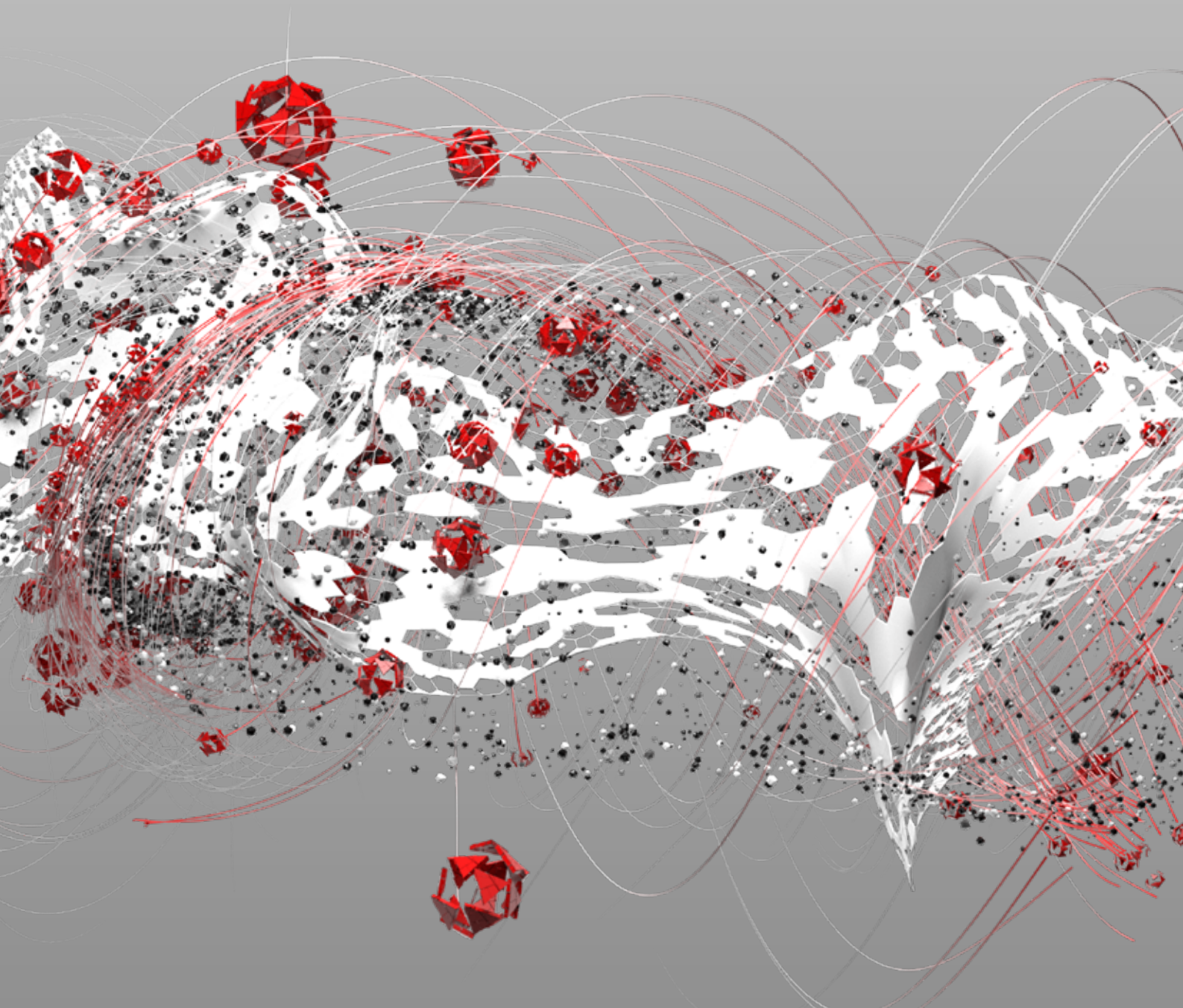
TREND MICRO™

A Global Study

BUSINESS FRICTION IS EXPOSING ORGANISATIONS TO CYBER THREATS



The psychology of risk

The past 18 months has been a boom for the cybercrime economy. Threat actors moved quickly to exploit the disruption and digital transformation driven by the pandemic. Losses reported to the FBI alone exceeded $4bn last year. The true figure is likely to be many times higher. Faced with these kinds of odds, you would expect boards and their IT and security decision makers to be pulling in the same direction. Unfortunately, a new study from Trend Micro finds that the opposite is true.

Business and IT functions have never seemed further apart. Getting them to sing from the same hymn sheet will require enhanced visibility into threats, and possibly even structural changes to the security function. But most importantly, it will need a change of culture, to one where security is embedded into everything the business does.

To find out more, Trend Micro commissioned Sapio Research to interview 5321 IT and business decision makers from enterprises of 250+ employees across 26 countries.

