Cyber Security, Data Protection and Remote-Working Concerns in a Covid-19 Business Context

16/04/2020

Around the world, employees across most sectors are staying home, using personal computers, home phones and having meetings over Zoom or Microsoft Teams. While these technological solutions have inspired widespread discussion about the 'new normal' of working from home, a trend many hope will remain after isolation measures are relaxed by governments, very little thought has been given to the significantly weaker digital security infrastructure most homes are currently enabled with. This briefing seeks to lay out these risks and provide a step-by-step guide as to how Boards and business leaders might mitigate them.

The challenge

Almost 90% of data breaches are caused by people: poor security, complacency or malicious intent and action. Conversely, developing a strong cyber security culture within your workforce significantly decreases the cyber risk, as this works to close down the easy routes available for e-criminals to access sensitive information. This sudden change to highly distributed working with decreased security oversight and support will have introduced even greater degrees of people-risk. It is imperative that everyone is encouraged to be alert, cautious and suspicious – and sadly, assumes they are being targeted constantly. Business leaders will be at particular risk.

The Covid-19 Context

Since the beginning of Covid-19 outbreak, there has been an over 600% increase in phishing attacks in the UK. Partly, this is because cyber criminals and malign actors were already operating with relative freedom and impunity, despite advances in cyber security and vulnerability awareness. The Covid-19 crisis created even more opportunities for criminals to exploit, in a context where global rates of successful malware and ransomware attacks were already growing rapidly with e-criminals and hackers industrialising the production of criminal software and sharing successful phishing and scam techniques.

Thus, it comes as no surprise that there has been a significant increase in phishing, ransomware and other cyber-attacks since the start of the Covid-19 crisis. Criminals are

seeing an opportunity in the mass move to remote working and taking full advantage. If your company pursued remote working to handle the current crisis, then you may have sowed the seeds of an even bigger company crisis in the months ahead. If your company Crisis Response Plan was found to be lacking, then almost certainly you will have taken additional unseen risks to continue functioning through the current period.

Boards urgently need to revisit their Risk Registers, health-check their recent decisions, communicate with and educate staff, and rethink their mitigation strategies for 2020 and beyond. It is not too late to take action.

Cyber-crime targets

The ruthless and relentless nature of cyber-crime has led to a significant widening of criminal targeting: big businesses remain the lucrative target of choice for organised crime, and sadly, they often represent the targets of least resistance because there are so many weaknesses to exploit. But now, government departments, hospitals, small and medium sized businesses, schools and the elderly are being targeted with a deluge of attacks and scams. Low-level on-line fraud targeted at small businesses and individuals is taking place around the world on an industrial scale with few, if any, national forces of law and order able to cope with the sophistication and sheer numbers of successful attacks.

Home-working weaknesses

Isolation measures changes working methodologies overnight: business operations moved from secure, centralised systems to comparatively insecure, highly distributed, socially distanced and often fragmented business ecosystem. This has heightened and exacerbated existing vulnerabilities and introduced new ones. The most obvious issues are related to: an overnight adoption of working-from-home; highly dispersed staff working off-LAN through home Wi-Fi and temporary internet-based systems; people being required to use unencrypted personal IT for business purposes; and the forcing of rapid changes to company IT network permissions and accesses. In addition, new risks involve sudden decreases in the physical manning of IT departments and help-desks, combined with the difficulty of maintaining alert company security and cyber governance regimes. Overall cyber-attacks have significantly increased, whilst cyber defences have significantly weakened.

Home IT infrastructure is generally poorly protected, for instance default passwords are typically left on routers and there are few security controls on the myriad of domestic and visitor devices which access the same infrastructure. These vulnerabilities are highly attractive to hackers, who only have to compromise a part of this infrastructure and then wait for the

home worker to remotely connect to their workplace, to be able to get into your networks. Use of a Virtual Private Network (VPN) does not, unfortunately, protect against this type of attack; indeed, it may lend a false sense of security. Fortunately, there are new and inexpensive ways of securing your network, such as employing a Software Defined Perimeter (SPD) service, which takes away all the responsibility for authenticating all remote connections and ensuring that they are healthy and safe before they connect into your business network and begin to access files and applications.

Data protection concerns

In addition to the practical and operational risks outlined above, there are knock-on effects if cyber-attacks are successful. More often than not, cyber security failings result in a data breach. For any company in the EEA (including the UK for the foreseeable future, as it has stated it will uphold the rules) GDPR regulations present a major financial threat to the company concerned. GDPR is also a global template even if the punishments are not as harsh elsewhere. In the UK it is necessary to make sure the Information Commissioner is informed about any breach within 72 hours and whether or not personal data has been compromised in a way that would mean customers must be informed. Companies need to have a plan for managing a significant data breach and its effects on customers' privacy.

Reputation management and communications requirements

In addition to the risks outlined above, there are far-reaching and complex reputational risks to businesses and other entities which do not have adequate cyber security measures in place. In March 2020, two British household brands made the news for all the wrong reasons: the Tesco Clubcard and the Boots Advantage Card were both hit by cyber-attacks, leading customers to wonder whether their data was secure. Regardless of the Covid-19 context and whether it was a factor in these attacks or not, both brands suffered a loss of customer trust and this can have a direct impact on subscription numbers as well as the more intangible notions of brand loyalty and brand confidence.

These are just two of many examples and in this context of heightened risk, all entities must be mindful of how cyber-security weaknesses could damage their image and have an impact on operations long after the security threat is addressed.

Communications strategies which cover internal, external and political / regulatory audiences are a key tool in managing any crisis emerging from cyber-security issues.

