ipost parcels

Getting to grips with

Cyber SECURITY

CONTENTS

Getting to grips with cyber security

The internet has changed the way the world does business. It's estimated that e-commerce accounted for nearly 6% of the total global retail market last year, with a massive $1.316 trillion (£850 billion) being spent online. By 2018 this figure is forecast to almost double to $2.489 trillion (£1.61 billion).[1] The vast markets of China and the US lead the way in terms of sales volumes but UK shoppers spend more online per capita than consumers anywhere else in the world. On average, UK shoppers will make more than 21 online purchases this year. The average purchase will cost £55.36 and each will spend an average of £1,174 over the course of the year.[2]

Cyber security issues are obviously paramount to any business that actually trades online but such concerns should not be limited to e-commerce businesses. Almost every company these days has its own website. We communicate and often market ourselves via email and many companies hold electronic databases containing customer details. Every business that runs a website, connects to the web or stores information electronically could potentially be a victim of the many, and increasingly sophisticated, varieties of cyber threat out there.

According to a study published by the Center for Strategic and International Studies (CSIS), cybercrime costs the global economy around $445 billion (£288 billion) annually.[3] High profile security breaches affecting the likes of Sony, Ashley Madison and eBay have all made headlines in recent years and pushed cyber-security further into the public consciousness. A Home Office report, however, found that small and medium enterprises in the UK were putting up to a third of their revenue at risk by falling for cyber security 'myths'.[4]

Highly placed on this myth-list and cited by 26% of SMEs surveyed by the government's Cyber Streetwise campaign, is the idea that only businesses that take payments online are vulnerable to cybercrime. Some 22%, meanwhile, believed that smaller companies were not targeted by hackers and other cyber criminals. According to the Home Office report, SMEs are actually being targeted with increasing frequency. The rewards gained or damage caused from a successful attack might not be as high as one that affected a major corporation but smaller businesses usually present 'softer' targets. According to the survey, two thirds (66%) of SMEs didn't consider their businesses to be vulnerable and only 16% listed cyber security as a priority.

Ed Vaizey, Minister for Culture and the Digital Economy, has voiced concerns over the approaches shown by many of the UK's businesses:

“Small and medium-sized firms are a key part of our long-term economic plan to back business, create jobs and secure a brighter future for Britain, and many are reaping the rewards from going digital and operating online. However this new research shows businesses can do more to understand and respond to cyber threats.

“There are some simple steps firms can take to protect themselves, their cash flow and their data. The government is providing a range of cyber security guidance and support and I encourage all small and medium-sized firms to take these simple steps and fully benefit from our growing digital economy.”

The costs of cyber crime

The CSIS report on cybercrime estimated losses to the global economy of $445 billion (£288 billion), which is roughly equivalent to 1% of total global income.

Stewart A. Baker, a former Department of Homeland Security policy official and a co-author of the report, said: “Cybercrime costs are big, and they’re growing. The more that governments understand what those costs are, the more likely they are to bring their laws and policies into line with preventing those sorts of losses.” [5]

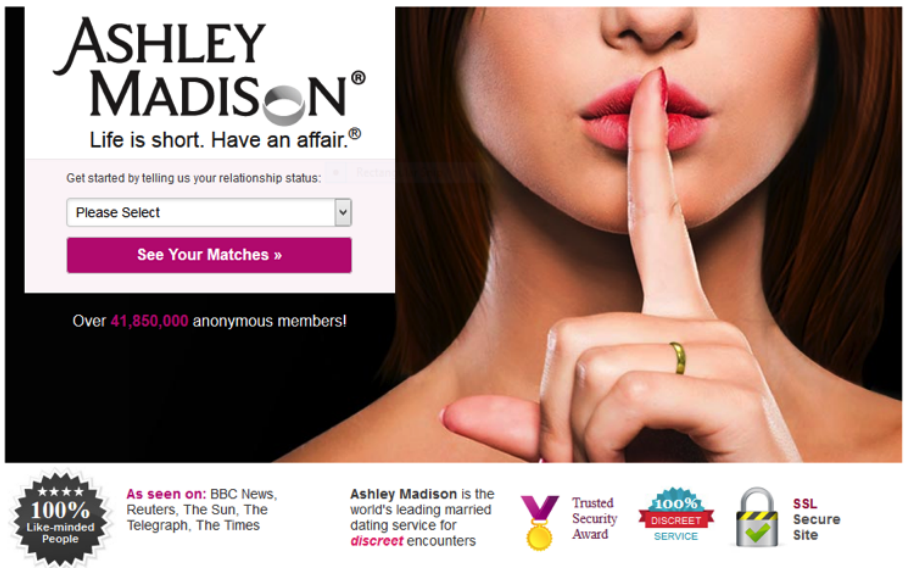
The types of figures involved can be mind-boggling and on this scale they are perhaps best left to governments and economists. The 2015 Cost of Cyber Crime Study: United Kingdom, conducted by the Ponemon Institute and sponsored by Hewlett Packard, looked at the costs to individual companies by studying 258 separate cyber-attacks. It found that the average (mean) annual cost to businesses was £4.1 million, with individual costs ranging from just over £628,000 to £16 million. The most costly cyber-crimes were those caused by denial of services, malicious insiders and web-based attacks. It also found that costs could mount up even more if attacks went undetected or were not dealt with quickly, with the average time to resolve a cyber-attack being 31 days. [6]

