The BCPcast:

Advice from the Experts

2016 SAW THE LAUNCH OF THE BCPCAST.WE TALKED TO BUSINESS CONTINUITY EXPERTS ABOUT THEIR EXPERIENCES WITH BC AND DR PLANNING.

POWERED BY:

Databarracks

B C P

WE ENDED EVERY INTERVIEW BY ASKING ONE FINAL QUESTION:

“What is something organisations could do in the next 24 hours to improve their resilience of any kind against disruption?”

John Robinson, INONI

“First thing I would do is build a risk register. If I’ve got 24 hours to do it, I’d probably get an Excel spreadsheet out, I’d get my key people around me - and I don’t just mean senior management, I mean people who understand the operation - and I’d ask them what they think the main threats are to the organisation. I’d spread that as wide as I could, and I’d build a genuine risk register.

“What I would then do is look at which of those threats are the most likely. It’s a very hard thing to do, but I would certainly try and grade them.I’d then want to know how good our defences are against each of them, so I’d effectively downgrade them. I’d start to find the areas of vulnerability and plan the scenarios in which they might materialise. Once I’ve got my list of scenarios, I want to know how well prepared we are to deal with each one.

“That simple three-stage approach is what we use. It doesn’t have to be in Excel, there are other tools you can use to do it, but with this approach you can find out exactly where you are, you can see how well prepared you are. If you don’t have a continuity plan at all, you can start to plan what you would do if each of those scenarios arose. That will get you from nowhere to somewhere really quickly.”

> “I’d start to find the areas of vulnerability and plan the scenarios in which they might materialise.”

Matt Hogan, London Fire Brigade

“At the risk of sounding like a salesman, go and have a look at the London Risk Register.

“It’s a place where we’ve captured lots of different scenarios that could potentially affect London, but actually they could apply across the country as well.

“Start there, think about whether those risks could affect you, and what you would do in response to that. And think about that as an organisation, but also think about how those risks might affect your customers and your suppliers, because that generates risk for you as well.”

Stewart Duguid, BP

“Take a time, say 11 o’clock tomorrow. And say ‘if this happened, how would I know that everyone is safe?’

“And then the answer from there is to set up a call tree, and have...” Well I would phone so -and-so, and so-and-so would phone three other people” and then the information would eventually filter down.

“That’s very slow and very cumbersome”

“It is liable to be broken because people are on holiday or won’t answer the phone, so the other thing is that people may look towards is an automated call messaging system. I believe there are ways round social media to keep things private as well so you could get everyone subscribing to private chats within social media. That might be a possibility. That’s not too expensive.”

Michael Faber, Regal Training and Consultancy

"Take an hour out and play a game - go through a test scenario.

> "You don't need to make it any more complicated."

"The scenario doesn't matter - if you want to choose a fire choose a fire - but for whatever reason, we're out of the building, we didn't take anything with us and we can never return. And whether that's a company with two directors or a very large organisation, it's a very simple first step. From that I will guarantee that you will identify the things that you need to do, things that you need to think about, things that you need to back up, things that you need to check.

"The other thing is to make sure you think about communication. And again it could be just a simple thing of making sure that you've got a few key telephone numbers; a couple of your key clients, your staff that you can communicate with, and any other sort of information that you need. I think those are the most important things, and they don't cost money."

Paul Kudray, KCL Consulting

"I think, fundamentally, it is just the self-assessment of knowing what their business does. It's as scientific as we want to make it, and sometimes it comes across as a bit of a dark art. But the bottom lines are what any organisation needs to look at. It's the basics. What do they do? What do they need to do it? What do they rely on? What could go wrong? And what would they do if something goes wrong?

"There's just five key elements as part of that process. And yes, it needs to be formalised, so it's not just personality dependent and reliant on certain individuals. It needs to be formalised so anybody could pick it up. But it's as simple as that, for me."

Vicki Gavin, The Economist

"I would say sit down as a team and talk about 'what would you do if...?' A lot of people will spend a lot of time and money to organise crisis exercises - but they don't need to be that complicated. If you're worrying about event X, sit down as a team and say 'What if it happened? What would we do?' And think about it. That'll do a couple of different things for you.

