Cyber Security Questions You Should Ask Your IT Staff
The Intersys Fact Sheet

Has our business been breached?

- **Who has been accessing our data and from where?**
- **Do you monitor activity logs for suspicious activity?**
- **How far back do security logs go?**
- **What type of sensitive data is held in mailboxes?**
- **Has a data audit and/or DPIA been performed?**

Due to the nature of your business, carriers and brokers are a top target for cyber criminals.
The pandemic saw widespread use of agile working come into play- ensure your cybersecurity at home matches that of an office standard.
We've investigated heavily regulated companies in the past and have found hackers had access for months, intercepting business communication, emails, appointments- all with the intention of diverting funds/ accessing data.
Suspicious activity that should raise alerts within your IT department:
Impossible travel, login from USA then Australia a few minutes later.
Log in from unusual location.
Email forwarding.
Mass file deletion and download errors.

How is our sensitive data stored?

- **Is access to our passwords & sensitive access codes audited?**
- **Is our data encrpyted at rest?**
- **Who has an administrator account?**
- **What happens when a key staff member leaves the organisation?**
- **What remote access tools are used to access devices?**
- **Do you monitor our prescence on the dark web?**

These questions are not only applicable to your IT department, they should also be asked of **anyone that handles sensitive/personal data**.
IT department and MSPs- especially important to secure data, as a small team will need to share highly privileged accounts which can function as a key to your entire infrastructure.
Storing usernames and passwords on an excel spreadsheet/word doc may be easier but if someone outside your organisation manages to get their hands on this, you've given a hacker access to your entire organisation. – **A definite no**. There are various tools your business can use that securely store company/employee login credentials, such as ***LastPass***.
When signing up to sites or creating accounts (e.g., LinkedIn & Adobe), your login details may be available to purchase on the dark web. If so, you may be at risk of a breach.
Here at Intersys, we use a dark web scanner that enables us to find out whether our clients have been breached in this manner. We can find out exactly what information has been leaked onto the dark web. Feel free to contact us and we can run a dark web scan for your organisation free of charge.

How are our accounts protected?

- **Is multi-factor authentication widely implemented?**
- **Can systems only be accessed from trusted devices?**
- **Is access to accounts audited?**
- **What security is enforced?**
- **Who has administrative access to the IT Estate?**

The simple, most effective security measure you can implement is **multi-factor authentication**.
If passwords are leaked through a breach or someone within the organisation falls victim to a phishing email scam, without multifactor authentication your account is no longer safe.
Admin accounts have the power to change users' passwords, silently access their data & operate their mailbox. Please ensure that these **administrative rights are given to a select few and necessary individuals** within your organisation. We've seen poorly configured organisations whereby all users were admins- if one account is breached this could cause immeasurable damage.
Consider locking down your system to a specific location or prevent admin accounts from being accessed by unsanctioned devices.

Where is our data stored?

- **Where is our data resident?**
- **Is it stored in the UK post-Brexit?**
- **Where does data traverse?**
- **What could happen if data is stored outside of the region where the business operates & what compliance do the regulators expect?**

Different countries have different data security regulations. Ensuring your data stays securely stored in the country where the business operates is very important when handling sensitive client data.

Companies typically use multiple cloud service providers, and it is your responsibility to ensure your cloud hosting provider's data is hosted where you want it to be.

A company we've worked with was an early adopter of the Office 365 platform and found that their tenant was hosted in the US, which meant that any personally identifiable information on the system was in breach of GDPR.

How do you manage company data stored on devices?

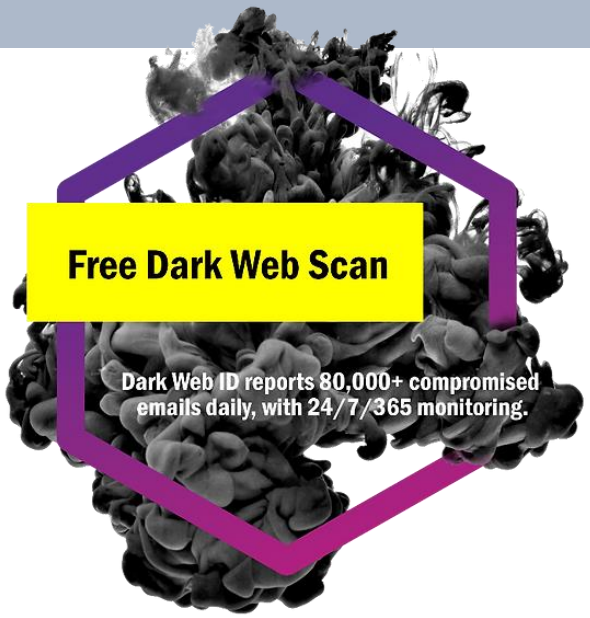
- **What happens if a member of staff loses a device with company data on it?**
- **Is data encrypted at rest?**
- **Do you know if there is company data on personal devices?**
- **What happens if the necessary management capabilities are not in place?**
- **What risk does this pose to the business?**

All company data should be encrypted so lost devices do not run the risk of causing a breach to your organisation. If an employee loses their device on a train and data isn't encrypted, a stranger can pick up your stolen laptop and plug it into their own computer like a USB drive. This would give them access to everything stored on there.
If an employee loses a company mobile device, we can issue a command to wipe all data from the phone.
However, if you use your personal device to access company data (SharePoint, OneDrive, Emails etc), this will be a little trickier. We can still wipe the phone to protect your organisation, but you will lose all your personal data.

When was the last time you performed a disaster recovery test/ restore?

- **How long would it take the business to recover from a ransomware outbreak?**
- **Are our backups monitored?**
- **Can data be restored from a backup successfully?**
- **Are offsite backups taken, where are they stored and are they encrypted?**
- **Do we have access to a disaster recovery environment?**
- **How does your disaster recovery tie into your business continuity plan?**

Test your backups in a real disaster scenario to discover what steps would be involved. Remember that downloading a backup from cloud storage can take days.
If communications are down, how are you going to inform your staff of the necessary steps to take? How will you manage client expectations?
In the event of a serious ransomware attack, often the only from of recovery is a full data restoration.



Here at Intersys, we use a dark web scanner that enables us to find out whether our clients have been breached. We can find out exactly what information has been leaked onto the dark web. Feel free to contact us and we can run a dark web scan for your organisation free of charge.

We look forward to seeing you at our next webinar.

For further information or enquiries into Intersys services, please contact us via email.

info@intersys.co.uk

www.intersys.co.uk