The study found that the overall costs to smaller businesses, as you might expect, to be less than those faced by larger ones. Smaller businesses did, however, face higher per capita costs. It’s also the case, of course, that a smaller business can often struggle far more to meet a relatively small cost than a larger business would to ride out a more substantial one.

For SMEs, the government’s Information Security Breaches Survey found that the average cost of the worst security breach experienced fell somewhere between £65,000 and £115,000. [4] Costs can include disruption to business, loss of custom, reputational damage and the costs of detecting, eradicating and protecting against further attacks. Fines could also be imposed if companies are deemed not to have taken appropriate precautions with personal data.

Costs and vulnerabilities also vary from industry to industry as well as individual businesses. The Ponemon report found that organisations in financial services, energy and utilities and communications tended to experience significantly higher cyber-crime costs than those in retail, the public sector, education and research.

Some individual businesses could be particularly vulnerable to certain types of attack. A high profile example is that of Ashley Madison, a website that puts people looking to have an affair in touch with each other – a business model that absolutely relies on discretion.



(PIC 1)

The total costs of the site's very public hacking in July 2015 have not been released, but on top of the usual costs it has been reported that a huge class action lawsuit totalling around £367 million is pending.

The two law firms handling the lawsuit – Charney Lawyers and Sutts and Strosberg LLP – said in a statement:

"Numerous former users of AshleyMadison.com have approached the law firms to inquire about their privacy rights under Canadian law. They are outraged that AshleyMadison.com failed to protect its users' information. In many cases, the users paid an additional fee for the website to remove all of their user data, only to discover that the information was left intact and exposed."

Types of cyber threat

There are many different types of cyber threat and new ones will no doubt continue to evolve in the future. The following list is not exhaustive, but these are the nine most common types of attack according to a recent Verizon report, accounting for 92% of incidents over the past decade:

• Crimeware
This is a type of malware designed specifically to automate cybercrime. Malware itself is an umbrella term for malicious, intrusive software and includes viruses, worms, trojans, ransomware, spyware, adware, scareware and other potentially harmful software.

• Insider privilege misuse
People within the organisation misuse their access to potentially sensitive data and intellectual property. 88% of information leaks are attributed to granting incorrect access rights.

• Physical theft and loss
As data and hardware becomes more portable, the risks of theft or loss increase. One high profile case involved a contractor working for the Home Office losing a memory stick containing personal details of tens of thousands of convicted criminals. [9]

• Web application attacks
Attacks of various types, such as SQL injections, can be carried out via or through web-based apps. Verizon states that virtually every attack in this data set (98%) was opportunistic in nature.

• Denial of service attacks
A DoS attack essentially makes a machine or network resource unavailable and therefore useless to its intended users, essentially by flooding it with useless data. Common targets for this sort of attack are web servers, as an attack can then cause a website to be temporarily disabled.

• Cyber espionage
This isn't just an issue for governments (or, for that matter, James Bond). Professional services, transportation, manufacturing, mining, and the public sector are all popular targets for cyber espionage as it can severely disrupt operations.

• POS intrusions
Point-of-sale intrusions are remote attacks against the environments where retail transactions (typically card sales where the card is physically present) take place. These can involve installing malware in tills and similar hardware.

• Payment card skimmers
Similar to POS intrusions but this involves taking information from cards at card points such as ATMs, ticket vending machines and automatic petrol pumps. Criminals have to physically plant a malicious card reader that can take information from your card as you make a legitimate transaction.

• Miscellaneous errors
This includes situations such as information being mistakenly sent to the wrong recipient or a public site. As well as instituting training and protocols to help minimise human error, data-loss prevention software can help prevent data from ending up where it shouldn't.

(PIC 2)

Types of malware

There are many different types of malware, including:

• Computer viruses
A computer virus, like a biological virus, is able to replicate itself and spread from one device or system to another, causing destruction wherever it goes. Viruses can corrupt or delete data and can cause severe damage or disruption if undetected or left unchecked.

• Worms
A worm can be as nasty as it sounds as, once on board, it is able to spread itself without further interaction. Most are spread via infected email attachments and, once in another system, will scan the surroundings for address books and the like before creating new infected emails.

• Trojans
Named after the Trojan Horse, in which Greek soldiers hid and secretly entered the besieged city of Troy), trojans hide inside other programs and provide a 'window' for hackers looking for a way into your system. One common type is a 'keystroke logger', which records the keys you use to type information into your computer. This can include information such as passwords and log-in details which can be very useful for cyber-criminals. A 'man in the browser' (MiTB) is a specific type of trojan that can alter the information you enter into a website. An example could be changing the destination bank account for a payment that you are making.

• Spyware and adware
Spyware and adware is not usually as serious as other types of malware but can still be troublesome and difficult to get rid of. Spyware will typically collect advertising and personal data but it can also change your computer's configuration and sometimes hijack and redirect your browser.

• Rogue security software
This can be more of a problem for personal users but small businesses are certainly not immune. Rogue security software will try to convince you that you already have malware on your computer and that you should download these often convincing looking programs to get rid of it. Once on your system, rogue security software can flag legitimate items as adware and prevent genuine security software from working. Ransomware can 'seize up' a system, preventing you from using it until you make an online payment.

Security software

Even personal users who occasionally browse the web and never shop or bank online are strongly advised to set up firewalls and suitable antivirus and antimalware software. If you're running a business it would be madness not to do the same.

The exact solutions required will vary from one set-up to the next and security software providers will, of course, all be keen to point out the usefulness of their own systems. There's no one-size-fits-all security solution but guidance published by The Centre for the Protection of National Infrastructure (CPNI) and CESG (the Information Security arm of GCHQ) says you should:

"Deploy antivirus and malicious code checking solutions with capabilities to continuously scan inbound and outbound objects at the perimeter, on internal networks and on host systems, preferably using different products at each layer. This will increase detection capabilities whilst reducing risks posed by any deficiencies in individual products. Any suspicious or infected objects should be quarantined for further analysis." [10]

(PIC 3)

Security solutions that provide multiple defensive layers (known as ‘defence-in-depth’) should be considered. Firewalls are a must and should be installed on both host and gateway devices and configured to deny traffic by default, only allowing connectivity for white-listed (pre-approved) applications. Content filtering capability can be deployed onto external gateways to try to stop attackers from delivering malicious code to common desktop applications such as web browsers.

Anti-malware should be deployed right across the organisation and active scanning should be implemented.

Using the cloud

The cloud has been a buzzword for some time now but essentially it just means using software and services such as data storage that are hosted remotely. The cloud used to have a reputation for being something of a security weak spot but, if you choose your providers wisely, this is not necessarily the case. In some areas it can actually be more secure. Reputable cloud service providers take security incredibly seriously. They will have protocols regarding access to data, state-of-the-art anti-virus software, firewalls and encryption, and heavy physical security surrounding their premises, servers and other assets. In fact they are likely to have far better security than the average SME.

According to Symantec nearly half of all business data is now stored in the cloud but you still need to do your homework before choosing a provider. Assess their credentials, clients, references and security policies and ensure they meet recognised industry standards including ISO 27001, ISAE3402/SSAE16 and CSA STAR. The latter, developed by The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), is the first internationally recognized cloud security certification program.

All the data moving from your business to anywhere on the cloud should be suitably encrypted and you should also institute protocols regarding the way employees use devices connected to the cloud. Cloud security is not a one-way street and you have to take care of issues at your end just as the service provider needs to at theirs.

Kaspersky Lab's David Emm says: "Before out-sourcing to a cloud provider, businesses need to assess the potential risks in just the same way that they would if they were managing internal business processes and systems. This includes staff education about login details.

"Other issues that need to be considered include where the company's data will be stored geographically, the legal jurisdiction that will apply to the data, what steps will be taken to secure the data on their provider's systems – including how it will be secured from other tenants of the cloud provider – and the logistics involved in migrating the data to another provider in the future."

Protecting customers' personal data

Many businesses collect and store customer data. In the UK the main piece of legislation that covers the collection, storage and use of data is the Data Protection Act.

Data Protection Act 1998

(PIC 4)

The Information Commissioner's Office (ICO) says that under the Act you should:
- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it;
- allow the subject of the information to see it on request.[12]

The Act also states that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Exactly what constitutes “appropriate technical and organisational measures” is to some degree open to interpretation. No single measure is ever 100% effective against cyber threats so the ICO advises that SMEs holding personal data should adopt a layered approach to security. Areas to think about include:

• Physical security
Protect against equipment containing sensitive information being physically stolen in a break-in. Provide extra security for servers and don’t leave storage or back-up devices unsecured.

• Anti-malware
Install extensive anti-virus and anti-malware software and, crucially, keep it up to date.

• Intrusion defence
Keep firewalls active and updated. Penetration tests can find weaknesses in your system by simulating a hostile attack.

• Restrict access
Only those who genuinely need to should have access to the data. Each individual should have their own username and a strong password. Alarmingly, the most popular passwords continue to be ‘123456’ and ‘PASSWORD’. [13]

• Training and policies
Institute security policies and ensure all staff are trained in following them.

• Segmentation
Consider separating or limiting access between network components such as your web server and main file server. This means that if your website was compromised, the attacker would not have access to your central data core.

Bring your own device (BYOD)

Bring Your Own Device or BYOD is an increasingly common practice but one that is not without its risks. Allowing employees to use their own laptops and mobile devices to connect to workplace systems does have its benefits. It can improve flexibility and productivity, as individuals can often work at a faster pace and are more familiar with their own devices. They can also use them at home or elsewhere offsite and it can be cheaper than providing corporate devices.

It might also be the case that employees are connecting via their own devices whether you want them to or not.

Dave Martin, vice president and CSO at US-based EMC Corp, says: “Ask anyone who says they don’t have BYODs to review their logs—I guarantee they’ll find Mobile Safari. Disallowing BYODs just pushes them underground where you lose visibility. I’d rather see BYODs and deal forensically with risk than try to convince myself that I can block them outright. Experience has shown that’s a failed strategy; users find a way in. But if you’re too permissive, you’re open to data loss. We are unable to lock down BYODs in the same way, so we need to be smarter about how we use them.”

If you are going to officially recognise and even encourage BYOD in the workplace, it’s important to have protocols and a security framework in place.

The CPNI and CESG has issued guidance on the matter for UK businesses. They recommend a range of measures and areas to consider, including:

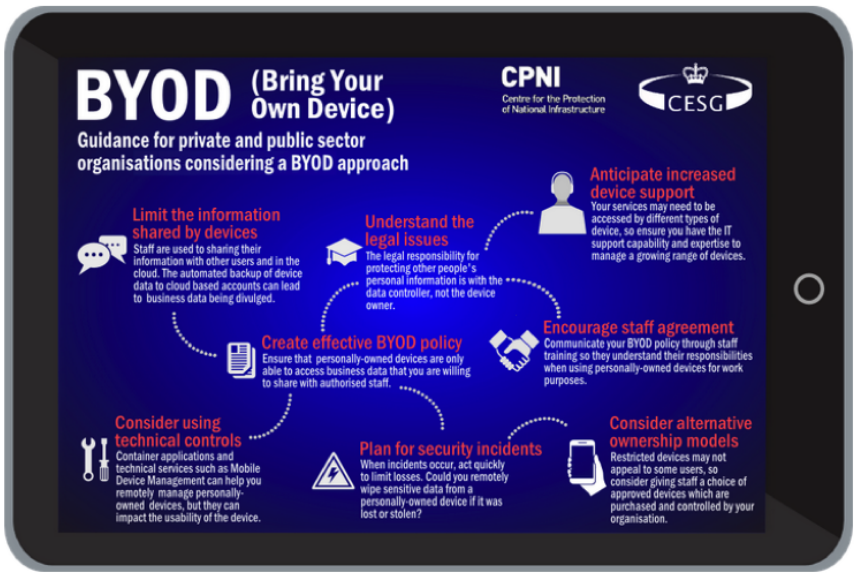
• Ensure that personal devices can only be used to access appropriate information and that protocols are in place for users to go through authorisation controls.

• Communicate the BYOD framework and personal responsibilities through staff training.

• Be aware that the legal responsibility to protect personal data lies with the data controller, not the owner of the device.

• Put limits on the information that can be shared between devices, or between devices and the cloud.

• Consider alternative ownership schemes, in which approved devices are owned and ultimately controlled by the company but used exclusively by individual workers. Think of it as the mobile IT equivalent of company cars.



(PIC 5)

The human element

An organisation can have all the security software and cutting edge technology defences in the world but it still needs people to follow security procedures and exercise common sense.

Following protocols and using their own devices sensibly under a BYOD policy is certainly one area but there are others where basic training should be provided, including general cyber safety. Phishing scams, for example, attempt to gain sensitive information. Phishing can be undertaken over the phone or even in person but the most common format is via an email masquerading as something other than it is. This could appear to be from a bank, supplier or other source and can often look very plausible. It may provide a link and ask you to provide financial or identity-based information.

Another area where many people could improve relates to using effective passwords. As already mentioned, the most popular passwords continue to be '123456' and 'PASSWORD'. Other easily guessed passwords, including ones based on personal information such as birthdays and relatives' names should also be avoided. The ideal password should have a combination of letters and numbers, with the letters using both upper and lower cases. You should also use different passwords for different purposes. Cyber criminals are aware that people often tend to use the same password for multiple purposes so if they crack one you use at home they might also find entry into your place of work.

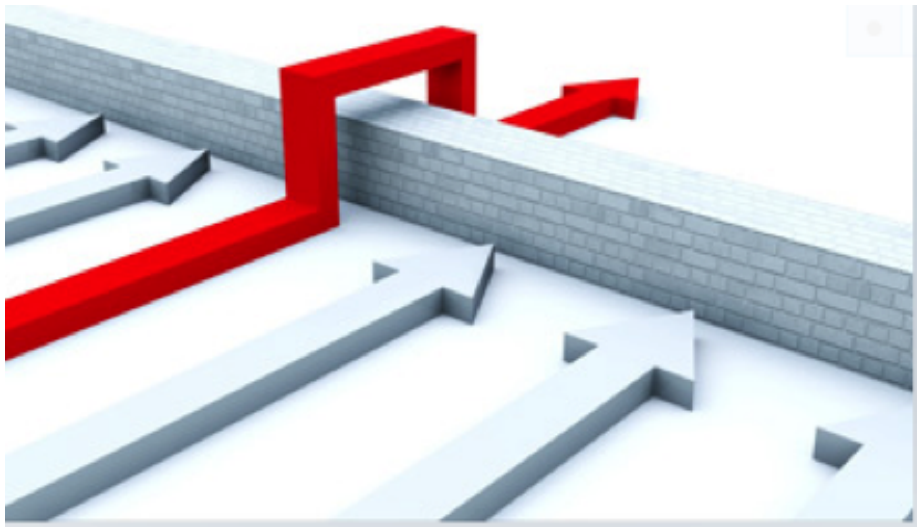
These are the very basics of cyber security, but at the other end of the spectrum, companies are also being hurt by a 'cyber security skills gap'. SC, the magazine for IT security professionals, reports that there will be a shortage of 1.5 million information security professionals by 2020.

According to the seventh annual (ISC)² Global Workforce Survey, the lack of skilled staff is already impacting on businesses, with 44% saying it takes up to a week to correct a data breach and another 19% saying it can take up to three weeks. Only 42% of organisations polled said that they were confident in their ability to recover from a cyber attack.

Dr Adrian Davis, CISSP, managing director at EMEA, (ISC)², said: "Our first workforce study was conducted in 2004 to illuminate critical concerns within information and cyber-security that were struggling for attention. The 2015 report shows that many of these issues are finally getting much needed budget and priority. Unfortunately, we are now facing new challenges and our skills and staffing challenge is growing."

Testing your security

Once you have all your security measures in place it makes sense to test them. Penetration tests, or pentests, can help by simulating a range of different attacks made on different parts of your system. These should help tell you where your defences are strong but, just as importantly, they can help you to identify any weak spots. If and where these do exist, it's better that you expose them in a simulation than a cyber-criminal finds them in a real attack.



(PIC 6)

Another related but distinctly separate area is load testing, in which you simulate a high volume of traffic in order to identify choke points in a system that could crash under too much pressure. The UCAS (Universities and Colleges Admissions Services) website has previously crashed on A-level results day while the London Olympics ticketing system almost crashed under the initial strain when tickets first went on sale. These types of 'spike traffic' crashes might not be cyber-attacks but having your website crash at a key moment could]have disastrous effects.

According to IT Pro, the majority of IT professionals believe that regular 'cyber security drills' are an important part in defending against attacks but around a third of firms are failing to carry them out. A survey by Lieberman Software showed that less than two thirds of companies (63%) actively carried out drills. 26% carried out bi-annual cyber security drills and only one in ten carried out quarterly drills.

Conclusion

It can sometimes seem like an arms race between cyber criminals and cyber security experts, with the businesses taking a buffeting in the middle. The costs of setting up and maintaining cyber defences always seem to be on the increase as cyber criminals come up with new techniques that have to be countered. As a result, cyber security is very much an ongoing and very challenging process, rather than a one-off task.

The costs of doing nothing can be even higher however. According to the latest government Information Breaches Survey, 90% of large organisations and 74% of SMEs reported that they had suffered an information security breach over the past year.

Andrew Miller, Cyber Security Director at PwC, states: “With nine out of 10 respondents reporting a cyber breach in the past year, every organisation needs to be considering how they defend and deal with the cyber threats they face. Breaches are becoming increasingly sophisticated, often involving internal staff to amplify their effect, and the impacts we are seeing are increasingly long-lasting and costly to deal with.” [17]

Cyber security can be a complex thing to get to grips with but it’s also an essential one for any company competing in the modern, increasingly interconnected age.

References

1 http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765

2 http://www.digitalstrategyconsulting.com/intelligence/2015/01/global_ecommerce_trends_2015_uk_leads_the_way_in_europe_and_north_america.php

3 http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

4 https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk

5 https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

6 https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5209enw.pdf

7 http://www.bbc.co.uk/news/business-34032760

8 http://www.cgma.org/magazine/news/pages/201511624.aspx?TestCookiesEnabled=redirect

9 http://news.bbc.co.uk/1/hi/uk/7575766.stm

10 https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-malware-prevention--11

11 http://www.techradar.com/us/news/internet/cloud-services/cloud-security-how-to-keep-your-data-safe-1260769

12 https://ico.org.uk/for-organisations/business/

13 http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

14 http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards

15 http://www.scmagazineuk.com/cyber-security-pros-blame-breaches-on-skills-gap/article/409393/

16 http://www.misco.co.uk/blog/news/03357/third-of-firms-fail-to-carry-out-cyber-security-drills

17 https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles

Picture original locations:

PIC 1 https://www.ashleymadison.com/

PIC 2 http://www.verizonenterprise.com/DBIR/2015/

PIC 3 http://www.4thavenuejones.com/major-antivirus-software/

PIC 4 https://www.ict4c.co.uk/support/service_information/data_protection_act/

PIC 5 https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary

PIC 6 https://www.sans.org/event/pentest-berlin-2013

ABOUT IPOSTPARCELS

ipostparcels.com offers next day collection and delivery services to the UK and over 160 international countries, at a time and location to suit you and all at fantastic prices too. So if it's one parcel or several you need to send, the ipostparcels service is ideal for anyone looking for convenience and great value.