Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2023

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

Introduction
Alan Charles Raul
Sidley Austin LLP

practiceguides.chambers.com

INTRODUCTION

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

Good Government is Fighting Back on Cybersecurity

In 2022, the world of cybersecurity response moved boldly beyond the realm of personal information data breaches toward focus on disclosure and disruption of cyber-events and critical infrastructure incidents.

In March 2023, the White House issued its major new National Cybersecurity Strategy. The Strategy replaces the prior strategy document issued by the prior administration in 2018. It is intended to reflect a considerably more pro-active role for the government in advancing cybersecurity, and has been characterized – and criticized – by some as too "regulatory."

Perhaps most significantly, the Strategy calls for a "rebalancing" of the responsibility to defend cyberspace by shifting liability for insecure software products and services to their developers and relevant tech companies and by constraining the ability of software developers to fully disclaim liability by contract (ie, pursuant to end user licence agreements, or EULAs). The Strategy states that the marketplace imposes inadequate costs on – and often rewards – those entities that introduce vulnerable products or services into the digital ecosystem. The document states that while "companies that make software must have the freedom to innovate… they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers". The White House indicates it will work with Congress and the private sector to develop legislation establishing liability for software, and to prevent developers and manufacturers from disclaiming liability. While this attempted shift is sure to be controversial, and the administration concedes it will take years (if not decades) to play out, it is an aggressive gambit nonetheless.

In addition to the striking initiative to impose new liability, shape market forces and constrain freedom of contract with respect to software and related tech products, the Strategy also includes numerous other important cybersecurity "pillars". Specifically, the Strategy contains details of how it will provide for increased protection for critical infrastructure, promote further disruption and dismantling of global cyber threat actors, forge international partnerships to pursue shared cyber goals, and invest in a more cyber resilient future.

The new document elaborately describes the administration's approach to implementing and co-ordinating elements of the Strategy, and discusses how the Strategy builds on various existing laws, Executive Orders and other policy documents. The White House Office of the National Cyber Director (ONCD) and the National Security Council (NSC) are accorded primary responsibilities, along with the Office of Management and Budget, Cybersecurity and Infrastructure Security Agency (CISA) and Sector Risk Management Agencies (SRMAs) (such as the Department of Energy, Department of Defense, etc).

With regard to disclosure of incidents, the Strategy highlights legislation enacted by the US Congress in 2022, namely the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Under CIRCIA, which will be implemented pursuant to final regulations by CISA, covered cyber-incidents and ransom payments must be reported to CISA, generally within 72 hours from reasonable belief that a covered incident

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

has occurred, or within 24 hours of making a ransomware payment.

These reports are intended to enable CISA to deploy resources rapidly and provide assistance to defenders to warn other potential victims. Co-ordination and harmonisation are also important objectives of cyber-incident reporting. CIRCIA calls on the US Department of Homeland Security to establish an intergovernmental Cyber Incident Reporting Council "to coordinate, deconflict, and harmonize federal incident reporting requirements". In the same vein, CISA has launched a Joint Ransomware Task Force.

Importantly, CIRCIA stipulates there be a clear line prohibiting cyber-reporting information provided to CISA for incident response purposes to be used by regulatory agencies for enforcement purposes. The Act states the following.

"Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to (CISA)… to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity".

Other US federal and state agencies also require or are contemplating requirements for reporting non-personal data breach cyber-events to the agency. For example, the lead banking agencies currently require their regulated entities to report certain cyber-incidents to their regulators even if only systems are impacted and customer data is not, and the New York Department of Financial Services requires the same for banks and insurance companies under its purview.

The SEC has proposed rules that, if finalised, could require publicly traded companies to submit filings to the SEC that would become instantly public – disclosing significant cyber-events regardless of whether law enforcement, national security or cybersecurity agencies call for continued confidentiality about the event; disclosure could be required even when the relevant cybersecurity vulnerabilities remain unpatched and premature exposure could exacerbate risks for companies generally. Needless to say, many commenters on the proposed regulation have suggested the SEC may be misguided with regard to requiring such premature public disclosure. In another, less controversial proposed regulation, the SEC would require that SEC-regulated investment advisers report cyber-incidents they experience privately to the SEC. Most recently, on 15 March 2023, the SEC announced a slew of additional proposed cybersecurity rulemakings, including with respect to safeguarding investor personal financial information and requiring investor notification of data breaches affecting such information.

