Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2024

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

Contributing Editor
Alan Charles Raul
Sidley Austin LLP

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 Austin'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 Austin's privacy and cybersecurity practice. He represents companies on US and international privacy, cybersecurity and technology issues, advising on global regulatory compliance, data breaches and crisis management. Alan previously served in government, and also handles enforcement and public policy issues involving the FTC, State Attorneys General, SEC, DOJ, FBI, DHS/CISA, the intelligence community, and other federal, state and international agencies. Alan gives lectures on Law at Harvard Law School, and is a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the governing Board of Directors of the Future of Privacy Forum, and the Council on Foreign Relations.

INTRODUCTION

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

Sidley Austin LLP

1501 K St NW Ste 600
Washington, DC 20005
USA

Tel: +1 312 853 7000
Fax: +1 312 853 7036
Web: www.sidley.com

Global Co-operation on Cybersecurity Is Crucial, and Happening

Nation-state threat actors have proven highly adept and relentless in exploiting vulnerabilities and planting offensive malware in critical infrastructure and internet networks around the world. This is likewise for ransomware, where reports indicate that payments doubled year over year in 2023, to more than USD1 billion (see therecord.media). In response, international government cybersecurity agencies are collaborating more extensively than ever to promote "Secure by Design" software, and are undertaking joint law enforcement and national security operations to counter ransomware attacks and take down networks of hijacked computers.

International Treaty Commitments for Co-operation Against Cybercrime

At the highest level, global co-operation on cybersecurity is demonstrated by the fact that, as of the end of 2023, 43 countries had signed the "Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No 224)" (see coe.int). The original Convention confirmed the "need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation" and committed the parties to adopting national laws to criminalise and investigate offences against the confidentiality, integrity and availability of computer data and systems, as well as computer forgery, fraud, computer-distributed child pornography, digital scale infringement of copyright, etc (see here).

The original Budapest Cybercrime Convention called for international co-operation and mutual assistance among signatories with respect to combating cybercrime. The Convention was first opened for signature in 2001 and came into force in 2004 upon ratification by five signatories.

The Second Protocol to the Convention, which was opened for signature in 2022, will add significant tools for conducting multi-jurisdictional cybercrime investigations more effectively. To date, it has been ratified by two signatories (Serbia and Japan), and will come into force when three more countries ratify. In the USA, the Second Protocol has been referred to the Senate Foreign Relations Committee, whose approval (and approval by the Senate as a whole) is a necessary step towards ratification. The US Department of Justice has stressed the importance of the Protocol for improving cross-border access to electronic evidence of cybercrime. The EU

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

has likewise expressed support for the Protocol, but no EU member states have yet ratified it. It should be noted that neither China nor Russia has subscribed to the original Budapest Cybercrime or its Protocols.

Once the Second Protocol comes into force and is implemented by the ratifying states, participating countries will be able to submit *direct* requests to domain name registrars and electronic service providers in foreign jurisdictions, in order to obtain registration and subscriber information and traffic data in support of national cybercrime investigations.

International Cybersecurity Agencies Agree on Principles for Software Security by Design

In October 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) announced an update to its Secure by Design Principles Joint Guide, along with eight international cybersecurity agencies (see here). This joint guidance urges software manufacturers to take urgent steps towards designing, developing and delivering secure products:

"This updated guidance… expands on the three principles defined in the initial guidance: Take Ownership of Customer Security Outcomes, Embrace Radical Transparency and Accountability, and Lead From the Top. This update highlights how software manufacturers can demonstrate these principles to their customers and the public, emphasising that software manufacturers must be able to compete on the basis of security. This joint guidance is intended to help software manufacturers demonstrate their commitment to Secure by Design principles, and give customers suggestions on how to ask for products that are secure by design."

CISA was joined in issuing this updated guidance by the cybersecurity authorities of Australia, Canada, the UK, Germany, Netherlands and New Zealand, who co-sealed the initial version, along with additional input and partnership with cybersecurity agencies in the Czech Republic, Israel, Singapore, Korea, Norway, OAS member states and Japan.

CISA Director Jen Easterly described the international partnership as leading to new "guidance to focus even more on how companies can demonstrate their commitment to Secure by Design principles. To achieve the National Cybersecurity Strategy's goal of rebalancing the responsibility in cyberspace, customers need to be able to demand more from their vendors – and this joint guidance gives them the tools to do exactly that."

In December 2023, CISA, Australia, Canada, New Zealand and the UK issued a further Joint Guide for Software Manufacturers as part of the Secure by Design Campaign. The Joint Guide "provides manufacturers steps for creating and publishing memory-safe roadmaps that will show their customers how they are owning security outcomes, embracing radical transparency, and taking a top-down approach to developing secure products – key Secure by Design tenets" and urges "C-suite and technical experts at software manufacturers to… implement memory-safe roadmaps to eliminate memory safety vulnerabilities from their product."

International co-operation on cybersecurity extends to artificial intelligence (AI). In November 2023, CISA (see here), the UK National Cybersecurity Centre (NCSC) (see here) and 23 other US and international cybersecurity agencies issued Joint Guidelines for Secure AI System Develop-

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

ment to address the intersection of AI, cybersecurity and critical infrastructure:

"The Guidelines, complementing the US Voluntary Commitments on Ensuring Safe, Secure and Trustworthy AI, provide essential recommendations for AI system development and emphasise the importance of adhering to Secure by Design principles. The approach prioritises ownership of security outcomes for customers, embraces radical transparency and accountability, and establishes organisational structures where secure design is a top priority."

The UK NCSC Guidelines for Secure AI System Development, incorporated in CISA's document, explain as follows:

"AI systems are subject to novel security vulnerabilities that need to be considered alongside standard cyber security threats. When the pace of development is high – as is the case with AI – security can often be a secondary consideration. Security must be a core requirement, not just in the development phase, but throughout the life cycle of the system.

For this reason, the guidelines are broken down into four key areas within the AI system development life cycle: secure design, secure development, secure deployment, and secure operation and maintenance. For each section, we suggest considerations and mitigations that will help reduce the overall risk to an organisational AI system development process."

Collaboration on National Security-Related Cybersecurity Threats

Zero-day software vulnerabilities are often exploited by nation-state threat actors, including Russia and China, and will thus typically involve US and international national security agencies. Speaking at the Munich Cybersecurity Conference in February 2024, US Deputy Attorney General Lisa Monaco discussed the US Department of Justice's (USDOJ) efforts to take down "an army of zombie computers, known as a botnet, used by Russian military intelligence to launch cybercrimes" (see here). The GRU's malicious efforts targeted internet routers to establish "a global cyber espionage platform" (see here). Attorney General Merrick Garland stated that "[t]he Justice Department is accelerating our efforts to disrupt the Russian government's cyber campaigns against the United States and our allies, including Ukraine."

In Munich, Deputy Attorney Monaco also addressed the efforts by the USA and international partners to disrupt Volt Typhoon, a botnet of hundreds of US-based small/office internet routers hijacked by China. The compromised devices "were vulnerable because they had reached 'end of life' status; that is, they were no longer supported through their manufacturer's security patches or other software updates" (see here). As described by the Attorney General and the head of the USDOJ's National Security Division, the Chinese-controlled botnet was being used to target critical infrastructure (communications, energy, transportation and water sectors), to cause real-world harm and undermine US national security.

While the national security threats they discussed were US-centric, in fact, the discovery of the malicious Chinese Volt Typhoon botnet reflected a broadly international collaboration among cybersecurity and national security authorities, such as the National Security Agency in the USA and its counterparts in Australia, Canada, New Zealand and the UK (see here). In February 2024, CISA and the international agen-

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

cies noted that the threat to critical infrastructure extended well beyond the USA:

"[T]he US authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions. The US authoring agencies are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts. CCCS assesses that the direct threat to Canada's critical infrastructure from PRC state-sponsored actors is likely lower than that to US infrastructure, but should US infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors."

The International Counter Ransomware Initiative and Co-ordinated Law Enforcement Operations

With regard to international co-operation on ransomware, in November 2023, 50 members of the International Counter Ransomware Initiative (CRI) met at the White House for the third conference of the CRI. In addition to nation-state members of the CRI, the EU and INTERPOL also participate. Notably, China and Russia do not participate.

At the White House meeting, the CRI members reaffirmed their:

"joint commitment to building our collective resilience to ransomware, co-operating to undercut the viability of ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to co-operate internationally across all elements of the ransomware threat."

The CRI gathering in Washington, DC identified key deliverables, including:

- leveraging AI to counter ransomware;
- launching information-sharing platforms to share threat indicators;
- encouraging reporting of ransomware incidents to relevant governments; and
- sharing blacklisted crypto wallets used by ransomware actors through the US Treasury Department, etc.

Moreover, a task force established by the CRI continues to support transnational law enforcement operations, like those described below (see also here).

International co-operation in disrupting ransomware groups has been increasingly robust and successful. In January 2023, the USDOJ announced its "months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms and critical infrastructure" (see here). The USDOJ recognised the critical co-operation of criminal authorities in Germany, the Netherlands and Europol, as well as substantial assistance from Canada, France, Lithuania, Norway, Romania, Spain and the UK.

In a similar international operation, in December 2023 the USDOJ announced the disruption of the ALPHV/Blackcat ransomware group:

"Over the past 18 months, ALPHV/Blackcat has emerged as the second most prolific ransom-

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

ware-as-a-service variant in the world based on the hundreds of millions of dollars in ransoms paid by victims around the world. Due to the global scale of these crimes, multiple foreign law enforcement agencies are conducting parallel investigations."

The disruption included the FBI's development of a decryption tool saving victims from millions of dollars of ransom demands.

Most recently, in February 2024 the USA and the UK, working together with other international law enforcement authorities, disrupted the LockBit ransomware group, which was described as the most active ransomware group in the world (see here). The agencies destroyed the online infrastructure of LockBit, seizing and disrupting servers, and filed criminal charges against implicated Russian nationals.

The UK National Crime Agency played the lead role in the disruption campaign (see here), and announced on its website that it had taken control of LockBit's "primary administration environment", including modifying the group's website to state:

"This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'."

In conclusion, the colourful and many-badged image the global law enforcement agencies placed on the ransomware group's website says it all about the seriousness of international collaboration against cybercrime (see here).

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com