so, businesses can protect their balance sheet, also ensuring that catastrophic loss is minimized, making sure there is value – even if the incidents are small. Cyber-insurance can also help to improve standards and give CISOs the tools or standards to get buy-in from the board for more effective security investment.

What Does the Future Hold?

Online operations are now essential to all modern business. With data the lifeblood of an organization, cyber-insurance looks increasingly likely to become the main type of insurance businesses look to take out. Other types of insurance that are currently more mainstream, such as property, will soon become a simple add-on.

In today's digital landscape, it's about organizations working more closely to reduce their levels of risk, and also protecting a company's balance sheet, when the worst does happen.

Writing for the Underwriter
Matt Cullina, CEO of IDT911



Matt Cullina is CEO of IDT911, a US-based cybersecurity and identity theft protection firm with a strong foothold in the cyber-insurance space. He explained that his biggest partner is the B2C insurance market and working with 17 of the top 20 underwriters, it develops a program that involves underwriting and coverage development for brokers.

He said: "To information security, at our core we manage crisis and if someone is calling fire and facing security incidents, for 90% to 95% of policies we are the first number they call. We create a coverage form and that goes to our our data breach response team."

The customer builds a co-branded program, builds a policy and a carrier underwrites it. With GDPR coming into force from May 2018, where the reporting of data breaches will become mandatory, Cullina said that users need to be sure there are the processes and abilities to make these cases and the correct steps are taken for the regulator.

So are cyber-insurance policies hard to write? Cullina said that normally it is an endorsement or add-on to liability insurance of £50, £100 or £200 to add the cyber element on, and that is typically the market we have gone with.

"The risk tends to be proportionate to the number of records, so you can have a small accountancy firm with sensitive data or have a large manufacturing company with exposure due to distribution, but it is not compared to number of employees they have, so it is about looking at risks and damage coverage," he said.

"For the average business, the best cost is not just for crisis response, it is also for coverage of downtime during ransomware, and if a small business is targeted and has its website taken down and money is lost, it is reimbursable. So it is not just for crisis cover, but if damage is done when business was down."

Cullina said that the company's fastest growing area is smaller retailers who deal exclusively through the Amazon Marketplace, and cyber-insurance covers them as the last thing that they want to do is blend cyber with personal risk.

So have they seen more interest and demand in the past few years? "The education issue with small businesses is that they don't understand the value of the records that they truly hold, and their element of IT is that they don't think they are responsible for risk, so we combat that with training sessions with the brokers."

"A lot of small businesses don't have budget to deal with pressures, so we went where there is high risk and no coverage. A small business with a total insurance spend of £2500 is not going to spend again on a cyber-risk that they don't deem to be important, so they can bring limits and policies and improve to a point, and it becomes a much more attractive proposition for them, and those businesses have some level of protection."

Cullina explained that in the USA, regulations are more developed and there is more of a reason to buy as if you are breached there are steps you have to take. "As soon as the CEO thinks logically about the requirements of a data breach, it becomes more and more worth it," he said.

"It's not about how many records or employees you have, it's about how you store the data and what type of business you are. In a typical claim scenario, legal is the biggest expense, but in cyber it is forensics and often it is a needle in the haystack situation."

"Information security costs range and that can create a limit. There are certain cases where a company has lost 4000 records, and should you be informing those customers or making better use of that spend."

Understanding What You Are Covered For
Norton Rose Fullbright partner Ffion Flockhart

Cyber-risk is constantly evolving. As IT professionals know, the risks are many and varied; with over one million new types of malware being developed every single day, cyber-attacks can cost companies dearly in terms of business interruption and reputational damage. Additionally, with cyber-security and data protection now firmly a priority on the global regulatory agenda, businesses may also be exposed to legal liability if they do not adequately protect the personal data of their customers and employees.

Cyber-insurance offers one way for businesses to manage these risks. It can be used to "plug the gaps" in cover which traditional insurance products leave behind.

Cyber-Insurance – What is Covered?

Cyber-policies cover certain direct losses to the business and/or liabilities to third parties that arise out of unauthorized access to, or use of, an organization's electronic information, or the destruction or loss of that information. Most policies in cybersecurity also offer a number of valuable add-on incident response services, such as legal, forensic, PR and crisis management support. Such services can be an invaluable means of swiftly dealing with adverse incidents and mitigating their impact including from a legal and regulatory perspective.

In terms of direct losses to the business, these may include instances where an

attack takes place and money is siphoned away from the company's account or valuable data or intellectual property is lost. Cyber data, policies may also cover business interruption where the interruption was caused by a cyber-incident, such as a system failure (whether due to malicious hacking or not). For these types of loss, cyber-insurance affords protection in circumstances where traditional lines of insurance are unlikely to respond.

For instance, under most property damage insurance, the insured would be unlikely to get business interruption cover unless there has been some physical damage to property, which is generally less likely where a cyber-attack has occurred. Cover is also now increasingly becoming available for losses caused by cyber-terrorism (i.e. acts of terrorism committed via an organization's electronic systems), which are usually expressly excluded from traditional terrorism cover.

Businesses are often concerned about reputational damage caused by a cyber-incident. This type of loss is, however, difficult to quantify in real terms and provides a challenge for insurers as they attempt to price the risk. At the moment, stand-alone cover for reputational damage is not generally available under cyber policies, but this is an area which the insurance industry is frequently being asked to consider.

In terms of potential liabilities to third parties, cyber-related losses are often not covered by professional indemnity insurance as they do not directly relate to the actual performance of professional services. For example, if an employee lost their laptop outside the workplace, inadvertently losing a vast amount of sensitive client data, a PI insurer might reject a claim on the grounds that it did not fall under the employee's performance of professional services. With the majority of cyber-breaches within organizations last year being caused by employees, either deliberately or accidentally, companies may be exposed to potentially significant losses if broader cover insurance is not in place.

Changes to the Risk Landscape

The risk landscape in terms of potential liability to third parties has recently been widened by the English Court of Appeal's landmark ruling in the case of *Vidal-Hall v Google*, which indicated that data subjects can sue without having suffered any financial loss. While this point is currently being appealed to the Supreme Court, the practical consequence could be that, if a business compromises an individual's personal information, it could be subject to liability in damages for emotional distress, even if the individual hasn't suffered any actual monetary loss.

From a regulatory perspective, undoubtedly the biggest development in terms of insurable risk is the General Data Protection Regulation (GDPR). Due to come into force in May 2018, the GDPR will place significantly enhanced data protection obligations on organizations whose goods and services are directed at EU citizens. The extra-territorial reach of the GDPR means that its provisions, including the substantial fines, will still apply to UK organizations even if Britain was no longer a member state. This will include any UK-based service providers who process personal data of EU citizens and, more widely, any UK companies that have an online sales presence in the EU, meaning the implications may be potentially huge.

Those companies are expected to look increasingly to cyber-insurance to cover the risks that arise out of these obligations. This growth in cyber-insurance uptake reflects the position in the USA, where cyber-insurance is a considerably more mature market.

Under the GDPR, national data protection authorities will have powers to impose fines of up to £20 million, or 4% of annual global turnover, on companies who breach their data protection obligations. However, the extent to which these fines may be covered under a cyber-policy is uncertain under English law.

> Cyber-insurance provides protection against a range of risks that may not be covered by traditional insurances
>
> Ffion Flockhart

As a matter of public policy, there is a general reluctance to allow companies to pass on liability for unlawful acts to insurers, and so the insurability of a fine will therefore depend on the nature of the business' conduct. English law suggests that any deliberate or reckless behavior is not insurable. The parties to a cyber-policy therefore need to be aware that the position on insurability of fines is not clear-cut, and the insured will need to carefully consider its potential exposure under the GDPR and put in place strategies to mitigate potential loss.

Cyber-insurance provides protection against a range of risks that may not be covered by traditional insurances, and is an increasingly attractive option for many businesses as they consider how to manage and mitigate the exposure they face.

As indicated above, the risk landscape faced by businesses is constantly changing as a result of ever-evolving cyber threats and a developing legal and regulatory environment. It is therefore increasingly important that businesses scope out the risks they face and consider whether to obtain cyber-insurance appropriate to their specific needs and exposure.

Malware *Swiftly* Goes Upscale

Commercial banking payments systems are under attack from malware, as hackers graduate from stealing millions from consumer-facing targets to even bigger game: siphoning tens of millions through the global financial messaging network used by banks around the world. **Karen Epper Hoffman** asks if such attacks will become more pervasive, and what are banks and payments networks doing to stop it?

Like anyone perfecting their craft, cyber-criminals are honing their skills and aiming upward, using malware to steal money not only from retail payments systems, but also from the global commercial payments systems used to transfer billions among banks every day.

In the months since the headline-grabbing story of a malware attack through the Bangladesh central bank in February, which reportedly netted crooks USD$81 million, at least two other major cyber heists at central banks in Vietnam and Ecuador have prompted questions and concerns about the security inherent in the payments systems of these international banks, and the over-arching banking messaging network that connects them.

That network, Brussels-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), a cooperative owned by about 3000 global financial institutions, is at the heart of these concerns – even though the network was likely not the point of entry for the cyber-thieves in most cases.

"As far as I can tell, the SWIFT core system itself was not compromised, mainly the access to it by its member banks," says Neira Jones, a former head of payment security at Barclaycard, and currently a consultant and partner in the Global Cyber Alliance. "Essentially, transfer messages were taken at face value and enabled criminals to syphon large sums of money."

