Deloitte.

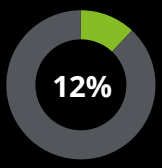
Cyber security in the Netherlands: a responsibility we share

Dutch cyber security survey

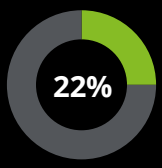
Cyber security is continuously in motion. It has to be in order to keep up with constantly changing cyber threats. At Deloitte, we were keen to know where Dutch organisations currently stand with respect to cyber security. What they are worried about, what their goals are, and what is needed to achieve success. How they see the future. And above all, their thoughts on making the Dutch digital ecosystem safer.

The ultimate goal of cyber security

25% of the respondents believe the ultimate goal of cyber security is to protect people and assets from harm, misuse and abuse, but there is some range of opinions



want to make the digital ecosystem a safer place



find protecting the vital assets of the company the most important objective

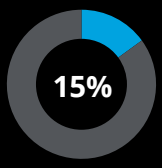
Larger organisations can best afford the luxury of fighting for the interests of society as a whole

"The Financial Sector agreed not to compete on cyber security years ago. Instead, banks are sharing information and helping each other with best practices. Other sectors have been following this example. By doing so, all can offer clients, themselves and society the best possible protection."

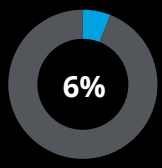
Kevin Jonkers
Director Cyber Risk Services

Cyber strategy

92% of organisations stated to have an up-to-date cyber security strategy; **80%** have a separate annual plan with a roadmap

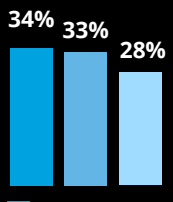


of organisations are already working on a next-level mature strategy



of organisations are starting with setting up their strategy

Key success factors for achieving cyber security goals:



- Compliance
- Operations
- Communication & training

"A cyber security strategy must first be realistic and workable for the rest of the organisation. For next-level maturity, it must be embedded in primary processes and the overall strategy."

Robbin van den Dobbelsteen
Director Cyber Risk Services

Cyber security on the executive board's agenda and the allocation of cyber security budget

42% of executive boards discuss cyber security at least every quarter, but **25%** of them do so once a year or less

The larger the organisation is, the more frequently cyber security is discussed at board level

Financial service providers are champions in board-level engagement on this topic

54% discuss cyber security at a board level at least once a quarter

Public sector awareness is significantly lower

28% are not aware of the frequency

"If CISOs start focusing more on securing emerging technologies, they can act as business enablers and strengthen the position of the company compared to competitors."

Dana Spataru
Partner Cyber Risk Services

61% of organisations allocate up to **11%** of the IT budget to cyber security

43% of the Public Sector do not exactly know how much they actually spend on cyber security

Sectors with relatively higher cyber security budget (as a % of IT budget)

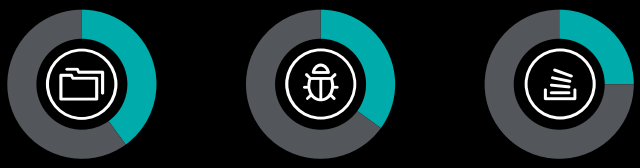
Life Science & Healthcare

Energy Resources & Industrials

Deep diving into our most commonly feared threats

Part of our survey focused on the results regarding anticipated developments on cyber security, (potential) cyber threats and the organisation's confidence in handling them

Most common feared threats are:



Data leakage (**40%**)

Phishing, malware or vulnerability exploits (**35%**)

Extortion of organisation's data (**25%**)

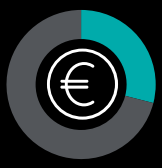
27% of the largest organisations (>10,000 employees) have an increased fear towards security breaches involving third-party organisations

"I don't believe digital threats are becoming more sophisticated overall, as easy hacks are still effective and lucrative. It's organisations themselves that are becoming more complex and losing track of their vulnerabilities."

Frank Groenewegen
Partner Cyber Risk Services

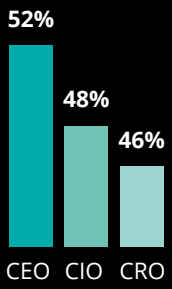
of the respondents are sure they would pay to get their data back. But opinions vary widely on this topic

Positions that most often choose to pay



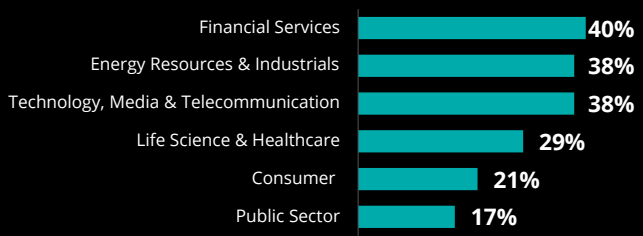
Only **29%** of the CISOs would pay

VS



Large organisations are less likely to pay to get their data back; the same is true for organisations in Public Sector, while those from Financial Services, Technology, Media & Telecommunications and Energy, Resources and Industrials are more convinced

By industry:



Towards a Dutch cyber security ecosystem

63% of respondents from large organisations with more than 10,000 employees see opportunities to contribute to a more resilient sector and a safer digital ecosystem

The surveyed **CISOs** leave little room for interpretation: **100% of these respondents agree** with this statement

The creativity, confidence and positivity in this regard seems to grow with organisation size. **These results highlight the evolution towards a safer and more resilient digital society**

"We need to exchange knowledge and collaborate together in order to keep our Dutch digital hub safe, to protect the privacy of our stakeholders and to safeguard the very functioning of our society."

Niels van de Vorle
Partner Cyber Risk Services

Development of the CISO role
Today CISOs often report to the CIO

49% Of the organisations agreed with their CISOs reporting to CIO

13% Agreed with their CISOs reporting to CFO

"The role of the CISO is changing from being "the department of no" to being a business advisor and enabler. A CISO no longer needs to rely on a deeply technical background. It's more important to be a people person."

Martijn Knuiman
Partner Cyber Risk Services

What gives the CISO headaches?

Managing too many organisational priorities simultaneously (**31%**)

Lack of integration of cyber risk priorities with business priorities (**28%**)

Inadequate governance across organization (**26%**)

Sign up for the full report