Skadden

Privacy & Cybersecurity Update

Biden Administration Issues Executive Order Focused on Improving US Cybersecurity and Incident Response

On May 12, 2021, the Biden administration issued an executive order (EO) focused on improving the prevention, detection, assessment and remediation of cybersecurity incidents by federal agencies. The Executive Order on Improving the Nation's Cybersecurity[1] follows recent attacks on critical infrastructure and technology companies that significantly impacted U.S. government agencies, private companies and consumers, including the Colonial Pipeline and SolarWinds incidents.

Outline of the Executive Order

The EO looks to improve several areas of the U.S. government's cybersecurity and incident response through updating standard contract language and setting forth requirements and guidelines for federal agencies and their software and technology providers.

Cyber Information Sharing. The Office of Management and Budget (OMB), in consultation with other federal agencies, must implement changes to the standard contractual language in the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFAR) for contracting with technology service providers to increase the sharing of cybersecurity threat and incident information. Under the new language, service providers will be required to:

- collect and preserve data, information and reporting relevant to cybersecurity event prevention, detection, response and investigation on all information systems over which they have control, including systems operated on behalf of agencies;
- share such data, information and reporting related to cyber incidents or potential incidents relevant to any agency with which they have contracted and any other agencies deemed appropriate;
- collaborate with federal cybersecurity or investigative agencies in their investigations of, and responses to, incidents or potential incidents involving federal information systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support; and
- share cyber threat and incident information with federal agencies.

[1] The Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) can be accessed here.

The EO also directs updates to the FAR to (1) require information and communications technology (ICT) service providers to report software-related cyber incidents to any agencies to which it has provided its products and the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of discovery and (2) standardize cybersecurity contractual requirements for all agencies.

New Federal Government Cybersecurity Standards. The EO requires all federal agencies to take steps to modernize their approaches to cybersecurity. For example, OMB, CISA and the Federal Risk and Management Program (FedRamp) must develop a cloud security strategy, a cloud-security technical reference architecture and a cloud-service governance framework for federal agencies. Each agency must then update any existing plans for the adoption and use of cloud technology and develop plans to implement Zero Trust Architecture in line with this guidance. The EO also requires federal agencies to adopt multifactor authentication and data encryption for data at rest and in transit to the maximum extent possible within 180 days.

Software Supply Chain Security. The EO notes that there is a need for increased security around the development of software used by federal agencies, particularly regarding "critical software" that performs functions vital to trust, such as affording or requiring elevated system privileges or direct access to networking and computing resources. This issue was put into the forefront following the SolarWinds incident, in which attackers used the software provider's technology to gain access to many federal agencies and private companies. To facilitate this increased security, the EO directs the National Institute of Standards and Technology (NIST) to develop guidance and standards for secure software development, including securing development environments; demonstrating the performance of secure environment processes; employing automated tools to ensure the integrity of source code and identify and address vulnerabilities; and engaging in a vulnerability disclosure program, among several other practices. The EO requires updates to the FAR to include contract language requiring compliance with NIST's guidance for suppliers of software available for purchase by federal agencies.

Cybersecurity Safety Review Board. The EO requires the creation of the Cyber Safety Review Board (CSRB), which will be tasked with reviewing and assessing "significant cyber incidents"[2] affecting federal and non-federal systems, threat activity, vulnerabilities, mitigation activities and federal agency responses. The CSRB's initial review will focus on the SolarWinds incident and offer recommendations on cybersecurity and incident response improvements. The CSRB will include representatives of the Department of Defense, the Department of Justice, CISA, the National Security Agency and the FBI, as well as representatives from private-sector cybersecurity or software suppliers and other participants as determined by the secretary of homeland security.

Standardizing Incident Detection and Response. The EO requires several activities designed to standardize the detection of, and response to, cybersecurity vulnerabilities and incidents for Federal Civilian Executive Branch (FCEB) agencies. First, CISA, in consultation with several other agencies, must develop a standard playbook for cybersecurity vulnerability and incident response activity for use by all FCEB agencies. Second, FCEB agencies must adopt and deploy a standard endpoint detection and response approach to facilitate the early detection of cybersecurity vulnerabilities and incidents on federal networks. Finally, federal agencies must implement requirements for collecting, maintaining and securing network and system logs for federal information systems.

