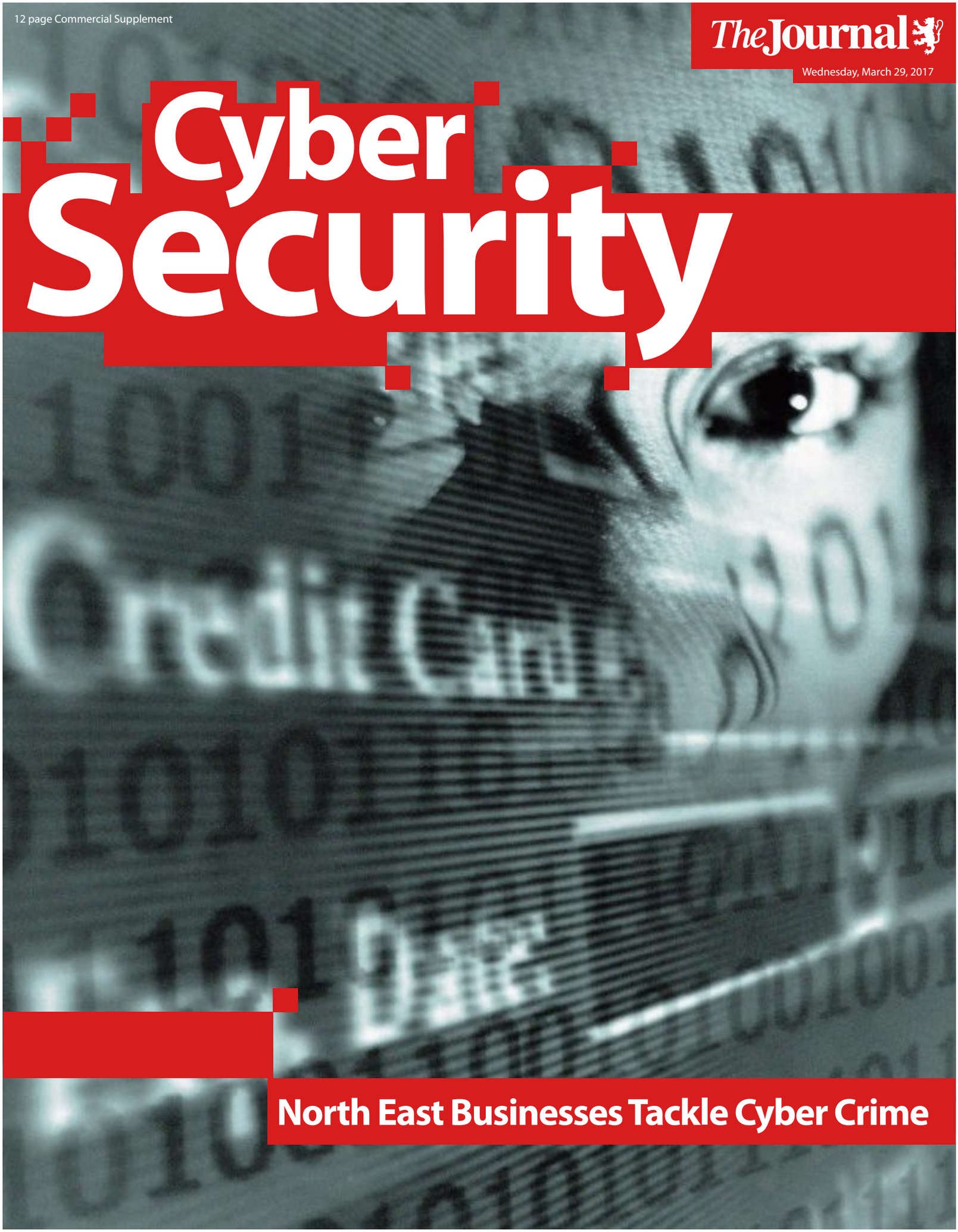
12 page Commercial Supplement

The Journal

Wednesday, March 29, 2017

Cyber Security



North East Businesses Tackle Cyber Crime

Microsoft Partner
Gold Midmarket Solution Provider
Gold Small and Midmarket Cloud Solutions
Gold Collaboration and Content
Gold Datacenter
Gold Enterprise Resource Planning
Gold Customer Relationship Management
Gold Cloud Productivity

The cloud and beyond.

Discover Technology that will transform your business.

futuretech. WEBINARSERIES

Covering new revolutionary applications from Microsoft to crucial IT security from Sophos, TSG's Futuretech webinars and events showcase ground-breaking technology.

Not only will we unravel the concept of 'digital transformation', we'll also break it down into its component parts to ensure that Futuretech is relevant to everyone from the CEO or the FD to the technical team.

