Nicole Eagan: “Cybersecurity is very fast becoming an all-out arms race”

blogs.lse.ac.uk/businessreview/2017/05/13/nicole-eagan-cybersecurity-is-very-fast-becoming-an-all-out-arms-race/

5/13/2017

A major cyberattack this Friday (12 May) disrupted services at hospitals and doctors’ surgeries in England, and a number of other targets throughout the world. The UK’s National Health Service, Spain’s Telefonica and the American logistics firm FedEx were the first organisations to confirm they had been targeted. Cyberattacks have intensified in the past few months and companies, governments and all types of organisations are scrambling to fortify their defences.

“Cybersecurity is fast becoming an all-out arms race,” says Nicole Eagan, the CEO of Darktrace, a British cybersecurity company created by mathematicians from the University of Cambridge. Darktrace uses machine learning algorithms to prevent attacks before they happen. She spoke with LSE Business Review’s managing editor, Helena Vieira, during the Collision Conference on 2 May in New Orleans. In light of the massive attack, Darktrace sent additional comments, stating that ransomware is too fast and automated for human security teams to keep up.*

So many companies have been broken into in the past few months, not only by private hackers but also by foreign governments. Is there a way out, or is it just a matter of keeping it under control?

The threats keep coming and I think one type of analogy I’ve come up with to think about this is the human body. So, our human bodies are constantly under attack and have been for as long as we know. And it’s attack by viruses, by bacteria, and they keep morphing and changing. And I think it’s a fair analysis to what we see in the cyberthreat community. Our human bodies, of course, have skin, and the skin keeps a lot of it out and I think that’s what we’re trying to do in the areas of cyberprevention and cyberdefence. But the reality is that some of that nasty stuff still gets inside. Our view is that if we had the equivalent of something like the human immune system we might be able to see a way out of the situation we’re in.

How does the "immune system" work in computers? With AI?

It's one of the great things about machine learning and artificial intelligence coming on to the scene, not just on academic levels, but they're now being able to commercially offer that as well. And so, in the case of the human immune system, the immune system understands its unique sense of self. And that's really how Darktrace is using machine learning. It's unsupervised. There's no training data sets. We're actually putting machine learning straight into a company's network, into the heart of the network and we're using it to understand its sense of self. And the way we do that is by analysing 400 data features for ever user and device and the data they access and that builds a pattern of life, and when something meets the pattern of life, then it's probably not under attack. It's behaving normally. When something doesn't act like the normal pattern of life, that's when we get suspicious. And we start doing a lot of analysis to understand whether there's an active threat that's evolving inside the network.

Does the growth of the Internet of Things (IoT) pose a challenge for this kind of protection?

I think in general the IoT poses a lot of challenges to IT and security teams. And partly because people can walk in with IoT on their wrists in the form of a watch or it can come into the company in the form of an Internet-connected vending machine or cappuccino maker, in all kinds of these IoT devices, and most of them can get purchased not by going through IT or security, so it's kind of like shadow IT on steroids. The interesting thing is that these devices in IoT still connect through the network, often through WiFi. And so as long as they're connecting up to the network, Darktrace can still model it just like we would a laptop or a server or a smartphone. And so we're actually able to see these devices In fact, normally when we drop in a company network there are 20 to 30 per cent more devices than we expect, and a good portion of that can be related to IoT.

In a recent report, the Institute of Directory calls cybersecurity the defining business challenge of the 21st century, and suggests it shouldn't be a concern only of the IT department, but a part of the company's strategy. Are companies doing that?

We started Darktrace back in 2013. Then it was mainly still being treated almost as just an IT issue, together with a security issue. I've seen a massive change in the last 6 to 12 months, where boards of directors are getting very interested in it. I think part of that is potential regulation that could come downstream that says that every board has to have someone who is really knowledgeable on at least assessing the risk of cyberthreat and the internet response plan. As a result of that I've been meeting a lot more with boards of directors, both at conferences and events as well as in the boardroom. And see a shift in thinking.

Right now they're like, "We can get briefed quarterly on the cybersecurity posture, we can get briefed once a year on the internet response plan, or we get reports that count how many times we had malware or spear phishing attacks, whether that number went up or down from last quarter." And I say 'Ok, that's all well and good,' but really, and the point you mention in your question is that it really comes down to every decision that gets to a board is of such magnitude that the question they should really be asking is, 'Is my cyber-risk going up or down based on this decision?"

