Is digital risk disclosure in need of an upgrade?

"...all companies are technology companies; most just do not realize it yet..."

Companies' reliance on technology, digital platforms, supply chains and data is growing. Reporting, therefore, needs to provide relevant information to investors and other stakeholders to assist them in assessing a company's ability to remain viable and resilient against the backdrop of digital security and strategy risk. Currently, it doesn't. An upgrade is needed.

By Andrew Hyland

Time for a system diagnostic

The FRC Lab's (the Lab) review of related disclosures identified that, while a significant proportion of companies had at least one digital-related risk among their principal risks (mainly cyber), the overall quality of resultant disclosure is not meeting investor needs and is often boilerplate and overly static. Discussions with investors highlighted four key reporting areas required to meet their needs: Strategy, Governance, Risk and Events.

Strategy – Establish how important digital security and strategy are to the company's current and future business model, strategy and environment.

Governance – Detail the governance structures, culture and processes the company has in place to support digital security and strategy.

Risk – Indicate the risks and opportunities connected to digital security and strategy that the company is facing both now and in the future.

Events – Highlight the impacts of events (internal and external) and the actions and activities which respond to these.

Cracking the code

While it is difficult to identify a list of disclosures that are always useful (every company is slightly different), the following highlights the key questions that investors want disclosure to cover:

- Strategy – Companies utilize and leverage digital technology and data differently. For some, it is fundamental to the execution of their business model and strategy. For others, it is just one part of the resources necessary to enable their strategy. Providing clarity on its relevance allows investors to assess the appropriateness of the linked processes, procedures and structures. Investors seek strategy disclosure that:
  - provides a context for digital security and strategy and its importance to a company's broader strategy, business model and ability to generate value;
  - indicates how external trends associated with digital security and strategy are integrated into the company's approach; and
  - links digital security and strategy disclosure to the company's broader strategy.
- Governance – Understanding risk is partly about understanding how the external environment impacts an organization and partly about how the organization manages and mitigates those risks. Business actions start with, and are driven by, the board, but what triggers their considerations and actions? Interviews with companies identified a number of drivers for board discussions, including; regulatory interest, strategic opportunities, employees, suppliers and wider considerations related to the S172 statement (in the UK) and ESG agenda. While company disclosures on governance often cover the "What", they neglect the "Why" and "How". Therefore, the opportunities for improving company disclosure are focused on a more integrated approach to digital security and strategy governance, which provides a clear connection to wider internal and external stakeholder context. Investors seek governance disclosure that:
  - links the governance of digital transformation and security risks to strategy and risk appetite;
  - shows how the board, and its committees, has oversight of these risks. This may also include who within the company has ownership of specific risks, and the access they have to senior leaders;
  - explains what a company has done to foster a digital security (or cybersecurity) culture and
  - outlines the relevant skills of the board and assurance obtained.

All stakeholders (including employees and third-party service providers) play a vital role in the mitigation of risk.

- Risk (and opportunities) – Digital security and strategy risks are cross-cutting risks. IT departments can, to an extent, mitigate many related risks, but risk management is ultimately owned by senior management and the board , who are responsible for ensuring that it is considered consistently and in the context of strategy. All stakeholders (including employees and third-party service providers) play a vital role in the mitigation of risk. Investors seek risk disclosure that:
  - links the digital security and strategy risks to strategic objectives and risk appetite;
  - considers the actions and activities taken to mitigate risk and how risks have evolved;
  - provides information about the risk and mitigations at the right level of granularity; and
  - connects digital security and strategy with disclosures on viability and resilience.
- Events – Companies face many internal and external factors that will impact their strategy, risk management and governance structures and processes. In addition to information about the action taken and events themselves, investors want to understand the effectiveness of a company's response and how lessons learned from the event will be, or have been, incorporated into changes to the relevant structures and processes.

DIGITAL SECURITY RISK DISCLOSURE REPORT

The full report from the Lab – Digital Security Risk Disclosure – is available free on the FRC website. The report provides more detail on each area and provides insights and examples from companies at the leading edge of disclosure:

https://bit.ly/3cbZvlD

Ctrl + Alt + improve

The Lab's review of digital security risk reporting identified that there is a need for more useful and fulsome disclosures around digital security and strategy risk.

Given the importance of these issues to investors, regulators and others (and their importance and contribution to building business resilience: https://bit.ly/3wmimRU), this is an area where regulation can provide real opportunities and which reporting teams, risk teams and audit committees should consider.

ANDREW HYLAND
is a Project Manager in the FRC's Lab. Andrew works to identify how external reporting can better meet stakeholder needs. He is a qualified accountant and has worked in technical accounting teams and as an academic.