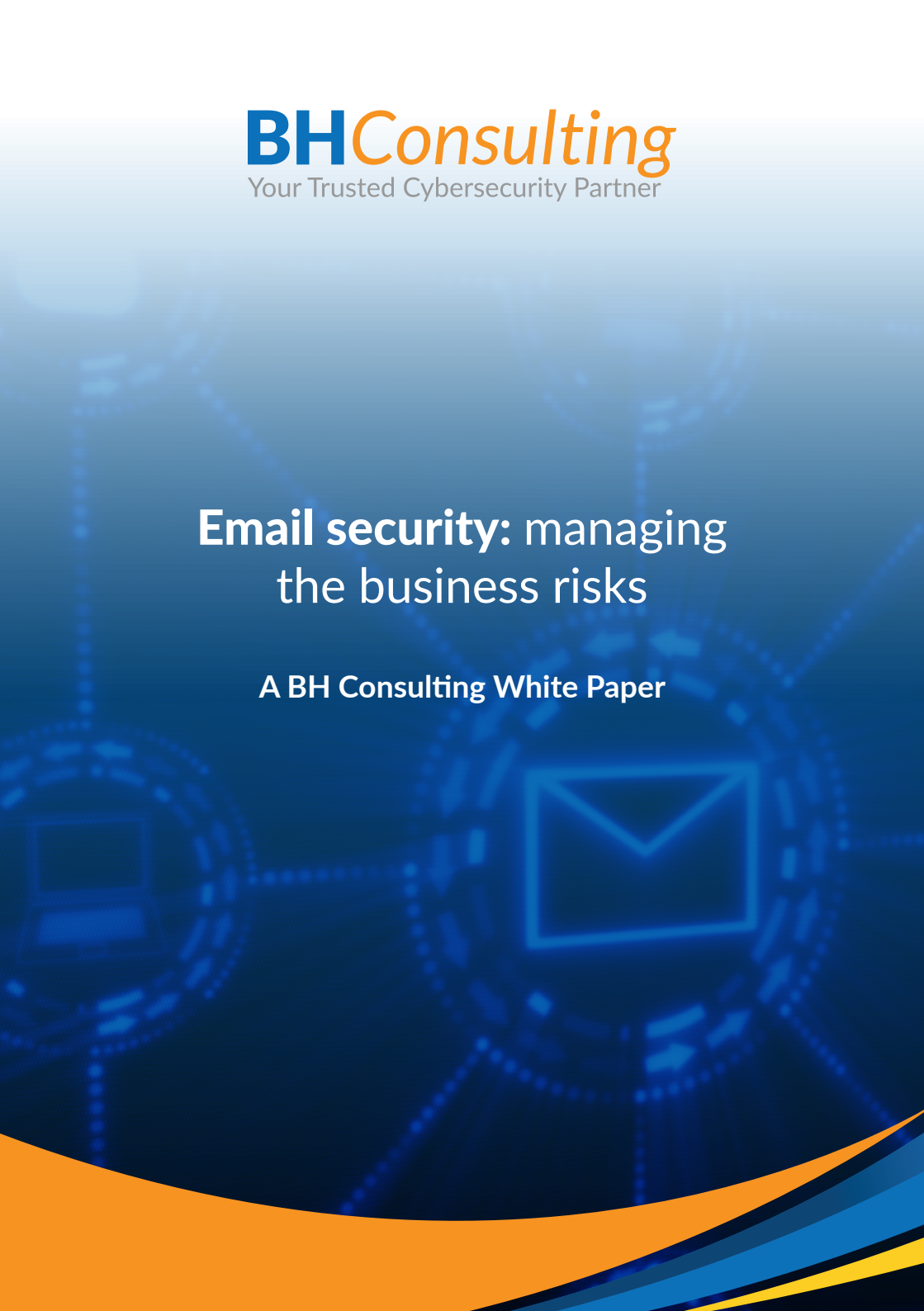
BH Consulting
Your Trusted Cybersecurity Partner

Email security: managing the business risks

A BH Consulting White Paper



Background to this guide

Email is arguably one of the most critical technology tools in any business or public sector agency today. It enables fast, effective communication with colleagues, customers, or business partners, whether they are in the same office, working remotely, or on the other side of the world. In 2019 alone, 293.6 billion emails were sent and received each day (source: Statista).

