

# Detect & Defend

Protecting your organisation against cyber threats

---

- Topical Features
- Event Previews
- Latest Industry Research & Tools
- Expert Opinions
- Career Advice & Guidance



[cyber.qa.com](http://cyber.qa.com)





NOT **SO** SECURE

# TIME TO RULE YOUR HACKING CAREER

---

WE HACK. WE TEACH.

PENETRATION TESTING AND INDUSTRY LEADING HACKING CLASSES

[WWW.NOTSOSECURE.COM](http://WWW.NOTSOSECURE.COM)



# Detect&Defend

Volume I • Issue 1

## Content

- 4 Welcome to the first edition of Detect and Defend
- 6 CyberWatch
- 14 Rise and Fall of Bitcoin
- 17 Is Mr. Robot a good representation of real-life hacking and hacking culture?
- 19 Sometimes an attack might be right in front of your eyes!
- 20 Evaluating persistent cyber threats for IoT in 2018
- 24 The Wannacry ransomware attack: is history doomed to repeat itself?
- 28 The Big Interview: Marc Avery
- 32 Reskilling the Cybergap
- 34 AI for fraud detection: beyond the hype
- 40 Cryptocurrency Mining: Does the reward outweigh the cost?
- 42 Time To Get Tough On Cyber Crime

**cyber.qa.com**

Detect and Defend is a trading division of QA Ltd

Director of Publishing Bill Walker • Editor: Dan Matthews: editor@pmtoday.co.uk

Subscription queries Nadene Gilchrist: Delta 1100, Delta Office Park, Welton Road, Swindon SN5 7WZ

© Copyright 2018 QA Limited • Printed by Barley Print

# Welcome to the first edition of Detect and Defend, QA's Cyber Magazine.

Cyber threats are evolving at an ever faster pace, which naturally requires your learning and organisational posture to remain in-step with the rate of change. As new cyber threats are identified, we must establish the countermeasures to defend against the additional risk and exposure to our businesses. Smaller organisations who often feel immune today, have their fair share of problems via traditional day to day cyber enabled crime, even if they don't realise it yet, whilst the majority continue to fall victim of low cost phishing attacks.

The evolving digital space, agile infrastructure, smart systems and automation of technologies provides an innovative environment for hacking and exploiting new technology. Growing your cyber security capability from inside your business, is now seen as the fastest route to address internal skills shortages. Especially as more and more organisations move their core business to the cloud and integrate with DevOps. Whether you are a seasoned 'red teamer' or project manager looking to step into a cyber role, we continue to develop our cyber learning solutions to meet this end to end opportunity.

You will find some intentionally thought provoking articles within the issue, including Industrial IoT security and the new challenges we will all face. Having spent time protecting thousands of SCADA end points in my career this is still close to my heart. Please do check out the 'big interview' (P28 – 30) with CISO Marc Avery and his perspective on developing in the industry. I first met Marc during my time as CISO within the critical national infrastructure where we collaborated (I was actually his customer) on a very interesting security project, UK Smart Metering!

I am proud to share with you, some of our new cyber partners who are featured in this edition. Here at QA we are passionate about cyber industry collaboration and have consciously partnered with leading innovators and niche specialists to augment and accelerate our cyber learning provision. Learning by doing is at the heart of our products and solutions, providing a safe place to practice, test and develop your skills, all the way to world class certification if required.

Organisations need to better prepare for detection and response measures as a study reveals that the ICO received over six thousand complaints between 25th May, post GDPR effective date, and the 3rd July. Household brands continue to fall victim to cyber-attacks and various degrees of data breaches. These reported compromises will become the litmus test for GDPR effectiveness as we watch for the enforcement mechanisms to support the step change still needed.

Detect and Defend is committed to identifying and offering expert advice, thought leadership and skills and talent solutions to help you and your organisation. Don't hesitate to contact me should you wish to be part of our future editions.

Enjoy reading and we'll see you in the next edition of Detect and Defend.

**Richard Beck**, Director of Cyber







# TRAIN AND CERTIFY ON RED HAT WITH RED HAT AUTHORIZED TRAINING PARTNERS

Maximize your skills and technology investments  
with Red Hat® Training and Certification.

## SKILLS ASSESSMENT

Not sure which course to take?  
Use our free of charge Technical  
Skills Assessment

**Start now: [red.ht/QA](https://red.ht/QA)**

**RED HAT®  
TRAINING +  
CERTIFICATION**

# CyberWatch



## Top cyber security threats to businesses revealed

Research from information security company, Clearswift, has shown that links within emails are perceived as posing the biggest cyber threat to UK businesses, with 59% of business decision makers highlighting this as a chief concern for their business, far more than any other threat.

The research surveyed 600 senior business decision makers and 1,200 employees across the UK, US, Germany and Australia. When asked what they see as the biggest threat to their organisation, business decision makers ranked phishing emails as the top threat in all four surveyed regions.

"Email security consistently rears its head as a key vulnerability in UK cyber defences. This highlights that businesses need to change the way they're approaching the task of mitigating these risks", said Dr Guy Bunker, SVP of Products at Clearswift

"It is easy for a company to perform mock phishing exercises and physical penetration tests to assess vulnerabilities, however this underhanded approach to catch staff out may not always prove to be the best way forward. The approach should be twofold, focused on balancing education with a robust technological safety net. This will ultimately help ensure the business stays safe."

A lax attitude by employees to sharing passwords was ranked second on the list, as a source of cyber weakness, with one-third (33%) of UK businesses listing this as one of the biggest threats. USBs sticks were the next offender, with 31% of respondents highlighting USB/removable storage devices as a major threat. Worryingly, before the GDPR deadline on May 25th, 30% felt that employees not following data protection policies could be one of the biggest threats to their organisation.

Failure by firms to cut off access to the network for ex-employees was next on the list with more than one in four (28%) considering this a major threat. Introduction of malware via personal devices was also present on the list, with more than a quarter (26%) highlighting this as a major threat to their organisation.

Despite some major hacks in 2017, hackers were only the seventh most selected threat, with 25% of businesses flagging this as a major threat.

Other threats to feature included the use of non-authorised tools/applications for work purposes (25%), including personal email drives and file sharing platforms. Additionally, threats coming from social media platforms, often used as a means of spear phishing, was a concern. UK businesses also saw stolen company devices as one of the biggest threats (23%), with these devices often containing critical information.

Dr Bunker added: "With the knowledge that most information breaches are inadvertent, technology can so often provide a clear solution. Like our content aware Adaptive DLP suite, the solution should focus on preventing the information from leaking out, but also provide feedback to the sender to inform them that they have violated policy. This way, a business can work towards a safer environment and a more security conscious workforce."

Top 10 Cyber threats according to UK Businesses:

Business decision makers were asked to choose the threats that they saw as posing the biggest threats to their businesses.

1. Malicious links within emails - 59%
2. Employees sharing usernames/passwords - 33%
3. USBs/removable storage - 31%
4. Users not following protocol/data protection policies - 30%
5. Ex-employees retaining access to network - 28%
6. Viruses via malware on personal devices - 26%
7. Hackers - 25%
8. Employees using non-authorised tools/applications for work purposes (personal email drives/File sharing) - 25%
9. Social Media viruses - 24%
10. Critical information on stolen devices - 23%



## Beyond Encryption formally launches in the UK

Beyond Encryption (BE), a new British cyber security business, has formally unveiled its flagship product: Mailock – Digital Recorded Delivery.

Mailock is a secure messaging platform which has been developed to protect sensitive information sent by email, with applications extending into instant messaging and documentation.

Since the first email systems surfaced nearly 50 years ago, usage has skyrocketed with over 240 billion emails sent daily across the world. Some 86% of professionals name email as their favoured communication method.

Mailock enables users to benefit from encryption in a simple and user-friendly environment. Senders can authenticate their intended recipients identity as well as ensure that no other party can intercept the communication, all using their existing systems and email addresses.

Aside from preventing unwanted interception, BE says senders can also track when messages have been opened by an authenticated recipient, revoke message access if mistakes are made and benefit from a full audit trail of delivery - Digital Recorded Delivery.

Companies that send confidential information electronically are often unwittingly breaching the Data Protection Act which can currently result in fines of up to £500,000 per incident. The General Data Protection Regulation (GDPR) will dramatically extend these penalties once effective in May this year.

The new technology is designed to help businesses meet Data Protection, GDPR and MiFID II obligations. With industry figures estimating that cyber-attacks are costing UK businesses more than £30bn a year, the potential financial implications, reputational damage and business interruption are huge.

Beyond Encryption started life nine years ago, created from a desire to find a way to send and receive messages securely whilst also verifying that the recipient was indeed the intended party.

Founder Paul Holland said: "The World Economic Forum has ranked cyber-crime as amongst the top three risks the world will face this year, so it is a very real threat.

"More words are shared in email than are spoken in the world each day, many carrying sensitive content which can be intercepted in much the same way as a postcard might be in the normal postal system.

"We've seen the regulator's teeth become 'sharper', but the Information Commissioner's Office also makes the point that businesses themselves need to take steps to improve processes and security. Mailock is part of that toolkit.

"Everyone that uses email faces the same security risks and numerous examples of data leakage are raising legal, moral and reputational issues on a daily basis. At Beyond Encryption we're passionate about protecting our users from cybercrime and the our platform has evolved over many years of research and development to enable its users to protect their digital communications data, and therefore their reputation."

According to Holland, Mailock also delivers a quantifiable enhancement to service levels by reducing the reliance upon traditional postal delivery. This improves customer service, reduces postal costs and creates a real ecological benefit. that not only aligns with Environmental Social Governance (ESG) standards but also safeguards senders and recipients alike.



