IRM INFORMATION RISK MANAGEMENT
.ALTRAN GROUP

CHECKLIST

COVID-19 - BUSINESS CONTINUITY CHECKLIST

ALTRAN

SECURE CYBER **UNLOCK OPPORTUNITY**

IRM**SECURITY**.COM

COVID-19: RAPID RESPONSE
BUSINESS CONTINUITY CHECKLIST

MANAGEMENT

1 Have you established a pandemic planning team?
- Consider a representative from each function
- Set up regular conference calls or Skype sessions to stay up-to-date
- Are you keeping executives/board members up-to-date?

2 Communication lines
- Who is responsible for keeping the organisation up-to-date as the situation and government advice progresses?
- Are you using only official trusted sources of information?
- Consider setting up helplines including IT (phishing attempts, equipment requests), HR (sick pay, sickness outbreaks) and ensure line management can be contacted
- External communications lines need to be set up to inform clients/customers of any changes to meetings, location of work and suppliers and business partners should also be kept up-to-date.

3 Financial
- What projects can be 'parked' to minimise risk?
- Consider revenue losses, emergency cash, cash flow, supplier payments and salaries
- Payments to suppliers and payments from customers are likely to be later than usual – consider changing payment policies to help businesses until we get back to business as usual
- Forecast future workforce downtime and the impact this may have on work output and customers.

4 Recording activity
- As part of incident response best practice, ensure all decisions made by the pandemic planning team are recorded

NOTES

HOW CAN IRM HELP?
SEE PAGE 5

HR

1 Policies
- Have you got policies and rules in place? Will they temporarily change in the meantime to allow more flexibility?
- Establish helplines for those that need guidance or support with business policy (see above)
- Ensure your sick pay policy is up-to-date
- Have you got working from home policies and guidance in place?

2 Organisational Risks
- Are there any members of staff who are at high-risk with COVID-19?
- Temporary staff availability is going to be scarce as companies look to replace sick staff with bank workers. Consider your other options should you need to do something similar
- Consider what the business' non-critical functions are if you need to streamline processes as more staff begin to isolate or work from home.

NOTES

HOW CAN IRM HELP?
SEE PAGE 5

CHECKLIST CONTINUED...

WORK FROM HOME

1 **Access**

- Does the business own the relevant software licenses and do they need to be amended to reflect new working set-ups?
- Do you have VPN access set up? Can it withhold the amount of employees that may be using it and will it be secure? (Learn more about how IRM can offer VPN security testing services on Page 5)
- Do staff have access to secure portable devices and equipment? Are you keeping track of who is taking equipment home?
- Consider display screen equipment health and safety requirements but understand that these may have to be relaxed if all staff are forced to work from home
- Will employees have access to the right utilities and telecommunications at home? Internet bandwidth may struggle when people work from home, so consider this impact
- Do staff have access to corporate information easily? E.G. intranets

2 **Protection**

- Ensure there is backup in place for business information and data
- Enforce strict change controls if people are taking laptops home
- Be aware of the increased rise of phishing attacks as outlined by the National Cyber Security Centre https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus
- Consider running a phishing campaign with your employees to see how reactive they are to reporting suspicious behaviour when at home. Use the findings to spread the word to employees and to remind them how important it is to stay vigilant. (Learn more about how IRM can help you with a third-party phishing attack campaign on Page 5)
- If you have staff training for cybersecurity, remind them where this can be located and encourage them to re-read and review the content
- Ensure your endpoint technology software is up-to-date and can offer as much protection as possible for those working from home.

HOW CAN IRM HELP?
SEE PAGE 5

NOTES

PHYSICAL SECURITY

1

- For staff not working from home, ensure that the existing work environment is secure and safe
- Ask all visitors to the workspace for contact numbers so they can be contacted in the event of a COVID-19 outbreak within your organisation
- Conduct a full risk assessment of physical security measures

HOW CAN IRM HELP?
SEE PAGE 5

NOTES

HOW CAN IRM HELP?

RISK ASSESSMENT

A risk assessment of COVID-19 and how this will impact your business would consider everything in this document and more. The outbreak has created times of uncertainty for many, highlighting gaps in their business policies and processes. IRM's experienced risk consultants can work with your organisation to conduct a risk assessment and streamline the business to ensure it stays effective.

VPN TESTING

If your organisation has adopted a work from home policy and the majority of staff will be using the VPN to access business information and assets, you should be consider assessing the reliability and security of your VPN. IRM's technical consultants can conduct off-site VPN assessments and provide you with a report outlining any remediation actions to ensure your VPN is safe to use.

BRING YOUR OWN DEVICE

If you want employees to start using their personal devices to continue working, but don't have any policies or rules in place, IRM can help. We have various policy sets which can be amended to be bespoke to your organisation and its specific needs during a period of work from home requests.

PHISHING CAMPAIGN

Cybercriminals are taking full advantage of COVID-19 to target businesses. When employees are new to working from home and don't have the support of colleagues around them, you may find that phishing emails become increasingly successful. IRM can organise a sophisticated phishing campaign targeting your employees. Rather than reprimanding staff who do click on the email, praise those who report the phishing email to IT in order to guide best practice across the business.

IRM INFORMATION RISK MANAGEMENT
.ALTRAN GROUP

Think cyber.
Think security.
Think data.

To speak to IRM about any of these services, or for more guidance on risk assessing COVID-19 for your business, email us at hello@irmsecurity.com

VISIT **IRMSECURITY.COM**

SECURE CYBER
UNLOCK OPPORTUNITY.