The breadth of information we routinely send and receive via email speaks to its importance. Valuable and sensitive documents like sales strategies, product details, contracts or invoices can be transferred quickly and easily. For an entire organisation, email is the communications channel that helps the flow of business and enables productivity.

For the individual, as lines blur between work and personal use with mobile 'always on' access, an email account not only helps them carry out their daily tasks, it is often the hub for their activities from utility bills to records of purchases. Email reaches into so many parts of our digital lives: if we forget the login to an online service we use, the password resets go to our email account.

What's more, when we receive an email, by and large we trust that it is coming from the sender whose name appears along with it. Yet it is relatively easy for an attacker to impersonate a trusted contact.

But are we taking this communication medium for granted? Do we really understand the risks as well as we understand the benefits?

It is those attributes described above that make email such a valuable target – and why it is so essential to protect it. There are many risks associated with email: just as it can distribute legitimate business communications, it can also send non-business related material such as malicious software, copyrighted material, spam, or content of an illegal, immoral or racist nature. It is also a very effective attack vector for criminals and fraudsters.

That is why it is essential to protect email: to avoid disrupting normal business operations and minimise any potential impact to your company's bottom line. This white paper is in two parts: the first gives an overview of the key risks to email and the second provides guidance on how to protect against them.

RISKS
Malware

Over the past number of years there has been a significant increase in the number of new types of malicious software, or malware for short. According to the 2020 Verizon Data Breach Investigations Report (DBIR), one of the most highly respected annual cybersecurity publications, links and attachments contained in email still account for the highest numbers of malware infections.

Over the past five years, ransomware in particular has developed into a serious threat for many businesses. Ransomware is an aggressive form of malicious software that criminals use to infect computers and encrypt the data on them. This blocks the victim from accessing their own data unless they pay a ransom. The WannaCry and NotPetya ransomware strains were among the most rampant over the past couple of years, claiming many victims and causing millions of euro worth of damage.

A social engineering email (see below) is an easy route into a target's IT systems. Once ransomware infects a victim's computer or server, it blocks access to their files unless they pay to have them released. Businesses and public sector agencies often fall victim to this type of attack, and the resulting disruption severely restricts their ability to keep working as normal. With IT systems offline, productivity suffers, which delays projects, and diverts management time to deal with frustrated customers and/or business partners.

Yet despite the attention these types of attack generate, some companies still seem to take a lax attitude to the threat. Some do not have anti-virus software installed on all of their systems; those that do, may not be updating the security tools regularly to guard against newly discovered threats. This can be worse than having anti-malware software installed because it leads to a false sense of security; the user believes they are protected when in fact they are not.

Social engineering, phishing and fraud

Email-related scams and social engineering attacks are a huge security risk. Social engineering scams are the most common way for online criminals to breach a target's defences. According to the Verizon DBIR 2020, 96 per cent of recorded incidents like phishing attempts arrive via email. Using this method, attackers try to steal victims' credentials, personal data, payment and banking details, or confidential business information.

Phishing aims to convince the recipient that the sender is genuine and then to trick them into doing something, which could be opening an infected attachment such as a spreadsheet or PDF file or clicking on a link that downloads cryptocurrency mining software that can slow down computers and waste precious internet bandwidth.

https://enterprise.verizon.com/resources/reports/dbir/
https://whatis.techtarget.com/glossaries
https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware
https://www.europol.europa.eu/wannacry-ransomware

Most malicious emails use simple spoofing techniques that could involve misspelling the company name in the email domain, or swapping characters or letters so they look very similar to the genuine email address. These tricks rely on people not paying close attention or being so busy that they do not immediately spot the difference. The fake just needs to be good enough to fool the naked eye long enough for the recipient to act on it. This can be especially hard on mobile devices where we tend to have smaller screens.

In other cases, there is a more direct financial motivation where criminals look to defraud businesses out of money. This type of risk goes by several names including “CEO fraud”, “fake boss scams”, “impersonation fraud” and “business email compromise”. These use social engineering to trick recipients into believing a trusted colleague needs urgent payment to an unfamiliar account. In 2018, the Pathé cinema chain lost more than €21 million to an email scam. The fallout led to the dismissal of the finance director and CEO of its Dutch division.

https://whatis.techtarget.com/glossaries

https://www.helpnetsecurity.com/2018/11/14/pathe-bec-scam/

Account takeover

The previous risk covered the scenario where an attacker pretends to be a known contact or a trusted colleague, but another risk is where the attacker takes over a victim’s actual email account? Think about the impact of that for a moment. An email can serve as a binding contract. Think of the damage to business relationships: how long would it take to send damaging emails to destroy your credibility, your career, or even your company? The attacker is no longer just impersonating you – as far as the email shows, they are you. And a victim might not even realise you have been compromised right away. An attacker who takes over an account could send stealthy emails to a manager, customer, competitor, wife, husband, partner or any other contact, and then delete all traces of it from the ‘sent items’ folder. Suppose they found an old message with company product plans or sales prospects; where might that end up?

An email account is the source of so much data about a person; it has the hallmarks of how we “speak” virtually to our extended contacts, from introductions (“Dear valued customer”), to signoffs (“Best wishes, Dave”). That is extremely valuable for any attacker who wants to impersonate someone. From a business point of view, an email account will have contact details for clients and colleagues ready to hand.

Historically, our mailboxes might contain valuable information - bank or other account details, client contacts, personal or financial information. Once an attacker has access to your mailbox, they may also have access to your other files too.

What about all those websites where you spend money? They are all password protected right? But if the attacker has access to your mailbox, they can just notify the organisation that you have forgotten your password – where will the password reset link be sent? That's right, directly to the mailbox that's already been compromised.

Remote working: the COVID effect

The growth of smartphones and tablets has blurred the lines between work and personal use with some company systems such as email, made accessible via small portable devices that we can access anywhere and at any time. In early 2020, this trend was exacerbated further as many organisations scrambled to enable remote working for employees during the lockdown to slow the spread of the Covid-19 corona virus. Email and other systems were very quickly opened up to enable staff to work from home and access company systems remotely, as offices were shut down to limit the spread of the virus. Where this may not have been possible, some individuals began using their personal email accounts for work, on their own personal devices.

The concept of 'access anywhere' has many advantages from a productivity standpoint, but there are serious security risks and concerns.

- Personal email accounts may not have managed backup, archiving, security or governance controls. Messages are not stored on company servers, which compromises the ability to carry out e-discovery or freedom of information requests. There is also the risk that personal email accounts could be accessible by unauthorised third parties.
- Personally owned devices may not have the same level of security controls as a laptop or desktop owned by the company and used exclusively for work. The organisation has no control or visibility of devices they do not own or manage, such as software to protect from malware, patching and updating of systems, and who else may have access to a personal device. Do you really want your confidential business plans stored on the same device used to access Facebook or TikTok, or to play Roblox?

