Taking aim at a moving target

Cyber lawyer RAJESH DE tells Brunswick's SIOBHAN GORMAN about lessons learned during his time with US intelligence

Rajesh De was General Counsel for the US National Security Agency during the period when Edward Snowden, a government contractor, copied secret documents detailing the NSA's surveillance practices and leaked them to the international media. The breach had severe repercussions not only for national security but also for governments and companies all over the world, exposing a threat that all data-collecting organizations face.

Now a Partner with international law firm Mayer Brown, De heads its Cybersecurity and Data Privacy practice, advising on the legal and reputational aspects of data risk. Cybersecurity is not static, he says, but "a moving target," and organizations need a long-term commitment involving every aspect of their business.

How did you end up focusing on cybersecurity?
I served in the White House as the Staff Secretary for President Obama, managing the documents that go across the President's desk. I handled all sorts of threat information – increasingly related to cyber. That was when cybersecurity became my passion. Later, as General Counsel at the NSA, I had a pretty good view of the types of cyber attacks the commercial sector was seeing.

What were the biggest cyber threats you encountered during your time at the NSA?
We saw an evolution of attacks, including some that really woke up the public to the cyber threat, such as those on Wall Street and at Sony Entertainment. It taught me how much public trust depends on secure networks.

What are the biggest lessons for business from the Edward Snowden breach?
Preparation, preparation, preparation. The NSA is prepared for many things, but we were not sufficiently prepared for managing this sort of significant leak by an insider. Dealing with the legal, reputational and public relations consequences all at the same time was not something that the agency – which prides itself on its secrecy – was prepared for.

Public opinion can be shaped very quickly, and it takes a long time to undo those perceptions. After Snowden's leaks, stories that had misstated or included incorrect information were almost impossible to fix. Those are lessons every business can learn from our experience. For the NSA, restoring public confidence was harder because the agency can't be completely open about what it does and doesn't do. The legal parameters within which it operates turned out to be a real hindrance.

Do you think companies appreciate the risks?
Companies underestimate the potential damage to their business when their reputation is compromised. Breaches can cause huge reputational harm. Make sure your entire organization is ready to manage that kind of damage – your legal staff, communications staff

7. HACKTIVISM (BREAKING INTO POP CULTURE)

Not all hackers are after money or sensitive information. Many businesses and governments find themselves targeted by "hacktivists" – attackers whose actions are politically motivated. These polarizing figures have also broken into pop culture. In 2014, actress Alyssa Milano published *Hacktivist*, a graphic novel that "questions the difference between good and evil in the age of technology." A year later, the TV show *Mr. Robot* premiered; its main character is a self-described "vigilante hacker."

LEGAL PERSPECTIVE

and business operations. They need to all be coordinated. Face the responsibility and own the problem. You want to be able to show that while your company may not be perfect, it can deal with the situation in the most responsible, forthright and transparent manner possible, both from a legal and a communications perspective.

How much do clients know about cybersecurity when they come to you for help?
One of the first discussions I'll have is about why the company might be attacked. There are many reasons why a business might be a target. Criminal groups try to get market-moving information that they can trade on, or other organizations connected to the business may have information the attackers want. They will often go through one business to get to another.

Increasingly, regulators are looking at data security in company supply chains. Contractual provisions need to be in place for managing cyber risk with all those business connections. Companies should exercise audit rights to ensure those parties are responsible stewards of their data.

When clients ask, "How do I protect myself against a cyber breach?" we explain that's just one element of a bigger strategy. Companies need to consider litigation risk, to structure their board of directors to oversee this risk, to manage increasingly complex compliance issues and to manage risk in their supply chain or cloud computing contracts. All of these issues have to be considered as part of an overall program.

What are the concerns you are hearing?
One is how to deal with the increasingly dynamic threat environment. The outlook is growing more complex on a daily basis, with the list of attackers including nation states, criminal groups and activists, and we see an increasingly complex regulatory and litigation landscape. Growing public awareness also increases pressure on companies across the board.

Companies want to know how to organize themselves. Legal affairs and information technology are relevant, but so are communications, human resources and just about every other department. The board has to be up to speed and able to ask the right questions. These concerns require a change in mindset. Cyber risk can't be solved overnight. It is a moving target in a landscape that is always changing and processes need to be in place to accommodate that reality.

> "In this environment, everybody needs to be ready. Lack of preparation can damage a company's reputation"

RAJESH DE

As a Partner in global law firm Mayer Brown's Washington, DC office, Rajesh De leads its international Cybersecurity and Data Privacy practice. He returned to Mayer Brown in 2015 after serving as General Counsel at the US National Security Agency. De has held senior appointments in the White House, the Department of Justice and the Department of Defense, as well as in the intelligence community. He served as Counsel to the 9/11 Commission and to the Senate Homeland Security & Governmental Affairs Committee.

How are cyber threats changing?
Ten years ago attacks were largely about stealing data, but they have evolved to a variety of more sophisticated and destructive goals and companies are being more open about their security and threats, so we have better information. We've seen distributed denial of service attacks where a lot of traffic is driven to a particular website to disrupt it. "Ransomware" is an important new threat, where an attacker locks data until a ransom is paid, often in digital currency. This raises complex legal and reputational issues. When is it appropriate to involve law enforcement? Can or should such attacks remain secret? How reliable is paying a ransom for restoring critical business functions? How will customers, shareholders, regulators and other stakeholders react to a company's response?

Does encryption have an important role?
The headlines have tended to paint encryption as a polarizing issue, something that can provide absolute security on the one hand and completely prevent law enforcement from doing its job on the other. But that really misses the point. Encryption is just one tool in a box of techniques. It is not a monolithic concept and its value depends on context. For example, the most secure encryption is not helpful if your employees do not know how to use it, or if the data it protects cannot be accessible to the business.

What should be a company's top priority?
Businesses typically get into trouble by giving the impression that they are not prepared. In this environment, everybody needs to be ready. Lack of preparation can damage a company's reputation. They might overreact, notifying the public or regulators before they know what actually happened. Or they may try to delay notification. That's not good and may not be legal.

Companies also need to show they have learned from prior incidents. Stakeholders understand that cybersecurity is a risk, but they have little tolerance for a company being hit twice in the same way.

SIOBHAN GORMAN is a Director in Brunswick's Washington, DC office and specializes in cybersecurity. She was formerly Intelligence and Cybersecurity Correspondent for *The Wall Street Journal*.