Security and the business: it's good to talk

Business and security leaders face big challenges if they don't build bridges together

Distinguished Analyst Paul Watts explores the shifting nature of business, the role of the security leader, and the implications of continuing to not align to each other's goals.

A (digitally transformed) life after the pandemic.

As recovery from the impact of the pandemic continues, digital transformation is dramatically changing how many organisations operate. Promises of innovation, efficiency and prosperity build pressure to transform as quickly as possible. However, uncontrolled and rapid transformation can increase both business risk and potential reward. Security and business leaders have become disengaged at a critical time. Change is urgently required on both sides to establish working relationships that ensure digital transformation risk is properly owned and managed. In this article, we will explore the reasons why disengagement has occurred, the implications of doing nothing, and the critical first steps to take in rebuilding those relationships.

The business relationship hits a rocky patch (or: "It's not me, is it you?")

"I just can't hold [the board's] interest" bemoaned a well-respected and long-standing Chief Information Security Officer (CISO) at a recent gathering of security leaders in London. Suggesting that perhaps it is because the business isn't finding it interesting or useful to them produces an interesting reaction: the CISO is not the problem; the problem is that business thinks it knows best and doesn't want the CISO's help.

I think there is a bit of denial here. The reality of the situation is that the problem is not one of interest, but one of relevance.

Technology in business has had an image problem for years. Expensive, difficult to understand and use. Hostile. Intimidating. But where technology was once a luxury that merely supported the business, it has now become the business. Teams created to manage technology on the business' behalf, partnered with security staff to ensure that it all remained safe. The business cared little about how it all worked and happily left them to get on with it, only engaging when they needed something, or something broke. And for many years, this was enough.

> *"… the reality of the situation is that the problem is not one of interest, but one of **relevance**. "*

Technology consumers now feel empowered. But the knowledge gap lingers on. As does the risk.

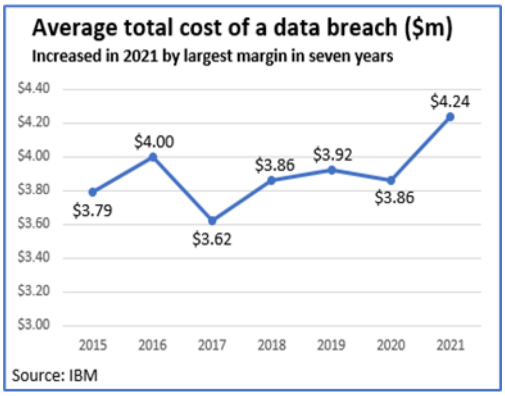
Technology has matured. Innovations have demystified it, made it easy to use and empowered their consumers. The dependencies on technology and security teams to keep things running are perceived to have vanished.

Here lies the metaphorical ticking time-bomb.

Modern, accessible technology introduces uncontrolled risk to businesses if implemented rapidly without any due diligence. Much like giving a small child a power tool and walking away, the outcome is likely to be a dangerous one without support and oversight. The same is true of business risk. The technology will either fail the business or, worse, could be exploited by criminals. Such exploitation cost global industry an average of $4.24m per data breach in 2021, according to research by IBM.

The security industry tells itself it must “move at the speed of business”. The business’ perception of security is the complete opposite. To them, security adds friction, like a motorist trying to drive their car with the handbrake still on. Legal and regulatory landscapes that govern the use of technology and data have adapted. Regulations are not negotiable, and they make the relationship with security teams more challenging, even revered: if the ‘security guy’ is in the room, it means bureaucracy and delay. The solution? Just don’t tell security what the business is doing.

There is a language barrier between business, technology and security. It is a long-standing problem. Technology and security staff struggle to speak the language of business, and most don’t bother to try – much like a stereotypical British tourist shouting in English at a bemused foreign restauranteur. Non-technical staff do not understand technical jargon and become frustrated and intimidated by it. This alienates both parties to the point that it is easier to avoid interaction.



Source: IBM

At a time when technology and security leaders need to be working more closely with the business than ever before, and with digital transformation showing no signs of slowing down, all this presents a real challenge. The tragedy is that that technology and security teams are very much alive and well. However, they remain forgotten by the business – at least until the business is in trouble and they are forced to pick up the pieces while business leaders stomp their feet and throw tantrums, conveniently blaming the very people who could have helped prevent trouble in the first place.

Engage earlier to shift-left.

Prevention is better than cure. The earlier a potential risk or issue is detected the easier it is to fix, and the likelihood of something bad happening reduces significantly. This proactive concept, known as ‘shift-left thinking’, is possible if business and technology teams are working together. If they are not, a reactive rather than proactive relationship exists; more fire-fighter than fire-preventer.

> *“Security leaders should know their stakeholders and learn their business. “*

Addressing this challenge requires a simple application of stakeholder management 101. Security leaders should take time to know their stakeholders and learn their business. They should be curious, ask questions, take an interest in what the business does, and in doing so make the conversation about the business – and determining the part they should play.

Gone are the days of behaving like a regulator, hiding behind rules and regulations; this is a redundant approach to managing security in modern business. Rather than saying “you must do it this way”, or “you cannot do it that way”, the language should reverse; “yes, and …” conversations do tend to strike a more conciliatory and engaging tone. The best question for a security leader to ask their business is simply this: “how can I help you to succeed?”.

Without a business, there is no need for technology or security. Nobody wins if everyone operates in silos. Security leaders have worked like this for many years. However, now is the time for them to get out of the information technology basement, appreciate the challenges of the ‘real’ business world, and demonstrate real value.

Change is a two-way street.

It is easy for business leaders to place all the burden on the security leader to change. However, they may not want to be so hasty.

In 2002 US Congress introduced the Sarbanes-Oxley Act, providing safeguards for investors against unscrupulous boards hiding behind financial misreporting. Many boardrooms were lacking credible financial skills, and the Act moved to change this, demanding proof of their ability to understand their financial data. The board's skillset had to adapt, as did their relationships with finance.

History may be about to repeat itself. The US Securities and Exchange Commission (SEC)'s attempts to require public companies to disclose their boardroom's understanding of cyber security will go some way to prevent denial of their responsibilities for it. Most experts believe this could cause a similar change to that seen in 2002. As former IBM executive and company director, Rodney Adkins, recently noted, the boardroom can no longer operate in a world of plausible deniability through their lack of skills: "Boardroom skills need to reflect the patterns of the marketplace."

> *"Boardroom skills need to reflect the patterns of the marketplace. "*

This could present an opportunity for both security leader and board member. Boards will become motivated to work with security leaders to understand and manage security and risk. Proactive, shift-left thinking between business and security teams will be encouraged. The management of risk will finally be acknowledged as a shared responsibility.

Without changing their approach to managing security and risk in business to be more engaging and business-orientated, security leaders could find themselves on the endangered species list. Business leaders similarly need to appreciate that security is everybody's responsibility, and that they cannot hide behind ignorance. If both sides make the effort, this could be the beginning of a beautiful relationship that benefits everybody. It just needs someone to make that first move, and the security leader is well-positioned to hold their hand out first.

Paul Watts is a former CISO, a NED, and a Distinguished Analyst at the Information Security Forum.

Paul Watts - Information Security Forum

Paul.watts@securityforum.org