Courtesy of
Crendon Insurance Brokers Ltd

CYBERRISKS&LIABILITIES_

Protecting Your Email

Email has become a critical part of everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Set up a spam email filter.
It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email accounts for more than 60 per cent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid anti-virus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Additionally, ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

Protect sensitive information sent via email.
With its proliferation as a primary tool to communicate internally and externally, business email often includes sensitive information. Whether it is company information that could harm your business or personal information, it is important to ensure that such information is only sent and accessed by those who are entitled to see it.

Email in its native form is not designed to be secure, so incidents of misaddressing or other common accidental forwarding can lead to data leakage. If your business handles sensitive information, you should consider whether it should be sent via email, or at least consider using email encryption. Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorised personnel. Only individuals or organisations with access to the encryption key can read the information. Cloud services can offer secure Web-enabled drop boxes that allow secure data transfer for sensitive information, which is often a better approach to transmission between companies or customers.

Implement a sensible email retention policy.
It’s important to manage the email that resides on your company messaging systems and your users’ computers. You should document how you will handle email retention, and you should also implement basic controls to ensure information is retained for the necessary period. Some industries may have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts.

To ensure compliance, consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as 180-360 days in archives. In addition, discourage the use of personal folders on employee computers (most often configurable from the email system level), as this will make it more difficult to manage company standards.

Develop an email usage policy.
Policies are important for setting expectations for your employees or users, and for developing standards to ensure adherence to your published polices.

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data is allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business, you may have a need for email monitoring. The rights of the business and the user as they relate to monitoring should be documented in your email usage policy. The policy should be part of your general end user awareness training and reviewed for updates on a yearly basis.

Crendon Insurance Brokers

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact a legal or insurance professional for appropriate advice.

Train your employees in responsible email usage. The last line of defence for all of your cyber risk efforts lies with the employees who use email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work and when to seek professional assistance. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and offering refresher courses every year. You can provide monthly newsletters, urgent bulletins when new viruses are detected and even posters in common areas to remind your employees of key security and privacy to-do’s. Crendon Insurance Brokers Ltd has access to a variety of materials to help you communicate virtual safety information to your employees. Contact your representative for more information.