

Are you prepared for the unexpected?



So “there she was just a-walking down the street” when the car swerves to miss the dog, leaps onto the pavement and knocks her over. She has a broken arm and a fractured knee. A small crowd forms to see how she is and to help keep her comfortable until the ambulance arrives. All except that is, the nasty piece of work that steals her bag and runs off with it. Cash, credit cards, mobile phone, today’s post, house keys and of course a laptop! The usual contents that most of us carry around each day.

This is the kind of event that could happen to any of us at any time. The implications and the repercussions to her will almost certainly be inconvenient and could be significant if she has not taken some basic precautions. But like any operational

interruption it can happen at any time and certainly when you are least expecting it. So then ask yourself, what would happen if my organisation was to face an incident from which it had to recover, and is it prepared to handle the fallout?

You will be pleased to know that this lady was taken to hospital and recovered fully. Her recovery was made easier because she had taken some sensible precautions which meant that the loss of her bag and contents did not cause her too much inconvenience.

It is worth spending a little time reviewing how the problems

caused by the loss of her bag were handled and then look at that in the context of a business continuity incident in a large organisation and observe the similarities.

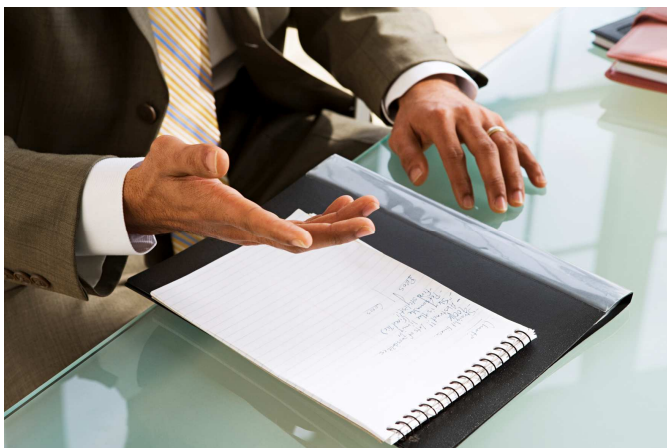
Cash

Fortunately our lady doesn’t carry all that much cash, never has done, it’s the first thing the thief will take. She has always seen cash as something she might have to give away if she was mugged so she always carried an amount of cash she was prepared to lose. This can be seen as her appetite for risk.

Corporate equivalent of stolen cash

As an organisation have you considered, and do your teams understand, what you can do without in the event of a major incident? This can be in relation to systems, office availability, staff etc. Do you know what processes you have to get up and running first?

This needs planning in the cold light of an ordinary day: staff get



very sensitive about being told in the middle of a crisis that they are not critical to the business! However, the reality is that in an emergency it takes fewer people to keep a business ticking over. You need to have this in a plan, have tested the plan and follow the plan. In the heat of the moment it is better for people who may be in a highly emotional state to have a plan to follow. This will reduce the number of “on the spot” decisions made to a minimum.

This is relevant to the cash example because the organisation needs to understand the risks it is running and the risks it is prepared to take. Your clients, whilst having an element of sympathy with the events unfolding around you, will rapidly lose that sympathy if you lose their money, their data, or don't deliver your service on time – because in this day and age you are expected to be able to cope with unexpected business interruptions.

Credit Cards

The good news is that our lady subscribes to a service whereby one phone call can get all of her credit and debit cards put on hold. And because she is smart, that phone number is kept in a small pouch she keeps in her coat. So she borrowed a phone and got that done really quickly. This risk was eliminated with no harm done.

Corporate equivalent of stolen credit cards

In the event of a business continuity incident it is important for the organisation early on to ensure it is safeguarding the assets of the clients and the company. These may be physical or financial assets. The company

should be holding key information about its financial assets – i.e. bank account records, signing authorities etc – in a secure offsite location with access restricted to key staff. It will be important to ensure that money to pay suppliers, staff etc does not get delayed as a result of any incident.

Mobile phone

These days losing your mobile is a great inconvenience. Ringing the mobile company and cancelling or putting a stop on the phone is relatively easy. Its just the loss of all the contact details that is the issue. Fortunately our lady keeps an old fashioned diary and address book at home so all is not lost. It just means taking time to re-input the data back into a new phone.

Corporate Equivalent of the stolen mobile

It does come down to the planning again. In the event of an incident the first thing any organisation should do is locate its entire staff, ensure that they are safe and communicate with them. The next most important people to talk to are the clients who need to be reassured that you are on top of the problem, and are managing their assets, information, services etc as well as possible in the circumstances. It is vital to communicate to these key stakeholders, keep them informed as to what is happening and manage expectations. Communication is key to surviving an operational interruption. Do you know how to contact all your staff and clients in a crisis? Have you got up to date contact details for your staff and clients held securely

somewhere outside of your premises?

Today's post

Actually whilst this is inconvenient the actual loss of the post is not the issue. Far more important is the personal information that might have been in that post. For example: address, bank account numbers, and other personal information. Fortunately she remembered what post she had received and was able to contact the senders and get information resent. She wrote to her bank to tell them what had happened and asked them to keep an eye open for irregular transactions on her account.

Corporate equivalent of lost post

Everyone in the organisation will be busy trying to get the company re-established and operating normally again. It is important for both employees and clients that normality be restored as soon as possible.

But there are people who may take advantage of the period of disarray within the organisation to infiltrate certain processes to gain illegally from the organisation. At times of stress when getting the company back working normally it is not easy to spot the unusual transactions; but vigilance is vital. People are most likely to try to take advantage of an organisation when it is at its perceived weakest moment. Training and educating staff to identify out of the ordinary transactions is very important for the long term well-being of the organisation.

Lost keys

The lost keys are now in the hands of the same person who

has her home address from the post which was also stolen. She is lucky because today her partner/flatmate is not working and is at home. So one phone call home and she managed to arrange for her locks to be changed. This might not have been such a good result had she had no one to call to get this done.

Corporate equivalent of lost keys

Similarly the effect of stolen or lost security passes can have an equivalent impact on corporations. One of the issues which many organisations struggle with is keeping a track on who has active security passes at any one time. It seems surprising to note that whilst most organisations have processes in place to take back or disable security passes from staff leavers, it often doesn't happen; or there can be some delay in catching up with the process. It is important therefore, when staff are being laid off in particular, to ensure that security /entry passes are made ineffective as soon as possible to avoid disaffected staff coming back to the organisation and causing damage.

Naturally in the event of a business continuity incident it

will be probable that some security passes may go astray. Importantly, part of the recovery process needs to keep a track on this as the last thing a company needs to happen at a time like this would be to have a security breach. Underlying this, all organisations need to have in place a robust starters and leavers process to ensure access to offices and systems is properly controlled.



Stolen laptop

Again, some more good news. Not only does her laptop have password protection but also it is one of those new ones with fingerprint recognition. More than likely the thief will just throw this in the nearest skip because it is too hard to get into and would be difficult to sell on if access to it was denied.

Although a more committed thief could easily remove the hard disk to access the data.

Corporate equivalent of a stolen laptop

“Personal data on stolen laptop” seems to have been a regular news item over the past couple of years. This

creates a huge reputational risk for organisations who suffer such a loss. It is relative easy for data on mobile technology to be encrypted and for laptops to be made secure but many companies don't do this. Also the use of wireless internet in public is becoming more and more prevalent, but do they understand the risks of someone hacking into their systems whilst they are using it? These events can be protected against; but

the security protocols need to be set up correctly and staff need to be trained in the importance of maintaining data security at all times.

Pandemics

Maybe our heroine was suffering from an infection! Probably the biggest issue for organisations preparing themselves for a pandemic is the availability of staff, particularly those with business-critical knowledge. Staff may of course be absent because they are infected; but it also needs to be remembered that they may have children or other dependents to care for. They may even stay at home simply from fear of infection. It is estimated that in a severe pandemic, you may assume that absentees will peak at up to 40% of the workforce.

You should consider multi-skilling your workforce; and pay much closer attention than might otherwise be the case to documenting your procedures and drawing up succession plans. This will put your organisation in a much better



position to react to difficult circumstances.

Another difference which a pandemic brings to continuity management is the planned response. Many business continuity plans will rely on the availability of an alternate site for the relocation of business processes. In a pandemic situation, this locality may not be available – suffering the same problems as the primary site. Indeed, the movement of available staff may be prohibited or simply impractical.

Conclusion

Of course all of this is blindingly obvious stuff isn't it?

But are your business contingency plans up to scratch, have you tested them, will you still be in business after an incident? In the changing times that the economy is going through you could be significantly changing the profile of your organisation e.g. changing product lines, reducing staff, reducing capacity etc. In the heat of striving to keep your business afloat in difficult times it will be easy to neglect your business continuity plans. Have your plans been updated for

these and other changes that have taken place in the last year?

Do you have the necessary business protection processes in place? Do you have a plan and understand what risks you are prepared to take to keep the business going, are you ready to communicate, can you spot unusual activity, is your physical security up to date and is your technology secure? Have you tested your arrangements to ensure they are appropriate and fit for purpose?

Your clients will expect you to have all of this in place!

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010 info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD