Tackling cyber risks

How can charities address the emerging area of cyber risks? *Charity Finance* convened a panel of interested parties, with Ian Allsop monitoring their responses.

TECHNOLOGY HAS dramatically changed the way charities operate in positive ways, both in terms of delivering on their objectives and in how they are run on a day-to-day basis. But one of the unfortunate downsides is that, as fast as new solutions are developed, risks associated with using them also emerge.

Security measures can quickly become obsolete, and both individuals and organisations have to constantly be on their toes to try and stay one step ahead. For charities the risks are both financial and reputational. For example, the British Pregnancy Advice Service recently endured adverse headlines after being fined for a data breach.

But what are the major barriers for charities when tackling cyber risks, how far can these risks be mitigated through insurance, and who in an organisation should take responsibility for managing this area?

The emergence of cyber risk as an area of concern for charities when reviewing their insurance provision was highlighted in *Charity Finance's* 2015 Insurance Survey, published in March. One charity said that new technology brings changes to its risk profile on a regular basis. Yet very few charities have arranged specific insurance against these risks – possibly because many are not completely aware of what the risks actually are, and because as a relatively new insurance area, premiums can be expensive.

> "Insurance solutions are now being developed for cyber risks"

Liam Greene, professional and management risk underwriting manager, and cyber specialist, at Markel UK, emphasised that cyber risks are an emerging threat, but insurance solutions are being developed for them.

Cyber liability insurance cover has been available in the market for around 15 years, and has been most successfully used as a risk transfer option in countries that have mandatory data breach notification laws – for example, in most states of the US. "It can be a tricky area to understand, and is a changing landscape. Cyber risks are attached to a number of employee issues, including home-working, social media and staff sharing increasing amounts of data. You can't ignore it – you have to react," said Greene.

Share points

In the UK, the impending EU Data Protection Regulation includes mandatory notification of data breaches, but the scale and timing of this new regulation is still to be determined. The impression remains that many charities think it won't happen to them. Therefore, if people are able to share information about any attacks they suffer to make others aware of the problem, it can be helpful – notwithstanding the balance that has to be struck with upholding reputational integrity.

Neville Kyrke-Smith is director of Aid to the Church in Need, which was one of the few charities to have spoken up and admitted an IT security breach, after its website was hacked.

Despite the obvious risk of doing so, Kyrke-Smith felt that it was an important thing to do and thinks the sector would be better off if more charities were as open. "Understandably people are scared of speaking out. They don't want to be under the spotlight.

"However, these things can be a wake-up call that you need to get the board involved. Trustees don't always take it seriously as they are not interested in IT and it is below their radar. We need greater board engagement, certainly at the small and medium level," he said.

Originally from a finance background, Paul Butterworth

Paul Butterworth, head of IT governance and performance, Cancer Research UK and Mindy Kilby, director of finance, Royal Opera House.

is head of IT governance and performance at Cancer Research UK, where part of his brief is responsibility for IT security. He agreed that getting trustee engagement was an important issue.

"At CRUK, IT security is taken very seriously at board level. We have a data security programme so there is definite interest there," he said.

Butterworth also called for an honest conversation about resource. "It is always a challenge for charities to justify any spend. They always have to ask whether donors would be happy. Smaller charities especially need expertise, but can they justify the cost?

"IT security isn't visible so, if it doesn't go wrong, you don't see it. Therefore it is harder to make the investment case. Trustees want to do the right thing but it is a real challenge," he said.

Mindy Kilby, director of finance at the Royal Opera House, said it was also a case of getting staff buy-in to the real issues: "How do you take something that seems so distant and make it their responsibility? Yes, you can take out cyber liability cover but often it is too late at that stage. You need to ask what steps exactly you can take before that?"

Responsible roles

So where in a charity should responsibility for cyber risks sit? Finance? Legal compliance? IT?

In smaller charities the problem can be that no one has responsibility for it, or responsibility is only figured out when things go wrong. Kyrke-Smith asked: "Why is it traditionally a finance issue?"

Panellists agreed that it perhaps did not matter as long as there was a clear definition of responsibility. Often what may happen is that it just merges into someone's job description over time. Kilby argued: "It can fall under one executive's job description but everyone needs to take responsibility, certainly among the senior management."

Neville Kyrke-Smith, director, Aid to the Church in Need and Liam Greene, professional and management risk underwriting manager, Markel UK. Photos: Yolanda Chiaramello.