## Cybercrime a 'serious threat' to public services

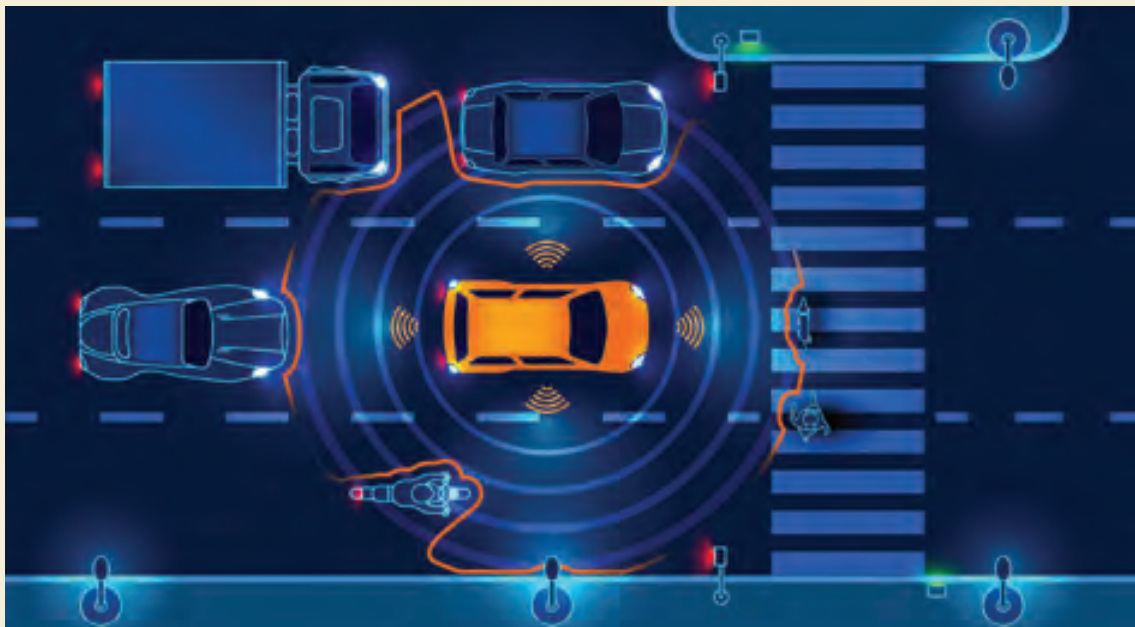
Speaking during a debate in the European Parliament, ECR Flemish MEP Helga Stevens has warned of the increasing threat posed by cybercriminals to our public services and that a dogmatic view of privacy will prevent proper police work to keep people safe.

As public services such as hospitals, governments and the energy sector move online the potential threat from cyber-attacks increases at the same time. These attacks are a continually evolving menace with more than 4,000 ransomware attacks per day and 80% of European companies have experienced at least one cybersecurity incident, making EU and international cooperation essential.

Today's debate in the parliament was launched by the ECR Group and led by Stevens, who sits on the special committee on terrorism and is rapporteur for their final proposals.

Speaking during the debate she said: "We are much more vulnerable to cybercrime attacks than we think. National and European authorities must do everything in their power to guarantee our safety online and we need better prevention, detection and response.

"A better legal framework in the fight against cybercrime isn't enough. We need local authorities to embrace technological innovation and better data access. Our police and intelligence services need data to detect crime and terrorist activity - a dogmatic view of privacy prevents proper police work and keeping us safe."



## AA calls on businesses to embrace connected car data

The AA is urging business owners and fleet managers to utilise the data behind connected car technology to keep their fleets breakdown-free for longer.

2017 saw the number of connected car-based insurance policies, which use data to calculate insurance costs, rise by 30% to nearly one million throughout the UK, across consumers and businesses.

As connected car technology products grow in usage across the UK's fleets, data generation has become a key part of the business owner or fleet manager's role. Yet just 33% of managers use connected car data to improve safety and efficiency across their fleets, according to the AA's own research.

"We're keen to help businesses and fleet managers to make best use of the available connected car technology benefits," said Stuart Thomas, director of AA Fleet and SME services.

"The AA's Fleet Intelligence system generates invaluable data that can deliver huge improvements in risk management and efficiency. A recent Fleet Intelligence review, which analysed fleet-wide connected car data, revealed that an astonishing 36% of fleet breakdowns could have been prevented.

"The data identified the top avoidable faults that drivers experienced as those incurred by coil, turbo and DPF (diesel particulate filter) issues. Our system also shows the average number of days that passed between fault development and breakdown, as well as identifying the total percentage of same day breakdowns.

"Not only does this highly valuable data have the potential to decrease levels of downtime, it also allows fleet managers to prioritise employee safety by allowing them to swiftly respond to dangerous faults which arise, providing the data generated is regularly analysed. We urge managers to get in touch to find out how we can help them to make the most of this opportunity."



## UK consumers target businesses with ‘onslaught of data privacy requests’

Many organisations are being ‘inundated’ with requests for personal information from UK consumers, with two in five (40 per cent) already planning to take advantage of their data privacy rights within six months of the new General Data Protection Regulation (GDPR) having come into force on May 25, 2018.

Under the new GDPR, European Union (EU) residents have greater control over their personal data. Before GDPR, EU residents already had the right to ask a company what personal data is held on them and since May 25, 2018, they have also had enhanced rights to ask to have their data deleted (‘right to be forgotten’). Businesses are now required to sufficiently respond to these requests within one month of receiving the request.

A study, commissioned by Veritas and conducted by 3GEM, surveyed 3,000 adults, including 1,000 in the UK. It reveals that consumers are most likely to target the following industries with personal data requests:

- Financial services companies, including banks and insurance companies (56 per cent)
- Social media companies (48 per cent)
- Retailers (46 per cent)
- Former, current or potential employers (24 per cent)
- Healthcare providers (21 per cent)

The findings came as consumers reveal an increasing need to regain control over their personal data as trust in businesses to protect data fades, and as more and more consumers express a desire to put organisations to the test to understand whether they value consumer rights.

“In light of recent events surrounding the use of personal data by social media, and other, companies, consumers are taking much more of an interest in how their data is used and stored by businesses across many industry sectors,” said Mike Palmer, executive vice president and chief product officer, Veritas.

“With a flood of personal data requests coming their way in the months ahead, businesses must retain the trust of consumers by demonstrating they have comprehensive data governance strategies in place to achieve regulatory compliance.”

GDPR is impacting any organisation that gathers, processes or stores the personal data of individuals in the EU. The research shows UK consumers welcome their enhanced privileges. Of those exercising their rights, two-thirds (65 per cent) request access to the personal data a company holds on them, while the majority (71 per cent) exercise their right to be forgotten under the new regulations.

### The key drivers for exercising their data privacy rights are:

**Increased control over personal data:** over half (56 per cent) of respondents don’t feel comfortable having personal data sit on systems that they have no control over.

**A clearer understanding of what data companies hold on them:** over half (56 per cent) want to understand exactly what personal information companies hold on them.

**Data breaches increase the likelihood of receiving requests for personal data:** nearly half (47 per cent) of respondents will exercise their rights to request personal data and/or have that data deleted, if a company that holds their personal information suffers a data breach.

**Businesses are not trusted to protect personal data:** over a third (37 per cent) intend to exercise their data privacy rights because they do not trust companies to effectively protect their personal data.

**Consumers want to put companies to the test:** over a quarter (27 per cent) want to test businesses to understand how much their consumer rights are valued before deciding whether to continue doing business with them.

**Consumers want to get revenge:** eight per cent will exercise their data privacy rights simply to irritate a company that they feel has mistreated them.

Under the new GDPR, this influx of personal data requests needs to be answered by organisations within a one month time limit. But meeting this timeframe can be difficult as many organisations have limited visibility into what data they have and where it is located.

Most consumers do not expect organisations to be capable of fulfilling their requests under the new regulation. The majority (79 per cent) believe that organisations won’t be able to find and/or delete all of the personal data that is held on them, and a fifth (20 per cent) believe that businesses will only be able to deliver up to 50 per cent of the personal data they hold.

“It’s imperative that businesses embrace technology that can help them respond to these requests quickly, with a high degree of accuracy. This means having the ability to see, protect and access all of the personal data they hold regardless of where it sits within their organisation. Businesses that fail to recognise the importance of responding effectively and efficiently to personal data requests will be putting their brand loyalty and reputation at stake,” added Palmer.

## Gov survey shows half of business targeted in cyber attacks

The UK Government has published a report revealing that more than half of UK businesses have been targeted by cyber-attacks in the last 12 months, using common hacking methods including fraudulent emails, attempts by scammers to impersonate the organisation online, viruses and malware.

The survey included finance and insurance companies, as well as the charitable sector for the first time, with one in five (19 percent) being targeted by fraudsters and hackers.

Fabien Libeau, EMEA VP at Risk IQ, said organisations need complete control and visibility over the threat to their brand: "As businesses move online, this Government report highlights the growing risk surrounding corporate digital assets – across mobile, social and web – that are still too often overlooked. For organisations, their brand is one of the biggest and most valuable assets – but it is also the biggest attack vector for opportunistic cybercriminals.

"As seen with this report, threat actors are exploiting brand trust to defraud an organisation's customers, partners, and prospects through phishing, malware, and online impersonation. Brands, particularly in the financial and charitable sectors, cannot afford to ignore - or fail to detect - these common attack techniques.

"As such, digital threat management needs to become a critical component of corporate security strategies. Organisations should be investing in technologies that boost visibility into fraudulent and unofficial websites, as well as identifies fake social media accounts that impersonate the company, its brand or executives. In addition, it is critical to use automated technology to understand exactly when and where company logos are being used across partner or competitor sites.

"When cybercriminals impersonate brands on the internet and mobile app ecosystem, they not only jeopardise customer security, but they can do serious reputational damage to the organisation. By having complete visibility and control over all digital channels, organisations will be able to spot suspicious activity immediately. It's this that will keep the Government figures down and help more organisations avoid the reputational and financial repercussions of an attack."





## Traditional security defences ‘inadequate’ for effective GDPR strategies

Companies risk falling foul of incoming GDPR regulations by relying on existing, piecemeal security measures, according to a new whitepaper published by Aruba, a Hewlett Packard Enterprise company.

The majority of existing defences, which use pattern matching techniques to find threats, are unable to detect new attacks that use legitimate user credentials to access sensitive information, meaning that companies risk not being able to detect and report a breach within the 72 hours stipulated by GDPR, says the whitepaper. The resultant fines can amount to €20 million, or four percent of annual turnover.

However far from calling for existing systems to be replaced, Aruba’s whitepaper suggests that these products remain essential as part of an effective GDPR strategy. Rather, it highlights the need to complement these defences with an additional layer of monitoring that utilises new types of attack detection, such as machine learning, to analyse the entire network collectively, and find the very small changes in activity that are indicative of an attack.

