A global study

Risk & Reward:

Reconciling the conflicted views of business leaders on the value of cybersecurity

March 2023
Trend Micro

Introduction

These are challenging times to run a business. High inflation, surging energy prices and rising interest rates in much of the world are taking their toll on many enterprises, their partners and their customers. Annual growth in advanced economies is predicted to be just 1.2% in 2023. In some cases, it will fall even lower than that. At the same time, the jobs market remains extremely tight, with unemployment at near-record lows in many rich countries.

It is the job of business leaders to navigate these choppy waters – managing talent acquisition and retention, keeping costs under control and finding areas to prioritise for sustainable growth. But what role do they see for cybersecurity in this?

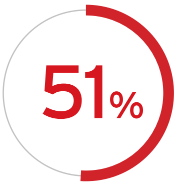
To find out more, we commissioned Sapio Research to poll 2718 business decision makers (BDMs) in 26 countries: Australia, Austria, Belgium, Denmark, Finland, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Netherlands, Norway, Philippines, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Taiwan, UAE, the US and UK.

2,718

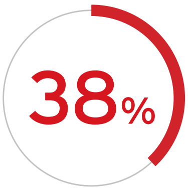
business decision makers

26

countries



consider it a necessary cost but not a revenue contributor



see it as a barrier rather than business enabler

Unfortunately, the headline findings show a siloed, often contradictory view of the value of cybersecurity for the business. On the one hand, 89% of BDM respondents acknowledge the link between business and cyber risk. Yet on the other, half (51%) claim security is a necessary cost but not a revenue contributor, while a similar share (48%) argue that its value is limited to attack/threat prevention. Around two-fifths (38%) even see cyber as a barrier rather than a business enabler.

Joining the dots between business and cyber risk

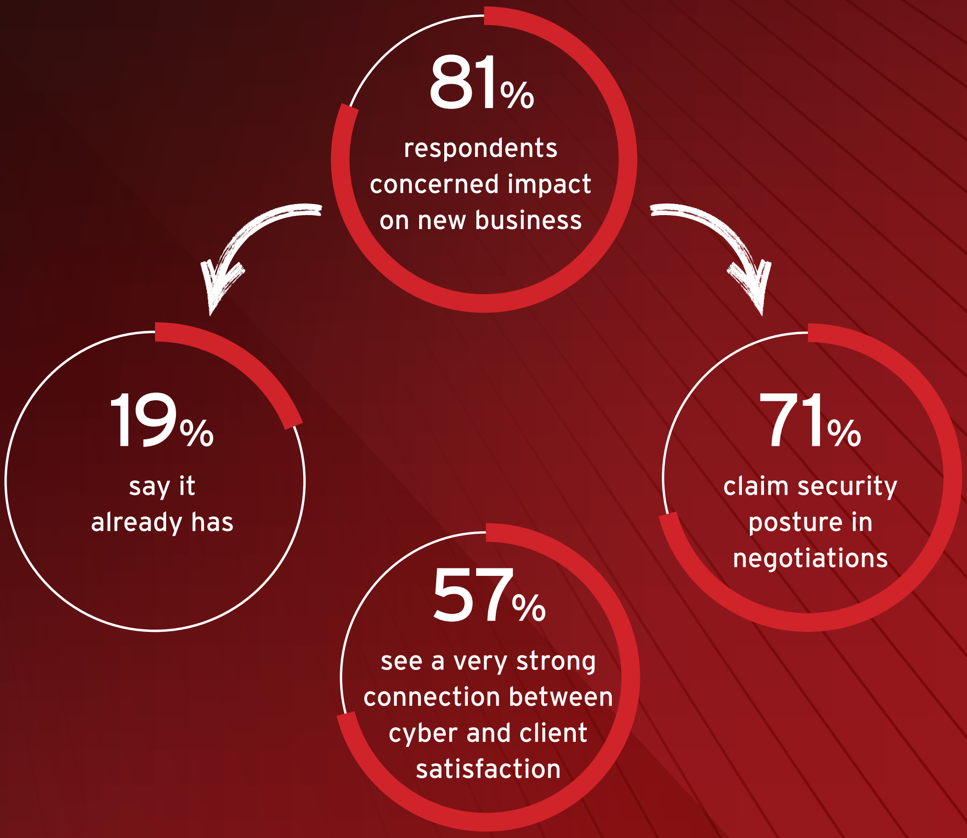
It should be welcomed that nearly two-thirds (64%) of respondents plan to increase their investment in cybersecurity in 2023. But blindly splashing cash on the latest high-profile technology solutions will not help the business. It will only create more product silos and more work for stretched IT teams tasked with managing point products.

