



# BAMBOO

► C O N N E C T ► G R O W



Developing futures with intelligent IoT, resilient connectivity  
and cyber-secure IT services.

*Lorrin White, Managing Director*

# Organisational Resilience

- Organisational resilience is the ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.
- More resilient organisations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal (Micro) and external (Macro) context.
- Enhancing resilience can be a strategic organisational goal.





# OR, DR or BC?

- 75% of businesses in the UK have a Disaster Recovery (DR) plan. *(Association of British Insurers)*
- 88% of UK SMEs have Business Continuity (BC) plans with only 50% of those having actually tested their plans. *(Crises Control)*
- Organisational Resilience linked to competitive advantage and should be a strategic imperative.



# Risk : Project v Business

## Project

- Health and Safety
- Public Liability
- Design liability
- Underestimation of costs or time required
- Organisation of contractors
- Unforeseen ground conditions
- Labour shortages
- Financial challenges
- Materials delivery
- Political factors
- Environmental

Detail to the level of defects trackers.

Risks and opportunities meetings.

## Own Business

- Owner related
- Contractor related
- External related
- Consultant related
- Labour related
- Equipment related
- Project related
- Materials related

All else covered in DR!



# BREAK OUT DISCUSSION

On a scale of Low to High how would you rate the following events in terms of risk?

Riots

Adverse/Severe Weather

Pandemic

Power Outage

War

Theft

Terrorism

Fire

# “It’ll never happen”

Event	Risk
Rioting	Low
Severe weather	Low
Pandemic	Low
Power Outage	Moderate
War	Low
Theft	High
Terrorist Attack	Low

‘It did’
2011
2004, 2007, 2017, etc
2020
Multiple
Location specific
Multiple
2001, 2005, etc





# Business Impact Analysis


- Team
- Scope & Objective
- Gather info
- Document findings
- Present findings
- Make a plan
- Review

Hazards	Assets at Risk	Impacts
<ul style="list-style-type: none"><li>- Fire</li><li>- Explosion</li><li>- Natural hazards</li><li>- Hazardous materials spill or release</li><li>- Terrorism</li><li>- Workplace violence</li><li>- Pandemic disease</li><li>- Utility outage</li><li>- Mechanical breakdown</li><li>- Supplier failure</li><li>- Cyber attack</li></ul>	<ul style="list-style-type: none"><li>- People</li><li>- Property including buildings, critical infrastructure</li><li>- Supply chain</li><li>- Systems/equipment</li><li>- Information Technology</li><li>- Business operations</li><li>- Reputation of or confidence in entity</li><li>- Regulatory and contractual obligations</li><li>- Environment</li></ul>	<ul style="list-style-type: none"><li>- Casualties</li><li>- Property damage</li><li>- Business interruption</li><li>- Loss of customers</li><li>- Financial loss</li><li>- Environmental contamination</li><li>- Loss of confidence in the organisation</li><li>- Fines and penalties</li><li>- Lawsuits</li></ul>





# Cyber Attack checklist



Type of attack	What does it look like?	Target audience	Intended impact/outcome
Malware: Ransomware	Email attachments or spurious links sent by email, text, etc providing access to systems for malicious software (spyware, worms, viruses, etc) to infiltrate PC/networks	Any small and medium businesses (SMB)	Systems rendered unusable Data encrypted/destroyed  Outcome- Payment for release of data/systems.
Phishing	Email, links in forums, social media, instant messaging applications.	Everyone and anyone.	Data theft – usernames, passwords, personal details to commit fraud
Spear-phishing	Personalised communications driving you to either pay a demand or enter your credentials into a website	Specific individual targets. Typically earlier reconnaissance has been carried out.	Immediate fraud or Data theft – usernames, passwords, personal details to commit fraud on a grander scale at a later date.
Social Engineering/ Vishing	Impersonation phonecalls	Typically but not limited to the Elderly, Financial industry, government employees.	Fraud. System access. Data theft.
Smishing	Texts hiding malicious URLs	If you have a phone you are a target.	Fraud. Data theft.
Whaling (Phishing)	Emails to arouse the interest or alarm of senior management, providing motivation for them to click the link.	Corporate officers and high level executives. Earlier reconnaissance has been carried out.	Immediate wire transfer of funds.

