INTERVIEW

BERNOLD NIEUWESTEEG

ERASMUS UNIVERSITEIT

The recent cyberattack at Odido has once again sharpened the discussion about how companies should deal with digital extortion. After a hacker group had made off with personal data of millions of (former) customers, Odido chose not to pay ransom. The company stated, as a matter of principle, that it does not negotiate with criminals and does not allow itself to be blackmailed. That choice, however, had direct consequences: the group Shiny Hunters began to publish the stolen data step by step on the dark web. Not everyone agreed with this strategy, which raises the broader question: how common is it that organizations refuse to pay after a cyberattack, and what actually is the wisest choice?

In this interview we discuss this with law and economics scholar Bernold Nieuwesteeg, who has been conducting research into cybersecurity for fifteen years and obtained his doctorate on this subject in 2018. According to Nieuwesteeg, the situation at Odido does not stand on its own, but forms part of a recurring pattern. In this interview we dive deeper into this, we examine how this cycle can be broken and which choices are needed in order to arrive at structural, sustainable change.

Question 1: In a recent article you describe a recurring pattern after cyberattacks, which you refer to as 'Groundhog Day'. What do you mean by this, and what do you consider to be the underlying problem?

BN: That term refers to the film 'Groundhog Day', in which a man wakes up every morning and relives exactly the same day. That image fits very well with the way in which we now deal with cyber incidents. There is a cyberattack, data are stolen, then the question rises whether payment must be made to prevent publication, and after that we move on again to the next incident. And then the whole debate begins again. It's good to have that discussion, but if that is all we focus on, then we should not be surprised that nothing changes in the future. After all, those attacks will keep coming. As long as we do not give companies other tools, incentives or reasons to secure themselves better, that pattern will continue to repeat itself. You can compare it with an epidemic: you can keep dealing with individual cases, but if you do not organize prevention, the situation as a whole does not change.

BN: The underlying problem, therefore, is that we now look too much at separate incidents, without taking sufficient structural measures. Companies make individual assessments, but in doing so they by no means always take the broader social consequences into account. As a result, we still too often look at cybersecurity as if it were only a technical issue, while in reality it is also very evidently an economic and policy issue.

Question 2: You approach cybersecurity not only as a technical issue, but also as a legal-economic problem. What changes concretely when we view it from that broader perspective?

BN: In that case, you no longer look only at what is technically possible, but above all at the question why certain measures are or are not taken in practice. Technically speaking, you can take a lot of measures to attain an optimal level of cybersecurity. But if a company does not have the money for that, or is not willing to spend the money on it, then it simply does not happen. That is a fundamentally different way of looking at the problem. Technically speaking, you can secure your house extremely well, but if you do not feel the necessity or find the costs too high, you refrain from doing so. A useful comparison is that of an open front door. Suppose that your front door is open and burglars come through your house into the neighbours' garden in order to steal everything there. If you yourself suffer little direct damage from that, then the incentive for you to close that door may not be very big.

BN: That is precisely the mechanism you sometimes also see in cybersecurity. The damage of inadequate security does not always remain limited to the company itself, but also affects customers, partners and society as a whole. From a legal-economic perspective, you therefore look at incentives and the distribution of responsibility. Ideally, you want the assessment that a company makes for itself to correspond with what is socially desirable. From economic logic, you then look at who could have prevented the problem most easily and at the lowest cost.

> The damage of inadequate security does not always remain limited to the company itself, but also affects customers, partners and society as a whole. From a legal-economic perspective, you therefore look at incentives and the distribution of responsibility.

Question 3: In the discussion surrounding Odido, the central question is whether companies should pay ransom after a cyberattack. You have previously indicated that this is not always the right choice. Why?

BN: The core of that is actually very simple: you do not want to reward criminals. The money they receive through such a payment is used by them to make new attacks possible. By paying, you therefore reinforce the business model of cybercrime. Naturally, there may be situations where a company has its back against the wall and the immediate damage of not paying would be enormous. In such cases, an organization might still consider paying. But especially then the lesson must be that you never want to end up in such a position again. You must prevent yourself from becoming so dependent on payment that you no longer see any other way out.

BN: At its core, the following applies: if we collectively were to never pay again, then these criminals would stop after some time. They do not do this for pleasure; they are not hobbyists. It's a revenue model. If the income disappears, then a large part of the attractiveness of this type of crime also disappears. That does not mean that reality is so black and white that you solve everything with one measure. But even if, for example, half of the companies stop paying, then in principle you halve the revenue for criminals. As a result, a country such as the Netherlands becomes less attractive as a target and those groups have fewer resources to set up new attacks. Economically, you can compare that with an enterprise that suddenly loses half of its turnover. A baker who sells only half as many rolls will at some point have to close branches or scale down. That is how it works in cybercrime too, although reality is of course more complex than such a metaphor.

BN: The problem now is that paying, for an individual company in the short term, sometimes appears cheaper than investing in good cybersecurity. The social costs of such a payment—namely maintaining the criminal business model and increasing the risk for future victims—are not fully taken into account by that company. As a result, a perverse incentive arises. In the worst case, an organization may even think: if I invest little in security and pay ransom from time to time, I may perhaps end up cheaper than when I invest heavily in cybersecurity on a structural basis. That is precisely the type of assessment that you as a society do not want to provoke. That is why those economic incentives are so important.

Question 4: If the starting point is that companies should not pay ransom, what legal instruments are conceivable in order to steer or enforce this and at the same time limit the negative consequences for victims?

BN: One of the most obvious instruments, which is actually lacking now, is a reporting obligation for ransom payments. That gives you insight into reality: how many payments are made, how often are they successful, and which ways are there to avoid payment precisely? At the moment, many of those payments take place in silence. As a result, we collectively learn almost nothing from them.

BN: A reporting obligation has multiple functions. First of all, it enlarges the knowledge base. If you know what is happening, you can also make better policy and offer support in a more targeted way. In addition, a reporting obligation raises the threshold for paying. You can then no longer make a payment entirely in silence without rendering account. That encourages companies to think better in advance about their security and about possible alternatives. Moreover, such a reporting obligation makes

it possible for the government or other bodies to offer support. A report need not only be a moment of control, but can also be an entry point for help: how can a payment still be prevented, which expertise is available, and which alternatives are there?

BN: Many companies fear reputational damage. They are afraid that customers will walk away as soon as it becomes known that they have become victims of a cyberattack. But research and practical experience show that that reputational damage is often less great than companies think. Consider, for example, major cyber incidents at enterprises such as Uber: despite the seriousness of such hacks, ultimately only few users actually stop using the service. Also in matters such as the one surrounding Odido, the number of people who actually switch is presumably limited. For many customers, switching is simply too much hassle, or they are still tied to a subscription. There is something else as well: consumers do say that they consider security important, but in practice they are often not willing to pay extra for it. They often simply choose the cheapest option. That too is an economic incentive that plays a role. As long as the market does not sufficiently reward security, companies will not always strive for the socially optimal level of cybersecurity. That is why it is all the more important that legislation and regulation adjust those incentives.

Question 5: In your article you emphasize the importance of an interaction between measures before a cyberattack (ex ante) and measures after it (ex post). Could you explain why that interaction is so crucial?

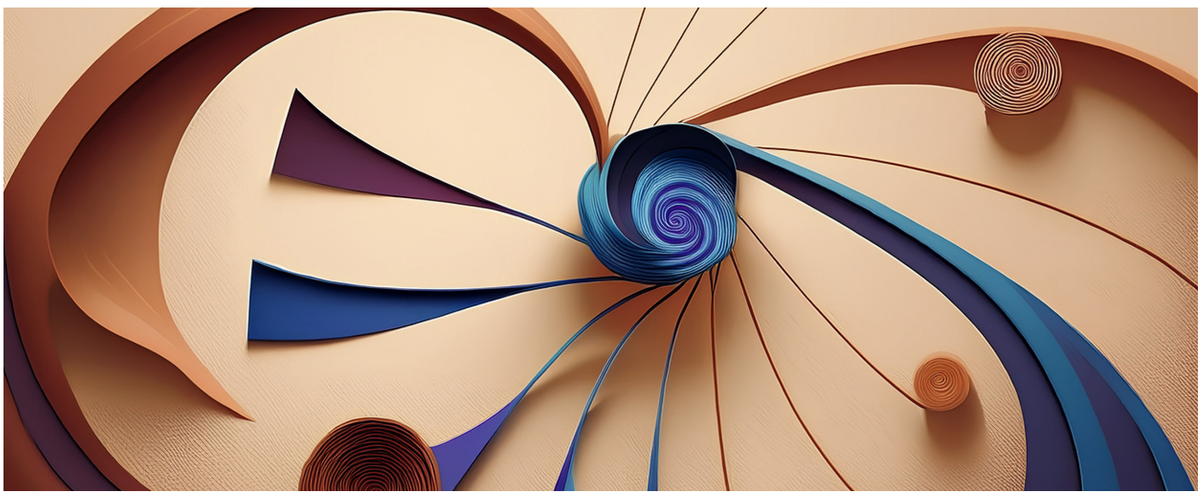
BN: That interaction is crucial because what you promote or discourage after a cyberattack directly influences what companies do before an attack. Take again the example of a reporting obligation for ransom payments. The idea behind that is not only that afterwards you get better insight into payments, but also that you raise the threshold for actually paying. If companies know they can no longer pay quietly, but must report it and may have to account for it, their assessment beforehand will change. Then they start thinking earlier about the question how they can organize their cybersecurity in such a way that payment is not necessary.

BN: When paying is no longer an option in the future, or in any event becomes a much more expensive and more difficult option, the incentive to invest in prevention beforehand increases. In economic terms, you can say that the risk then becomes more internalized. The problem of moral hazard also decreases: companies can less easily permit themselves to let risks continue to exist in the knowledge that afterwards they can still buy an escape route. That does not, however, mean that every company that is hit by ransomware automatically did not have its cybersecurity in order. It is not that simple. Cyber incidents can in principle happen to anyone. But it is true that the impact of an attack is often much greater at organizations that are less well prepared. Precisely for that reason, it is important that ex-post measures be arranged in such a way that they stimulate ex-ante investments.

Question 6: Where does the responsibility ultimately lie for tackling this problem?

BN: That responsibility lies with several parties at the same time. In the first place, companies themselves are of course responsible for the data of their customers and for the security of their own systems. But it does not stop there. We live in a strongly connected digital chain, in which suppliers also play a very large role. You can also see that reflected in the example of Odido and Salesforce. If a supplier gives clear warnings or recommends certain security measures, and these are not followed, then that is relevant to the question where in the chain things went wrong. Sometimes, therefore, the key to better security lies not only with the directly affected company, but also with suppliers, software providers or other service providers in the chain.

BN: For that very reason, the role of the government is so important. The government must think carefully about how it ensures that companies receive the right incen-



tives to organize their cybersecurity in the smartest and most effective way. That requires policy that looks not only at the individual company, but also at the relationships between suppliers, buyers and other involved parties. In addition, the government has an important task in facilitating knowledge-sharing. If information about incidents, vulnerabilities and effective measures is shared better, organizations can learn from that and mistakes do not have to be made again and again. A reporting obligation can help in that respect, but one can also think more broadly of rules or structures that promote cooperation in the chain.

Question 7: If we look at the current state of affairs surrounding cyberattacks and the approach to them, how do you see the future developing? Are you optimistic that we will get this problem better under control?

BN: Yes, I am actually quite optimistic about that. Not because I think cyberattacks will ever disappear completely, but because I do think that we as a society can become better able to deal with them. There will always be new types of attacks and criminals will continue to adapt. But that does not mean that we by definition have to lag behind the facts. If we make good policy, if we become more open about cyber incidents and if we share knowledge better with one another, then we can be stronger than the cybercriminals. Then we also need to allow ourselves to be blackmailed less easily. The key lies in the fact that we learn faster and adapt faster than the attackers. For that, it is necessary that we stop doing the same thing again and again and then hoping for a different outcome. That is precisely why that Groundhog Day metaphor is so apt. As long as we remain stuck in the same pattern of incident, panic, debate about paying and then simply moving on again, fundamentally nothing changes. The real task now lies with the government and with other involved parties to follow through and make policy that breaks that pattern. If that works, I am convinced we can bring this problem under much better control than we currently do.

About the Author

Bernold Nieuwesteeg is founder of the knowledge platform CyberSecurityBooster and board member of VNO-NCW MRA. He works on solutions to complex societal challenges, such as cybersecurity, digital autonomy and AI. He does not do this from a single discipline, but by combining roles as an entrepreneur, researcher, and creator. As a frequent speaker and columnist, he explains how digital transformation reshapes society.

> “The problem *now* is that paying, for an individual company in the short term, sometimes appears *cheaper* than investing in good cybersecurity.”