Two decades ago, the internet was a very different place – the World Wide Web resembled the American “Wild West” of the 19th century; beyond the reach of established regulations and lawmakers.

Today, the question of how to regulate the internet more effectively is high on government agendas. In part, this is because cyber risks – such as the recent WannaCry and Petya ransomware attacks – are becoming more prevalent. The Internet of Things (IoT) is providing ever more points of access for cybercriminals, and nearly every business now has digital, networked elements.

The increase in cyber threats is driven by a range of factors. Some of these stem from new sources of cybercriminal activity, like state actors and more organized criminal networks. But the underlying trends revolve around business and technological innovations.

“In terms of what’s driving these cyber threats, the underlying sources are many: cloud computing, IoT, mobility, social media, big data, AI, automation and ever-expanding connectivity," says CJ Dietzman, Vice President of Cyber Resilience at Stroz Friedberg, Aon.

“And a more digitally integrated business means one that’s more vulnerable to cyberattack. “As technology continues to have a transformative impact on business operations, risk profiles will change rapidly and significantly,” says Dietzman.

The need to control these risks is prompting a renewed commitment to comprehensive regulatory responses. But as regulators look to manage certain areas of risk, they create new difficulties for organizations to navigate.

Here are just three ways new cybersecurity regulations could create business challenges – even though they contain other risks:

Local Laws Have Global Implications
A company might not operate from – or even have offices in – a certain country. But that doesn't mean it isn't affected by that country's regulations. The regulations of the New York Department of Financial Services (DFS) demonstrate this. Effective as of March 1, 2017, these regulations apply to all DFS-governed financial services institutions, and include a range of cyber mitigation provisions.

Suppose Company A is operating in New York in a way that comes under the purview of the NYDFS. It must now engage in annual IT Risk assessments, and establish a Chief Information Security Officer (CSIO), and a relevant cybersecurity function. It must also put in place multifactor identification processes around vulnerable information, and engage in cybersecurity training, among other measures. Now suppose a breach happens. Company A has 72 hours to report that breach to the DFS.

And the DFS regulations don't just regulate one industry in one city: they regulate one of the most global, connected industries in one of the world's most global, connected cities. "Because you just have to do business in New York without necessarily being domiciled there means that this regulation can impact almost anyone," says Jackie Quintal, Financial Institutions Practice Leader, Aon Risk Solutions.

Because these regulations are so thorough, they will likely set the tone for future U.S. policy. "As New York goes – from a financial services standpoint – the other states will certainly take notice, and likely follow suit. There's a high probability that we're going to see the ball continue to advance in this direction," says Dietzman.

Your Customers Are Global – And May Have Different Digital Rights

The European Union (EU) has also ramped up its cybersecurity provisions over the last year. The General Data Protection Regulation (GDPR) will come into effect in May 2018 and is designed to protect the digital rights of EU citizens with regards to the use and storage of their data.

While the DFS regulations apply to businesses, GDPR applies to customers. Once again, companies don't have to be based in an EU country to be affected. Any company handling the data of any EU citizen as part of its operations must abide by the rules.

Kevin Kalinich, Cyber Insurance Global Practice Leader, Aon Risk Solutions, explains that the GDPR will affect "organizations of every size, industry and geography that process data of EU citizens."

"It applies broadly to personal data, including customer lists, contact details, genetic / biometric data and potentially online identifiers, such as IP addresses. Companies must obtain explicit clear and affirmative consent prior to processing personal data – assumptions based on silence do not comply."

It so happens that Company A is just such a firm which, while based in New York, also handles the data of EU citizens in its day-to-day operations. This means, in addition to complying with the DFS regulations, it must also abide by those of the GDPR. Some of these regulations are familiar – Company A must report to regulators within 72 hours in the event of a breach. But there are also new obligations. For instance, Company A now needs explicit consent before processing its customer's data. And suppose the same bad luck befalls Company A in Europe as it did in New York. If found guilty of misdemeanor or noncompliance, under the GDPR, Company A may have to pay a penalty of up to €20 million, or 4 percent of its total global revenues.

Adam Peckman, Global Practice Leader, Cyber Risk Consulting, Aon, advises organizations to take the following actions to comply with GDPR to meet the ongoing data privacy rights of their customers and employees:

- Understand where European personal data is stored and how it is used
• Review existing security controls
• Assess third parties’ personal data security standards
• Be prepared to report data breaches within 72 hours

A Threat To Business Integrity?

In June, China introduced its own far-reaching cyber regulations. While it is looking to address the same issues around cybercrime and data privacy as the U.S. and the EU, China’s policies take a different approach – creating yet another regulatory framework for businesses to navigate.

For instance, China shares concerns with the EU about how its citizens’ data are used. However, to address these, the Chinese regulations require all data relating to its citizens to be stored domestically. Any firm looking to send bulk data overseas must obtain permission to do so. In effect, this means firms looking to operate in China must have physical sites within the country. If the hypothetical Company A also has customers in China, on top of those in New York and the EU, then it now has yet another set of rules to comply with, and yet more complexity added to its digital operations.

Data that must be stored in China can also include intellectual and operational property. Microsoft has already shared proprietary code with officials to ensure that its products stay on sale in China. This has become one of the more contentious cyber regulations, with critics saying that aspects of it amount to threats to the integrity of business processes and assets, or function as a de facto protectionist barrier around domestic brands. Chinese officials, however, say that the regulations are essential for protecting its digital integrity while allowing non-Chinese firms access to Chinese markets.

Other Complications

Individually, each of these regulations poses challenges to businesses and as the Company A hypothetical example shows us, the complexities can quickly multiply for multinationals.

Potential conflicts quickly emerge. For example, the Chinese provision requiring operational data to be stored on Chinese territory, may run the risk of infringing on the stringent personal data protection controls covered in the GDPR. Navigating between these imperatives will be difficult, and will only become more so as further regulations are introduced – Japan is another major economy to have recently updated its data privacy regulations, with laws which again regulate the transfer of personal information over international boundaries.

While some larger companies may already be on their way to being compliant, others could struggle. As Quintal notes: “organizations, especially smaller ones, that don’t have dedicated in-house expertise in dealing with such issues might experience a bit of shock.”

Nevertheless, cyber regulation is essential to improve the digital system as a whole. As events like the WannaCry and Petya hack demonstrate, our data is more vulnerable than ever as we become more and more reliant on deeply interconnected digital infrastructure. Shouldering the burden may not be easy, but it will be something that companies need to do if they are to ensure they continue to operate in a safe, stable digital ecosystem, rather than the lawless, digital frontier towns of the recent past.

TALKING POINTS

“The New York law is the first proposed law, however, it will not be the last. Other states will follow, as well as other governing bodies. Cyber security has become an increasing enterprise threat to the continuation of many businesses and needs to be managed. Assuming “it will not happen to me” is no longer realistic.” – Michael Mihalik, CISO, Sphere Technology Solutions

“The truth is, financial services organizations aren’t alone when it comes to taking cybersecurity very seriously. Governments and other regulatory organizations have also put financial services cybersecurity to the spotlight over the past year.” – Bill Hogan, VP, Strategic Accounts and Global Financial Services, Fortinet

FURTHER READING

• China’s New Cyber Law Is Worryingly Vague – The Economist, June 1, 2017