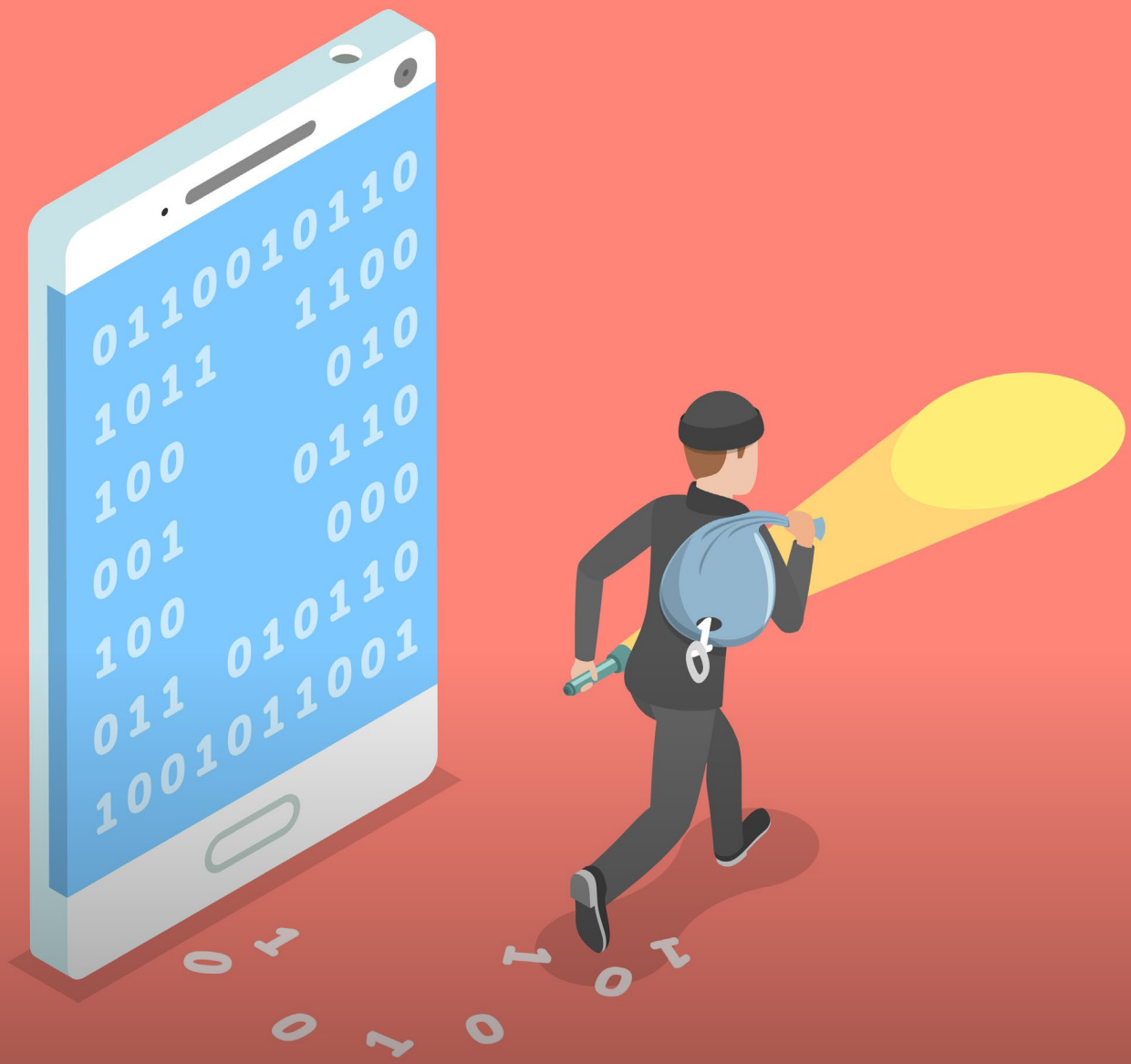
GAUNTLET
RISK MANAGEMENT LTD



JAMES AND THE GIANT BREACH

Ahead of 2020's Roald Dahl Day on September 13, we've taken up the baton here at Gauntlet Business Insurance (gauntletbusinessinsurance.com) to urge the UK's SME community (and that may include you) to not let coronavirus, and working from home, distract it (or you) from doing things by the book when it comes to cyber protection and GDPR compliance.