We'll be looking at key topics such as:

- **Business Continuity**
- **Office 365**
- **Security**
- **Hosted Telephony**
- **Business Intelligence**

Join one of TSG's webinars and discover technologies that will dramatically enhance security, communication, collaboration and process efficiency in your business, as well as making your business mobile and flexible to maximise productivity and profitability.

Tel: 0333 220 0777 tsg.com/events

TSG®
TECHNOLOGY SERVICES GROUP

Microsoft Office 365 SharePoint NINTEX TERMSET Gamma Qlik Pulsant SOPHOS datto

Bigger the firm, bigger the risk

CYBER security breaches cost British businesses almost £30 billion in 2016, according a new survey.

Beaming, the business ISP, reveals that more than half of British businesses fell victim to some form of cybercrime last year.

Beaming's study, which was conducted by researchers at Opinium, indicates that 2.9 million UK firms suffered cyber security breaches nationwide last year, at a cost of £29.1 billion.

Computer viruses and phishing attacks were the most common corporate cyber threats faced by British businesses last year, in both cases impacting 23% of the businesses surveyed.

Just under a fifth (18%) of businesses suffered some form or hack or data breach in 2016.

The risk of cyber security breaches increases with business size. 71% of organisations with more than 250 employees were victim to some form of cyber crime last year, compared to less than a third (31%) of enterprises with fewer than 10 people.

Sonia Blizzard, managing director of Beaming, explained: "Large organisations are more likely to become a victim of cyber crime due to being more valuable targets and because employees are often the weakest link in the cyber security chain. They are also more resilient as they have resources to aid their recovery. Successful cyber attacks on smaller businesses are less frequent but cause disproportionately more harm. It is encouraging they are taking the threat more seriously and investing in their cyber defences, as a single attack could potentially break them."

> File photo dated 06/08/13 of a woman using a laptop as the cost of fraud to Britain rose above £1 billion for the first time in the last 12 months.

In an effort to protect themselves from the cyber criminals, more than half a million British businesses took out cyber insurance policies for the first time in the last 12 months. Nearly 20% of UK companies are now covered for losses associated with cyber security breaches and data theft.

And adoption of new cyber security technologies increased the fastest amongst smaller businesses in 2016. Demand for unified threat management devices, web application firewalls and network access control systems increased by 71%, 59% and 45% respectively amongst those employing between 10 and 49 people.

Professor Alastair Irons, the academic dean for the faculty of computer science at the University of Sunderland and expert adviser on cyber security, believes digital crime is high on the agenda for Government too.

"Cyber crime is now a top priority for the UK Government as we saw with the recent opening of the National Cyber Security Centre (NCSC) to identify threats to individuals and organisations," he said.

"It's been reported in the last three months alone there were 188 cyber attacks against the nation.

"The threat has never been greater, as a nation we are defending attacks from everywhere, it's a cyber war of pandemic proportions and is never going to stop. No matter how much we defend and prepare, it's always going to be there.

"Whether it's nation-state attacks, the hacking of large corporations or an individual's credit card becoming compromised, no one is immune from becoming a victim."

Cyber security - the fightback starts here

Stew Hogg
Information security lead at Waterstons

THE Government's Cyber Security Breach Survey 2016 identified that 69% of businesses say cyber security is a top priority for senior managers, yet only 29% had established formal security policies and only 10% had a formal incident plan. So if this is a top priority, why have so few embarked upon the journey to protect their organisation from attack?

We think the trouble may be the alarmist headlines that describe state-sponsored hackers, or teenagers in their bedroom bringing large corporations to their knees, even the devices in your house being compromised to launch attacks on a global scale. What's more, we're told it could be us next and with all this scaremongering it's hard to know what steps to take first.

At Waterstons we believe that every organisation, large or small, can take simple steps to greatly improve their security defences by engaging their business, implementing a number of basic security controls and over time evolving their approach to provide a holistic defence against a range of security threats.

Getting the basics right

All too often organisations can fail to get the basics right when it comes to security, leaving them open to drive-by attacks from opportunistic cyber criminals.

However, starting the fightback can begin with a few basic steps such as those outlined within the Cyber Essentials standard. We find by focusing on these key areas, from firewall security to anti-malware protection, an organisation can dramatically reduce the risk of a cyber attack.

The next step is Cyber Essentials PLUS, which involves technical network scans to validate that the organisation has indeed guarded against the most common security threats.

By engaging with a certification body, most organisations can attain Cyber Essentials in a matter of weeks, providing reassurance to customers that they've got the basics right.

Every organisation can take simple steps to improve security defences

Stew Hogg

Engage your people

For a long time security professionals have claimed that "people are the weakest link".

However, we're strong believers that they're actually your greatest asset.

People can innovate, spot problems, design creative solutions and work with you to secure an organisation's other important assets.