5,321
IT security decision makers

26
countries

250+
employee companies

Threats are everywhere

Trend Micro blocked almost 63 billion threats in 2020, and a further 41 billion in the first half of 2021, putting this year on track to set a new record. Success rates have rocketed for threat actors because organisations are in flux. Many have invested big in digital projects—whether it's to support remote working, build new business processes, or drive new business models and customer experiences. The result: more unmanaged endpoints and cloud infrastructure for the bad guys to aim at. Some 80% of organisations now have a hybrid cloud and 92% have a multi-cloud strategy, for example.

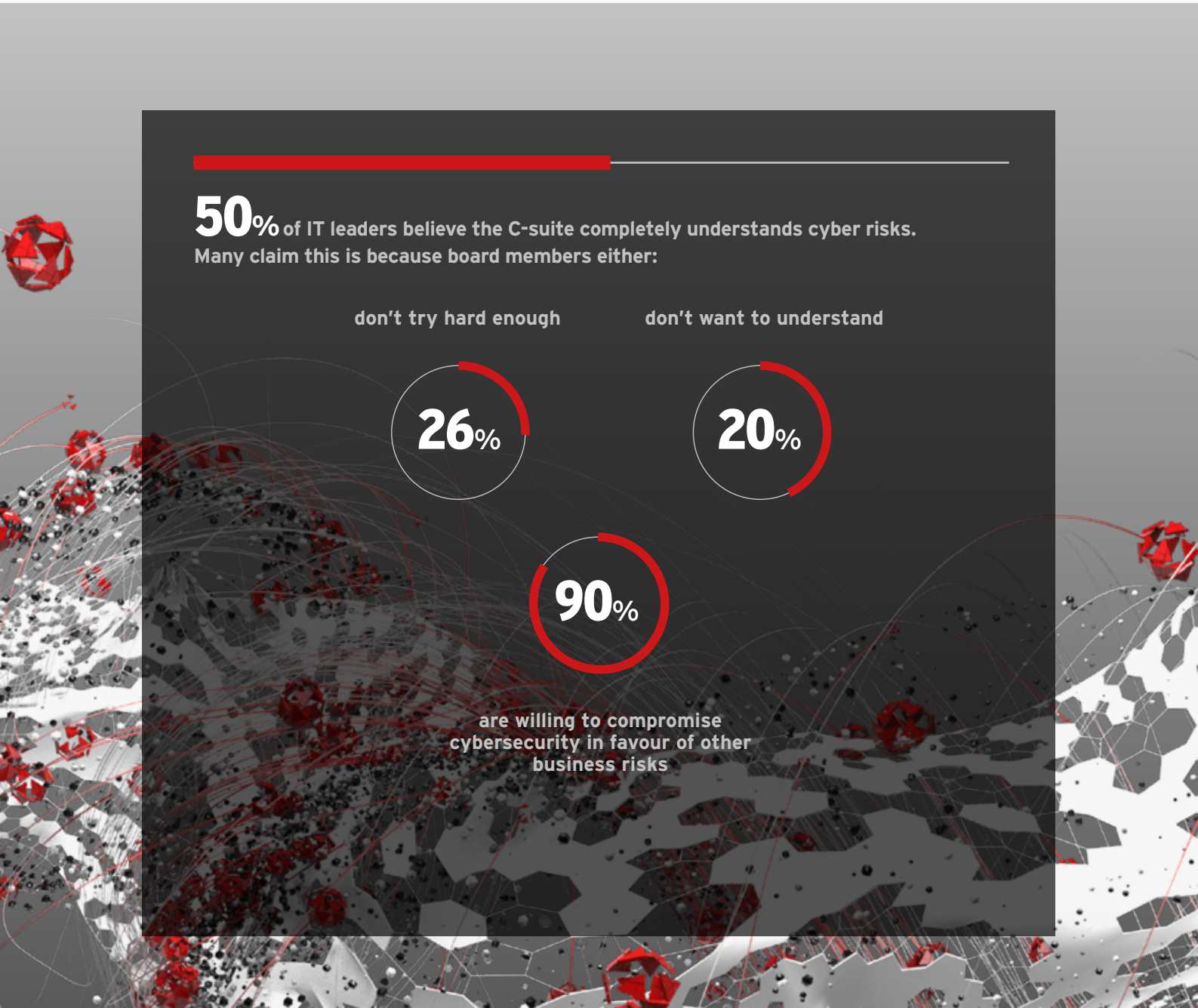
The stats tell their own story. Globally, ransomware surged by 150% year-on-year in 2020 with average extortion amounts doubling. In the UK, almost two-thirds of medium and large businesses admitted said they've suffered a breach over the past 12 months. Attacks are hurting victim organisations financially and reputationally. The average cost of a breach today now exceeds $4.2m, although the figure can reach much higher if ransomware is involved. Some organisations have admitted losing tens of millions due to attacks and their aftermath.

How friction is hurting businesses

Yet in spite of these escalating risks and costs, boardrooms appear to have other priorities. According to our research, 90% of IT decision makers claim their business would be willing to compromise on cybersecurity in favour of digital transformation, productivity, or other goals. Why is this? A second finding reveals more: only 50% of IT leaders believe the C-suite completely understands cyber risks. Many claim this is because board members either don't try hard enough (26%), don't want to understand (20%), or see it as an impenetrable technology issue.

