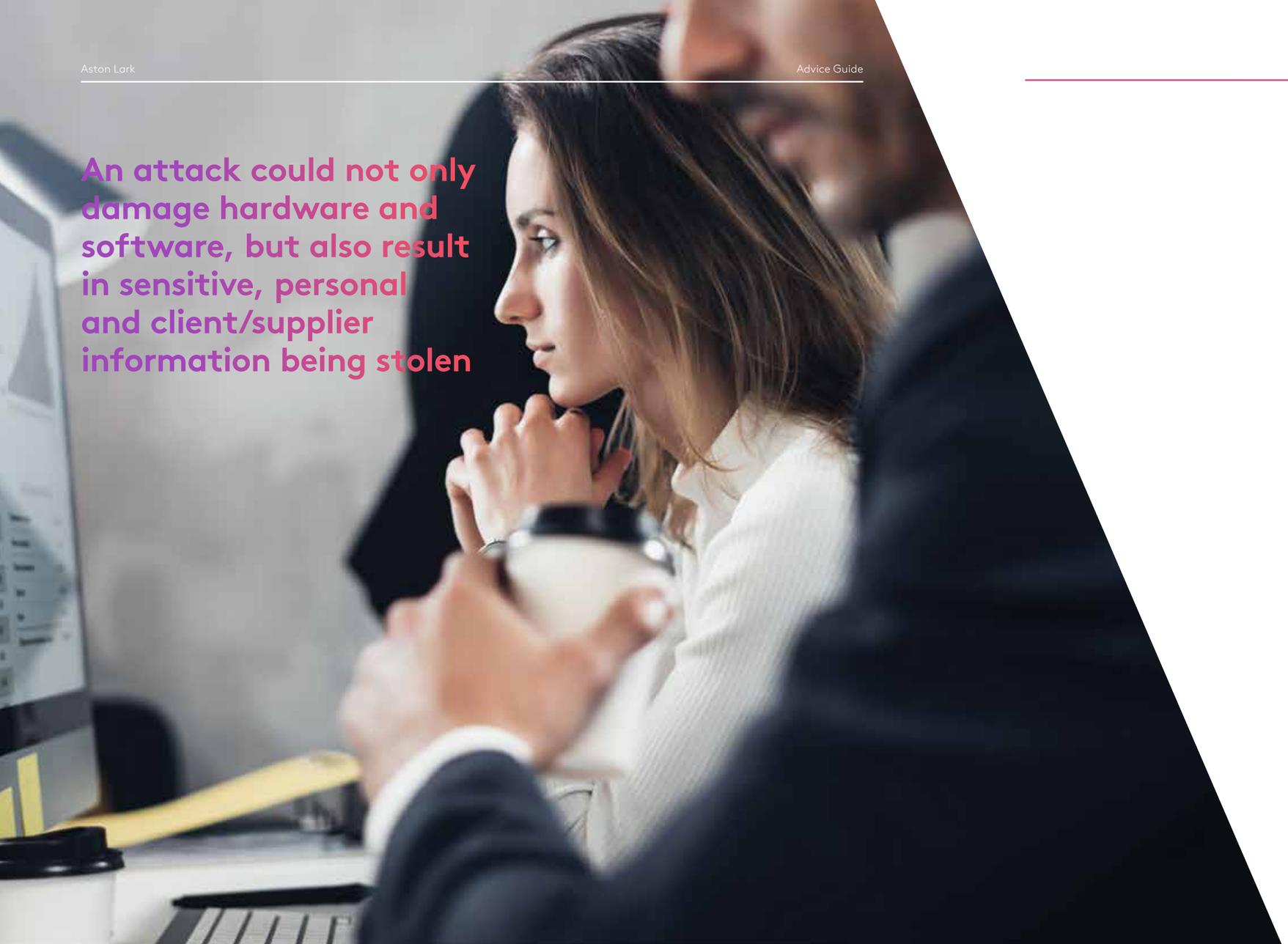
ASTONLARK
A howden company

ADVICE GUIDE

Fighting cyber crime together

YOUR WORLD IS OUR FOCUS

www.astonlark.com



An attack could not only damage hardware and software, but also result in sensitive, personal and client/supplier information being stolen

A broad view of the problem

Cyber crime is a genuine threat to any business which has a digital presence.

Where important physical assets, such as documents and data, used to be protected by locked doors, security guards, and intruder alarms, our new reliance on technology presents a challenge to effectively protect our digital assets.

Unfortunately, many businesses are still not taking the right steps to protect themselves. Here are a few reasons why:

THERE MIGHT BE A "IT'LL NEVER HAPPEN TO US" TYPE OF ATTITUDE

- Even though the press reports breaches of high-profile FTSE 250 companies, it fails to mention how regularly SMEs are affected.
- There's no central European repository detailing all of the reported breaches.
- When a breach takes place, the companies involved don't make it public knowledge, in order to avoid the stigma of vulnerability.