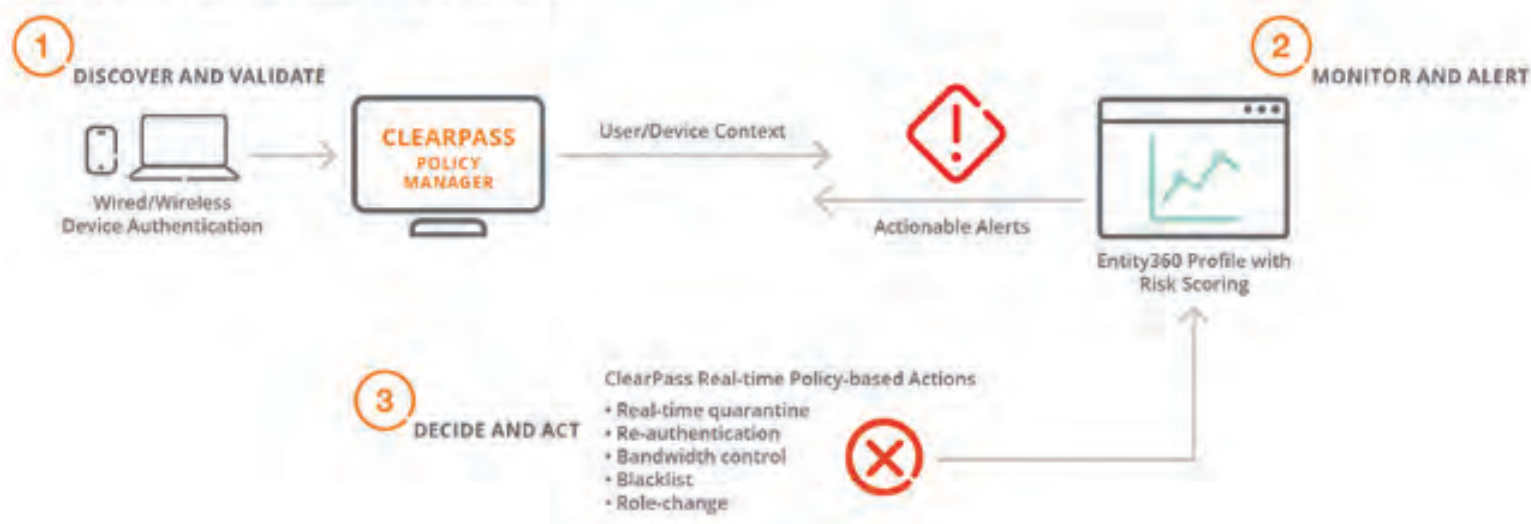
“Personal information is absolute gold dust for attackers, because it can quickly be sold on the Dark Web” said Morten Illum, VP EMEA at Aruba. “It’s almost certain that your business will see its personal data targeted in future, and attackers will appear to be a trusted user while they are carrying out their work.

“Without using automation tools to spot the unusual activity that’s going on, it could take months to detect what’s going on. And that’s bad news both for your customer relationships, and your GDPR strategy.”

As hacks become increasingly sophisticated and often spread out over many months it’s very difficult for security teams to identify small anomalies in how a device is accessing the data stored in an application. The Aruba 360o Secure Fabric offers a combination of network access control capabilities to view the millions of devices accessing the network, and provide policy-based, device-specific access that can significantly limit access to user personal data.

### DETECT, RESPOND, INVESTIGATE, THEN REMEDIATE

#### CLEARPASS + UEBA = 360° PROTECTION



The solution also includes the new Aruba IntroSpec, which uses machine learning to determine where personal data resides, and search the entire network for anomalous activity that could indicate a potential security breach. IntroSpec uses this learning to generate ‘risk scores’ for each connected user, device, system and database, focusing the attention of IT and security teams and ensuring future attacks do not go unnoticed.

Reports from users of IntroSpec have shown that new threat investigations have been completed 30 hours quicker than previously-used systems, a significant reduction in the fight to meet the 72 hour reporting deadline of GDPR.

“There is no single product or combination of security solutions that can guarantee GDPR compliance”, continued Illum, “so it’s time that we bring existing solutions together. A holistic GDPR strategy can only be achieved if the security teams have the right tools to do their job. We think a single view of the network, and the ability to automatically create new policies based on incoming activity, is our best chance of staying ahead.”



# CyberSecurityJobsite.com

The UK's largest online job board for cyber security professionals...

Cyber Security Jobsite.com is a specialist Job Board which caters for candidates and clients who operate within the Cyber Security arena. The Job Board hosts hundreds of jobs daily from apprenticeships through to C-suite level vacancies.

The site was established in 2013 to cater for the increasing demand for cyber security vacancies and to assist in addressing the skills shortage that we are seeing in this marketplace.

Candidates can utilise the Job Board in many ways and is a free service.

#### Site functionality for candidates:

1. Search our current vacancies through the multi-faceted search function
2. Upload a copy of your CV and make it available to the plethora of companies and recruitment agencies that have access to our secure candidate database.
3. Register yourself for tailored job alerts that meet your specific criteria. Once registered matching vacancies will be emailed to you.

#### WE ALSO HOST THE CYBER SECURITY EXPO

The EXPO provides job seekers with the opportunity to meet with companies in a secure environment on a face to face basis. The EXPOs are currently hosted in both London and Bristol and attract a high number of cyber professionals with varying levels of experience. The EXPO is now in its 5th year and provides candidates a great opportunity to meet the teams that are recruiting and gain a deeper understanding of the roles and the culture of the companies they may be applying to.

As a group we work closely with QA to promote their courses to our users and to assist them resource qualified trainers through both our Job Board and the Cyber Security EXPO.

If you have recently completed or are thinking of embarking on one of the many courses that QA offer, then your new skills are in high demand and a world of opportunity awaits you.

QA offer a comprehensive list of courses for all levels of experience providing a springboard into the cyber marketplace or to further your knowledge in this competitive but growing industry.

If you are interested in looking at new opportunities, please visit the sites and see where your new skills may take you.



#### 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...

**CYBER SECURITY**  
**EXPO**





The shortfall of qualified candidates within the cyber security market has led to a competitive industry with above average salaries being offered.

JOB TITLE	EXPERIENCE	SALARY BANDS
Analyst / Associate	1-3 Years	£28,000-£40,000
Officer / Senior Analyst	3-7 Years	£40,000- £80,000
Manager	7-12 Years	£60,000 - £75,000
Senior Manager	7-20 Years	£75,000 - £95,000
Head Of	3-7 Years	£110,000 - £150,000
Director	7-12 Years	£120,000 - £170,000
Global Head /CISO	12- 20+ Years	£175,000 - £450,000
SOC Analyst	1-3 Years	£35,000 - £55,000
Penetration Tester	2-7 Years	£55,000 - £90,000
Check or eqv Qualified	4-12 Years	£60,000 - £110,000
Data Protection Manager	4-12 Years	£60,000 - £120,000
Incident Response	3-7 Years	£65,000 - £90,000
Security Architect	7-12 Years	£80,000 - £110,000
eForensics specialist	4-7 Years	£30,000 - £65,000
IDAM specialist	4-7 Years	£40,000 - £75,000

Daily rates for contractors remain high with the majority earning over £500 per day. Rates for in demand roles such as architects, data privacy and pentesters are largely over £650 per day and beyond.

Salary survey reference Beecher Madden 2017-18.

# Rise and Fall of Bitcoin



With the popularity and value of crypto currencies growing, so do the security and anonymity concerns.

## Graeme Batsman

As with everyone we all regret not doing something, be it not buying shares in Apple or not buying 100 LTC (Litecoins) two years ago. Bitcoin and newer crypto currencies were created as a non-capitalist, de-centralised and likely anti-government establishment alternative to the Pound, Euro or Dollar which is extremely widely accepted and has regulators. The funny thing is Bitcoin is slowly becoming more mainstream and you could argue has become part of a capitalist system!

Two years ago, 1 BTC (Bitcoin) was worth \$319 and today (31/01/18) \$10130 – an increase of over 3000%. A single share in Microsoft has only just about increased 100% in two years. Recently BTC dropped by about £1000 in a single day, which a share would just never do. Volatile it is, it usually jumps back and there is speculation it could hit \$50,000 next year. A bank account from NatWest, Barclays and HSBC is where people normally store their cash, from pounds to hundreds of thousands until now.

To get a bank account with the above you need to show a passport, driving license, proof of address, utility bills and days or weeks later subject to their terms you get a bank account number, sort code, online logins and a physical card. The bank and the state can freeze your cash if they wish. With crypto currency it is very different and without any checks you can create your own local 'bank account' in under a minute.

## What does it look like?

The public address is as it sounds, people can look it up, see the value and transaction history. The private or secret key is used to transfer money out.

With a conventional bank account, the security of the bank is down to the bank and the security of the account is down to the bank as well as you. With a virtual wallet (account) it is 100% down to you and you are on your own. If you lose it or lose the password (if you set one) you are stuffed.

## Crypto currency security

NatWest, Barclays & HSBC force you to login with a unique username, password & PIN and they enforce two factor authentication. Out of the box a crypto wallet can be in plain text, protected with a password or passphrase or stored on a special USB stick. Two years ago, what sounded more appealing breaking into someone's bank account at HSBC and stealing say £9,000 or stealing \$319? Jump ahead two years and \$319 is now worth well over £9,000 and guess what HSBC is not responsible for it.

From an end-users view security concerns do not lie in the 'network' but in the actual wallet. Wallets can be stored on a desktop, laptop, tablet, smartphone, USB stick, piece of paper or online. Simple, if someone can access the wallet, recovery words or the private key they can transfer the money out. Wallets in the electronic format can be password protected but with passwords they can be guessed or key logged. Some of the online wallet stores have been breached. Like with anything it is better to keep it close to your chest

Phishing usually goes for your email address, bank details or PayPal logins however lately the phisher men are going for wallets due to the sharp increase in value. The bad guys & guys are creating fake sites which ask for online wallet login details or even the private/public key address. A better storage method is a normal or special USB stick which is intended to store wallets. Now to steal the wallet you need to steal the stick or get lucky and hijack the wallet whilst the USB is connected to a computer.

The most secure storage method is a paper wallet which you can see above. You get a public/private key along with QR codes to print off. Though if you lose it, you have lost £x or leaked it to someone else. Best to store such paper wallets in a safe and keep spare copies. Better still you can password protect a paper wallet with BIP38. Storing a paper wallet in a safe raises an interesting and likely unknown question. If the safe is rated to £4,000 and your paper wallet is stolen from it, can you file against the safe manufacturer or the insurance provider?



## Crypto currency 'anonymity'

Compared to a bank account crypto currencies are more anonymous and that is why the underworld likes them. Unlike a bank account you cannot simply look up an account number and see the total nor past transactions. Anonymity depends on your usage. Anyone can generate an 'account' without providing a name, address, date of birth or any ID by visiting a wallet generator such as <https://www.walletgenerator.net> or using a local generator. Once generated and empty it is pretty much anonymous since there is no value nor history.

The audit trail begins when you receive money. If you are an average user you will go to an exchange, provide them a name, address, email address, password and proof of address then you can buy currency. To buy it you would select the amount and it would ask you to transfer £x to a bank account and minutes later your wallet now has £x in it. If someone was going to hack or subpoena the exchange your identity would be exposed. They could see who sent you the money.

Slowly you can spend crypto currency in the real world. Some shops (more independents) and even food market stalls accept Bitcoins. Let's imagine your wallet had £1,000 in it and every Friday there was a food market near your office. Instead of paying £5 you could transfer a fraction of a Bitcoin over. If you did this a lot and with different food stands someone could figure out where you eat, what you eat and where you likely work. This is assuming someone knew Bitcoin public address x belonged to food stand(s) x.

## China

A quarter way through the first month of the year and the Chinese state announced a clampdown on Bitcoin mining in China. Why? Due to the state not being able to control it, the tax rules around crypto currency being a very grey area and because of 'high' power consumption - reports say around 0.2% of the countries power consumption is from miners. Currently China has the highest number of miners and the reasons are simple, 1. The population is 21x that of the United Kingdom and 2. Power (and labour) is cheap.

