A global study

Risk & Reward:

Joining the dots between security and data-driven insight for sustainable growth

April 2023
Trend Micro

Introduction

Global data volumes are exploding. They have reached almost inconceivable levels today – and will surge to an estimated 180+ zettabytes by 2025. To put that in perspective, one zettabyte is a billion terabytes. Much of this data is created by organisations, their customers and suppliers. So it follows that those able to derive insight from it faster and more effectively than their rivals will gain a competitive advantage. The technology is already there to do so. Some estimates put the market for data analytics at $54bn this year.

But what happens if this data is stolen, destroyed or sabotaged? As organisations become more reliant on data-driven insight for sustainable growth, their risk exposure grows. Those business leaders unwilling or unable to consider the worst-case scenario may find their digital transformation plans eventually unravel.

To find out more, we commissioned Sapio Research to poll 2718 business decision makers (BDMs) in 25 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

25

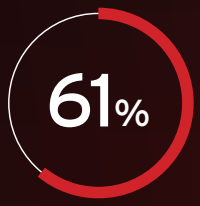
countries

We found that although most business leaders acknowledge the importance of data to unlocking new insights and growth opportunities, many don't see the relevance of cybersecurity. That could be a costly oversight.

The path to sustainable growth

These are precarious times to be a business leader. Persistently high inflation, interest rates and energy bills in many countries have stifled growth and driven up the cost of borrowing. The IMF forecast is for a "pronounced growth slowdown" among advanced economies – from 2.7% in 2022 to 1.3% in 2023. However, a decline to below 1% is not out of the question as inflation remains stubbornly high.

Against that backdrop, it's perhaps unsurprising that 61% of BDMs agree there's an urgent need to diversity revenue streams in 2023. Done right, this can help to reduce corporate risk, add value and reach new customers and opportunities. Even more telling is the fact that 68% of respondents acknowledge the fundamental role data will play in unlocking these new revenue streams. A further 91% believe they can also drive cost savings through better use of data.



of BDMs agree there's an urgent need to diversity revenue streams

acknowledge the fundamental role data will play

believe they can also drive cost savings through better use of data

They're right. According to analyst firm Forrester, companies with advanced insight-driven business capabilities are eight times more likely to say they grew by 20% or more than "beginner" firms. They use these insights to discover new sources of revenue and create market differentiation, and more frequently commercialise their data, it claims.

Cloud-based data analytics tools are an increasingly popular way to harness these business benefits. By applying intelligent algorithms to huge datasets of high quality, current data, organisations can do everything from anticipating emerging market trends to running financial forecasting scenarios. But data insight can go even further, in scenarios like:

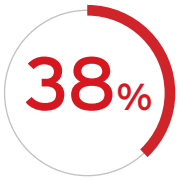
- **Using IoT sensor data to detect maintenance requirements before equipment fails**
- **Uncovering hidden user behaviour patterns in web data, to build more personalised customer experiences**
- **Leveraging real-time analytics to direct spot and direct loyalty programme customers to products they favour, as they shop**

In fact, according to McKinsey: "By 2025, smart workflows and seamless interactions among humans and machines will likely be as standard as the corporate balance sheet, and most employees will use data to optimise nearly every aspect of their work."

Building on secure foundations

So what role should cybersecurity play in this new data-centric enterprise environment? It's heartening that 62% of responding BDMs believe security policy can accelerate digitalisation – and with it the kind of projects that could help to unlock data insights. Yet, disappointingly, two-fifths (38%) claim not to understand the connection between cybersecurity and data insight. Even more fail to connect the dots between security and generating new revenue streams (48%) or reducing costs (55%).

of responding BDMs believe security policy can accelerate digitalisation



claim not to understand the connection between cybersecurity and data insight

fail to connect the dots between security and reducing costs

In fact, cyber is critical to all of these aspects. If intelligent use of data is key to reducing costs and driving revenue, then protecting that data from accidental and deliberate loss, theft and damage must also be a priority.

Data is created in huge volumes all over the modern enterprise, with often chaotic results. From financial reports to CRM/ERP systems, and email marketing metrics to IoT sensors – data is created and stored in often siloed IT environments, on-premises and across multiple hybrid clouds. Strikingly few organisations have true visibility into everything, meaning they can't protect what they can't see.

That opens the door to data theft, destruction and sabotage via:

- **Malicious third parties**
- **Accidental exposure**
- **Malicious insiders**
- **Supplier compromise**

Serious data breach incidents can take weeks or even months to investigate. During that time, business-critical digital initiatives may be disrupted or halted completely. If systemic risks are uncovered, projects may be shelved for good.

Getting it right

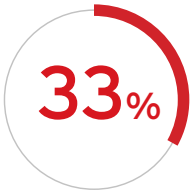
That's why it makes sense to address cybersecurity as a priority at the outset of any major data-centric enterprise initiative. Relevant stakeholders should be brought on board from the start to add their input and follow security and data protection-by-design and default principles. That's not just the way to satisfy GDPR regulators. It's a best practice for minimising cyber and business risk, and maximising the value of data-driven insight projects.

In practice, a good starting point would be:

1) **Discover and classify data according to your risk appetite**
2) **Map data flows, who has access and how it is used**
3) **Put in place continuous monitoring of data and management of risk across the enterprise attack surface**

In more positive news, nearly three-quarters (72%) of IT decision maker respondents already track and report on cyber risk levels, with a third (33%) reporting this to the board as a business risk measurement. A further 79% say their organisation has a Cyber Improvement Program to help meet its digital transformation goals.

of IT decision maker respondents already track and report on cyber risk levels



report this to the board as a business risk measurement

say their organisation has a Cyber Improvement Program

This is a good start, but CISOs must get better at communicating in business risk language, and boards need to take more accountability for advancing cybersecurity initiatives within their organisation. Cyber should be baked into business as a fundamental growth enabler. Until that's the case, digital projects to unlock data-driven insight will always be at risk.