There is more to cyber risk than security

By Riaan Bekker

20 Feb 2019

Risk experts hold no doubts: the changes technology is bringing to businesses has far-reaching consequences. But the conversation is still split between two poles, those of business and technology. It's more convenient and seems to simplify the issue. But that is not true.

Riaan Bekker is Force Solutions Manager at thryve

Just look at risk registers and predictions for 2019. Cyber risk has risen to the near top, often only competing with business continuity as the biggest concern. This is ahead of other risks that at face value have a clear connection to business operations.

Are we prepared for 2019's cyber security challenges?

Grant Hamilton 15 Jan 2019

A number of traditional risks now play second fiddle to cyber risk. Skill shortages, regulatory changes and global political uncertainty are all serious factors, yet cyber risk routinely appears above them.

Why is that? Cyber elements are now crucial to modern business practices. But misunderstandings about cyber leading to much more uncertainty.You cannot operate a business today without a smartphone. Nor can your employees, plus there is an indefatigable desire from customers for mobile services.

This concentration on mobile services alone shows how prominent cyber has become in business corridors. It’s hardly the only example. Hence why, despite attempts to downplay its significance, cyber risk nonetheless bubbles to the top. The elephant in the room that is becoming noticed because it’s taken up all the space.

So the time has come for companies to have a more sober and encompassing appreciation of cyber risk, starting with what cyber risk is:

> *“Cyber risk is often defined as a security topic, which can then be conveniently mandated to IT or technology leaders in a business. There has been progress in terms of boards and CEOs realising they should take closer responsibility for the risk, but that still often happens under the security assumption. The impact of cyber as a risk is much, much wider.”*

Cyber risks often arise due to the following factors:

- **Globalisation**: Cyber technologies have enabled businesses to reach much further afield than before, the most potent example being globalisation. But this creates a variety of risks, such as meeting regulatory demands in different jurisdictions.

- **Adoption of new technologies**: Technology is a two-edged sword. For example, employees being able to access company systems via their phone is a massive productivity boost, but also creates issues around security and device management, not to mention on- and off-boarding processes. Though new technologies get attention from the board and c-suite, their underlying complexities and impact on processes are still often brushed aside.

- **Mergers and acquisitions**: Bringing one company into the fold of another or creating business synergy between them are already fraught with challenges. Yet even those concerns often overlook the extreme complexity of merging very different business systems and technologies. In most cases, this is not addressed at all for the sake of expediency, creating untold cyber risks that could appear in the long run.

- **Outsourcing**: While outsourcing is a good way to save money, increasingly around technology it is done to mitigate skills shortages which itself is a risk. But outsourcing also doesn’t absolve a business from responsibilities around cyber currencies such as data. There is also the additional risk of an outsourcing partner not being secure and thus a target for cybercriminals.

- **Extension of third-party networks**: A huge benefit around digital technologies is the ability to integrate with third-party networks, such as supplier databases. This is providing great improvements around value chains. But it also risks exposing company data and interactions if not secured properly - not only technologically but through training and culture.

How can a business track these risks? They should identify the factors that cause them, then collate data from the different departments involved. For example, is HR satisfied that offboarding processes cover the risk of company data leaving on a former employee’s device?

Gathering that data would normally be very difficult, but modern service platforms such as Riskonnect have been built to address such specific needs. Risk is about measuring input and impact, then using that information to mitigate and

improve. Gathering that information is a lot simpler if you use GRC integration platforms. These let different employees and departments input metrics in the way they capture them.

The service then balances that information in formats that risk managers want to see. Since these are service platforms, they are very simple and cost-effective to deploy in a company, no matter the footprint. You can start small, focusing on acute areas, and expand as the service proves its worth.Cyber risk isn’t only about security. It’s a broadside on business operations and ambitions.

Traditional risk assessment approaches are not equipped to handle that and the conversation is often kept narrow and technology-focused. But by looking at the above factors, combined with an integrated GRC management platform, risk managers can define cyber risk in a much better way.

ABOUT RIAAN BEKKER

Force Solutions Manager at thryve

- There is more to cyber risk than security - 20 Feb 2019
- Prepare for 2019: Weaponise Risk - 6 Feb 2019
- #BizTrends2019: The year disintermediation is put to the test - 14 Jan 2019

View my profile and articles...