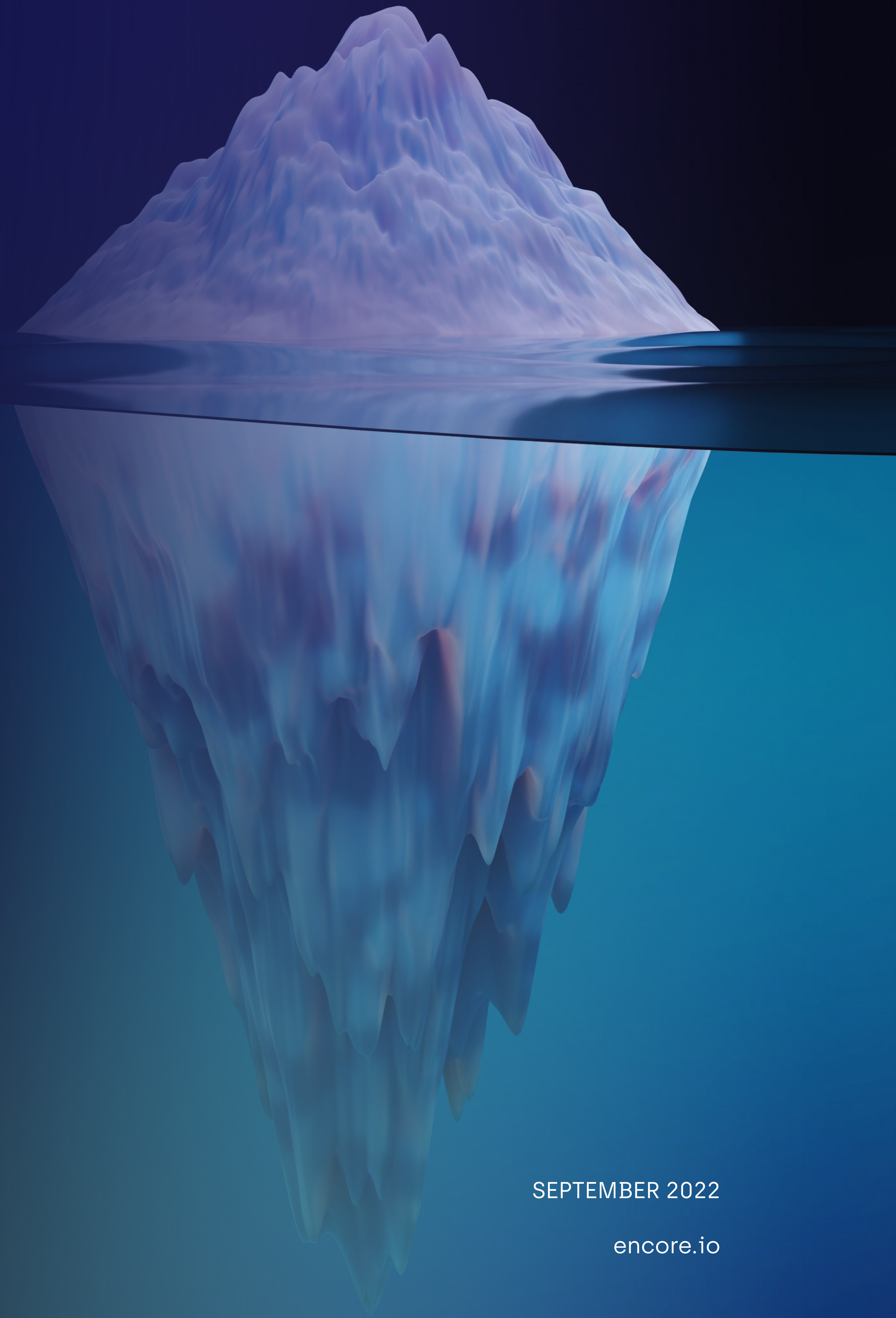
ENCORE

Industry Research Report

THE TRUE COST OF CYBER

WHAT HIDES BELOW THE TIP OF THE ICEBERG?

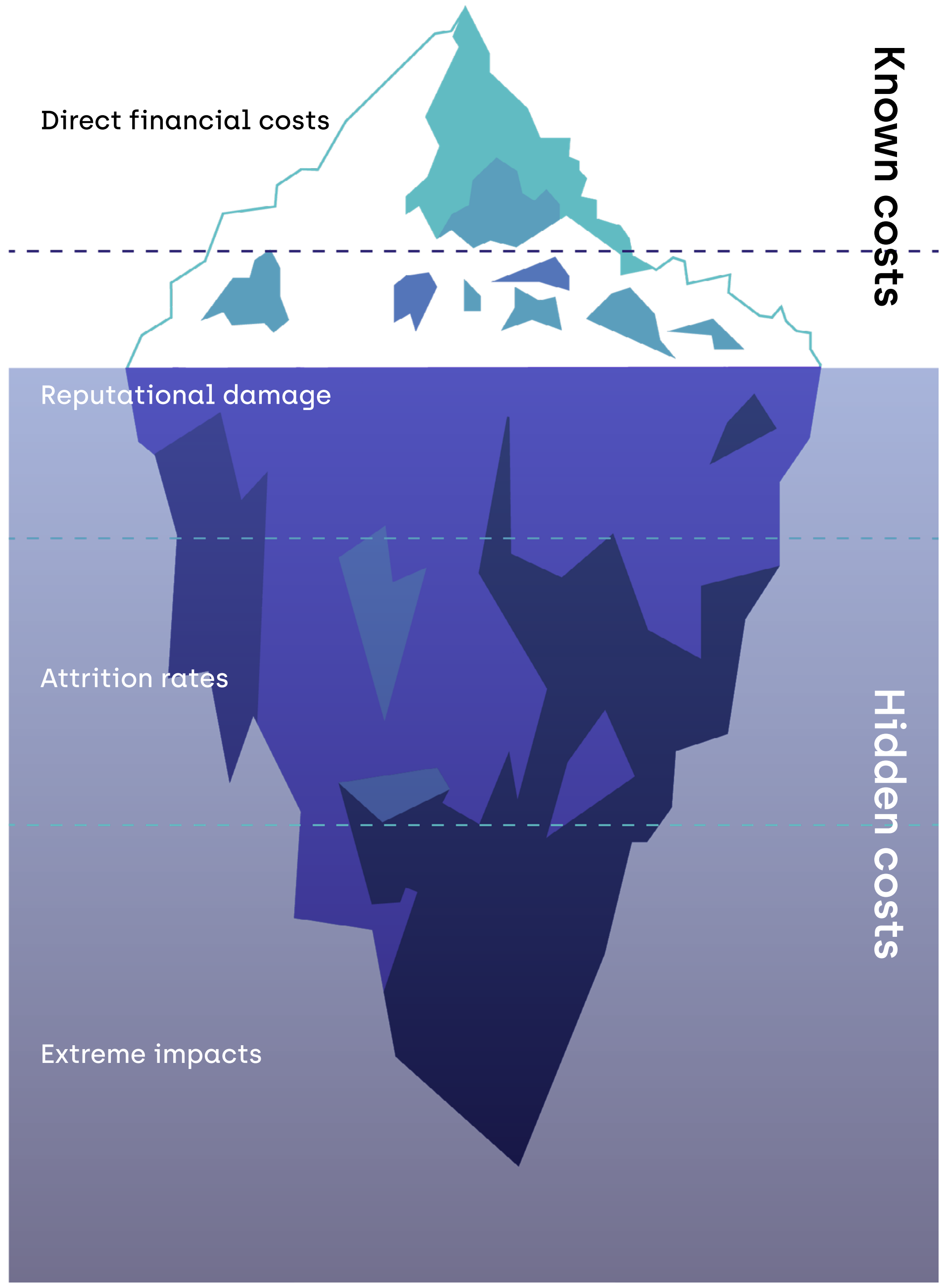


SEPTEMBER 2022

encore.io

Table of content

Introduction



When you think about the cost of cybersecurity, do you picture the total budget spent on defences each year, or do you think of the cost and reputational damage of a successful breach on your business?

The former is essential, the latter is avoidable.

Imagine it this way. Your business is situated at the bottom of a valley, surrounded by a huge dam: your security stack. Behind those defences lies a vast expanse of water – the cost impact of a cyberattack – that will flood your business at the slightest breach.

The conventional wisdom is that the more you invest in those defences to keep the dam impenetrable, the less likely you will be to experience a cascade of costs.

When it comes to defining these costs, the obvious split is into two categories: known and unknown.

For further clarity, let's go back to the iceberg analogy:

- **The tip of the iceberg:** direct financial costs, including recovering lost assets and ransom payments
- **At the water's edge:** reputational damages, including loss of client trust, loyalty and new business
- **In the shallows:** attrition costs, including the impact on staff retention and ongoing recruitment
- **Deep waters:** extreme impacts that are becoming more common, including national security issues, cyber warfare and even loss of human life

The impact of each cost is dependent on the size and type of business, but every single one is a real possibility and needs to be acknowledged and actioned.

Our latest industry research reveals the most widely recognised repercussions of experiencing a cyber breach, and whether the attention placed on effective defences matches the concerns around business costs. Encore commissioned a poll of C-suite executives, CISOs and office workers, which was conducted by international research consultancy, Censuswide.

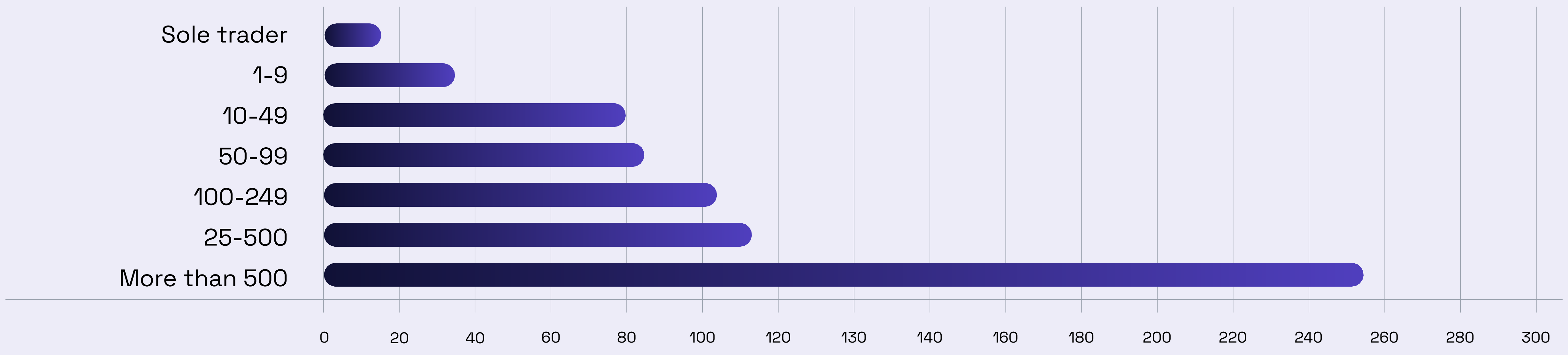
Within this eBook, we will explore each category in full and identify the key priorities for organisations looking to keep the cost floodgates closed.

Foreword by Brendan Kotze, CEO and Co-founder of Encore

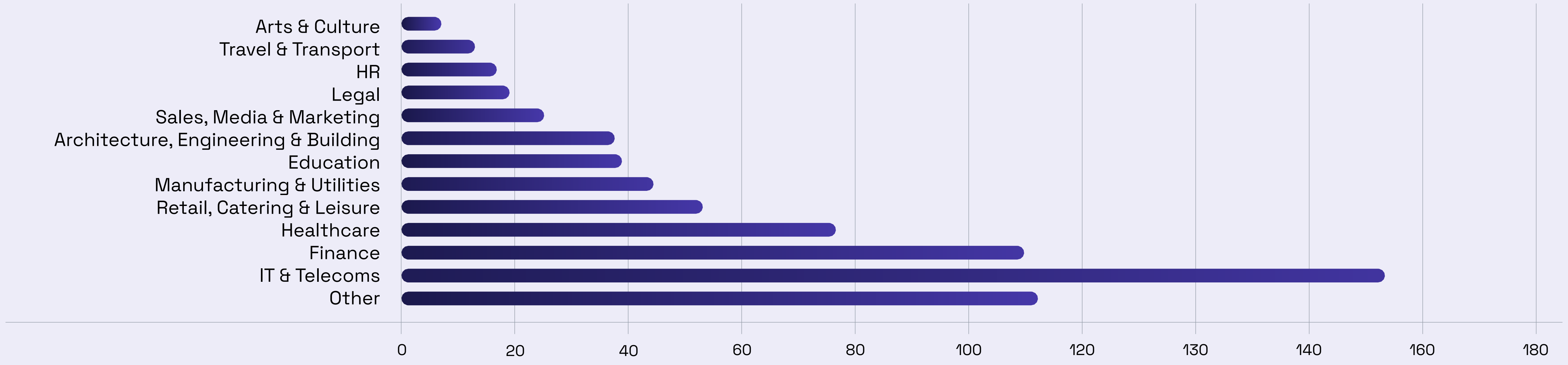
Methodology

The study polled 100 C-level executives, 100 CISOs and 500 office workers from the UK and US. The research was conducted by Censuswide and commissioned by integrated security provider, Encore, to analyse the differing attitudes between business levels regarding the education and application of everyday cybersecurity.

Size of company (number of employees)

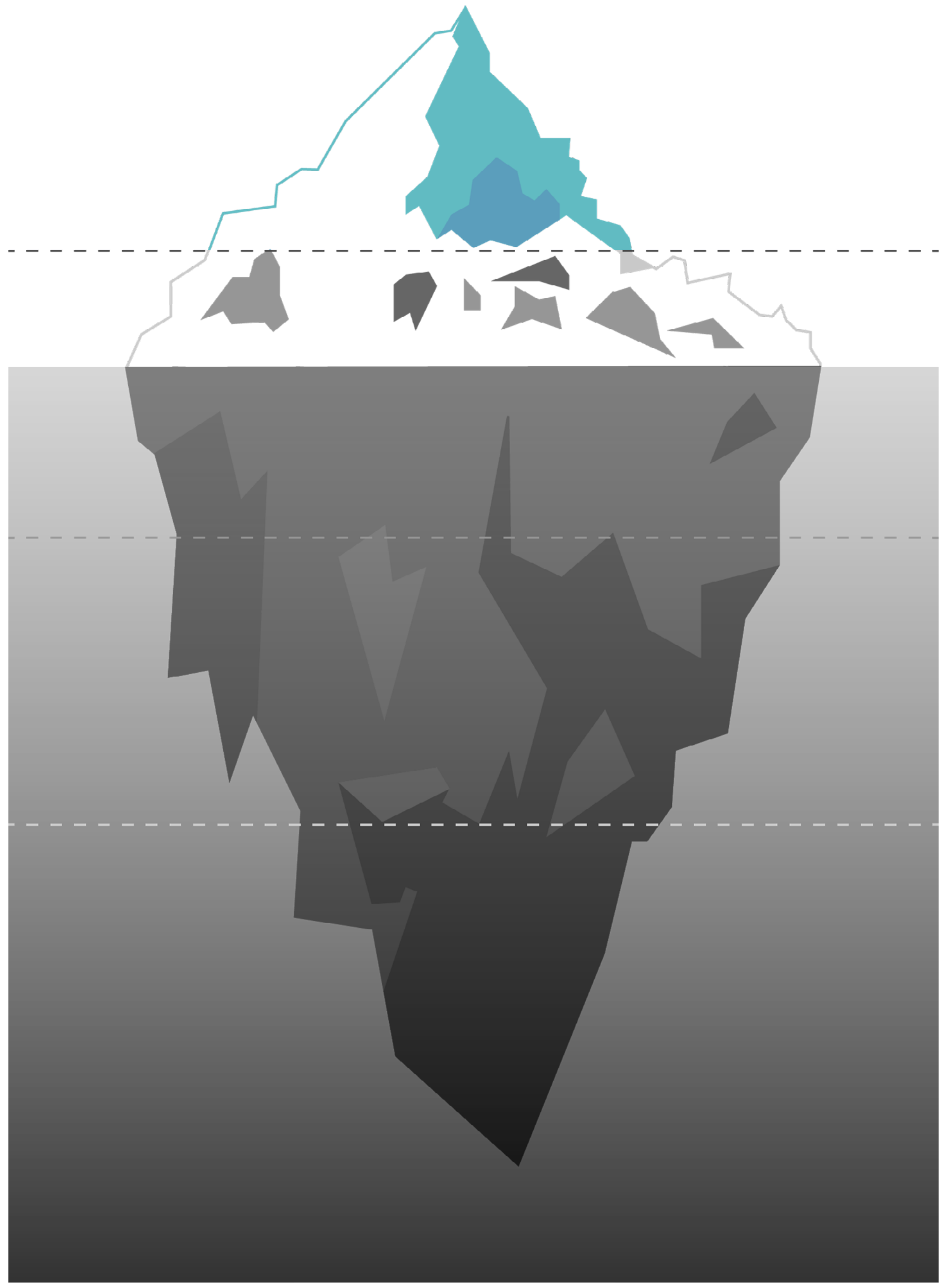


Industry sectors



Tip of the iceberg:

Direct financial costs



In most cases, when an organisation is breached, one of the immediate considerations from executive teams is this: ‘how much is this going to cost us to recover from?’

As of this year, the average cost of a data breach has now risen to $4.35 million, with ransomware attacks costing $4.45 million. This figure doesn’t even include the ransom cost itself. It’s substantial for all, but catastrophic for many.

Our research shows that recovery costs are considered by C-suite executives to be the biggest financial impact of a cyberattack. This includes replacing systems with new technology, updating processes and introducing training programmes.

54% **of C-suite executives rank recovery costs as being the biggest financial impact post-breach**

Additional costs often incurred following a data breach or ransomware attack include retrieving intellectual property, making up for any operational disruption, paying the ransom, and providing compensation to impacted customers or partners.

