The CFO checklist to stop cyber attacks

The threat of cyber attacks is growing. Corporate victims of attack know the experience can be costly and damaging. HUGH CALLAGHAN director at EY writes on the role the chief financial officer can play to prevent an attack or to minimise any damage caused.

In November of 2013 EY launched its 16th Global Information Security Survey report entitled *Under Cyber Attack*, which polled over 1900 client organisations across 64 countries. This was followed up a month later with a short companion guide, intended for the CFO outlining why cyber security is without doubt one of the fastest rising issues for executive management and company boards alike.

The CFO has a long list of critical functions to oversee including; profitability, cost analysis, financial reporting and evolving regulatory compliance. Therefore, cyber attacks are likely an unwelcome addition to the list, but belong on the agenda of those accountable for managing the financial risks of a business.

So why exactly should the CFO be concerned about cyber attacks?

The risks associated with this are too big to ignore due to the increasing amount of money that they cost businesses – both in terms of the direct cost of dealing with incidents as well as the brand and shareholder value that can be lost in a breach.

Indeed over recent years, more and more companies have faced severe financial and reputational costs as well as adverse regulatory attention from highly public data breaches. Research conducted by the Ponemon Institute shows the cost of cyber crime rising for the fourth consecutive year, with an annualised cost of $11.6M for the 60 US-based organisations benchmarked, ranging from $1.3M to $58M. The average cost of resolving a single successful cyber attack exceeded $1M, with cyber crime costing smaller organisations almost 5 times more per capita than larger organisations.

Our recent *Global Information Security Survey* shows that external threats rose for 59 per cent of organisations and actual incidents rose for 31 per cent, so the trend of rising cost is likely to continue. Governments and regulators have been taking up the issue due to the drag created by cyber attacks and cyber crime at a macroeconomic level.

The US Securities and Exchange Commission published guidance in late 2011 on cyber security disclosures, which was a strong sign that security is seen as one of the factors used by the market to judge a company's value. Other regulators have also taken steps to outline specific expectations, such as BaFIN's banking supervision expectations for IT security published in late 2013.


Hugh Callaghan

Some regulators have gone even further. For example, in November 2013, the Bank of England, the Treasury and Financial Conduct Authority oversaw *Walking Shark 2* - measuring the City's level of readiness in handling major cyber-attacks on the UK banking organisation. An unprecedented step in 2013 saw the UK government's Department for Business Innovation and Skills (BIS) prompting the auditors of the FTSE 350 companies to interview top executives and board members on cyber security as a part of the statutory financial audit, which is likely to be a model for other countries in future.

Last year's World Economic Forum in Davos clearly demonstrated EU-level thinking to complement the draft EU cyber security strategy, with EU Commissioner and Vice President Neelie Kroes stating: '…cybersecurity is a matter that cannot be left to the technical people. It is a matter for board levels...The big opportunities of the digital economy will not be realised if people are worried about security and do not trust networks and systems.'

In the same speech, Commissioner Kroes made a reference to regulating for this rather than allowing companies to implement strong security on a voluntarily basis: 'Cybersecurity is too important to be left to the goodwill of companies.'

The combination of rising regulatory focus, the increasing threat to business and heightened governance expectations mean that cyber security is now firmly a board-level issue and a top concern for the CFO. Assuming that IT security and risk functions have the task in hand and dealing with any incidents is no longer a viable strategy, since the likelihood of a cyber attack has risen to the extent that it is a question of when, not if, an organisation will experience an issue.

A company can protect itself from cyber attacks by having a clear understanding of the risks, a security strategy that is formally aligned to the business and IT strategies, and a structured information security programme. In particular, finance leaders should play a lead role in:

- Winning top-level commitment from senior managers and the board, for investing in security - protecting what matters most and adds value to the business.
- Integrating security risks with core risk management activities rather than standing alone as a separate discipline, including articulating a clear risk appetite with relation to information security that is consistent with the overall organisation's risk appetite.
- Evaluating and making investment choices is a core competence and the CFO can bring structure and business disciplines to investments in information security, such as challenging rationale, measuring benefits and tracking cost. Our survey shows that organisations are generally willing to spend on security improvements, with 43 per cent of global respondents increasing their security budgets. However, that investment may fall short or wide of the mark compared to the business needs as 65 per cent of respondents still indicated budget constraints as the biggest obstacle to delivering value.
- Establishing information security governance frameworks and processes based on formalised governance structures, which the CFO can help shape. This includes a clear charter for information security and an operating model that keeps it aligned to the business through strong relationship structures with major stakeholders.
- Measuring information security performance by identifying the right criteria and tracking progress towards meeting those objectives. The CFO can also help to set the right incentives across the business to encourage timely remediation of security issues and ensuring that information forms part of employees' overall performance assessments.

Hugh Callaghan is director in financial services advisory at EY.