Similar to CIRCIA, the EU's new Network and Information Systems Security Directive (NIS2 Directive) would establish a minimum level of cybersecurity across the Union. NIS2 entered into force on 17 January 2023, and aims to harmonise and strengthen security and resilience throughout the EU. Significantly, the Directive imposes direct obligations and liability on senior management of companies, including administrative fines and potential employment-related discipline.

Two related EU laws entered into force simultaneously with the NIS2 Directive. The new EU Digital Operational Resilience Act harmonises cybersecurity and resilience of IT systems used by the financial services industry, and the new

INTRODUCTION

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

EU Critical Entities Resilience Directive does the same for critical infrastructure (namely 11 critical sectors such as energy, transport, financial market infrastructures, and digital infrastructure).

NIS2 applies to "essential" and "important" entities, and requires security elements such as the following:

- internal policies on risk analyses and IT security;
- measures and policies on incident handling;
- business continuity measures, eg, disaster recovery;
- supply chain security measures;
- measures related to securing network and information systems acquisition, development and maintenance;
- policies and procedures to assess the effectiveness of cybersecurity measures;
- basic cybersecurity hygiene and cybersecurity training for staff;
- HR security, access controls and access management; and
- the use of multi-factor authentication or continuous authentication solutions and secure communication channels.

Essential and important entities are required to notify relevant authorities, and (as appropriate) their service recipients, of any cyber-incident with significant impact – meaning incidents which:

- have caused or are capable of causing severe operational disruption or financial loss for the entity; or
- have affected or are capable of causing considerable material or non-material damage to other (natural or legal) persons.

Importantly, such incident reporting requirements will be triggered as soon as there is an incident with significant impact, and irrespective of whether or not personal data is involved. Early warning reports must be provided within 24 hours of becoming aware of the incident, followed by a more formal notification within 72 hours, and lastly a final report a month later. The relevant authority can also compel or itself provide public notice of the incident.

With regard to disruption, the US Department of Justice and Federal Bureau of Investigation have had considerable success against ransomware threat actors. In 2021, they recovered substantial ransomware payments in the millions of dollars from the attackers against Colonial Pipeline. On 26 January 2023, DOJ announced that the FBI had infiltrated the Hive network, thwarting over USD130 million in ransom demands. DOJ's release stated the following.

"Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay USD130 million in ransom demanded. Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims. Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims."

INTRODUCTION

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

Also, in April 2022, DOJ/FBI disrupted a global botnet known as "Cyclops Blink" controlled by the GRU, Russia's military intelligence agency. The US Deputy Attorney General stated in February 2023 that, working with the UK, the US "disabled Russia's control over those devices before they could be deployed in an attack – against Ukraine, against us, or our allies. Our work protected innocent victims in the United States, the UK, and around the world".

Global cyber co-ordination among western allies is thus ascendant. In November 2022, the White House brought together 36 countries and the EU for the Second International Counter Ransomware Initiative (CRI) Summit. Throughout the Summit, CRI and private sector partners discussed and developed concrete, co-operative actions to counter the spread and impact of ransomware around the globe.

Over the next year, the White House indicated that the CRI will carry out the following actions.

- Establish an International Counter Ransomware Task Force (ICRTF), led by Australia, and create a fusion cell at the Regional Cyber Defense Centre (RCDC) in Kaunas, led by Lithuania, to test a scaled version of the ICRTF and operationalise ransomware-related threat information sharing commitments.
- Deliver the following:
  - (a) an investigator's toolkit, including lessons learned and strategies for responding to significant ransomware events and proactively tackling major cybercriminal actors;
  - (b) resources to build capacity to effectively disrupt the threat of ransomware; and
  - (c) consolidated "tactics, techniques, and procedures" (TTPs) and trends for key identified actors.
- Institute active and enduring private-sector engagement based on trusted information sharing and co-ordinated action to improve joint work towards operational disruption.
- Publish joint advisories outlining TTPs for key identified actors.
- Co-ordinate priority targets through a single framework, focused on hard and complex targets. These initiatives will be translated into concrete disruption results with law enforcement groups.
- Develop a capacity-building tool to help countries utilise public-private partnerships to combat ransomware.
- Undertake biannual counter ransomware exercises to further develop, strengthen, and integrate a collective approach to combatting ransomware from resilience to deterrence.

In all, while the scourge of both nation-state sponsored and sophisticated cybercriminal attacks is not abating, the world's democratic governments are taking increasingly meaningful and effective steps to fight back.

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 US 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 US Chamber Litigation Center, the governing Board of Directors of the Future of Privacy Forum, and the Council on Foreign Relations.

Sidley Austin LLP

1 S Dearborn St
Chicago, IL 60603
United States

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

SIDLEY

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