In practical terms this means ditching outdated security controls such as regular password changes and instead working with colleagues to understand the key risks and find measures which optimise security without stifling innovation or inhibiting the business.

Go on the journey of security maturity

Once you've engaged your people and put in the simple controls you're ready to start the journey towards security maturity. Often this can be aided by using standards such as ISO 27001:2013 which are designed to give you a framework to manage risk, implement best practice security and continually improve it across your business.

In the face of the General Data Protection Regulation this will become increasingly important as every business needs to be aware of the information they hold, how it's protected and be able to demonstrate to their customers that protecting their personal data is a top priority. By starting with the basics, all organisations can embark on this journey of security maturity and start the fightback against cyber crime.

Safeguard your data, safeguard your business

CHRIS GRAHAM, head of Watson Burton law firm's commercial litigation, fraud and employment team – and member of the management committee of the NE Fraud Forum - explores the challenges facing businesses in the cyber security arena

> Chris Graham, left, with Jonathan Smith, IT manager at Watson Burton and CEO Patrick Harwood

IT'S startling to think that the UK is second only to Colombia on cybercrime's global league table.

Yet that's exactly the case, according to Kroll's recent Global Fraud and Risk Report, which stated that 92% of executives at British companies had experienced an attack or information loss in the last year.

Cybercrime is very much in the headlines: last month, for instance, saw the Association of British Travel Agents hit by a hacking incident, putting the records of about 43,000 people at risk.

It's very clear, therefore, that businesses need to put both technological and legal measures in place to mitigate against the risk of cybercrime and data theft. That risk may come from both external threats, such as hackers, but also staff or former employees who may have a motive to access confidential information.

Ex-employees may wish to access data to give their new firms a competitive advantage, while current staff may exploit security loopholes to commit fraud.

Any business can fall victim, from large multi-nationals to SMEs, but especially vulnerable are firms which have developed their IT systems and associated policies on an ad hoc basis.

It's also vital that businesses quickly access specialist legal advice if a data breach or cyber security incident comes to light. It may be a case of damage limitation, but the sooner action is taken, the better.

Watson Burton's commercial litigation, fraud and employment team have comprehensive experience in advising businesses on taking legal steps to minimise the risks posed by cybercrime, and in dealing with actual cases of data theft and breaches of security in companies from a wide range of industries.

And at Watson Burton, we also practice what we preach. This month, our firm achieved Government-approved Cyber Essentials Plus accreditation. The Cyber Essentials scheme identifies the controls an organisation must have in place in order to have confidence that they are addressing cyber security effectively.

To be awarded the Cyber Essentials Plus certification – the highest Cyber Essentials standard available – an organisation's systems must be independently tested by an external body.

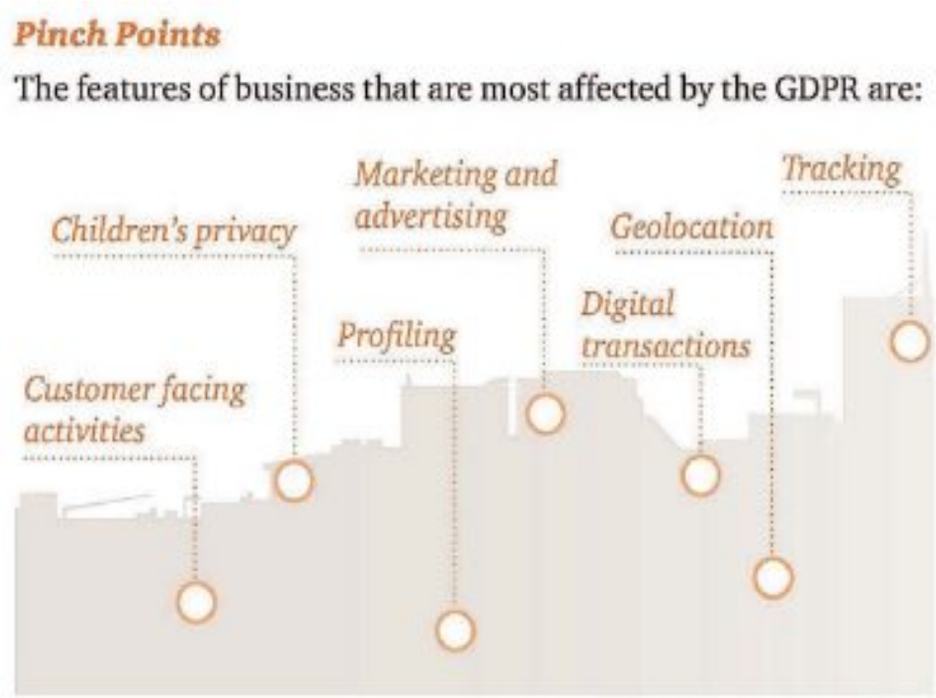
We are the only North East-based legal practice to be listed on the Cyber Essentials website as holding this certification – and we have been named among only 16 law firms in the country to be awarded Cyber Essentials Plus.

Achieving this accreditation is a demonstration of our commitment to our clients' data security and it also shows Watson Burton's support of initiatives that are helping to protect operations and business reputation.

If you want to know more about cybercrime, or feel like your business needs a security upgrade, we will be offering guidance and expert advice at our forthcoming seminars entitled Cybercrime and data theft: Understanding the Threat, Managing the Risk, on April 25 and May 11 at our Newcastle offices.

■ For more information visit www.watsonburton.com

Implications of new data



BUSINESSES need to focus on data and cyber security, not simply because of the costs and the reputational damage breaches cause, but also because of incoming legislation which steps up security and breach reporting requirements and provides sanctions for non-compliance.

The EU Commission has reached an agreement on two key data protection regulations – the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD), also known as the Cyber Security Directive.

Whereas the GDPR will give individuals stronger rights, empowering them with better control of their data and ensuring that their privacy remains protected in the digital age, the Cyber Security Directive will complement the GDPR, providing protection of IT systems in critical national infrastructure.

■ The GDPR and Cyber Security Directive will apply to UK businesses.

The GDPR and Cyber Security Directive are both EU pieces of legislation. This, of course, begs the question as to how far UK businesses need take notice following the results of the EU Referendum.

The Information Commissioner's Office (ICO) has said that UK businesses, with operations and/or services within the EU, should work on the assumption that the GDPR will apply. This will ensure the UK maintains 'adequacy' for EU purposes and can continue to receive EU personal data.

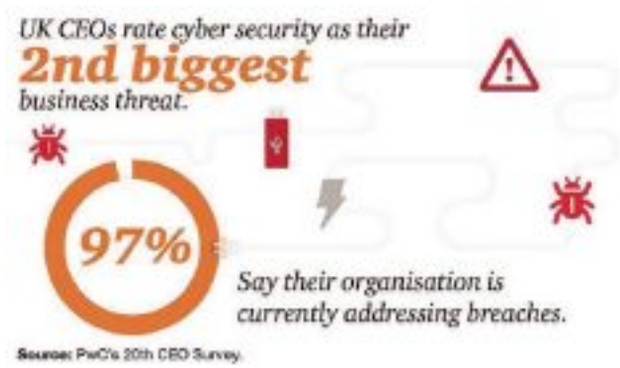
The Cyber Security Directive will also apply to businesses that provide elements of a country's critical national infrastructure – i.e. operators in energy, transport, health, and banking – and operate and/or provide services within the EU.

The new Cyber Security Directive, coupled with the GDPR, means another element of compliance for all UK businesses which must adjust how they handle data and, in turn, their cybersecurity.

■ GDPR & National cyber Security Directive, and its main implications for business.

Although the GDPR and Cyber Security Directive came into force in April 2016, they will not apply until May 2018. This has provided a two-year transition period before both pieces of legislation become enforceable across EU countries,

Cyber security: It's time to take it seriously



THE PwC 20th Annual Global CEO Survey has found that UK CEOs rate cyber security as their second biggest business threat. And 97% of CEOs stated that their organisations were currently addressing cyber breaches.

Many businesses and boards recognise that cyber security is a risk that requires their specific attention.

However, most struggle to define a comprehensive approach to cyber security that genuinely manages risk rather than implementing "standard" control frameworks in the hope they are sufficient. As a result, the question remains as to whether their response to cyber security threats is adequate.

From our engagements with businesses across numerous sectors of all sizes and across various regions it is apparent that there is a need for a pragmatic, recognised approach to governing cyber security risk that is grounded in practical experience.

There are many frameworks for the management of cyber security focusing on the definition and build of security controls.

But there is little real practical guidance as to what businesses should consider in the governance of their organisations with regard to cyber security.

All organisations are different and each needs to set its own direction and tone for cyber security.

Given the nature of cyber security, this will impact all aspects of a business including strategy, development, supply chain, staff and customer experience.

In coming years, managing cyber security risk will potentially require radical change to businesses and their operations – to make themselves more able to be secure, as well as building security controls.

For this reason, a rigid standard would not be appropriate for governing cyber security, but a principles-based approach allows each business to establish and review its own direction within a recognised framework.

We have developed a concise and comprehensive set of principles for governance of cyber risk.

To combat cyber security effectively there is a need to build confidence within your business, identifying the potential touch points and having the right strategy in place to respond to the potential threats.

■ How to build confidence in your business

- Recognise it's not if, but when.
- Build an intelligence-led defence, enabling rapid detection and containment.
- Continuity and resilience.
- Crisis management.
- Incident response and forensics.
- Monitoring and detection.

■ Fix the basics

- Fix the vulnerabilities that are easy to exploit.
- Configure and patch technology appropriately.
- Identity and access management.
- Information technology, operations technology and consumer technology.
- IT security hygiene.
- Security intelligence and analytics.

■ People matter

- Build and maintain a secure culture, where people are aware of their critical security decisions.
- Insider threat management.
- People and "moments that matter".
- Security culture and awareness.
- You can't secure everything.

■ Set the right priorities and know where the "crown jewels" are when it comes to your data

- Enterprise security architecture.
- Protect what matters.
- Strategy, organisation and governance.
- Threat intelligence.

■ Seize the advantage

- Exploit the digital opportunity with confidence.
- Digital trust is embedded in the strategy.
- Privacy and cyber security legal compliance.
- Risk management and risk appetite.

■ Their risk is your risk

- Understand and manage risk in your interconnected business ecosystem, in particular with third parties that carry out activities on your behalf.
- Digital channels.
- Partner and supplier management.
- Robust contracts.

a protection regulations

Points to consider
- *Core components of your business that will be affected.*
- *Encompassing the three key components of the GDPR.*
- *You only have until the 25th May 2018 to comply*

cluding the UK.
A two-year grace period may und generous, but in reality, given e number of teams that will need to e involved to help a business mply with the new regulations uch as IT, marketing, legal and mpliance, as well as management d business teams) businesses must nsider the implications and plan r the new regulations right now.

Five key implications to UK usinesses:

1. The GDPR introduces a requirement for all data breaches to be ported as soon as possible and, here feasible, no later than 72 hours ter discovery of a breach.
2. The definition of what constitutes personal data will expand significantly under GDPR, with personal data now extending to location, IP address, as well as whole new swathes of medical data, including genetic information.
3. There are new requirements under the GDPR to carry out Privacy Impact Assessments (PIAs), which are reviews carried out within businesses to ensure that personal data is sufficiently protected and privacy of the individual maintained.
4. Responsibility for protecting personal information under GDPR will extend to data processing as well as data controllers. Some IT services companies that are currently sheltered by the fact that the client often is responsible for the data will find this a big change.
5. The Cyber Security Directive requires operators of essential services in the energy, transport, banking and healthcare sectors, as well as providers of critical digital services like search engines and cloud computing to be expected to take "appropriate security measures" relating to breach detection, response and reporting.

PwC has carried out GDPR readiness assessments for over 100 organisations across a range of industries and sizes. If you would like to have a more detailed discuss on how the GDPR and the Cyber Security Directive could impact your organisation contact one of the team.

■ **Jayne Goble, PriceWaterhouseCoopers Cyber Security Services, tel: 07525 926356, email:jayne.goble@pwc.com**

Denial of service attacks: the growing threat

Judging by recent denial of service attacks, most companies would not be able cope if they were targeted.

By Michael Farrell, Head of Newcastle Office, Lockton

Companies need to re-evaluate their defences against distributed denial of service (DDos) attacks. This follows a spate of DDos attacks towards the end of 2016 and the start of 2017, which were larger than any we had seen before. DDos attacks involve flooding a website with traffic to prevent legitimate users from being able to access it. Imagine jamming so much gunk into a drain pipe that water can't pass through. It's like that – in cyber space.

Many large companies with sophisticated cyber defences used to prepare for DDos attacks of around 200Gbps (gigabits per second). Until recently the largest-known attack was about 500Gbps. We're now seeing DDos attacks of between 600Gbps and 1Tbps (terabits per second).

An attack of this size would blow most companies' cyber defences out of the water. A third-party provider of cyber defence might fare no better. The business interruption (BI) caused by one of these attacks could be enormous, particular for companies whose sales pipeline is largely internet-based. And it's not just the directly attacked companies that might be disrupted.