Indeed, in the case of the Bangladesh central bank, digital forensic experts investigating the incident found that the online crooks had used fraudulent SWIFT messages and installed malware inside the Dhaka headquarters of that bank, which hid and delayed discovery of their theft of USD$81 million from a central bank account held at the Federal Reserve Bank of New York. Similar cyber-attacks were discovered and reported later in the spring at Vietnam's Tien Phong Bank and Ecuador's Banco del Austro, from which thieves stole at least USD$12 million.

Mark Weatherford, former undersecretary for cybersecurity at the U.S. Department of Homeland Security and currently chief cybersecurity strategist for data center security vendor vArmour, points out that these attacks are not really using any new techniques or even targeting new victims, just new vectors. "While SWIFT was the attack vector, the primary security weakness is at the local bank level," Weatherford continues. "Many organizations are still missing the mark when it comes to developing a culture of security that is ingrained across that organization."

After the attacks, SWIFT issued a letter that seemed to convey this sense of increasing threat, while making it clear that it is the duty of their bank-partners to shore up their security.

"SWIFT has recently shared information regarding a number of fraudulent payment cases where affected customers suffered a breach in their local payment infrastructure," the letter to bank-customers read. "We would like to reassure you again that SWIFT's network, services and software were not compromised. While customers are responsible for the security of their own environment, security is our top priority and as an industry-owned cooperative we are committed to helping our customers fight against cyber-attacks."

Steve Durbin, managing director for the Information Security Forum, says that "technical capabilities and reach of cyber-

> Human nature is very stubborn, so until something happens to you, it's easy to think that it only happens to 'the other guy'
>
> Mark Weatherford

criminals now equals those of many governments and organizations. In the next few years, these capabilities will extend far beyond those of their victims." As a result, he says the ability of current control mechanisms to protect organizations, even central banks, is likely to diminish, exposing them to greater impact.

Criminals will follow the money, and while attacking a major central bank or its payment network might not be the easiest target, it stands to be the most lucrative or the most damaging. Arbor Networks' most recent Worldwide Infrastructure Security Report found that in the last year, the financial services sector moved from the fifth most attacked industry sector to second, according to Richard Brown, director EMEA channels and alliances at Arbor Networks. "There is no doubt that the banking sector is a lucrative target for cyber-criminals, so we can expect to see a continued rise in attacks against the sector…whether attackers go directly for the money held in the bank, the personal details of those using it, or simply look to disrupt their operations, it is a very real threat," Brown says.

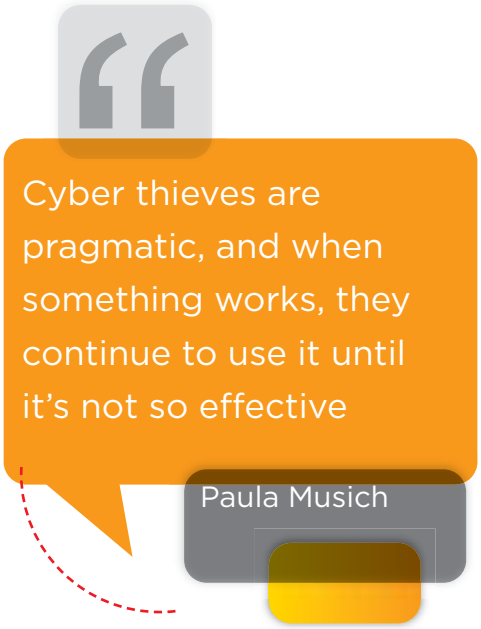
With the plethora of high-profile cyber-attacks and ongoing hacktivism targeting banks, cybersecurity has "never been more of a priority for financial services organizations," according to Paul McEvatt, senior cyber threat intelligence manager in the United Kingdom and Ireland for Fujitsu. "With reports of customized malware used in the SWIFT attacks aligning to the environment it executed in, it's difficult to imagine a traditional anti-virus system detecting these attacks, and it is also safe to assume there was an element of insider knowledge or an actor being inside of the network for a significant amount of time."

The organized crime rings operating around the globe that perpetrate these crimes are not just your run-of-the-mill hobbyist hackers, experts say. Instead, they are employing a host of various exploits in concert – social engineering, phishing, malware, ransomware, brute force attacks – to achieve their desired goals.

"Malware attacks such as those used in the Bangladesh Bank heist illustrate some sophisticated choreography by criminals

who exploited bank employees that didn't instill a cyber-aware culture," says Yong-Gon Chon, CEO of Cyber Risk Management. "It also illustrates a predictable messaging system process that was cleverly timed and exploited. Malware was only part of the recipe, which cloaked the discovery of the bogus transactions."

As Paula Musich, research director for NSS Labs, puts it: "Cyber thieves are pragmatic, and when something works, they continue to use it until it's not so effective."



Effective Response?

In the interest of trying to mitigate the risk and impact of such attacks, SWIFT and its bank-members are making an effort to mount a better defense. In May 2016, SWIFT CEO Gottfried Leibbrandt outlined a plan to improve information-sharing in the global financial community, harden security requirements and enhance security audit frameworks for customers, support payment pattern controls to locate suspicious activity, and introduce certification requirements for third parties (which are increasingly being used as a way into bank and payments networks).

Specifically, the international financial network has announced it will broaden its use of two-factor authentication when banks move funds, and require more information from, and communicate information about incidents to, its customers. SWIFT also established a centralized hub, accessible only to its banks, to share information about malware and security issues. While SWIFT caught flack for not instituting more vigorous security requirements sooner, industry insiders see their recent announcements as a positive first step.

Durbin believes these proposals are "absolutely spot on and long overdue." The ISF had previously highlighted that third parties were becoming a key route for cyber-criminals and have long been proponents of better information sharing, he says.

Geoff White, business group leader at Lloyd's Barbican Insurance Group underwriters, says that SWIFT's recent decision to demand minimum standards of security shows the importance of "maintaining cybersecurity standards throughout your supply chain." He believes this is a useful precursor to the upcoming General Data Protection Regulation which will mandate businesses to adhere to strict data protection compliance standards or face fines of up to 4% of global revenue.

Weatherford also believes SWIFT laid out a good, if overdue plan, which he believes will be effective "because it will require companies to invest in security products and services and also, perhaps most importantly, it will require banks to raise their overall security IQ." From a timing perspective, Weatherford says these security enhancements should get immediate traction but longer term, "they will probably require development of audit standards and certifications."

In a speech in Beijing in late May, Andrea Enria, chairman of the European Banking Authority, which coordinates banking rules across the European Union, called on regulators to stress-test local banks in their own countries to better understand potential risks. Around the same time, the Bank of England, as well as central banks in Singapore and the Philippines, announced that they would ask their banks to improve security systems and protocols. Similarly, Mary Jo White, chair of the U.S. Securities and Exchange Commission, is just one of the U.S. regulators who has publicly pointed to cybersecurity as the biggest risk facing the financial system. In May, the Hong Kong Monetary Authority launched a program, the Cybersecurity Fortification Initiative, to help its lenders protect critical technology systems.

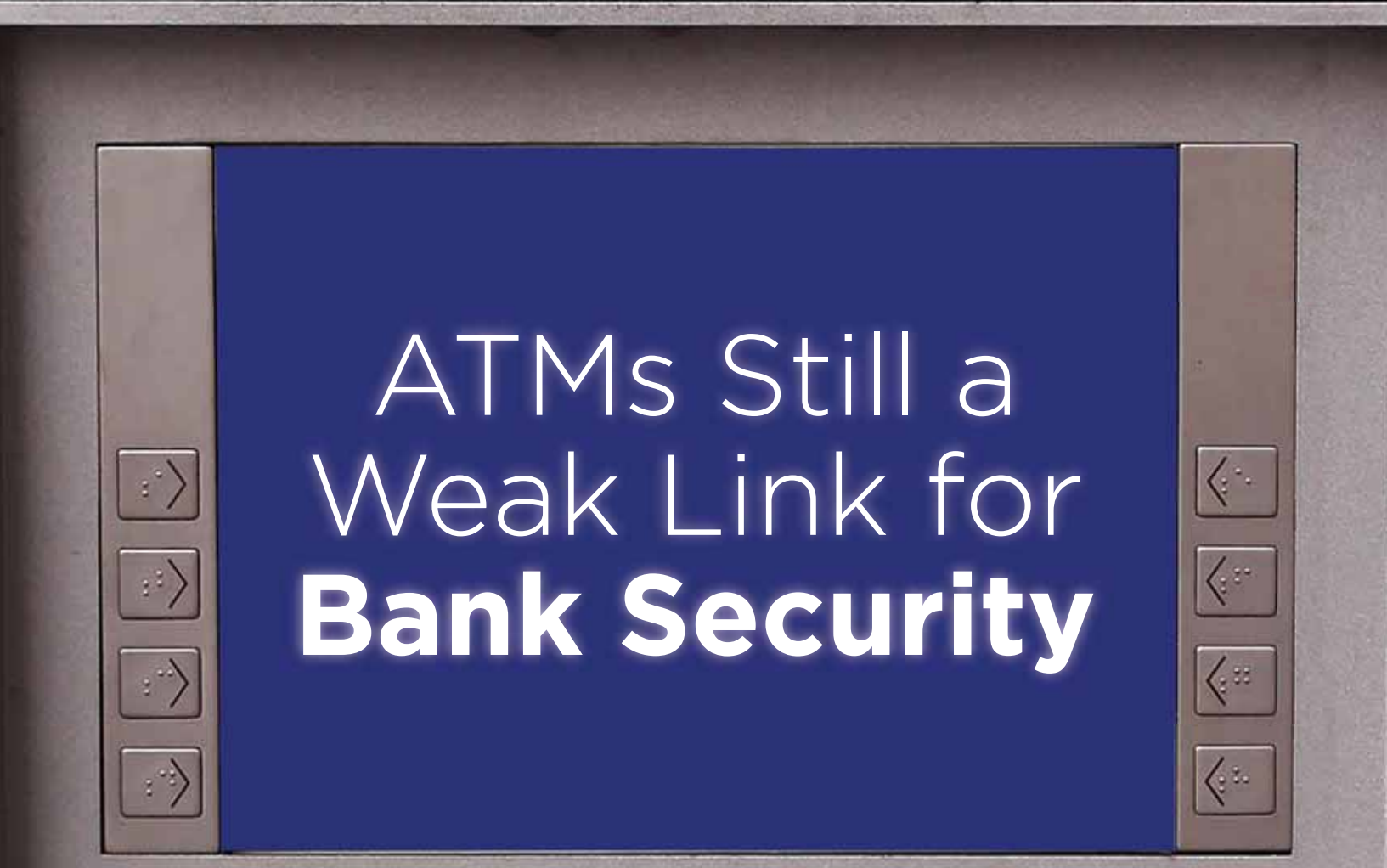
Stephen Migliore, senior director of cybersecurity for the Global Financial Services unit at Unisys, believes that these cyber-attacks and the various global responses underscore the "fact that banks need to be responsible for their own security. In a system based on trust, the whole is only as strong as its weakest link."