Enforcing this new law could be tricky since China is about the same size of Europe and with a massive population. It maybe easy to shut down giant mining farms but they could keep moving or split up to evade detection. Money also talks... Even if Bitcoin dropped by 2/3 it would still be profitable to mine them in China or elsewhere (Switzerland or Russia are possibilities). The impact is unlikely to be great and from 3/1 - 10/1 it has only dropped by 3.73%. That said crypto currencies are very unstable generally - with Ripple being branded as amazing, then dropping 38.3% in seven days and then Ethereum jumping 33% in the same time frame.

## Graeme Batsman

### Cyber Security Trainer

Graeme joined QA in 2017 and has worked in security on and off for 13 years. His last role was as a Senior Technical Security consultant at Capgemini covering public and private sector. From the age of 17 he was running investigations into online scams and phishing. Today his experience is in OSINT and thinking like a hacker to review + tweak settings with a fine tooth comb.





Certified Training



# Quickly identify high quality cyber security training

## Why choose a GCHQ Certified Training Course?

- The course materials have been rigorously evaluated against the exacting standards of GCHQ.
- Trainers have been assessed to ensure quality of delivery and cyber security knowledge.
- Provides assurance that you are investing in quality training.


Find out more at  
[www.apmg-international.com/GCT](http://www.apmg-international.com/GCT)

---

 **APMG** International



# Is Mr. Robot a good representation of real-life hacking and hacking culture?



QA Cyber Security Researcher, **James Aguilan**, looks at several scenarios featured in the hit US TV series Mr. Robot and how they may represent real-life hacking.

Mr. Robot is an American Drama Thriller television series that depicts hacking culture. Elliot, cybersecurity engineer and hacker, is recruited by an anarchist to join a hacktivist group called 'fsociety'. The group aims to destroy all debt records by encrypting the financial data of the largest corporation in the world. This blog post focusses on several scenarios and how it may represent real-life hacking.

## **Scenario 1: Eavesdropping a coffee shop public WIFI (Man-in-the-middle attack)**

In the beginning, Elliot confronts a man who owned a coffeeshop. He confesses that he intercepted the WIFI network traffic. Knowing that most public WIFI networks that are unencrypted, this is completely possible. Anyone can join the network, and anyone who joins the network can eavesdrop using simple web traffic analysing tools such as Wireshark. Any communication that is not properly encrypted, including email or your browsing data, can be viewed by attackers. To prevent falling victim to a man-in-the-middle attack, avoid using unsecure public WIFI networks. Additionally, if you must use public WIFI, use a VPN and make sure your traffic is encrypted by looking at the green lock in the upper URL bar.

## **Scenario 2: Elliot exposes child pornography site owner in the dark web (Hijacking Session or Brute Forcing Cookies)**

Elliot gained access to e-mail, figures and pictures. He figures out that the owner runs a childporn website on the Tor network. Tor can be used to maintain anonymity on the internet. How he exactly hacked him is not mentioned. He did mention that, "whoever is in control of the Tor exit nodes, is also in control of the network". When you intercept traffic, you can launch an exploit against the Tor browser when JavaScript and plug-ins aren't disabled. NSA FoxAcid program tries to exploit Tor users. However, how he got control to the exit nodes and how many exit nodes is not mentioned. So that a single person could have controlled enough exit nodes to do this could be dubious. Assuming either unencrypted network traffic or a way to get his SSL certificate accepted by users without raising suspicion or a known vulnerability, such as brute forcing cookies and hijacking the session of a logged in user, intercepting information when controlling the exit nodes can take a very long time. In addition, breaking TOR anonymity or sniffing TOR traffic in a targeted and systematic way requires advanced state actor capabilities and funding. Typically, it is very opportunistic, and mainly applies to applications that do not use SSL. This scenario is therefore quite impractical and unrealistic.

### Scenario 3: Elliot hacks personal accounts (Social Engineering)

Elliot got the password by using a custom script and using a combination of a wordlist and a brute force attack. This password was based on her favourite artists and the year she was born but written backwards. A lot of people have this type of information on social networks sites and reuse password these days. These types of attacks exist in real life and this could be possible as well. Even with today's advanced security solutions, hacking into personal accounts such as email, dating services, and social media is relatively easy. The attack is usually based on brute force attempts to crack your password. This is unfortunately still effective, especially with ready-made, off-the-shelf tools that are available to anyone who wishes to launch such an attack. Choose strong passwords for your accounts, do not share the same password across accounts, and apply two factor authentications when possible.

### Scenario 4: E-Corp servers are attacked as a diversion to another attack on the servers (DDoS)

Needless to say, this is realistic. a Distributed-Denial-of-Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources and present a major challenge to making sure people can access important information, thus effecting daily business operations. DDOS attacks at 3AM and E corps is down for one hour, resulting in a total revenue loss of approximately 13 million dollars. In reality, DDOS attacks can cause severe revenue losses. The average distributed denial-of-service (DDoS) attack costs a business roughly 40,000 dollars per hour. This technique has been used in several past real-life security incidents, most notably the Sony PlayStation breach in which the account information of 77 million users was stolen under the cloak of a large-scale coordinated denial-of-service attack. Network protection is not enough. You must also protect your data.

### Scenario 5: E-Corp servers are infected that crashes the servers on boot up (Rootkit)

Elliot recommended restarting the services that are not coming back up. After rebooting the services, there was a destination unreachable error for the IP-addresses of the servers. After that a connection rejected, because of too many connections error was shown. A custom script was used for a port scan to uncover which users were logged in. It was determined the hackers broke into the server. Elliot mentions that the attack was coming from IP-addresses from everywhere around the world and Elliot's boss suggested to use load balancer to redirect the traffic to counteract the DDOS attack. However, Elliot doesn't think that it is just a DDOS attack, but that there's a rootkit inside the server as well. They redirected the traffic to another server and update some network settings. After that Elliot checked the running processes at the infected server and inspected some files – he uncovers a rootkit install. A rootkit is a software that is made hard to detect and remove and can completely take over the system, install/change/delete everything it wants. These rootkits run as part of the operating system itself with the highest privileges and can modify start up code like Master Boot Record (MBR) and crash the server on every restart. Removal of kernel-mode rootkits often results in reinstallation of the operating system. Therefore, it is advisable to back up your server data regularly.

### Conclusion

Mr. Robot is a great TV series and it offers some real-world advice on how to keep your data and systems secure. Overall, it provides a realistic depiction of what is possible. Mr. Robot has been widely praised for its technical accuracy by numerous cyber security firms and bloggers who dissect and comment on the technology and the technical aspects of the show after every episode. The only issue is how fast he hacks. Granted, the speed at which Eliot Hacks isn't possible with standard computers, the process is pretty realistic. The speed of Eliots hacking is to fit in a typical tv episode. Typically, a hacker would need to spend some serious time finding potential security issues that can be exploited. Social Engineering takes time and brute force attacks take time. With somewhat complex passwords, it can take months to directly crack a password.





# Sometimes an attack might be right in front of your eyes!

QA Cyber Training Delivery Manager, **Mark Amory**, discusses a new exploit in X.509 certificates that allows malicious code to be inserted into a network.

Attackers have for many years tried to find ways to get malicious code inside a victim's network; Some new research by fidelis security has uncovered another, novel way to achieve those aims which your security systems might not pick up. The original research in pdf format can be found at the following link (<http://vixra.org/pdf/1801.0016v1.pdf>)

The attack exploits the fact that X.509 certificates have a number of fields which can contain arbitrary values. In their research, Fidelis proved that data can be transferred within the SubjectKeyIdentifier field of the X.509 certificate and is not limited to any size constraints other than the extents of device memory.

The SubjectKeyIdentifier field is supposed to hold a hash value that identifies the public key being certified. This value enables distinct keys used by the same subject to be differentiated.

In an attack using this approach this field can be used to pass through any form of data, including executable code.

In many cases, the SubjectKeyIdentifier value is not validated by either firewalls or IDS as they typically are set to look for data being transmitted in a protocol payload such as a TCP, UDP or SMTP packet.

In the case of the X.509 certificate the code is passed as a part of the handshake process, and as such no data payload is being transmitted.

Fidelis produced a proof of concept attack and included a Mimikatz payload in the X.509 certificate and transferred it to an already compromised device via the TLS negotiation phase.

There are ways to check to see if a certificate is being used in these ways. For example, the common hashes used in the SubjectKeyIdentifier field are MD5, SHA-1, SHA-256, SHA-384, or SHA-512. As such, if SHA-512 is used that would create the longest hash value at 128 characters long. Rules can be established (normally with the use of a Regex query) to look for values in this field which are longer than 128 characters and flag them if they are.

But how many of you reading this have such rules?

How many of you reading this even contemplated someone using X.509 to attack your organisation?

**How many of you are about to go check and update your firewall rules?**

## Mark Amory

### Cyber Training Delivery Manager

After leaving a career as a Mechanical and Electrical Engineer in 1998, Mark started out with a fresh career as an IT trainer. Spending the first few years as an applications trainer, Mark excelled in delivering Microsoft Office and Adobe products. In-line with his background as an Engineer, Mark soon shifted focus to more technical deliveries, including hardware and networking topics; a field he has remained in ever since. As a natural progression of his career saw Mark start to explore the security aspect of his existing competencies and since 2005 has specialised in the Cyber Security domain. Mark has been the author of a number of QA Cyber Security courses. Mark is a CIEH and is currently undergoing the process of becoming an NCSC Certified Cyber Professional.



# Evaluating persistent cyber threats for IoT in 2018

by QA Cyber Security Trainer, **James Aguilan**

Welcome to the era of the Internet of Things (IoT), where digitally connected devices are encroaching on every aspect of our lives, including our homes, offices, cars and even our bodies. An IoT device is defined as a physical device, vehicle, home appliance, or other item with embedded electronics, software, sensors, actuators and/or connectivity which enables said device to exchange data. IoT is growing at a dangerously fast pace, and researchers estimate that by 2020, the number of active wireless connected devices will exceed 40 billion. The upside is that we can do things we never imagined possible. But as with every good thing, there's a downside to IoT: It is becoming an increasingly attractive target for cybercriminals. The increased popularity of the IoT leading to growing adoption is one of the main reasons for more cybersecurity attacks against enterprises. With IoT popularity, new threats are coming in and the need for a stronger IoT security remains. Every year we see new persistent cyber threats, from new targets for hackers to new issues cropping up in the cybersecurity space. As the use of such IoT devices has increased in both the public and private sectors. In this editorial, I will highlight three persistent cyber threats to IoT devices that I believe enterprises need to be aware of:

## **Industrial IoT Devices Secured Poorly and Problematic to Patch**

It is expected that 25% of cyber-attacks will target IoT devices by 2020, many of which will be deployed in industrial environments. The Shodan search engine is the Google for the Internet of Things, a playground for hackers and terrorists. However, it is a useful tool for companies looking to lock down their own environment. Infection and covert usage of IoT devices to mine cryptocurrencies or conduct DDoS attacks is a trend that isn't slowing down, and one that is especially problematic in the industrial space because Industrial IoT devices tend to be both secured poorly and problematic to patch. Typically, smart devices purchased by organisations do not allow sufficient access to native operating system security features. This means security professionals have a limited set of security features to work with. In some cases, there may be none.