THEY MIGHT BE UNDERESTIMATING THE COST

Many business managers don't understand how much it actually costs to get the business back on its feet after a cyber breach.

THEY BELIEVE THEY HAVE A ROBUST NETWORK

IT professionals believe they are fully protected with enhanced physical security and contractual protection from third party suppliers.

A look at the realities

Malicious attacks and breaches have become more sophisticated, so it's worth knowing what threats your business faces.

From damage to your businesss hardware and software, to the loss of sensitive personal and client/supplier information, here are some of the risks you should consider:

BUSINESS INTERRUPTION

When systems are put out of action, your income flow could be affected. The level of interruption is dependent on the speed of recovery.

TRANSMITTING VIRUSES

Damage to a third party caused by a program originating from your system.

LOSS OF INTELLECTUAL PROPERTY

Theft of digital intellectual property such as creative works or new products.

FIRST PARTY PROPERTY DAMAGE

Damage to hardware (servers, networked computers, etc.)

REPUTATIONAL DAMAGE

An attack through social media (Facebook, Twitter, etc.) which could explode into a detrimental PR event.

EXTORTION

Demanding money (or making another condition) in exchange for sensitive data or information.

LIBEL, SLANDER AND COPYRIGHT

Email mishaps and off-hand conversations going viral to the detriment of your company.

FINES AND DAMAGES

Fines issued by the Information Commissioner's Office for breach of the GDPR.

DATA BREACH

When stored information is compromised.

PRIVACY BREACH

When the security of customer and/or employee personal data is compromised.

COPYRIGHT

Inadvertent infringment on another business' or person's copyright.

SOCIAL ENGINEERING

The methods attackers use to deceive victims into performing actions, often phishing but also phone calls, fake LinkedIn accounts, etc,

RANSOMWARE

A piece of malicious software that encrypts or blocks access to data or systems, with a decryption key only being provided upon payment of a fee.

A look at "Who"

Cyber criminals don't discriminate on business size, and they're not all after the same thing.

While it's true that the press only tends to report on attacks at the likes of Sony or Google, there are many more incidents which never get mentioned.

SMALLER COMPANIES

Symantec (a leading cyber security organisation behind the Norton Security software) reported that in 2014 attacks on small- and medium-sized companies accounted for 60% of targeted attacks. That accounted for a staggering increase of 30% on the 2013 figures. Symantec added that cyber attacks are the fastest growing crime in the UK, with the number of incidents increasing by 80% since 2010.

Research shows two thirds of Federation of Small Businesses (FSB)* members have been a victim of cyber crime in the last two years, costing an average of £3,000 per business. This is a serious barrier to growth. Businesses need to take steps to assess the risks of online crime and fraud

*Source ref: https://www.fsb.org.uk/standing-up-for-you/policy-issues/business-crime/cyber-security

THE 'CLOUD'

Many businesses see 'Cloud' technology as a safer and more economical alternative to hosting and storing data. Unfortunately, Cloud technology is no different to traditional outsourcing methods. In fact, rather than reducing the risk, it can actually increase risk due to the loss of control to third parties and the fact that data is stored at shared data centres.

Clearly, what was and still, is a significant issue and challenge for FTSE 500 companies is now a serious problem for every business, including yours. If you have any kind of IT footprint however big or small the threat of cyber crime has to be taken seriously.

An example of this is a data breach that happened in June 2018. Typeform is a survey company which suffered a data breach. This breach affected several businesses who use its software to conduct customer surveys/quizzes. Attackers managed to gain access to data backups which contained information people had submitted via these forms.

BUT ARE YOU REALLY AT RISK?

If you have, or do, any of the following, then yes, your business is at risk:

- Require computers for work
- Allow staff to use email and the internet.
- Store any customer or supplier details (specifically addresses and credit card details).
- Have a website.
- Have a transactional website (where customers can send their personal details).
- Keep employee and payroll details on a network.
- Allow suppliers to access your network or an extranet.

The individuals, groups and organisations behind cyber attacks are located all over the world and are notoriously difficult to track down. And while there is a huge variety in the nature of attacks, here are most, if not all, of the reasons the attacks are carried out:

FINANCIAL GAIN

There are people who have criminal intentions and wish to gather debit or credit card details, and other personal information, which they can use for their own financial gain.

Due to low levels of expertise, this group targets the smaller, 'easier' targets, such as small companies that might not have the resources to employ effective security but still might have a wealth of financial details stored in their systems.

HACKTIVIST

Digital hackers known as 'hacktivists' are generally assumed to be driven by political or ethical values. One of the most well-known hacker groups is Anonymous, who have been responsible for a number of high profile attacks. Including an attack on PayPal and MasterCard when they pulled their services from WikiLeaks over the affair of the leaked US embassy cables in November 2010. Lulz Security (or LulzSec), another well known group, were behind the compromise of Sony user accounts in 2011.