While McEvatt believes the Bank of England's CBEST security framework "is a welcome measure and ensures strong guidance is complied with," he also thinks that CIOs and chief information security officers in the banking industry are facing an unenviable challenge: securing multi-channel environments while ensuring customer experience does not suffer.

To this end, Durbin recommends banks conduct strong reviews of third party access, refocus more security emphasis on mission-critical information assets and systems, as well as conducting audits of their own security systems and procedures. White also believes SWIFT, for its part, needs to increase its communication with its bank-customers, and through groups like the Financial Services Information Sharing and Analysis Center.

However, experts also agree that it will likely take more than better technology and even better protocols and policies to reduce the risk of such attacks. "While there is certainly a technology component and things like two-factor authentication, encryption, increased monitoring etc. are critical, increased security awareness across the board will have the biggest impact," says Weatherford.

"Human nature is very stubborn, so until something happens to you, it's easy to think that it only happens to 'the other guy.' As cyber-related attacks have become mainstream and increasingly common, companies are beginning to realize that maybe they are 'the other guy' and that they should be investing more and paying more attention."



ATMs Still a Weak Link for **Bank Security**

More than physical distraction and rogue software applications on the ATM itself, the securing of the hole in the wall has become a priority in banking security. **Robin Arnfield** looks at threats and developments

Despite security advances such as EMV, ATMs remain vulnerable to physical and software-based fraud attacks. As consumers generally aren't liable for ATM fraud, card issuers and ATM operators face potentially heavy fraud losses. Counter-measures include deploying anti-skimming technology, installing OS security updates, and "locking down" ATMs so they can't be controlled by hackers.

"ATMs have long been a source of profitable fraud, principally via skimming devices that grab card information to be used to create fraudulent cards for withdrawing cash or for point-of-sale purchases," says Bob Meara, senior analyst, Banking Group, at U.S.-based Celent. "Generally, non-bank ATMs are thought to be more likely targets because of the comparatively lighter security surrounding them, although bank-owned ATMs have routinely suffered losses due to skimming."

EMV

As part of the U.S. payment card industry's migration to EMV chip cards, MasterCard and Visa have respectively set October 2016 and October 2017 as EMV migration deadlines for U.S. ATM operators.

After these deadlines, if an EMV card is used fraudulently at a U.S. ATM that doesn't support EMV, the acquirer will be liable for the issuer's fraud losses. Non-EMV-compliant ATM deployers face being charged by their acquirer for fraud losses, or being disconnected from their acquirer's network if they don't migrate to EMV.

"EMV migration will theoretically lessen ATM fraud, but it will take some time for U.S. ATM deployers to accomplish the migration," says Meara. "In the interim, liability shift rules offer deployers a compelling incentive to make the change. Contactless ATM user authentication – involving the use of contactless cards or smartphone-based m-wallets – may be a better long-term solution, but will be slow in coming."

As of January 2016, 51% of the 120 U.S. ATM deployers participating in the 2016 ATM Channel EMV Readiness Survey from the ATM Industry Association (ATMIA), had already upgraded over half their fleets to be EMV-capable. However, the survey found that 44% of EMV-capable ATMs weren't accepting EMV transactions, primarily because that functionality had been turned off by the operator.

When Canada migrated to EMV in 2012, some ATMs were disconnected by their acquirers for failing to migrate to EMV. Ben Knieff, a senior analyst at U.S.-based Aite Group, says some ATMs could be disconnected in the U.S. for the same reason. "But U.S. ATM deployers make a lot of money from surcharges on withdrawals – $3 to $4.50 per

European ATM Crime Statistics – Summary

ATM Related Fraud Attacks	2011	2012	2013	2014	2015	% +/- 14/15
Total Reported Incidents	20,244	22,450	21,346	15,702	18,738	+19%
Total Reported Losses	€234m	€265m	€248m	€280m	€327m	+17%
ATM Related Physical Attacks	**2011**	**2012**	**2013**	**2014**	**2015**	**% +/- 14/15**
Total Reported Incidents	1818	1920	2102	1980	2657	+34%
Total Reported Losses	€28m	€19m	€23m	€27m	€49m	+81%

Source: EAST https://www.european-atm-security.eu

withdrawal – so there's an incentive to migrate to EMV," he says.

Skimming

In April 2016, U.S.-based fraud analytics software firm FICO said the U.S. had seen the highest ATM compromise rate ever recorded by its FICO Card Alert Service. The number of ATMs compromised by skimming devices in 2015 rose by 546% in the U.S. since 2014.

Criminal activity was highest at non-bank ATMs such as convenience store ATMs, where 10-times as many ATMs were compromised compared to 2014, FICO says. In 2015, non-bank ATMs accounted for 60% of all compromises, up from 39% in 2014.

"Criminals realize EMV's coming to the U.S. and want to skim while they can," says Knieff. "You can skim mag-stripe data off EMV cards, but it's extremely difficult, although technically feasible, to skim card data from EMV chips. Criminals can't skim from EMV chips on a scale that would be profitable."

According to Ed O'Brien, director of U.S.-based Mercator Advisory Group's Banking Channels service, U.S. issuers are absorbing large losses from their cards being skimmed. "Consumers don't pay for card fraud, except for a few hard-to-prove instances, e.g. you wrote your PIN on a post-it note, stuck to your debit card, which you left on your desk," says Knieff.

"Criminals have been using mag-stripe skimmers to read the mag-stripes on European EMV cards at EMV-compliant ATMs in Europe and make cloned cards for use at non-EMV-compliant ATMs in the U.S." Lachlan Gunn, executive director at European ATM Security Team (EAST), says. In order to allow European cardholders to use their cards in the U.S., European cards still have mag-stripes.

In April 2016, EAST said skimming losses relating to the usage of stolen European card data outside Europe had risen to the highest level since 2008.

"To combat skimming, FICO recommends increased physical security around ATMs, particularly around free-standing ATMs," TJ Horan, FICO's vice-president of fraud solutions, says. "We advocate using anti-skimming devices that can detect or inhibit the attachment of alien objects to card readers. These devices come in a variety of forms, but the best anti-skimming devices include functionality allowing the device to shut down the ATM and generate an alert or alarm if it detects tampering."

"ATM deployers have invested in anti-skimming technologies such as jitter (which uses a jitter motion when a card is inserted in an ATM, to distort the card's mag-stripe data so it can't be skimmed) or jamming (which creates random frequencies to scramble skimming devices)," says Knieff. "Many manufacturers are implementing multiple anti-skimming technologies in their devices so, if one tool doesn't catch the fraud, another will."

"ATM skimming appears to be slowing in countries that have fully implemented EMV chip cards and deployed enhanced security features such as active jamming and skimmer detection devices," says Douglas Russell, director of U.K.-based DFR Risk Management. "But it's still the most prolific ATM fraud type experienced globally. Sophisticated criminal enterprises have learnt to overcome many of the mainstream anti-skimming solutions by making their skimmers extremely thin – so-called 'insert skimming devices' – so they can be positioned inside the actual ATM card reader, avoiding active jamming and most detection technologies currently deployed. Eavesdropping, which involves connecting a recording device to the genuine ATM card reader, is also increasing as a popular way to compromise card data at ATMs fitted with anti-skimming solutions."

Mobile ATM Access

"There are two ways mobile phones can be used to reduce ATM fraud," John Gunn, vice-president Corporate Communications at U.S.-based VASCO Data Security, says. "One is with standard bank cards and one is cardless. For the first, a bank could send a one-time-password to the customer's registered smartphone via secure push methods for keying into the ATM when they use their card. The bank could choose to do this only under higher-risk circumstances – not for one of the customer's usual ATM locations, withdrawal amount, or time of day."

Banks can also let customers do cardless ATM transactions using smartphones, which removes the vulnerability of cards from ATMs, says Knieff.

"In a mobile ATM withdrawal, the customer enters all the transaction details into their m-banking app," says Gunn. "The bank then presents a QR code on the ATM screen that's read by the smartphone. If the device and the user match, the transaction goes through and the cash is dispensed. It's easy for hackers to clone mag-stripe cards, but very challenging to clone smartphones if the device ID is handled properly."

While U.S. banks are rolling out QR code-based mobile ATM access, other cardless ATM access options are one-time PINs sent by SMS, a method used by British banks, and NFC-based m-wallets. NFC readers attached to ATMs can also be used for contactless cards.

