KYND

A GUIDE TO: KYND ON 1.0

2. OVERVIEW

2.1 Individual Cyber Risks

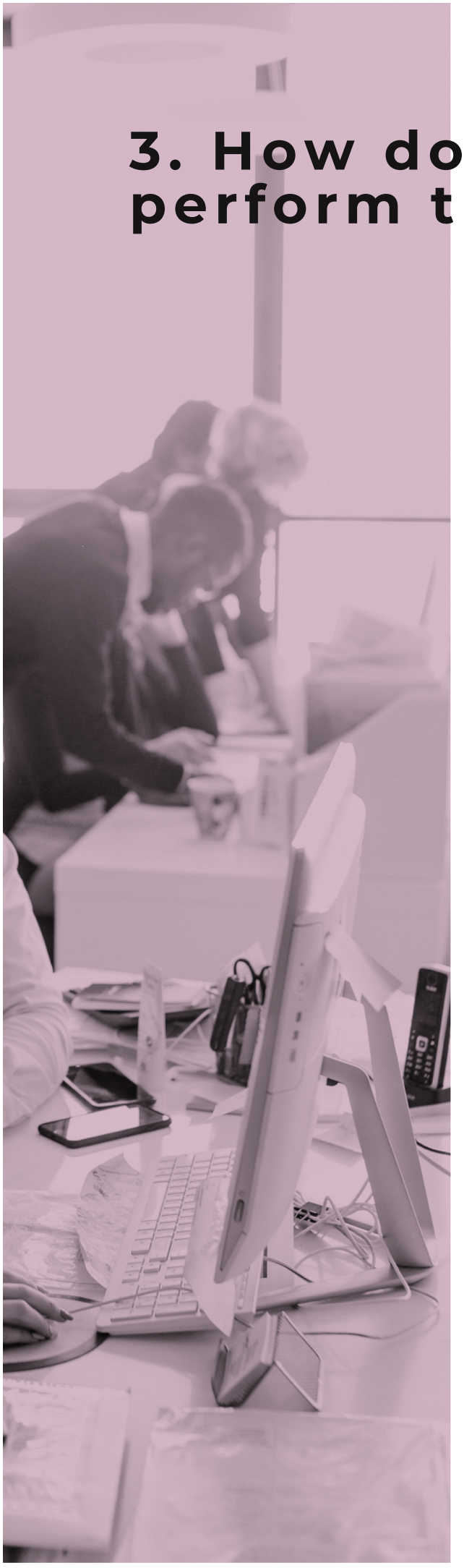
KYND On continuously monitors and analyses the identifiable cyber risks facing an organisation. Different elements of risk are monitored at various intervals over a repeating 30 day period and during this analysis, KYND assesses more than 250 cyber risk factors and ranks them either Red, Amber or Green.

- Red risks are those that KYND believe will affect the organisation if not addressed;
- Amber risks are those that KYND believe may affect the organisation if not addressed;
- Green factors appear to not carry an immediate risk based upon the information KYND has access to.

The KYND On summary screen includes a count of all the Red, Amber and Green risks found. The KYND On risk report also includes details of each of the Red and Amber risks identified and guidance on how the organisation can fix these.

2.2 Comparative Operational Cyber Risks

KYND On also includes a continuous comparative cyber risk analysis of the organisation versus its industry sector peers. This comparison measures the organisation in its performance of key operational processes that affect cyber risk, and shows how the organisation ranks against its peers for each of those processes.



KYND

3. How does KYND perform this analysis?

3.1 Domain Discovery.

KYND tries to find the names of all the Internet domains that we believe are connected to an organisation. An Internet Domain is the part of the Internet that an organisation or individual has registered for itself to use. An example would be mycompany.com or mycompany.co.uk.

Organisations or individuals never permanently own a particular domain name. They are registered for a period of time and the registration has to be renewed at regular intervals. The registration of a domain by an organisation or individual and all the details about that registration are managed by an authorised Domain Registrar such as GoDaddy or Names.

In simplified terms, KYND performs this Domain Discovery process by examining the registration details of the seed domain(s) provided for the organisation and then connecting other domains that have been registered using similar details, such as the registrant email address and the registrant organisation name.

3.2 Service Discovery.

For each of the domains discovered above, KYND then identifies all of the external Internet facing services that are being run by the organisation from these domains. Some examples of 'Services' would be a Database (e.g. *MySQL*) or a Web Server (e.g. *Apache*). For each of these services KYND collects all the external information available about and related to that service.

3.4 Synthetic Identities

KYND On allows users to create a number of unique, fake (synthetic) individual identities that do not exist anywhere else in the world. The maximum number that can be created is determined by which plan the KYND user is using. The user is able to insert these synthetic identities into databases being used within their organisation or inserted into data shared with data processors. KYND monitors the use of these synthetic identities to identify any potential data breach or security risks (see 'Data Breach Risks' below).

