GRC:
Governance, Risk & Compliance, or Generating Real Capability!

How do we use GRC as a business enabler, and focus on the benefits it brings?

Whitepaper – May 2021

technology leaders club

The challenge: What is 'risk'?

Business is now digital. From day-to-day remote working to merging complex systems in an M&A, businesses cannot avoid the growing threat from cybercriminals. Regardless of the specific nature of one particular event, risk is never siloed, isolated, or unique to one platform. Therefore, every cyberthreat, irrespective of the industry or business it targets, poses a risk to the entire organization.

The concept of 'risk' is quite subjective, and the terms used about cybersecurity are far from standardised. What one CXO identifies as risk will likely sound different to the response of other CXOs. We suspect this is common in the C-suite and across an organisation and indeed, the whole of the business world.

There are also widely differing perceptions of 'risk'. Largely seen as a negative beast – a dragon that needs reining in – risk management is a discipline and profession of its own, and the language around it needs to be articulated in a way that businesses understand. There needs to be a softer, gentler approach that will foster an attitude of vigilance, rather than fear; a culture that permeates the whole of the organisation.

Understanding the problem

Currently, the C-suite is kept informed of cyberthreats and risks, but this doesn't necessarily mean they have a full understanding. One question that should always be considered when a security manager hears of an attack is: Could we be next? The perception of risk varies widely from person to person, function to function, and department to department, and it is critical that the behavioural economics at play are understood.

Organisation of feedback

As a result of countless threats, the way in which threat information is collected – and how easily it can be accessed – is critical to a robust response. Currently, many businesses hold huge swathes of data that are too abstract to be readily useful, coming in the form of piles of paper document reports. Rather than sift through these files, it is critical that businesses have a GRC tool that forms a 'central source of truth'.

Also of concern is that many of today's security functions are immature, simply recording threats as events without further investigation. Clearly, it is critical to gain a better understanding of these events, and bring about a wholesale change in the ethos of such processes.

Governance, Risk Management, and Compliance

Governance, Risk Management, and Compliance (GRC) can and must act as a central tool when it comes to cybersecurity, even bringing opportunities to leverage value to the table. It can serve both to protect your brand and differentiate your company in the marketplace. It can also offer value that is both emotional and rational, fostering a secure sense of confidence throughout the enterprise.

Yet, even good cybersecurity governance can lack a clear streamline. As with cybersecurity itself, GRC is a highly complex area: 'compliance' will refer to many specific pieces of legislation and these will vary – and occasionally even contradict each other – with operations conducted in different parts of the globe. Some immediate examples include FCA and ICO Regulations; ISO certifications, and Sarbanes–Oxley ('SOX') compliance. These each serve different taskmasters and all are mandatory. Governance is a discipline around control, and more education is needed, and cybersecurity needs to be articulated in a way that businesses understand. Breaking risks into different segments – tactical strategic level and operational level – is effective.

Culture within the company

C-suite

Firstly, the C-suite needs to be aware of the benefits of GRC and the opportunities it can bring. Cybersecurity is often conflated with cyberattacks, and is either discussed when there has been an event or treated as something that must 'go away'. A culture of communication is key – there has historically been a culture in which IT management communicates in a top-down way, focusing on weak links and not using language that can easily be understood, whether by the Board or employees. The perception of what risk is often may not resemble the reality of the risk – certain terminology can both raise concerns while also miss the key point being made.

CXOs are often asked about risk within their function. Turning this around can lead to a wholly more productive, healthier dynamic. So, don't ask about risks, ask about goals: let the driver be need over compliance; introduce policy, not paperwork. All goals, from emotional and personal, to those at a business level. Be holistic and make this about 'them' – it will get them thinking about the benefits and oil the communication wheels, replacing the suspicion that perhaps was there in the past. Being hacked is not something that 'just happens' – it should be viewed as a risk just as running out of supplies is a risk.

Healthy open lines of communication can help identify sticking points, and lead to productive talks around objectives and the solutions available through robust GRC. Understanding their place on the InfoSec Journey will also offer a window into their concerns and mindset. Remember that it is not worth trying to change a culture that is often ingrained over many decades.

"Just because I'm aware, it doesn't mean I care"[1]:

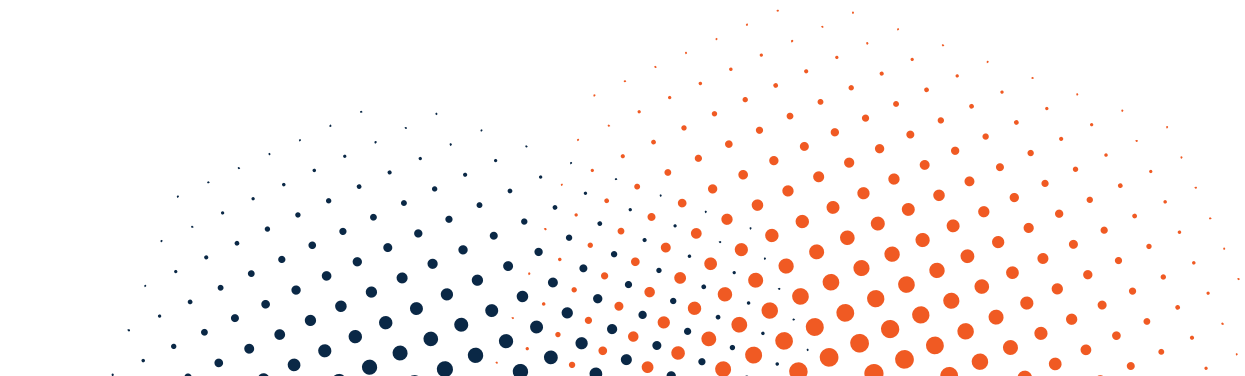
Everyday workers

A successful tactic can be to teach employees about protecting their own devices, fostering an attitude within a culture of awareness with which, once understood by the worker bee, can create an awareness of 'What threatens my device could threaten my work laptop.'

Conclusions

It is critical that the Board understand that GRC, when considered from both a cultural and technological point of view, can business enabler rather than an inhibitor:

- Focus on the culture of understanding and caring about risk – to build a foundation of attitude that makes dealing with risk easier
- It is reductive to think of risk in only negative terms – GRC can be effectively harnessed
- Risks will always exist, but they can and should be manageable
- Prefer using the carrot to the stick – discard the 'old-school' mentality of pushing something out to everyone, and prefer to educate kindly via a series of platforms tailored to different demographics
- Bring people together, equip them with the tools – it's a scaling challenge
- Let everybody join the conversation – there will always be one!



rela8 group