# Bernold Nieuwesteeg
# Cybersecurity

**This summer I celebrated the fact that I defended my PhD thesis. My friends gave me a present: a *single* ticket to Bhutan. I am excited. It is unknown territory for me. To go somewhere where I have never been but also not knowing when (or whether…) to return. I will fly this December.**

During the second half of the previous century, we all got a single ticket. A single ticket into digitization, the Internet and the World Wide Web. The further integration of our analogue lives with the digital world will inevitably continue. It has brought us unprecedented prosperity and empowerment. But also unprecedented downsides, such as a vast increase in digital insecurity, posed by ransomware, DDoS (Distributed Denial of Service) attacks and data breaches amongst others.

We are all entering unknown territory of the digitization and its downsides: cyberinsecurity. Everyday. It does not surprise me anymore that I often hear that key professionals in the industry, such as CIOs, lawyers and civil servants sometimes feel overwhelmed by the vast amount of possibilities to secure the Internet.

Indeed, there are many tactical choices to make: Which security measures should I take? Should I notify this data breach? How to be compliant with the General Data Protection Regulation (GDPR)? Should I purchase cyber insurance?

A lack of options is not the problem. The cybersecurity and privacy industry are growing and there are all kinds of goods and services to use, from legal advice to monitoring and detection systems. But instead of drowning in the operation of 'running cybersecurity', like a vacuum cleaner that collects all the bits and pieces of dust without thinking, society is in desperate need of zooming out and taking a birds' eye view.

What we need is intelligent cybersecurity strategy. A perspective to work towards in order to choose which tactical measures to take: which dust to clean, and which dust to ignore. We cannot do everything, especially because cybersecurity expenditures will rise exponentially in the future caused by future digital waves, such as the Internet of Things, robotics and artificial intelligence. We need to determine how many locks we want on our digital doors.

That's what kept me awake at night for the past four years when writing a PhD thesis that is now called 'the law and economics of cybersecurity'.

So what should we do, what should be the vision? Well, first we must acknowledge that cybersecurity is largely an economic problem where access to the right information is both vital and often absent. Hence, the stimulation for a diffusion of the right information is paramount.

Please give me permission to return to June 2017 when I wrote the final words of my thesis. The Wannacry and NotPetya cyberattacks dominate world news and their impact is colossal. Wannacry infects over 300,000 computers. NotPetya disrupts a quarter of the Rotterdam harbour for six days and its total cost estimations exceed €100 million. The world sees, more than ever before, that cybercriminals can relentlessly punish suboptimal security.

Wannacry and NotPetya also show that there is a problem with information in cybersecurity. How can it be that some organizations suffered huge amounts of damage while others suffered hardly any harm at all? Apparently, Telefónica, FedEx, Deutsche Bahn, Maersk, DLA-Piper and Vodafone and many other organizations that were hit in these sunny days in June did not install the right patch that could have done the job (and which was already available for a few months). But was it really as simple as that? Large organizations have to install tens of thousands of patches per year. Installing them all immediately would significantly hamper business availability and continuity, possibly more than the attacks they are preventing. An appropriate cybersecurity strategy is not straightforward and hence, organizations have to learn from each other.

Naturally, Wannacry and NotPetya are mere examples of cyberinsecurity. But they certainly demonstrate the importance of my studies' contribution to a cybersecurity strategy. Namely to stimulate a diffusion of the right

information about the nature of cyber risk and the return on investment of cybersecurity expenditures.

On a macro scale, currently, society lacks sufficient actors and institutes that can contribute to the creation and diffusion of information in cybersecurity. We must constitute a 'cybersecurity information diffusion' agenda for university, government and industry. Each party within this 'triple helix' has different roles, responsibilities and tools to stimulate information diffusion.

*Government* can adopt legislation to stimulate information diffusion, for instance a data breach notification obligation. *Industry* innovation can in itself result in incentives for organizations to better diffuse knowledge, for instance cyber insurance. And the *University* helix can scrutinize the deeds of government of industry on their societal effectiveness, for instance my piece of work.

The deployment of the individual tools available to these three parties combined with their mutual cooperation will yield the most fruitful results.

Hence, in my thesis I came up with solutions for university, government and industry that could lead to smarter investments in cybersecurity. I studied new legal instruments, such as the possibility of insurance against cyber risks, the opportunity for mutual insurance by means of 'pooling' and the data breach notification obligation in the GDPR.

Let's discuss this data breach notification obligation first, which is part of the GDPR. A crucial element for the notification obligation to function is a clear notification threshold. When this threshold is not clear, organizations will notify every little data breach threatened by high sanctions. This leads to notification fatigue and unnecessary administrative and communication costs. However, a well-tuned data breach notification obligation can provide the necessary information diffusion about the cyber risk 'coping strategy' of organisations. One should however be aware that the social effects of any data breach notification law depend upon the actions taken by the Data Protection Authorities (DPA) after they have received the information on data breaches. If by the end of the day notifications would merely end up in a digital drawer at the DPA and no further action is taken to promote cybersecurity, then obviously the entire notification obligation would only be an extremely costly exercise without any social benefits as far as improving cybersecurity is concerned. This necessity for action points at the crucial role to be played by the DPAs to make the EU data protection breach laws a success.

Secondly, there is a lot of potential for improvement regarding the cyber insurance market, especially for SMEs. For instance, I requested ten cyber insurance policies on behalf of six organizations. It turned out that most insurers do not require a certain base level of cybersecurity before providing the insurance. The insurance policies are also too complicated for SMEs. There are simply too many differences in premiums and policies and it is hard to determine the value of each little difference. For example, it took me three months too thoroughly compare the ten cyber insurance policies that were offered. That's impossible for a small company. Solution? A basic insurance coverage could for instance stimulate efficient comparison between insurance companies.

And last but not least an unconventional solution: a pool for organizations that mutually shares their cyber risks. A kind of 'Broodfonds' for cyber risks: organizations have a share in each other's cyber risk. Hence, if one participant experiences a cyberattack, other participants contribute. This 'share' stimulates information diffusion, because one has an incentive to reduce damage at other organizations in the pool. I have analysed the feasibility of such a cyber risk pool together with several higher education institutions.

Data breach notification obligations, cyber insurance, a cyber risk pool. It is all hands on deck to keep up in the unknown territory of the future waves of digitalization.

**About the author**
Bernold Nieuwesteeg is director at the Erasmus University Centre for the Law and Economics of Cyber Security (CLECS) and partner at CrossOver. CrossOver is an innovation and action agency focused on solving the shortage of skilled technicians in the Netherlands.

*Photo: Arenda Oomen*