Interview met Anne Hännikäinen

# Zichtbaarheid effecten informatiebeveiliging en heldere communicatie naar topmanagement essentieel

23 april 2019

Jean Jacques Bistervels

**Informatiebeveiliging was tot voor kort nogal eens een ondergeschoven kindje in veel organisaties. Gelukkig is er de laatste jaren ook in de directiekamer steeds meer aandacht voor en krijgt de CISO-functie erkenning als cruciaal voor de bedrijfsmissie. Wij kregen de kans om de CISO van een groot mediaconcern en leverancier van educatieve oplossingen en systemen te interviewen. Anne Hännikäinen heeft ruim negentien jaar ervaring in de IT-wereld en binnen wereldwijd opererende, internationale fysieke en virtuele organisaties.**

Anne heeft functies vervuld binnen security- en IT compliance-management, consulting en auditing van leveranciers, waaronder ook cloud-dienstverleners. Ook was ze betrokken bij diverse overname-, fusie- en verkooptrajecten van bedrijven of bedrijfsonderdelen. Sinds drie jaar is ze verantwoordelijk voor de beveiligingsorganisatie binnen het Sanoma-concern. Ze woont in Finland, maar haar werkterrein ligt in alle landen waar Sanoma vestigingen heeft. Momenteel is dat België, Finland, Polen, Zweden en Nederland.

Anne heeft nog een half jaar in Amsterdam gewoond en kent hierdoor een paar woorden Nederlands, maar het interview hebben we toch in het Engels gehouden – een taal die ze vloeiend spreekt. De weergave van het interview hieronder is dan ook in het Engels.

## Anne, Sanoma is active in a number of European countries, in the industries Media and Learning / Education and comprises a number of more or less semi-autonomous companies within a corporate group structure. What is in your opinion special about being a CISO in a multi-country and multi-industry organization like Sanoma?

'Information security challenges are, to a great extent, shared regardless of whether your company is multi-country or not as the internet is global. However, I enjoy working in a

diverse, multi-cultural environment. Professionally, my main experience is from working in large multi-national companies with presences in many countries. Through my work, I have become familiar with cultural differences but also understood that diversity is a major asset for the company. Several stints outside Europe – two years as an expat in Singapore, for instance – have deepened my cultural awareness. The main lesson I have learned is never to assume anything. This understanding is equally relevant in any culture. Clear instructions and rules are important, not only in Singapore but also in other countries.'

'Clear communication and change management are extremely important in information security implementation, especially as information security is relevant in different ways to so many business processes. Without clear guidance, employees may, for example, find it difficult to identify the information security concerns relevant for their work, and the processes needing adaptation. It´s vital for each employee to be aware of information security as they are the first and best line of defence against malicious attacks.'

'It's a business decision how and whether acquired companies should be integrated into the parent company. If the acquired company stays semi-autonomous, we can gain the necessary assurances for information security through alternative methods. Sometimes, we can offer our security product portfolio to the acquired company, making the integration of the acquired company irrelevant in terms of information security. Alternatively, a semi-autonomous company could also have its own security resources and tools or we may need to create a hybrid model. The information security approach will always be aligned with whatever business approach is chosen.'

'An information security improvement program is needed as well. These programs are based on security assessments of the semi-autonomous companies to create a security baseline, understand the existing maturity levels and identify areas for improvement.'

## Sanoma also owns a newspaper in Finland. Are you also involved in the more technical automation aspects linked to, for example, running a printing facility as part of the Media organization?

'Certainly; we are involved with the technical automation security aspects of our printing facility, but at the same time, we are focusing more and more on digital media automation in the Cloud. Sanoma is an intensive user of cloud services, especially IaaS services such as AWS with their own security challenges. We are not concerned with the security aspects that AWS is responsible for, but rather with those that we as customers are. We need to, for example, ensure that our development teams are trained in how to configure AWS to fulfil our own privacy and security standards. The integration of Sanoma Standards has also been our focus when designing Development Security Operations (DevSecOps)

awareness training courses – DevSecOps means integrating security practices within the DevOps process.'

## Board meetings and management meetings are important for gaining insight. Do you have access to the Board or management teams about matters that may be technical in a way they understand?

'Clear communication skills are becoming all the more important as cyber security professionals are invited to join board level discussions more and more often. 'Osmo A. Wiio, an academic and member of the Finnish Parliament, nailed the challenge by saying "Communication usually fails, except by accident". I try to be as clear as possible in my board and management level presentations. Although sometimes if there are questions I had not prepared for my answers may not always be as clear as my audience expects. Some topics in cyber security can be extremely complex, and consideration is needed to determine what is relevant and what is not. But communication can always be clearer; it´s an on-going process of development. It is also becoming more important for IT security professionals to strengthen their business understanding. I am, for example, enrolled in the Global Leader program at Aalto University to ensure that I have broad and current understanding of best business practices.'

## Sanoma is doing a lot of its business in the cloud, with cloud solutions, or is migrating 'classical IT applications' to there. Can you indicate how this movement changes your work or the work of information security within Sanoma in general?

'Sanoma was an early adopter of cloud services, and the strategy has been to also adopt cloud services broadly. As such, Sanoma has developed its use of cloud services now for some time. One of the lessons I have learned is how crucial it is to focus on change management activities concerning important initiatives. Looking back, it would have been helpful to put more effort into identifying change agents on time and communicate clear messages about major initiatives.'

'In general, cyber security awareness in development teams requires strengthening Privacy and Security by Design, as well as focus on secure maintenance by implementing DevSecOps. Showing the effects of cyber security measures per service is important to ensure the service/product managers, and development teams know their existing status and can plan possible fixes based on factual insight. To provide sufficient insight, integrating information from different kinds of environments is a challenge on its

own. There may be so-called "lift and shift" environments which do not use cloud-native solutions. There may also be environments which are already in serverless mode and therefore require a different kind of security measures than most of the existing environments. Making visible the cyber security level to everyone and providing clear guidelines requires cloud security-specific knowledge from the cyber security team as well as from the development team.'

## What security policy is in place within your company – while it may be specific for your industry, its basic principals may be helpful to other companies?

'Yes, many companies, Sanoma included, use information security standards such as the ISO 27001 framework and the ISO 27002 best practices. However, there may be some insights from Sanoma´s broad adoption of cloud services. If you use cloud services, you should, for example, understand the division of roles and responsibilities between your company and the cloud provider. Ensure privacy and security compliance on the side of suppliers through contracts as well as capability and willingness of the supplier to protect your company data and assets. Also remember your own security role and required competence level. Ask help from your cyber security department as well as from the cloud provider. Many cloud providers offer cyber security best practices guidance and training courses that may be of interest. Cooperation to create better protection against cybercrime is the interest of both parties.'

## What do you perceive as the future's biggest information security challenges to you and Sanoma its Operating Companies?

'Sanoma´s challenges are probably quite similar to the challenges of other companies. Awareness has always been the main challenge in cyber security, and that´s unlikely to change anytime soon. At the moment, certainly concerning are cyber-attacks aimed at states which may result in collateral damage to companies, even when they are not the intended targets. The example of Maersk is quite well known. Such attacks are quite often very sophisticated, which raises the bar for protective measures.'

The audience of our professional magazine consists of both internal, external IT-auditors. What role do you see for an IT-auditor, either general or specialized in information security, in your area of work?

'I would like to see auditors who can also make assessments about the technical security implementation – assessments of, for example, the configuration of anti-malware software or SIEM solutions. I have seen some very interesting configurations on paper, even though on closer inspection nothing really was in place in practice. Excellent documentation does not guarantee that the implementation was actually based on that documentation. However, high-quality documentation does ensure that someone in the company could know how IT security measures should be implemented correctly. Due to changing and complex environments technically capable auditors are needed more than ever.'

*Informatiebeveiliging krijgt ook bij Sanoma ruime aandacht en Anne heeft dan ook een overvolle agenda. Hierdoor was het nogal een uitdaging voor haar om ruimte te maken voor een afspraak voor het interview. Uiteindelijk bleek de enige manier om de zaak rond te krijgen een schriftelijk interview te zijn. Ondanks deze – letterlijk – afstandelijke aanpak hebben we een informatief verslag kunnen maken. Net als wij vindt Anne deze werkwijze lang niet ideaal, maar in elk geval kan ze langs deze weg haar internationale inzichten in recente ontwikkelingen en de rol voor de IT-auditor met onze lezers delen. Samengevat is haar belangrijkste boodschap dat een heldere communicatie richting topmanagement essentieel is, en dat het gebruik van de cloud ook weer andere eisen stelt aan het pakket van kennis en vaardigheden van de IT-auditor.*

## ir. J.E. (Jean-Jacques) Bistervels | Informatiebeveiligingsmanager en privacyspecialist bij Sanoma.

Voordat Jean-Jacques begon bij Sanoma, werkte hij ongeveer twintig jaar in verschillende GRC & audit-functies in de zakelijke dienstverlening, in de farmaceutische industrie en in de financiële dienstverlening. Veel van deze bedrijven en voormalige klanten zijn actief op sterk gereguleerde markten. Jean-Jacques heeft een brede interesse in zowel zakelijke, regelgevings- als technische onderwerpen. Sanoma is een mediabedrijf, uitgeverij en producent van leer- en opleidingsplatforms en -materialen voor scholen en universiteiten. Het bedrijf is actief in verschillende landen, waaronder Finland, Zweden, Polen, België en Nederland.