3.5 Individual Risks and Comparative Risk Analysis

Using all of the information collected in the previous steps, KYND then applies its proprietary cyber risk technology to create the individual Red, Amber, Green risks presented in the report. These risks are reported across different categories. KYND also compares the results for this specific organisation with a cohort of its peers to produce the comparative risk profile analysis shown in the report.

KYND

4. RISK CATEGORIES & COMPARATIVE RISK PROFILE

What do they mean for an organisation?

4.1 Email Security Risks.

Any organisation that has not put the standard email protections in place is immediately at high risk of having these addresses spoofed or impersonated to defraud its employees, customers, partners and suppliers. Email impersonation fraud (called variously Spoofing, Business Email Compromise or CEO fraud) is the most frequently reported cyber fraud loss however, standard protections are available which should be implemented by every organisation to reduce this threat.

KYND comment: *Missing or incomplete standard email protection within any organisation raises the question of whether it is being advised correctly by its own internal or external cyber security teams.*

The impact of these risks: *Financial loss, business and individual impersonation, fraudulent instructions to staff and 3rd parties, brand damage, reputational damage.*

4.2 Domain Registration Risks.

Any organisation relies upon the continued control of the domain names it uses to operate online. Losing control of one or more of these domain names would severely impact the ability of the business to trade. Having control means;

- The domain name continues to be registered to the organisation.
- The domain registration details are accurate, up to date and remain secure.
- Any changes or security issues regarding the domain are directed appropriately.

When a domain is registered using a personal or individual company email address this represents a significant risk to the control of the domain.

Firstly, If the individual were to leave or be absent from the business for any period then vital emails from the Domain Registrar will be missed or lost. This particularly affects registration renewals and account security. Ultimately the domain registration can expire, the control of the domain will be lost and the organisation's services will stop working on the affected domain. Over the last few years there have been numerous examples of such domain expiry and the chaos that results as the organisation tries to regain control of this important asset.

Secondly, the individual email address is more prone to social engineering attacks to try and obtain login and account details. If successful this could give attackers access to the organisation's account at the Domain Registrar, giving total control to a 3rd party. In the worst case scenario all or selected traffic to the organisation's websites could be redirected to fake or malicious locations designed to defraud customers, employees or suppliers, steal personal data and ruin the organisation's reputation and brand.

Finally, if an employee's personal email address or a third party's email address and details are used to register the organisation's domains, the organisation may have difficulties assuming ownership of those assets if that employee leaves or ownership is challenged.

KYND comment: *Internet domains are critical assets for any organisation that trades online. The ownership, management and protection of these is a priority but is often miss-understood and overlooked.*

The impact of these risks: *Severe business interruption, brand damage, reputational damage, 3rd party liability.*

4.3 Service Risks.

4.3.1 Known vulnerabilities

This risk relates to Services that have been identified which contain a known vulnerability to attack or compromise. Newly discovered software vulnerabilities are disclosed publicly to warn all users of the vulnerable products and versions and as part of the resolution process for software developers. Unfortunately, attackers also share tools and techniques that can be used to exploit these weaknesses as soon or even before they are publicly disclosed. Search engines are then used to easily identify and target services which are known to have a specific vulnerability. All of the above can happen within days or even hours of a new vulnerability being disclosed.

Running services which are known to be vulnerable carries a real risk of:

- Theft of data (hackers can easily exploit vulnerabilities to directly access sensitive data).
- Loss of control of website (website owner and visitors can be unaware that the site and traffic to the site has been compromised).
- Ransomware (a malicious program that removes access to electronic files, usually by encryption)
- Malware (software specifically designed to disrupt, damage or gain unauthorized access to a computer system).

The Equifax breach in 2017 which compromised the personal information of more than 148 million individuals and the Marriot Hotels breach in 2018 for which the UK ICO is proposing a £98 million fine are high profile examples of breaches caused by a failure to update vulnerable services.

- *KYND comment: Having vulnerable services accessible directly from the Internet raises the question of why the organisation has not hidden or updated these to mitigate the known risk that exists.*

- *The impact of these risks: Severe business interruption, the loss of personal data and possible regulatory fines, the loss of commercially sensitive information, 3rd party liability, reputational damage, loss of customer confidence, brand damage.*

4.3.2 Obsolete (out of date) services

This risk relates to Services that have been identified and are using software which is out of date and no longer supported or maintained by its developer. This means that bugs won't be fixed and vulnerabilities will not be patched and may not even be publicly disclosed until they have been exploited by attackers. Running any out of date software makes an organisation extremely vulnerable to attack (just like running vulnerable services) and service failure.

The origin of the global ransomware attack that affected many companies in June 2017 was a service at a small software provider that was using out of date software. The ransomware spread by exploiting vulnerabilities in other out of date software it identified. The NHS estimated they lost £92m and global shipping company Maersk lost $300m as a result of these attacks. In both examples the exploit used was patched by Microsoft earlier in the year - had these companies ensured they were keeping their services up to date these losses would have been avoided.

KYND comment: Once again having out of date services accessible directly from the Internet raises the question of why the organisation has not hidden or updated these to mitigate the known risk that exists.

The impact of these risks: Severe business interruption, the loss of personal data and possible regulatory fines, the loss of commercially sensitive information, 3rd party liability, reputational damage, loss of customer confidence, brand damage.

4.3.3 Misconfigured Services

Some services should never be directly accessible from the Internet. Examples of such services include;

- Databases which may contain personal or sensitive commercial data
- Developer or administration access points to computers
- Routers or network equipment

These types of services will immediately attract the attention of attackers and should be hidden behind firewalls, strong enforced logins or be only accessible via a VPN. There are regular incidents reported of organisations leaving databases containing sensitive data freely accessible directly from the Internet. Some of the most high profile include Accenture, Dow Jones and Attunity (which affected Ford amongst others). Not only can these errors lead to a loss of data and reputation; under the new, stricter data protection regulations now in place in many countries, the financial penalties that can arise as a result of these errors are significant.

***KYND comment**: Having misconfigured services directly visible from the Internet raises the question of why the organisation has allowed this to happen and whether appropriate administrative controls are in place to protect against this type of mistake.*

***The impact of these risks:** Severe business interruption, the loss of personal data and possible regulatory fines, the loss of commercially sensitive information, 3rd party liability, reputational damage, loss of customer confidence, brand damage.*

4.4 Certificate Risks

Security certificates are used to create secure connections to a Service via the Internet. A valid certificate is essential in order to protect the contents of the communication in this connection against being intercepted or changed. The most well known use of certificates is to create secure connections between a web browser and a website but they are also used to secure the connection between applications where no human being is involved.

These risks relate to services which are using security certificates that have either expired, been issued by an untrusted certificate authority, been revoked or been distrusted. This means customers or applications are not able to securely connect to websites using such a certificate. Visitors to a website with an expired, revoked, invalid or distrusted certificate will see a security warning in their browser and will not be able to visit the site. Applications which use a security certificate to create a secure communication channel to protect data in transit will no longer work if the certificate is expired, revoked, invalid or distrusted. Invalid certificates represent a significant risk to security, business continuity and reputation. The most recent, high profile failure caused by certificate expiry was the Telefonica UK (O2) network outage in December 2018 which affected more than 30 million UK 4G customers but less high profile service incidents occur almost daily.

***KYND comment**: Using invalid certificates within any service that is directly accessible or visible from the Internet raises the question of why these have not been re-issued or if the service is no longer needed then retired and removed.*

***The impact of these risks**: Severe business interruption, reputational damage, loss of customer confidence, brand damage.*

4.5 Phishing and Malware Risks

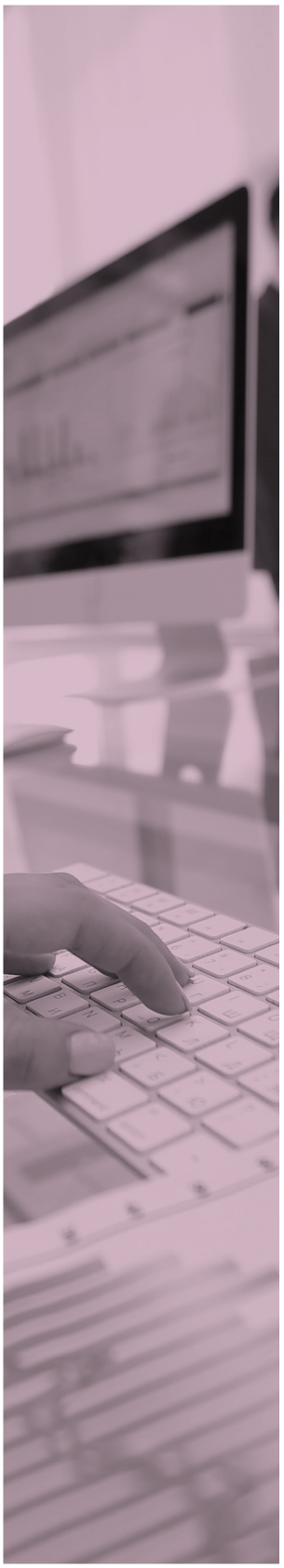
This means that KYND has found that one of the organisation's web pages is being used in a phishing attack and also possibly hosting malware;

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details for malicious reasons, Malware is malicious software designed to infect the computer of any visitor to that page, with the intention of gaining control of the computer, stealing data or even holding that data to ransom (also known as ransomware).