"First of all, it helps you start to develop a shared risk appetite, because everybody who's sitting around that table is going to be able to hear what each other are saying, and you will come to a consensus of what you're going to do. That's a shared risk appetite.

"The other that it does is it stores away in your brain the what-to-do-if-this-happens. So the human brain is an amazing thing. And in there, we've got a little bit called the Amygdala. It's where the fight or flight reflex is, and essentially what it does it intuitive decision making. And it uses all of that information that we've seen, that we've heard, that we've felt, everything that we've ever experienced is stored in there.

"Not in an accessible kind of way, but in an intuitive way. And that immediate decision-making, when your gut says 'this is what I should do' is your Amygdala kicking in and saying, 'Based on everything we know, this is the answer'. The rest of your brain then gets involved and says 'Oh, but what about this and what about that, and what about the other thing'. So the more things that as an organisation you need to have immediate responses to, that you talk through, that you work through, the more that's intuitively stored in your collective brains, and the quicker and easier it's going to be to respond to them in the future. So if an organisation does nothing else, if they just start talking through 'What would we do if...', it will put them in a significantly better place to recover."

> "It helps you start to develop a shared risk appetite."

Paul Butcher, Fujitsu

"One of the things I've used on a number of occasions, whether it's a new customer or somebody who's got nothing in place, is getting their senior people around a table and presenting them with a scenario.

"'Your building's gone up in smoke, it's a pile of burning rubble, what do you do? And just talk them through that process. So...' 'I don't know, I don't know who we'd contact.' Right, great. You don't know. Jot that down. What else? What's going to be the impact? 'Oh, customers can't call in or we can't get the goods out the door, or we can't contact our suppliers' - whatever it might be, jot it down, grab it. Who's going to make up that team? Who would you contact within the organisation to get the IT going, to get the phone going, to get whatever else, jot it all down.

"So at the end of that day, you can come out with a very rough and ready plan of action of what you would do if that happened. Or, what are the questions I need to now go away and find out? Who would I call? You could almost get your Crisis Management Team together in terms of roles and responsibilities. Who's going to look after the cash? Who's going to look after the media? Oh, we've got a marketing person, you can do that, great."

> **"Your building's gone up in smoke, it's a pile of burning rubble, what do you do?"**

Mel Gosling, The Continuity Shop

"The answer to that is being able to have access to your business data whatever happens, and to be able to communicate with your customers. That means making sure you've got all your data backed up and you can recover it, and you can communicate with the people you need to communicate with.

"If you've got those two things nailed down, you're a long way towards solving the problem."

Rob Dartnall, Security Alliance

“I would start developing your insider program. I’m not talking about insider threats as in you’ve got your malign guy who is working against you, but insider threats can also be unintentional - your guys who are getting spear phished or phished and clicking on inappropriate links, people moving and deleting files, all that kind of stuff.

“So starting there is great, but the bit I’d add is disseminating that information as well. One of the major issues from the conventional intelligence world is sharing of intelligence. Governments are getting better at it - within the UK, we’ve got the Five Eyes, which is the UK, the US, Canada, Russia, New Zealand. Historically, there has been this need to know, need to hold principle. So people go, “I’ve got this piece of intelligence, this information, it’s really sexy, it’s really important, I’m going to hold onto it,” and they don’t share it.

“But there is another principle which works against need to know and need to hold.

“That’s making sure that everyone that needs to know the information really does need that information. If you’re talking about a sibling or a similar industry being attacked, share that, but don’t just share the news story. That’s information, that’s not intelligence. Intelligence is the ‘so what’, it’s the assessment, it’s what it means to you. “If we were attacked in this way, we would also likely suffer losses similar to that, around this amount of hundreds of millions, therefore it is likely there will be job losses.” etc.

“Make it valuable for people to understand and make sure they know why you’re telling them. That is intelligence. Sharing a news story, that’s information, two different things.”

> “One of the major issues from the conventional intelligence world is sharing of intelligence.”

www.thebcpcast.com