INSIGHT

Scripturient

Learning from the loopholes

> **Criminals seek opportunity in a changing technological landscape and institutions learn how to counter their actions.**

"I've always been very intrigued by how much one can abuse a system – without, of course, doing it myself! What loopholes are there, how can people take advantage of them? I'm interested in how institutions can respond to this, but it's also exciting to work on issues of transgression." – Nicole van der Meulen

FOR cybersecurity expert Nicole van der Meulen, who has worked with institutions including Europol, RAND, and the Dutch Banking Association, finding safety in our digital world has always been about understanding the ways that rules and safeguards can be breached and broken.

When she began researching identity theft in the 2000s, the crime still had a strong physical component: "It was almost impossible to focus exclusively on the digital aspect. Cybersecurity wasn't a common concept then, though we could already see that data breaches facilitated identity theft."

Since those days, digital technology has transformed the scope and scale of cybercrime. However, Nicole sees this as an evolution rather than a revolution.

"Criminals running so-called advance fee scams, where they con you out of money that is supposed to unlock some supposed monetary benefit, used to steal hotel telephone books to gain contact details of potential victims," she explains. "Data breaches are different because the information is protected, but it is all about acquiring information."

Nicole is now paying attention to how the new generation of artificial intelligence may transform the game again – or not. She sees the potential for the technology to make threats more effective and lower criminals' barriers to entry, but doesn't think the type of threats will fundamentally change: "There are dangers in terms of cybercrime, but they are familiar dangers."

She says there is always a kind of "arms race" in this work. Criminals seek opportunity in a changing technological landscape and institutions learn how to counter their actions. She gives the example of financial service providers, who have taught themselves to detect fraudulent transactions by analysing their customers' data.

"Financial services might not always seem like the most thrilling industry, but they've been confronted with these threats for a long time, and done well to protect themselves by adapting to criminals' modus operandi – for example, bringing in two-factor authentication early. They tend to be ahead of the game because they are a primary target – money is their business – and they are inherently better prepared when it comes to identification of the entities they are dealing with."

Other sectors such as healthcare or energy can be more worrying, because the stakes are so high: "Those sectors so directly connect the digital to the physical, in terms of the consequences and physical impact on patients or communities."

As a researcher, Nicole explains, she has a creative and exploratory role, trying to find those areas which are not being addressed: "It's not possible to know everything, but my job is to find the blind spots, not just the things that everyone is already aware of."

She recognises that threat intelligence itself is a challenge, and one in which information professionals' skills can be very useful: "There is so much out there. It becomes an issue of trust, constantly doing the work of determining credible sources: the question becomes who is giving me this information and how can I then validate it? Source laundering is an issue, where reputable agencies, in their desire to be comprehensive, draw on open source material that may be of lower quality."

So what can institutions do to prepare themselves in a world where it feels like it's not a question of if, but when, a breach happens?

"I think you need to know your company, your assets, your processes, your people, in order to establish what kind of threats you are particularly vulnerable to. Know yourself, know your niche, look to the threat landscape and know why you specifically could be a target, as well as those general risks which may not be unique to your organisation."

"Then: accept that something will happen, you will face this issue. Have processes in place to detect it, respond to it, and recover from it. How will you deal with the fallout? Security is not always about invulnerability, it's also about securing yourself after an adverse event." IP

Matt Finch (@drmattfinch) is a writer and consultant who specialises in strategy, foresight, and innovation work with institutions worldwide. See more at www.mechanicaldolphin.com