If a company's websites are being used to host phishing and/or malware attacks they will be immediately blocked by all the major browsers and their customers will not be able to reach them. Visitors to their site will also be exposed to the threats mentioned above. This represents a significant risk to business continuity and reputation.

KYND comment: *Having phishing or malware hosted within any organisation's own infrastructure raises serious concerns over the security of their platform and how the attackers were able to gain access.*

The impact of these risks: *3rd party liability, reputational damage.*



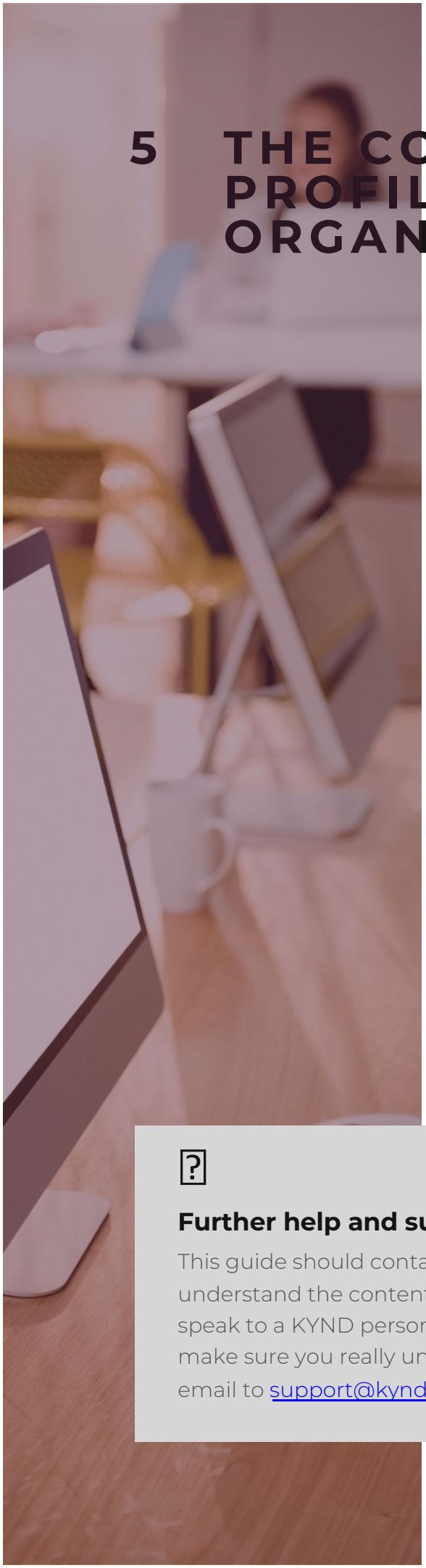
4.6 Data Breach Risks

KYND continuously monitors for the use of any of the synthetic identities created by the customer. The first indication of any risk will be that the fake email addresses are being sent email from outside of the user's organisation. This will indicate that the data could have been breached (stolen) or is being used inappropriately. Data Breach risk alerts relate to these incidents.

The longer it takes for a company to detect a breach, the more costly the impact of that breach is likely to be. Research by IBM states that, on average, a breach take 197 days to detect and that companies that are able to detect a breach in less than 30 days can save more than $1 million in resolution costs compared to those that take longer. With new legislation such as GDPR now in place, reacting swiftly to a breach is more important than ever.

KYND comment: *Data breach incidents often go undetected for extended periods of time and can grow in severity. Data breach risk alerts are designed to detect the first instance of personal data misuse so that the loss can be stopped, assessed and the correct incident response to be quickly put in place.*

The impact of these risks: *Severe business interruption, the loss of personal data and possible regulatory fines, the loss of commercially sensitive information, 3rd party liability, reputational damage, loss of customer confidence, brand damage.*



5 THE COMPARATIVE RISK PROFILE OF AN ORGANSISATION

The KYND ON report includes a comparative cyber risk analysis of an organisation versus its peers within its specific industry sector. The analysis covers four operational cyber risk processes.

- The use of out of date or vulnerable software
- The management of its Internet Domains
- The presence of mis-configured services
- The management of security certificates

In each area an organisation is ranked either inline, falling behind or weaker than its peers.

KYND comment: This comparative analysis aims to give insight into potential underlying issues that may exist at an organisation or guide further investigation of operational improvements that need to be made.

Further help and support

This guide should contain most of the information needed to help you understand the contents of the KYND ON report; but if you would like to speak to a KYND person about the specifics of a particular report or just to make sure you really understand what the report means, then send an email to support@kynd.io and we will be happy to help.