Cyber Security Forum

Presentation C.B (Sam) Mulholland

Good Afternoon

My name is Sam Mulholland and I am the Managing Director of Standby Consulting.

Just a little bit about myself. I have worked in IT for over 30 years. Prior to setting up my company in 1997, I worked for a company called Databanks Systems in New Zealand. Databank was owned by a consortium of Banks to carry out the cheque processing, settlement and posting of transactions. Databank was the first nationally integrated cheque clearing system in the World.

I worked my way up through the ranks of Databank doings such key roles as a shift manager for a central processing data centre, to a data centre manager for 16 years prior to establishing up my own company initially in partnership with IBM New Zealand.

In 2009 we commenced a project for American Excess, Middle East and North Africa. Shortly after that we established our Middle Eastern regional head office in Bahrain. From this office we carry out consultancy services across the Middle East.

Moving on into Cyber Security

There is nowadays, a significant library of cyber security research and cyber breach examples available for us to work and learn from. During this presentation, I will be working primarily from a small selection papers which after reading through the majority of the other research offer an excellent representation of the current trends in Cyber security.

Two phases of Cyber security

There are two main phases;

1. Security and prevention
2. Breach containment and Crisis Management

- Slide 2

When we discuss Security and prevention we tend to focus in 3 key areas

The 1st is Technology – which is your anti-virus and sandboxing software, the behavioural threat detection type software. All of which I'm sure you will hear a lot about over the course of the next few days

The 2nd is IT Governance; – this tends to be activities that regulate good and safe usage of the IT systems such as

- blocking the use of USB's;
- regular forced changing of passwords,
- regular updating and patching of systems,
- Business partner IT governance assessments
- Cloud or Internet of Things governance items.

Again, I'm sure these items will be covered in greater detail over the course of this forum.

The 3rd and just as important as any of the others; is the education of staff and management. This education is to make sure they are fully aware of the governance policies as well as good habits that they should use when on the corporate network.
Your organisation needs to have in place strong IT governance polices followed up with education to make your personnel aware of the risks of opening emails from unknown sources, in particular with attachments, going onto unusual web sites and clicking onto links.

Train your personnel to be aware of “unusual events or responses” and have them report them to your IT Security Department.

Education and training needs to be supported by the senior management of your organisation. It will not happen unless you do this.

Even if all of this is covered though and lots of time and money has been spent throughout your organisation, there is still no guarantee that you are fully protected. Hacking is a major business both for the criminals and also the minds who find it a challenge. Because of this one can never truly stay ahead of the hackers;

Slide 3

So

It is WHEN and not IF!!

Significant time and resource should be given to the preparation on the basis that you *will* have a breach.

You have to ensure that your organisation, staff and management are trained and prepared to manage a Cyber breach crisis, quickly and effectively.

By using the ***When not If*** approach, your organisation will be far better prepared to deal with a breach should it occur

The following sections of my presentation will focus on the actions your organisation should take to prepare for a cyber breach.

Cyber Security is ***NOT*** Just a IT Problem

Many organisations still think that Cyber Security is just an IT problem and if the breach occurs then IT will fix it. Yes, IT will fix the operational problems, IT are not, and should not however be responsible for the other damage that will likely occur to your organisation if management has not prepared for such an event.

- Can IT deal with the financial impact of a breach?
- Should IT communicate directly with your regulators and stakeholders during and after a breach?
- Should IT be calling your customers individually to let them know they are dealing with the event and they should not panic?

No, these actions are not the role of IT.

Let IT deal with the attack and focus on that. It is the role of the other departments to deal with the ancillary activities that will occur because of this breach

The importance of being prepared for a cyber breach, has been highlighted in two papers released last year.

Slide 4

The first was from Ponemon[1] on behalf of IBM which stated;

"The biggest financial consequence to organisations that experienced a data breach is lost business. Following a data breach, organisations need to take steps to retain customers trust to reduce the long-term financial impact."

