Bad for Business: The Need to Up-Skill the C-Suite on New Risks

Both government and industry agree that fraud, bribery and corruption are bad for business, encouraging unfair advantage and anti-competitive practices. Based on in-depth interviews with over 2,700 individuals, including chief financial officers ("CFO"), chief compliance officers ("CCO"), general counsel and heads of internal audit across 59 countries, EY's 13th Global Fraud Survey, ***Overcoming compliance fatigue: reinforcing the commitment to ethical growth,*** revealed concerning levels of perceived fraud, bribery and corruption across the world, with 48% of executives working in financial services indicating that bribery and corruption were widespread in their country.

With management struggling to respond to long-standing and emerging fraud risks, it is imperative that boards ensure that they have a C-suite in place that not only understand the varying threats to their business but also have the knowledge and resources to address the emerging external threats – such as cybercrime – that have the potential to cause significant reputational and financial damage.

Understand your risk universe

Boards and management need to regularly refresh their views of risk drivers for the business. New risks emerge from what the organisation does, from changes in the markets in which it operates and from developments in external threats. One of the most significant examples of these developing threats is cybercrime. Cyber attacks are now a fact of life for business, posing a dynamic, relentless menace for leading companies. The threat is growing, and our survey suggests executives may be naïve regarding the scale and severity of the threat posed to their business.

- Forty-nine percent of respondents globally say that cybercrime poses a fairly or very high risk to their organisation, compared to 65% of respondents working in financial services.
- CEOs view the risk as less significant than CCOs — 50% of CEOs view it as a high risk compared to 61% of CCOs.

Developing an effective response is more difficult without a proper understanding of the potential sources of attacks. 56% of financial services respondents were most concerned with the risks posed by hackers, potentially indicating that the nature of the threat may not be fully thought through.

Only 32% of financial services respondents recognised the potential threat posed by employees and contractors, which, whilst in line with the global average of 33% and UK average of 36%, may still signal the need for a greater awareness around the so-called “threat within”. Employees are often the vulnerable link within an organisation due to their susceptibility to phishing emails – where spoof emails are sent out in an attempt to gain password or confidential information, downloading viruses and transferring files to unauthorised personal devices – and, while these incidents often happen accidentally, they still serve as an Achilles Heel within organisational structures. Training and awareness of employees who may be vulnerable is imperative for organisations seeking to address these risks.

Who owns the risk?

Cyber risks manifest themselves in areas beyond the scope of the IT department. They affect employees, business systems and interactions between an organisation and its stakeholders — including regulators. Governance of the risks, therefore, needs to be built around several executives including the CEO, CFO, chief information officer (CIO), chief technology officer (CTO) and the general counsel. In the event of a breach, the general counsel’s role quickly increases in significance as managing the messaging for authorities and the content and timing of any disclosures are critical.

Clear up the grey areas

Insufficient awareness of potential risks will only heighten the C-suite’s difficulties. When asked what was acceptable to help a business survive, 32% of financial services respondents said they were willing to offer corporate entertainment in order to retain business, suggesting the need for further clarity on ethical business conduct guidelines. For a lot of organisations there is somewhat of a grey area when it comes to the definition of appropriate conduct when building relationships with clients and the onus is on organisations to communicate to their employees what is and is not acceptable business conduct. Boards need to ensure their companies have clear policies in place in order to protect themselves and their employees from

potential allegations of misconduct, for example in awarding a contract. Policies should be framed in consideration of:

- which employees could be at risk,
- when they are likely to be at risk; and
- what the company's tolerance is for these risks

Regulators are investing heavily to bolster their ability to mine big data from corporations for potential irregularities, and boards should be asking how management is leveraging forensic data analytics to get the most from their big data in order to improve compliance and investigative outcomes and raise red flags earlier and more efficiently.

The need to reinvigorate compliance

With more focus on driving revenues from less mature markets, the challenges for companies are getting more complex and regulators are working together across borders like never before to hold companies and their executives to account.

Despite this, respondents described a largely static internal compliance environment, with many companies continuing to miss opportunities to implement robust ABAC policies and risk assessments and conduct anti-corruption due diligence. Whilst financial services leading the way with the implementation of ABAC policies it is worth noting that

- ► 16% of businesses in Ireland still do not have an ABAC policy
- ► 49% of Irish organisations have not introduced a whistleblowing hotline
- ► Less than a third of businesses are conducting anti-corruption due diligence as part of their mergers and acquisitions process

Markets are never static. New risks constantly emerge, and the matters that regulators and the public consider inappropriate or fraudulent are evolving. In performing its oversight role, the board must challenge the business on whether the right compliance risks have been identified and are being effectively managed.

To meet the significant compliance risks facing businesses, management needs to recognise that policies and training are really only a starting point. Boards should be demanding that the

C-suite go beyond the basic building blocks to promote ethics within their organisations and intensify their efforts to challenge management to reinforce their commitment to ethical growth.

Julie Fenton leads the Fraud Investigation & Dispute Services practice at EY Ireland.

PANEL #1:
What does good look like?

Board engagement — boards need to appropriately challenge management and request regular updates regarding fraud, bribery and corruption risk.

Big data — mining big data using forensic data analytics tools can improve compliance and investigation outcomes and can help management provide useful summary information to the board.

Anti-corruption due diligence — such specialised due diligence should be the norm, not the exception.

Escalation procedures — companies should have clearly defined escalation procedures, whether to respond to a whistleblower or a cyber incident, to minimise the damage being done.

Training — companies should have tailored ABAC training programs; business unit leaders should be evaluated on participation levels, and C-suite executives need to lead from the front.

Budget support for internal audit and compliance functions — they play essential roles in both improving standards of business conduct and in keeping the company out of trouble.

PANEL #2:

Detecting and diagnosing a cyber threat

Cyber attacks probe defenses, searching for weaknesses.
An effective defense requires scrutiny of a company's entire IT platform using diagnostic testing. Diagnostic testing should encompass all networks, systems, logs and events and search for evidence of the four elements of a cyber attack:

1. **Entry** — to identify evidence of malware that provides the attacker with a digital "beachhead"
2. **Lateral movement** — identifying evidence of the extent to which an attack has spread across different parts of the network
3. **Harvesting** — identifying unusual activity or tools across accounts and data sources that indicate the unauthorised capture of information
4. **Exfiltration** — identifying efforts by the attacker to remove data