Death by a thousand cuts

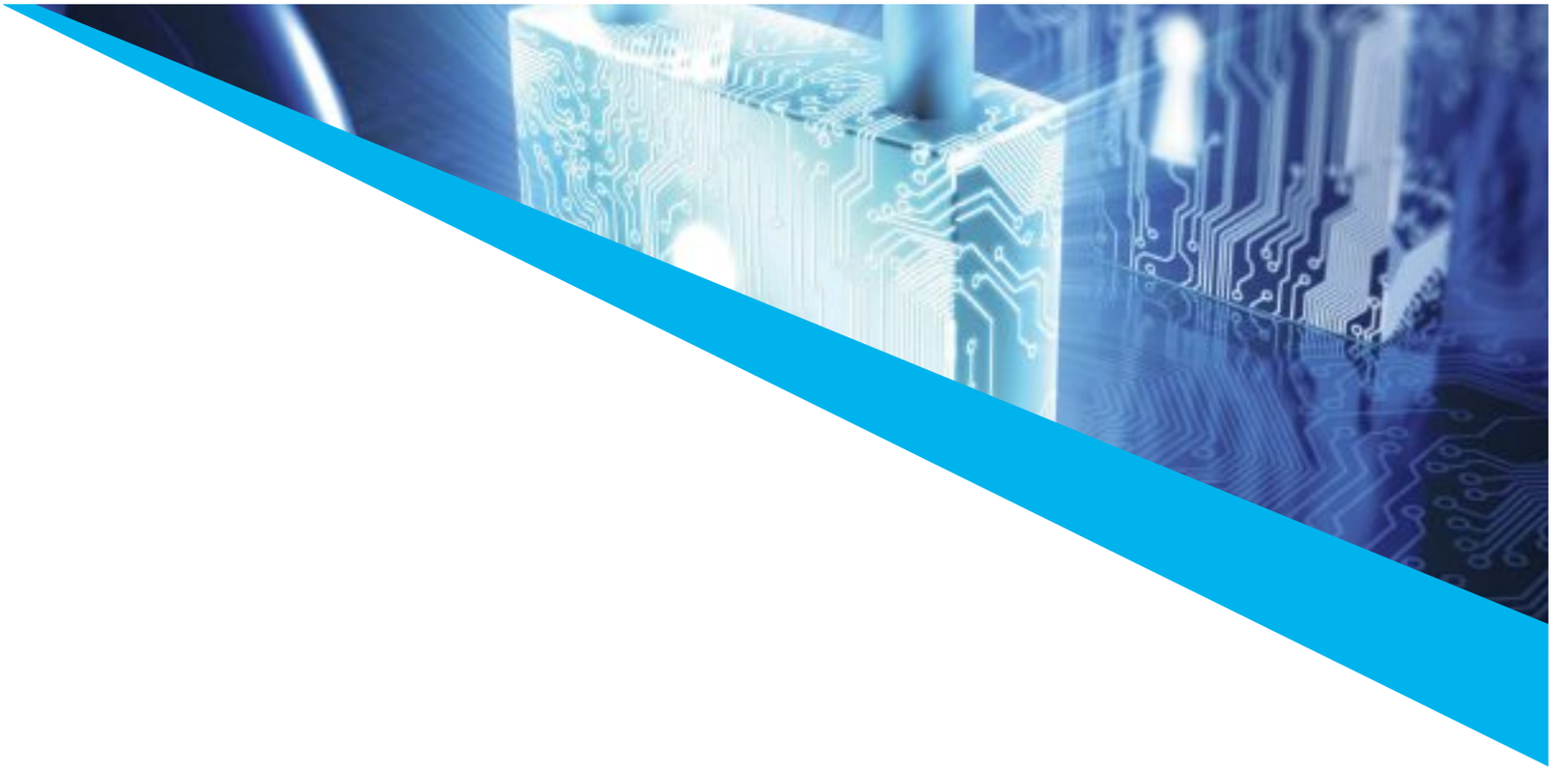
In September 2016 we saw the world's largest single targeted DDos attack. Security blog Krebs on Security – a regular exposer of cyber criminals – was flooded with more than 650Gbps of traffic. Krebs on Security used cloud-hosting giant Akamai Technologies to protect against DDos attacks. However, the attack was nearly twice as big as any Akamai Technologies had seen. In the end Akamai Technologies cut off the Krebs on Security website, and Google had to step in and mitigate the attack.

Then in October 2016, a huge number of internet-connected devices – from security cameras and video recorders to home routers – were hijacked and used to direct huge amounts of junk traffic at servers operated by US-based Dyn.

Dyn provides domain name system (DNS) services for various websites. When one of these websites is visited, Dyn helps the visitor's browser or app find the right system to connect to. So when Dyn went down, hundreds of websites – including those belonging to GitHub, Twitter, Reddit, Netflix, AirBnb – became inaccessible for several hours.

In 2017 there will be a total of 10 million DDoS attacks, predicts a Deloitte report, Technology, media and telecommunications predictions. The report predicts the average attack size will be 1.25Gbps to 1.5Gbps – large enough to take many organisations offline.

A DDos attack of this size would blow most companies' cyber defences out of the water."



Smart weapons

The driver of these DDos attacks is the Internet of Things (IoT). The proliferation of smart devices (TVs, fridges and so on) has provided cyber gangs with far more potential weapons than when a PC was our main way of accessing the internet. The attacks against Krebs on Security and Dyn were initiated from IoT devices compromised by the Mirai botnet malware. Mirai malware targets and enslaves IoT devices – such as routers, digital video records and webcams/security cameras – and then uses them to conduct DDoS attacks.

Smart devices, while convenient, are not built with rigorous security in mind. Their front doors are weaker than most people imagine. In some cases, cyber gangs can pretty much walk straight in by logging into devices using their factory-set passwords – which many people still don't change.

Next steps

So what practical steps can companies take to minimise the threat of DDos attacks? If you have a DDos attack mitigation plan, now is the time to re-examine it. In light of recent attacks, your plan might be insufficient.

Do you have a business continuity (BC) plan in place that covers a large-scale DDos attack on your company? After an attack, how would you continue to trade, and how would you inform customers of what had happened? And if you outsource your attack mitigation to a third-party provider – talk to them as soon as possible. Is your provider aware of these recent attacks and, if so, what is it doing in response? How confident is the provider that it can mitigate a DDos attack of 500, 600 or even 700Gbps? How exposed is the provider, itself, to such an attack? What is your contractual position? Would your provider drop your sites to protect their service?

If you don't have a DDos attack mitigation or a BC plan in place – now is the time to implement one.

An Allianz Risk Barometer listed BI as the top global risk for the fifth year running. It also noted that the number of non-physical causes of BI was only likely to increase. Look no further than DDos attacks – what we've seen so far could be just the beginning.

Michael Farrell, Partner

0191 261 3059
michael.farrell@uk.lockton.com
lockton.uk.com

LOCKTON®

Is the North East one of Britain's best-kept cyber security secrets?

By David Carroll
Managing Director
XQ Digital Resilience

THE news headlines are increasingly dominated by the activities of cyber criminals and nation states.

Economic loss is an unfortunate consequence of the rather haphazard manner in which the Internet and the digital economy have evolved, and it will be an enduring fact of life for the foreseeable future.

The good news is that, despite the headlines, this isn't all necessarily bad. Far from it. Cyber insecurity is the price we pay for the overwhelmingly positive economic effects of the Internet and the web.

Cyber insecurity also presents a significant opportunity for those regions and cities possessing the vision and skills required to address it.

The domestic cyber security market is already worth £3.5bn, and is growing at around 10% every year. The Government estimates that cyber security spending unlocks £17bn in terms of economic benefit. And cyber security exports are forecast to be worth a further £4bn by 2020.

So which regions are best placed to benefit? If you were asked to name the UK's main cyber security clusters, which names would spring to mind?

I'd hazard a guess that your answers would include established names like Cheltenham, Malvern and Tewkesbury.

Cambridge and Corsham might feature. London would inevitably dominate, accounting, as it does, for one quarter of the domestic market.

Take a look around the North East, however, and you may be pleasantly surprised by our own cyber security credentials.

Every year the North East's universities and colleges produce around a thousand graduates and apprentices possessing cyber security and related computer science skills.

This figure is set to increase dramatically as our institutions gear up to address a skills shortage so severe that there are likely to be one and a half million unfilled cyber security jobs globally in 2020.

The North East also has a strong research base. Newcastle University is a GCHQ accredited Academic Centre of Excellence for Cyber Security Research, one of only two in the North of England and Scotland.

Last year, at a showcase co-hosted by Dynamo North East and the Newcastle University Cloud Innovation Centre, there were presentations from our universities covering almost every facet of cyber security research.

The North East, therefore, has a tremendous opportunity: an opportunity to diversify and grow our workforce and to create high skills jobs within the region; an opportunity to support Government transformation and to address regional demand for cyber security goods and services across all of our industries.; an opportunity to foster cyber innovation and to encourage the formation of new cyber security businesses; and an opportunity to attract inward investment to the region.

At Dynamo North East we're working hard with our partners to realise this opportunity and we would like you to join us.

Whatever your sector, and whatever your interest in cyber security, we would like to work with you. Join us at: www.dynamonortheast.co.uk

David Carroll is CEO at XQ and is joint chair of the Dynamo Cyber Workstream.
david.carroll@xqdigitalresilience.com

Choosing your security partner

By David Horn
Sales director of Net Defence

IT'S a blue one, a pink one or a green one isn't it?

All information security providers are the same right?

Maybe, maybe not....

In a world where risks are everywhere and solutions to problems, perceived or otherwise, are readily available, how do you know who to engage with?

Each provider professes to be unique and yet are they really?

Let's take a step back and look at what's actually available.

In essence organisations that provide solutions to information security issues may be broadly divided into two camps. Those that provide technology solutions and those that provide service solutions.

Both types of solutions can be both proactive in stopping the threats and reactive in tidying up post incident. Interestingly though, the majority of suppliers specialise solely in one area.

If your business is looking for a more rounded approach you may want to consider engaging with an organisation that deals with both technology and services.

However, usually you will find that organisations providing technology are aligned with specific vendors so it is often very difficult to obtain truly impartial device.

There are, of course, two schools of thought here. The first being that if you know which technology you want, then it's better to engage with a specialist in that area as you can be assured of first (and very often second) line support from that provider. The second school of thought is that by engaging with a vendor agnostic provider you will not receive the same level of service.

Personally, I believe this is incorrect. In fact quite the opposite. In many cases your support will be directly with the vendor and as you are therefore cutting one link out of the chain any issues can actually be resolved more quickly.

However, ultimately, the choice will come down to personal preference and be influenced by previous working relationships or knowledge of an organisation and their reputation.

So far, so good. I don't suppose that there is anything mentioned so far that is ground-breaking.

Let's stop for a moment then and think about the term information security and what it actually means. How do we secure our information? Typically, we think about information assets, intellectual property and

proprietary information.

What if we extended the scope to include the devices that carry information, or perhaps what we might also consider physical security.

Protecting assets by using humans is fraught with problems, can be ineffective and is also costly.

Imagine if we could protect assets that carry information or perhaps assets where their locations are confidential, all by using technology?

What if this type of technology was also able to remotely monitor activity using fibre and communicate in incredible detail based on signatures, what is actually happening in real time?

What if this information could link and effectively be an additional sensor on a SCADA system?

What if this level of protection and its associated reporting could then integrate into your existing SIEM solution?

What if the same technology could also provide intelligence around potential issues? This intelligence is based on disruptive patterns in the fibre signature which can provide advance warning of potential issues.

Imagine the savings of being able to have in place a dynamic preventative maintenance plan with reduced downtime?

It's interesting to see how we have now made the leap from good old information security to preventative maintenance in one small step. This technology exists. The technology is available now and in a world where collaboration, shared resources, improved communication, better cost management and improved efficiency are all buzz phrases, it's definitely worth looking beyond the normal offerings that are available.

So, next time you are about to start on a security discussion, take a step back and look at the business, the risks, challenges and objectives. Even if you think the issues are beyond the remit of the organisation you are engaging with, ask the question anyway as you may just be surprised at the answer.

I speak from experience as the solutions that Net-Defence deploy encompass all of the above... now that's what I call a technology and service set.

For more information contact Net-Defence 0845 456 5567 or www.net-defence.com

In association with BIC

Silver lining for companies as BIC launches cloud solution

FOR many companies, buying in computer services makes good business sense.

Cloud computing allows us to do all of our computing on the Internet as a cost effective alternative to buying, installing, upgrading, backing up and otherwise managing physical hardware and software.

Continuing its commitment to helping businesses work more efficiently, securely and cut costs, the North East Business and Innovation Centre (BIC) is delivering a tailored Cloud Solution.

This allows for the centralised storage and access to company data over the internet instead of an individual computer hard drive and is available to businesses across the North East.

IT manager, Colin Turnbull explains: "The Cloud allows a flexible, cost effective approach to working. Some businesses have peak seasons or ever changing staffing demands.

"Our BIC Cloud ensures that businesses only pay for what they use and can scale up or down when needed.

"We understand that the working environment is changing and people are no longer confined to the desk.

"BIC Cloud allows businesses access to their data wherever they need it via smartphones, tablet, laptop or desktop.

"This secure solution provides a managed firewall, email and web spam filter with off site data back-up, giving you peace of mind and keeping you in the know whilst on the go."

The BIC Cloud Solution proves to be the perfect answer for ARC Adoption North East Limited, director Terry Fitzpatrick explains: "There are many reasons the BIC Cloud works for us.

"We work with confidential matters and have a responsibility to maintain records for a considerable period of time, therefore knowing that our systems are backed up and maintained by security experts gives us peace of mind.

"The nature of our work and our

> ARC Adoption director Terry Fitzpatrick and the team are enjoying the benefits the BIC Cloud offers

geographical spread means that we often need to work remotely, the Cloud has made this process so much easier as it has enabled colleagues to access our system from wherever they are, and still maintain data security, which is vital.

"The BIC team were beyond helpful in the lead up to the implementation of our Cloud Solution and have continued to provide high quality support throughout.

"We would highly recommend the BIC team."

As a not-for-profit organisation the BIC is committed to reinvesting in support and facilities to best meet the needs of the business community.

The BIC Cloud Solution forms part of a suite of services designed to support the growth and development of businesses across the North East.

To find out how cloud computing can be of benefit to your business call 0191 516 6170 to arrange an informal chat.

Secure your business. Protect yourself from cyber risk.

Most business owners now appreciate the importance of cyber security to protect networks, computers and programmes from attack.

Contact our IT experts and ensure you have the correct levels of security in place to protect your emails, back up your data and enable safe and flexible remote working... without breaking the bank.

BIC

NORTH EAST **BIC**

0191 516 6170 **www.ne-bic.co.uk/it**