Slide 5

The other report of interest is one by PWC on Cyber security in the Middle East published in March 2016[2] which states;

"Cyber security is not just a technology issue. It's a business issue. Digital is no long the sole domain of IT and there are very real risks in allowing it to remain so,: not just the risks of lost opportunity but financial, commercial and reputational risks too".

This report also states that;

"Companies can have a greater tendency to believe they can fix cyber security by buying a technology "fix". But this needs to be supported by a parallel investment in awareness and training".

The buying and committing to quality technological fixes is very important but also there needs to be significant effort put into , good IT governance and user policies as well as general cyber security awareness training, as previously highlighted.

It is also essential that were a breach to ever happen, management and other stakeholders are trained and experienced to know how to deal quickly and effectively with the crisis. This is not only mid-level

[1] Ponemon Institute, 2016 Cost of Data Breach Study: Global Analysis

[2] A false sense of security? Cybersecurity in the Middle East, March 2016 published by PWC.

management but it applies to Senior Management and Board members as well.

Why do I say this?

These breaches can happen incredibly fast, and have a wide impact in a very short time. The technology people will be onto it quickly however your business will suddenly grind to a halt and may be out of operation for days or even weeks.

Slide 6

A report by Timico[3] in the UK showed a company can be brought own in 60 seconds:

Of the companies hit by Ransomware that 85% of them were down for a week or more".

As financial institutions have you considered how you will keep operational if your IT systems were down for a week or even two weeks.

That is how long it *could* take to rebuild your systems. Replicating to a secondary site may not be of use in the recover, - as the malware could well be on your DR site before you realise the danger. The only thing that save you from Ransom ware is taking backups and then removing them off your system.

In a very short time after a cyber breach you need to have plans to deal with the situation.

To paraphrase an article in the Journal of Business Continuity and Emergency Planning[4]

[3] Timico – Gone in 60 Seconds – The grim reality of RansomWare

[4] Journal of Business Continuity & Emergency Planning Vol six Number 4 Spring 2013

"A response that appears to be inept, will be seen that an organisation is not adequately or professionally prepared to deal with such an event. This will result in massive damage to your organisation from which it may never recover."

Consider, for example how you will meet your customers needs, if you were down for say a week. Then consider the highly important transactions such as interbank settlements. This problem is even more critical as countries move more and more into electronic transactions. Cash is slowly disappearing .

So, what can we do about this?

Your organisation needs to have a cyber response plan in place.

Slide 7

Time is your enemy in these events and you will not be able to decide on roles and responsibilities after the breach.

Your organisation must be prepared. Organisations no longer have the benefit to be able to keep these events to themselves for hours or even days as they used to. Social media will soon pick up on such events and then next thing you know you will have the news media on your door step and everyone around the world will know about your problems.

Also consider that organisations are being encouraged to make people, in particular the central banks and other important legal groups, aware of a breach so that others can learn and take precautionary actions to isolate their exposure.

So you need to be prepared and have a plan in place.

What sort of Plans – what preparation measures can we have in place?

You need a purpose built Cyber Response Plan

You may have a Business Continuity Plan but the action and roles that people need to take are different to your normal business continuity plan.

A cyber breach is a scenario that needs to be covered in your Business Continuity Plan.

This plan needs to identity the type of Breach and the range of the impact. It may be a breach of non-sensitive information, or it may be critical information. The levels of reaction needs to be defined and the actions to be taken listed, who needs to be informed and the level of escalation that needs to take place.

Specific Elements in a Plan for a cyber breach:

Slide 8

You will need a **Communications Plan** – The plan needs to define the following roles:

- Who the spokesperson or the organisation will be for this event it has to be the CEO. By using the CEO your organisation is showing how important it considers the event is and how hard the organisation is working on it.
- The media support personnel who will be working with the CEO preparing press statements etc
- Your social media person
- Who will update the web site
- Who will contact your Board Members and other key stake holders

- Who will contact the respective central banks
- Who will communicate with your personnel, and also key vendors, other suppliers.

The communication plan needs to contain contact details for the various media organisations

Pre-pared press releases

Boiler plate emails, letters and other anticipated communications

Some of these items need to be printed and filed ready for use. In a bad breach you may not be able to print them out and send emails, so think of alternative ways of getting your message out to the interested parties.

On click ===Social Media === (half way through presentation)

Your media plan needs to cover social media. Social media can be a good thing and a bad thing. It can be a great source of intelligence, it can point to issues that you were not aware of, and it can also be used to communicate out to your client base and the news media.

Always run the test, if you are going to put anything up on social media, "how will this look if it got onto the front page of the news paper tomorrow morning.

Other Items to have in your Cyber Breach plan

1. Scripts for your call centre for when customers ring.
2. Talking points to discuss with customers. Not only do you need to keep your callers informed but also you need to gather information from them as this sort of intelligence may help you to define where the breach occurred and the extent of the breach
3. Automated responses via IVR should be pre-set up and can be activated as your call centres will soon become over loaded
4. Frequently Asked Questions (FAQs)

5. There also needs to be defined the trip point where your organisation reports it to your central bank.
6. Pre-defined mitigation actions – for example, how you respond to customers who are desperate for cash? Do you make a cash advance to them with minimal information about their financial situation or you just ignore them? Remember in a bad breach you may not have a computer system to be able to look up the customers details and identify them, by such means as CPR, date of birth etc.
7. Do you need to get more cash in from the Transit cash people? With the ATMs down and cards not being honoured, customers will come into your branches looking or cash.
8. Manual processes to deposit funds from your retail outlets or do you tell them to keep their cash in their offices?
9. How do you process credit and debit card transactions? Ok some base information is kept at the credit and debit card switches but there will be limits and the system will soon exceed the levels set.

And so, the list goes on. These are all issues that you should have thought about before you have a cyber breach. Remember time is your enemy and if you do not cope with the situation quickly your organisation will suffer.

So, you have your draft plan developed.

Can you rest and have a coffee – ***no;*** now you need to test it.

Slide 9

This is where a simulation test will highlight shortages in your plans and things that you have not thought about. Try to make these exercises as realistic as possible and have the people who have roles assigned to them carry out the actions they need to take. Items that were not thought of are soon highlighted and as a team they can decide on the best actions to take.

Assign external roles to “players” in the exercise who will act as customers, news media representatives, and concerned stakeholders in your organisation.

In carrying out these cyber simulation exercises your teams will become trained and better prepared for such events.

These simulation tests or exercises must be supported by the senior managers in your organisation. The results of these exercises need to be part of the reports made to your Board and your Audit and Risk Committee.

Does this planning pay off?

Slide 10

Yes it does. Another of IBM’s papers on Data Breach – the impact of Business Continuity Management[5] shows that

there is significant savings and a great improvement in recovery times if you have a business continuity plan to deal with a breach in place.

[Read from Slide]

Companies that involve BCM achieve an average per day savings of $6,591 through the containment phase of the data breach response”

“The average cost per lost or stolen record can be as high as $167. With BCM involvement the average cost can be as low as $149”

“The average cost per lost or stolen record can be as high as $167. With BCM involvement the average cost can be as low as $149”

“A 52-day reduction in the mean time toidentify a data breach”

[5] 2016 Cost of Data Breach Study: Impact of Business Continuity Management by Ponemon Institute.

“36-day reduction in the mean time to contain a data breach”

“29% decrease in the likelihood of a data breach over the next 2 years”

So, what this IBM paper is saying is that Business Continuity Planning is the foundation that you need to build your specific Cyber breach plan on and even though there is a cost in developing a Business Continuity Plan, you will get a financial benefit if a cyber breach occurs .

In conclusion:

When you have, a cyber breach occur it is not just an issue for IT, it is an issue for the whole of your organisation and senior management must be involved.

You must have a cyber breach plan in place and then train yourselves and your personnel to be able to re-act to such an event; positively, quickly and efficiently otherwise your organisation will suffer major outage of services, brand damage and reputational damage which could to be fatal.

Thank you