A recent discussion hosted by EY for nearly 250 finance professionals, outlined that organisations and their boards expect an increased level of threat and therefore an increased proportional spend on their cybersecurity defences. Companies are becoming more sensitive to the reality that how they respond to these threats does not solely affect their revenues, but also their corporate brand and market reputation.

The event, entitled ‘protecting your corporate brand’, included EY speakers Richard Brown, IT Risk and Assurance Partner, and Mark Brown, Executive Director in the Cybersecurity & Resilience practice.
Business today is critically dependent on technology. Digital systems are now the lifeblood of companies, creating new links with customers and suppliers, but they also have the potential to bring about a company’s demise.

Given the mission-critical nature of data in nearly every aspect of a modern enterprise, organisations are facing not simply an escalating risk, but the near-certainty that they will suffer a cybersecurity breach.

**Threat awareness**

Based on feedback from over 1,800 clients in EY’s 2014 Global Information Security Survey, both the volume and sophistication of cyber-attacks has increased over the last year. Many entities have to work harder to protect themselves. Awareness of incidents is also increasing – including within finance teams.

**Constantly evolving threats**

Cybersecurity threats are evolving rapidly. They do not always take the form of highly public ‘big bang’ attacks. They may also have a ‘malarial’ effect, being hidden in systems for months or years, slowly eroding competitiveness and business value over time.

In 2010, the Government’s National Security Strategy, identified cybersecurity as a UK tier one threat highlighting its significance to the UK’s intellectual property.

Mark Brown, Executive Director in EY’s Cybersecurity & Resilience practice outlines: “Organisations cannot make themselves 100% secure all of the time. The nature of the threat is no longer stemming from opportunistic teenage hackers experimenting in their bedrooms. Attackers today are sophisticated, planning attacks for monetary gain by accessing millions of pounds worth of corporate know how. Individual attackers now operate at the same level only recently achievable by state-sponsored attacks. Today’s attackers are patient, persistent and target not only technology, but increasingly people and processes.”

As a result, businesses are posing themselves a different kind of question. Rather than asking ‘are we secure?’ they are seeking to identify ‘what it is’ they need to protect, then asking whether it is ‘secure enough?’

In doing so, they may find that digital security solutions offered by IT departments have become misaligned with organisational priorities. Security has become synonymous with compliance and response frameworks have been too focused on technology and bolt-on upgrades. Lines of accountability may be unclear, particularly in terms of who is responsible for a response to a breach. Boardrooms increasingly recognise this isn’t just a matter for technologists, but for them too.

Data analytics provides the opportunity for organisations to analyse all the data they have around security incidents to try to understand not just what has happened in the past, but to start to identify what may happen in future. Trends may emerge, but managing security across geographies is highly complex, not least due to different regulations that create inconsistencies in organisational approaches. It is vital therefore that organisations view cybersecurity not as a compliance topic, but address it at enterprise risk level.
Cybersecurity: poll results

250 finance professionals

How many Cybersecurity incidents have occurred in your organisation within the past 12 months?

- 45% 1-10
- 38% None (that I am aware of)
- 15% >25
- 2% 10-25

In 2014/15 will your organisation:

- 79% Expect an increased level of threat and therefore increase proportional spend on cybersecurity defences
- 21% Anticipate a reduced/status quo level of threat and therefore maintain spend or reduce current investment on cybersecurity defences

Have you heard or read any of the following?

- 25% Payment Card Industry Data Security Standard
- 21% Cybersecurity for Business – 10 Steps to Cybersecurity
- 19% EU General Data Privacy Regulations
- 18% ICAEW Audit Insights – Cybersecurity
- 10% Cybersecurity Essentials
- 7% EU Network Information Security Directive

Where do you see the biggest threat to your organisational cybersecurity emanating from?

- 28% External hackers
- 23% Technical system vulnerability
- 21% Employees (Insider threat)
- 14% Technology failure
- 8% Uncontrollable risk events (“Black Swans”)
- 6% Supply chain
Balancing cost, risk and value

Throwing more resources at the problem isn’t always the answer. Company chequebooks should not be opened until the organisation has prioritised what it is aiming to achieve. This is about balancing cost, risk and value.

Richard Brown, Partner in EY’s IT Risk & Assurance practice explains: “The first step is to understand the business risks associated with the cyber threat. IT exists to enable the organisation – not as an end in itself. Once organisations have identified the business risks that are causing concern, then they can target their security investment appropriately. There is also a cost-benefit discussion to be held – achieving maximum security may require a disproportionate spend.”

Richard continues: “Finance professionals have an important role to play here in educating security and IT functions about the benefits of risk. Risk can be good for business – it’s how companies make a profit. Finance can question IT and security departments about what they are trying to protect and why. Finance can explain that IT and security should be an enabler, not a constraint on business, and that some degree of risk is acceptable – even necessary. Finance can also encourage organisations to review their security policies to ensure they form a simple set of guidelines that employees are made aware of and understand.

Insuring against cyber risk

Companies are increasingly looking to insurers for protection against financial losses in the face of cyber-attacks. In the UK however, the cyber risk insurance market is immature – perhaps a decade behind the US market. Insurers in London are responding to an emerging demand, although organisations are finding it difficult to buy insurance at an economic rate.

Insurers suggest that the finance community needs to be clear about exactly what it is insuring. Is it seeking cover for loss of assets as a result of a cyber-attack, or for the cost of remediation efforts? Is protection sought for loss of generic brand value? Organisations often fail to forecast accurately the levels of indemnity coverage required. Cyber risks may be addressed by existing insurance cover, so organisations should start by understanding the protection they already have.

