PHYS ORG

What's your IT department's role in preventing a data breach?

May 21 2014, by Rob Livingstone

Who is really in charge of an organisation's IT security? Credit: Flickr/Pacific Northwest National Laboratory, CC BY-NC-SA

How do organisations and their Information Technology departments rate when it comes to protecting themselves and their organisations against the ever present cyber risks and cybercrime? The answer is, on average, poorly.

This was a point highlighted by Wade Baker, principle author of the 2014 Data Breach Investigations Report from the US mobile communications company Verizon.

After analysing 10 years of data, we realise most organisations cannot keep up with cybercrime – and the bad guys are winning.

So what role does the organisation's IT department play in helping to win this war – if any?

If the executive and leaders in organisations expect their IT departments to carry the full accountability for protecting them against the risks – of either an accidental data breach or a loss from cybercrime – then they may want to pin the tail on another donkey.

Let me explore the rationale behind this position.

Quo Vadis – IT department?

Much has been said in the business and IT industry media in recent years about the transformation underway of the role, structure and leadership of IT departments within organisations.

These changes are in response to influences such as the rapid change in technology, financial austerity, globalisation, easy access to user-friendly consumer technologies, cloud computing, the need for speed, smartphones and other mobile computing devices.

Within most organisations the demands placed on their IT departments are diverse and complex. They include aspects such as risk management, cost control, driving innovation and so on.

The fact that information technology pervades almost every aspect of the contemporary organisation is widely understood and acknowledged. But the interdependencies between differing systems, technologies, business processes, governance and risk profiles are often not, and this is a challenge facing all executives.

Everyone's an IT expert these days

The ease of access to many business-ready technologies makes it easier for executives and managers to take on the roles and responsibilities normally held by IT departments. This is often driven by the need to meet short term, localised demands.

It should come as no surprise that the resulting influence of the IT department is being diluted. Analysis of recent IT project spending trends show that, on average, more than half of IT projects are now being funded by the business executives, and not the IT department, with that trend expected to continue rising.

Organisations that are at war with their own IT departments should raise the white flag now. This situation should be remedied swiftly if the organisation is to maximise the value of enterprise technologies with known risk and known cost.

In places where IT is continually blamed for the poor "delivery" of IT projects, shadow IT (out of sight of the IT department) is flourishing across the organisation.

Vendor predation, where new technologies are pitched direct to the business leaders and bypass the IT departments, is also rife. Executive discussions always boil down to cutting IT costs and usually have little to do with the technologies used or how they are managed.

It is in such environments that cybercrime is likely to be a real threat.

What do IT departments need to do to protect their organisations?

Or, perhaps this question should be reversed: What should the organisation be doing to develop an effective, trusted and engaged IT function?

The most effective antidote to cybercrime and the associated risks of data breaches is having a high performing IT function with a truly peer relationship with every level of the organisation.

This will allow for the optimal design, development, implementation and ongoing management of information security measures that make sense for the organisation.

But the reality is that there are two underlying organisational factors that play an important part in limiting the potential effectiveness of IT departments:

1. the mythology of IT-business alignment
2. the relatively low levels of digital literacy at the Board level

So let's explore these in more detail.

1. The mythology of IT-business alignment

A recent worldwide survey of more than 2,300 executives asked how they approach the development of a corporate (not IT) strategy.

The survey found that just 19% said their companies "have a distinct process for developing corporate strategy". More importantly nearly a quarter thought their companies "should engage in corporate strategy development on an ongoing basis (as opposed to episodically), compared with only 8% who say they currently do".

Therein lies the challenge for IT departments. If organisations have an illdefined, outdated or poorly articulated business strategy, then the idea of developing a secure, high value, resilient and adaptive enterprise IT capability is nirvana.

It would be like asking a builder to build the foundation of a building when the architect cannot clearly define the structure and shape of the building.

2. Board level digital literacy

Many Boards of non-IT organisations have low levels of digital literacy, a fact not lost on the Australian Institute of Company Directors.

Digitally illiterate directors are easy prey for technology evangelists and vendors who may promote a technology solution or approach – but one that may not be the right one for the organisation.

The analogy here is like having a bank without any of the board members having any substantial banking and finance experience.

It takes two to tango

Change is inevitable – and that will arise on both sides of the business/IT department fence.

It's time that appropriately skilled and structured, business relevant IT departments are brought in from the cold and allowed to make a real contribution to the organisation's goals and objectives with known value, known cost and known risk.

If not, chances are their competitors are already well down this path.

This story is published courtesy of The Conversation (under Creative Commons-Attribution/No derivatives).

Provided by The Conversation

Citation: What's your IT department's role in preventing a data breach? (2014, May 21) retrieved 23 April 2024 from https://phys.org/news/2014-05-department-role-breach.html