THE FUTURE OF THE SECURITY DOMAIN: A BOARD LEVEL PERSPECTIVE

It's been a busy year in Europe's and the Netherlands' security domain. The notorious 'toeslagenaffaire' (benefits affair), the log4j incident and the tight labor market conditions have certainly left their marks. From our discussion with 15 directors of large organizations in the Dutch security domain, we can conclude that security organizations' ability to change has been crucial in the bygone two years. Now that a new balance has to be struck between old and new ways of working, we have to make sure that security is safeguarded in all circumstances. This effort results in all kinds of challenges – and as we speak, Europe is already dealing with yet another crisis. The question remains what the security domain will look like a few years from now.

Main takeaway from our discussion is that the digitalization of society has penetrated every aspect of our lives and work. Digitalization no longer has a merely supporting role, we have become wholly dependent on it. Take our personal lives, for instance: ordering drinks at a bar has become a question of scanning a QR-code or using an app. Shopping, lectures and meetings have become online activities – or at least hybridized ones. And the developments are not only apparent in society; digitalization also has a big impact on the security domain. Here, work has shifted from a mostly physical way of working towards a new, hybrid way of working.

Innovation in the security domain: 'A person says no'

Innovation is still an important topic in the security domain, with technological capabilities an important driver for renewal. This often results in great innovations, but at the same time can sometimes turn out badly. The directors we spoke to all stressed that innovation and renewal should always be people oriented.

The benefits affair is a harrowing example of what can go wrong. In this affair, thousands of parents were unjustly labeled as fraudulent, due to an AI-based, discriminatory risk model. This affair, the effects of which are felt to this day, serves as proof for the notion that innovation should always retain a human – and humane – touch. As discussed in chapter 9 of this TiS report, unbiased Artificial Intelligence as of yet doesn't exist[1].

The directors we interviewed reaffirmed the importance of human intervention in the execution of processes. Processes today are mostly digitalized; with new techniques, they will become wholly automated. This automation is a promising development, but humans must always have the final say. Computer says no should no longer occur; when 'no' needs to be said, it should always be a person saying it. Innovation and automation, then, should never go without a solid analysis of ethical aspects. New processes and innovations should always be ethical by design.

Citizens first, in an information-driven world

A successfully matured innovation within the security domain is the use of sensors and data in policing. The quick, successful tracking of the suspects in the murder of Peter R. de Vries on July 6th, 2021, is a good example. Thanks to security cameras of citizens and companies, automatic number plate recognition (ANPR) and supplementary witness statements, the police was able to detain the getaway

car only an hour later, on the A4 highway at Leidschendam. It's an important example of the added value of information-driven working for quick detection. A traditional investigation, aimed at apprehending suspects, would have taken up a great deal of resources; resources that, thanks to information-driven working, can now be used to build the case, or contribute to other investigations.

The directors we spoke to recognize the crucial role of data management for the correct functioning of their organizations. Gathering, processing, and deploying data requires a complete ecosystem. And this, in turn, requires a clear description of internal processes and chain processes, and of data gathering methods. According to directors, ethics, privacy, and security are crucial considerations in drawing up such a description. They are fully aware of the fact that data gathering, and processing have their drawbacks, and may result in the general public's perception that they are living in a police state.

Directors expect that people, vehicles and weapons will only get smarter. Increasingly fitted with sensors, they will become a breeding ground for information-driven working. New developments revolving around technologies such as cloud and AI will serve as a further impulse. Here, too, we will have to put citizens first and keep ethical aspects top of mind.

In this regard, directors point to the growing need to draw smart comparisons between different organizations' data, without exchanging actual information. Their experiences point out that this is not always easily done, due to legislation such as GDPR. In response to this, there is a growing determination to collaborate, and collaborate more effectively, between both private and public organizations in the security domain. In achieving this, differences in IT maturity can be problematic. Legacy IT is currently hampering digital collaboration.

Digital security figures prominently on directors' agendas

The world is changing. Both for citizens and for organizations in the security domain. But crime and outside threats, too, are changing – migrating from the physical to the digital world. Already since 2012, traditional crime is waning, and online crime is on the rise[2]. Covid 19 has exacerbated this development, because of the large increase in online activity, and growing insecurity and lack of trust in information, institutions, and the government. The digital resilience of the Dutch people is being tested.