Although Bank of America said in May 2016 that its customers will be able to use digital wallets such as Android Pay for cardless ATM withdrawals, Knieff doesn't think most banks will want to let customers use third-party NFC-based m-wallets for cardless withdrawals.

"Potentially Apple Pay, Android Pay, etc. could be used for ATM withdrawals, but issuers want to retain control over ATM transactions," says Knieff. "I don't see issuers allowing these third-party wallets to be used for ATM withdrawals."

"Using bank-issued m-wallets for ATM withdrawals that are based on tokenization of card numbers and Host Card Emulation (HCE) is a counter-measure to criminals who try to capture card information at ATMs," says Joseph Walent, senior analyst, Emerging Technologies Advisory Service, at Mercator. "Even if a criminal captures a token, there's very little they can do with it."

Tokenization involves replacing card numbers in ATM and POS transactions with one-time numbers, with the actual card number being stored in a cloud-based HCE software vault run by an issuer or a third-party such as MasterCard or Visa.

"NFC-based mobile ATM access will migrate quite quickly to the UK, as NFC is far better accepted there than in the U.S.," says Knieff. "Most banks will look for multiple modalities of authentication, as some people don't have smartphones or aren't comfortable with QR codes."

Mercator's O'Brien says a gating factor for NFC-based ATM withdrawals is the need for smartphones to be NFC-compatible. "QR codes and one-time PINs represent an easier, interim solution for banks," he says. "They can roll out QR code-based solutions now and migrate to NFC-based ATM withdrawals once NFC becomes widely available on smartphones."

Biometrics

"ATMs supporting biometric authentication are finally gaining traction, driven by a need for enhanced security and as a means of improving financial inclusion," says DFR Risk Management's Russell.

"Japan has led the way with many, if not most, of its ATMs having fingerprint/finger-vein scanners or palm vein scanners. Elsewhere, voluntary consumer acceptance of biometrics is helped by the number of consumer electronic devices, particularly smartphones, that incorporate biometric capabilities, but biometric systems aren't inherently secure. Attacks can be successful in compromising biometric ATMs as well as other biometric implementations."

> Non-bank ATMs are thought to be more likely targets because of the comparatively lighter security surrounding them
>
> Bob Meara

Malware

Malware poses a major threat to ATMs. "The challenge with malware is that many ATMs – even in the U.S. – run old versions of Windows that aren't supported by Microsoft and aren't patched with the latest security updates," says Knieff.

Since April 2014, any ATMs still running Windows XP instead of Windows 7 no longer receive Microsoft security patches, making them vulnerable to malware and network intrusions and in breach of the Payment Card Industry Data Security Standard (PCI DSS) requirement for ATM operators to update their operating systems with security fixes against known vulnerabilities.

"PCI DSS requires ATMs to use patched Windows 10 or Windows 7 software," says Knieff. "But it takes time to update a bank's systems. For a large bank with tens of thousands of ATMs, it's a big project to get all those terminals updated, especially if the bank has ATMs from different vendors."

"Most of the malware attacks I've seen require some degree of physical access," Knieff says. "It's quite easy for criminals to plug in USB sticks to ATMs. The question is whether they can scale these physical attacks. If it takes half an hour to infect each ATM with malware and then you have to pay money mules to withdraw the cash, when does it stop being worth it, if you can't scale the attacks pretty significantly?"

Knieff says that, while there are network software vulnerabilities letting criminals into ATM networks remotely, this attack method is more complicated and requires a lot more skill. "Hackers need to get through a lot of technological gates to break into ATM networks remotely," he says. "This doesn't mean it can't happen, but some criminals have found it easier to go after the physical device, and they get enough of a payday that they're happy with."

Kaspersky Lab Research

"In some cases, attackers use malware such as Skimer to turn ATMs into card skimmers for further carding fraud," says Juan Guerrero, a senior security researcher at Kaspersky Lab. "In most cases, the attackers seek to get cash disbursements from the ATMs. Countermeasures include replacing the default locks and updating the software used to operate the ATMs, removing unnecessary overheads like remote administration software that may grant remote access to attackers, and employing robust anti-malware solutions."

According to Kaspersky, in 2014-2015 around 100 banks worldwide were affected by the Carbanak ATM malware attack, with losses per bank ranging from $2.5 million to $10 million.

"In Carbanak's case, ATMs were instructed to disburse cash at a predetermined time, raiding the contents of the ATM, with a money mule standing around waiting for the cash to come out with no interaction required," says Guerrero.

To guard against malware, ATM applications must run in a locked-down account with minimum privileges, ATM vendor NCR says. Also, ATM deployers should implement effective firewalls and anti-malware software.

However, ATM security is more than just best practice. ATM deployers and acquirers are required to comply with the Payment Card Industry Security Standards Council's standards such as PCI DSS. Penalties for PCI DSS non-compliance include fines as well as liability for fraud losses resulting from breaches.

Time for an Overhaul?
Awareness Training

Is the current cybersecurity awareness training system broken? If so, how can we fix it? **Robert Schifreen**, founder of Securitysmart.co.uk learns from industry expertise on what does and does not work

Back in June, a couple of hundred people packed into a conference hall at Infosecurity Europe 2016. The title of the session was 'Securing the Connected Human' and it was described in the show guide as being about security awareness training. Those who attended in the hope of getting some tips on how to do it, or some reassurance that what they're currently doing is right, probably walked away mightily disappointed.

Those on the panel clearly know what they're talking about. One was the awareness training program manager at Uber and another was a leading academic in the field. One was a well-known CISO, and yet a common message from the majority of the panel was that the current system is broken. So badly broken, in fact, that we need to stop doing any more training in security awareness while we all go away and start again from scratch.

You could almost hear the audience gasp. It's hard to say whether this was in surprise or grudging agreement.

The aim of the game is clear, though. "To date the security community has focused on using technology to secure technology, totally ignoring the human element", says Lance Spitzner, director of the SANS Securing The Human program. "As a result", he continues, "the human is the weakest link. Until we also start securing people, the bad guys will continue to win".

The science (or is it an art?) of educating someone to take security seriously is not easy. The typical IT kit on a modern employee's desk is massively overpowered and expecting them to protect it all from the bad guys is asking a lot. This is exacerbated by the fact that there is no single authoritative place they can go for help. Yes, there's Action Fraud (or non-action Fraud, as a senior security person described it to me recently), and there's Get Safe Online, and there's also the dedicated cyber section on every one of the 40-odd UK police force websites. There's every bank site too, and as one panelist said, "there's a lot of conflicting advice. Even worse, a lot of it is rubbish." I recently heard someone suggest that a password should be considered insecure if it results in more than three hits when you type it into Google!

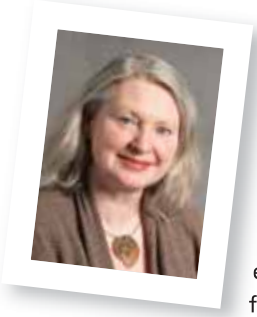
If there's a topic for which the moniker "death by PowerPoint" fits perfectly, security training must surely be it. We take people away from a task they're perfectly happy doing, and which they're keen to finish by the end of the day. We sit them in a room and bombard them with a list of 500 things not to do. Then we send them away and expect them to remember them all for the next six months. Not only do they not remember more than three of those 500 things, we as managers have no way to discover which three they do recall, or, more importantly, which 497 they forget.

> We are assuming that just because we train people, they will change behaviors
>
> Kai Roer

There are alternatives to classroom-based learning with online courses offered by many companies. In corporate land they're known as computer-based training (CBT). Educationalists are keen users of the Learning Management System (LMS) or Virtual Learning Environment (VLE). Think of them as an intranet that also hosts CBT courses. University students nowadays spend more time in their LMS or VLE than attending lectures, but while it's easy to get students to log into a separate system to undertake learning, pulling employees

away from the day job can be a distraction regardless of whether the destination is a website or the conference room.

So if the current training methods are broken, how can we mend them? One of the panelists was Professor Angela Sasse from the Institute in Science of Cyber Security at University College London. She says that the advice given must be actionable, i.e. that people can actually take it away and make use of it. Don't use a training session as an excuse to read out your corporate IT security policy. Instead, tell them about a real risk, explain the consequences, and teach them how to mitigate it. If it turns out that staff aren't following the advice you give them, find out why and adapt the training accordingly, and don't expect the complete program cycle to take less than two years.



While Professor Sasse says that we need to work with those who don't follow our advice, not everyone takes the same attitude. In March Sir Bernard Hogan-Howe, head of the Metropolitan Police, suggested that banks should stop compensating victims of online fraud because it merely rewards bad behavior. Support for the idea was, unsurprisingly, limited, but it did initiate a much-needed debate in the media about who is to blame when a company PC gets hit by ransomware or data theft.

Are we giving employees too much responsibility and too much access to data? Are we ignoring the Need to Know rule? "Too often we see businesses giving social media responsibility to the youngest member of the team, with no experience of marketing, based on the fact that they use social media in their personal life" says James Dempster, managing director of Brighton-based Cobb Digital.

We need to be careful not to throw the baby out with the bath water. While there may be problems with the current methods of security awareness training, describing it as completely broken is unfair. It does work, but clearly we as an industry must do better. We need to be able to measure the success of whatever program we deploy, and we need to train people more often than once or twice a year, and we need to understand what we mean by training.

> Don't use a training session as an excuse to read out your corporate IT security policy
>
> Angela Sasse

"We are assuming that just because we train people, they will change behaviors", says Kai Roer, founder and CEO of CLTRE. "What we need is not a new approach to training employees, what we need is a way to measure that change in behaviors."

Start again from scratch? Not necessarily, but clearly a rethink of security awareness training is called for.

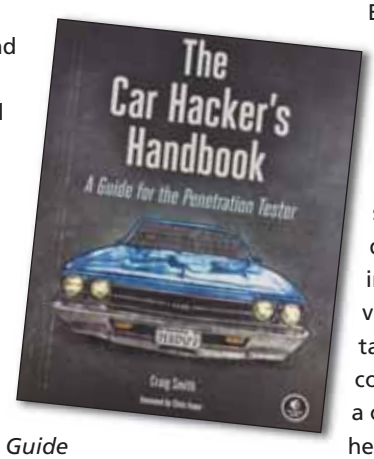
Book Review: The Car Hackers Handbook

Reviewed by
Jay Schulman,
principal, security and
privacy at RSM US LLP

Title:	*The Car Hackers Handbook*
Author:	Craig Smith, CEO of Theia Labs
Pages:	304
Publisher:	No Starch Press
Price:	$49.95

The Internet of Things (IoT) is getting noticed within the security community as an area which needs much improvement. Overall, though, IoT devices are just mini versions of desktops and servers. They run Linux or Windows variants and connect via Bluetooth, Wi-Fi and Ethernet. There is one exception: cars.

Automobiles are built using mostly proprietary protocols, technologies and interfaces. Just look down under your steering wheel and you'll find an ODB-II port. It's a 16 pin connector to interface with your car.



After spending the past year trying to figure out how to interact with my vehicle, I picked up Craig Smith's new book *The Car Hacker's Handbook. A Guide for Penetration Testers*.

This is the type of book you read while sitting next to your Linux workstation. In fact, I read at least half of it sitting in my car with my laptop in one hand and the book in the other. Most of the tools and examples are for Linux systems. (Note: I'm sure everything will run just fine on OSX but it was much faster to get running in Linux).

As you get more advanced, you can move beyond just an ODB-II connection into additional hardware such as a JTAGulator. Luckily, there is something in everyone's price range.

The first 60 pages of the book is less about hacking and more teaching the basics of in-car communications. The author does a great job of giving you the right amount of background so you can properly test a car.

Even if you're not interested in hacking your vehicle, it's a good foundation in understanding the basics of how a car's network operates.

After the basics, each section of the book tackles a different part of the car. This includes attacking the in-vehicle infotainment system, tapping the Bluetooth connection and how to hotwire a car. The appendix is also really helpful as it walks through the "Tools of the Trade" – all of the software and hardware described in the book.

One of the biggest challenges in car hacking is avoiding messing up your primary mode of transportation. The book helps you explore and potentially modify your car. The author walks through some of the potential issues that can arise such as your vehicle not turning off anymore (it's apparently rare). There is a section on ICSim – the Linux instrument cluster simulator – a great way to start understanding a car's network by using a virtual simulator.

As a tester, the book covers a number of different entry points to the car including using a software defined radio to attack the door locking system. Whether you're interested in reverse engineering, changing the performance of your car, or just understanding how vehicles work, there is something for everyone.

My main issue with the book was that I already was playing with my car so, at first read, I struggled to stay and finish one chapter. Once I got up to speed on the basics in one area, I wanted to jump to a more advanced topic in that area. I understand car hacking by the tools I use, not the concepts. This book is written based upon concepts.

I have come to recognize this book is more a battlefield manual that you'll jump around constantly than a book you read cover-to-cover. As much as the author talks about this book as a guide for penetration testers, it reads more like a guide for hackers, specifically the hobbyist hacker who wants to play with their car.

However, if you have your own car and are interested in understanding the ins and outs of its networking and security, this is the reference book to use.

info security
STRATEGY | INSIGHT | TECHNOLOGY

INFOSECURITY AUTUMN VIRTUAL CONFERENCE

27TH - 28TH SEPTEMBER 2016

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

THE INFOSECURITY AUTUMN 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 CALIBER 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.COM/VIRTUAL-CONFERENCES

Machine Learning – Keeping Us One Step Ahead of Fraudsters

Jackie Barwell director of fraud product management at ACI Worldwide, looks at the trend of machine learning, asking how effective it is in detecting and preventing fraud

The topic of machine learning in the fraud prevention space is one which is constantly on the lips of both financial institutions and merchants looking to exploit advances in IT infrastructure and intelligent computing to protect their businesses from possible danger. However, we may find ourselves asking what really is machine learning? Is it actually that effective in not only detecting fraud, but preventing it too?

To explain the first question: machine learning relies on algorithms which employ pattern recognition techniques to explore and learn the underlying structures in the data. By using past transaction data from fraudulent activity, alongside information from genuine customer transactions, these algorithms can be used to build predictive models which can forecast the probability of a transaction being fraudulent.

Predictive models deliver very tangible results in fraud detection. Their ability to extract meaning from complicated data means that they can be used to identify patterns and highlight trends which are too complex to be noticed either by humans or through other automated techniques. By running specific, effective algorithms and using them to make automated decisions, or generate alerts for suspicious activity, these techniques can save manual review time, reduce the number of false positives and quickly stop attempted fraud.

However, this approach is by no means new. In fact, predictive models first became popular almost two decades ago, particularly with financial institutions which successfully used models to detect significant volumes of card-present fraudulent transactions and save millions.

Back then, however, fraud problems were simpler and patterns were easier to identify. Fraudsters have since become savvier and more innovative, driving demand for further change in fraud detection techniques to ensure that defensive capabilities can match fraudsters' offensive capabilities.

Technology advances over the last decade in particular have aided the evolution of machine learning and ensured it has remained an effective fraud prevention measure. For instance, the increased availability and scale of raw computing power means that we can now process, segment and analyze data on a much larger and more complex scale. This allows fraud analysts to understand both localized and widespread occurrences of fraud. It also enables these complex processes to be accomplished faster, frequently in real-time.

Additionally, other information, such as data resulting from web-behavior analysis, can be fed into the predictive models, creating a new and valuable dimension to the model's accuracy.

The development of new algorithms, machine learning techniques and programming expertise have also all kept pace with changes in the payments and ecommerce landscape, with these latest techniques giving businesses the power to explore a much larger search area in the model optimization space and increase detection rates.

While it is clear that machine learning has a lot to offer to financial institutions and merchants in an effort to detect and prevent fraud, the approach does have its limitations.

As they learn from experience, predictive models cannot learn or spot monolithic events such as data breaches. For these you need to be running a rules-based model which uses negative lists and, preferably, consortium data.

Predictive models are also less adaptive at learning one-off events or transient phenomena. Our experience with customers around the world has taught us that combining predictive models with a customized rules engine delivers the optimal fraud prevention solution. The ability and flexibility of a comprehensive rules engine to deal with seasonal changes, emerging trends and one-time events complements the sophisticated pattern recognition techniques deployed by predictive models.

In the future it seems that machine learning and predictive models will be an integral and vital part of a winning fraud strategy. Backed by these predictive models, rules-based systems are constantly updated to augment performance and provide multifaceted coverage and protection. It is this holistic approach to fraud prevention that provides effective protection against the risk of fraud.

The Best View

If analysis technology is the next trend, how is it being deployed? **Dan Raywood**, talks to Gigamon's Marshall Wolfe about his deployment and what he feels he gets from it

If user behavior analytics, machine learning and even artificial intelligence are the direction that security is taking, how are they actually being deployed and used?

Brian Kelly is chief security officer of Rackspace. He told *Infosecurity* that he did not believe that a new wave of technology was imminent. "The Holy Grail used to be full packet capture, now we say 'why,' as can we derive the same value with metadata and collecting everything, and we need data scientists to resolve this," he said.

Kelly claimed that old technology is often flawed and there are elements of future state architecture being driven by cloud, and as users migrate from a client server and the "hierarchical driven model that we have today," and move towards a more distributed principle where the controls are removed from the network and we put controls outside the stack and outside the operating system and closer to the workload, there will be better controls and better contextual awareness where they can talk to each other.

"So think of future state, I think that is where we are now but I think to manage that kind of environment we have to solve some of the analytics issues as we are dealing with a lot more data in real time or near real time," he said. "So we have got to be a lot more sophisticated with our behavioral analytics and all of our data models to allow the distributed model to work quickly and effectively."

I also spoke with Marshall Wolfe, senior IT officer for the networking company Gigamon. Joining the company in October 2014, he adopted a strategy to have best-in-class preventative security, augmented with the ability to detect an attacker as quickly as possible.

By establishing ongoing profiles of all users and network devices, Gigamon has a "known good" model for network and endpoint activity. From this, they can find anomalies that are indicative of an attack.

"Gigamon taps every ingress and egress point across the world and brings data to a central spot in our headquarters," he said. "We get the speed and reaction we need to control security."

He explained that this area of technology is moving pretty fast as "there is a new company coming up every five minutes it seems," and analysis of these companies led him to opt for LightCyber technology. "Others were bothersome in terms of sending data to another site, and others were operationally difficult or we could not get customer support, and with LightCyber we get huge support as a customer. They have got a great team of people and for me this is the big differentiator, and not just keeping up with technology," he said.

Wolfe's team is relatively small and doesn't permit him to spend a lot of time and labor on analysis, and he said that what he needed was "a tool like LightCyber that slaps you across the face with what is potentially wrong and what you need to act on now."

He said: "On a daily basis, all we can attack is what LightCyber refers to as confirmed threats, and remediate immediately and as we go through we have time to figure out what is needed and accepted, as unverified pieces are coming up as suspicious and we don't have time to look at those in a small team."

"We all receive all of the alerts constantly, and that is what we determine upon and triage to do. If there are attacks going on, this shows us everything and we can determine what to work on with lists of things remediated."

I asked him if the deep-dive technologies were more usable, and Wolfe said that if he had a choice he would not bother with endpoints as they cause more problems than they solve, as today's consumer systems use Mac and Linux, and the different platforms are hard to work with.

"The world has got to turn towards behavioral analytics, profiling and trying to separate profiling from the network, endpoint and user; they are the same in conjunction from user to network and destination, and to see it graphically and figure out what is new and what cannot be explained and the ability to dig down is fantastic," he added.

The Future of Regulation in the Digital World

As innovation is made, privacy and security needs to keep pace. **Derek Cummings**, director at global consulting firm Protiviti, looks at historical examples and future cases

Technology adoption and digital innovation has revolutionized the current commercial environment – from driverless cars and drones delivering goods to digital payments, innovation is pushing ahead at a significantly faster pace than regulation.

Regulators in the financial services industry have indicated that they do not wish to stifle innovation from financial technology (fintech) companies, but equally they acknowledge that new risks are created with new products and systems. The big question supervisors and lawmakers need to address is whether more regulation is required, or if current regulation is sufficient to respond to new digital business models and when should it be applied in an ever-changing and expanding marketplace.

Historically, in the financial services sector, regulators have stepped in only after a watershed moment has occurred to prevent a repeat of specific events. Regulation needs to be more future-looking in this rapidly-changing environment but it also needs to strike a careful balance between "stifling innovation" too early in the process and using regulation to ensure that risks are being managed that will enable the industry to flourish.

Regulators need to balance protecting consumers with enabling effective and efficient markets to operate for the benefit of those same consumers and the broader economy. Over-regulated markets stifle competition and create barriers to entry. New entrants may not be willing to launch their innovative and disruptive ideas if there is little profit to be made.

The alternative though is an unregulated market where the harm to individual consumers can significantly outweigh the benefits gained from innovation, or where the lack of regulation creates a barrier in itself due to issues associated with the establishment of trust between counterparties.

Consider the driverless car industry as an example. Applying too much regulation at the early stages of its development could result in increased costs that make it prohibitive for new market entrants to pilot their ideas and bring solutions to market quickly.

However, with inappropriate controls and safety measures in place, the industry as a whole may suffer a lack of confidence if serious safety concerns are not addressed early in the product lifecycle. Rather than introduce new regulation specifically targeted at driverless cars, the car industry's well-established safety measures, regulatory guidelines and standards on road safety could be adapted and updated to consider risks associated with the new digital technologies coming to market.

In the financial services sector, the peer-to-peer lending market in the UK is another great example of an innovative and disruptive business idea that has grown rapidly by achieving an appropriate balance between protecting individual consumers, and helping them to better understand the risks associated with their engagement with the market. While regulation was very light touch to start, this industry was rapidly put back into control as it grew through new entrants and consumer demand.

In the UK, consumers are highly protected already but regulations do need to evolve with shifts in the market. One case in point being the emergence of the payday lending industry several years ago, which was followed by changes in regulation forcing

firms to better assess affordability and to curb some of the more extreme excesses associated with this business model. This has now led to significant adjustments to how short-term credit is provided and the demise of a number of firms operating in this space.

There have been other failures, such as the PPI scandal in the UK. Although digitization and innovation cannot be blamed for this specific case, it does highlight that many products in the financial and digital world are now virtual as opposed to physical.

Another key area for consideration is the thorny subject of data privacy and data protection. Often consumers are giving away significant personal data to third parties where they have a tenuous relationship in exchange for mobile entertainment (free mobile apps), digital services or as a result of purchasing goods via digital channels. This data enables the consumer to be located in the physical world and to be targeted for follow on promotional activity as well as potentially becoming available to others for more nefarious uses.

Data such as postal address, email address, date of birth, payment card details, internet behavioral patterns etc. are all extremely valuable, and consumers are right to be concerned about how their data is used beyond the original transaction. Regulations already exist in relation to data privacy and data protection and work is ongoing to strengthen existing provisions – most notably in relation to European regulations and the General Data Protection Regulation (GDPR).

The global payments cards industry has established a clear set of data security standards (PCI DSS) for payment details, which are enforced through commercial penalties and contractual liabilities. These have been in place for around 10 years with compliance actively monitored through annual assessments undertaken by qualified assessors. Most other regulations do not come with this level of active monitoring.

Global application of this regulation, which emerged directly from the industry itself as opposed to direct government intervention, also represents an interesting case study in how the interests of both consumers and industry participants can be addressed when reduction of losses through fraud prevention acts as a focal point.

Companies producing digital products and offering digital services will need to be held more accountable for failures

Despite the fact that many financial services companies feel that they are subject to much higher levels of external scrutiny, this isn't necessarily reflected in the effectiveness of the internal controls they have established. Few organizations are likely to be able to state with a high degree of confidence that they meet all of the obligations of the current data protection rules.

Lack of a requirement for independent assessment in this area by regulators is undoubtedly a factor here, as is the level of penalties associated with breaches. The benchmark is about to be raised much higher however in relation to GDPR and the penalties that could be applied will be much more significant. Organizations will therefore need to focus on this or suffer the consequences in terms of penalties impacting their bottom line. Those organizations embarking on digital transformation programs need to ensure that they have factored in data privacy considerations at an early stage or they may find data privacy becomes a significant disruptor to their business model.

The level of consumer protection supplied by regulation varies massively across industries. Those that have operated in the digital world for some time have evolved mechanisms to establish trust between counterparties through effective identification of individuals and registration of businesses operating in the market. Many that have not are operating like the Wild West, where anything goes and *caveat emptor* needs to be scrawled in red paint wherever contracts are implied and payments are exchanged.

Consumers need to be able to better recognize the risks they are facing while governments gear up and step in to address the most significant emerging risks where self-regulation proves to be ineffective.

Many of the risks identified above are not new. These risks exist in the physical world to a greater or lesser extent. There is a danger of overreaction and a rush to implement poorly thought through laws and regulations.

Consumers, manufacturers and service providers do need to be better educated however about the risks of cross border transactions and impacts on consumer safety. They need to assess whether existing laws and regulations are required to be modified to reflect a changing world so that existing rules can be extended into the digital world and be enforced across national boundaries in similar ways to international extradition agreements. This will take some time to emerge and become established in the same way that anti-money laundering regulations have taken some time to promulgate around the globe.

As the digital revolution continues to evolve, companies producing digital products and offering digital services will need to be held more accountable for failures that occur in the products and services provided to consumers. This is of particular importance if those products impact the safety and general rights of consumers, such as the developers of software on driverless cars.

While regulations exist in different industries to protect consumers in many situations, further consideration will be required to reflect the new risks to consumers in the digital world and be updated accordingly. This is not a revolutionary change but it is evolutionary and will require attention from lawmakers and regulators.

Wolf in Sheep's Clothing: Combating the Insider Threat

What can you do to defend against the unknown quantity that is the insider threat? **Adam F. Godfrey**, CISSP looks at some solutions and if your ally is actually your enemy in disguise

Amidst droves of sophisticated malware and external threats that target our sensitive data, the most prevalent and destructive security threat we face today lurks silently within the confines of our organizational boundaries. While vendors dazzle us with the latest threat and vulnerability detection technology on the market, our own employees are positioned to sidestep these advanced solutions with ease and raise the gate on our protected information assets.

The insider threat not only consists of those who engage in intentionally-malicious behavior which compromises information security, but also those who remain completely unaware of any wrongdoing, due to lack of education pertaining to safe information handling practices.

In a 2015 study commissioned by CompTIA, it was revealed that out of a survey pool of approximately 1,200 full-time US employees regarding their technology use and cybersecurity awareness habits, a staggering 45% of employees received no cybersecurity training from their employers.

Additionally, the survey went on to reveal that 63% of employees use work-issued mobile devices for personal activities, and 94% of employees connect their work-issued devices to unsecured public Wi-Fi networks. These figures reflect a frightening reality that corporate America has yet to not only take cybersecurity as seriously as it should, but also realize the ever-present insider threat it continues to foster through lack of cybersecurity awareness education.

Corporate and economic espionage is a booming business across the world, and lack of user cybersecurity awareness training grooms easy targets for attackers seeking access to proprietary information via social engineering, malware infection, recruitment of internal employees and even personal insertion into the corporate construct for direct access to targeted information.

In a 2011 report, The Office of the National Counterintelligence Executive estimated that financial losses to foreign competitors resulting from theft of trade secrets ranges from tens to hundreds of billions of dollars annually. In a recent FBI survey, it was discovered that roughly half of the 165 participating companies claimed to have fallen victim to economic espionage or theft of trade secrets. It was also revealed that 95% of those attempts originated from parties associated with the Chinese government.

There are a number of preventative measures that all organizations must take into consideration and, where possible, implement to mitigate the insider threat. To begin, a comprehensive cybersecurity awareness program must be established to educate all inbound personnel, as well as facilitate continuing awareness of existing personnel via annual refresher training. Regular training encourages users to remain

vigilant against new and previously-known threats via employment of information handling best practices, including education pertaining to various methods of social networking attacks. Such attacks include vishing, phishing and whaling, all consisting of attempts to bait users and executive leadership into divulging sensitive information, whether by phone, email, social media or other means.

Far from Hollywood portrayals of corporate espionage one may envision, these antiquated and downright basic measures are weapons-of-choice for establishment of advanced persistent threats (APT) that reside on corporate information systems for years on end, exfiltrating priceless trade secrets via a "low and slow" approach to avoid detection. It's in this very manner that, in 2009, a senior Coca-Cola executive facilitated an attacker's establishment of remote access to the corporate network by clicking on a link contained within a seemingly-harmless email, through which the attacker set up shop and covertly exported countless confidential files over an extended period of time.

Additional training elements should include responsible use of social media, maintaining confidentiality of user credentials, acceptable use of email, fostering workplace awareness through identification and reporting of suspicious behavior, etc. Any cybersecurity awareness program must also be backed by organizational policy to detail not only acceptable use practices, but also punitive measures resulting from policy violation.

A policy without teeth to back it up is an ineffective one. Knowledge of punitive action resulting from non-compliance is crucial to ensuring users remain vigilant in adherence to safe information handling practices.

Where possible, enforce job rotation to rotate personnel across positions and avoid long-term stagnation of an employee under any given role or responsibility. Job rotation interrupts collusion between two or more employees working together to execute organized attacks against an organization, and may also be utilized as a detection mechanism to identify suspected insider threat activity. Mandatory vacations are also an effective implementation to support such efforts. Removal of an employee from the workplace for an extended period of time can reveal changes in information handling activity that validates suspicions of foul play.

Enforcing separation of duties ensures employees are restricted to access only those areas required to carry out their professional duties. Excessive and unnecessary employee access to sensitive physical and virtual locations is a primary method of data exfiltration and one often overlooked by many organizations.

Prevention of data exfiltration, or loss via establishment of a comprehensive data loss prevention (DLP) strategy is crucial to controlling means of information loss, whether intentional or unintentional. To support such a strategy, DLP software implementation can be leveraged to detect and prevent external information transfer, as well as connectivity of unauthorized mass storage devices to corporate assets via notification of administrative personnel upon attempts to do so.

Data-at-rest (DAR) encryption, which works to encrypt data while not in motion, such as that stored on a hard drive, may be employed as part of your DLP strategy to ensure information contained on a compromised physical device does not risk exposure to unauthorized parties. Remote connections into the corporate network should also utilize virtual private network (VPN) connectivity to encrypt and secure the integrity of sensitive, work-related data transmissions.

These measures are far from exhaustive and are merely considered sub-components of a complete cybersecurity program, but serve to provide business owners some recommended cybersecurity best practices to safeguard their information assets from the insider threat.

Behind the façade of technical complexities that rule our enterprises with beautiful precision wages a war that devours our sensitive data from the inside out, necessitating a defensive stance that begins with getting up front and personal with our employees about their positions on the cyber battlefield.

Can Ransomware Ever be Defeated?

...Point...

Reaching an Acceptable Level of Ransomware

As much as I would like to say that one day we will eliminate ransomware, I'm afraid it's not true. In security we can never truly eliminate anything, but there is a level we can accept and manage. It's a similar concept for when we buy cars – we accept that traffic accidents still happen, and we have laws against crime but it doesn't mean it never happens – we just accept that it still happens. An acceptable level for an organization is when we can still operate whilst under threat, where it's not too costly to keep doing business.

Ransomware is very different to typical malware and, as a phenomenon, is just getting started, so detection methods are not yet as good as they need to be. However, as we get more familiar with the latest forms of ransomware – how it operates, how it works – we are getting better at detecting it. It's easy for us to get better at ransomware detection because very few people were good at it to begin with.

We can never eliminate hacks and threats; we can never eliminate SQL injections. What we can do with ransomware is take the appropriate steps. Traditional methods and standard anti-virus solutions are no longer sufficient to deal with the fast-evolving ransomware landscape, and experts agree that fighting it requires a new approach – one that is based on behavior analysis rather than signature comparison.

While there are many hands looking at the ransomware problem including researchers, academics, vendors, and so forth, there is definitely no slow-down in infection rates. So far, no one really has found the answer that the market has accepted. If the FBI's numbers are correct, we're probably looking at a billion plus in ransom payouts by the end of the year, or easily over 2017.

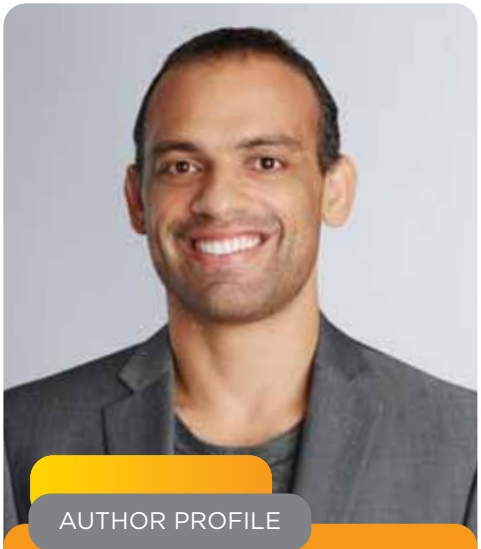
So, the guidance I'd give is to set aside incident response dollars, like everyone should be doing anyway, for any such circumstance — not just ransomware. Then they should strongly consider purchasing some cyber-insurance to help cover the losses of ransom and clean-up.

Ransomware may have many variants, but they all share a set of common traits which can be detected during execution. With newer security tools, processes are scrutinized based on their behavior and blocked if they are found to be undertaking malicious activities.

The best thing an organization can do to protect against a ransomware attack – aside from having appropriate security products and controls in place – is to have regular backup processes in place, either on another machine or, preferably, somewhere offsite. If you're then unfortunate enough to be the victim of an attack, you can either recover your data or roll back to an earlier version of it. Having a good backup system is the best thing anybody can do.

We can, most definitely, effectively manage ransomware by making ourselves difficult to infect. The challenge is, most companies don't have a good system configuration, they don't have good endpoint protection and backups are few and far between, especially when it comes to endpoints and desktop PCs. That's why ransomware is so effective; few organizations have adequate controls in place.

Ransomware is here to stay, but, with good endpoint protection, regular patch updates and an effective backup system, any organization can take measures to protect itself against infection and have the recovery processes in place should it be necessary. If we can effectively manage our organizations, we can manage ransomware.



AUTHOR PROFILE

Jeremiah Grossman, Chief of Security Strategy, SentinelOne

Founder of application security company, WhiteHat Security, and now Chief of Security Strategy at SentinelOne, Jeremiah's career spans nearly 20 years and he has lived a literal lifetime in computer security to become one of the industry's biggest names. He has received a number of industry awards and been publicly thanked by Microsoft, Mozilla, Google, Facebook, and many others for his security research. Jeremiah has also written hundreds of articles and white papers. As an industry veteran, he has been featured in hundreds of media outlets around the world. Jeremiah has been a guest speaker on six continents at hundreds of events including many top universities.

.....Counterpoint....

Take an Intelligence-Led Approach Towards the Cyber Extorters

The first cyber extortion attacks can actually be traced back to the early 1970s – just as the first 'connected' computers started to evolve. Ransomware, although it may appear relatively 'new,' is just the latest incarnation of a trend that has been with us for some time.

Extortive DDoS was originally the domain of criminals who specifically targeted companies in the gambling industry prior to major sporting events, where tailored attacks were carried out on specific targets right at a point where 70% of turnover was made in a few short days in a year. Caught between a rock and a hard place, many companies paid up. This has since evolved further into the production of 'attack tool kits' such as Shenron and Bangstresser that can be used by groups or individuals with less technical knowledge.

The point is that threats constantly morph, evolve and fragment and it is highly likely that various forms of extortion will continue to present threats to organizations, companies and individuals in the foreseeable future.

There is another crucial factor that also makes firms more vulnerable – not having actionable intelligence on the specific threat actors which may be targeting them. In the context of ransomware, the tools and processes used by actors to employ DDoS-based extortion and compromised data release extortion can vary sector by sector and between the criminal enterprises behind them. Many firms lack cyber-situational awareness: the ability to gain a clearer understanding of what's going on around them from a cybersecurity perspective. This means they do not understand how they appear to the eyes of an attacker and cannot address the weak points that may let the extorter in.

Similarly, they don't have the advanced knowledge of the typical demands of a threat actor nor are they aware of their capabilities – information which can be extremely valuable to organizations that might need to make complex decisions.

> Ransomware is just the latest incarnation of a trend that has been with us for some time

Extorters, just like all cyber-criminals, are comprised of individuals with varying degrees of technical knowledge and sophistication. Many are highly opportunistic and will target just those organizations that have obvious weak spots in their security – the low hanging fruit if you will. However, others are very targeted in their approach with (for example) spear phishing emails to company executives with names and job titles and/or network intrusion techniques specific to the systems in place at a given organization. It's with this latter classification of threat actors where cyber-situational awareness is particularly key.

For a long time in malware, analysts have observed the 'water-bed effect', a term originally attributed to Larry Wall in relation to software engineering. This effect states that in a complex system, that attempting to 'push down' the complexity of a system in one place will invariably cause complexity to 'pop up' elsewhere. It can be argued that this is true of criminal eco-systems too, in that attempts to counter extortive behavior of one type, simply leads the attackers and criminals to move their focus to another place.

So the threat is constantly changing and gaining the latest insight into organizational vulnerabilities, and learning how cyber-criminals operate, and how they may target an organization in a particular vertical sector is at the heart of an intelligence-led approach.

Extorters can never be totally defeated but the risk to firms can be managed.

AUTHOR PROFILE

James Chappell, CTO and Co-Founder of Digital Shadows

James has over 14 years' experience of technical information security acting as an advisor to large private sector and government organizations. Much of his work has involved counteracting the growth of crime and fraud in computer networks and developing effective ways of measuring and managing the information security big picture.