Richard adds: “Organisations also need to be able to explain the actions they are taking to defend themselves from cyber-attacks. Insurers need to know they won’t be insuring the equivalent of a house with an open door. It will never be possible to buy a blanket cover for cyber risks – organisations have to demonstrate they are being prudent and careful. Just as you should never outsource a problem, neither should you insure one.”

A raft of EU regulation

Various UK and EU bodies have issued or are drafting guidance and regulation on cybersecurity and privacy. Awareness of such developments in the finance community is relatively low. The EU Network Information Security (NIS) Directive, part of a wider EU cybersecurity strategy, broadly requires member states to have a cybersecurity strategy in place and involves some information sharing and cooperation. It will also introduce mandatory breach disclosure for specific sectors.

Only 7% of polled finance professionals were aware of the EU NIS Directive
More news headlines will be triggered by companies being forced to openly disclose to their customers that they have suffered a cyber breach, causing potential loss of trading revenues through brand and reputational damage. Another issue is that the directive is aimed at critical national infrastructure, but there is no common definition of what this is. There is some uncertainty about exactly which organisations and sectors fall into its scope. Legislation implementing the directive is due to come into force in 2017.

The EU General Data Protection Regulation (GDPR) poses significant challenges for business. In particular, it changes the power to consumers via the ‘right to be forgotten’ and introduces significant penalties for loss of data. The European Parliament, for example, has a penalty target of 5% of turnover, which will be discussed at a trilogue with the European Commission and Council. The regulations are scheduled to be agreed in 2016, with a two-year implementation period to follow, meaning they could enter UK law in 2018.

Richard Brown, Partner in EY’s IT Risk & Assurance practice outlines: “From a cybersecurity perspective, the EU GDPR will increase consumer awareness around the rights of their own data and put pressure on businesses to take more action around data capture and privacy, as well as security.”

Turning to frameworks and guidance, HM Government’s Cyber Essentials Scheme, launched in June 2014, provides a set of basic controls to help all organisations protect themselves against the most common cyber threats. Its assurance framework offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

In addition, HM Government’s 10 Steps to Cybersecurity (updated version launched in January 2015) takes a holistic approach to security. It identifies practical steps that organisations can take to improve the security and information of their networks.

The ICAEW’s document, Audit Insights Cybersecurity, captures the experiences of external audit experts from large and medium-sized audit firms. It also includes a number of recommended actions for boards.

Where does the threat come from?

One of the challenges in cybersecurity is that the threat to an organisation can come from multiple sources and causes. Employees may at times be the weakest link in an organisation’s defences – despite training and awareness campaigns.

Mark Brown, Executive Director in EY’s Cybersecurity & Resilience practice comments: “The threat posed by the supply chain shouldn’t be ignored – even though it lies beyond the boundaries of an organisation’s direct area of control. Organisations need to consider whether contractors and suppliers have access to data assets, what those assets are and how suppliers and contractors can demonstrate their ability to protect those assets.”

Businesses are now deploying more dynamic organisational security and may seek to pass sound foundations of cybersecurity (e.g., through their participation in the Cyber Essentials Scheme) down their business value chain. They are looking to review their supply chain and technology strategy to understand the agreed security limit, the variable factors (e.g., social media) and those outside their organisational control (e.g., government regulations or world events).
Cybersecurity: balancing risks and controls  Protecting your corporate brand

Passing cybersecurity standards down the value chain may initially be viewed as a necessary ‘hygiene’ factor. However, it then becomes seen as beneficial by companies as they realise the important role certain suppliers play in their business value chain. Supply chain risk is not just determined by the value of spend on services. In fact, suppliers critical to the business can be small in terms of their cost, so analysis of where the business truly needs resilience cannot be based simply on spend. Production and release of year-end results, for example, could involve a range of suppliers for legal, PR and printing support. These may well not be large, sophisticated businesses with advanced security systems and processes.

Built-in bolt vs bolt-on security

“In terms of cybersecurity system maturity, organisations can be divided into three groups”, Mark Brown, Executive Director in EY’s Cybersecurity & Resilience practice adds. “Some (perhaps 60% of companies) are still at the ‘Activate’ stage – the foundation level, focused on protecting the business as it is today. They still need to take some basic necessary measures and are tackling the cybersecurity challenge through buying solutions and bolting them on”.

Mark explains: “Increasingly, however, companies are seeing the weaknesses of such an approach and are moving into an ‘Adapt’ stage. These organisations realise that the return on investment from a bolt-on response is inadequate and are moving to built-in security. They appreciate that change in the business has change implications for cybersecurity and want to focus on protecting the business of tomorrow”.

“Even more advanced is the ‘Anticipate’ stage – an emerging level of cybersecurity. This approach is about using cyber threat intelligence to identify potential hacks and taking action before any damage is done. It involves a full move to built-in security,” Mark outlines.

Realism and response

As a final thought, organisations and their boardrooms need to understand that preventing a cyber-attack or breach is almost certainly impossible. Whilst taking steps to prevent a breach is important, it is not sufficient. Organisations need to develop a holistic approach to cybersecurity, which includes responding effectively to any breach. Crisis management plans need to be developed, involving technologists and the boardroom. How effectively the business responds can have a substantial impact not only on any immediate financial loss, but also on corporate reputation and brand.

For more information, please contact:

Richard Brown
Partner,
IT Risk & Assurance, EY
Email: rbrown@uk.ey.com
Tel: + 44 20 7951 4090

Mark Brown
Executive Director,
Cybersecurity & Resilience, EY
Email: mbrown1@uk.ey.com
Tel: + 44 20 7951 7519
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.
© 2015 Ernst & Young LLP. Published in the UK.
All Rights Reserved.
ED None

In line with EY’s commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk