ASSESSING THE CYBERSECURITY RISK

Bart Groothuis is a Dutch politician serving as a Member of the European Parliament since 2020. He is a member of the Dutch conservative-liberal People's Party for Freedom and Democracy and is the Rapporteur on Europe's cybersecurity directive, NIS putting his years of experience in cyber security into legislative practice.

INTERVIEW BY
JENNIFER BAKER

What are the most prominent cybersecurity threats? Have these changed as a result of the war in Ukraine?

'Well, it's always good to start with Adam and Eve, because the cyber threat is always evolving. I think that the cyber threat has actually evolved significantly because of COVID already. We saw a doubling of the number of incidents in my home country in 2019, and according to the FBI, a tripling in ransomware worldwide in 2020.

In 2021, we saw new spikes, and now, in 2022, we are being overloaded by the numbers of incidents across the Western economies. Worryingly, a majority of the ransomware gangs have their activity or are being nurtured by the masterminds in Russia. It is not just a criminal problem therefore, it is also a foreign policy instrument for the Russian state: weakening the Western societal infrastructure. Weakening the way we earn our money. And that is not just a technical problem. It Is not just a problem of insurance or cybersecurity measures. It Is also a diplomatic effort that we should lay on the table and that, I think, is the phase that we're in right now.

Now, the security factor has evolved significantly in Europe. We see companies across sectors being attacked significantly, with demands of between 1.4% and 2% of their yearly revenue. So it's a significant threat by only a couple of gangs costing billions! As a politician, I must say it is just unacceptable that we tolerate this, that a couple of gangs are getting into our economic structure and making us bleed every day. That's why I'm in Brussels making new legislation as a rapporteur on Europe's new cybersecurity legislation.'

How has demand for cyber-related insurance coverage changed since the start of this year?

'Well, I see insurance as a top up, as something extra, as a dessert in a good dinner. But as a basis, of course, you need a good meal. And the good meal is of course, good cybersecurity measures such as basic hygiene, password hygiene, two factor authentication, good >

> ***the actuary has a crucial function in protecting and guarding our society***

backups, etc. That's what will be demanding for the majority of the 160,000 new entities across Europe that will be assigned in this new legislation that I'm drafting. And these 160,000 entities will be heightening their cybersecurity posture in general. But there's also liability being introduced in this legislation. And guess what – the liability is 1.4% to 2% of their yearly revenue!

The philosophy is, you either give in to ransomware gangs because your cybersecurity wasn't that good. You pay a fine because your cybersecurity wasn't that good. Or, guess what, you invest in cybersecurity, because that's what we want – it's a waterbed effect. In the US, which is now introducing new emergency legislation, we can see a waterbed effect, so the hackers would rather go to Europe than to the US if you would heighten the posture there.

Now, back to the question on insurance. What I see in US insurance is that through legislation, CEOs are ensuring their cybersecurity posture. I think we could have something similar in Europe. I encourage companies to look at that because insurance companies don't have a large risk appetite – I guess that risk appetite is even much smaller than the legislation I'm drafting. So I see insurance as a dessert on a good meal and I therefore encourage companies to do it. Meanwhile with this new legislation, the liability to the CEO is also about encouraging entities – those 160,000 entities – to do something with insurance. Ask yourself, what are my crown jewels? How can I segment my networks? How can I monitor this? How can I lower the risk appetite and therefore lower the amount of money I spend on my insurance? That's very important.'

Are insurance policies appropriate or do we need to see more evolution as cyber activity grows? Are war and terrorism exclusions still common?

'Let me first start with the duality of the security legislation in general that Brussels is working on. We have two main directives coming through in the next month. The first is the Network and Information Security (NIS) Directive, which is in the digital domain, and I'm the rapporteur on that one. But there's also the Critical Entities Directive, and that is about the physical security of critical infrastructure. But the annexes, or let's say the entities, overlap 100%. So it's very interesting to see that Brussels is working both on the digital and the physical security of these entities. Now, I think that in general, you could say that whenever there's an act of God, an act of terror, an act of nature, that there is a certain responsibility there for governments to backfill that risk.'

Looking to the future, the so-called NIS2 Directive is an overhaul of what was the original NIS. What are your expectations and hopes for the outcome looking to the medium or longer term? What would you like to see as the legacy of these new instruments?

'Well, that's the best question. If you ask me, we're in a new phase. We used to be more reactive. An incident would occur and you would see how we could share information. Evaluate how you could share it among the community and see what you can do to support others. Now, what I want to see in this new legislation is a more *pro*-active ecosystem. If you have knowledge on new domains or IP addresses that could be used by threat actors, then you have to have something in place to thwart it. You must operationally work with the information to do something including outside of your own network. I want us to move from reactive, seeing what incidents are there, and how can we prevent repeats, to asking how can we even prevent incidents from occurring in the first place with more preventive action, >

> *I think governments have been too lazy, to be honest*

BART GROOTHUIS

better servicing our entities, and especially thwarting those attacks before they even occur. We must do more to protect our entities and our businesses than we do now.

I think governments have been too lazy, to be honest. And I think that we're demanding a lot more from our entities and vital infrastructure to share information. I want that ecosystem to work. And unfortunately, it has to have teeth, so the CEO is now liable for the cybersecurity in their company, or entity, and this is very important, because otherwise nothing will happen. I've seen it and we've tried it before, and what we want now is to make sure that CEOs feel comfortable with cybersecurity because they have control. We can do it! It's not that hard, and we can do so much more to thwart about 90% of the incidents. I think we are in a new phase and will have the best legislation this continent has ever seen – we'll do our best.'

Finally, within that future, do you see a role for the European actuary as the risk manager of society?

'Well, first of all, if for example, an entity would say 'I don't feel comfortable with the liability I currently am exposed to,' then you need the actuary as a sort of middleman to come as an expert and say, what are your crown jewels? How did you segment? What is the policy that you have? If I were an attacker, I would do this or this or this. Because you want to be sure that you segment it, that you do something extra on top of the measures that I'm asking for in the new legislation being put forward.

So the actuarial advice is an extra, it's an add on, and it's very important to do so. And you can really reduce the bounties that people pay every month to the insurance companies. If you really look carefully at your network and work out what it is you actually want to protect, that is a very, very important job. So the actuary has a crucial function in protecting and guarding our society. And I wish you all the best and good luck with that because we're on the same page. We're fighting the same war. So let's make the best out of it.' <