Mirai is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. It's true that Mirai, and variants such as Okiru and Satori, pose a major risk, where the reduction of a connected device's processing power can seriously impact safety or disrupt processes. But there is also the potential for untargeted, collateral damage in this space. The prospect of motivated attackers leveraging destructive malware such as BrickerBot to wipe devices is highly concerning, but such 'attacks' need not even



be targeted to cause damage. A wormable exploit such as the one used by WannaCry could cause widespread infection of industrial IoT devices – to devastating effect – quite regardless of the original intentions of the attacker.

## **Humans are still the weakest link in the security chain**

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. Humans are still the weakest link in the security chain, but hiring and training people who can understand and respond to issues in the threat space is only becoming more difficult. Demand is rising much faster than supply, with 3.5 million unfilled positions in the cyber security field expected by 2021. At the same time, the eternal catch-up game played between criminals and analysts continues, with threats becoming more sophisticated and widespread every day.

According to NIST, as we further integrate IoT technology into our lives and into sectors including critical infrastructure, this problem is not going to go away – it is going to get worse. The skills we need to protect ourselves: analysing information, separating intelligence from noise, and understanding the motivations of threat actors, are in short supply. They need to be refined. To some extent this is happening; however, it's simply not doing it fast enough. If this skills gap widens too fast, and too quickly, it won't matter how much organisations are willing to pay to fill these vital positions; we will all become victims.

To alleviate this problem, Organisations need to put more effort than ever into hiring, training and retaining the next generation of cyber security experts. Information security is increasingly being viewed as more than an IT-only problem, which is a big step, but budgets don't always scale with intentions. Working to improve the "cyber hygiene" of employees is important, but no organisation is unbreachable and organisations need many more skilled people if they want to be prepared for when the worst happens.

## **Theft and manipulation of personal information from IoT devices**

While the Internet of Things (IoT) may make our lives easier, the security considerations are sometimes an afterthought and are sacrificed to get a product to market faster. Theft and manipulation of personal information from IoT devices is a growing concern. With IoT machines becoming ever more popular with consumers, we need to come to terms with the idea that our personal information is more at risk than ever. Devices such as Amazon's Echo and other virtual assistants allow us to sacrifice convenience for security – as we learned when a researcher used malware to stream audio to a remote server. Or when a Bluetooth vulnerability rendered Echo, Google Home and billions of other devices vulnerable to hijacking. Hackers would use Reconnaissance, such as Foot printing, Scanning and Enumeration, to covertly discover and collect information. With IoT devices this can be what we say and do in our own homes. Identity theft and the resale of shopping habits are all perfectly possible, but this data can also enable crime in the physical world.

Mitigating data theft from devices like Echo is both a manufacturer issue and a consumer one. The more these devices are sold and used, the more attractive targeting them becomes for criminals. At the same time, the longer consumers wait before purchasing, the more tried and tested (and secure) this technology becomes. Purchasing from quality vendors will also reduce the risk of security 'oversights' and make sure that vulnerabilities are patched. Fundamentally, it also comes back to the very personal question of convenience versus security; to what extent are the risks worth the rewards?

## **Mitigating Steps**

Many severe cyber security issues stem from poor security design and bad practice in products sold to consumers. Security by Design, a new report from the UK's Department for Digital, Culture, Media and Sport (DCMS) suggested a code of practice for security in consumer IoT products and associated services. The report specifies 13 principles for assuring that security is incorporated by design in newly developed IoT devices. The Code of Practice sets out practical steps to improve the cyber security of consumer IoT products and connected services. Security by design is a good concept when delivered correctly. It helps users understand the requirements and helps make the right decisions to ensure their safety is sustained. The biggest issues for the consumer are not knowing they need protecting. The code of practise set by DCSM are important for the following stakeholders:

1. Device Manufacturer
2. IoT Service Providers
3. Application Developers
4. Retailers

**In short, the code of practise consists of the following:**

### **1. No default passwords**

IoT device passwords must be unique and not resettable to any default value. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and authentication methods should be followed.

## **2. Implement a vulnerability disclosure policy**

Companies must provide a public point of contact as part of a vulnerability disclosure policy so security researchers can report issues. Knowing about a security vulnerability allows companies to respond in a timely manner. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Reports of vulnerabilities can be sent to: [security@ncsc.gov.uk](mailto:security@ncsc.gov.uk).

## **3. Keep software updated**

Software components in internet-connected devices should be securely updateable. Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support must be made clear to a consumer when purchasing the product. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

## **4. Securely store credentials and security-sensitive data**

Credentials must be stored securely within services and on devices. Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Security-sensitive data that should be stored securely includes, for example, cryptographic keys and initialisation vectors.

## **5. Communicate securely**

Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. All keys should be managed securely. The use of open, peer-reviewed internet standards is strongly encouraged.

## **6. Minimise exposed attack surfaces**

Devices and services should operate on the principle of least privilege, unused ports must be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

## **7. Ensure software integrity**

Software on IoT devices must be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

## **7. Ensure that personal data is protected**

Where devices and services process personal data, they should do so in accordance with data protection law. Device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service.

## **9. Make systems resilient to outages**

Resilience must be built into IoT services where required by the usage or other relying systems, such that the IoT services remain operating and functional. This includes building redundancy into services and mitigations against DDoS attacks such as firewalls, load balancing and filtering.

## **10. Monitor system telemetry data**

All telemetry data from IoT devices and services should be monitored for security anomalies. Any unusual activity can be identified early and dealt with, minimising security risk and allowing quick mitigation of problems that do emerge.

## **11. Make it easy for consumers to delete personal data**

Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their data.

## **12. Make installation and maintenance of devices easy**

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. This is to prevent security issues caused by consumer confusion or misconfiguration, caused by complexity and poor design in user interfaces.

## **13. Validate input data**

Data input must be validated. This ensures that systems are not easily subverted by incorrectly formatted data or injected code.

## **Conclusion**

The IoT device market is still relatively immature and somewhat of a Wild West. By 2020 there will be over 50 billion connected devices. Understandably, manufacturers are racing to capitalise on the opportunity, but unfortunately, many are doing so at the expense of basic security measures. As more smart devices with weak or no security connect to the internet, the world will become more exposed to attacks like the WannaCry ransomware that hit UK National Health Service.



# Educate Your Employees on the Importance of **GDPR** with



MetaCompliance®

## COFFEE BREAK LEARNING COURSES

Bite-Sized Learning in 3 mins or less!

### GDPR Titles Available:

What Is GDPR?  
Identifying Personal Data  
Personal Data Inventory  
Data Breach Reporting Guidelines  
Data Minimisation  
Data Subject Rights  
Does It Apply To Me?  
What Is Sensitive Personal Data?  
Processing Subject Access Requests  
What Is Personal Data?  
What Is Processing?  
The 7 Principles Of Data Protection  
What Is Consent?  
Privacy Notices  
The Background  
Am I Compliant?  
Accountability & Compliance  
Transferring Data  
Withdrawing Consent  
The Penalties

## FREE! GDPR FOR DUMMIES GUIDE





# The Wannacry ransomware attack: is history doomed to repeat itself?

By Katie Gascoyne



On Friday, 12 May 2017, just over a year ago, a global ransomware attack began that would change the way the world looked at cyber security forever. Within 24 hours of the initial infection, WannaCry had affected an unprecedented number of more than 200,000 computers in 150 countries.

As we know, the NHS was crippled by the attack. Thousands of appointments and operations were cancelled and patients had to travel further to receive medical care at accident and emergency centres. This national emergency proved a startling realisation of how vulnerable our infrastructure can be.

Last month, despite promises that lessons had been learnt and impactful changes would be made, an official government report found that out of 200 hospitals and NHS trusts tested for vulnerabilities one year on, not one has passed cyber security assessments.

This report, while quick to diagnose the failings and shortcomings, says little about real, concrete ways in which the NHS can adapt to prevent an attack of this magnitude ever happening again.

Here, we critically examine specific areas of the report to determine how these vulnerabilities can be rectified to avoid history repeating itself.

### **‘Communication during the cyber attack’**

The Public Accounts Committee (PAC) describes in its findings that, while a plan had been developed for responding to a cyber attack, it took three hours to be initiated and had not been tested with local organisations – a “huge mistake”, according to Peter Godden, VP EMEA at IT resilience provider Zerto. “Strict testing of your disaster recovery (DR) plan should be done on a continuous basis... in highly regulated industries, such as healthcare, testing should be undertaken as often as monthly. As well as habitually testing the DR plan, it should also be thoroughly documented and understood so that the entire team know what to do if it needs to be engaged.”

However, argues Stephen Moore, chief security strategist at Exabeam, over-complicating an incident response plan can also lead to failure, particularly if they are “based on elaborate hypothetical scenarios and guesswork.”

“In the event of a real breach, not only might the attack be completely different in terms of attack vector and ferocity than those modelled, but in many cases, the sheer scale of the attack can be far greater than anticipated. As a result, the plans are often dropped as the response team goes into full firefight mode. Where organisations should be careful is in how elaborate they make those plans. Whilst clear procedural information on what to do is valuable, overly complicated steps can be difficult to follow in the heat of the moment, leading to frustration and abandonment.”

### **‘Local organisations’ readiness for a future cyber attack’**

The report found that before May 2017, NHS Digital needed far more visibility over its entire infrastructure to ensure a level of readiness for a cyber attack. It became apparent in the aftermath that local organisations had operated in silos with no overarching structure to provide centralised visibility – a problem that Paul Parker, Chief Technology of Federal and National Government at SolarWinds, thinks could be solved through network monitoring. “This would enable IT leaders to pull together information about the devices being used on the network, including operating systems, current patches and security protocols, as well as any malicious traffic targeting the system – all in one single program.

“Using a software like this, NHS Digital would have full visibility of its entire network, and could provide recommendations and guidance on security vulnerabilities, as well as taking proactive next steps towards a more secure infrastructure. In an absolute worst-case situation, like we’ve seen previously, they could still perform a damage assessment and quickly identify a root cause.”

### **‘Updating and protecting systems without disrupting patient care’**

The issue of patching became a huge problem area brought to light by the attack. Most NHS organisations could have prevented the virus by simply applying the patch issued by Microsoft for Windows 7 – the operating system used by more than 90% of devices in the NHS. The reason given for this huge oversight, and the continuous problem seemingly as yet to be solved, was that the process of patching could lead to disruption of medical equipment and ‘present a clinical risk to patients’ – this consideration would have been unnecessary had the NHS implemented the latest version of Windows, claims Mat Clothier, CEO, CTO and Founder of Cloudhouse.

“By upgrading to Windows 10, these organisations could avoid this disruption and simultaneously avoid the security vulnerabilities of running older systems. Because they do not receive regular security updates and patches, legacy systems are less likely to prevent a cyber attack.”

“The problem is, upgrading isn’t always that easy. Not only is it time-consuming and sometimes expensive, the thought of having to migrate bespoke applications from the current system to a newer version can lead some to believe that their apps need to be rewritten from scratch.

“To ensure that they can complete their migration smoothly, IT teams in the NHS – and the wider public sector – should use compatibility containers to ‘lift and shift’ their applications to the newer Windows 10, reducing

complexity in the process as well as saving time and money. This would provide a protected system environment for the NHS that would help to prevent another cyber attack of the same scale as WannaCry striking again."

Despite the clear patching problem, the Department of Health could have mitigated with added layers of security, referencing networking segmentation as one example. Hubert Da Costa, VP and GM EMEA at Cradlepoint would agree: "Deploying air-gapped – or parallel – networks either physically or virtually, can limit the attack surface should one of several security mechanisms fail." But how does this process work in reality

"A parallel network takes non-essential or non-secure applications off the secure network. This can be achieved virtually – by overlaying the network with a software-defined perimeter and/or routing hardware – or physically, by creating a separate network connected via 4G LTE.

"Isolating mission-critical devices makes it easier to monitor, lock down and prevent hackers from crossing over from one application to another. This would allow the NHS to maintain a higher level of security for its network, and its patients' sensitive data."

But missing layers of technology are not the only problem here. An inherent technology skills gap within healthcare is claimed to be a contributing factor to the mass aftermath of Wannacry, with three potential roles available for every cyber expert. This means that naturally the private sector can afford to pay potential employees higher salaries than the NHS, and this is a fact that is causing talent to reside elsewhere.

The revelation that there are only 18-20 suitably skilled cyber security experts working for NHS Digital should come as no surprise according to Steve Wainwright, Managing Director EMEA at Skillsoft, who claims IT education should be made an intrinsic part of employee development through online tools. "Skilled teams aren't made by magic, they are created through good recruitment and effective training. Forward-thinking organisations are turning to intelligent eLearning solutions that provide engaging, multi-modal content and tailored learning paths. This approach can meet each individual's learning requirements, and encourages people to fit learning into their working day when and where they can."

### **'Wider lessons for government'**

The report gives the rather uncomfortable conclusion that, had the attack not taken place in the summer or on a Friday, it could have been much worse. This like stands as little consolation for those affected given the severity of the situation, and the repercussions for businesses affected by cyber attacks in the future looks bleaker still: "With GDPR on the horizon, it's not going to get any easier," comments Luke Brown, VP EMEA at WinMagic. "Falling victim to cyber criminals is a simple matter of fact these days."

It's not all doom and gloom, however. Under the new data regulation that comes into effect on May 25, businesses that do fall under attack can still save themselves a hefty penalty by implementing tools that make data unreadable. "In the event of a data breach, encryption acts as a last line of defence, making data illegible when in the hands of unauthorised parties," said Brown.

Ultimately, this latest government report proves that, even one year on from the worse cyber attack the UK public sector has seen, the NHS has a long way to go before remedying the deep-rooted issues that proliferated the spread of WannaCry. This is particularly worrying as we increasingly hear stories about other areas of critical national infrastructure, such as utilities companies, becoming targets.

What is clear across all areas of this extensive report is that investment in tools, technology and talent is vital for impeding the force with which another cyber attack could strike. Experts in technology will welcome the recent news that £150 million is to be spent by the NHS to bolster its defences, and Jan van Vilet, VP and GM EMEA at Digital Guardian, claims that "the issue of funding is always going to be a hot potato when it comes to the NHS," but that "two obvious areas to start would be improving user training and awareness."

It can only be hoped that the negative furore around this incident will mark the start of a new wave of heightened, collective consciousness when it comes to IT resilience in the face of adversity, both in the health service and beyond.



# WannaCry



# Build your cloud skills and become an AWS Cloud expert.

[aws.amazon.com/training](https://aws.amazon.com/training)



training and  
certification

# The Big Interview: Marc Avery

**Marc Avery**, CISO at smart meter network company DCC, tells Detect & Defend how he developed as an information security professional, how, as a recruiter, he gets around the UK's STEM skills gap and why a major data leak at HMRC in 2007 changed his perspective on the industry.





## What first prompted your move into information security?

As with most security professionals starting their career in the late 90's or before, I kind of stumbled into it without really knowing what it was! Information Security as a career was quite rare back in 2000 and most roles were based upon IT skills and security wasn't something that was a unique role. My career was a natural progression from IT into IT Security and then Information Security.

## Take us through your career to date

I started my career after university supporting IT and Networking Infrastructure at the Jaguar plants in the Midlands. Information Technology was pretty new to me and I didn't even own a computer at the time! It was the security aspect of IT that I naturally found interesting and hence, I then progressed into IT Security and Information Security roles within TNT Express Ltd. It was during this time in 2007 that the HMRC Child Benefit Data Loss event occurred which for me, was a game changer in terms of large scale loss of Personal Data.

I then had a short stint in a facilities management company who held a number of contracts with Central Government. This provided me with a massive exposure to some of the challenges within the Public Sector which I found a really interesting and a welcome challenge. This exposure continued as I moved to a large outsourcing organisation and worked on a number of high profile Central and Local Government projects.

I have now been working on the Smart Metering Programme for almost five years which is definitely the highlight so far. The opportunity to help shape and secure one of the UK's biggest networks which unlocks so much consumer and market potential is really exciting.

## What are your main responsibilities today?

Functionally I am accountable for all aspects of Information Security, Privacy and Business Resilience. Larger organisations may typically separate these responsibilities out to avoid conflicts but I also see the benefit of bringing them together under the CISO because of their importance and common potential impact on the business.

If that wasn't enough, I am fortunate enough to be a direct report to the CEO and a member of the Executive Team which allows me to contribute and be part of the decision making for all other aspects of the business such as People, Technology and Operations.

The powerful thing for the CISO in this scenario is that this responsibility is reciprocal i.e. it is the responsibility of other Executive Team members to contribute and help make decisions on security matters. CEO's pay attention...this is how to effectively embed security within your organisation!

## What drives you to get out of bed in the morning?

I am very honest about my career aspirations and as long as there is a challenge in front of me then I will continue to get out of bed and go to work. I would not consider myself a perfectionist but I do expect the basics to work and in security terms, getting the basics right isn't always as simple as it sounds! Building a security function and an organisation that is capable of driving such a revolutionary transformation within the energy industry is a pretty big challenge....and I sometimes choose not to think about it too much! As individuals I think it is extremely important for us to always seek out new challenges.

## What would you say are your key strengths and how are these useful to your work?

Simplicity, transparency and a willingness to learn. I tell people that the concept of security is pretty simple and shouldn't be made into a complex industry. For many years the security guys held all of the answers and we were seen as disabling the business but I believe in making security as simple and as accessible as possible. The key benefit is that with the correct control framework in place, you put a lot more understanding and decision making into the business, resulting in an easier return on investment discussion.

## What would you say is your biggest professional challenge?

I spent many years as a consultant working in relative isolation but building a good team around me was a really big challenge. It is true that you are only as good as your team achieving that has been hard. In a saturated market with well-publicised skills shortages, I have found myself looking less at technical skills and certifications and looking more at the experience and characteristics of individuals.

Diversity and positive inclusion is becoming more and more important for organisations and this is particularly true within the security sector. We need to continue to educate and develop in non-traditional populations so that we can continue to maintain the good teams we have and ensure they are resilient for the future.

## What training have you received and how has this helped you progress?

I do believe that good security professionals should have a foundation in some kind of technical skill; be that IT, Engineering or a Science. The art of analysing a problem and finding the right solution is critical and that is why I am supportive of STEM within schools. I did some technical IT Security training when I was at the start of my career and was very proud of being a Certified Ethical Hacker!

As a consultant, I then naturally opted for either broader certifications such as CISSP or CISM or specialist certifications such as PCI-DSS. I found that the more generalist Information Security qualifications tend to 'teach' you less but are beneficial in terms of demonstrating to clients or future employers a good baseline understanding managing security risk.

As I moved into more of a leadership role, formal skills training became less valuable than networking and good simple conversation but you certainly can't get by on that alone. I believe it is important to spend time creating and regularly updating a personal development plan which delivers a good balance of formal training, qualification, self-taught skills and knowledge gathering.

## What characteristics do you think make a great CISO?

Without doubt, a willingness to step outside of your security comfort zone and understand how your business really operates is key for a successful CISO. Only then can you contribute something of value back to the business which in-turn earns you the right to expect others to help you with your security programme.

## What do you see as the key threats online (generally speaking) now and in the near future?

1) Near-term continued prevalence of relatively low-complexity untargeted attacks such as Ransomware and Phishing for criminal gain or denial of service from poorly secured mass-market IoT devices.

2) The diversity in the way in which technology is being applied is growing at a rapid pace which presents criminals and other threat actors with a broader opportunity for exploit. This has been seen more recently with Cryptocurrency attacks but we should be conscious about our increased adoption of technology into our lifestyle.

## Where do you see yourself in five years?

Hard to say but I don't think I will be doing something that is 'routine'. It is important to be challenged and the most valuable thing about the security profession is that the subject matter can be applied in a fairly standard manner in any sector.

I had never worked in the Energy sector before I started in my current role and I was able to adapt quickly and embed good security practice fairly quickly without affecting the business. My next role could be in any other sector but it will have to be just as; if not more exciting and challenging than this.

## What is your advice to others with their eyes on a CISO role in future?

Get yourself a well-rounded set of skills and experiences; as irrelevant as they may seem at the time, they may come in useful. Capture and celebrate your successes because nobody else will; confidence is something you will need a lot of. Most importantly, don't just focus on security matters, the only way you can enable the business is by understanding it as much as anybody else.







**Learn anywhere, anytime.  
Live. Virtual. On-demand.**

## Google Cloud Training

Equip yourself with the technical skills to leverage Google Cloud technology. Learn technical skills and best practices from Google experts and take advantage of self-paced labs for hands-on training.

- Learning tracks to build skills in specific areas of expertise
- 30+ courses for foundational to advanced learning
- 150+ hands-on labs let you practice with our technologies
- Updated curriculum keeps pace with evolving technologies

---

[cloud.google.com/  
training](https://cloud.google.com/training)

## Google Cloud Certified

Show the world that you have the skills and expertise to leverage Google Cloud technology in a way that transforms businesses.

Professional and Associate level certifications so you can:

- Gain industry recognition
- Validate your technical expertise
- Take your career to the next level

---

[cloud.google.com/  
certification](https://cloud.google.com/certification)



# Reskilling the Cybergap

Written by **James Aguilan**, QA Cyber Security Researcher.

McAfee, security firm, states that UK education systems are providing minimal insight into careers in Cyber Security. Government bodies have addressed the skills gap with plans to triple the amount of Computer Science teachers in schools and introducing a National Centre for Computing. CWJobs found that 65% of employers thought the Government had not invested enough in training the next generation of tech employees, which is causing a gap in the field of Cyber Security. Notably, with recent high profile Cyber-attacks including Uber and NHS data breach, the importance of robust Cyber Security is clear, or at least it should be. Here I discuss the concern with Cyber Security gaps:





## **Skill Shortage in Secure coding, Cyber Security and Cloud Migration are Widespread**

The main concern for the shortage in Cyber Security is the inadequacy preparing for the demands of technology. Specifically, within secure coding and cloud migration. 31 percent of Cyber Security professionals state that organisations have a shortage of application security skills. When you think about the whole Digital Transformation trend going on across all industries, it's easy to conclude that this mismatch can only result in a lot of insecure code being developed and deployed. Additionally, 29 percent of Cyber Security professional state organisation have a shortage in Cloud Security skills. ESG research indicated that 42 percent of organisations currently use IaaS and/or PaaS services today, and these percentages are poised to increase in the future. Beyond this, survey respondents point to skills shortage in areas like Penetration Testing, Risk/Compliance Administration and Security Engineering. The overall picture is bleak – many organisations may not have the right skills and resources to adequately secure new business and IT initiatives and may also lack ample skills to detect and respond to incidents in a timely fashion.

## **Lack of Readiness for a Cyber Security Attack**

With numerous high-profile security breaches in recent years, UK businesses are facing greater pressure to ensure their security measures are up-to-date and in place. However, despite the increase in both attacks and warnings, many companies remain complacent as some believe they can't be hacked. As a result, they lack the right approach or plan to protect themselves against attacks. With organisations confidence so low, it is unsurprising only 50 percent of Small Business Enterprises (SME) are prepared for a cyber-attack. On the other hand, the other half of organisations are said to look for Cyber Security skills when recruiting new tech talent. Experis research found that 65 per cent of employers thought the government had not invested enough in training the next generation. Beyond the recent budget however, the Government has taken steps to address the problem of a skills shortage. For example, the UK Government launched the National Cyber Security Strategy in 2016 – part of which incorporates a plan to make sure there is a constant supply of home-grown Cyber Security talent. However, 80 per cent of technology organisations stated that they are currently struggling to fill Cyber Security roles, with 30 percent believing this is due to an industry skills gap.

## **Educating the Cyber Skills Gap**

In 2017, GCSE/GCE/Degree grades have marginally improved. However, there are still systemic issues when it comes to Cyber Security. So how can businesses address the skills gap? Organisations can deploy an innovative recruitment process in a bid to resource the skills that they can't currently find. An example and a good place to start is implementing Gamification. The National Cyber Security Centre's (NCSC) codebreaking exercise is a playing field for all applicants that the recruitment process can use to find prospective candidates from all backgrounds. Not only did it enable NCSC to see how well potential candidates would fare on the job, it gave them access to a larger pool of raw talent. In turn, this results in a greater diversity of skills – an essential asset for any business looking to contend with a threat landscape that evolves by the minute.

## **Introduction to Apprenticeships and The CyberFirst Programme**

Alternative to the traditional education system, another route to bridge the security gap is for businesses to offer Apprenticeship Programmes for young people looking to get into the industry. A Cyber Security Apprenticeship Programme involves the hiring of raw talent after having completed their GCSEs or GCE. Apprentices can work, develop new skills on the job, while learning and earning at the same time. This way, Apprentices can study for the certifications they require, with businesses also getting the exact Cyber Security skills they need to protect their organisation from threats. What's more, Apprentices don't have to attend University or College to do Apprenticeships. Taking on Apprentices is the perfect way for businesses to nurture a robust Cyber Security team that is fit for purpose and has the technical and practical know-how to fend off Cyber Threats. Introducing Cyber Skills and awareness early is often key to encouraging the next generation to consider Cyber roles later on. The CyberFirst Programme targets children from GCSE age onwards. – CyberFirst is a collaboration between NCSC, QA and The Small Piece Trust. It is a pivotal part of the UK Government's National Cyber Security Programme and aims to embed Cyber skills to give talented young people the support, experience and exposure they need to become the Cyber Professionals of the future.

To prevent a worst-case scenario—technological change accompanied by talent shortages, mass unemployment and growing inequality—reskilling and upskilling will be critical. Every industry is being impacted by the rise in technology and an increased reliance on the Internet of Things (IoT). Thus, businesses are being forced to rethink the way they work and turn to new technologies to remain successful. The upsurge will see countless new roles created as employers seek digitally-savvy workers to help them master these technologies. However, to thrive the modern employee will need to learn new skills and have some form of Cyber Awareness. Apart from a reform in basic education, it is simply not possible to weather the current technological revolution by waiting for the next generation's workforce to become better prepared. In its place, it is critical that businesses take an active role in supporting their current workforces through reskilling and upskilling. This approach of cross collaboration between Business Sectors, the Government and the Education System is mandatory, if millennials and future generations are to become the sharp, aware and talented Cyber defenders our societies need.

# AI for fraud detection: beyond the hype

By **Sundeep Tengur**, Senior Business Solutions Manager at SAS



The financial services industry has witnessed considerable hype around artificial intelligence (AI) in recent months. We're all seeing a slew of articles in the media, at conference keynote presentations and think-tanks tasked with leading the revolution. AI indeed appears to be the new gold rush for large organisations and FinTech companies alike. However, with little common understanding of what AI really entails, there is growing fear of missing the boat on a technology hailed as the 'holy grail of the data age.' Devising an AI strategy has therefore become a boardroom conundrum for many business leaders.

How did it come to this – especially since less than two decades back, most popular references of artificial intelligence were in sci-fi movies? Will AI revolutionise the world of financial services? And more specifically, what does it bring to the party with regards to fraud detection? Let's separate fact from fiction and explore what lies beyond the inflated expectations.

## Why now?

Many practical ideas involving AI have been developed since the late 90s and early 00s but we're only now seeing a surge in implementation of AI-driven use-cases. There are two main drivers behind this: new data assets and increased computational power. As the industry embraced big data, the breadth and depth of data within financial institutions has grown exponentially, powered by low-cost and distributed systems such as Hadoop. Computing power is also heavily commoditised, evidenced by modern smartphones now as powerful as many legacy business servers. The time for AI has started, but it will certainly require a journey for organisations to reach operational maturity rather than being a binary switch.



```
If “OffSec” == 1;  
do $unlock_root;
```



**Getting locked out is no fun.  
Get real-world, hands-on  
Penetration Test training from  
the creators of Kali Linux.**



**OFFENSIVE  
security**

Contact us at [info@offensive-security.com](mailto:info@offensive-security.com)  
or through QA at [cyber@qa.com](mailto:cyber@qa.com)

## Don't run before you can walk

The Gartner Hype Cycle for Emerging Technologies infers that there is a disconnect between the reality today and the vision for AI, an observation shared by many industry analysts. The research suggests that machine learning and deep learning could take between two-to-five years to meet market expectations, while artificial general intelligence (commonly referred to as strong AI, i.e. automation that could successfully perform any intellectual task in the same capacity as a human) could take up to 10 years for mainstream adoption.

Other publications predict that the pace could be much faster. The IDC FutureScape report suggests that “cognitive computing, artificial intelligence and machine learning will become the fastest growing segments of software development by the end of 2018; by 2021, 90% of organizations will be incorporating cognitive/AI and machine learning into new enterprise apps.”

AI adoption may still be in its infancy, but new implementations have gained significant momentum and early results show huge promise. For most financial organisations faced with rising fraud losses and the prohibitive costs linked to investigations, AI is increasingly positioned as a key technology to help automate instant fraud decisions, maximise the detection performance as well as streamlining alert volumes in the near future.

## Data is the rocket fuel

Whilst AI certainly has the potential to add significant value in the detection of fraud, deploying a successful model is no simple feat. For every successful AI model, there are many more failed attempts than many would care to admit, and the root cause is often data. Data is the fuel for an operational risk engine: Poor input will lead to sub-optimal results, no matter how good the detection algorithms are. This means more noise in the fraud alerts with false positives as well as undetected cases.

On top of generic data concerns, there are additional, often overlooked factors which directly impact the effectiveness of data used for fraud management:

- Geographical variances in data.
- Varying risk appetites across products and channels.
- Accuracy of fraud classification (i.e. which proportion of the alerts marked as fraud are effectively confirmed ones).
- Relatively rare occurrence of fraud compared to the huge bulk of transactions; having a suitable sample to train a model isn't always guaranteed.

Ensuring that data meets minimum benchmarks is therefore critical, especially with ongoing digitalisation programmes which will subject banks to an avalanche of new data assets. These can certainly help augment fraud detection capabilities but need to be balanced with increased data protection and privacy regulations.

## A hybrid ecosystem for fraud detection

Techniques available under the banner of artificial intelligence such as machine learning, deep learning, etc. are powerful assets but all seasoned counter-fraud professionals know the adage: Don't put all your eggs in one basket.

Relying solely on predictive analytics to guard against fraud would be a naïve decision. In the context of the PSD2 (payment services directive) regulation in EU member states, a new payment channel is being introduced along with new payments actors and services, which will in turn drive new customer behaviour. Without historical data, predictive techniques such as AI will be starved of a valid training sample and therefore be rendered ineffective in the short term. Instead, the new risk factors can be mitigated through business scenarios and anomaly detection using peer group analysis, as part of a hybrid detection approach.

Yet another challenge is the ability to digest the output of some AI models into meaningful outcomes. Techniques such as neural networks or deep learning offer great accuracy and statistical fit but can also be opaque, delivering limited insight for interpretability and tuning. A “computer says no” response with no alternative workflows or complementary investigation tools creates friction in the transactional journey in cases of false positives, and may lead to customer attrition and reputational damage - a costly outcome in a digital era where customers can easily switch banks from the comfort of their homes.

## Holistic view

For effective detection and deterrence, fraud strategists must gain a holistic view over their threat landscape. To achieve this, financial organisations should adopt multi-layered defences - but to ensure success, they need to aim for balance in their strategy. Balance between robust counter-fraud measures and positive customer experience. Balance between rigid internal controls and customer-centricity. And balance between curbing fraud losses and meeting revenue targets. Analytics is the fulcrum that can provide this necessary balance.