Using handheld devices for business purposes also carries other risks; as noted earlier, the user may not be as vigilant when looking at a smaller screen and may be less likely to spot a suspicious message. It is also easier to accidentally send messages to the wrong recipient(s) which could inadvertently result in sharing confidential or personally identifiable information with the wrong person.

https://searchsecurity.techtarget.com/definition/electronic-discovery-e-discovery-or-ediscovery

https://www.citizensinformation.ie/en/government_in_ireland/national_government/standards_and_accountability/freedom_of_information.html

Leaking confidential information

Every company has confidential information stored on its computer systems in one form or another. This information ranges from HR and payroll records, customer lists, price lists, client correspondence and in-house intellectual property. The ever-present risk of releasing information to the wrong party can happen either deliberately by an employee who may be leaving or is involved in industrial espionage, or accidentally through someone sending a message to the wrong email address or recipient. No matter what way the information is released, the consequences can be serious.

The EU General Data Protection Regulation obliges companies to protect and keep safe any information that could personally identify an EU resident or citizen. Not only are there potentially heavy financial penalties for data breaches, there are additional sanctions including a ban on processing, and the reputational damage of such a breach may be significant.

Spam

Unsolicited commercial email, more commonly known as spam, can also hit your bottom line. Spam emails can clog up expensive internet and network connections with unnecessary traffic and expose recipients to unwanted and indeed unsavoury content. Spam emails may also contain malicious software or include links to fake sites designed to trick visitors into giving away personal information. There is also the productivity issue, because without a way to identify and stop spam from arriving into employees' inboxes, it becomes a drain on their time to sort through and delete unwanted email – along with the possibility of accidentally deleting a legitimate email while doing so.

Employees should also be advised not to forward spam emails, such as heart-rending chain letters, potentially virus-ridden attachments and using "reply all" to emails sent to a large distribution list, as this can cripple email networks and systems filling mailboxes with 'junk' email.

Exposure to litigation

The content of an email can often lead to embarrassing results for a company and, in extreme cases, may result in court action. Abusive, derogatory, or defamatory statements in an email can expose a company to loss of reputation, damaged customer relations or litigation. Take for example the case where an employee emails a fellow employee defaming a competitor. That email can be subsequently forwarded to another person(s) resulting in a "private" joke becoming public material and the defamed company taking action. There have also been documented cases of employees' use of derogatory statements within their emails leading to embarrassing public relations situations.

Distribution of racist, bullying, sexual or pornographic material via email can lead to claims against your company on the grounds of bullying or sexual harassment as people may find the content distasteful and feel that the distribution of this type of material leads to an unsafe or unhealthy working environment.

Distributing copyrighted material

Although file sharing services have reduced the reliance on email for distributing large files between people, some accounts still allow generous limits for their inboxes. Software can be exchanged from one user to another via email, as can music files, picture files and movie files – if not as attachments, then possibly as links to online storage services. There is a twofold risk to businesses: the first is malware infection, as such files or links may have come from illegitimate sources. Secondly, this material may be protected by copyright and often requires a licence before it can be lawfully used.

It is important to note that even though employees may be distributing these files without the knowledge or sanction of the company, it is the company and the directors of the company that will ultimately be held liable for any breach of copyright, and for failing to take steps to protect against it.

Lost productivity

Inappropriate use of company email accounts can hinder employee productivity both directly and indirectly. Staff members can be unproductive by spending excessive business time reading, forwarding and composing personal emails, jokes or viewing non-business related attachments.

Indirect impact on productivity can result in valuable computing and networking resources being chewed up while processing personal emails, especially those that contain large attachments such as movie, image or music files. This can result in slower response times from the email server and/or slow response from the internet as the download of these emails contends with legitimate network traffic.

Equally, it is unhealthy and arguably unproductive to expect staff to access their email any time of the day or night. With remote working now more prevalent than ever, good practice should aim to encourage a better work-life balance and minimise email communication, unless urgent, outside normal working hours.

Mitigating the risks

Technical controls

Configure your email systems to provide better protection:

- Use DMARC, DKIM SPF, TLS, malware and spam checks, quarantining and other techniques to detect and protect before the email reaches the user. These technical controls validate that an email comes from a legitimate source. DMARC is not a panacea against phishing attacks, but it helps reduce the risk. The Global Cyber Alliance has a free simple step-by-step guide on how to ensure your mail service has DMARC configured correctly.

- Check auto-forwarding rules so that you know when someone is passing all company email to another email address. There may be a valid reason for doing so, but it's worth checking in case it's not legitimate and authorised.

https://dmarc.globalcyberalliance.org/

- Consider using DLP (data loss prevention) technology that checks to ensure sensitive information doesn't pass from your organisation without the correct authorisation. If you switch on DLP, consider being open and transparent with users on what is being monitored, how and by whom, to remove suspicion of over-zealous monitoring and targeting.

- Turn on MFA (Multi-Factor Authentication) for all email access. Passwords can be easily compromised, so MFA immediately increases account security by requiring multiple forms of verification to prove someone's identity when they sign into an application. For example, in addition to typing in a username and password, they might also get a prompt sent to their phone or a dedicated security fob. This increases the chances that the user is genuine. Whilst using MFA isn't perfect and certainly not infallible, when you turn on MFA, your business accounts are 99.9% less likely to be compromised.

People controls

One of the greatest weapons to protect a company or public agency from the threats outlined above is user education. Everyone in the organisation needs to know about the risks involved when using email. Security awareness training helps employees to know about common email risks and identify them.

https://csrc.nist.gov/glossary/term/MFA
https://www.microsoft.com/en-ie/security/business/identity/mfa
https://www.virustotal.com/gui/home/url

Users should learn what is and what is not acceptable use of the company email system – how to keep work and personal life separate, and be educated as to how they should treat email, for example:

- Be suspicious when receiving an email from someone that you do not know. It could be a spam or worse, it may contain malware

- Do not open attachments if the email is from an unfamiliar sender or if it has no other content apart from an executable file (this is often a giveaway that the mail is not genuine).

- Don't click on links in emails unless you're confident they are genuine and safe.

- If you suspect an attachment or link may be malicious, you can check it by uploading it to a service such as VirusTotal which will run it through several virus scanning engines.

- Keep checking your junk email folder in case legitimate email is flagged incorrectly.

Cut out spam from your diet

To reduce the amount of spam you receive, educate users on the following:

- **Never** reply to a spam email, even to unsubscribe, as this simply confirms that the target email address is an active address and more spam will subsequently be sent

- **Never** open a spam email. These emails often have hidden scripts or programs in them that acknowledge back to the spammer that the address is real

- **Always** use a filtering solution to prevent spam from reaching your mail server (or check that your service provider offers this feature). This will reduce the amount of spam that the users get and also reduce the overhead on your network and email system

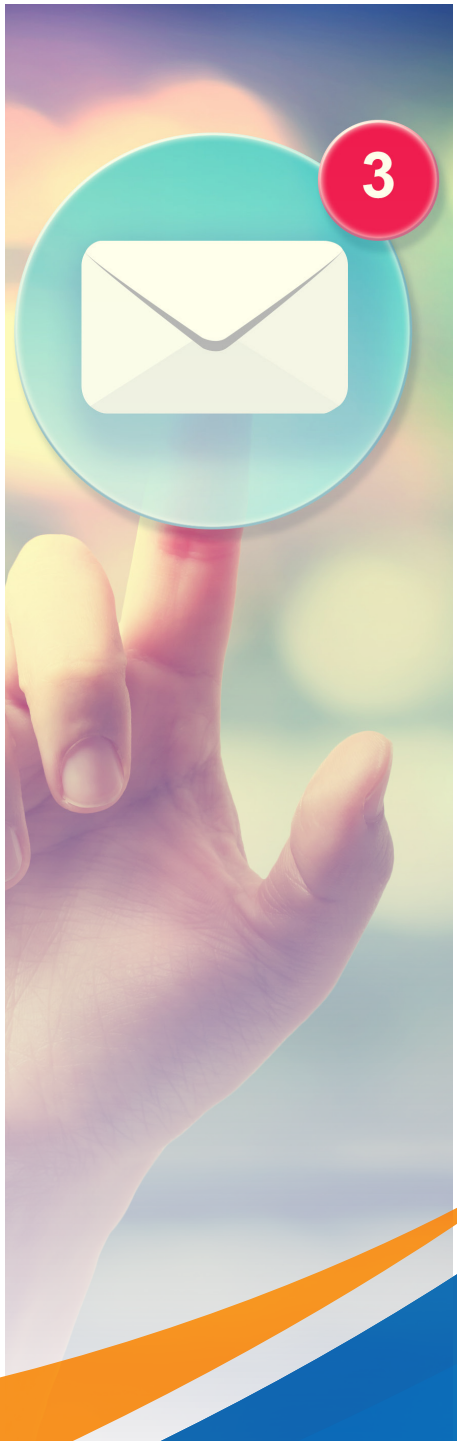
- **Never** "reply all" to emails sent to a large distribution list. Consider technical ways to restrict this within your email system.