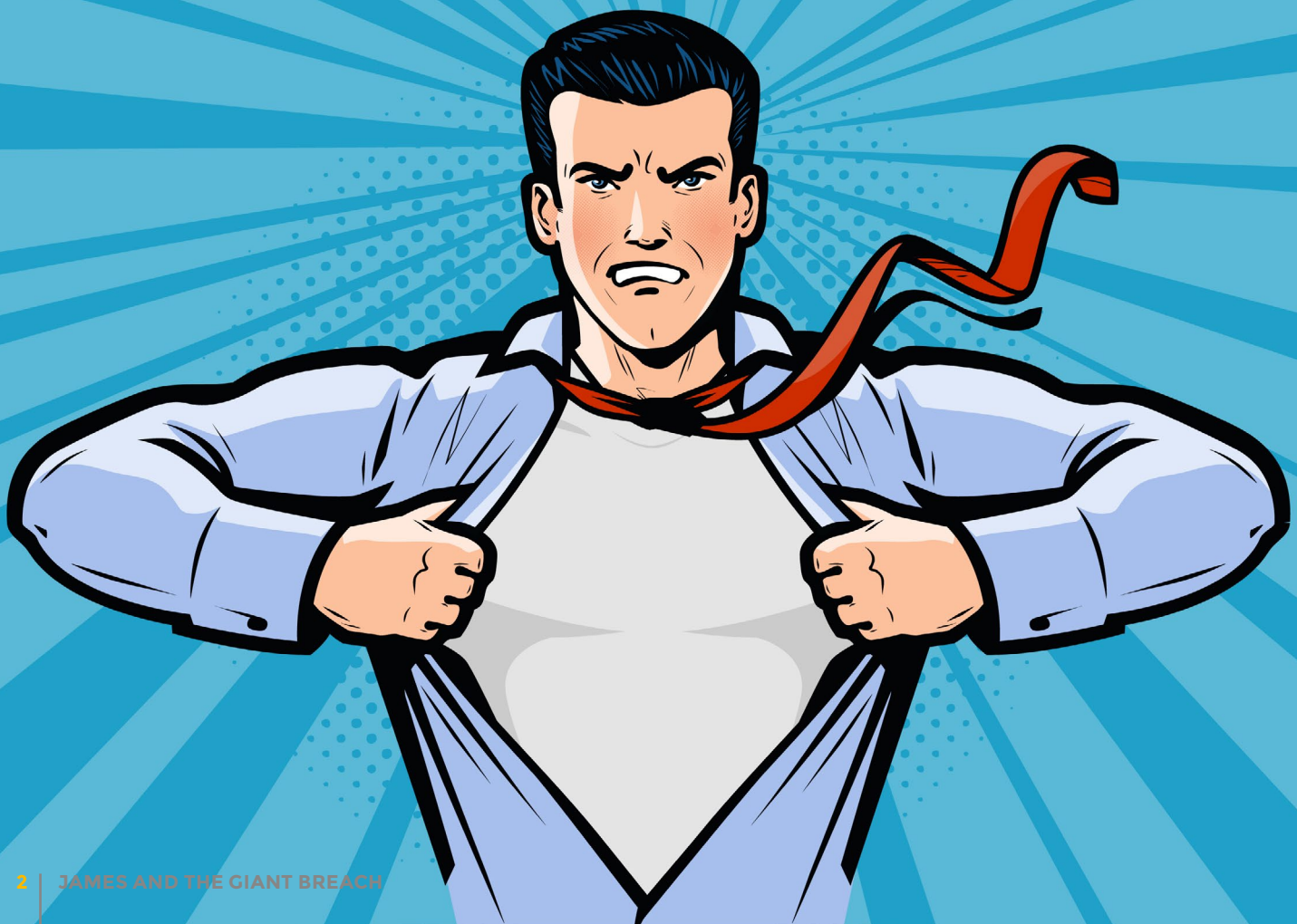
In the year, up to and including July 2020, there have been more than **19 billion data breaches**, with key sectors attacked in July being healthcare and health science, education, tech and media.[1] June saw Avon's UK website attacked and taken offline.[2] In May, EasyJet had 9m records breached.[3] But it's not just the big boys. **88% of UK businesses have experienced breaches in the last 12 months.**[4] And still the cyber insurance message does not seem to be getting through.

We are on a quest to do something about this. We have commissioned our own research[5], to assess how lockdown may have affected cybersecurity but to also find out how the average Charlie, in or outside of his chocolate factory, knows about cybercrime and how it ticks.

Read on, to discover how various tales of the unexpected could catch you out and make you the central character in a 'James (or Jane) and the Giant Security Breach' tale of woe.

DANNY: SUPER-CHUMP OF THE WORLD

The trouble is, we all feel we're invincible. Hackers won't fox us. We're far too small for them to bother with. Well, ahem. **One small business in the UK is breached every 19 seconds**, according to Hiscox and there are 65,000 attempts per day, to hack small businesses.[6] 4500 of those are successful. Yes, every single day.



In the past 12 months:

- Nearly 9-in-ten UK companies were breached by cybercriminals in the past 12 months
- 37% of UK companies reported a data breach to the ICO (Information Commissioner's Office).
- 17% reported more than one breach
- 33% of UK organisations lost customer data
- 48% of UK organisations have been hit by a ransomware attack in the past year (source: Sophos)

So, are we really so much cleverer than all of these companies? Or do we just not appreciate the size of the threat? Maybe not.

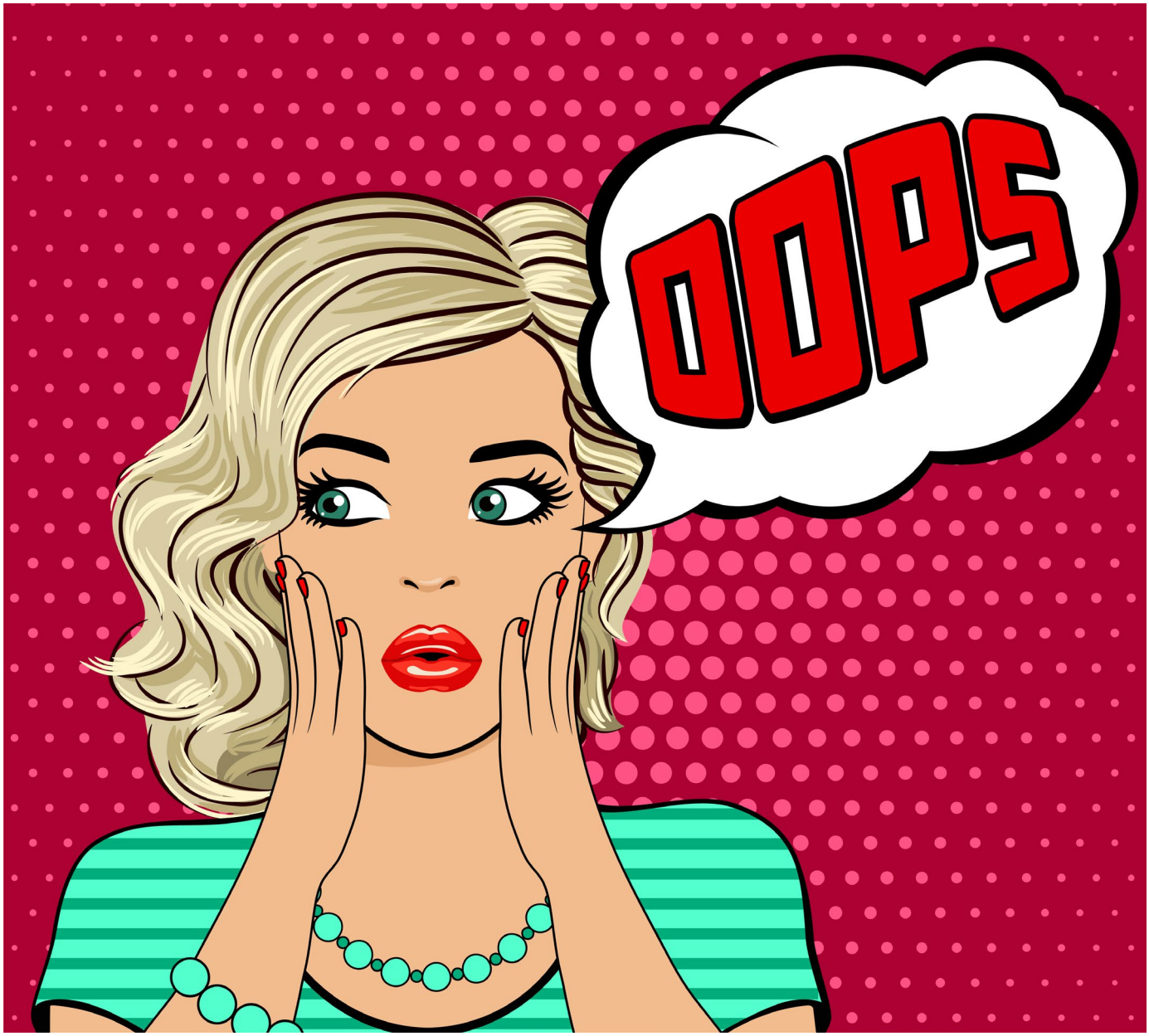
When we had an independent research company carry out our Gauntlet Business Insurance survey, we discovered that:

- **Nearly a third of Brits (32%)** feel they are more likely to get coronavirus than suffer from cybercrime
- **More than one in 20 (6%)** just don't feel a cybercriminal would be interested in attacking their place of work. This is despite 12% saying they, personally, have been a victim of cybercrime and 41% believing more British businesses will be victims of cybercrime because of working from home.

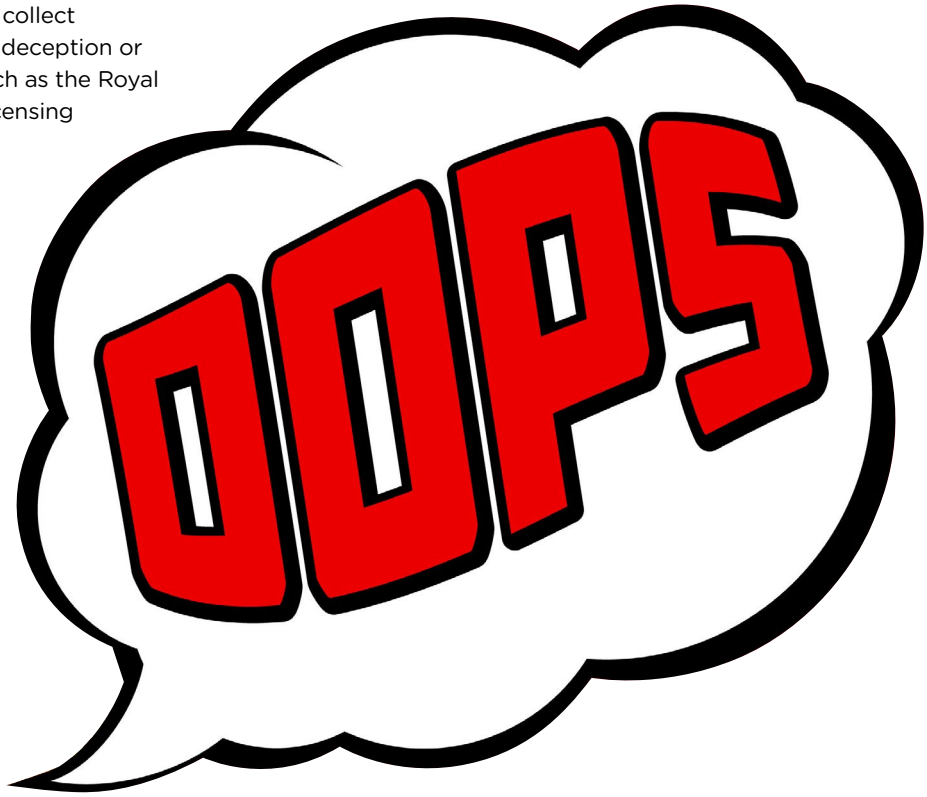
Nervous? We think British businesses should be, according to what else we discovered. Do read on!

THE BIG FOOLISH GAFFE

According to security software provider , Symantec, **one in every 3722 emails in the UK** contains a phishing attempt.[7] The trouble, according to our own independent Gauntlet research survey, is that a **third of people (33%)**, don't know what phishing is and, if you don't know what something is, how can you avoid it? The other issue is that such phishing attempts have increased even more during the coronavirus pandemic. "Oops" indeed.



Phishing is an attempt by a cybercriminal to collect information from an email recipient through deception or passing themselves off as another entity, such as the Royal Mail or a bank or building society; the TV Licensing Authority or Paypal, all of whom have been victims. Basically, the cybercriminals dangle a hook within your inbox and hope you will take the bait and bite, hence the term phishing.



The Big Foolish Gaffe that people make within the world of phishing, tends to be that of clicking on a malware link. And, according to Gauntlet's research, **only just over half of people (55%)** know what that is.

