Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Cybersecurity 2022

Introduction
Alan Charles Raul
Sidley Austin LLP

practiceguides.chambers.com

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Cybersecurity Is Not Just about Personal Information Any More; Critical Infrastructure, Business Continuity, Social Services and Human Life Are Profoundly at Risk from Malign State Actors and Affiliated Cyber Criminals

Russia's invasion of Ukraine has focused the world's mind on the myriad ways that evil can be perpetrated on law-abiding society. Very much included among such depredations are cyber-attacks levelled against the essential foundations of life, social organisation and commerce.

Given the broad danger to national security and general welfare posed by today's cyber-attacks, governments are now acutely focused on knowing when, why and how public companies and significant private organisations are attacked – regardless of whether personal information is compromised as part of an attack.

Just in March 2022, the United States Congress enacted a new law, Cyber Incident Reporting for Critical Infrastructure Act, requiring companies in critical infrastructure sectors to report significant incidents and ransomware attacks to the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the Department of Homeland Security, and the Securities and Exchange Commission proposed new requirements for publicly traded companies to disclose cyber-attacks in their public filings.

Similar trends are developing internationally. In the United Kingdom, for example, the National Cyber Security Centre (NCSC), which is part of the General Communications Headquarters (GCHQ), takes the lead in providing proactive advisories and guidance to achieve effective cyber defence – especially where malicious state-sponsored actors may be involved. Companies must thus be mindful of the numerous other government authorities that play an increasingly consequential role in cybersecurity. Of course, data protection authorities and privacy commissioners continue to be relevant for personal information data breaches and corresponding security practices.

Ever since the State of California enacted the first data breach notification law in 2003, government regulators, privacy commissioners, cybersecurity lawyers and compliance officials have recognised that attacks on sensitive personal data could significantly damage the privacy and financial identity of hacking victims. In recent years, though, the realm of greatest cyber risk has shifted from personal data to information technology systems, hospital and government databases and servers, essential business assets and, of course, critical infrastructure of all types – power generation, energy distribution, financial services, food and water delivery, shipping and transportation, etc.

In the latest "Annual Threat Assessment" issued by the Office of the Director of National Intelligence (issued 9 April 2021), the US Intelligence Community warned of acute cyber threats from nation states and their surrogates, primarily Russia, China, Iran and North Korea. The US Intelligence Community Assessment described the threat as follows: "Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. Although an increasing number of countries and nonstate actors have these capabilities, we remain most concerned about Russia, China, Iran, and North Korea. Many skilled foreign cybercriminals targeting the United States maintain mutually beneficial relationships with these and other coun-

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

tries that offer them safe haven or benefit from their activity.

"States' increasing use of cyber operations as a tool of national power, including increasing use by militaries around the world, raises the prospect of more destructive and disruptive cyber activity. As states attempt more aggressive cyber operations, they are more likely to affect civilian populations and to embolden other states that seek similar outcomes".

"Authoritarian and illiberal regimes around the world will increasingly exploit digital tools to surveil their citizens, control free expression, and censor and manipulate information to maintain control over their populations. Such regimes are increasingly conducting cyber intrusions that affect citizens beyond their borders – such as hacking journalists and religious minorities or attacking tools that allow free speech online – as part of their broader efforts to surveil and influence foreign populations."

Increasing Scope of Cyber-Attacks and New Methods

During the past decade, state-sponsored hackers have compromised software and IT service supply chains, helping them conduct operations – espionage, sabotage, and potentially prepositioning for warfighting.

Public advisories issued by CISA have disclosed that Russian state-sponsored cyber threat actors have targeted an extensive array of US and international critical infrastructure organisations, including defence, healthcare, energy, telecommunications and government facilities. The list of cyber devastation and disruption is nearly endless and includes the SolarWinds and Active Directory/M365 compromises, and the NotPetya malware that has been described as the most devastating cyber-attack in history. The malware caused USD1.4 billion damage to the Merck pharmaceutical company and disabled international shipping and logistics around the world.

In 2020, the US Department of Justice indicted Russian military intelligence (GRU) officers associated with the hacking units known as "Sandworm" or "Voodoo Bear" for engaging in a global hacking and destabilisation campaign carried out for the strategic benefit of Russia. Most recently, the GRU's cyber hacking unit, Sandworm, has been identified as the perpetrator of malware and denial of service attacks intended to paralyse Ukraine's critical infrastructure – including banks and government websites – in preparation for Russia's invasion.

But Russian state actors are reported to have extended their malicious reign of cyber terror by sponsoring or harbouring affiliated cyber criminals who attack business and civil society for profit. No organisation is safe from their cyber-attacks. On 9 March 2022, the US Department of Justice won a significant cyber victory by obtaining the extradition to the USA of a Ukrainian national tied to a ransomware group of Russian-based actors. The individual, who was a member of the Sodinokibi/REvil group, was charged with attacking multiple victims, including the July 2021 attack against Kaseya, the IT and security management provider. He was taken into custody in Poland.

Protective Measures that Organisations Must Take

Given the potentially devastating impact on organisations of all kinds from cyber threat actors, companies are well served to heed the advice and warnings provided in numerous cybersecurity advisories issued by the likes of CISA and the NCSC.

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Businesses should be familiar with frequent alerts from CISA and the NCSC such as these: "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure", "Shields Up", and "NCSC advises organisations to act following Russia's attack on Ukraine".

In sum, while global data protection authorities play an important role in helping to protect personal data, they are not enough. Organisations must also protect their critical information systems and assets by looking to the world's leading cybersecurity agencies for information, guidance and co-operative initiatives to resist and combat the world's most sophisticated cyber threats.

INTRODUCTION

Contributed by: Alan Charles Raul, ***Sidley Austin LLP***

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Geneva, Hong Kong, Singapore and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, tech, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, digital governance, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as GDPR and CCPA; legislative and policy developments; and international data transfers.

CONTRIBUTING EDITOR

Alan Charles Raul is the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on US and international privacy, cybersecurity and technology issues. Alan advises on global regulatory compliance, data breaches, and crisis management. He also focuses on issues concerning national security, constitutional and administrative law. He handles enforcement and public policy issues involving the FTC, State Attorneys General, SEC, DOJ, FBI, DHS/CISA, the intelligence community, as well as other federal, state, and international agencies. Alan previously served in government as vice chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the U.S. Department of Agriculture, and Associate Counsel to the President. Alan serves as a lecturer on Law at Harvard Law School, where he teaches a course on Digital Governance: Privacy and Technology Trade-offs. He is a member of the Technology Litigation Advisory Committee of the U.S. Chamber Litigation Center, the governing Board of Directors of the Future of Privacy Forum, and the Council on Foreign Relations.

Sidley Austin LLP

1501 K Street, N.W.
Washington, DC 20005
USA

Tel: +1 202 736 8477
Email: araul@sidley.com
Web: www.sidley.com

SIDLEY

Chambers Guides to the Legal Profession

Chambers Directories are research-based, assessing law firms and individuals through thousands of interviews with clients and lawyers. The guides are objective and independent.

practiceguides.chambers.com