Cyber Security

Executive Briefing

Things you need to know to protect your organisation

This document has been prepared on behalf of WPLC Digital to raise awareness of a number of issues relating to Cyber Security.

It is aimed at Senior Executives, Directors and Managers of any business who have individual and/or collective responsibility for the security and integrity of data held within their respective Organisations.

It is hard to escape the news - on an almost daily basis - that significant Cyber Security Breaches are a regular occurrence, and the days of Cyber Security being just an ICT issue have gone.

We consider Cyber Security to be the **number ONE** risk for 95% of all organisations. Cyber Security needs to be understood at Board Level and, broadly speaking, it isn't.

Not knowing the real position in your organisation is a high risk strategy. Validation is key: if your organisation demonstrates it has taken the necessary steps to prevent a Cyber Security Breach, it will go a long way to protect you and your organisation's reputation.

Important elements to consider:-

- The most important point to consider as a Senior Executive in your organisation is that you don't need to understand technology, but you need to understand Cyber Security Risks. In particular, where is your data, how is your data stored and who has access to it and your IT systems?
- It is unfortunately inevitable that your organisation will have some sort of Cyber Security breach - they happen all the time - **YOU MUST** have **ROBUST** plans for when a Security Breach does happen. Your plans should include a Communications, a Business Continuity Plan, an Information Security Policy Document and an Acceptable User Policy Document. Make sure these are practiced and kept up to date and that senior member/s of staff are responsible for their sign off.
- Know what ICT Assets you have and **WHO** can connect to them. Technology professionals find this job boring and tedious and it is therefore often overlooked. Not knowing what or whom is connected to your network is a **HIGH RISK** strategy, Cyber Criminals often exploit this factor and it makes their access to your systems much easier. For example, did you know it is easy to turn a printer into a device through, which Cyber Criminals can gain access to your systems - it is very simple to do.

WPLC Digital LLP, Kemp House, City Road, London, EC1V 2NX
Enquiries@WPLCDigital.com – www.WPLCDigital.com
+44 (0) 203 394 0114

- Old legacy ICT systems make easy "pickings" for Cyber Criminals and Hackers. All the information required is readily available on the internet. It is therefore necessary to upgrade or replace these legacy systems or as minimum deploy specialist security software to ensure their continued integrity.

Always consider your Senior Technology management will not necessarily be aware of all Cyber Security threats. It's a fast changing landscape and ICT & IT Security staff are often stretched dealing with other projects. You may employ IT Security professionals, but bear in mind that no one likes to admit they may not know everything to their bosses and peers. If you are being told everything is "in hand" or it is "too expensive" to truly tackle the threat then there is probably an issue. Try and cultivate a culture of openness and a team from all aspects of the business when it comes to Cyber Security as the **WHOLE** organisation is in this together. We have seen this strategy work and it has saved organisations millions of pounds in technology costs and loss of business.

- Third party suppliers often have access to your ICT systems - are they, themselves, secure? We have seen the **MOST** secure organisations let Cyber Security Criminals into their systems using this method, who have had major teams of IT Security professionals working for them. Why? Because it was never checked and planned for.
- Have you recently made an announcement in the media which makes your organisation more likely to attract unwanted attention? If so, have you thought what additional measures you may need to take to protect your organisation?
- Do not get bogged down in what is seen as complex IT security technology. This should be the last part of the strategy, make your plan and planning robust first, and secondly implement the right IT Security systems based on a thorough understanding of your business and your planning.
- Your organisation is only as strong as your "weakest link". Many organisations spend significant sums on capital and operational expenditure trying to protect the "Front door" only to find they left the "Back door" wide open. For example, third party suppliers, ISP providers and contractors often have unsupervised access and if they do not themselves have robust Cyber Security measures in place, Cyber Criminals will access your organisation by piggy-backing off them. It is likely to be the first thing Cyber Criminals will look at, to determine how easily they can hack in.
- **ALWAYS** encrypt your sensitive and important data. Whilst not full proof from State Sponsored attacks, this strategy will protect most organisations and is cost effective and painless to do. We assume you know where and what data is important to you.
- How attractive is your organisation to Cyber Criminals? For example, if you turnover more than £5 Million; hold consumer data or are in the media, you are extremely attractive to Cyber Criminals.

WPLC Digital LLP, Kemp House, City Road, London, EC1V 2NX
Enquiries@WPLCDigital.com – www.WPLCDigital.com
+44 (0) 203 394 0114

- How do you protect your devices, especially Smart Phones? Smart Phones are seen as the next major trend in Cyber threats to organisations.
- Cyber Criminals often use Social Media engineering to obtain information to their advantage. We would always advise you not to put up your location on Social Media sites, such as Facebook, until after you return. Why? Because millions of pounds are taken from organisations every year by changing supplier bank account details of legitimate suppliers whilst the credit controller / CFO is away from the business. At least one of your competitors will have suffered such an attack. We have seen up to £10 million at a time taken using this method.

Next Steps

If you haven't taken the above steps then **NOW** is the time to do so – the future of your organisation, the reasonability to your customers and shareholders and your personal reputation are all potentially at risk.

Technology departments often work to serve the organisation, but often with a disconnect or lack of understanding on both sides. Cyber Criminals understand this, and often exploit this to their advantage. Make sure you have a panel, which meets every month to address Cyber Security Threats with representatives of all areas of the organisation.

In Summary

In considering the above points and implementing a robust Cyber Security Plan, you will make yourself a significantly **LESS** attractive target to Cyber Criminals. As an organisation you will be able to demonstrate to your customers and shareholders that you have reduced the risk of a Cyber security attack and that in the event of an attack are able to deal with it in an appropriate matter.

The good news is over 80% of Cyber Security threats can be combatted with common sense and a logical approach. Time and time again we see the simple cost effective measures have not been adequately implemented as they lack the "kudos" of implementing complex and expensive Cyber Security systems.

If there is one message you take away from this document it should be that adopting a simple, logical approach, which is understood by both the business and technology professionals, is the key to effective and successful ways of protecting your organisation from Cyber Security threats.

If you have any questions or would like confidential advice please contact Jonathan Palmer on +44 (0) 7836 542 197 or Jonathan.Palmer@WPLCDigital.com

WPLC Digital LLP, Kemp House, City Road, London, EC1V 2NX
Enquiries@WPLCDigital.com – www.WPLCDigital.com
+44 (0) 203 394 0114