COVID-19: DATA PROTECTION & CYBER SECURITY

INTRODUCTION

We face significant challenges with the current global pandemic and the spread of COVID-19. Whilst inevitably there is a focus on our physical and environmental safety at home and at work we must also maintain our individual cyber security health and wellbeing, including the protection of personal data and maintaining cyber security standards.

DATA PROTECTION CONSIDERATIONS

Obligations and responsibilities to safeguard personal data are as important now as ever. There is potential for requests for personal information at short notice, and many organisations are rethinking how they work with a large increase in people working from home.

We must strive to safeguard personal information at all times and, as with the pandemic itself, our response must be considered, proportionate and effective.

As resources become stretched individuals may find themselves in unusual situations to provide 'business cover' for absent colleagues.

At times of additional stress, it is important to remain vigilant about the authenticity of requests for personal information (see Phishing & Ransomware Attacks below) and take appropriate steps to validate the requestor.

Although there is a focus on personal safety and wellbeing, standards and their associated timescales with data protection are not being relaxed (at least not yet); organisations are advised to provide timely notification if they experience delays or difficulties when responding to individuals exercising their rights.

Adopt a common sense approach to the sharing of personal data regarding the health of staff who may be infected by COVID-19. Avoid directly naming individuals and only provide relevant information to those who have business justification and need.

It is permissible within data protection legislation to ask staff if they have underlying medical conditions which expose them to greater risk; information they may not have previously declared. Do not collect any more than is necessary whilst ensuring appropriate controls and safeguards are applied.

REMOTE / HOME WORKING

As governments and organisations rush out plans to respond to the pandemic there has been an exponential increase to facilitate home working. Where previously a few people had this ability and frequently on a part-time basis, there are now potentially many thousands who are going to be trying to work from home.

Initial challenges faced by organisations:

- The number of technical devices, software, licensing available to hand out to a wider workforce;
- The availability of VP tokens (software or hardware) to enable people to connect securely;
- Sufficient network bandwidth and connectivity to cope with the increase in demand.

The last point is outside your organisational control, but will there be sufficient core bandwidth? Remembering that schools, colleges and universities are also vying for their slice. Do not forget those who are not working but downloading various box sets to binge watch, and then there are the gamers with Fortitude, Call of Duty, etc. We may find that, due to demand, the internet runs much slower than we anticipate. Remember those buffer overflows and watching pages load – it may be coming back with a vengeance!

When laptops for remote working are provided,

- Provide a clear warning that these devices are for business purposes only;
- Corporate policies will apply (organisations may need to review and revise them).
- Prohibit the devices being used by family members, installing applications or any other software without proper authorisation and change control (record and manage any exceptions).
- Ensure the availability and methods of providing technical support to a larger group of remote workers; particularly in the early stages when there will likely be many teething problems.
- If time and equipment exists conduct some remote work tests with groups where they all try and work from home for a day. Note successes and create actions plans to address any issues arising.

PHISHING & RANSOMWARE ATTACKS

- Cyber criminals are sending more and more phishing emails to lure people into giving away personal and sensitive information.
- These attacks are becoming very sophisticated and often difficult to identify, particularly when people are under pressure.
- Websites and information particularly at high-risk are: Those giving medical information, updates on the virus spread, actions individuals should take, those selling masks, sanitisers and similar products.
- In recent months there have been a number of high profile ransomware attacks which have targeted the user end points (i.e. laptops and workstations). The ability to recover and restore when individuals are isolated these will be severely impacted.
- Ensure that remote users' data is backed up and tested as part of resilience planning.

- The underlying advice is as always - be suspicious of unexpected or unusual correspondence; take greater care on the links you click, the websites that you visit and the information you provide.

THE HUMAN FACTOR

COVID-19 has introduced scenarios that virtually no organisation has prepared for. The global scale and impact is now starting to really take effect, and we are still at the start of this pandemic.

Over time there will be considerable pressures upon individuals. Some people will be working extended hours every day, but for how long and at what cost in the longer term?

Do not neglect the additional stress and strains the IT team may be under as they look to safeguard themselves and their families whilst responding to a dispersed workforce who will be demanding more support from them. People will need some downtime. Remember that the longer this goes on, the longer it is likely people will have been without leave and a break – at some point in time they will need to stop.

During 'lockdown' periods there could be considerable pressures on individuals at home, particularly if there are already stresses and challenges that can be avoided by going to work. Some individuals will find it very difficult to work from home, due to young children and pets causing distraction.

Do not forget the potential that your staff will want to take leave when this situation subsides, to go on a holiday to relax, just at a time when management is trying to recover the business, to develop new products and services, to catch up with a myriad of things that have been put on hold – and suddenly the people you need to help achieve this are wanting a holiday!

SUMMARY

As businesses strive to plan their corporate survival, whilst trying to ensure their workforce is kept safe and informed, also give serious consideration to the organisations cyber security defenses and well-being.

These are unprecedented times for all of us. We are all impacted, and are likely to be for many months. Consider flexible working and work breaks for people. Start planning for the longer term.

This paper only touches on some key points for consideration if further assistance or advice is needed please contact IRM.

THE AUTHOR:

Paul Sexby – Head of Strategic Practice

Paul has also written: "Practical Pandemic Planning (P3)" providing organisation some practical advice and guidance consider in their preparations. This can be found via the following link:

https://www.irmsecurity.com/resources/practical-pandemic-planning-p3-coronavirus-COVID-19/