ESPIONAGE

Disgruntled employees, who may have insider information and active login details, are also a potential (and often underestimated) cyber threat.

Competitors, with the wish to obtain insider information, have also been known to use untoward methods to gain an upper hand in a competitive market.

Cyber attacks are no longer just restricted to the Sonys and Googles of this world. For every high profile attack we hear about in the press, there are many others that go unreported.

A look at "How"

Cyber criminals are clever, resourceful and unrelenting in finding new ways of getting what they want.

While there are several ways in which attackers can breach your security, here are some common methods they employ.

PHISHING

Attempting to acquire data such as passwords or banking details by masquerading as a trustworthy email sender.

TROJAN

A program with a benign capability that conceals another malicious program behind it.

ROOTKIT

A malicious piece of software designed to enable ongoing access to a computer while hiding the processes or programs from detection.

VIRUS

A program that can replicate itself and spread from one computer to another.

SPYWARE

A piece of software that is installed on a computer to collect information about users' actions without their knowledge.

DRIVE-BY DOWNLOAD

A download that happens without the person's knowledge or without them understanding the implications.

FUNDS TRANSFER FRAUD

A type of fraud that typically involves promising the victim a significant share of a large sum of money. It begins with the fraudster requiring a small up-front payment. If a victim makes the payment, the fraudster then invents a series of further fees for the victim or simply disappears.

MALICIOUS MEMORY STICK

An Infected USB stick (for example those received by corporate employees as an unsolicited gift) that contains a piece of malicious software that is uploaded when the USB is plugged into a computer.

DDoS (DISTRIBUTED DENIAL OF SERVICE) ATTACK

This is caused by flooding a website with more traffic than the host server can handle, forcing it offline. It is a favourite tool of 'hacktivist' groups such as Anonymous.

CRYPTOJACKING

The unathorised use of a target's computer systems to mine cryptocurrency.

A look at "What"

It may be easy to put a monetary value to physical stock, and estimate the risk of its loss, but what about data?

Businesses naturally gather and store much larger amounts of data than physical assets. But because it can be so hard to understand the financial value of the data you hold, it's not always easy to know what measures you need to take to protect it, or what would happen and how to respond if that data were lost.

In addition it is not just a loss of data, it is also access to, if and when the data subject requires it.

PROTECTING YOUR DATA

The first step is to take a good look at your digital set up and to answer the following questions:

- Are you aware of your obligations under the GDPR?
- What cyber security precautions have you put into place?
- What measures have you taken to keep your customer and supplier data safe?
- Are you aware of the remit of the GDPR and of the financial consequences?
- Do you have the appropriate insurances in place should you become the victim of a cyber attack?

THE NEXT STEP IN THE CASE OF A BREACH

In such a case, you'll need a clear answer to the following questions:

- What do I do next?
- What is my security policy and disaster recovery plan?

THE COST

This can be broken down into First- and third-party costs. First-party costs involve the cost of recovering the lost data (if at all possible) and the cost of rectifying the disruption (if there was one). Third-party costs, on the other hand, are those you incur from any customer and supplier actions taken against you, as well as what you have to pay in fines and penalties from regulatory bodies such as the Information Commissioner's Office (ICO).

The GDPR

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed.

The GDPR has seven princples which provide:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

The Information Commissioner's Office is the UK's independent authority who upholds rights in the public interest. There are a number of enforcements the ICO have imposed since GDPR came into force. You must report notifiable breach to the ICO without undue delay, but no later than 72 hours.

IMPACT ON BUSINESSES

- The reforms create a more efficient business environment by cutting red tape and reducing the costs many businesses must endure if they process personal data across borders.
- The reforms also make new data protection standards extraterritorial by requiring all businesses to comply while they do business in an EU member state. This ensures that all players within the EU are bound by the same rules, regardless of where they were established.
- Finally, the new rules call for data processors to implement data protection safeguards from the early stages of product and service development to ensure that data protection becomes the norm—by design and by default. This includes appointing a data protection officer (DPO) responsible for data protection compliance.

IMPACT ON SMALL AND MEDIUM ENTERPRISES

The new rules also level the playing field for SMEs by requiring them to:

- Appoint DPOs only when the SMEs' core activities require regular and systematic monitoring, or if they process special categories of personal data (for example, data that reveals racial origin or religious belief);
- Keep processing records only if processing is not occasional or is likely to put rights and freedoms at risk; and
- Report data breaches to individuals only if the breaches place their rights and freedoms at high risk.

In situations where SMEs must appoint DPOs, the new rules do not require that officers be full-time employees. The use of ad hoc consultants is sufficient to satisfy this requirement.

Key Facts about the GDPR

What rights does the GDPR give individuals?

- Right to be informed: Organisations must be transparent about how they use personal data
- Right of access: Individuals have the right to access their personal data
- Right to rectification: Individuals have the right to have their personal data rectified (for example, if it's inaccurate or incomplete)
- Right to erasure: Individuals have the 'right to be forgotten'-meaning, they have the right to have their data deleted
- Right to restrict processing: Individuals have the right to block or suppress processing of personal data
- Right to data portability: Individuals have the right to obtain and reuse their personal data for their own purposes across different services
- Right to object: Individuals have the right to object to processing of their personal data
- Rights in relation to automated decision making and profiling

WHAT ARE THE MAXIMUM FINES THAT CAN BE IMPOSED?

€10 million (roughly £8 million) or 2% of your annual turnover-whichever is higher-for not keeping proper records, violating data breach notification requirements, failing to appoint a Data Protection Officer when necessary, and more

€20 million (roughly £16 million) or 4% of your annual turnover-whichever is higher-for violating the basic principles for processing, ignoring data subjects' rights, incorrectly transferring personal data, and more.

WHAT QUALIFIES AS PERSONAL DATA?

Any information that can directly or indirectly identify a person, such as:

Name, identification number, location data or an online identifier

Factors specific to a person's physical, physiological, genetic, mental, economic, cultural or social identity

If you're unsure whether something is personal data, the best practice is to treat it as such.

WHERE CAN I GET HELP?

Support can be found on the ICO website (https://ico.org.uk fororganisations/guide-to-the-general data-protection-regulation-gdpr/)

With most cyber incidents, there are five key stages:

INCIDENT

Digital data has been lost or leaked from the company system. It could be a loss of data from a PC, laptop, mobile phone, or tablet, or it could be misappropriated personal details, a breach of client information, or a full-scale cyber attack.

FINANCIAL CRISIS

The financial ramifications can begin to stack up after a data breach:

- Possibile regulatory fines.
- Legal action from the wider network of victims.
- Cost of diagnosing the breach and determining what has been lost.
- Cost of reconfiguring networks, re-establishing and increasing security, restoring the data, and rebuilding systems.
- The financial impact on the business' ability to operate.

IT CRISIS

The IT department or agency needs to quickly assess the situation and answer the following questions:

- Was it a leak, a loss, or has the company been hacked?
- How was the data lost or taken?
- When was it lost or taken?
- Where is the data now?
- Can the leak be contained?
- Will the server have to be shut down?
- Will the server need to be replaced?
- Does the business need to replace its software?
- What does the disaster recovery plan state?

LEGAL AND REGULATORY

- Legal advisors will need to establish if the incident amounts to a breach for the purposes of GDPR. Not all security incidents amount to personal breaches.
- Legal team will need to maintain a log of the breach, recording the breach management process. This may need to be submitted as evidence to the Regulator.
- In accordance with the GDPR, failure to notify the regulator or affected data subjects can result in a fine up to €10million or 2% of the organisation's global turnover.
- YOU WILL NEED TO Demonstrate there have been learning and consequential improvements to data security following the breach.

PR CRISIS

The news of a cyber breach can spread quickly, especially through social media, and this can have an immediate effect on people's confidence in the company. This type of situation requires careful management:

- Do customers have to be told that their data is lost?
- Who else has to be informed?
- What is the best way to do this?

You'll need to take swift action and have a carefully managed PR response to regain trust.

A Denial of Service (DoS) & Business Interruption Scenario

INCIDENT

To most competitive companies, access to the internet and internal systems is imperative in order to function normally and provide services to customers. Accordingly, a malicious DoS (or DDoS) cyber attack poses a significant risk of major disruption, which may in turn may have serious financial and reputational ramifications. A swift and effective response is crucial to contain the breach, and mitigate exposure to business interruption losses and third party claims. Some issues to consider are:

FINANCIAL

- Threat actors may hold the system to ransom until a ransom payment is made;
- As soon as the system is offline, the organisation will be incurring business interruption loss;
- The ICO, or other relevant regulators may impose a fine;
- In the longer term, there may be reputational consequences, with customers switching to alternate providers due to their concerns about unavailable services or security issues.

IT AND FORENSIC EXPERTS

- IT vendors will provide a quick determination of the cause of the incident, analysis of system logs and securing/isolating affected systems;
- It is crucial to get the system back online as quickly as possible using clean back-ups where possible, and check whether data has been lost or compromised in some way;
- In the longer term, a number of system improvements should be implemented, including protective firewalls, larger and more robust networks to absorb DDoS attacks and monitoring software to keep track of network traffic.

LEGAL AND REGULATORY

- Determination of whether the event amounts to a personal data breach and whether a notification needs to be made to regulators and law enforcement. Time limits need to be considered for regulators – for example, in the UK the ICO must be notified within 72 hours of awareness of a breach;
- Advise upon preservation of evidence and the importance of ensuring privilege is maintained;
- Advise on potential civil liabilities as a result of system downtime. For example, if customers are prevented from accessing financial records during an attack, this may lead to claims for the distress and inconvenience, and/or lost profits. DDoS attacks could also give rise to claims against service providers for failing to provide contractually-guaranteed service levels.