BDMs need to understand which areas require funding most urgently, taking a risk-based approach to prioritise them. Yet many seem unclear about the strategic importance of cybersecurity – even when presented first-hand with evidence. We can highlight several key areas where they're failing to join the dots between business and cyber risk:

Hampering new business

On the one hand, 81% of respondents are concerned that poor security posture could impact their ability to win new business. And a fifth (19%) say it already has. An additional 71% claim they're already being asked about security posture in negotiations with prospects and suppliers and 78% that these requests for more information are growing more frequent.

Yet in spite of this, just 57% of BDMs we polled see a "strong" or "very strong" connection between cyber and client acquisition/satisfaction.



81% respondents concerned impact on new business

19% say it already has

71% claim security posture in negotiations

57% see a very strong connection between cyber and client satisfaction

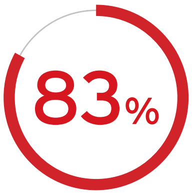
Is there a connection between cyber and new client acquisition?

Talent acquisition/retention

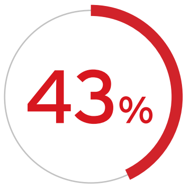
Nearly three-quarters (71%) of respondents claim the ability to work from anywhere has become vital in the battle for talent. Yet just two-fifths understand the strong connection between cybersecurity and talent attraction (43%) and retention (42%).

That's despite recognition about the impact of cyber on the employee experience:

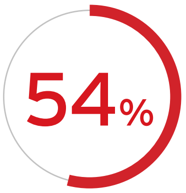
- 83% say current security policies have affected remote employees' ability to do their jobs (e.g. network and information access issues, and slowing the pace of work)
- 43% say current security policies place restrictions on employees' ability to work from anywhere
- 54% say current policies restrict what devices/platforms employees can choose to use



say security policies have affected remote employees' jobs



say security policies place restrictions on remote working

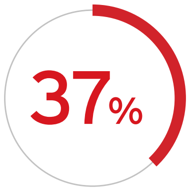


say policies restrict what devices/platforms employees can choose

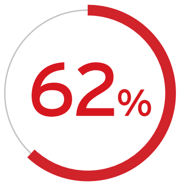
Innovation

Some 68% of BDMs say their organisation needs to innovate quicker in order to be more competitive. Yet only half (52%) see the strong connection between cyber and innovation. That's in spite of the fact that:

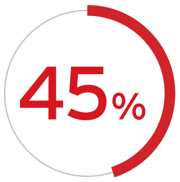
- 37% claim that security increases their willingness to embrace innovative technologies like cloud, AI and digital twins
- 62% say current security policies increase the speed at which their organisation is able to roll out new digital technologies
- 45% believe these digital transformation projects could be accelerated further by enhanced cybersecurity



claim security increases willingness to embrace technology



say speed increase in rolling out technology



believe enhanced cybersecurity accelerate projects

Data insight

Three-fifths (61%) of BDMs claim there's an urgent need to diversify revenue streams in 2023 and even more (67%) argue that access to data will be fundamental to unlocking these new revenue streams. An additional 90% believe they could achieve cost savings partly through better use of data.

However, on the other hand, nearly two-fifths (38%) claim not to see a strong connection between cybersecurity and data insights.

Seeing eye to eye

The truth is that effective cybersecurity is an essential foundation for business success. As the report shows, it can reassure prospective partners and clients, drive innovation-fuelled digital transformation, unlock data insight and help with talent acquisition/retention. But how?

The key is to take a risk-based approach to cybersecurity, which will help BDMs:

- ✓ Identify their key assets
- ✓ Continuously calculate the business risk/impact of cyber-incidents across these assets (e.g. how much would a ransomware outage cost the business per day?)
- ✓ Work more intelligently to continuously manage risk across their top-tier assets

Closer IT/business communication will be essential to make this a reality. Security teams not only need to get better at articulating cyber in business risk terms, they also need to understand business workflows more empathetically when designing policies.

Unfortunately, there's still some way to go. Only a third (33%) of respondents say their organisation reports cyber as a business risk, and over a quarter (28%) don't even track cyber risk. Over half (55%) say their organisation's current cybersecurity policies/processes create information siloes. And a fifth of businesses don't have any cyber improvement programme in place.

Ultimately, progress will come not just from IT and security leaders getting closer to the business. BDMs must also recalibrate their view of cybersecurity. They can see how much it can impact the business. Now it's time to make sure that impact is positive.

To find out more, head to **www.trendmicro.com**

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy