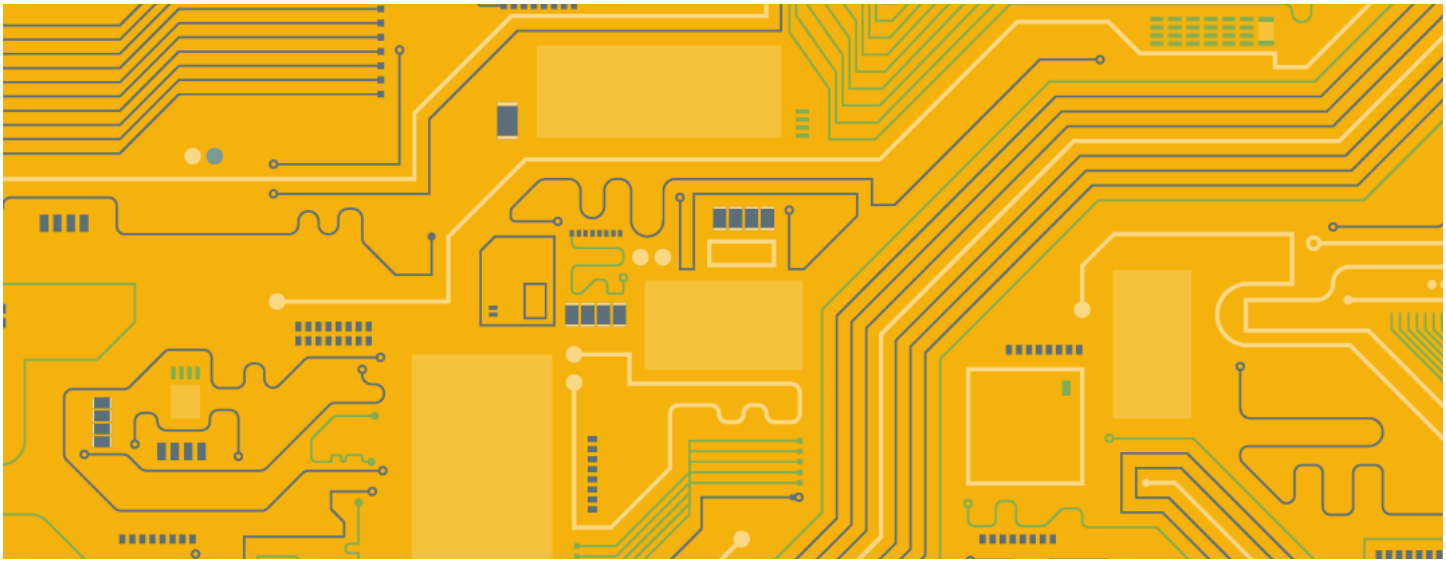


“The Business of Cybersecurity Is Business”: Kevin Powers on Managing the Risks and Consequences of Cyberattacks and Data Breaches

Kevin Powers and **Mihran Yenikomshian** — 5 MIN READ

In a digitized world, cybersecurity has become paramount.

Businesses today must commit more attention and investment than ever before to cybersecurity. The internet’s ubiquity has made the once-relevant distinction between tech businesses and non-tech businesses largely irrelevant when it comes to protecting corporate and customer information.

Take the Colonial Pipeline cyberbreach as an example. In May 2021, the Houston-based fuel pipeline system was taken offline after being hit with a ransomware attack. Even though the attack was centered largely on Colonial’s billing software, the pipeline shut down all operations for six days because of fears that information obtained by the hackers could be used to launch attacks on other parts of the pipeline.

Episodes like this make clear that any business, no matter its nature, must take steps to safeguard the security of its network systems and sensitive information and, if necessary, deal with the legal consequences of cyberattacks and data breaches.

To sort through those consequences, Analysis Group Managing Principal Mihran Yenikomshian spoke with academic affiliate Kevin Powers. Professor Powers is the founder and director of the Master of Science in Cybersecurity Policy and Governance program at Boston College, and teaches in the university's law and management schools. Additionally, Professor Powers is a cybersecurity research affiliate at the MIT Sloan School of Management, where he teaches the Cybersecurity Governance for the Board of Directors course in the MIT Sloan Executive Education program.

He and Mr. Yenikomshian discussed the increase in cyberattacks, fiduciary duties, and the cyber-regulatory landscape.

The world has seen a proliferation of cyberattacks and data breaches over the past few years. From your vantage point, how has the treatment of cybersecurity evolved?

One of the biggest changes I've seen is in the culture surrounding cybersecurity. Not long ago, cybersecurity was regarded as an IT issue, something for "the computer people" to be concerned about. Because it was treated as an IT matter, senior leadership typically did not understand cybersecurity as a business concern. That is changing and changing fast, due to the immense proliferation of data and the rising incidence of cyber-related crime.

Now, the business of cybersecurity is business – that is, all companies, regardless of industry, are tech companies because their entire business operations are interconnected to technology. As such, if their network systems go down, their business goes down as well and cannot function. Thus, digital information security has to be part of a firm's culture, and needs to be built from the top down, rather than from the bottom up. Cybersecurity is the responsibility of boards, C-suite executives, and all employees – not just IT departments.



> *Not long ago, cybersecurity was regarded as an IT issue, something for 'the computer people' to be concerned about. ... [Now], digital information security has to be part of a firm's culture, and needs to be built from the top down, rather than from the bottom up."*
>
> KEVIN POWERS

What kinds of risk do companies face with respect to cybersecurity?

Along with various risks presented by cybercriminals, nation states, and insider threats, where a cyberattack could result in the loss of business operations and sensitive data, businesses are faced with risks from regulatory actions and litigation. For example, regulatory bodies will often bring enforcement actions against businesses after a data breach, focusing on the reasonableness of their cybersecurity programs: Are such programs aligned with recognized industry best practices?

Likewise, if a company doesn't have the appropriate cybersecurity program in place based on its unique risk profile and suffers a data breach, can it be sued by its shareholders for any harm the business suffers? In other words, have the CEO and board of directors breached their fiduciary duty of care when making decisions related to cybersecurity and data privacy?

What are the circumstances under which this could happen?

The fiduciary duty encompasses a number of more specific duties, including those of care, candor, and loyalty. As such, the CEO and board could be found liable for breaching those duties if they failed to implement (and oversee and monitor) cybersecurity reporting or information systems, or any internal controls related to those systems, thereby allowing a risk situation to develop or continue and causing the business to suffer a loss due to a cyberattack.

What sorts of issues do you look to when you have been engaged as an expert witness and give testimony on these issues?

There are a number of things I typically evaluate when looking at a firm's cybersecurity and data privacy programs. For example, what is the maturity of its cybersecurity and data privacy programs? How do they align with the company's business risk profile, and are such programs reasonable based on the company's unique risks? What is the scope of responsibility for the firm's CISO [chief information security officer], or their equivalent? What authority does he or she have to make the necessary upgrades to the firm's cybersecurity and information infrastructure to keep an attack from happening? Is there a firmwide, top-to-bottom cybersecurity culture? What communication channels are being used to keep everyone informed of cybersecurity and data privacy priorities?

It sounds like the communication aspect of these activities is essential.

Absolutely. It's important to understand how policies are communicated to company personnel, and how frequently such policies are re-evaluated and updated to ensure compliance with best practices. How much are the CEO and board involved in, or at least aware of, these efforts, and how do they manage and monitor their due diligence and risk assessments?

Looking outward a bit, what does the regulatory landscape in this area look like?

There's been a flurry of new rules and regulations coming from various federal agencies and states. Based on these new rules and regulations, it's no longer the case that a business should be using best practices in developing and implementing its cybersecurity programs; rather, it must do so.

A lot of the impetus for requiring firms to be more proactive about their cyber and information security comes from New York's enactment of Department of Financial Services Part 500, which codified cybersecurity requirements for financial services companies. It requires them to implement a cybersecurity program "designed to promote the protection of customer information as well as the information technology systems of regulated entities." It also mandates that companies conduct a risk assessment and implement a program with security controls for detecting and responding to cyber events.



Based on these new rules and regulations, it's no longer the case that a business should be using best practices in developing and implementing its cybersecurity programs; rather, it must do so."

KEVIN POWERS

Similarly, for example, the FTC [Federal Trade Commission] promulgated the Standards for Safeguarding Customer Information under its rulemaking authority. The Standards include more specific criteria for what safeguards financial institutions must implement as part of their information security programs, including limiting who can access consumer data and using encryption to secure such data.

Companies must also explain their information-sharing practices, and designate a single qualified individual to oversee their information security programs, who will report periodically to an organization's board of directors or a senior officer in charge of information security. In short, many of the items we discussed earlier pertaining to implementation and oversight of cybersecurity standards by senior executives and boards. They will have to understand why the creation of and investment in cybersecurity programs are necessary, and how they are being used in order to best protect their businesses. ■