Make haste slowly

The 'ping' that signals the arrival of a new email can sometimes create a false impression of urgency, but there is never any harm in asking people to take a moment and think twice before forwarding a message or opening an attachment. The best countermeasure against social engineering is time; taking a moment to stop and think – and to doubt. Is this message legitimate? Is it really from who it purports to be from? If you are unsure, ask someone you trust.

Suppose the email was requesting an urgent payment to a new bank account; doesn't it make sense to slow down and ask: is this genuine? Better still, before acting in haste, why not confirm – ideally by a separate communications channel – if the supposed sender really did contact you. Pick up the phone and call the sender (preferably using a number you already have or find independently, i.e. not using details in the suspicious email).

These procedures and practices, supported by acceptable usage policies (see below), could save the business from an embarrassing scam, financial or reputational damage.



If you receive a suspicious email on your mobile device, wait until you are at your desktop PC or laptop to take a better look before opening, as you may have a chance to investigate more thoroughly on a bigger screen.

Make it plain in a policy

A clearly defined Acceptable Usage Policy (AUP) explains very clearly to staff the do's and don'ts and what is expected of them. A well written AUP will protect the company in the event it has to take disciplinary action for any breach of conduct. Make sure that the policy is distributed to all employees and that it is enforced consistently. This is a threefold approach that involves:

- Being clear in the policy what the company expects by good and bad behaviour: do not have any ambiguity around the rules

- Telling all staff what is expected of them regarding their correct use of company email. Encourage staff to report any suspicious messages or an inadvertent mistake such as an email sent to the wrong recipient. Unfairly punishing accidental incidents will discourage people from reporting such breaches in the future - do not shoot the messenger.

- Implementing technical controls that improve security, protect your business and employees, and support the right behaviour.

Some security controls include:

Businesses that don't have in-house IT resources to set this up should ask their technology support provider to do this for them.

Cloud email does not necessarily mean secure email

Many companies now use cloud-based email services, but it is a mistake to assume that the email provider is automatically applying the best security settings for your organisation. It is the responsibility of your business, not the service provider, to tailor the level of security to your risk. Many companies, especially small businesses, use Microsoft Office 365 or Google suite for email. Often, their accounts have the same default settings they had when first set up.

Microsoft 365 and Gmail, two of the most popular email clients, have self-assessment tools that offer extra security features to add to email which check the current email settings and assign a rating based on the level of security. Applying stronger controls will improve the score.

Conclusion

Email is a powerful business tool. Used effectively, it can increase business and profits for a company while enabling its employees to be productive. Used ineffectively and not managed correctly, it could expose an organisation to financial, commercial and reputational damage. The technical and educational methods to implement good email security are within easy reach; there is no reason not to protect against the risks.

If you need help applying the technical or educational requirements of email to better protect your business, contact us on:

+353 (0)1 440 4065 | info@bhconsulting.ie | www.bhconsulting.ie

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie