Connected Risks

Cybersecurity regulations and mitigation approaches in US, Europe & Asia

Protecting data is tricky business. Data is a modern-day Frankenstein: what was once an asset is showing signs of becoming a liability. As the fourth "Industrial Revolution" progresses, odd bits of machinery are fused with data from real-world systems (transportation, power plants, patient records, ride-sharing details, bank and credit card information, etc.), breaking down political and physical boundaries while artfully dodging definitions of private and public ownership. While its complexity and reach fill one with a sense of awe, this big global IoT beast – with data as its life-blood – is powerful, yet dangerous.

In this article, global professionals from FTI Consulting – Anthony J. Ferrante in the United States, Pablo Lopez-Alvarez in Europe and Amrit Singh Deo in Asia – share perspectives on evolving cybersecurity regulations and how governments and businesses are preparing for the next data breach. These perspectives capture current regulatory approaches and policies, while offering details on the ways in which business and policy leaders can prioritise the myriad issues linked to cybersecurity.

Cybersecurity is a human issue when broken down into its constituents, but it is a geopolitical one in the aggregate. In recent years, we have seen growing efforts in global cooperation on cybersecurity policy. However, malicious threats are continuing to advance each and every day. For both the public and private sectors, this landscape frames the complexity and challenges associated with mitigating cyber risks.

United States Regulatory Approach

The United States is a global leader in cybersecurity: regulations, enforcement capacity, private sector capacity and technical expertise are all quite advanced. In many ways, the world has followed its approach to technology.

> Cybersecurity is a human issue when broken down into its constituents, but it is a geopolitical one in the aggregate.

A key advocate for protecting consumer privacy, the U.S. Federal Trade Commission ("FTC") is empowered by the FTC Act 15 U.S.C. with wide-ranging powers to prevent "unfair or deceptive" methods of conduct deemed injurious to consumers. From a cybersecurity perspective, this includes failing to protect personal data, disclosure of information without users' permission and failure to comply with a published privacy notice. The FTC can issue cease-and-desist orders, obtain restitution for consumers and impose fines and criminal penalties (including imprisonment of up to 10 years). Other landmark legislation, including the Homeland Security Act and the Federal Information Security Management Act ("FISMA"), requires the U.S. Department of Homeland Security ("DHS") and the Office of Cybersecurity and Communications ("DHS CS&C") to develop and implement information security standards.

Under the Financial Services Modernization Act ("Gramm-Leach-Bliley Act), financial institutions are required to have a security program in place that protects private personal information from unauthorised disclosure – with a range of financial and criminal penalties for lapses (for frauds, penalties can go up to USD$1 million and imprisonment of up to 10 years). By virtue of being a vulnerable target of breaches, the financial services sector has taken additional steps to address cybersecurity vulnerabilities. In 2016, the three federal banking regulators – the Federal Reserve Bank ("FRB"), Office of Comptroller of the Currency ("OCC") and Federal Deposit Insurance Corporation ("FDIC") – defined rules for cybersecurity breaches or "incidents" at large financial institutions (those with consolidated assets in excess of USD$50 billion) and critical financial infrastructure. By requiring vulnerability or penetration tests to prepare for cyber incidents, these rules can ensure financial institutions effectively plan for, respond to and quickly recover from disruptions caused by cyber incidents.

The United States already has a significant amount of collaboration between the public and private sector, but industry-specific approaches on cybersecurity are good opportunities to demonstrate strong leadership.

Last year, the New York Department of Financial Services' ("DFS") 23 NYCRR 500 cybersecurity regulation went into effect. This requires banks in New York to report any cyber incidents that could compromise data to the DFS within 72 hours, have a robust cybersecurity plan in place and employ a Chief Information Security Officer ("CISO") to oversee security processes and meet a series of compliance deadlines over the next two years (a full transition deadline is set for March 2019). These cybersecurity regulations are likely to be implemented in other states across the country.

Recognising the vulnerability of connected infrastructure facilities, the Obama administration passed an executive order launching the Critical Infrastructure Cyber Community, or C³ ("C Cubed") Voluntary Program, to enhance critical infrastructure cybersecurity and encourage adoption of National Institute of Standards and Technology's ("NIST") Cybersecurity Framework (issued in 2014). The C³ Voluntary Program is housed under the U.S. Computer Emergency Readiness Team ("US-CERT") in DHS. The NIST Cybersecurity framework is being referenced and applied in other sectors, and sector-specific CERT organisations have been created. For example, after it was revealed that malicious hackers had breached the Department of Energy's ("DoE") (which oversees the U.S. power grid) computer systems over 150 times between 2010 and 2014, the National Cybersecurity and Communications Integration Center ("NCCIC") and the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") were created to boost digital defense for utilities and control systems. In a similar vein, the Health Care Industry Cybersecurity Task Force at the U.S. Department of Health and Human Services ("HHS") has recommended that the Food and Drug Administration ("FDA") develop mitigation strategies for cybersecurity risks in medical technology. Following the 2016 cybersecurity incident in which a Mirai botnet created an internet outage by hacking DVRs and webcams, Congress also passed the IoT Cybersecurity Improvement Act 2017 to cover security of connected home solutions, wearables, sensors and other IoT devices, holding suppliers responsible for security updates while imposing strict guidelines for any such products or solutions sold to the U.S. government.

To ensure that information about a cybersecurity breach is communicated in a timely fashion, the Cybersecurity Information Sharing Act of 2015 (CISA) ensures that both the public and private sectors share information on cybersecurity incidents, effectively fostering collaboration to combat threats. From an industry perspective, the financial services sector works through FINRA, the Financial Industry Regulatory Authority, in a self-regulatory capacity by raising cybersecurity standards for brokers/dealers and encouraging firms to share cyber incident information through the Information Sharing and Analysis Center ("FS-ISAC").

Implications for Global Corporations

Companies operating in the United States need to comply with local cybersecurity regulations or be ready to pay stiff fines. A concerted regulatory and enforcement effort across sectors means that companies will be routinely audited for cybersecurity vulnerabilities. Global companies need to expand their information security budgets and resources, develop cyber risk disclosure policies, obtain cybersecurity insurance, and simply undertake more routine vulnerability testing activities. The United States already has a significant amount of collaboration between the public and private sector, but industry-specific approaches on cybersecurity are good opportunities to demonstrate strong leadership. Financial services players will have to up their cybersecurity game to meet new regulations from the New York DFS, as other states may soon follow its lead. Companies should expect more fines for inadequate safeguards against breaches – creating an incentive to strengthen corporate cybersecurity policies and procedures at-large.

The European Way

The European Union's Global Data Protection Regulation ("GDPR"), which will enter into effect on May 25, 2018, establishes one set of data protection laws across all 28 European Union member states. By harmonising data privacy laws across Europe, GDPR protects and empowers all EU citizens. In the event

of a cybersecurity breach that compromises EU citizens' data, an organisation may face fines of up to 4% of their annual global turnover, or €20 million – whichever is greater. GDPR shifts the balance of power to the citizen to whom the personal data belongs, and away from organisations that collect, analyse and monetise such data (GDPR also applies to data brokers, processors and controllers). This attempts to address breaches such as the one that hit Experian, one of the largest credit agency data brokers; this breach led to the public exposure of personal information for over 15 million T-Mobile customers (including many Social Security numbers). Additional requirements under GDPR include reporting breaches as soon as possible (no later than 72 hours after discovery), and enables the "right to be forgotten" – allowing people to request search engines to delete links to personal data. All companies that handle EU citizens' data will be liable under GDPR and will have to seek active consent to use personal data as well as carry out Privacy Impact Assessments ("PIAs") to ensure that personal data is sufficiently protected.

The EU has also passed the Network and Information Security Directive ("NIS") that introduces new cybersecurity requirements and breach reporting obligations for entire sectors (including energy, transportation, water/utilities, banking, and healthcare, among others) deemed part of Europe's critical national infrastructure ("CNI"). Interestingly, the definition of CNI also includes providers of digital services, such as search engines and cloud services, but under a different NIS regime. Under NIS, member states will be required to adopt national cybersecurity strategies and create national authorities for this purpose.

The EU has already created its own cybersecurity agency: the European Union Agency for Network and Information Security ("ENISA"). ENISA has the resources to support member states on cybersecurity matters, including NIS implementation. ENISA has also rolled out a joint initiative for the European Commission and industry around cybersecurity certification that will embody a "duty of care" principle to reduce products, services and systems vulnerabilities while putting the onus of cybersecurity for all connected devices on the private sector. ENISA will also prepare a blueprint for rapid emergency response so that member states have a well-rehearsed plan in case of a large-scale cross-border cyber incident in the EU. Whilst the increased mandate of ENISA and the proposed certification scheme are ambitious, the exact scope of these measures (known as the Cybersecurity Act) remains to be clarified as they will not be formally adopted by EU institutions before June 2018.

Implications for Global Corporations

By putting citizens' privacy at the heart of the European cybersecurity efforts and implementing unprecedented penalties for lapses in data protection, the EU has clearly indicated where its priorities lie. Providers of digital services are now categorized within the ambit of CNI, and CNI regulation will apply to all companies with operations in Europe – even if they are headquartered elsewhere. This will require greater operational rigor around consent to use personal data. Global organisations collecting EU citizens' data will need to carry out PIAs to ensure that personal information is sufficiently protected and privacy of the individual is maintained. Furthermore, the liability of data brokers (anybody who stores large sets of personal consumer data), as a result of recent regulations following the Experian and other breaches, is expected to increase significantly. It will be interesting to see how ENISA rolls out and enhances its cybersecurity enforcement capabilities when GDPR goes into effect later this year.

By putting citizens' privacy at the heart of the European cybersecurity efforts and implementing unprecedented penalties for lapses in data protection, the EU has clearly indicated where its priorities lie.

The Wild East: The Asian Perspective

Competing national interests, growing economies and geopolitical competition make Asia a playground for state and non-state cyberpunks. Whether they're pulling off a bank heist (Bank of Bangladesh) to splurge in the casinos in Manila or breaking into Sony's servers to leak the latest film or television series, hackers will continue to compromise public infrastructure and private assets. This vulnerability is compounded by the relatively low level of preparedness, defense and cross-jurisdictional cooperation on cybersecurity policy in Asia (as compared to the West).

Here's a quick regional view of the latest cybersecurity regulations among key players:

CHINA – China established the Central Leading Group for Internet Security and Informatization in 2014 under President Xi, bringing a number of sectoral legislations, linking national security and counter-terrorism laws with cybersecurity, culminating with China's Cybersecurity Law. The Cybersecurity Law went into effect on June 1, 2017, bringing financial services into the ambit of critical information infrastructure ("CII"). Government authorities can request access to data for all CII entities, and such entities are obligated to provide it. Also, as per the new law, data collected in China must be stored on local servers and cannot be moved overseas without permission. The provisions are onerous on global technology firms and could mean obligation for ICT suppliers to hand over their encryption keys to Chinese authorities. Given the entwined political and national security objectives of the Act, the emergence of state-owned or controlled Chinese cloud and data-mining assets seems inevitable.

INDIA – India's National Cyber Security Policy ("NICP") of 2013 led to the establishment of the Office of the National Cyber Security

Chief in the Prime Minister's Office in 2015. With a sharply rising internet-connected population, India's national digital transformation policies and its national biometric identification system have permeated discussions of privacy and data protection. In November 2017, India's Ministry of Electronics and Information Technology ("MeitY") instituted the Srikrishna Committee to prepare a white paper and recommend a data protection and privacy framework. The final report of the committee, expected in March 2018, will cover use of sensitive personal data, consent requirements, accountability of data controller, penalties for wrongful processing, cross-border flows, data localisation, data breach notifications and enforcement of a data protection framework by a statutory authority. The Srikrishna report will form the base for India's Data Protection and Privacy Legislative Act. The CERT-IN is the lead organization on cyber-incident reporting and response, complemented by sector-specific CERTs. In 2017, four power-sector CERTs (each for transmission, thermal power, hydropower and power distribution) were created and a financial-sector focused CERT-FIN was proposed. The central bank has created a subsidiary called ReBIT to work with the banking sector on cybersecurity as well.

Asian governments will have to look beyond nationalist impulses to encourage closer collaboration on cybersecurity within the region. As regional economies facing geopolitical pressures undertake technology transformation projects to drive economic growth, securing Asia's critical infrastructure becomes important.

JAPAN – Japan's Basic Cybersecurity Act (enacted in 2014), amended Personal Information Protection Act (amended 2015, effective 2017) and Basic Policy for Critical Information Infrastructure Protection (3rd Edition 2014, published by Information Security Policy Council) make up its core cybersecurity legislation, covering data privacy and critical infrastructure. The Ministry of Economy, Trade and Industry ("METI") established the Industrial Cybersecurity Center of Excellence ("COE") under the Information-Technology Promotion Agency ("IPA") in April 2017, and is focused on building cybersecurity talent as well as security of industry control systems ("ICS"). The Japan Institute for Promotion of Digital Economy and Community ("JIPDEC") operates an information security management system ("ISMS") assessment to certify companies on cybersecurity.

ASEAN – Singapore (along with Australia, Japan, New Zealand and South Korea) is a member of the "Cyber Five" – a group known in cybersecurity circles for its vulnerability to cyberattacks in a world of high-level technology adoption. This title comes despite significant cybersecurity incident preparedness: The International Telecom Union ("ITU") ranked Singapore first and Malaysia third in its 2017 International Cybersecurity Index, a report measuring national commitment to cybersecurity. Singapore's Cyber Security Agency ("CSA") proposed new cybersecurity legislation in 2017 that led to the passage of the Cybersecurity Bill on 5 February 2018.

Singapore's Cybersecurity Bill envisions creation of a Cybersecurity Commissioner (acting as lead regulator) and Assistant Cyber Commissioners (acting as sector leads), and is expected to be implemented by mid-2018. In Malaysia, Cybersecurity Malaysia (earlier called the National ICT Security and Emergency Response Centre) is the national agency for cybersecurity within the Ministry of Science and Technology and Innovation ("MOSTI"), overseeing breach incident and response, industry collaboration, protection of critical infrastructure and cybersecurity capacity building. The Malaysian Computer Emergency Response Team ("MyCERT"), Digital Forensics Lab ("CyberCSI") and Malaysian Vulnerability Assessment Centre ("MyVAC") are housed within Cybersecurity Malaysia. Vietnam was the victim of a major breach in July 2016 when a hacking group named 1937CN hijacked Vietnam's information systems at Vietnam Airlines and some of its largest airports. Following this incident, Vietnam created a strategic plan to strengthen cybersecurity, and a law on digital information security ("LCIS") took effect in 2017. Indonesia formed its National Cyber and Encryption Agency in 2017 and appointed Djoko Setiadi, as the head of the Agency in January 2018.

AUSTRALIA – The Australian Cyber Security Centre ("ACSC") and CERT Australia look after all cybersecurity matters, with a particular focus on critical infrastructure. On 22 February 2018, Australia rolled out the Notifiable Data Breach ("NDB") scheme covering all entities (government agencies, businesses and not-for-profits) with an annual turnover in excess of AU$3 million, if they share personal information of customers with suppliers (including those based overseas). Failure to report sensitive data breaches within 30 days to the Australian Information Commissioner could result in fines of up to AU$2.1 million for organisations.

Asia cannot afford to be a digital third-world region without a regional and global view on international cybersecurity and privacy rules and standards. Asian governments will have to look beyond nationalist impulses to encourage closer collaboration on cybersecurity within the region. As regional economies facing geopolitical pressures undertake technology transformation projects to drive economic growth, securing Asia's critical infrastructure becomes important.

Implications for Global Corporations

Global companies should review local data governance in China and keep an eye on other Asian jurisdictions that may be considering similar data localisation policies. Asia represents a tremendous opportunity for transnational companies (in technology and other sectors) to strike public-private partnerships and shape the emerging cybersecurity frameworks in the region. Governments across Asia have also identified the lack of trained

cybersecurity professionals and skills as a major gap in their preparedness. Corporations can propose collaborations that support long-term corporate strategies, but this will require open, creative thinking and a buy-in from the global head office. Companies that demonstrate agility will strike meaningful partnerships with governments early on – and can leverage these relationships to reaffirm their license-to-operate and make plays for greater market access in the future.

A Coordinated Approach

Cybersecurity is an international issue that requires a globally coordinated response – whether it be a multi-jurisdictional approach on regulation (government-to-government level) or close collaboration between the private and public sectors (government-to-business level). Countries that opt for a "closed-box" approach will risk building digital islands that are even more vulnerable to an attack. At the same time, leaving large parts of the global economy out of the cybersecurity standards-setting process is the easiest way to pool risks, leaving open the possibility for breaches. Global technology companies and industry leaders in the private sector have significant roles to play in working with governments to secure critical infrastructure.

Significant technical expertise and resources resides in the private sector, and companies have the most to lose in terms of the commercial impact from a data breach. Transnational companies can leverage their tech-superiority as a differentiator to work with governments by matching public cybersecurity investments and contributing to the global cybersecurity agenda. The imperative for Asian nations to build coordinated cyber-resilience strategies is significant, as many recent cyberattacks have emanated from the region (many are non-state actors, with tacit support from some states). As we have seen with NotPetya (malware that began infecting organizations in Ukraine, but quickly spread to global private companies like FedEx, WPP, Rosneft and Maersk) and WannaCry (ransomware that targeted outdated Windows software), the speed with which breaches can spread is concerning. Taking a nationalist or even a solely regional approach to tackling these threats will be ineffective. Western governments and tech enterprises should recognise the imperative of working with the East in developing a global cybersecurity regulatory architecture. Bilateral cooperation between national governments is a first step, but a global treaty on cybersecurity is becoming an imperative. When large Asian economies like India, Russia and China hold out on signing the Budapest Convention on Cyber Crime, it is a sign that global cybersecurity governance requires some adjustments.

Beyond cybersecurity policy enforcement, securing critical national infrastructure is a clear area for cross-jurisdictional collaboration since network weaknesses could quickly undermine public and private assets alike. Cyber diplomacy will have to evolve beyond the current "skunkworks projects" model that most bilateral collaborations demonstrate in order to facilitate truly global collaboration. INTERPOL has taken the lead on cyber enforcement with its Cyber Research Lab and its own private Darknet network, private cryptocurrency, and simulated marketplace to recreate the virtual "underground" frequented by criminals for police departments to use in training. In 2015, INTERPOL, with the aid of multiple governments and industry players, took down the Simda and Dorkbot botnets that had infected an estimated 1.75 million computers worldwide. The Singapore-based INTERPOL Global Complex for Innovation ("IGCI") and Digital Forensics Lab ("DFL"), and the Cyber Fusion Center within it, are an example of global cooperation between government agencies from a number of countries, the private sector, and academia. The IGCI conducts routine National Cyber Reviews for its members and assists in transnational Digital Crime investigations.

Global technology companies and industry leaders in the private sector have significant roles to play in working with governments to secure critical infrastructure. Bilateral cooperation between national governments is a first step but a global treaty on cybersecurity is becoming an imperative.

In the financial services sector, the FS-ISAC is launching a new regional governance structure to create Regional Threat Intelligence Committees ("RTICs") and Regional Strategy Committees ("RSCs") in the EMEA and APAC regions. This effort will expand the geographic scope of threat intelligence and address region-specific challenges.

There is a significant amount of opportunities for further cross-jurisdictional, worldwide cooperation in other critical sectors of the global economy. Private sector leaders play a key role in shaping this global cybersecurity architecture. Malicious cyber actors are advancing at a rapid pace, and the longer we delay the development of concerted global responses to cybersecurity threats, the more vulnerable we all become – individually, as citizens and consumers; and institutionally, as global organisations and governments.

Anthony J. Ferrante
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

Pablo Lopez-Alvarez
Managing Director
+32 475 601 410
pablo.lopez-alvarez@fticonsulting.com

Amrit Singh Deo
Managing Director
+91 916 742 8242
amrit.singhdeo@fticonsulting.com

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.