CYBER RISK MITIGATION
EASY STEPS TO TAKE AT WORK

Email

Cybersecurity professionals often recommend implementing a strict no email forwarding policy as the threat of rogue employees stealing large amounts of confidential information is a major concern for many companies. If an employee wanted to pass on data from company systems, they could simply forward an email with that data to their personal account. This type of activity would easily go unnoticed by IT staff as it would be similar to normal behaviour. Once a policy is in place, other countermeasures are more easily possible, such as awareness campaigns to prevent accidental leakage and data loss prevention tools to look for large volumes of data exfiltration.

Security, not to mention privacy, concerns also exist around company data sitting on servers controlled by third parties, which makes it difficult to control security standards. For example, one controversy around Hillary Clinton's use of a private email server in the run-up to the 2016 US election hinged upon the perceived lack of security of the servers managed outside of the government.

Protecting Data on Mobile Devices

If employees are using mobile devices to access work emails, the most important course of action is to implement full device encryption of their devices. This protects the organization's data if the device is lost or stolen. For more information on this subject, please see the Device Encryption Guide on the CFC Risk Management Portal. In addition, companies should consider implementing a mobile device management solution to allow device wiping of all data if it is lost or stolen. A BYOD policy is also useful if employees are using their own devices to access work email, in particular around ensuring the employer has the rights to wipe the phone in the event it's lost or stolen.

Wire Fraud

When transferring funds into bank accounts that have not previously been used, verbal communication with the recipient – over a verified telephone number – should be used to approve the request. It's a simple way of verifying the recipient's identity and avoiding phishing scams, as scam emails will often include false contact numbers.

Passwords

To protect against simple types of password attacks, it is recommended to adopt a password policy which requires the use of symbols, uppercase letters, lowercase letters, and numbers. To create a complex password that is nonetheless memorable, one useful method is to base it on a personal passphrase (e.g. 'I really love my dog Buster'. Now turn that into a password, using a mixture of symbols, cases and digits. An example would be Ir<}md8USTER. As long as the user can remember the sentence, they *should* be able to remember the password too.

Often companies will require users to change their passwords on a monthly or bimonthly basis. The UK's National Cyber Security Centre (NCSC) recommends a different approach, as regular password changes '.. imposes burdens on the user (who is likely to choose new passwords that are only minor variations of the old) and carries no real benefits as stolen passwords are generally exploited immediately.' To combat the 'long-term illicit use of compromised passwords' the NCSC instead recommends to monitor logins 'to detect unusual use', and to notify users of attempted logins – both successful or unsuccessful – encouraging users to report any logins which they are not responsible for.

Defamation Issues and Social Media use

In many jurisdictions defamation laws are quite broad. It is advised speak to a lawyer or other trusted legal professional before posting content which has the potential to reflect negatively upon or lower the esteem of an individual, enterprise or other entity.

Data Storage

While consumer focused cloud storage platforms like Dropbox are attractive because they offer an easy and cheap way to back up data, security issues do exist with using these types of services. Dropbox is often blocked by system administrators because it is another path used by rogue employees to exfiltrate company data, or to deliver ransomware or other malware. Even as a backup solution, some types of ransomware can even affect data stored in Dropbox, making it inaccessible. The only type of backup that is safe from ransomware are external hard drives that are not continuously connected to a system.

Many alternatives exist to Dropbox that provide similar functionality, including secure private cloud based solutions or setting up your own server to back-up data. Regardless of the solution you choose, it is important to select only one and then design tools and processes around the chosen solution. The decision on provider should be made working in conjunction with IT in order to better understand the implications on the rest of the environment.

Copyright infringement

The easiest way to make sure you use loyalty-free images on your website is by purchasing them from providers such as iStock or Shutterstock. However, if you do source an image online, ensure that they are not copyright protected by conducting a 'reverse image search'. Google provides a simple how-to guide on this here. If you find the image, go to the website to see if there are any usage restrictions.

Alternatively, if you are searching for an image to use in a post, Google can search for images that are available for re-use by going to *search tools* and filtering by *usage rights*. If you are using an image for commercial purposes, be sure to search by *labelled for reuse*.