Internal communications

As has been outlined above, almost 90% of data breaches are caused by people. Strong internal communications are needed to foster a security culture across the workforce. This is a key defence and will significantly decrease the risk of attack. These strategies can be simple, in the form of emails and texts, but must be consistent and supplied regularly in order to make sure standards are maintained. Additional measures, such as training for employees and advice on cascading messaging from leadership, are also advisable in order to insure teams are prioritising security measures and recognising that business-as-usual when working from home is security focussed.

External communications

All entities affected by a cyber-attack are also at risk of unwanted media attention and uncomfortable questions about what was done to mitigate the risks. In addition to having a robust strategy in place, it is highly advisable to develop a reputation crisis management protocol so that you can respond quickly and appropriately and protect your brand. Such strategies are highly tailored and many large entities run regular crisis communications simulations in order to test how protocols work under pressure and refine it in the process. How well you prepare in advance of a crisis often dictates how successful you are in managing it. Thus, we strongly advise crisis planning and capability development though training, so that your management team are ready for all eventualities.

Political, regulatory and government communications

The UK Government does not follow closely cyber security issues and is inclined to have knee jerk reactions against companies who have cyber security failings. Such failings are often perceived by media and public alike as a failure of Government regulation. The Government of course will attempt to deflect it back on the company potentially damaging its reputation.

This is because the lack of real understanding of the issue, especially at senior levels of Government, means that such events are treated as a matter of media handling to prevent reputational damage to the Government rather than engaging in helping the company concerned to resolve the issue through Government support or regulatory change.

Reputational risks, then, have the potential to become operational risks and must be expressly accounted for in any cyber security strategy.

Immediate Actions

Remote working is likely to be with us for some time, and could become the norm for many people. Thus, the cyber security perimeter of a company must be extended to include employees' home IT infrastructure.

Actions to take should include:

- Have Remote Workers change and strengthen their home Wi-Fi credentials immediately
  - Ensure passwords on Internet-of-Things (IOT) devices of remote workers are sufficiently strong and not duplicated across devices (8-12 characters, numbers, letters, capitals and lower case plus special characters).
- Ensure employees working from home on personal devices keep their home software updated.
- Health check mobile phones: update software, delete old Apps, tighten privacy access on the Apps you keep, use automatic screen lock, disable public Wi-Fi access.
- Only download software from trusted sources.
- Use end-to-end encryption for email and other correspondence.
- Report suspicious activity when you see it.
- Phishing – in particular watch for mail from fake medical or health organisations.
- Ransomware attacks – have mitigation plans in place and know what to do.
- Identity theft – your passwords may be at risk so change them and make them more secure.
- E-crime epidemics – malware is on the increase, be highly suspicious unsolicited emails with any form of link or attachment. If in doubt, delete.
- People are the weakest link in remote working – maintain constant communication to keep people alert and to update procedures and patches.
- Alert your families to increased low-level on-line fraud, especially elderly parents who come from a more trusting generation. Scams are ever more clever and more convincing, and the isolated elderly in particular are at high risk.

Immediate questions for business leaders to ask

Your Board and your Executive Leadership need to seek answers to the following questions:

- Does your current Board Risk Register reflect the changing risk environment?
- Are your current set of mitigations sufficient for handling the increasing threats?
- Do you have the requisite skills and knowledge on the Board to handle the changing threat landscape?
- Was your Crisis Response Plan adequate when Covid-19 hit?
- Do you have appropriate external and internal communications strategies in place to support operations during these exceptional times?
- Have you done enough to educate and support staff working from home, noting that in cyber security your people working remotely will be your weakest link?
- Have you increased and adapted your internal communications output in order to build a culture of security into your approach to working from home?
- Have special measures been incorporated into your crisis communications plan, enabling you to be ready to respond to the associated threats to your brand reputation that may arise from security weaknesses? For instance, is your CEO media trained?
- What are the Covid-19 implications for your digital and other transformation programmes?
- What are the short and long-term implications for staff welfare and retention?
- What is your supply chain doing to ensure cyber security standards are maintained? Many of the most damaging breaches have come from cyber security weaknesses in supply chains.
- Can you survive and then thrive in the current global economic turmoil; how do you mitigate your current business risks and how do you posture for post-Covid-19 success?

Your company leadership needs to consider taking the following actions:

- Health check your change management, oversight and governance.
- Ensure heightened alert and threat awareness for all – people need to be much more alert and cautious when working from home.
- Communicate security messages frequently. Make sure everyone is familiar with new security systems and precautions, especially if working on new IT, VPN and communications arrangements.
- Check the state of your IT services and call centres/desks.
- Patching – now is not the time to get lax with software patches. VPNs need care and attention to ensure they stay secure. Consider a Virtual Software Perimeter for enhanced security.

- Know where your high-value company data resides and control who has access – seek to reduce access not increase it.
- Implement Multi Factor Authentication (MFA).
- Ensure Board members visibly demonstrate good security behaviours.
- Review and update your Board Risk Register.
- Review your security services and, where necessary, add cyber-security tools and applications purpose built for distributed working. Take advice when doing this; poor choices can result in large additional costs with minimal increases in security. At the very least, use basic VPNs and other tools to support remote workers.

Finally, at the end of March the UK National Cyber Security Centre published guidance for employers on homeworking - see https://www.ncsc.gov.uk/guidance/home-working - this provides a very useful and common-sense reference.

Conclusion

The cyber-crime industry is taking every opportunity that the Covid-19 crisis presents. We all need to be aware of the threats and to understand the huge increases in vulnerability that comes with a sudden move to sustained remote working. Whether you are a global corporation, an SME or a start-up company, instilling a culture of heightened alert, getting the cyber security basics right, and making quick but well thought-through adjustments in your security posture will prevent cyber criminals from destroying your business.