Malware is a condensed word standing for 'malicious software'. It can harm computers, devices and your cybersecurity in general. It's a type of software, built by cyber attackers and malware comes in various forms. It comprises viruses, spyware, ransomware and what are known as Trojan Horses.[8]

Malware can actually be installed on your computer or device for very many months without you knowing. Some is injected into your computer through security flaws – gaping holes so far as a cybercriminal is concerned. **This is why you should always update your software, as soon as a new software update is issued.** You can also pick up malware by visiting an infected web page. There are now even mal-advertising sites, which are hosted in legitimate advertising sections, on legitimate websites, but which contain malware code, so when you click, 'bingo', malware is injected into your system.

But the **malware link** is really the stuff of everyday life and so productive for cybercriminals because it uses a technique called s**ocial engineering**. The phishing or spam email will probably play on an emotion – often fear – urging you to check on your bank account or a delivery – or something else that, in the moment, panics you or compels you to click on the link provided in the email. It might not be a rational thing to do, but you could be busy, in a meeting and just wanting to quickly check, on the school run before you get to work, or somewhere where you just don't have the time or means to check it out by calling someone or not using that link at all, but going to the website or bank or shop, or whatever it is, direct.

Despite the lack of knowledge of malware and phishing, **22% of people told the Gauntlet research survey that they know what social engineering is**. We suspect, in the time of coronavirus, some may have confused it with social distancing … but that's what cybercrime does … it confuses you and makes you commit that gaffe.

Some of those we surveyed have already been caught out. **One-in-eight people said they have clicked on a malware link in the past**. Yet, alarmingly, **only 8%** worry about clicking on a malware link causing an issue in their workplace – not very comforting for employers!

But there is another Big Foolish Gaffe of which to be aware, which is nothing to do with cybercriminals. In 2018, it was said that a staggering **88% of data breaches in the UK are caused by human error** (Kroll).[9] This includes sending sensitive data to the wrong recipient, losing or leaving paperwork in a public place and storing data where it is publicly accessible. With GDPR regulation coming down hard on data negligence, and basing fines on company turnover[10], this is a very worrying statistic. When there's no cybercriminal to blame, the buck really does stop with you and your company.

This has been all too well appreciated by the Just Eat brand in June 2020, as its Cleveleys branch, in Lancashire, chose to dump dozens of receipts, showing customers' personal details, in an alley, breaching GDPR regulations. Another human error causing data breach issues.

The Information Commissioner's Office said of this: "All organisations have a duty to keep personal data secure, whether in electronic or paper format. Where necessary, we will take appropriate action, which can range from giving advice, to fines."

THE FIENDISH MR FOXER

Cybercriminals are clever manipulators, knowing how to push your buttons and play into their hands. In 2019, **48%** of British companies were hit by what is known as a ransomware attack (Source: Sophos).[11]

Such an attack is carried out using a type of malware that encrypts files and which then swiftly leads to the victim being told to pay a ransom, if they wish to have their system restored. **In 2019, 13% of the UK organisations hit by a ransomware attack, paid the blackmailers request.** Having paid, the victim typically receives a decryption key, which they can use to restore their system. There is no way around this, if you need your files back, as the clever Mr Foxers are the only ones to know the mathematical key that will decrypt their ransomware.

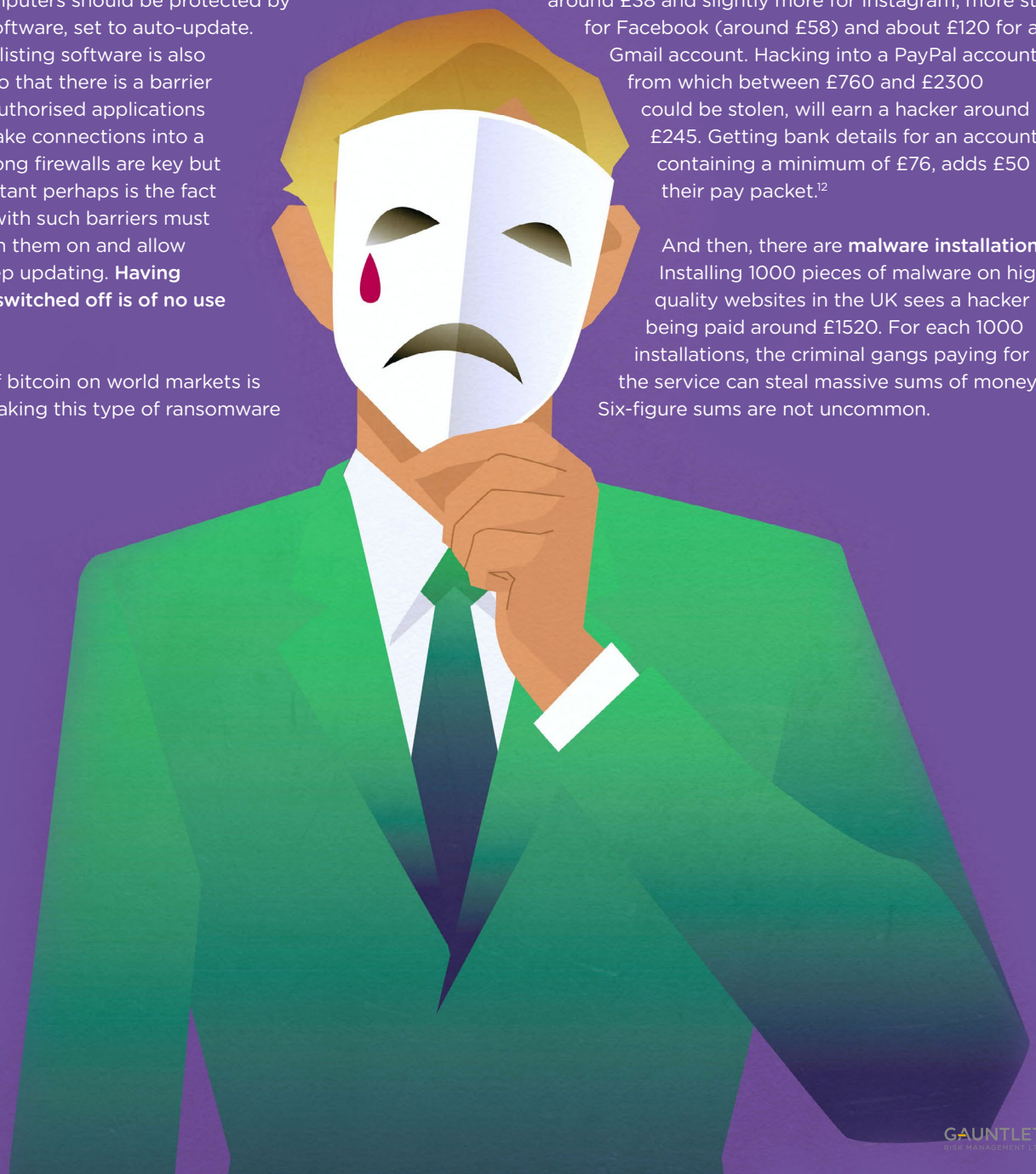
Best practice, to try to minimise damage and lower the chances of this happening, is to make sure staff do not install any software, unless they know and trust the source. Computers should be protected by anti-virus software, set to auto-update. Using whitelisting software is also advisable, so that there is a barrier against unauthorised applications trying to make connections into a system. Strong firewalls are key but more important perhaps is the fact that those with such barriers must actually turn them on and allow them to keep updating. **Having protection switched off is of no use to anyone.**

The price of bitcoin on world markets is currently making this type of ransomware attack less popular. The monetary returns from it are typically lowish per case anyway – between £550 and £1000 typically (to encourage the 'hostage' to pay) and there are other ways for Fiendish Mr Foxers to make money.

When people ask the question 'Why would they bother with me?' what they fail to see is that attacks are often not personal but driven by monetary greed and bankrolled by criminal gangs. What these guys want is data and the means to get data – often bank records – by guessing passwords or obtaining one password and hoping the user has operated that one password across all of their online activity – from Twitter to their banking sites. **They simply employ hackers and pay them the going rate – well-publicised on the dark web – for whatever it is they want to access or breach.**

The price paid for the hacking of a Twitter account is around £38 and slightly more for Instagram, more still for Facebook (around £58) and about £120 for a Gmail account. Hacking into a PayPal account, from which between £760 and £2300 could be stolen, will earn a hacker around £245. Getting bank details for an account containing a minimum of £76, adds £50 to their pay packet.[12]

And then, there are **malware installations**. Installing 1000 pieces of malware on high quality websites in the UK sees a hacker being paid around £1520. For each 1000 installations, the criminal gangs paying for the service can steal massive sums of money. Six-figure sums are not uncommon.



The Fiendish Mr Foxers will scour social media accounts and other information, to try to guess passwords that could have been used but also to build up a profile of targets, so that social engineering attacks can be more successful. Knowledge is power, so **the less you give away on social media, the better,** particularly if it links to your password.

These cunning hackers, once into your system, can spend months searching through files and building up a picture of how your organisation operates – often with a view to knowing who organises what, when it comes to bank transfers and payments, payroll, even the transfer of house purchase monies by solicitors. All they then need do, is to replicate that procedure, but divert money into a bank account that they operate – and then close very quickly - once the money is in.

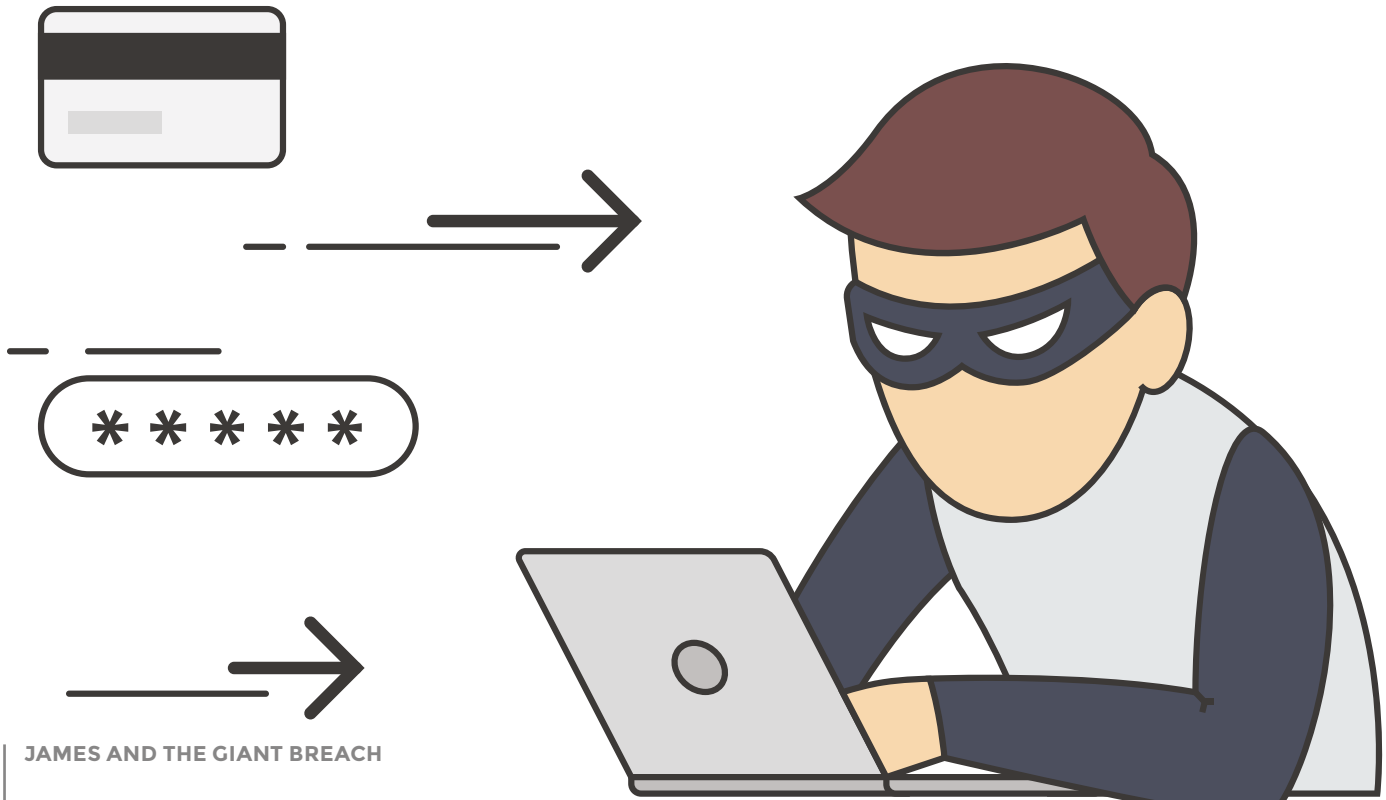
To reduce your exposure to these manipulators:

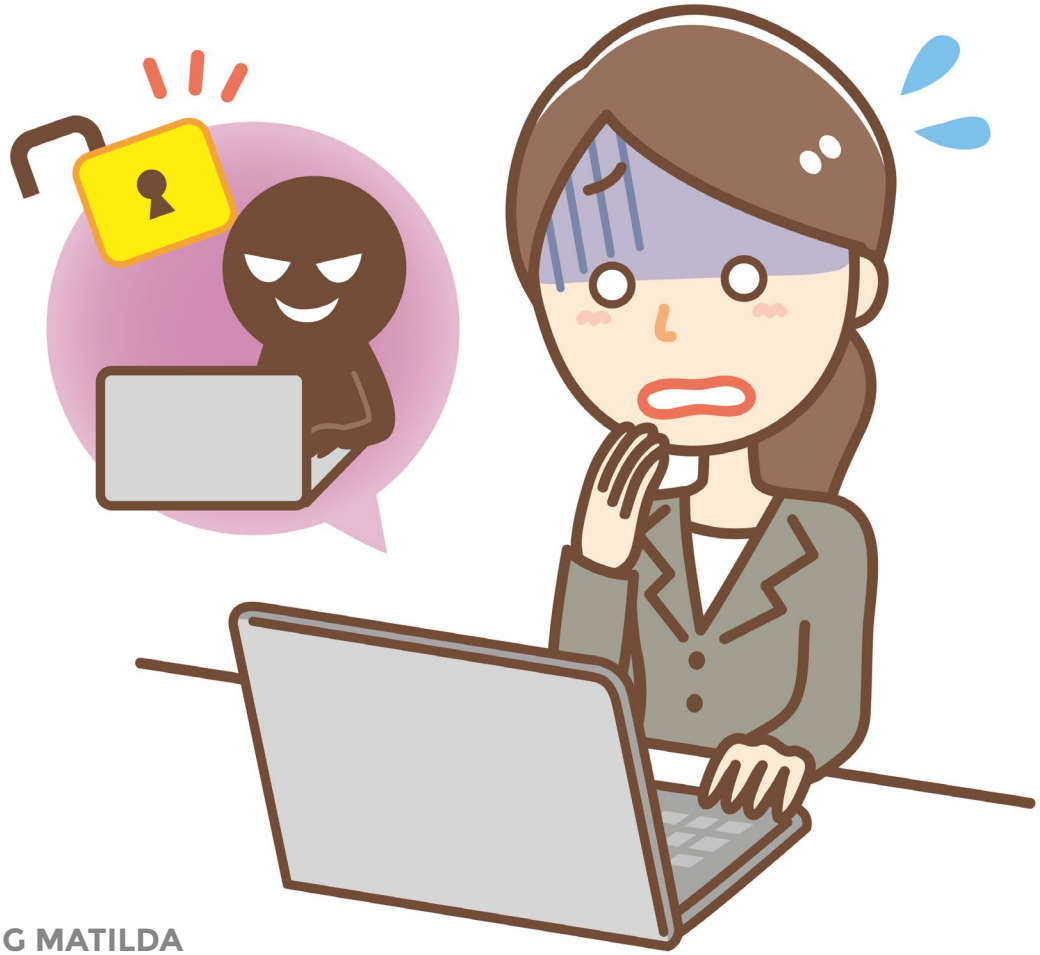
- Make it part of your HR policy to train staff not to click on links but take the direct route to a supplier or bank account, if they have any concerns about an issue.
- Tell staff to look out for any poor English, or wrongly spelt words, that could highlight that an email is not from the organisation is purports to be from.
- Highlight how examining the actual email address from which an email has been sent, may show that it is not from an address that you would expect to be attached to the company it purports to be from. Alarm bells should sound if the email address is one attached to an Eastern European country, in particular, but hackers can be from anywhere. If you don't recognise the email address, do NOT click on anything.
- Put a ban on downloading any software, without permission.
- Make regular checks, to ensure firewalls and virus software are turned on.
- Do not use easy-to-guess passwords.
- Do not use the same password, everywhere! Use a password manager, such as Lastpass or Keepass, which are free-to-use and which only require you to remember one master password.[13]
- Delete old website accounts that you no longer use, but which could contain your details.
- Never give out sensitive debit or credit card details or passwords to anyone who calls up. Again, if you feel it could be a supplier, hang up and call them direct. It's OK to say 'No'!

General research data suggests that only **31%** of UK companies carried out a cyber risk assessment in the past 12 months and only **22%** regularly offer cybersecurity awareness training when it comes to email alertness.[14]

Our own specially commissioned Gauntlet research found only **one-in-eight people** said they had been specifically trained in how to avoid doing something that could lead to a cyberattack issue. **Four-fifths (80%)** said their place of work has no specific cyber risk policy or procedures in place.

