Disruptive trends: Technology

Disruption on multiple fronts is putting audit committees on high alert

Audit Committee Institute part of KPMG Board Leadership Centre

Technological disruption continues to appear on the audit committee agenda. With many audit committees looking to ensure risk management and internal control systems are addressing the full range of existing and emerging risks, ensuring that the technological expertise on the committee is appropriate is an increasing challenge.

Cyber security risk

With cyberattacks on corporate networks and systems becoming more advanced, cyber security remains a major oversight concern for audit committees (and boards). Years ago, retail and financial services organisations were most at risk due to the processing of credit card data. Today, personal information is frequently targeted over credit card data, placing a much broader range of organisations at risk. The cyber security challenge can be broken into five more granular topics:

1. Data protection – Data protection, while clearly connected to cyber security, actually falls into a larger business security category, as data loss can occur in many ways. When considering data protection, audit committees often receive from management a list of security programs that are currently in place; however, the first step should really be making sure the right information has been identified and data sets clearly defined. This can be a challenge as what is considered relevant continues to change. Today, things like user names, passwords, awards program profiles and social media accounts are being targeted. Given that this list will continually evolve, audit committees should regularly confirm that the definition and protection of alternative data sets -beyond standard credit card information -is being carried out. To augment the information they have at hand, audit committees can also request relevant data directly from IT, for example, testing results, reviews of key data and hacking reports.

2. Social engineering – Social engineering is a broad term for any kind of psychological deception or exploitation of the "human factor" to gain access to information. Email phishing is one form, but attacks can be much more complex, employing phone calls, physical impersonation or any scenario that plays on the target's sympathy, fear, greed, etc. Proper oversight should involve social media acceptable use policies and organisational workflows detailing proper account usage.

3. Auditing of third-parties – Many organisations are relying more and more on third parties as part of their business model. The audit committee should ensure that management has considered and evaluated whether appropriate controls are in place to prevent misuse of any confidential customer information aggregated by third-party vendors. To be more certain that the organisation is not creating additional liabilities, third-party audits are becoming more common.

4. Cyber insurance – Cyber insurance addresses an organisation's liability when faced with cyber-based risks, such as a data breach or data destruction resulting in the loss of sensitive information. Organisations are beginning to purchase these types of policies, but there remains some confusion over exactly what is and isn't covered. The audit committee should have oversight over whether such policies appropriately address the organisation's significant financial exposures.

5. Remediation procedures – Too often, audit committees look at a cyber breach, ensure an established process is being followed, then move on. More and more, however, we see audit committees getting involved in post-mortem follow-up reviews, sometimes even going beyond the standard oversight role in order to understand what went wrong, ensure remediation compliance and probe for other areas of vulnerability to help combat future attacks.

Business model risk

When an organisation effectively implements an industry changing technological innovation, one major effect is that their competitors' business models -and possibly a business model that has been an industry standard -can be disrupted. Consider the effect ride sharing has had on the way the taxi industry has been operating for decades or how internet-based streaming services have changed the way television is purchased and consumed. Going forward, audit committees will need to pay greater attention to how, and which, disruptive technologies could potentially put the organisation's business model at risk

Technology project risk

Despite the impact of the current economy on some sectors, organisations continue to undertake IT and strategic transformation projects. This can be a concern if organisations lack proper IT experience on the board. Is significant expenditure being incurred on big transformation projects without the proper governance to protect or maximize the investment? At the same time, regulators are raising the bar in the area of IT risks and controls, signalling the fact that it's time for boards, and potentially audit committees, to address this as part of their risk portfolio.

D&A privacy risk

D&A is changing business significantly and the organisations that are best leveraging it are seeing dramatic

results. However, like all disruptive technologies there are corresponding risks, including increased privacy risk. Customers and other stakeholders entrust information to organisations for specific purposes, but those organisations may exploit that information in other ways using D&A. This creates significant privacy oversight challenges that boards and audit committees need to be aware of and address.

Putting the audit committee on high alert

Virtually no strategic conversation proceeds without someone citing the need to either be disruptive or to respond quickly to disruptive market and industry trends -trends that have typically been connected to technology in one way or another. We don't, however, generally think about the concept of disruption when talking about the audit committee, even when we're discussing its changing role and responsibilities.

However, the concept of disruption is broadening its meaning beyond its current association with the interaction between technology, business and market forces. It is being applied in other areas and to other, broader trends. One might talk, for example, about the disruptive impact of demographic or regulatory trends, rather than just technological ones. To that end, a high-level concept of disruption provides a valuable framework for discussing many of the changes and challenges currently facing the audit committee. And there are, without question, a range of audit trends (auditor rotation, reporting, D&A, etc.), that can only be seen as disruptive, given the kind of substantive change they are driving and their potential to transform the way audit committees do what they do -and what they are increasingly being asked to do.

Disruption can affect audit committees in different ways. In some cases -for example, cyber security -audit committees might need to become more knowledgeable and more vigilant in their oversight due to the rapid, ongoing evolution of the field. In other areas, such as oversight of reporting and compliance, it is their own approaches and processes that are changing, as complex standards up the regulatory ante.

Going forward, managing inevitable change will be both an audit committee priority and a challenge and one that all audit stakeholders -directors, management, auditors, regulators, shareholders and even the public -have an interest in facilitating.

For more information on ACI please contact:

Timothy Copnell
Chairman of the UK Audit Committee Institute
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk

www.kpmg.co.uk/aci