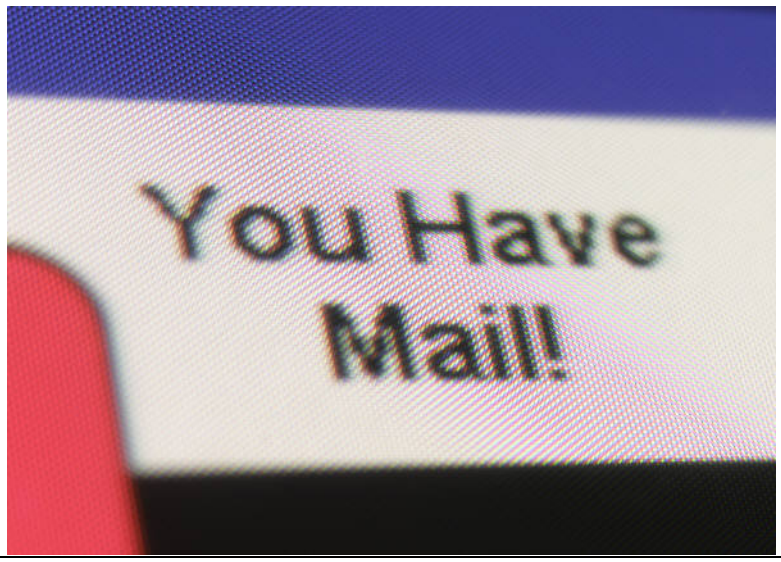
BH Consulting

Helping you piece IT together

Managing the Business Risks Relating to Email Security



Disclaimer:
BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. Business Risks relating to Email Security.

Email has become an indispensable business tool allowing us to communicate quickly and effectively with work colleagues, customers and business partners, be they in the same office or on the other side of the world. Documents and information can be transferred quickly and easily at the click of a button resulting in email becoming embedded in our daily business and personal lives. However, are we taking this communication medium for granted? Do we really understand the risks posed by this tool as well as we understand the benefits?

Just as legitimate business communications can be distributed using e-mail, so too can non-business related material such as computer viruses, copyrighted material, spam or content of an illegal, immoral or racist nature. All these items can expose your business to risks that need to be managed to minimise their impact on your company's bottom line.

1.1 The Risks Posed by Computer Viruses

Over the past number of years there has been a huge increase in the number of new and more sophisticated computer viruses circulating the Internet via email systems. The fastest ever virus, the Sobig virus, brought many email systems to a grinding halt as they tried to cope with the amount of email traffic generated by this virus as it spread. The resulting chaos meant many companies' email systems were offline until the infected systems had been restored to working order. Productivity was lost, projects were delayed, important deadlines missed and management time diverted to deal with frustrated customers and/or business partners.

Yet despite all the above and the resulting media hype generated, some companies still seem to take a lax attitude to this business threat. Many companies do not have anti-virus software installed on their systems and off those that do, many are out of date or do not update correctly. This in fact can be worse than having anti-virus software installed as it leads to a false sense of security as the companies feel they are protected when in fact they are not.

1.2 The Risks Posed By SPAM

Unsolicited Email, more commonly known as SPAM, can also hit your bottom line. SPAM emails are moving from a slight annoyance to a major threat as they clog up expensive Internet and network connections with unnecessary traffic and expose recipients to unwanted and indeed unsavoury content. Each SPAM message has to be processed by your network and your mail server. Recent surveys indicate that SPAM emails can account for up to 70% of emails. In effect this means that 70% of your email traffic is SPAM email. There is also the productivity issue as employees sort and deal with the deluge of unwanted email in their inboxes and the invariably lost legitimate email accidentally deleted when dealing with SPAM.

1.3 The Risks Posed by the leak of Confidential Information

Every company has confidential information stored on it's computer systems in one form or another. This information ranges from HR and payroll records, customer lists, price lists, client correspondence and in-house intellectual property. The risk is ever present of an employee releasing information to the wrong party. This can be a deliberate move on behalf of an employee involved in industrial espionage or quite simply typing in the wrong email address. Whatever way the information is released, the consequences can be quite serious.

1.4 The Risk posed by exposure to litigation

The content of an email can often lead to embarrassing results for a company and indeed in extreme cases could result with court action. Abusive, derogatory or defamatory statements in an email can expose a company to loss of reputation, damaged customer relations or litigation. Take for example the case where an employee emails a fellow employee defaming a competitor. That email can be subsequently forwarded to another person(s) resulting in a "private" joke becoming public material and the defamed company taking action.

