National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

The CSAN 2023 in a nutshell

June 2023

Due to interwovenness of processes in the digital ecosystem, everyone is at risk of experiencing a cyber incident, even if it seems unlikely. Furthermore, state actors use cyberattacks to achieve their geopolitical goals, extortion represents an attractive business model for cybercriminals, and new technologies such as AI bring along new threats. Those are some of the conclusions from the Cyber Security Assessment Netherlands 2023 (CSAN). The CSAN calls on organisations to expect the unexpected.

Principal findings

The CSAN 2023 concludes the following six principal findings.

1. The security of digital processes is and remains essential in our highly digitised society and is therefore linked inextricably to national security.

2. The digital threat for the Netherlands remains as high as ever. That threat does however change continuously.

3. The strategic themes set out in the CSAN 2022 still fully result in complications for risk control.

4. Reduction of the imbalance between the digital threat and resilience referred to in the CSAN 2022 remains a major task.

5. Despite growing attention to resilience of Operational Technology (OT) as a building block of vital processes, there is room for improvement.

6. Digital risks demand a broader method of risk management and should be considered as an integral part of the risks to national security. Here, the angle of 'assume breach' (assume that there is a cyber incident) could be useful.

Reflection strategic themes

In the CSAN 2022, the NCTV identified six strategic themes that will be relevant to the digital security of the Netherlands in the coming years. These themes formed a substantive basis for the Dutch Cybersecurity Strategy 2022-2028.

The six themes are:

1. Risks form the downside of a digitised society.
2. Cyberspace is a playing field for regional and global dominance.
3. Cybercrime is industrially scalable, while resilience – for now – is not.
4. Market dynamics complicate controlling digital risks.
5. Coordinated and integrated risk management is still in its infancy.
6. Restrictions in digital autonomy also restrict digital resilience.

In the reflection upon these themes, several changes stand out:

- The additional digital security requirements that arise, inter alia, from new European legislation and regulations.
- The further hardening of geopolitical tensions.
- The insurability of digital risks is under pressure.
- The ever-increasing interwovenness within the broader ecosystem.
- The opportunity structure for cyberattacks formed by the digital ecosystem.
- One “new” insight is that digital risks are integral parts of a broader and complex array of risks and have some other special characteristics. As a result, digital risks require a broader way of managing than other risks.

Four national security risks

There are four risks to national security. They also apply to specific sectors and organisations and individual citizens.

1. Unauthorised access to information, in particular through espionage. Examples include espionage targeting communications within the central government or the development of innovative technologies.

2. Inaccessibility of (vital) processes, due to (the preparation of) sabotage of processes responsible for the energy supply, or from cybercrime.

3. Breaches of cyberspace, such as through the misuse of global chains of ICT service providers, the exploitation of internet protocols or the sabotage of cables.

4. Large-scale outages: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action.

Threat scenarios

The CSAN 2023 includes threat scenarios that can help organisations choose and deliberate in order to increase resilience. These scenarios point out the risks that arise from the fact that organisations are part of a digital ecosystem. Three fictitious scenarios show how an incident not only leads to problems within the organisation, but can also damage society or other organisations in the ecosystem.

The CSAN has been drawn up by the National Coordinator for Counterterrorism and Security (NCTV), in close cooperation with the National Cybersecurity Centre (NCSC). It is defined annually by the NCTV.

Read the entire CSAN 2023 online:
english.nctv.nl/latest/news/2023/07/03/cyber-security-assessment-2023-expect-the-unexpected