Alarmingly, **14%** said they, or a family member, was working from home, with access to work computer systems, but nobody had checked whether they have anti-virus software or other security measures in place, to protect their employer's data.





WALTZING MATILDA

Let's play a little word association ... and we love how Matilda helps us with this. If your name is Matilda and your password is waltzing, isn't that just a tad predictable? So predictable, in fact, that a hacker can guess it within seconds? And yet, this is the sort of thing that even top businesspeople do all the time; choosing their child's name, the dog's name, the name of their road or building and using it again and again, on every website they use.

Worse than this, many businesses share the password around the entire office, forgetting the degree to which internal crime is rife in UK workforces and how it only takes one disgruntled employee to want to pay an employer back by using their password to wreak havoc. **This common sharing of an unprotected password takes place in nearly one-in-ten workplaces, according to our survey.**

Zoom and Teams have boomed in popularity during lockdown but, worryingly, even at the start of it, when video conferencing had been in a more formal setting, **10%** of those who had used video conferencing **had either never used a password to enter the session, or used the same password each time**, according to responses to our Gauntlet research survey. What might it be now that they aren't within an office?

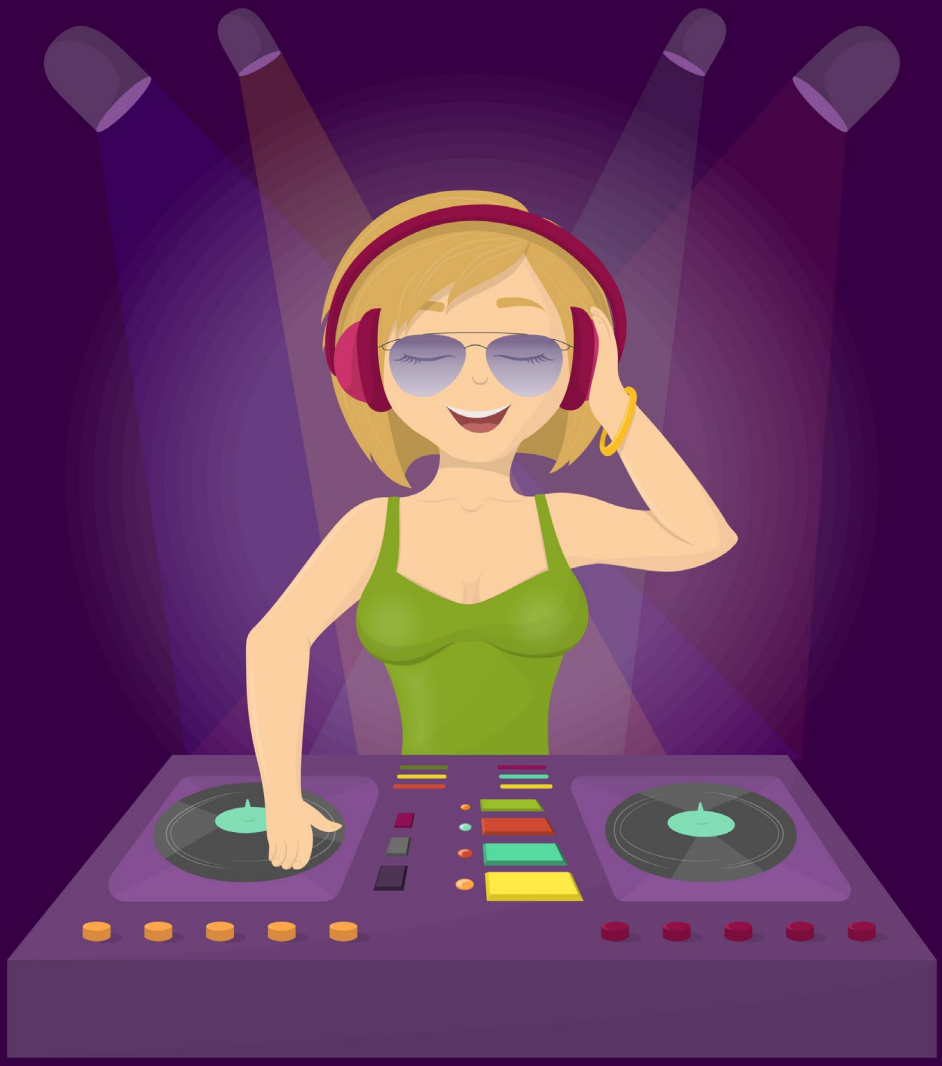
Some video-conferencing systems have been proven to have security weaknesses in the past[15] with Zoom being particularly exposed,[16] so why make it even easier for hackers to access your systems, by not using a password? Why make it easier by always choosing the password 'Matilda' or 'waltzing'!

Then, there are the issues associated with not having an appreciation of why passwords matter, when out and about and working in free public hotspots. In these situations, a hacker has some easy pickings, if they can situate themselves between you and the Wi-Fi connection point. Unless you are operating a secured device, the hacker can divert all of your emails, and possibly credit card details, security credentials and other data, to theirs.[17]

The best way to protect your systems, if you have to work on public Wi-Fi systems, is by using a **VPN – a virtual private connection**. Various systems are on offer, which you can install as software and then use when working in a public place. Turn off file sharing on your devices. If you are just working in a public place and don't need Wi-Fi or Bluetooth, turn them off.

Don't be tempted to go into your financial or healthcare accounts, whilst working in a public hotspot. Also, make very sure that the public hotspot you think you are in, is actually a legitimate one. Cybercriminals may set one up with a name that sounds or is spelt similarly, appearing in the same list of options as the authentic one, to try to catch you out. Double-check before you join a network and do not allow auto-connection via your Wi-Fi. If you must visit websites, make sure they are HTTPS secure ones and not just HTTP.