There have also been documented cases of employees' use of derogatory statements within their emails leading to embarrassing public relation situations. The now infamous Claire Swire email, whereby an employee of a financial institution in London graphically boasted to his friends about his sexual exploits with his girlfriend, resulted in a large amount of negative publicity to both employees' companies.

The distribution of racist, bullying, sexual or pornographic material via email can lead to claims against your company for constructive dismissal on the grounds of bullying or sexual harassment as people may find the content distasteful and feel that the free distribution of this type of material leads to an unsafe working environment.

1.5 The Risk posed by the distribution of Copyright material

Emails have fast become the most popular way of distributing files from one person to another. Documents, spreadsheets and presentations can be quickly sent to those who require access to them. However other material can also be quickly sent around. Computer software can be exchanged from one user to another via email, as can music files, picture files and movie files. Aside from the risk of computer virus infection by distributing such software as it most likely will come from illegitimate sources, this material is protected by copyright and often requires a license before the software can be lawfully used.

It is important to note that even though the distribution of these files maybe by employees without the knowledge or sanction of the company, it is the company and the directors of the company that will ultimately be held liable for any breach of copyright.

1.6 The Risks posed by Loss of Productivity

Inappropriate use of company email systems can negatively impact productivity of employees both directly and indirectly. Staff members can directly be unproductive by reading, forwarding and composing personal emails, jokes or viewing non-business related attachments. Indirect impact on productivity can result in valuable computing and networking resources being chewed up while processing personal emails, especially those that contain large attachments such as movie, image or music files. This can result in slower response times from the email server and/or slow response from the Internet as the download of these emails contends with legitimate network traffic

2. How best to mitigate these risks

The greatest weapon to protect your company from the above threats is education and awareness of your email users. All users should be made aware of the risks involved when using the corporate email system. Users should be taught as to what is and what is not acceptable use of the email system and be educated as to how they should treat email, for example:

- Never open an email from someone that you do not know. It could be a SPAM email or worse it could contain a new computer virus.
- Do not open attachments that could contain computer viruses such as executable files. If in doubt about whether the email you received is genuine you should contact the sender of the email to verify the content.
- Major companies such as Microsoft never distribute software updates via email and only make them available for download from their website. Never use such an attachment purporting to be from Microsoft or some other major vendor.
- Do not use the preview feature available within your email client. This in effect opens the email and will run any automated scripts within that mail

A clearly defined Acceptable Usage Policy is a major first step in achieving this. As well as highlighting the issues to the users and inform them of what is and what is not acceptable, a good Acceptable Usage Policy will protect the company in the event it has to take disciplinary action for any breach of conduct. Make sure that the policy is distributed to all employees and that it is enforced predictably and consistently.

With the growing threat, numbers and sophistication of today's computer viruses it is essential that all incoming and outgoing email be scanned for computer viruses. Email is now the most common avenue for computer viruses to spread with over 85% of all computer infections originating from email borne computer viruses. Ensure that your system uses up to date virus scanners to prevent the latest computer viruses impacting your network. If possible you should also employ a method of preventing certain file types entering your network via email attachments. Computer viruses are spread by running programmes and macros, files with extensions of .EXE, .SCR, .VBS or .COM amongst others. By blocking emails with these types of attachments you can minimise the risk of a new computer virus infecting your network.

Peoples email addresses get on spammers' mailing lists by several routes. The most common is posting a reply to a newsgroup on an Internet website. Spammers have automated programs that crawl through newsgroups harvesting anything that looks like a valid email address. Another common route is by subscribing to mail lists or filling in forms on websites. Many spammers also have automated programs that guess the email address of the recipient. Finally there is a lucrative market where spammers exchange and sell their list of email addresses to each other.

To reduce the amount of SPAM you receive, educate users on the following:

- Never reply to a spam email, even to unsubscribe, as this simply confirms that the target email address is an active address and more spam will subsequently be sent.
- Never open a spam email. These emails often have hidden scripts or programs in them that acknowledge back to the spammer that the address is real.
- Use a filtering solution to prevent spam from reaching your mail server. This will reduce the amount of spam that the users get and also reduce the overhead on your network and email system

Education and policies will be effective to a certain extent, however you will need to deploy tools to help manage and mitigate the risks. There are many tools available that can be employed to ensure that the content of your incoming and outgoing emails do not expose you to any of the above risks. These tools can be deployed in-house or alternatively you could partner with a third party service provider who could provide this service remotely.

Email is a powerful business tool, used effectively it can greatly increase the bottom line for your company. Used ineffectively and not managed properly, exposes your company to financial, commercial and professional damage.

3. Contact Us

Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : **+353-(0)1- 4404065**
Website : **http://www.bhconsulting.ie**
Email : **info@bhconsulting.ie**