AI is a huge cog in the fraud operations machinery but one must not lose sight of the bigger picture. Real value lies in translating ‘artificial intelligence’ into ‘actionable intelligence’. In doing so, remember that your organisation does not need an AI strategy; instead let AI help drive your business strategy.



# How not to code

*At SCADEMY Secure Coding Academy, we are focused and dedicated to a clear goal. The ever-evolving landscape of cyber crime makes the continuous application security training of each and every developer a must. Developing your engineers into motivated secure coders by changing their coding habits is essential to keep you renowned as a trusted and reliable vendor.*

## **WHAT ADDED VALUE DO DEVELOPERS GET AFTER HAVING COMPLETED OUR COURSES?**

*Your developers will among others*

- *Understand basic concepts of security, IT security and secure coding*
- *Understand the architectural protection techniques, along with their weaknesses*
- *Learn about typical coding mistakes and the best practices to avoid them*
- *Be informed about recent vulnerabilities in various platforms, frameworks and libraries and learn how to handle them*
- *Have a practical understanding of cryptography and some recent attacks against cryptosystems*
- *Learn about denial of service attacks and protections*
- *Understand security testing methodologies, get practical knowledge in using security testing techniques & tools*







# **Are you an IT Trainer or Coach looking for a new challenge? Or do you have skills in Cyber and Technology?**

How about working for one of the UK's largest Education providers, supporting apprenticeships and industry professionals in career and personal development.

## **What is the role?**

With our support, you will deliver/coach using face to face or e-Learning techniques to help individuals and organisations achieve their potential through world-class skills training, talent and learning solutions.

Roles are available in multiple UK locations, you will be delivering/coaching both public scheduled and bespoke courses for all appropriate areas of QA's Portfolio.

## **How will we support you?**

From day one you will be assigned a co-pilot/buddy to help get you up to speed with our processes and ensure you can help deliver our award winning programmes.

## **Find out more**

Visit our website and search out latest vacancies

**CAREERS.QA.COM**





# Become part of something special.

## The benefits

We are offering a base salary of up to Salary per annum (dependant on experience), private pension as well as **25 days holiday**.

**2 days paid Charity work** each year for a charity of your choice (which we actively encourage), **3 days of additional training** which does not need to be relevant to your role from our very own course selection (1,200 to be precise), **subsidised gym membership** and **cycle to work scheme**.

## About QA

As one of the largest learning services organisations in the UK. We like to help develop skills and capabilities for everyone from apprentices to business leaders. With our HQ in London and 20 training centres nationwide, QA Group is comprised of four fast-growing divisions - QA Learning, QA Apprenticeships, QA Consulting and QA Higher Education - all of which deliver innovative, award winning (2016 Top 20 IT Training Companies List) & ever evolving skills solutions.

## Find out more

Visit our website and search out latest vacancies

**CAREERS.QA.COM**



# Cryptocurrency Mining: Does the reward outweigh the cost?

QA Cyber Security Researcher, **James Aguilan**, looks at the practice of mining cryptocurrency.





Before, hackers would try to gain access to systems with the aim of leveraging profit through tricking users into clicking a malicious links or MITM. Since the rise of cryptocurrency, there has been a new mark in the world of cybercrime. Hackers are predominately less keen on our money – and more into our computer power instead. As a result, the chips that power our devices are being silently hijacked for mining cryptocurrency.

Hackers can use computer power to complete the complex mathematical puzzles that validate a block of cryptocurrency transactions. If a hacker manages to solve those tricky sums, they're rewarded. However, this is no easy task. Nonetheless, enthusiastic miners have found themselves investing huge sums in computer hardware in the hopes of winning these rewards, but as cryptocurrencies gain more power, more power is required to mine them.

One of the ways in which nasty mining tools end up on our device comes from the same method a malware would – clicking on a malicious link or opening file from emails. Zero-day attacks and new threats are appearing more constantly, as in recent news many android users were infected with a tool that mines a cryptocurrency called Monero (XMR). The result of such scheme has infected more than 500,000 window users and generated \$3.6 million. More recently, malicious mining software has introduced its way onto mobile devices via text messages, rogue links on FB messenger and even via maliciously embedded google ads. As mentioned earlier, hackers are 'silently' hijacking power making victims unaware of what is going on with their infected slow running device.

Despite the potential rise of cybercrime, the rise of cryptocurrency has also caused a flash of positive global effect. As of recently, UNICEF have appealed to gamers with powerful Graphical User Interface (GPU) to mine Ethereum to help raise money for children in Syria. In addition, the GPU are now selling to gaming and mining customers which facilitates the mining of a certain cryptocurrency. Beyond the world of graphics card, demand has soared for dedicated mining rigs, such as AntMiner S9.

Miners require an enormous amount of electricity. The main expense for miners is the power and this helps to explain why hackers are now trying to get that power for free by stealing it. Anyone thinking 'if you can't beat them, join them' should maybe think again. Cryptomining is outweighing to be impractical and the volatility of the market means that the amount spent on mining coins might be better spent buying the coins from an exchange service.



## **James Aguilan**

### **Cyber Security Researcher**

James has worked on many high complexity eDiscovery Projects and Forensic Investigations involving civil litigation, arbitration and criminal investigations for large corporation and international law firms across UK, US, Europe and Asia. James has assisted on many notable projects involving: one of the largest acquisition and merger case of all time – a deal worth \$85 billion, multijurisdictional money laundering matter for Government bodies, and national cyber threat crisis including the more recent ransomware, phishing campaigns, and network intrusion. James has comprehensive knowledge of the eDiscovery lifecycle and forensic investigation procedures in both practise and theory with deep focus and interest in Forensic Preservation and Collection and Incident Response. In addition, He holds a first class bachelor's degree in Computer Forensics and is accredited as an ACE FTK certified examiner.

# Time To Get Tough On Cyber Crime

By **Simon McCalla**, CTO of Nominet

Experience shows that along with its many benefits, the internet is also an ideal breeding ground for cyber crime. The toxic mix of anonymity and a vast audience is profitable for those with criminal intent.

The growing consumer interest in spending money over the internet is only adding fuel to the fire.

Online spend grew 12.6% from 2015 to 2016, with expectations that national spending will approach £70 billion in 2017 [Retail Research]. Concurrently, the cost of online scams is rising: Action Fraud claims fraud and cyber crime cost the UK nearly £11bn in 2015/16.

However, not all incidences are reported – the true cost could be much higher. Cyber crime covers a wide range of offences, from online abuse, financial fraud, online shopping scams and hacking to the growing occurrence of so-called romance fraud. The last refers to an overseas ‘lover’ asking for money, whether for flights or other needs, and the number of victims hit a high in 2016: almost 4,000 people paid out over £39m [National Fraud Intelligence Bureau]. With the rise of digital devices and infiltration of data networks in our lives, it’s easy to understand why the cost and prevalence of online scams are growing. Thankfully, national efforts in prevention and prosecution have increased too.

Just last month, the City of London confirmed plans for a new court complex to focus on fraud and cyber crime, both currently at “epidemic proportions” according to Sir Tom Winsor, Chief Inspector for Constabulary for England and Wales in an interview on BBC Radio Four. This is supported by the work of Action Fraud, the UK’s national fraud and cyber crime reporting centre. This Government-funded body provides guidance to those who have been caught out and share warnings on current threats. There is plenty of media attention to add to the mix, with high profile cyber attacks inciting an atmosphere of fear, but is this translating into better protections by the individual? Unfortunately, probably not.

The research from get Safe Online and Action Fraud is stark: 42% of Britons use the same password for multiple accounts, 23% never update their privacy settings on social media, and 12% don’t change passwords even when their company asks them to. Alarming, of people who have already been victims of cyber crime, over a third thought nothing could be done. That isn’t to say there is a shortage of advice on protective actions, including updating software and passwords, researching common scams and treating all online communication with caution. Fundamentally, the crucial change is one of attitude.

We can no longer afford to be ambivalent about the risks associated with using the internet, and must learn to own our vulnerabilities as a pivotal part in the rising crime rate.

Part of this is understanding why we fall foul of online criminals when physical aggression is taken out of the equation. Research into the issue has revealed that social engineering is often at the root.

We tend to pay more attention to information that supports our existing beliefs thus ignore the warning signs, or else we are preyed upon in moments of desperation or distraction. Scammers promote a sense of urgency and often have detailed information about us, fostering a false impression of authenticity.

Older and younger people, or those with cognitive impairments, are easy targets, but we are all vulnerable for our innate kindness and an over-confidence in our judgement. We harbour a desire to please, stay out of trouble and grab a bargain, thus we fall prey. Having an awareness of these vulnerabilities could help increase awareness of the potential for abuse, and hopefully improve our safe responses.

Try telling someone else about anything you are unsure about – sharing removes the emotional reaction and could help you think more clearly. It is also worthwhile identifying your own vulnerable attributes so you can be sensitive to attempts to infiltrate your systems.

Cyber scams and fraud happen almost constantly; you are now 20 times more likely to be robbed at your computer than in real life [Crime Survey of England and Wales]. As we move closer to Christmas, it seems likely that criminals will maximise their opportunity to manipulate your last minute shopping rush.

We must all get tougher: be vigilant, be alert and be sceptical about everything that arrives in your inbox. Guard your assets carefully and take all steps to protect yourself, even if it seems unnecessary. We needn’t feel powerless to protect ourselves from cyber crime. There are no prizes for staying safe, but the cost of not doing so is too high a risk.



# Oracle's Security Learning Subscription

**Cybercrime and hacking costs the global economy about 300 billion dollars per year!**

Want to learn how to protect your company? Get all the training you need to be proficient on security with **Oracle's Security Learning Subscription.**

## Key Features:

- 12 months of 24/7 access
- Comprehensive training with product demonstrations
- Delivered by Oracle experts
- Guided learning path
- Quizzes available for key areas
- Dynamic updates for new features and product enhancements



**Preview at:**



**ORACLE®**

**Contact us:**  
**0845 777 7 711 (Toll-Free)**  
**[edenrollment\\_uk@oracle.com](mailto:edenrollment_uk@oracle.com)**



# HACKERS ARE HERE. WHERE ARE YOU?



## Get Globally Recognized Cybersecurity Credentials!

**C|EH**

### Understand Hacker Mindset

- Master Attack Vectors
- Hands-on Program
- ANSI 17024, NICE 2.0 FW

**ECSA**

### Master the Methodology

- Comprehensive Methodologies
- Create Pentesting Report
- Industry Recognized Exam

**C|EH (Practical)**

### Validate White-Hat Skills

- Mimics Real-Life Networks
- Remote Live Proctoring
- Master Ethical Hacking

**ECSA (Practical)**

### Validate Pentesting Skills

- Advanced Network Scans
- Test Skills Beyond Knowledge
- Show Pentesting Methodology

Advanced Penetration Testing Program

**L|PT (Master)**

### Validate Your Mastership

- Test Perseverance & Focus
- Time-bound Gamified Design
- Remote Live Proctoring