> "IT security isn't visible, so it's harder to make the investment case"

Butterworth said that one of the problems and challenges is that people are confused about what cyber risks actually are, which can make delegating responsibility difficult. "Some charities are only able to have short IT updates at trustee meetings so there is not enough time to explore what their cyber risks are. For non-IT people too much detail will make them glaze over and move on."

Risky areas

Greene commented on how the areas of cyber risk have changed. "Historically it was viruses and website hacking, but now it is more about data security," he said. "Credit card companies have responded to tackling fraud in recent years. Now, there has been a shift towards healthcare and other personal data. Building a profile is easier with this. This is a particular concern for the care sector and the potential access to sensitive patient data," Greene warned.

Butterworth said that charities should ask: "What are our information assets? What are their value? It is not only credit card details but email credentials that have a value on the black market. Charities might not think they are a target but they have supporter data. Therefore it is really important that all charities recognise that they have data that is of value to criminals."

He outlined a number of ways in which charities could be targeted: "Employees can be seen as the weak point in an organisation and are often targeted to bypass organisational security, for example in phishing attacks. Then there is the risk of 'hacktivists', especially for campaigning charities. Or there are people who are simply opportunists and spot a weakness.

"Once you have been breached it is important to investigate the reasons properly as much as just closing down gaps," he said.

Greene agreed, but noted that IT forensics is a suppliers' market, and therefore expensive.

Kyrke-Smith emphasised how important it was to understand all of the risks. "An IT security breach is not just an inconvenience,

or the cause of some website downtime. It can mean full business interruption. Charities need to appreciate the full impact of things going wrong," he said.

He also observed how smaller charities are often targeted as they are seen as a soft touch: "Some organisations have taken on new personnel who have spotted opportunities to breach their own security structures. You need to have a degree of trust but also constantly review. It is easier to blame outsiders but you often need to look inside."

So with limited budgets how can charities prioritise cyber risks? Are they moving up the risk register?

Kilby said that she preferred to see it as part of overall operational risk. "There is a worry about whether the cyber risks have a high enough profile on your risk register. But, if you moved those risks higher up, you're then forced to look at moving another risk down the risk register," she observed.

Doing the basics

Butterworth mentioned Cyber Essentials, a government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks.These include self-assessment questions around basic potential problem areas, including robust password protocols and closing down inactive accounts. Organisations can be audited and accredited as part of the assurance framework.

Greene pointed out that accreditation is now a condition of some government contracts. Indeed, from 1 October 2014, the government requires all suppliers bidding for certain sensitive and personal-information-handling contracts to be certified against the Cyber Essentials scheme.

Ensuring peace of mind

Kilby said insurance was often a response to trying to make sure you are doing everything you can. "If something happened, you would hate to think afterwards that you could have had cover in place, and failed to do so," she said.

Greene cited the analogy of how just because people have burglar alarms it does not mean they do not have buildings insurance cover.

> "Employees are often targeted, to bypass organisational security"

Butterworth agreed that the combination is important. "Insurance is never a catch-all and isn't meant to be. You need to take sensible precautions along with insurance. You need to think and answer the questions at different levels. You need to get buy-in at senior management team and board levels about risk, but with other employees and volunteers it is about day-to-day awareness. Why people don't think the same at work about passwords as on their personal accounts is an interesting issue," he commented.

The panellists then pondered how charities dealt with cyber risks around third-party suppliers.

Butterworth said that like any supplier relationship it is about asking the right questions: "What are their credentials? Is the lower-cost provider robust? It is increasingly a part of procurement to do rigorous due-diligence on suppliers. It is important but can be a point of friction. For example, with fundraising third-parties. Do they have the infrastructure to deal with controlling data protection adequately? IT security can be seen as a blocker in the process. It is a balance between governance and assurance, and moving forward and raising money for the cause."

As with any insurance, there can be a perception that you may spend a fortune on premiums but exclusions then render the policy worthless but, as Greene pointed out, good insurers will uphold a responsibility to not have too many exclusions, while brokers need to make things clear in the language used.

Opportunity to build trust

Greene mused about how cyber risks could be an opportunity for charities to enhance trust by being open when they did experience problems.

Butterworth said: "Charities need to come together and share their experiences, and recognise that positive reputation is an asset. More than any other sector, charities are able to learn from each other."

In summary, panellists agreed that the risk of data loss was increasingly important to recognise, but to tackle it you first need to engage people, and then implement systems. It should be regarded as part of overall operational risk. And it is important for people to realise that, while an evolving challenge, it is not impossible to deal with.

There is always a starting point and little steps that can be taken. ■

With thanks to Markel UK for their support with this feature.

***Ian Allsop is a freelance editor and journalist, and regular contributor to* Charity Finance**