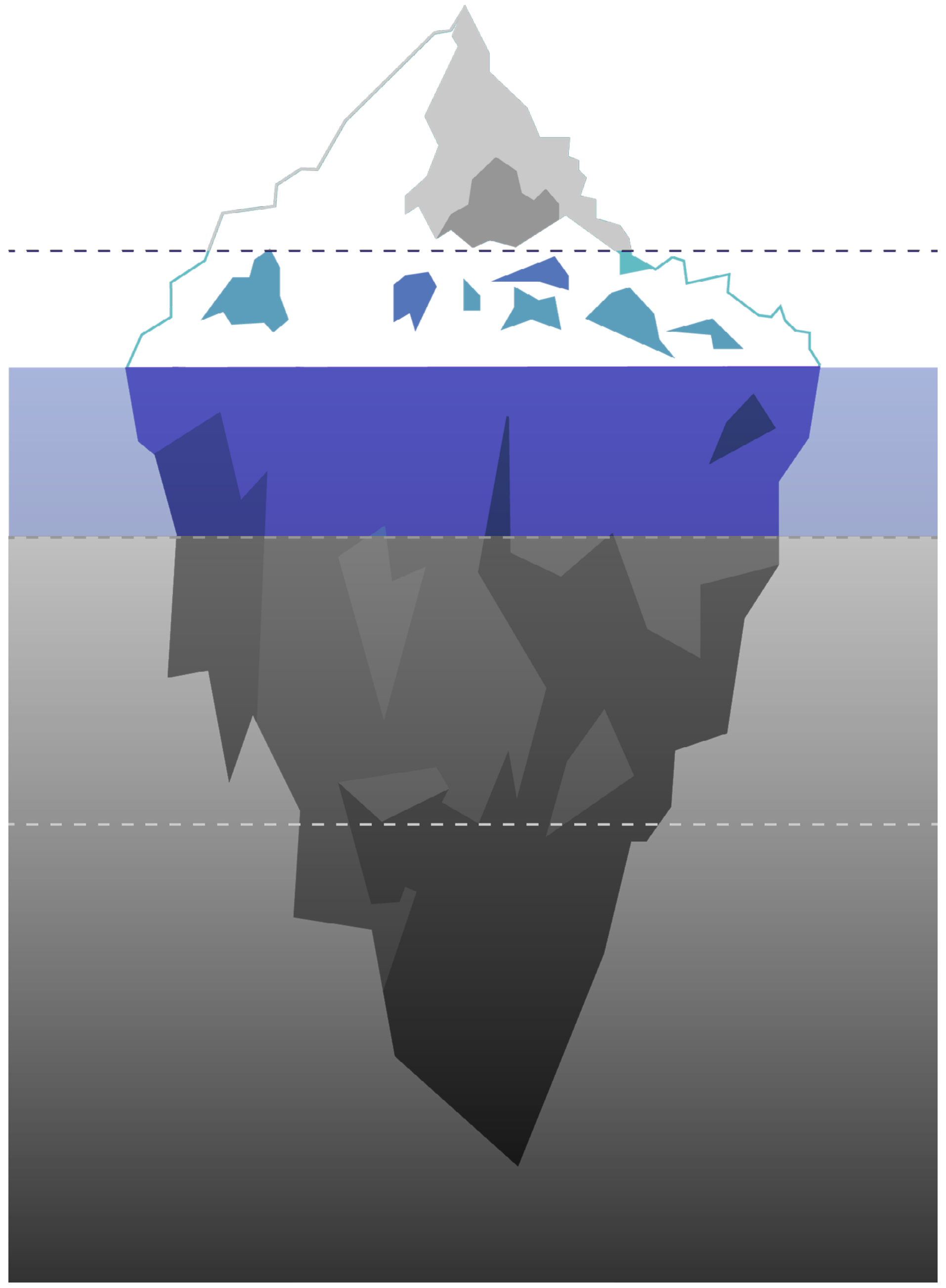
CISO respondents named data theft (69%) and ransomware (44%) as being two of the most likely threats to impact their organisation. Both attack vectors are popular amongst cyber criminals given their propensity to make more money and cause further damage beyond disrupting operations, compared to a DDoS (distributed denial-of-service) attack, for example.

The secondary challenge – and cost – is that, once you’ve been breached, the likelihood of being breached again is much higher. In fact, a recent study revealed that 80% of ransomware attack victims are repeat victims.

A single pay-out could very quickly become a sequence if the organisation fails to strengthen their defences.

At the water's edge:

Reputational damage



We've established that financial loss is concern number one, but this is closely followed by the long-term damage to a company's reputation amongst customers, partners and the wider market.

These reputational costs are not unknown to CISOs and C-level executives and are becoming more of a concern as time passes. In fact, 41% of CISOs and C-level executives named reputational damage as being one of the biggest costs to their business following a cyberattack, and 34% agreed loss of clientele was a significant cost.

Losing future business from existing customers is a real possibility if confidential data or assets are put at risk by a successful breach. Some clients may also feel forced to terminate contracts early if the situation is considered severe enough, resulting in immediate impact on revenue.

For start-up businesses, suffering a breach can also result in damage to investor relations and potential business opportunities.

Brendan Kotze, CEO and Co-Founder of Encore, comments:

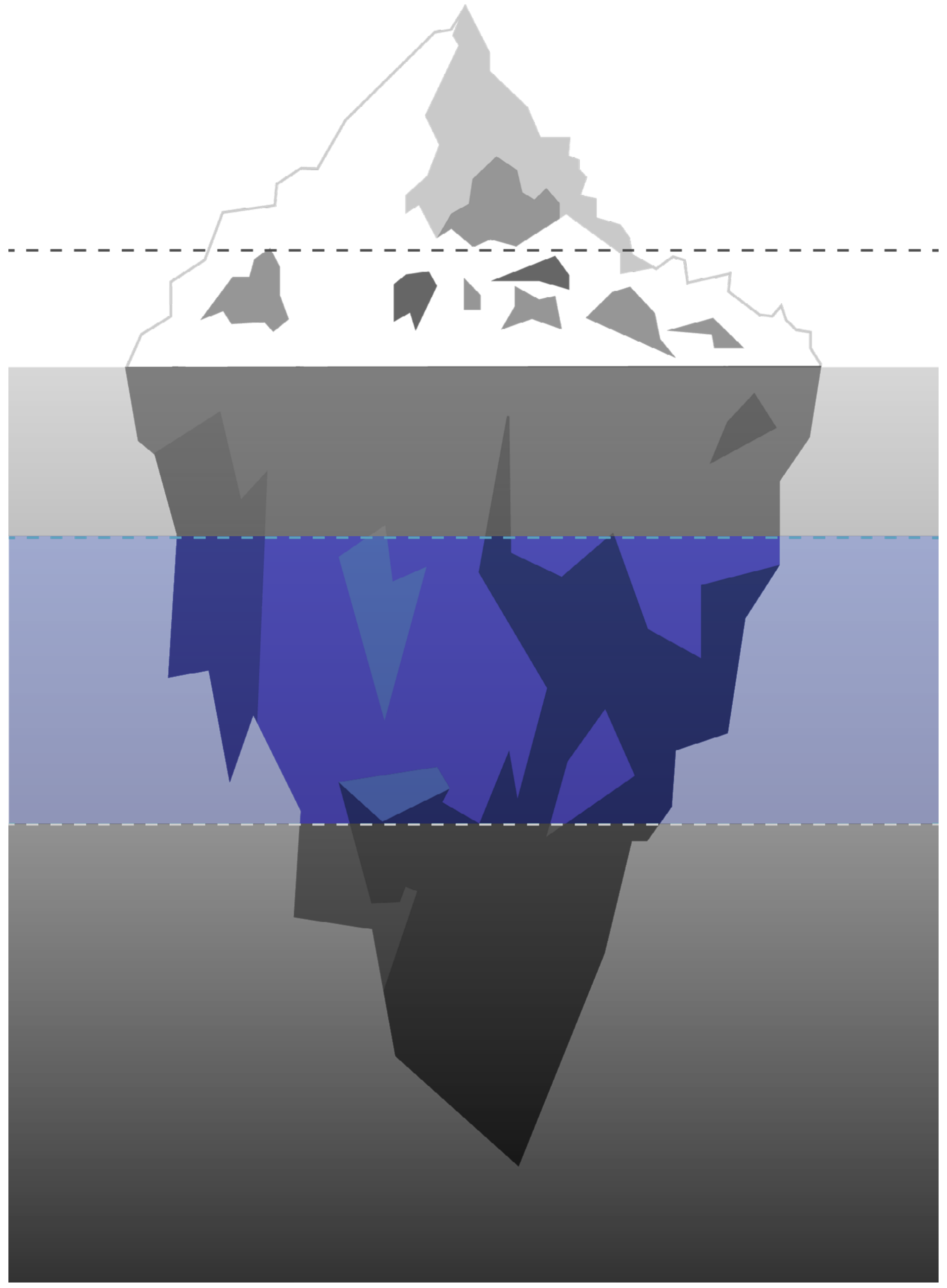
"Damaged business reputation has the potential to impact relationships not only with clients, but also with potential partners, investors and future employees. This particular cost has the propensity to send damaging shockwaves beyond the immediate hit."

Being able to instil complete confidence and trust in your existing and future clients and partners is paramount to strong business relationships. Any threat to your trade name – or risk of devaluation – is therefore potentially ruinous.

However, partners and clients are not your only business relationships at risk of erosion following an attack.

In the shallows:

The Great Resignation



As we dip below the surface, hidden costs start to appear. According to our latest research, cyber breaches can also directly impact staff attrition rates and future recruitment efforts.

We are currently experiencing unprecedented attrition rates, now dubbed 'The Great Resignation.' Employee expectations around their work environments are soaring post-pandemic, and the number of resignation letters continues to grow.

With such high numbers of workers on the precipice of jumping ship, businesses cannot afford to give them any reason to make the leap.

However, cybersecurity continues to be a concern.

Our research revealed that more than half of surveyed office workers (54%) say that if a business experienced a recent cyber breach, it would influence their decision to work with that company. Only 33% would be completely unphased by a cyber break-in.

