Underwriting the unmeasurable

Risk Cooperative CEO **DANTE DISPARTE** sits down with Brunswick's **SIOBHAN GORMAN** to discuss how cyber attacks are redefining what "risk" means for M&A

THE INFAMOUS POLITICAL ADVISER Niccolò Machiavelli wrote, "Never was anything great achieved without danger." Sage words for an aspiring politician, but not comforting for CEOs leading what they hope are transformative mergers or acquisitions.

Executives overseeing deals have undoubtedly heard that their businesses are vulnerable to cyber attacks. But how much more vulnerable are they when hosts of advisers and third parties are involved, millions – or billions – of dollars are at stake, and employees, customers, regulators, investors, and even the media are watching closely? The fallout from a 2016 cyber attack on Yahoo!, as it was in the process of being acquired by Verizon, lowered the deal's price tag by $350 million.

In response to this growing threat, and amid an uptick in global M&A activity – which climbed almost 9 percent in Q1 2017 (see "Dealmakers see 'Trump Bump,'" Page 10, for more insight) – a niche solution to manage cyber risk is gaining popularity: insurance policies tailored to cover the damage caused by cyber attacks during M&A.

Dante Disparte is CEO of Risk Cooperative, which operates at the intersection of three complicated, technical fields: insurance, risk management and cybersecurity. In a conversation at Brunswick's Washington, DC office, from which this interview is excerpted, Disparte acknowledged the challenge of quantifying the risk a cyber attack poses. "The events that are much harder to measure are the ones that scare us: the theft of IP, crippling of systems, permanently rendering data useless."

Today, having cybersecurity policies during an M&A, or even conducting basic cyber due diligence, aren't regulatory requirements. Disparte thinks that's likely to change. But rather than simply a compliance box to tick, Disparte believes the best practices and transparency involved in insurance have a much broader role to play, acting as "a catalyst for business rather than a cost of business."

What cyber threats are unique to M&A?

One big one – we actually call this kind of concept, "cyber-cultural assimilation." To use a metaphor: in a car with all the safety technology in the world, the best defense is a well-trained driver. We think that the human factor in cyber risk is an enormous gap.

And clearly in an M&A scenario, you run a very high risk of alienating staff in the acquired company. People might think through what role they have in the post-merger world, if any. That's an enormous area of opportunity for improvement: in any M&A transaction, how do you get the human element brought into light and focus?

How can businesses manage the flood of cyber risks that accompany a merger?

I think step one is to never assume that the current due diligence frameworks pick up cyber risk.

Why?

When companies go into an M&A scenario, oftentimes for regulatory reasons or competitive reasons, it goes into a very silent, hermetically-sealed black box. And the tools that we currently have in our arsenal today – legal background, financial due diligence – often only the board or the C-suite will

"This is a risk for which there isn't singularly a technological solution"

ILLUSTRATION: ROLAND SÁRKÁNY

know about these possible talks. Any leak will have potential damage. So, the toolset really is not picking up cyber exposure. We need a slightly more invasive process, which will create some discomfort and transparency, but will ultimately enable M&A.

How do you create more transparency, and how do you get both companies on board?
I think you need to have a model in which the acquired company and the acquirer are coming into this under the view that, absent a deeper level of due diligence around cyber risk, the deal may not go through – almost a good-faith mechanism.

Can insurance help solve such a big problem?
In the insurance and technological industry around cyber risk mitigation, we most often get called almost like the fire brigade – when there's a problem. Many of the tools that we rely on, whether it's endpoint threat detection systems or crisis management, are of the "break in case of emergency" variety.

But imagine if you brought that capability into the deal room, if you will. Now instead of waiting for a crisis to emerge before you're addressing it, you're embedding that capability as a part of the investment review process. Suddenly, you now have a mitigation strategy around different scenarios. It's an issue, in my mind, of enabling these deals to go through in the first place at fair market value – as opposed to stopping them altogether or, worse yet, having the market decide how to price these risks.

Insurance in cyber is harder to gauge than, say, health insurance, where you have a track record and a lot of data you can point to.
In my view, cyber is more akin to life insurance; if you're buying a high-value life insurance policy, the underwriter doesn't just take your word for it. They actually go check your blood.

I think it's critically important for insurers, people like myself and companies like ours to not just take the customer's word for it, but to do endpoint-level threat detection to understand the hygiene of an enterprise and how it evolves over time.

Then we underwrite cyber risk using an evidenced-based approach. Two houses are insurable, but the one with smoke detectors, sprinklers and an alarm system is a better risk. We apply a system of credits and debits to cyber risk as we're working through underwriting them. We see cyber as a standalone risk. It needs a standalone solution – that only makes up 5 percent of the market today. The rest is what I call a "Frankenstein policy," it's bundled alongside other classes of insurance.

"Cyber is more akin to life insurance; if you're buying a high-value life insurance policy, the underwriter doesn't just take your word for it. They actually go check your blood"

Cyber risk is woefully underfunded and unhedged – to the tune of trillions of dollars of market value. A lot of firms are going to find themselves either in courtrooms or getting short shrift when it comes to this exposure and a similar number of investors may find themselves facing unforeseen losses.

What is the biggest misconception you see with cyber insurance? What are people not getting?
Well, one, they're not getting it enough. Because in part there's the placebo effect. Many believe that this risk may be covered elsewhere in their insurance and risk management framework.

A lot of it is also internal; if you're the chief information security officer of even the very biggest companies on the planet, you have a powerful inducement to say "It's all fine." It's called paycheck persuasion, hubris, organizational silos and territorial defense.

Cyber does not singularly reside in IT. It's a governance issue, it's an enterprise issue. And it starts at the C-suite and board levels. They're the ones who own the risk at the end of the day, not the IT security professionals, not the marketing and public relations professionals. There we find that there's a lot of work to be done yet. If you need help with your iPad, you are going to have a hard time in a boardroom asking questions and querying the state of play inside an organization's risk management frameworks.

What do you say to leaders who say: "I get that cybersecurity is an issue, but I'm going to invest in better, secure systems, not insurance?"
I would say, "Great, prevention is often better than cure. But I think a part of the whole spectrum of solutions needs to incorporate equilibrium." All too often you have enormous financial institutions spending hundreds of millions of dollars on cybersecurity, and it is easy to gravitate toward spending money on technology.

But this is a risk for which there isn't singularly a technological solution. Cyber risk advances according to Moore's law; bad actors have the benefit of patience and the organization and staff are the first lines of defense.

DANTE DISPARTE

Founder and CEO of Risk Cooperative, a strategy, risk and insurance advisory firm founded in 2014, Dante Disparte is also a strategic adviser to Rezon8 Capital, a US private equity firm. He co-authored the book *Global Risk Agility and Decision Making*, published in 2016.

SIOBHAN GORMAN is a Director in Washington, DC and advises on public affairs and crisis, with a focus on cybersecurity and privacy.