PR

- A PR team will be able to draft a carefully curated media response and communications to affected customers.
- If the system remains inaccessible for an extended period of time, the PR team will assist with the ongoing management of media reports and customer expectations.

The potential fallout

Should you be the victim of a cyber attack, valuing your data would only be a part of the overall cost that your business could face. In both the short-term and the long-term, the damage to your company could be much more serious and wide-ranging than you initially thought.

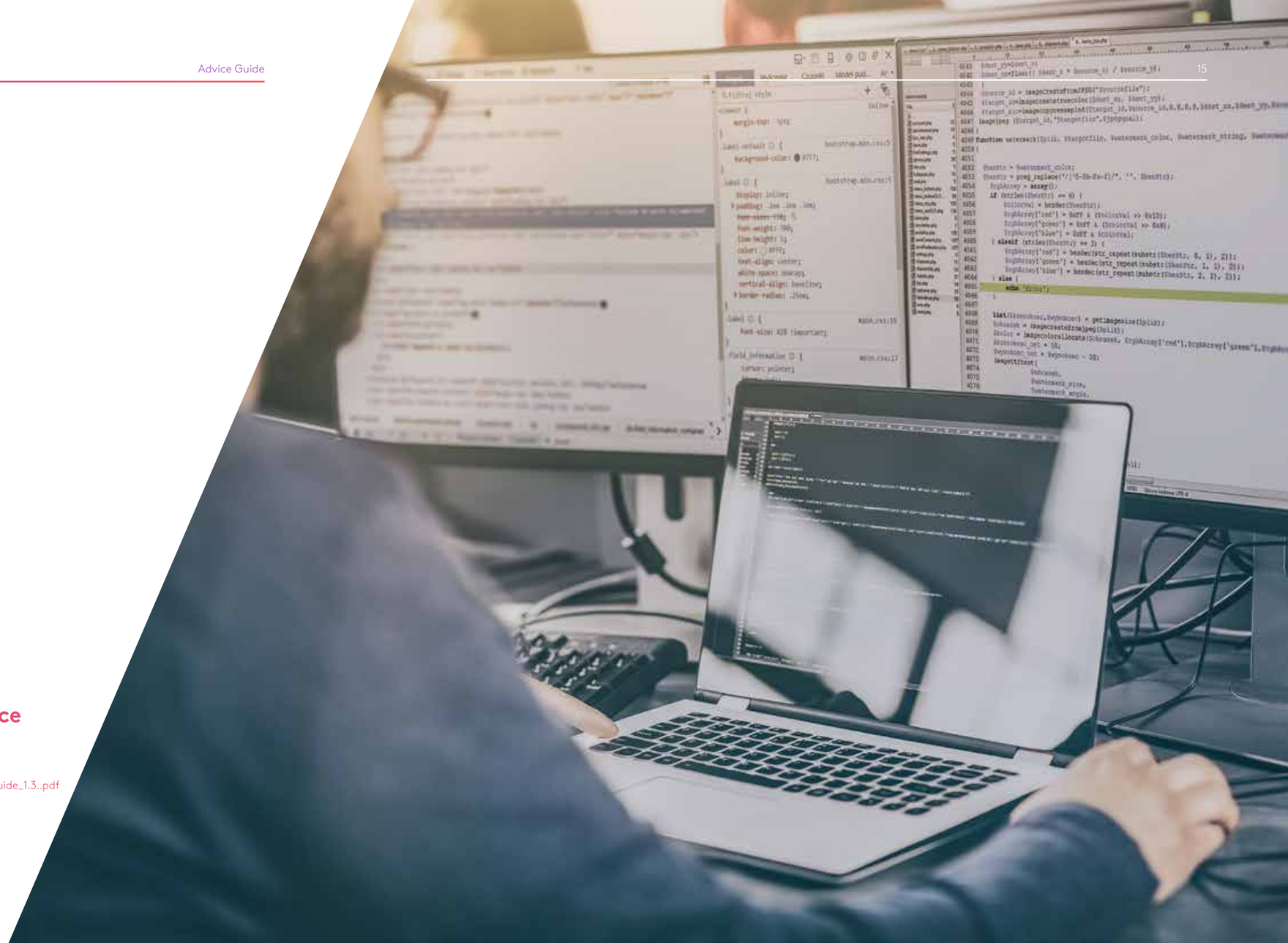
As with most types of 'incidents', the initial preperations aren't necessarily what cause the issue - it's the consequential costs that flow from the incident. For example, if you were to purchase just property insurance, then your premises, its contents, and your stock would be covered in the event of a catastrophic fire. But what about the financial impact of not being able to trade while the building is being rebuilt and your stock is being replaced?

This is why most businesses will also purchase Business Interruption insurance to cover their losses during the period in which they are unable to trade.

Businesses need to use the same rationale when considering the financial impact of a cyber attack.

If you're a small or medium-sized enterprise, there's around a 50% chance that you'll experience a cyber security breach.

Source (pg 4) - https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/cyber_security_small_business_guide_1.3..pdf



Breach Scenario

JobChamp is a fictional online start-up recruitment agent. They are a subscription-based service, and use social media to target customers. JobChamp have experienced rapid growth: they have 100,000 customers on their database and a turnover of £5m per year.

Imagine that JobChamp have discovered that hackers have accessed their customer database and stolen all 100,000 customer details (including names, email staff addresses and financial/salary information).

Who will they need to help with the fallout, and how much will it cost them?

There are many different ways a cyber attack can affect your business, and the impact will depend upon the severity of the incident. Whilst the above example represents the type of losses a business could suffer, those losses could be smaller, or a great deal larger. Many of the costs which arise in the aftermath of a breach are hidden, or intangible. Initial response costs (such as legal, IT and PR) are incurred immediately and are of crucial importance to comply with regulatory requirements. Other costs may take years to unfold as the true effects of business interruption reverberates over time, and legal costs will increase as stolen data is used against the company or third party claims start to materialise. With this in mind, the importance of understanding what is at stake is of paramount importance to stakeholders of your business.

LEGAL

advice on legal and regulatory exposure and immediate steps

notification to regulator (ICO or any other EU regulators)

notification to customers

defending third party claims from affected customers

advising on potential recovery actions against third parties

INDICATIVE COST: £15,000 - £20,000 PLUS VAT

PR

assist with managing media response and press releases

draft messaging to customers

assist with website FAQs and social media response

back to business advice

INDICATIVE COST: £5,000 - £10,000 PLUS VAT

HIDDEN COSTS

cost of sending bulk emails to affected customers through a dedicated platform (to avoid email bounce-backs and spam filters)

possible need for external call centre to handle potentially hundreds of calls from affected customers

bespoke complaint management system

INDICATIVE COST: £10,000 PLUS VAT

THIRD PARTY CLAIMS FROM CUSTOMERS

INDICATIVE EXPOSURE: £200,000
OVER A 5 YEAR TIME FRAME

IT

secure critical evidence

determine source and scope of the attack

advise on future threat protection

advise on hardware replacement

assistance with ICO notification

INDICATIVE COST: £15,000 - £20,000 PLUS VAT

CUSTOMER GESTURES

Dark Web / Credit monitoring offered to customers
This cost is based on an average of 10% take up by Jobchamp customers

INDICATIVE COST: £100,000 PLUS VAT

LONG TERM EXPOSURE

Business Interruption / lost value of customer relationships

Increased cost of developing new business

Devaluation of trade name

Loss of intellectual property

INDICATIVE EXPOSURE: £300,000 OVER A FIVE YEAR TIMEFRAME

TOTAL COST TO JOBCHAMP

This is before regulatory fines or sanctions are considered, which can be up to 4% of annual turnover, or Euro 20m under the GDPR.

INDICATIVE TOTAL COST / EXPOSURE: £660,000 PLUS VAT

Source: Indicative figures provided by Kennedys Law

Effective solutions

There are two categories of exposure: first party exposure, which relate to your company's own incurred costs, and third-party exposure, which are the costs you incur from the wider effect of the fallout.

First party

CRISIS MANAGEMENT AND NOTIFICATION COSTS

Sometimes the consequential losses can far outweigh the cost of fixing the initial problem.When a network or cyber incident occurs, it can have a devastating effect on the reputation of your business and the confidence of your customers. This, of course, needs to be carefully managed.

The initial investigation into what happened and how may necessitate the specialist services of a forensic expert to understand. Your business may then need to notify any individuals whose data may have been breached, which all comes at a cost.

BUSINESS INCOME AND EXTRA EXPENSES

In the event of a cyber 'incident', this cover ensures that your business can survive the impact of the loss of revenue as a direct result of failure of its systems.

DATA COVER

Loss of data is not only a third-party issue. While there are financial consequences that you may face following a breach, there are also first-party costs which need to be considered.

Most policies will cover the costs associated with the inability to access, or loss of, data as a result of a network security breach or unauthorised use of IT system by a disgruntled employee, a virus, or even simply human error or IT malfunction.

Data Cover typically includes the cost to reinstate the data.

HARDWARE COVER

Physical loss/damage to computer hardware.

Third party

PRIVACY BREACH

Liability arising from such breaches.

VIRUS TRANSMISSION

The transmission of a virus to a Third Party can have the same effect on their IT systems, triggering a claim for damages.

INADVERTENT ACTS

Liability for damages due to activities perpetrated through a business's IT systems.

COPYRIGHT

Inadvertent infringment on another business' or person's copyright.

And a real cost solution

Even though Cyber Insurance is relatively new to the UK, it's not a new type of coverage. As with any market environments a range of choices is good for businesses.