Over 1/2 of office workers would reconsider working for a business that had recently experienced a cyber breach

It's clear that office workers are becoming increasingly concerned about cyber threats, but are they being reassured by company policies regarding cybersecurity.

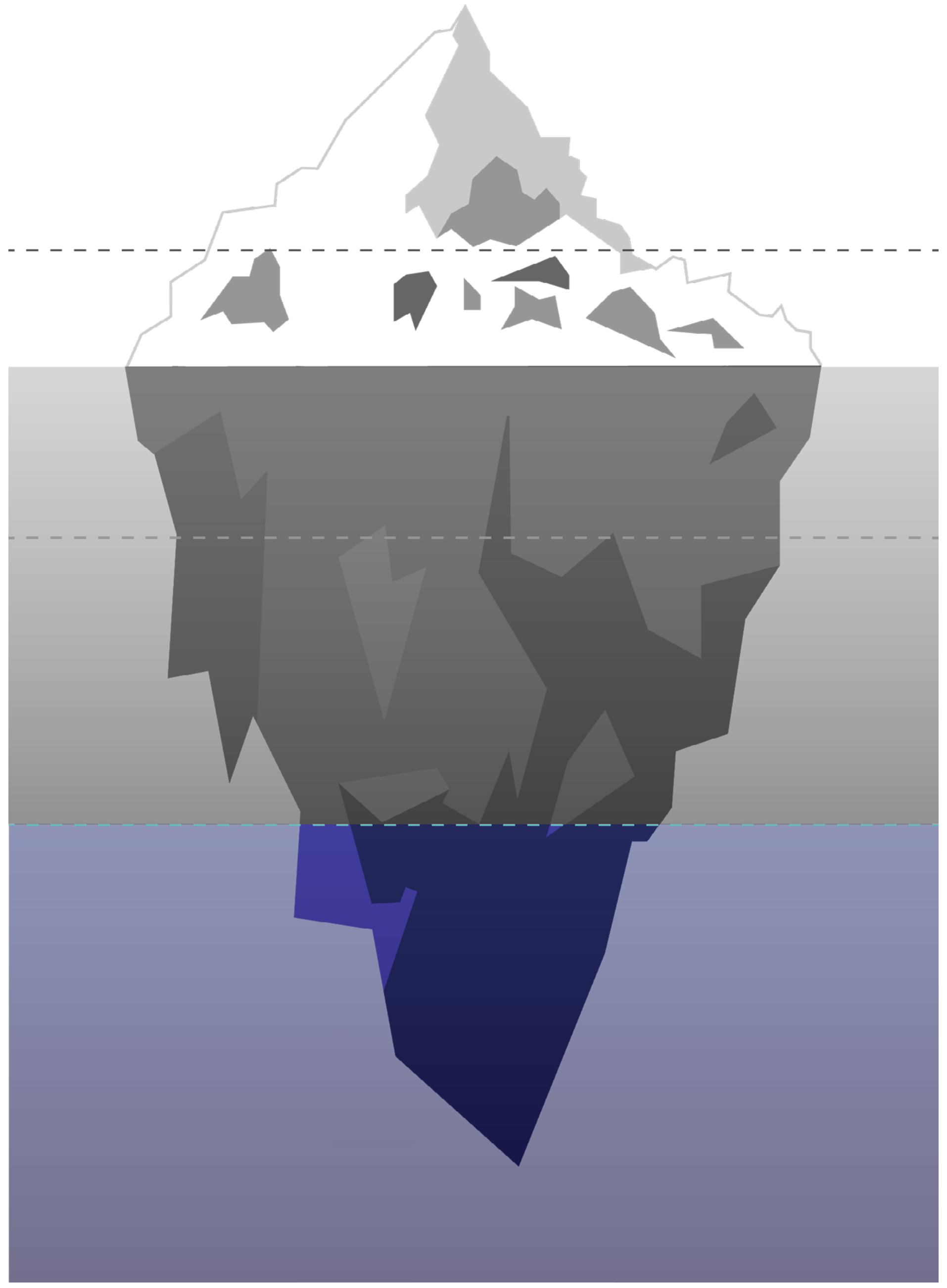
More than 1 in 2 C-level executives (57%) say they have been breached in the last 12 months alone, but most office workers are unaware – only 39% believe their organisation had been breached. A lack of transparency and awareness may exacerbate the impact on attrition rates, once the true position is revealed.

The damage caused by cyberattacks and the impact on individuals is now recognised by all members of an organisation, not just the senior and executive members.

Being breached is one thing, keeping your workforce in the dark is another.

Deeper waters:

Extreme, but possible



As the threat landscape expands, the repercussions of a successful cyberattack become ever more damaging. It's no longer just personal information and business operations at risk, the overall cost is much greater.