Now consider your assets and the impact on them of the incidents. How do you rate risk now?

Hazard	Risk Perception <i>What are the chances?</i>	People Impact <i>Skills &amp; Knowledge</i>	Premises Impact <i>Buildings &amp; Facilities</i>	Resources Impact <i>IT, data, equipment &amp; materials</i>	Supplier Impact <i>3<sup>rd</sup> party products &amp; services</i>	Impact Assessment <i>How much will it hurt?</i>	Mitigations <i>What can I do now to eliminate or minimise the impact?</i>
Theft	High						
Local/National Terrorism	Low						
Pandemic	Low						
Utility outage	High						
Supplier failure	High						
Cyber attack	Low						
Recession	Moderate						

Hazard	Risk Perception <i>What are the chances?</i>	People Impact <i>Skills &amp; Knowledge</i>	Premises Impact <i>Buildings &amp; Facilities</i>	Resources Impact <i>IT, data, equipment &amp; materials</i>	Supplier Impact <i>3<sup>rd</sup> party products &amp; services</i>	Anticipate	Prepare
						Impact Assessment <i>How much will it hurt?</i>	Mitigations <i>What can I do now to eliminate or minimise the impact?</i>
Theft	High	Low	Low	High	Low	Low – Mod/High	Asset Trackers Site Cameras
Local/National Terrorism	Low	High	High	High	Moderate	Mod-High	Fully tested failover Diversified revenues Drone technology
Pandemic	Low	High	High	Moderate	High	Mod-High	Safe access to data Secure, clean homeworker kit On site Thermal Imaging health checks Access to PPE Virtual compliance Site security: drones/trackers/camera
Utility outage	High	Low	Moderate	High	Moderate	Low- Mod/High	UPS Alternate/back up connectivity source
Supplier failure	High	Low	Low	Low	High	Low – Mod/High	Supply chain Due Diligence Project financing options Stock pile core materials
Cyber attack	Low	Low	High	High	High	High	Threat intelligence – open & dark Penetration testing Remote shut down/kill capability Continual off site back up Virtual server environment Practiced protocols, MFA Education
Recession	Moderate	High	High	Low	High	High	Drone surveyors Project/contract spread

# Respond and Adapt

		1 Aspirational	2 Essential	3 Optional	4 Useless	
<b>Advisable</b>		Key to operation in order of priority (1=Aspirational, 2=Essential, 3=Optional, 4=Useless)				
	Pre pandemic	Pandemic lockdown	Primary homeworking	Staged return to office	Lose some commercial footprint	Lose all commercial footprint
	<i>The old norm</i>	<i>Social and economic lockdown (except key workers). All non essential offices closed. All workers who can to work from home.</i>	<i>10% office workers. IT/one department in office, all others operating remotely but unable to travel.</i>	<i>Multiple departments/age groups able to return to office intermittently under social distancing regulations. At least 50% of workers operating remotely at any one time.</i>	<i>Businesses make the decision to lose some commercial office space and operate at least 50% of business from home working environments. Travel restrictions and social distancing lifted.</i>	<i>Businesses make the decision to lose all commercial office space and operate all business from home working environments. Some restrictions</i>
<b>Respond</b>						
Thermal Imaging solution	3	3	2	2	2	4
Interactive whiteboards	3	3	1	1	3	2
Compliance dashboard	3	1	3	3	1	2
Compliance consultancy	3	3	3	3	3	3
Compliance auditing	3	3	3	3	3	2
Cyber training	1	1	1	1	2	2
High quality cameras	3	3	1	3	1	2
Back up WiFi for homeworkers	3	1	2	2	2	2
<b>Adapt</b>						
Software to manage individual performance remotely						
Travel technology pack for home workers						
Retina scan access to offices						
Dictation software						
Stylus operation						
Personalised removable keyboard and phone covers						



# 75%

of survey responders are moving to a more flexible working environment, keeping some teams working from home and some in the office



**BAMBOO**  
CONNECT GROW

## Business continuity solutions considered with either a phased return to work or restrictions being imposed again.

LONE WORKER SOLUTIONS 31.76%  
REMOTE WORKER CONNECTIVITY 56.47%  
RIDDOR COMPLIANCE 16.47%  
CYBER PROTECTION 45.88%  
ALREADY HAVE THIS ALL IN PLACE 40%  
OTHER 7.06%  
OTHER REASONS:  
- SOCIAL DISTANCING  
- ALREADY A REMOTE WORKER  
- CAN'T DO ANY OF THOSE OPTIONS



**BAMBOO**  
CONNECT GROW



# 20%

of survey responders did NOT close their normal place of work

**BAMBOO**  
CONNECT GROW

# 43%

of survey responders are NOT AWARE of the additional regulations HSE has imposed as a result of the pandemic.



