AS SEEN IN:
INNOVATIE NU | MARCH 2021

CYBERSECURITY

A WAY TO IMPROVE BUSINESS CONTINUITY IN DIGITAL TRANSFORMATION

In collaboration with:

The Cyber Partners

ADVANCED MANUFACTURING CENTER

ISSN 2772-428X

CYBER SECURITY

> *Cyber security is not a goal, nor will it ever be. Business continuity, however, is.*
>
> *Accordingly, cyber security is a topic that should be addressed every once in a while. Cyber security - digital safety & security - is a precondition for safely using the opportunities digital transformation offers.*

Nowadays entrepreneurs face cyber threats on a daily basis. Measures must be taken and investments should be made to defend your core business against these threats.

However, where to start?

The best way to deal with cyber security depends on the type of company. Some examples are:

- Large enterprises have a (non-executive) board which should monitor the cyber resilience of the organisation, as is stated in the Dutch 'corporate governance code'.

A WAY TO IMPROVE BUSINESS CONTINUITY IN DIGITAL TRANSFORMATION

- Fortunately, most large enterprises have invested in technology, processes and education of their staff. Yet, they typically remain vulnerable through their connections with business partners.
- In some cases these companies need to find an effective strategy to regularly update their ways to stay ahead of the newest threats.
- Medium-sized enterprises usually do have some measures in place, but in about 60% of the recent assessed cases, the compliance to these measures depends on only a few staff-members that recognise the importance.
- Cyber security threats to smaller organisations are similar to enterprise-sized risks. Without large IT and security teams, these organisations depend on external technology and cyber security providers. Asking the right questions not only helps to assess the company's cyber risk better, but also evaluate the right security partner for you.
- In specific industries e.g. the defence, or medical industry, specific cyber security standards have been developed.
- When running an international business, international and foreign laws could influence your cyber security.

Since the start of the COVID-19 crisis, the urgency to invest in cyber security has increased tremendously.

Building and growing awareness of cyber threats and security should be a continuous process in every organisation. Seeing the ongoing developments in this area it is necessary to keep on learning continuously as well.

Fortunately, no one needs to start from scratch. We have collectively gathered quite some experiences over the last couple of years.

Let us look into the example of so-called "phishing" mails. Experience has taught that phishing mails can be identified by a combination of the following three characteristics:

1. **The sender is a person (CEO, "CEO-fraud") or an organisation (tax office, bank) with authority**
2. **The recipient is a staff member with digital authorisation power, e.g. someone who is authorised to carry out a financial transaction or software update.**
3. **There is always a means of (psychological) pressure involved, such as time. "You need to act quickly", "Pay before tomorrow, otherwise..."**

How to train the workforce to recognise these types of threats?

And, when being recognised, what should people do?

Specifically for industry 4.0 there is more to know. Production should never be interrupted. And it is highly important that the data received from partners and clients are protected in your organisation as well. Yet, in most manufacturing environments, not all updates and upgrades are implemented automatically, even if they are available.

Industry 4.0 environments are more dependent on their technology supplier. What questions should be asked and what can be done in your network architecture?

Cyber security is not the goal, but a way to be able to stay in business.

Did you know?

- that since the start of the COVID-19 crisis, the amount of cyber attacks has increased five fold?
- that remote working has significantly increased the dependency on digital infrastructure?
- that most cyber incidents (80%) are (unkowingly) caused by own staff or from their account?

The human factor is the most critical aspect in keeping your business safe.

Evelien Bras

Director

The Cyber Partners

The Cyber Partners is founded by Evelien Bras.

Evelien has finished her degree in Computer Science more than 25 years ago. She started her career implementing solutions in securing international telecom infrastructures. She turned to the aerospace and defence domain leading innovation and public-private partnerships. Cooperation and cyber security became the key focus.

Nowadays, she is a non-executive board member in a multinational organisation in the automotive domain, guest lecturer at the University of Leiden for the part-time executive master Cyber Security, she chairs an assessment committee of NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek) and is recently appointed as director of FERM, an initiative to evolve cyber security in the Rotterdam harbour.

The Cyber Partners is a cooperation between professionals, focusing on the governance of cyber security within commercial organisations.

WORKSHOP

How to organise resilient digitalisation?

CYBER SECURITY Search

With examples of small, medium & large enterprises. The agenda:

- Governance
- Cybersecurity
- Privacy & Compliancy
- Standards & investments
- Ethics
- Awareness & the human factor

THE CYBER PARTNERS

Contact: **info@thecyberpartners.com**