The impact of cyberattacks has now breached the threshold between digital and physical, where threat to human life and international warfare are very real possibilities.

Although 92% of CISOs and C-level executives believe their business is secure at any given moment, would they feel as confident if there was more at stake? Whilst a lot of organisations may feel that these costs don't apply to them, the potential severity of cyber breaches should be recognised and understood at the business level.

Brendan Kotze, CEO and Co-Founder of Encore, says:

"Regardless of whether a business believes these extreme repercussions are relevant to them or not, when it comes to combatting the expanding cyber threat landscape, a united front is a resilient front. If all companies prepare and respond to threats as if their existence (or at least a very substantial part of it) is at risk, our chances of blocking or swiftly responding to attacks is considerably higher. Cybersecurity is no longer enough; we need to channel Cyber Safety to build resilience and establish trust both internally and externally."

Cyberattacks are increasingly impacting areas of greater concern to countries and businesses alike, such as highly sensitive data and critical infrastructure, where attacks pose a real threat to life.

The rise of attacks on healthcare organisations, in particular, is a worrying trend. According to the **US Department of Health and Human Services**, in the US alone, there were at least 125 electronic data breaches in healthcare businesses since the beginning of April 2022. These institutions are targeted with a mixture of ransomware and DDoS attacks; and loss of data and denial of access make for a life-critical combination in hospital environments.

Nation-state attacks are also becoming more common, with adversaries no longer solely targeting government buildings and infrastructure, but also influential organisations, both in the public and private sector.

There's a growing trend of nation-states attacking flagship companies. Higher stakes mean higher rewards for threat actors. For example, the reputational damage of an attack on Facebook in the US or Huawei in China could easily be seen as an indirect attack on a nation.

Conflict between countries now directly involves businesses and the costs are far greater than any ransom pay-out.

Visibility is key

Industries across the board have varying levels of visibility over the potential costs of a successful cyber breach. How many will remain preoccupied with the costs at the tip of the iceberg, and how many will look below the surface?

In most instances, the costs you see straight away are often the least of your concerns; it's the costs you don't see immediately that could do the most damage.

Cybersecurity is a top priority throughout organisations; 53% of businesses have it at the top of their agenda, and 33% have regular discussions. Part of understanding the importance of cybersecurity is also recognising that the price of prevention significantly outweighs the resultant costs of a successful breach.

According to our research, 60% of businesses intend to spend more on cybersecurity this year. To avoid incurring hidden and unexpected costs, long-term cyber strategies should have cost visibility at the centre.

To build a business case around a robust cybersecurity strategy, recognising these hidden costs is a good start.

- Direct financial costs from ransom payments and recovering lost assets
- Rises in insurance premiums after declaring a cyber breach
- Compensation for any impacted customers or partners
- Immediate reputational damage amongst partners and customers
- Long-term loss of trust and business, both existing and future
- Increased numbers of employees leaving, and direct impact on recruitment
- Worst case scenarios: loss of human life, national security, and international warfare

Visibility is key

Encore grants organisations a new level of insight by bringing the entire security stack into one simple interface – nothing is left in the dark.

The cloud-based platform uses APIs and custom queries to connect with security controls to analyse them directly and report results in a coherent and unbiased data format. Encore delivers a consolidated dashboard view of the entire security estate, including performance, risk, gaps, and activities – all ranked by levels of security and urgency.

"Businesses are becoming increasingly aware of the potential costs of a cyber breach, but conversations immediately form around financial loss, and stop short of acknowledging the hidden costs beneath.

Short-term monetary expenses will very quickly become negligible when the true extent of hidden costs behind the wall of defences come to light. It's our aim and mission to help businesses keep that wall strong,"

Brendan Kotze, CEO and Co-Founder of Encore.

How Encore can help

Encore's integrated platform will help you:

- Make quick, informed decisions about your security strategy with real-time information
- Improve compliance and coverage to ensure maximum security while aligning with updating industry regulations
- Manage threats and minimise the attack surface to reduce the risk of a breach in the first instance
- Deliver immediate insight into regulatory and audit compliance for easy reporting and ongoing management
- Ensure better ROI from existing investments, helping teams get the most out of each individual security solution in their stack
- Provide proof and visibility of security to boost overall security management 24/7

About Encore

With more than 25 years' experience providing professional services and cyber security consulting for the largest companies in the world, we brought this knowledge to Encore, the leader in internal and external cybersecurity (CAASM and EASM). Our team is comprised of offensive security experts and security engineers, and consultants that know the mindset and tooling of the attackers, the internal operational obstacles, the challenges faced by security management and how to get the most out of security tooling.

Encore visualises information that can be confusing and often overwhelming, providing accurate and action-based reporting and visibility across numerous security controls, through one secure portal.

encore.io ›

ENCORE

www.encore.io