Key Takeaways

While the EO's impact on the nation's cybersecurity will not be fully understood until after the relevant agencies publish their new guidance, standards and contractual language, some aspects will likely have a wide impact. In particular, the secure development standards likely will be widely used and improve the security of federal and private systems given the broad scope of enterprise software used by federal agencies. These standards also may increase the costs of development for many providers. The uniform cybersecurity contractual language and cybersecurity standards also will likely improve the nation's cybersecurity and bring needed consistency. Finally, while the CSRB is clearly modelled after the National Transportation Safety Board (NTSB), it is unclear what impact it will have on the nation's security as it will lack the NTSB's regulatory authority to push through needed changes following an incident.

Return to Table of Contents

[2] As defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination).

Irish High Court Allows Investigation Into Data Transfers From the European Economic Area to the US

On May 14, 2021, the Irish High Court dismissed Facebook's challenge to the Irish data protection commissioner's (DPC) draft decision to investigate and suspend the company's data transfers from the European Economic Area (EEA) to the U.S. The decision allows the DPC to proceed with its investigation and, potentially, suspend Facebook's data transfers between the two regions. The decision is the latest in a series of decisions that stem from complaints issued by Austrian privacy activist Max Schrems in connection with international transfers of European individuals' personal data.

The Irish High Court Decision

In July 2020, the Court of Justice of the EU handed down its judgment in the *Schrems II* case. The decision invalidated the EU-U.S. Privacy Shield as a means of transferring personal data from the EEA to the U.S. and imposed enhanced due diligence requirements on companies seeking to use the European Commission Standard Contractual Clauses (SCCs) as a data transfer mechanism. Following the S*chrems II* decision, the DPC launched an investigation into Facebook's arrangements for EEA to U.S. data transfers and issued a draft decision stating the SCCs used by Facebook could no longer be relied upon as a transfer mechanism. This was, per the DPC's draft decision, because the SCCs could not compensate for the inadequate protection of EEA personal data under applicable U.S. laws, as well as Facebook's seeming lack of supplementary measures to address such inadequacy. Facebook disputed the draft decision and the investigation itself, arguing that the DPC should not have commenced an investigation until further regulatory guidance was published concerning possible supplementary measures. In the May 14, 2021, ruling, the Irish High Court dismissed all of Facebook's claims, ruling that the company did not establish a valid basis to strike down the DPC's investigation or its draft decision. The decision does not mean that Facebook's EEA to U.S. data flows must stop immediately, but the DPC is now free to continue its investigation and potentially finalize its draft decision.

Key Takeaways

The Irish High Court's ruling does not have immediate consequences for data transfers or the validity of SCCs. However, organizations that use SCCs to transfer personal data from the EEA to the U.S. should note these factors:

- The court ruling, and how the DPC will proceed in the near future, will inform how supervisory authorities in the EEA and the U.K. may act when reviewing data transfers taking place on the basis of SCCs. On May 27, 2021, the European Data Protection Supervisor (EDPS), the EU's independent data protection authority, announced that it has launched two investigations into cloud service providers concerning their compliance with *Schrems II*. If supervisory authorities find that SCCs cannot be used for EEA to U.S. data transfers, organizations will have limited options to make such transfers validly (*i.e.*, binding corporate rules, derogations). Accordingly, this might impact global data flows generally from the EEA.
- The European Commission continues to develop a new set of SCCs, a draft of which was first published in December 2020 with the final set of new SCCs expected to be published in the second quarter of 2021. If supervisory authorities deem the existing set of SCCs inadequate to protect personal data transferred from the EEA to the U.S., the European Commission may be incentivized to expedite the finalization of the new SCCs.
- In the Facebook case, the DPC will have to submit its decision to the other EEA supervisory authorities under the cooperation and consistency mechanism set out under the General Data Protection Regulation 2016/679 (GDPR). If there are no objections, the decision will become binding, though it is unclear what the outcome may be. The cooperation and consistency mechanism that potentially may be used in the Facebook matter was recently used in relation to the DPC's administrative fine against Twitter. In that matter, the mechanism slowed down the data transfer process considerably, with the final decision issued in December 2020, 23 months after the DPC commenced the investigation.
- Since the U.K. is no longer a member of the EU, the decision does not have direct consequences for data flows from the U.K. to the U.S. However, the U.K.'s Information Commissioner's Office (ICO) may find the DPC's arguments persuasive. That said, during the ICO's Data Protection Practitioners' Conference, the ICO revealed that it was working on a new set of SCCs to cover U.K. to U.S. data transfers under the U.K. GDPR. Similar to the European Commission and the potential new EEA SCCs, the ICO may be further incentivized to promptly finalize U.K. SCCs, with the consultation period for the U.K. SCCs expected to begin this summer.

Return to Table of Contents

The GDPR: Three Years on and Looking Ahead

On May 25, 2021, the GDPR marked its third anniversary since coming into force in 2018. Although the impact of the regulation has been significant for companies and data subjects, certain challenges remain for the future of the legislation.

The GDPR is widely considered one of the most fundamental pieces of data protection legislation in the EU and across the world. Accordingly, three years on, the European Data Protection Board (EDPB) still describes the GDPR as "a lighthouse for the entire global policy-making scene […] illuminating long-held privacy and data protection values enshrined across the horizon of the European legislative landscape." The regulation is designed to protect what the EU considers fundamental rights of data subjects, and holds both controllers and processors of personal data to a high standard of security, transparency and accountability. However, despite its evident successes, the GDPR still suffers from shortcomings that policymakers and data privacy professionals are eager to address in the coming years. In particular, the effects of Brexit, Schrems II and other recent developments in the European data protection space have presented challenges that will need to be considered going forward.

Three Years of the GDPR

The International Association of Privacy Professionals (IAPP) marked the GDPR's anniversary by releasing an infographic[3] pointing to several noteworthy statistics from the past three years:

- **GDPR Compliance.** Of the companies surveyed worldwide, 47% now self-report as "fully" or "very" compliant with the GDPR, compared to 39% last year. The IAPP noted that U.S.-based companies are outspending EU-based ones on privacy, though more EU companies responded as being very or fully compliant with the GDPR compared to U.S. companies.
- **Enforcement and Fines.** There have been more than 630 GDPR enforcement actions since 2018. Fines for noncompliance have totaled over €283 million in the last three years, including the €57 million fine issued by the Commission nationale de l'informatique et des libertés (CNIL) against Google and the €41 million fine issued by Germany's data protection authority against H&M.
- **Global Impact.** Since the GDPR came into effect, 17 countries around the world have enacted their own national privacy laws, including Brazil and New Zealand; 11 countries have imposed a data protection officer requirement, including the United Arab Emirates, Serbia and Thailand; and six countries have introduced a privacy enforcement authority. In addition, there have been 67 U.S. state-level comprehensive legislative proposals, with Virginia passing its Virginia Consumer Data Protection Act on March 2, 2021, and data privacy bills in Colorado, Connecticut, Illinois, Massachusetts, New York and Texas currently being discussed in committee.

Recent Developments

The GDPR has had a sustained impact over the last three years. Following the inevitable flurry of activity after May 25, 2018, (as companies subject to the GDPR scrambled to put comprehensive compliance programs in place), countries around the world have had relevant changes pertinent to the data protection framework.

In the last 12 months alone, we have seen a number of landmark changes to data protection in Europe:

- **Brexit and U.K. Adequacy.** The U.K.'s withdrawal from the EU on January 31, 2020, resulted in significant uncertainty regarding financial, trade, regulatory and legal implications. In particular, companies feared the potential for divergent national laws and the possibility of the U.K. being considered a third country for the purpose of transferring data outside of the EEA. On February 19, 2021, the EU issued a draft adequacy decision for personal data transfers from the EEA to the U.K., finding that the UK ensures an adequate level of data protection. The EDPB offered comments on this decision on April 14, 2021, acknowledging that the U.K. has largely mirrored the GDPR and the Law Enforcement Directive in its data protection framework (which includes the U.K. GDPR). However, the adequacy decision must still be officially approved by each EU Member State, and there is currently uncertainty as to how long this process will take. In the interim, transfers of personal data from the EEA to the U.K. will not be considered transfers to a third country.
- ***Schrems II* and Data Transfers.** On July 16, 2020, the European Court of Justice reached a decision in the landmark case of *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II)*. The court invalidated the EU-U.S. Privacy Shield as a legitimate mechanism for transferring personal data from the EEA/U.K. to the U.S. and other third countries, while also casting doubt on the validity of the European Commission's SCCs. Companies are therefore opting to add supplementary measures to their SCCs in order to afford additional protections to transfers of data outside of the EEA/U.K. Additionally, as mentioned earlier in this mailing, the European Commission is expected to adopt a new set of modernized SCCs better suited to today's digital framework

[3] The full IAPP infographic can be viewed here.

(possibly in the second quarter of 2021), with the ICO also promising a bespoke set of U.K. SCCs by the end of 2021. Until these new SCCs are released, significant uncertainty remains regarding international data transfers.

Key Takeaways

Looking to the future, the EDPS described the GDPR as a "three-year-old who must still learn to walk before it runs," and stated that the focus in Europe must be on enforcement actions going forward. This sentiment has been echoed by the CNIL, which announced on March 2, 2021, that enforcement in the targeted advertising and cookies space would once again be one of its top priorities this year.

Companies also should pay close attention to the looming threat of data-led class action lawsuits, particularly in relation to cookies violations. The recent parallel claims brought against Oracle and Salesforce in the Netherlands (as a class action) and in the U.K. (as a representative action) demonstrate an increased appetite in this space, though the outcome of these proceedings may still be a long way off.

In today's ever-growing and ever-changing data protection landscape, the GDPR likely will continue to need to adapt to new challenges and developments going forward.

Return to Table of Contents

European Data Protection Supervisor Provides Guidance on Distributed Ledger Technology

The EU's European Data Protection Supervisor released an "Opinion on the European Commission's Pilot Regime for Market Participants Using Distributed Ledger Technology," providing insight into how blockchains may be regulated by European data protection authorities in the future.

Background

On April 23, 2021, the EDPS provided an opinion on the European Commission's "Proposal for a Regulation of the European Parliament and of the Council" (the proposal) regarding a pilot regime for certain market participants using Distributed Ledger Technology (DLT), most commonly known as blockchain technology. The proposal, which was implemented on September 24, 2020, establishes requirements for specific market participants (including investment firms, market operators and central securities depositories) to be granted permission to operate DLT market infrastructures in a supervised environment and to be permitted specific exemptions for compliance with financial regulations. Among other aspects, the proposal seeks to provide legal certainty for crypto assets and protect consumers and investors, while also enabling innovation in blockchain, distributed ledger technology and crypto assets.

The opinion provides data protection guidance from the EDPS on the proposal, while also including general guidance on the application of privacy regulations to DLT. Over the past few years, the EU has been shaping its strategy on data protection and blockchain technology. Accordingly, many in the sector have questioned how the GDPR can be applied to blockchain applications given the technology's highly decentralized and immutable structure. Concepts in the GDPR, such as identifying data controllers and data processors and providing data subjects with the right to have their data erased, present interesting challenges in a blockchain ecosystem. In 2019, the European Parliament Panel for the Future of Science and Technology released a report that provided clarity on some of these issues (the STOA Report).[4] Prior to the STOA Report, the only other official statement on blockchain and GDPR was a much shorter overview of the issues published by the CNIL.