We can conclude that digital security is lagging behind digitalization itself. It urgently needs extra attention. Directors indicate that through their organizations' CISOs, security figures prominently on the board agenda, and this urgency also transpires from our interview with Hans de Vries (chapter 1). The Log4J incident of end November 2021, in which a vulnerability of this widely used software was exploited to execute cyberattacks, serves as further proof for the urgency of the matter. Mitigation of the risks incurred by this software was the security domain's top priority.

Directors tackle challenges in digital security in different ways. Budget is reserved to safeguard software and infrastructures, and keep them secure. Security is a by design feature of newly developed systems, and the same goes for privacy and ethics. On top of that, teams are formed as flying squads, and deployed wherever and whenever they are needed. The opposite is also true; directors indicate that successful track security track records of services are not celebrated in any way, to avoid drawing the attention of bad actors. Progress, then, is certainly being made.

With the rise of distributed working, new security issues are emerging. How can you make sure that co-workers can work at home safely and securely? That sensitive information is destroyed? And how are the related responsibilities governed? Currently, answers to such questions are not always readily available – but they are being discussed at board level.

The search for talent

Corona has irrevocably changed the collaboration between organization and co-workers. During the lockdown, many organizations shifted from a traditional office culture, via a virtual culture, to a hybrid work culture. According to directors, this new way of working is here to stay – caused in no small part by the ongoing trend towards more sustainable business practices. Continuing business as usual in this new context does require an extra effort. As an added challenge, organizations need to attract and retain new professionals and new expertise, in order to keep on adding value to the security domain. In a tight labor market, with demand for new talent far outstripping supply, organizations in the security domain often have to compete with other organizations – both private and public. And having to vie for the attention of the same, dwindling group of potential new co-workers, does not seem like a sustainable strategy in the long run.

Many of the directors we interviewed agree that organizations' ability to grow and innovate depends on their ability to attract sufficient - and sufficiently skilled - co-workers. Organizations need to anticipate the point where they are no longer able to attract qualified external personnel, and assess the own organization's capacity to train or re-skill existing personnel. In this, strategic personnel planning (SPP) may be of help.

At the same time, directors point out that innovation also plays a part in attracting and retaining co-workers. Starting with the development process, time and money are reserved for innovation; based on best practices, for instance through the SAFe network. The expectation is that such efforts will result in cross-pollination within the organization. New ideas will be shaped and new experiments conducted, with new technologies – even without the explicit expectation that the results will immediately be implemented in work processes. Money is reserved for the further development of the most promising ideas. Such efforts always have to revolve around the co-workers, and not around productiveness. It's a delicate balance.

Conclusions

Every director we interviewed across many organizations within the security domain confirms the big picture. Digitalization has accelerated and shifted from a supporting role into an executive role. With that shift, digitalization has become crucially important for any organization. To drive further digitalization, innovation needs to be embedded in organizations' development processes, in order to allow for continuous renewal. On top of that, innovation can help organizations to attract and retain co-workers. On the other hand, organizations need to stay aware of citizens' interests; just like security and privacy, ethical aspects are essential and require a by design approach. As a result of the shift from a physical towards a hybrid society, crime and threats are evolving, too – a development that calls for new answers.

In the coming decade, digitalization will continue to expand, and the security domain will continue to adopt new measures towards further professionalization. This will result in a transformational process for all organizations – both in the way they execute primary processes and in the design and execution of supporting processes. Every living system – including our society – needs a certain amount of dynamism, in order to adapt to changes. But systems also need stabilizing elements, to avoid disintegration. A security domain that keeps on professionalizing is such a stabilizing element. A safe haven, in disruptive times.

About the authors

Marcel Kordes
Director public sector

Marcel is responsible for the public order and security domain within Business Technology Services. He has more than 15 years of work experience in this domain.

Erik Staffeleu
Senior director public sector

Erik Staffeleu is senior director in the public sector. Among other things, he is responsible for the Security and Justice Chains expertise group. Erik is a change expert, and an experienced advisor within the security domain.
His assignments mostly revolve around strategy design and organizational development.

[1]Unbiased AI is a lie
[2]https://www.cbs.nl/nl-nl/nieuws/2022/09/minder-traditionele-criminaliteit-meer-online-criminaliteit