# 7%

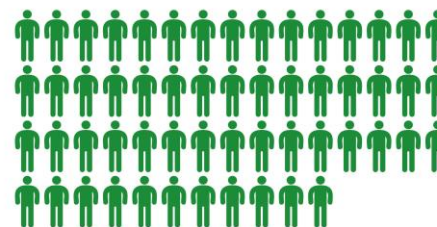
of survey responders are looking to adopt a completely new way of working (i.e. no permanent office space, remote applications etc.)



**BAMBOO**  
CONNECT GROW

# 59%

59.34% of you felt your IT and communications provider responded well to the COVID-19 situation



56 survey responders are currently discussing their return to the office plan.

**BAMBOO**  
CONNECT GROW

## BUSINESS CONTINUITY IN A PANDEMIC LANDSCAPE

We conducted a survey to help us understand how companies are approaching business continuity and regulatory compliance with other pandemic working measures and in the future. This was intended to assist in the planning of our compliance and consulting services and get an insight into the business around us and the results have proven very interesting.

Take a look for yourself.

# 59%

59.34% OF YOU FELT YOUR IT AND COMMUNICATIONS PROVIDER RESPONDED WELL TO THE COVID-19 SITUATION

# 56

56 SURVEY RESPONDERS ARE CURRENTLY DISCUSSING THEIR RETURN TO THE OFFICE PLAN



# 20%

of responders did NOT close their normal place of work

LONE WORKER SOLUTIONS 31.76%  
REMOTE WORKER CONNECTIVITY 56.47%  
RIDDOR COMPLIANCE 16.47%  
CYBER PROTECTION 45.88%  
ALREADY HAVE THIS ALL IN PLACE 40%  
OTHER 7.06%  
OTHER REASONS:  
- SOCIAL DISTANCING  
- ALREADY A REMOTE WORKER  
- CAN'T DO ANY OF THOSE OPTIONS

Business continuity solutions considered with either a phased return to work or restrictions being imposed again.



# 43%

of survey responders are NOT AWARE of the additional regulations HSE has imposed as a result of the pandemic.



# 73%

of responders felt CONFIDENT they had continued to meet all GDPR, HSE ISO or equivalent regulations during lockdown



# 7%

of responders said to completely revise their compliance position post lockdown

75% of responders are moving to a more flexible working environment, keeping some teams working from home and some in the office  
16% are returning to working exactly as they did before the lockdown measures were put in place  
7% are looking to adopt a completely new way of working (i.e. no permanent office space, remote applications etc.)  
2% are moving to a predominantly home working environment, hence reducing commercial space accommodation and travel expenses.

Visit [www.bambooback.co.uk](https://www.bambooback.co.uk) for products and services.



73% of survey responders felt CONFIDENT they had continued to meet all GDPR, HSE ISO or equivalent regulations during lockdown

22% of responders felt they had met some but not all

5% of responders did not feel confident they had met their regulations

**BAMBOO**  
CONNECT GROW

# Agile and Able



- Don't rely on just your DR or hearsay to carry you through this
- Next Steps for Now

Model the potential scenarios

Assign the team

Set the objective

Take critical operations into account

Evidence the position

Relay, act, review

- Next steps when you can

Full Business Impact Assessment

Review and renew Business continuity plan

Test it.



# Technology

What are customers asking us for?

## Immediate

Cyber attack awareness updates  
Short term contracts  
Mobile devices  
Homeworker tech  
Thermal Imaging solutions  
Drone technology  
Anti-virus  
Software

## Mid

Cloud back up  
Penetration testing  
Traceability/tracking  
Compliance software

## Long game

Technology workshops  
Infrastructure review and change program  
GDPR, Cyber and ISO compliance





# BAMBOO

► C O N N E C T ► G R O W