FOLLOW US ONLINE

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

TWITTER: **@INFOSECURITYMAG**

LINKEDIN: **INFOSECURITY MAGAZINE**

FACEBOOK: **INFOSECURITY MAGAZINE**

GOOGLE+: **INFOSECURITY MAGAZINE**

WWW.INFOSECURITY-MAGAZINE.COM

Slack Space

Your Wi-Fi Will Cost You a Firstborn

When it comes to free Wi-Fi and social media sign-ups, most parents are more likely to sign over their firstborns to faceless, nameless corporate drones than actually read the terms and conditions that come with access to either.

A security firm set up an open Wi-Fi network in a busy public area in London; hidden in the T&Cs was the tiny fact that gaining access would require an unusual payment: they would need to sign their firstborn child away to the hotspot provider.

However, it's not just Wi-Fi aficionados that neglect to read the full details. Meanwhile, Jonathan Obar, a professor of communication technology at York University, and Anne Oeldorf-Hirsch, a University of Connecticut communications assistant professor, set up a fake social network dubbed "NameDrop" to test out just how much of a lie "I have read and agree with the terms and conditions" clause can be. They included the firstborn clause, along with a specific caveat that would enable the network to share all of a user's persona data with the National Security Agency (NSA) and employers. Almost all (98%) of the test subjects missed both 'gotcha' clauses.

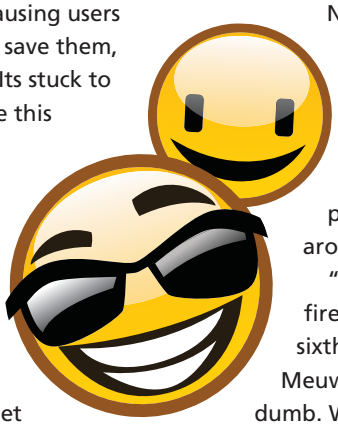
Clearly, ignoring privacy policies and T&Cs is an endemic issue, even in this somewhat paranoid, post-Snowden era.

The researchers modeled their fake ones on LinkedIn's actual policy, reaching a weighty 7977 words, and about 74% of the test group signed up with NameDrop and selected a "Quick Join" option. The rest spent an average of 51 seconds reading the policy.

☺ for Emoji Authentication

On 17 July, millions of smiley faces, poops-with-eyes, dancing twins, hearts, pizza slices and more were sent around the globe via text and social media in celebration of World Emoji Day. After finding success in the digital messaging world and having a day dedicated to them, these colorful icons might soon be testing the waters in a new field – authentication.

As passwords become more complex, they become harder to remember causing users to employ insecure methods to save them, like writing passwords on Post-Its stuck to their computer screens. To solve this security issue, companies have begun exploring the use of emoji as passwords. Due to the high rate of visual recall and the more than 3.5 million unique arrangements of non-repeating emoji, some believe emoji authentication could eliminate the need to reset passwords and even boost mobile use, particularly mobile banking.



In fact, UK-based Intelligent Environments last year commercialized the concept, announcing a new tool via its Android banking app that lets users log into their bank account using emoji instead of the typical four-digit PIN. Users can choose a combination from 44 emoji instead of 10 digits, meaning there are 480-times as many combinations possible versus a standard four-digit PIN.

Still, there are downsides: for one, most keyboards and some websites aren't compatible with emoji, which would get in the way of web-based authentication. Even with a bank of 44 emoji to choose from, brute-force attacks are still a concern.

Girls Rule, Hackers Drool

A new crop of female campers at one of the 119 GenCyber camps sponsored by the NSA and the National Academy of Sciences show how keen young minds can represent a match for any hacker.

These just-for-girls US day camps focus on how to use computers, smartphones and other wireless devices to protect against bullies, hackers, spies and terrorists. There are expected to be 200 such camps next summer.

In one camp in Virginia profiled by the *Washington Post*, campers aged 11 to 13 created a honeypot to attract hackers and chased electronic footprints to track down cyber-espionage actors, among other things. They also visited NSA's National Cryptologic Museum near Fort Meade in Maryland, and talked to experts from Facebook about the social network's approach to ensuring the privacy of 1.7 billion users around the world.

"I loved learning about firewalls," said Bethesda, Md., sixth-grader Victorine Meuwissen, 11. "Hackers are so dumb. We could watch and trace the attack back to them…So cool."

GenCyber says the United States may fall short by 600,000 professional computer security experts this year – and the campers represent the front line in fixing the issue. It would pay off well for any motivated young lady: The Bureau of Labor Statistics says average cybersecurity pay is $116,000 per year, nearly three-times the national income for full-time work.

"They all can't be boys," D.C. seventh-grader Ashley Romero told the Post. "Not many girls do computers, but we can do anything in the future."

"I never knew much about computers," added Sofia Wimblerly, 13, of Washington. "I could see a future using this."

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

If there's one thing the last few years have shown us it's that hackers have evolved into sophisticated, organized criminals, capable of orchestrating well-oiled, imaginative attacks.

They have adopted organizational shifts in how they carry out their work by implementing corporate best practices and established professional businesses to increase the efficiency of their malicious toils against enterprises and consumers.

They even now work within structured setups with their own HR departments to manage employment documents and recruitment processes akin to those used in legitimate business, designed to identify high-quality talent that fits their needs and weed out people with no genuine technical skills.

"The professionalization of cyber-criminals is a concerning trend," Sian John, chief strategist EMEA at Symantec told *Infosecurity*. "Our research shows that advanced cybercrime groups now mirror legitimate organizations in the way they operate, with networks of partners, associates, resellers and vendors. Some groups even deploy call center operations to ensure maximum impact on their scamming efforts, and in some instances employees of the call center are oblivious to the fact they are working for criminal groups executing low-level campaigns like tech support scams.

"The business-like structure in which cybercrime groups are operating, allows them to carry out highly sophisticated attacks and target both consumers and enterprises of all sizes. It also provides better resources and greater efficiency. We're increasingly seeing hackers work normal 9 to 5 business hours and even take weekends and holidays off just like the rest of us," she added.

What's also clear is the techniques cyber-criminals use in their labors have developed to become just as diverse and complex as the individuals who carry out the attacks, with crooks continually devising new ways to target their victims or even designing completely unique assaults for one specific target. This inevitably leaves companies struggling to keep pace – once they seem to have cracked it hackers simply find another, often more imaginative way to break through.

"Cyber-criminals have evolved the 'distribution channel' they use in their attacks," said Luis Corrons, PandaLabs technical director at Panda Security. "Most malware 10 years ago was distributed through email, and although it is still being used nowadays, they are using new ways that didn't exist 10 years ago – social networks are a great example of this. It is now very easy to find personal information about anyone online, and that is being used to send more sophisticated, targeted attacks."

"Also the (in)famous exploit kits that are so popular now were not there in the past. Now they include more exploits and on top of that they use reputable websites to infect users via malicious ads, something that didn't happen years ago," he added.

Furthermore, hackers today also demonstrate the savvy nature to quickly shift their focus of attack to achieve the highest profit. Cybercrime used to be 99% about stealing credit card details for quick financial gain, but numerous recent breaches on hospitals and industrial control systems throughout the world are prime examples of cyber-criminals recognizing that the wealth of data these services store is now just as (or even more) valuable to them in the long-term than much of the information they can access from targeting the financial industry.

In fact, modern-day cyber-criminals have to be so skilled, knowledgeable and capable in what they do that there is a growing skills gap in the hacking market with criminal groups often struggling to find the high-level talent they need.

"It's just as hard now for an organized criminal to recruit technical skills as it is for anyone's business, and actually in some cases they have it harder," James Chappell, founder and CTO at Digital Shadows told *Infosecurity*, arguing that criminal groups often face the challenge of promoting their services without exposing their illegality.

So, with cyber-criminals now such skilled, organized opponents, it's clear that organizations, security professionals and vendors need to be just as forward-thinking as those who seek to breach our perimeters if they are to keep up with their evolving nature and ultimately keep our data safe.

If you are connected to the internet you are at risk of cyber-attack, said Chappell, and staying one step ahead of the opportunistic threat that hackers constantly pose is now very, very important.

"It's about putting yourself in the shoes of the attacker and looking for the places that are your weakness. It's also about looking for those things that happen by accident and understanding the threat by having an insight into what's likely to happen to you when someone is targeting you maliciously."

"If you know what's going on around you, you can make better, smarter decisions about how to defend yourself and recognize the type of incident that can affect you and you can respond effectively," he added.

> Hackers have evolved into sophisticated, organized criminals, capable of orchestrating well-oiled, imaginative attacks

Michael Hill, Deputy Editor

White HAT BALL 2017

Friday 27 January 2017 at the Lancaster London, Hyde Park

The White Hat Ball is the cybersecurity event of the year, in aid of Childline. Tables of ten start at £1,950 and new sponsor packages have just been released.

This sell-out event is one not to be missed and is in aid of a great cause. In 2016 the White Hat Ball raised more than ever before for Childline; a record breaking £162,000. Join us for an amazing evening and help us to be there for children when they need us most.

Your evening will begin with a champagne reception followed by a luxurious three-course dinner. There will be lots of entertainment including silent and live auctions where fantastic prizes will be won.

JOIN THE SPONSORS | RESERVE A TABLE

020 3772 9500 **mary.dobson@nspcc.org.uk**

Support the White Hat Ball
Make a Difference

in aid of the NSPCC's ChildLine Service

#WHB17

www.whitehatevents.org

ChildLine

info security
STRATEGY | INSIGHT | TECHNOLOGY

INFOSECURITY AUTUMN VIRTUAL CONFERENCE

27TH - 28TH SEPTEMBER 2016

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

THE INFOSECURITY AUTUMN 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 CALIBER 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.COM/VIRTUAL-CONFERENCES