Cybersecurity: trust in a digital age

How can you protect your organisation against ever more sophisticated cybercriminals and invisible breaches of trust? This is one of the key themes explored in our Trend Report. In this report, BDO looks ahead to 2030 together with trendwatcher Tom Palmaerts. We show how Belgian companies can shape the future with agility and confidence. Technology and good old common sense must go hand in hand.

Cybersecurity: trust in a digital age

Technology creates unprecedented opportunities but also makes companies more vulnerable than ever. Cybercrime ignores borders and has become a daily reality, including for Belgian businesses. Hackers no longer focus solely on multinationals but also target SMEs as they are often less protected. Cyberattacks cost billions globally but the greatest loss is often invisible and impossible to quantify: trust.

"Cyber risks remain one of the most underestimated threats to companies. Despite growing awareness, many organisations continue to underestimate the impact of data breaches, ransomware and poor data integrity. The damage rarely stops at financial loss: reputation, trust and continuity are also at stake. On top of that, poor data quality poses a creeping risk. Incorrect or inconsistent data inevitably leads to flawed decisions, undermining trust in both systems and leadership."

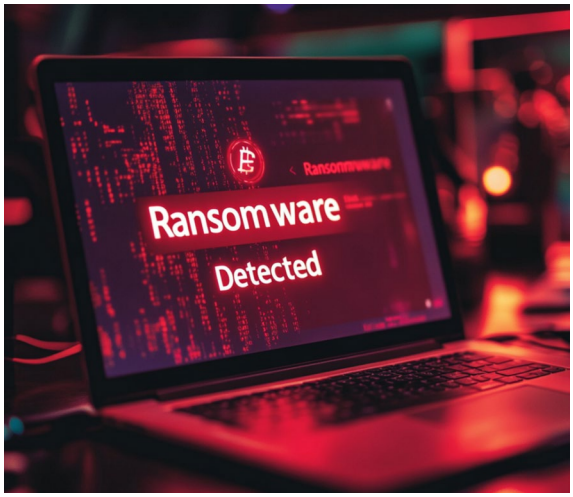
Sam Nelen, Partner Risk Advisory
BDO Belgium

MISINFORMATION AND DISINFORMATION

Not every attack is technical. Companies are increasingly confronted with disinformation campaigns. Sometimes they originate from competitors, sometimes from malicious actors. Such a campaign can confuse both customers and employees. A false post on social media or a leaked document can damage a company's reputation within hours.

TRENDS IN CYBERHACKING

Cyberattacks are becoming more complex and more sophisticated. Ransomware remains the most popular method: systems are locked and only released after payment. Also on the rise: supply chain attacks, in which hackers don't target a company directly but hack a supplier or freelancer to gain access. It shows how vulnerable networks are and highlights the fact that any chain is only as strong as its weakest link.



DEEPFAKES: TRUST AS A WEAK POINT

Cybercriminals exploit our trust. A recent example comes from Ferrari, where criminals mimicked the voice of an executive to force an urgent payment. What halted the attack was not complex technology but a simple piece of common sense: the employee asked a question only the real executive could answer ('Which book did you recommend yesterday?'). The incident shows how convincing deepfakes have become but also that vigilance and critical reflexes remain our first line of defence.

THE QUANTUM ERA

A new threat is looming: quantum computing. Computers capable of calculating millions of times faster would render many of today's encryption methods useless. Although the quantum era hasn't dawned yet, banks, governments and technology companies are already preparing for when it does. Belgian businesses would also do well to follow developments closely and gradually make their security 'quantum-safe'.

EU CYBER RESILIENCE ACT

The EU Cyber Resilience Act requires companies to design products and software in a more secure way and to take responsibility for vulnerabilities. That may sound like additional regulation but it also yields an important benefit: greater trust among customers, suppliers and investors. Like the AI Act, this legislation aims to provide frameworks and certainty. The CRA is not all-encompassing and its strength will depend on enforcement, collaboration and innovation.

"Despite rapid digitalisation, too many companies are standing still in terms of cybersecurity. We see that smaller players in particular lag behind due to a lack of knowledge, a weak security culture and the mistaken belief that they are not an interesting target for cybercriminals. This is high-risk behaviour: a hack doesn't just cost ransom but also undermines revenue, continuity and competitiveness. The impact is always far greater than the investments required. Beyond basic measures such as password policies and firewalls, we advise companies to put in place a risk analysis, a clear roadmap and advanced detection measures. A layered approach remains the best defence."

Sam Nelen, Partner Risk Advisory
BDO Belgium

DOS AND DON'TS FOR BUSINESS LEADERS

DOS

- Do: plan crisis drills so teams know what to do in the event of a hack or data breach.
- Do: screen suppliers and freelancers for their cybersecurity measures.
- Do: invest in employee awareness as human behaviour is often the weakest link.
- Do: familiarise yourself with European initiatives such as the Cyber Resilience Act, which provide guidance and strengthen trust.

DON'TS

- Don't: assume that you are not a target because you are 'just' an SME. Hackers know that smaller companies are often less protected.
- Don't: place blind trust in technology. Human reflexes and common sense remain indispensable.
-