WORKING WITH THE UK'S TOP CYBER LIABILITY INSURERS

Being a "whole of market" broker, we have full access to the leading Cyber Liability Insurers in the UK, to include Hiscox Insurance Company Ltd, CFC Underwriting Ltd, Chubb European Group Ltd and AIG Europe UK Ltd.

Premiums can start at £500 for a £1M limit subject to completion of a onepage proposal form.

Frequently Asked Questions

We realise that every business is different. This is why we tailor everything we do to your individual requirements. However, here are the most common questions we get asked.

WON'T OUR OTHER INSURANCES COVER US?

While it's true that policies such as Professional Indemnity and Crime offer an element of cyber cover, they only offer minimal protection compared to a true Cyber Liability policy.

For instance, the main purpose of Professional Indemnity is to protect you against the consequences of a wrongful act. In other words, it is there to protect you if you do something wrong. However, a lot of the exposures and risks faced with cyber crimes are not the fault of one individual, and therefore a Professional Indemnity policy wouldn't respond.

Professional Indemnity is also mainly a third party policy that is more concerned with post-loss costs (the costs of defence for example). A lot of the costs associated with a cyber incident are investigation costs associated with trying to understand what has happened, when it happened, and how.

Unlike a Cyber Liability policy, a Professional Indemnity policy won't cover first-party losses, such as damage to hardware and software.

In the event of a cyber breach, a Professional Indemnity policy also won't cover notification costs (these are the costs of a breach consultant to advise whether or not the business needs to notify its clients as well as the costs of actually notifying individuals).

In short, if we were to compare a cyber incident to a house fire, using a Professional Indemnity policy to respond would be like using a watering can.

WHAT IF WE HAVE A ROBUST SOLUTION?

No company is safe from a data breach, irrespective of security standards. It's practically impossible to negate all internal and external threats. A lot of claims come from human employee errors.

WHAT IF WE OUTSOURCE OUR SECURITY?

More companies outsource elements of data storage to Cloud and other third-party platforms. The security standards of any company to whom you outsource data must be vetted to ensure they maintain approved requirements, particularly as the nature of their activity and the volume of data they store makes them an attractive target. Regardless of the contract the outsourcing company will not be held responsible.

WHAT IF WE'RE NOT IN A TARGETED INDUSTRY?

You may think this to be true but cyber criminals are opportunists and will attack any easy targets. You may also be open to attacks by employees or even competitors. Also, criminals often use 'non-targeted' organisations as a backdoor entry to a larger, more desirable target.

WON'T THE COST OF THIS COVER BE HIGH?

As highlighted on page 19 premiums can be modest in comparison to the potential cost of cyber incident. Premiums can start at £500 for a £1M limit.

WHAT IF WE'RE NOT SUBJECT TO REGULATION?

Regulation only represents a single cost of a cyber breach. Organisations have a responsibility to their clients to keep their data as secure as stipulated under GDPR. Also, the reputational harm of a data breach can out-price any regulatory cost associated with a data breach. Even without regulation, industries (such as the payment card industry) can, and do, issue rigorous fines. Everyone is subject to GDPR, even if only handling employee data

ARE WE TOO SMALL TO WORRY ABOUT CYBER CRIME?

As the large organisations continue to enhance their security infrastructures, criminals have started to look for smaller 'easier' targets. The dangers are therefore not restricted to FTSE 250 companies. Smaller organisations might not have the resources for effective security to prevent a loss, or for effective recovery strategies after a loss.

WE'VE NEVER HAD A CYBER BREACH IS THIS COVER REALLY FOR US?

Although the majority of businesses have not had a claim, the environment has changed and will change even further in the near future.

Companies are more susceptible to cyber threats than ever before. Future legislation is likely to augment current industry standards, suggesting that the financial and operational effects of a data breach will become more onerous for organisations that have suffered or contributed to a breach.

Examples of claims

To illustrate how we can help your business to protect itself from the effects of cyber crime, we have included the following real-world examples. They show just how much damage cyber crime can cause.

CLAIM 1: SOCIAL MEDIA CONTENT

A charity was sued for social media content posted by an employee.

Understanding that social media was becoming key in fundraising and gaining awareness for their organisation, a UK-based charity's marketing department became very active on several networks including Twitter, YouTube, and Facebook. It also actively encouraged their employees to post content on these networks.

Even though the charity had a fairly stringent social media policy in place, one of its employees posted defamatory content out of hours about a rival charity. The comment led to a defamation claim against the organisation.

COVER RESPONSE

Some policies not only include content posted during the course of regular hours, but also content disseminated after hours and even for non-business related activities.

CLAIM 2: ONLINE RETAILER'S SITE CRASHES AT CHRISTMAS

For an online retailer, the weeks before Christmas are some of the most crucial in meeting income goals for the year. In fact, one online retailer who specialised in gadgets took over 40% of its annual income during the months of November and December.

When the gadget retailer's website was brought down for an extended period of time due to a Distributed Denial of Service attack (DDoS), just three weeks before Christmas, the system downtime resulted in a much larger percentage of annual earnings being lost than there would have been for the same amount of time at any other point in the year.

COVER RESPONSE

Some policies not only include business interruption or loss of business income, they additionally provide this cover on an adjusted basis, ensuring that the level of cover under the policy matches clients' fluctuating needs.

CLAIM 3: HUMAN ERROR

Many businesses don't think they need cyber insurance because they have good IT security in place. But it's people who are often the weakest link.

A law firm was tricked into transferring money to fraudsters following an email purporting to be from Microsoft. An employee clicked on a link which took them to what appeared to be a legitimate looking webpage and entered their credentials, providing their login details to a fraudster. This allowed the fraudster to monitor communication and gather confidential data including details on an imminent property transaction. A fake email was sent providing the seller with wire instructions and the money was transferred to the fraudster's account.

COVER RESPONSE

Some cyber policies provide crime coverage to protect against losses such as this.

CLAIM 4: BREACH OF COMMERCIAL CONFIDENTIALITY

As part of a tender for business, a supplier sent its price list to an engineering firm. The list was subsequently forwarded, inadvertently, to a rival of the original supplier.

Once in possession of the list, the competitor was able to undercut the supplier's prices in order to win business.

The supplier therefore brought legal proceedings for loss of future earnings against the engineering firm.

COVER RESPONSE

Due to the loss emanating from a cyber 'act' or 'incident', the engineering firm's Commercial Combined could not respond (due to a E-Risk exclusion) and therefore the loss fell under the Cyber Liability policy.

A Cyber Policy can cover the legal expenses and the cost of settlement.

CLAIM 5: ROGUE EMPLOYEE

An employee of a large consumer reporting agency stole the personal information of a number of clients to sell on to other parties.

COVER RESPONSE

- Costs of forensic experts to establish what Data was stolen and from which individuals.
- Costs of notifying the individuals concerned.
- Costs of credit monitoring for the affected individuals to make sure they suffered no ongoing losses after the information theft.
- Costs of a legal breach coach to prepare the business for investigation.
- Costs of representing and defending the business in the ensuing legal action.
- Costs of damages that were awarded against the business.

CLAIM 6: HACKING

A payment card processor's system is hacked and the credit card data it holds is compromised.

COVER RESPONSE

- Costs of forensic experts to establish what data was stolen from which individuals.
- Costs of notifying the individuals concerned.
- Costs of credit monitoring for the affected individuals to make sure they suffered no ongoing losses after the information theft.
- Costs of a legal breach coach to prepare the business for investigation.
- Costs of PR consultancy to advise and guide the firm with its external media communications about the event.
- Costs of professional representation or the investigation by the payment card industry.
- Costs of representing and defending the business in the ensuing legal action.

In short

Cyberspace has made life and business easier, but with that added ease come new risks to mitigate and challenges to overcome.

Once you are aware of the dangers of cyber crime, your business needs to quantify the possible financial impact should it be the unfortunate victim of an attack. As we keep saying, no business is safe from cyber crime.

THE COST OF A CYBER ATTACK SHOULD NEVER BE UNDERESTIMATED

With the average cost of the worst security breach for small organisations being between £35,000 and £65,000, companies are being urged to take the threat of cyber attacks more seriously. Armed with the information in this document, you should be able to start the process of making an informed decision on how best to protect your digital assets.

While the IT security of your business will form a solid front-line defence, thought still needs to be given to how to protect your business should this fail.

THE VALUE OF CYBER RISK INSURANCE

Only a cyber Insurance policy can significantly mitigate the financial impact to your business in the event of a significant cyber breach occurring.

Your world is our focus

We're proud to be one of the top five independent Chartered Insurance Brokers in the country, with over 700 staff in 21 regional locations. Trusted by over 100,000 clients across the UK, our services are wide-ranging, but our customer service is always personal. We treat everyone as an individual, paying close attention to the smallest detail.

At Aston Lark, we work across all commercial sectors, and a wide range of specialisms in areas such as Motor Trade, Haulage, Construction and Film & Media. We have an Employee Benefits team who will work with you to implement a suitable benefits package that aligns with both your budget and your staff profile. We have a dedicated in-house claims team on hand when you need us the most, and an award-winning Private Clients division providing expert guidance for individuals.

We pride ourselves on our integrity, our experience and our commitment to always deliver. We are proud to be recognised for our ethical good practice, the pursuit of excellence, and for achieving the highest standards for our clients. By getting to know you, we understand you better, and while insurance can be complex, we aim to make things simple and clear. What matters to you, matters to us.

Call us on 020 3846 5274

If you're interested in learning more about how to fight cyber crime, you can find more information on our website.

astonlark.com/cyber

ASTONLARK

A howden company

YOUR WORLD IS OUR FOCUS

www.astonlark.com

AL-COM-110-0522

Chartered Insurance Brokers