waystone | Compliance Solutions

Data and Cyber Security 2023

Introduction

Data? Information? What is it?

We all have personal data and if we work at a company will also have data relating to customers and/or suppliers/employees.

Information as such is very valuable, and everyone (yes you) needs to exercise extreme caution to protect it from those bad actors, so they do not gain unauthorised access and misuse occurs.

It is often said that criminals see individual employees as gateways to gain access to personal and organisational data. It could be a Monday morning or late on Friday, or any day, and an employee just does not notice or do what they should do, ask the correct questions to ID a customer or reply to an email, we all need to be alert and STOP, THINK, if in doubt DON'T and REPORT.

Information security primary function is protecting information from misuse, in general and secondary cyber security is protecting information from digital threats (e.g., through the world wide web).

The key is to have systems and controls! Having systems, software, processes, and procedures in place to protect information and the internal company systems from any unauthorised access/misuse is critical.

The information created and used for business purposes comes in many categories and therefore legal/ regulatory obligations, such as disclosure, requirements can differ.

The categories include:

- public Information
- internal private information
- internal confidential information
- external private information
- external confidential information.

Travel!

We all do it, either to get to work or for work, but do you do it with security in mind!

Some simple tips could protect you, contact your own IT or Compliance team for what they recommend, but some we would recommend are:

Don't:

1. use easy free Wi-Fi (or Bluetooth) points to undertake business activities, unless appropriate protection in place (e.g., VPN).
2. store business data on your personal device unless authorised to do so.
3. leave your business laptop unattended or at least locking the screen if you leave it with a trusted colleague.
4. create passports that use information that people can guess or is weak (e.g., wife name, surname, sports team, pets, password,12345678, etc.) or use the same password for multiple accounts, allow others to use them, write passwords down, or continue to use a default password on new equipment. Your company will have own criteria, we would suggest three random words (not linked to you or your company) as a core basis of the passwords but check your firm's policy so you comply.
5. select links that are embedded in emails! all emails and not just for phishing scams.
6. think the approach to information security is 'tick box' exercise! It's a culture, we all have a part to play, with policies and procedures to support.

Do:

1. be aware of common methods of accessing your data if use public USB charge ports (e.g., 'juice jacking') which exploits a mobile device's power supply as it passes over the same USB cable the connected device uses to sync data.
2. implement privacy screens.
3. switch off the very useful function 'save password' on all devices, although useful, if falls into the bad actor's dirty paws, they will be very happy.
4. keep all paper files with you always.
5. use nondescript travel bags.
6. be extremely careful when giving out any business information on the phone (or online meeting) in case anyone nearby can hear you.
7. when providing any information to others over the phone ensure they are who they say they are.
8. when sharing data over email (a) consider whether information needs to be sent electronically at all (b) check that the person you are sending information to is entitled to receive it (c) make sure that all information included in the message is relevant. Check your own firm's policy and shared in line with it.
9. consider best practice approaches to reduce information security risks, such as (a) a clear desk' policy, making sure that no items are left on desks whilst you are not there. (b) sending classified, sensitive, or confidential information using encryption (c) protecting the secure transfer of all electronic data through the use of passwords. (d) using secure file transfer protocol (SFTP) sites.
10. provide employee training on common threats such as Spamming and Phishing.
    - Spamming involves using of electronic messaging systems (e.g., email) to send unwanted mass messages indiscriminately. Common methods are for advertising purposes, although sinister spamming can involve spreading malware, or phishing.
    - Phishing gets users to download software capturing keystrokes, credit card numbers, passwords, etc. Phishing emails usually consist of two parts: an initial email, which contains a link – and a fake website, which looks like it belongs to a legitimate company. This is just to trick people into revealing personal information like passwords and bank details.

11. prior to closing any web browsers, log out of any accounts signed into. It is a common mistake, which can allow others to have access to your account, by looking at the last pages you were on (e.g., one of our staff recently stayed at hotel in Singapore and the previous guest Netflix account was still logged in on the smart TV, which is not a massive risk, but think it was something more confidential!).
12. understand, failing to protect personal information can result in a breach of Singapore data protection regulations, which have specific requirements that firms, and their staff must follow to keep personal data secure. Which if breached, can then lead to regulatory enforcement action by MAS who take the loss of customer data very seriously.

So, if you become aware of an information security issue, you should report it to the appropriate person in your firm immediately.

As part of operational resilience, in the event of an incident there are a number of parts to the reporting process for a firm to consider:

- containment and recovery
- assessment of ongoing risk
- notification of the breach
- evaluation and response
- communication.

Finally, this is not a “one off” activity, it is ongoing obligation and the risk of not taking seriously can be significant, we would urge you to review your existing framework, and ensure all in order or if you require enhancements.