For example, I was working with a regional bank in the United States, and their strategy was to grow through accretive acquisitions. They were going to acquire lot of the small community banks and roll them up into a regional banking system. I asked them, 'How does cyber factor in that decision?", and they said, "What do you mean by that?" I replied, "That probably changes your cyber-risk profile and, it's probably fair to say, it increases your cyber-risk profile." I asked, "Tell me about the first bank you acquired," and they replied "In that particular one, there was one IT guy.' I asked, "Did he come over with the acquisition?" They replied, "For three months." I said, "What damage did you do? He had unlimited access to that during those three months. He could have stolen all the customer data or records, right?"

And that's one of the things. Mergers and acquisitions are something that boards understand very well. And we see cyber risk in M&A transactions on a regular basis. The first area is, during due diligence, why wouldn't you want to

go in to the target network and actually figure out whether a competitor or maybe a state-sponsored attacker from some other place in the world has stolen that intellectual property? That's one of the ways Darktrace works. We call it an M&A cyber toolkit. So you can actually use it in due diligence. We've had customers who have decided to use it as a way to negotiate down the purchase price when the network had already been infiltrated. Maybe intellectual property has been lost and stolen.

So that's an example of where the board can kind of understand this, because we're no longer talking about kinds of technical attacks of IP addresses. We're talking about concepts they understand, terminology they can relate to. Another area is cyber-risk insurance. Boards also get involved in whether they take cyber-risk insurance policies. So that has been another area. We have been able to come up with a scoring system, like a FICO credit score, for cyber-risk insurance. So that's another area. Then, finally supply chain. Supply chain is one of the biggest areas we're starting to target. A refrigeration company, and of course no one remembers the name of a refrigeration company, got inside and hacked Target's point of sales systems. So, supply chain is another area that boards of directors can understand that introduces a lot of risk. And that's an area we have worked with boards on.

AI is also available to hackers, so will this start an arms race to see who's going to be the most nimble?

It's very quickly becoming an all-out arms race. Definitely between the attackers and the defenders and I think what's up for grabs is all of the information and intellectual property inside corporate networks. It definitely is a battle of mathematical algorithms against mathematical algorithms. When you think about the nation states, we tend to be concerned about it. A lot of those nation states have very good universities, they have good mathematicians, and they likely have AI labs similar to what the universities do in the US and the UK. I think that raises the level of concern we need to have. We have seen one such attack and they are very rare at the moment. We actually saw an AI attack inside a network in India. We don't think it started in India, but we saw the AI attack inside the network and we could tell it went in and started looking around, trying to understand how to blend in the very noisy background of the network. Luckily Dartktrace algorithms were superior and our machine learning, because we've had to use it in commercial settings, works very quickly. And so we were able to detect it and get it out of the network quickly. Now what we don't know is when we're going to see more of these attacks. Is it going to be in 2017, 2020, 2025? No one really knows that yet. What we do know is the sooner corporations put machine learning in the networks and build up their immune system, the stronger they're going to be when that day comes.

Did we humans make a mistake when we created the Internet so open and vulnerable? Could we have done it differently?

One of the ways I've come to look at that is that in some ways it's almost like saying well, I'm afraid of catching a cold or the flu. I could stay home. And I wouldn't be here meeting with you, wouldn't be going to work and wouldn't be traveling on planes all over the world exposing myself to all of this. But at the same time that is the power of human civilization. Even compared with other species on earth. So, for humans to make progress like we do, to make advancements, we have to be social. And I think the Internet is just another manifestation or extension of that. So, I'm sure there's ways that security could be better adjusted on the Internet, but at the same time I think companies and individuals are willing to take that trade-off and risk because it helps move society and technology forward.

** Additional comments:*

"Software patching has always been a problem amongst most organizations, as patches usually require testing before being deployed to hundreds and thousands of devices. Basics such as patching systems and virus definitions will always be a problem for organizations, which is why comprehensive visibility is so critical. Organizations need the ability to spot anomalies as soon as possible. Quite simply, ransomware is too fast and automated for human security teams to keep up. In addition to securing networks from the inside, companies should also invest in disaster recovery plans: files should be backed up and a restoration protocol should be put in place. Our new reality is that these forms of automated attacks will only continue to occur with increasing sophistication. Corporations need to run

drills and have recovery plans in place so that they can take immediate action if there is a 'worst case scenario'. Ultimately, there is no silver bullet to these types of cyber-attacks. Our best chance is to identify and neutralize them before they can cause this scale of damage."

More on cybersecurity: Despite major cyberattacks, businesses have been slow to react and Cybersecurity is the defining business challenge of the 21st century

♣♣♣

- *This Q&A is the second in a series of 10 interviews done with tech leaders during the Collision conference in New Orleans, 2-4 May 2017.*
- *The post gives the views of the interviewee, not the position of LSE Business Review or of the London School of Economics and Political Science.*
- *Before commenting, please read our* Comment Policy.
-