Even worse: 82% of IT decision makers have felt pressured to downplay the severity of cyber risks to their board. Nearly a third claim this is a constant pressure.

The friction between business and IT functions extends throughout the organisation. IT leaders are nearly twice as likely as their business counterparts to say IT teams and the CISO are ultimately responsible for managing information security risk.



What happens next?

The challenge is clear: boards and business leaders don't see eye-to-eye with IT decision makers on security. In fact, half (49%) of respondents claim that cyber risks are still being treated as an IT problem rather than a business risk. Most also suggest that the only way the C-suite would actually sit up and take notice of cyber is if:

- The organisation suffered a breach (62%)
- Customers started to demand enhanced security (61%)

This must change. But how? It's about IT and security leaders speaking to the board in a language it understands: business risk. Two-thirds of respondents claim cyber has the highest cost impact of any business risk. These are the sorts of stats to grab the attention of boardrooms everywhere. Yet before they can even start these conversations, security leaders need better insight into cyber risk.

Here are some recommendations on next steps:

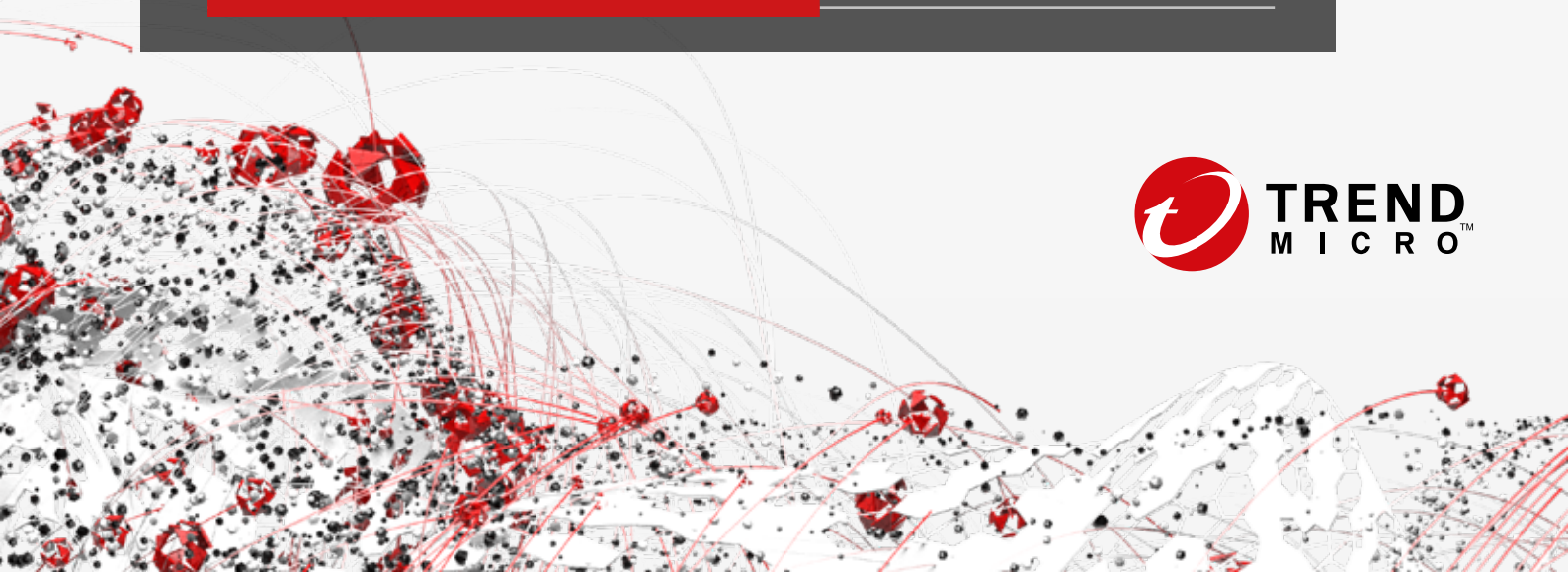
1) **Formalise cybersecurity** with documentation, KPIs and established metrics. This will help to drive a business risk discussion about cyber.
2) **Consider a new role** of Business Information Security Officers (BISOs), who can help embed security into business processes and align cyber with business demands for productivity.
3) **Restructure reporting lines** so that the CISO reports directly into the CEO—this will expose the latter to cybersecurity matters and will help provide more business input for security leaders.
4) **Formalise cybersecurity** with documentation, KPIs and established metrics. This will help that business risk discussion about cyber.
5) **Deploy an XDR platform** that correlates and analyses threat data from across the IT environment (endpoints, servers, cloud workloads, networks and email) to provide maximum visibility into threat and risk levels).

The end goal is to build a culture of security-by-design, where awareness of cyber risk is built into every business process, and the behaviour of all employees. It won't be an overnight journey, but the stakes are too high to ignore the challenge.

The only way the C-suite will sit up and take notice of cyber risks is if:

- the organisation suffers a breach 62%

- customers demand enhanced security 61%



TREND MICRO™