While the opinion is advisory in nature and leaves open many questions regarding the compatibility of blockchain technology with the GDPR, it outlines how companies that use blockchain technology must continue to take data protection and privacy into consideration. We detail the key takeaways from the opinion below.[5]

The Opinion

General Recommendations Regarding DLT

The EDPS found that, depending on the DLT's configuration, transactional or metadata stored on a DLT may be considered personal data if it relates to an identified or identifiable natural person. Further, even if transactional data is encrypted or hashed, such data also may be considered personal data according to the EDPS, as it is not irreversibly prevented from identification. This finding is somewhat consistent with the findings in the STOA Report, where the European Parliament found that public keys qualify as personal data, though it was noted that further guidance would be required to clarify whether it is possible to identify an individual based on a single set of data (*e.g.*, public keys), as well as how this should be viewed from the perspective of the data controller or from any third party who might be able to access the data. The STOA Report left open whether encrypted data could be deemed anonymous to anyone other than the holder of

[4] See Skadden's September 2019 client alert "The Distributed Ledger: Blockchain, Digital Assets and Smart Contracts" for further discussion on the STOA Report.

[5] The EDPS opinion can be accessed here.

the decryption key (and thus outside of the GDPR). This opinion therefore suggests that the EDPS would likely consider such data to be personal data and therefore within the scope of the GDPR. However, the opinion leaves open a number of challenges presented in the STOA Report, including, for example, whether a set of off-chain data that has been deleted remains personal data.

The EDPS also noted that certain DLT systems may use different technologies that store content off-chain, and therefore controllers must carefully analyze and document the DLT's configuration in order to determine whether personal data is processed and whether the operations are subject to data protection obligations accordingly.

Similar to the STOA and CNIL reports, the EDPS acknowledged that data categories stored through DLT systems may vary significantly depending on the particular technology, including if a DLT system is public and permissionless (*i.e.*, a system where anyone can validate transactions or submit transactions). The EDPS recognized that public and permissionless blockchains create unique challenges under the GDPR, particularly regarding determining controller and processer roles, the cross-border scope of the transactions the DLT permit, and the immutability and perpetual data storage capabilities, which contrast with European data protection principles regarding accuracy to the right to object. How the EDPS, or other data protection authorities, will resolve such challenges, however, was left open for further discussion.

Specific Requirements for Market Participants Under the Proposal

The EDPS also included specific recommendations for participants of the proposal in its opinion. Notably, the EDPS found that because the rules of the proposal relate to proprietary DLTs (that participants operate and use to provide certain services or activities), participants would likely be considered controllers under the GDPR when recording and settling transactions in DLT transferable securities involving on-chain personal data.

In addition, the EDPS noted that, in situations where DLTs contain on-chain personal data, processing operations will likely meet the criteria that result in the classification that the processing operation is high-risk (*e.g.*, there is data processed on a large scale, datasets that have been matched or combined, innovative use or applying technological or organizational solutions, and/or data transfer across boarders outside the EU). As a result, the EDPS also found that controllers would therefore need to carry out a data protection impact assessment prior to the processing of personal data.

The opinion also includes, among other things, recommendations regarding the activities and roles for the processing of personal data within the operation of DLT market infrastructures and makes specific recommendations for data protection safeguards within the DLT market infrastructures. This includes safeguards that ensure the integrity, security and confidentiality of data stored, and the availability and accessibility of such data.

Key Takeaways

The opinion demonstrates that companies that use blockchain technology cannot disregard privacy and data protection considerations, even in the absence of formal regulation under the GDPR or from European data protection authorities. However, the opinion also highlights the many challenges in applying the GDPR to blockchain technology, particularly with respect to public and permissionless blockchains. Companies should therefore continue to monitor developments in the space in order to stay apprised as data protection authorities continue to develop and shape their position on blockchain technology.

Return to Table of Contents

FTC Offers Guidance to Corporate Boards Regarding Their Role in Data Security Oversight

The Federal Trade Commission (FTC) published informal guidance directed to corporate boards of directors that reinforces data security as a board-level priority for companies.

On April 28, 2021, the FTC published informal guidance on its business blog highlighting the prevalence of cybersecurity threats to businesses and the need for corporate boards to become more involved with their respective companies' data security and data management programs.[6] The guidance suggests that boards should adopt practices such as routine security briefings and continued monitoring of industry- and organization-specific security risks, as well as resulting regulatory enforcement efforts.

FTC Recommendations

The FTC's blog post included the following "common-sense" recommendations:

1. **"Make data security a priority."** Data security programs should incorporate stakeholders from departments across the company at both the executive and operational expert levels. Cyber risk oversight duties, whether delegated to a particular

[6] "Corporate Boards: Don't Underestimate Your Role in Data Security Oversight," Federal Trade Commission Business Blog (April 28, 2021).

board committee or another body, should be a priority for the board, with all members being informed, engaged and updated on a regular basis.

2. **"Don't confuse legal compliance with security."** Risk programming should aim to go beyond merely meeting the requirements of compliance obligations. Rather, boards should evaluate their company's actual security practices and consider whether such practices are sufficient in the context of the company's business, including consideration of data processing practices and related security risks.
3. **"It's more than just prevention."** A strong data security program alone is not enough; companies also should implement a robust incident response plan to ensure that if and when an attack or data breach incident occurs, such incident can be managed quickly and effectively.
4. **"Learn from mistakes."** Boards should use the opportunity, either from their own company's data breach or from incidents experienced by other companies in a similar line of business, to understand the risks facing the industry.

Key Takeaways

With the increasing prevalence of data breaches and cybersecurity incidents, the FTC's guidance is a reminder to corporate boards of their role in preventing and managing data security issues. Companies should take steps to make sure that their boards are updated regularly regarding cyber and data security issues, including regarding specific issues that the company is facing and issues that are applicable to the company's industry as a whole.

Return to Table of Contents

Ninth Circuit Affirms IT Cyber Insurance Coverage Does Not Apply for $4.75 Million Email Scam Loss

The U.S. Court of Appeals for the Ninth Circuit has declined to revive information technology company Alorica, Inc.'s (Alorica) lawsuit against its cyber insurer seeking coverage for an approximately $4.75 million loss arising from an email scam.[7]

On April 9, 2021, the Ninth Circuit affirmed a ruling from the U.S. District Court for the Central District of California holding that Alorica's cyber insurer, Starr Surplus Lines Insurance Company (Starr), did not owe Alorica coverage for its $4.75 million loss stemming from an email scam on the basis that there was no "claim" under Starr's policy.

Alorica's Email Scam Loss and Insurance Claim

Beginning in October 2017, hackers gained access to Alorica's email system, likely through a phishing attack. The hackers posed as an Alorica employee and communicated directly with Alorica's clients, asking them to route payments to a "new" account controlled by the hackers. One of Alorica's clients, Express Scripts Holdings Inc. (Express Scripts), complied with the request, inadvertently wiring $4,807,115 — an invoice payment that was intended for Alorica — to the hackers' account.

Not long thereafter, Alorica alerted Express Scripts that it had not yet received the $4.8 million payment for its services. Express Scripts responded by letter explaining that it had already paid the invoice, albeit to the hackers' fraudulent account. Express Scripts offered to pay Alorica the $56,791 that its bank was able to recover, but stated that it would not make any additional payment on the outstanding invoice. As a result, Alorica was left with an approximately $4.75 million loss.

Alorica turned to its cyber insurer, Starr, to cover the loss. The policy included coverage for loss arising from any "Claim" made against Alorica for a "Security Failure," with "Claim" defined, in relevant part, as a "written demand for monetary or non-monetary relief." While Starr acknowledged that a "Security Failure" had occurred, it disclaimed coverage on the ground that Express Scripts' letter did not constitute a "Claim" under the policy, and therefore the policy's insuring agreement was not triggered.

Coverage litigation between Alorica and Starr then ensued. On the parties' cross-motions for summary judgment, the district court agreed with Starr, ruling that Alorica failed to demonstrate that Express Scripts' letter constituted a claim under Starr's policy. Alorica appealed.

The Ninth Circuit Ruling

A three-judge panel for the Ninth Circuit affirmed the district court's ruling, reasoning that Express Scripts' letter did not constitute a "Claim" under the policy because it was not a "demand for monetary or non-monetary relief." To the contrary, Express Scripts' letter affirmatively *rejected* Alorica's demand for full payment of the $4.8 million invoice, with the court explaining that "a refusal to accept a demand is not itself a demand; it is only a refusal." The court further reasoned that Express Scripts' letter asked nothing of Alorica. Rather, in the letter, Express Scripts offered to cooperate with Alorica's investigation into the fraud and agreed to pay the amount that Express Scripts' bank had recovered, with no consideration from Alorica expected.

[7] *Alorica, Inc. v. Starr Surplus Lines Ins. Co.*, 843 F. App'x 927 (9th Cir. 2021).

The court also rejected Alorica's argument that Express Scripts' letter should be read as a demand that Alorica forgive a debt, which, in Alorica's view, would constitute a demand for monetary relief. Here, the court observed that Express Scripts denied that it owed Alorica any money, and Alorica had no made no further effort to collect the invoice from Express Scripts.

The court concluded its opinion by reiterating that the refusal of another's demand without more actions involved does not constitute a demand.

Key Takeaways

The Ninth Circuit's decision serves as an important reminder that not all cyber-related losses fit neatly into coverage under a policy. Policyholders and insurers alike would be well-advised to review their insurance policies to ensure that they understand the scope of coverage provided for potentially costly cyber losses. This is particularly true of fundamental provisions and definitions, such as the "Claim" definition at issue in *Alorica*, which can dictate whether a policy has been triggered in the first instance.

Return to Table of Contents

UK and US Agencies Issue Advisory on Practices Associated With Russian Intelligence Cyber Actors

On May 7, 2021, the U.K. National Cyber Security Centre and several U.S. federal security agencies jointly released an unclassified cybersecurity advisory titled "Further [Tactics, Techniques, and Procedures] Associated with SVR Cyber Actors." The advisory details several methodologies that Russia's civilian foreign intelligence service, known as the SVR, uses to target overseas networks and extract intelligence. This publication follows the U.K. and U.S.'s attribution to the SVR of the SolarWinds supply chain compromise and the targeting of COVID-19 vaccine developers through WellMess and WellMail malware attacks.

Background

The U.K.'s National Cyber Security Centre, together with the U.S. National Security Agency, CISA and the FBI, jointly released an unclassified cybersecurity advisory detailing several newly identified tactics, techniques and procedures (TTPs) used by the SVR, as well as vulnerabilities the SVR leverages in its attacks. The advisory also provides updated mitigation advice and guidance to protect against SVR activity, especially in light of the rising prevalence of SVR supply chain attacks.

Updated SVR TTPs

SVR actors target overseas victims for intelligence gathering through active vulnerability scanning and exploitation of public-facing applications.

The advisory warns that the SVR monitors, and quickly pursues, new common vulnerabilities and exposures (CVEs) upon its announcement. For example, SVR actors have recently scanned for Microsoft Exchange vulnerabilities and targeted mailbox administrators to further access and understand networks.[8]

The SVR is known to target organizations that supply software to intelligence targets by manipulating and compromising such software prior to the final customer's receipt, then deploying additional malware post-compromise. The advisory identifies certain malware and command-and-control tools utilized by the SVR in these so-called supply chain attacks, including GoldFinder, GoldMax and Sibot, which were deployed against victims in the SolarWinds campaign post-compromise, as well as Silver — a new open source Red Team command-and-control framework.

Mitigation Advice and Guidance

The advisory provides guidance on mitigating the threat of SVR attacks, including the following recommendations to:

- regularly scan for and apply network security updates as soon as possible to prevent SVR actors' network access through CVEs and publicly known software vulnerabilities;
- respond promptly to CVE announcements;
- ensure compliance with basic cybersecurity practices, including the use of sound network security controls and effective management of user privileges to limit SVR movement between hosts;
- adopt detection methodologies to identify unusual network activity;
- implement adequate cloud and on-premises logging and storage practices to detect compromised accounts and exfiltrated information;

[8] The advisory details several such CVEs that the SVR has used. More information about the Microsoft exploits can be found here.

- adjust mail and content retention policies to limit the quantity of sensitive information accessible in the event of a system compromise; and
- Protect sensitive information, including that related to network architecture and security, with heightened standards.

Key Takeaways

As supply chain attacks become increasingly prevalent, companies should examine their systems to identify key threats, as well as recommended prevention and mitigation techniques. In particular, as the advisory suggests, companies should implement a patch program to close vulnerabilities in vendor software before such weaknesses can be exploited by threat actors.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000