Cybercriminals can "snoop and sniff" in public hotspots, using special software that lets them eavesdrop on Wi-Fi and access all that you are doing whilst online, and on your device or computer. This includes viewing web pages you may have visited and on which you may have filled in your log-in details, which they can capture and use.[18]



THE SWITCHERS

One-in-twenty of the people Gauntlet surveyed felt that the cyber threat in the UK was lessening, because of greater awareness of criminal tactics. As we have seen, there is an alarming lack of awareness about many tactics and the threat is by no means going away.

What we are seeing, however, are new tactics being developed by cybercriminals all the time. One of these is lesser-known – that of **vishing**. Vishing is the new phishing – the same tactics but played out as a voice-based scam that involves trying to elicit important log-ins or financial details over the phone. The caller ID is often cleverly manipulated, to make it appear as if it could come from your trusted supplier or financial services provider.

In our Gauntlet survey, **86% of people did not know what vishing is**.

Much vishing is based around some sort of scare that you just have to deal with immediately, in just the same way as phishing. Often, there are phone buttons to press, in order to respond. Don't do that! If you know it's a scam call, just cut it off dead and block the number.
But there can also be **scams based around voice and our general recognition of the voices we often hear**. Mimicking a chief executive, having studied their voice in corporate videos, podcasts, YouTube, private social media channels, or even recorded phone conversations, can result in a call to a financial controller that leads to requests for bank transfers to be made. In many ways, this is harder for an employee to question than an email.

92% of the people that we surveyed believed it **would** be possible to mimic a boss's voice effectively enough to carry out such a cybercrime.

This process is already becoming more sophisticated, with the arrival of Artificial Intelligence. In August 2019, a UK CEO thought he was talking to the boss of his German parent company and transferred €220,000 into a fraudster's bank account, in one of the few cases in which AI has been used in hacking. The accent and even the melody of the boss's voice was apparently mimicked to a tee and recognised by the CEO, even though he was not actually talking to his German boss.[19]

It appears that commercial voice-generating software was used, although it is not known whether bots were utilised, to answer questions from the victim. **Software that mimics voices is available on the market and audio files can also be stitched together, to mimic a person's voice**, as demonstrated at a security conference last year. Applying machine-learning technology to spoof voices, makes cybercrime easier, according to experts. Some even predict that fake videos that show a CEO supposedly speaking the words in an audio file, could be the next cybercrime on the block.

The answer is to stay alert, put protocols in place where staff are told **never to respond** to such requests for money transfers, unless several authenticity checks have been made and recognise that, in a myriad of ways, your business could be the next target that makes the headlines.

SUMMING UP

Cybercrime takes place in an avaricious, fast-moving world where there is money to be made out of people's misery. In a Tenable Survey – The Rise of the Business-Aligned Security Executive Survey – which interviewed 851 business and security leaders, it was found that **44%** of businesses had lost employee data to hackers, **36%** had been victims of financial loss due to cyber theft and **34%** had lost customers because of a breach.[20]

The costs of restoration, lost income and business interruption can be extensive. A recent cyberattack at Redcar Council cost **£10.4m**.[21]

But it is the risk of losing customers that should strike fear into the heart of any business that knows how difficult it is to acquire them. An IBM and Ponemon study found that **44%** of UK consumers say they will stop spending with a business that has been subject to a security breach temporarily, whilst a further **41%** say they will never return to it.[22]

Cyber insurance is becoming what could be regarded as a necessity, not a nice-to. The Government's National Cyber Security Centre (ncsc.gov.uk) says:

"With more organisations moving operations online, it has never been more important to ensure your defences are as robust as possible.

"In a world where cyber threats are varied and constantly changing, cyber insurance can help your organisation to get back on its feet, should something cyber-related go wrong. Managing cyber incidents (such as ransomware, data breaches) may require in-depth technical knowledge. As well as minimising business interruption and providing financial protection during an incident, cyber insurance may help with any legal and regulatory actions after an incident."[23]

Here at Gauntlet, we couldn't have put it any better ourselves.

It is vital, however, that you buy the right cover and ask the right questions. Some policies will not cover you for ransomware attacks. Not all will provide IT, legal and PR support, to assist you, if your company is breached and needs expert help. The cover limits may not always be appropriate for your company and not all policies will cover actions brought against you, by third parties whose personal data has been compromised.

To find out what sort of cyber insurance cover you may require, **you can call us at Gauntlet on 0113 244 8686** and let us guide you not just through premiums, but the process and the practicalities of staying cyber-secure. **Together, we may not be able to defeat cybercrime but we can become the best equipped and protected we can be.**

Visit www.gauntletbusinessinsurance.com
or call 0113 244 8686

Endnotes

1 https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-july-2020-77-million-records-breached
2 https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2020
3 https://www.itgovernance.co.uk/blog/list-of-data-breaches-cyber-attacks-may-2020
4 https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
5 Research conducted by Gorkana Surveys, in late March 2020, surveying 1000 consumers, UK-wide. Results are licensed to Gauntlet Risk Management
6 https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
7 https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
8 https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html
9 https://www.decisionmarketing.co.uk/news/human-error-to-blame-for-88-of-data-breaches-in-uk
10 https://www.gdpr.associates/data-breach-penalties/
11 https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
12 https://www.privacyaffairs.com/dark-web-price-index-2020/
13 https://www.privacyaffairs.com/dark-web-price-index-2020/
14 https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
15 https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives
16 https://www.tomsguide.com/uk/news/zoom-security-privacy-woes
17 https://www.kaspersky.co.uk/resource-center/preemptive-safety/public-wifi-risks
18 https://uk.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html
19 https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
20 https://www.cbronline.com/news/uk-businesses-cyber-attacks
21 https://www.bbc.co.uk/news/uk-england-tees-53662187
22 https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html
23 https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

T: 0113 244 8686
info@gauntletgroup.com
www.gauntletgroup.com
Head Office: Gauntlet House . 15 Acorn Business Park . Killingbeck Drive . Leeds . LS14 6UF