Skadden

Privacy & Cybersecurity Update

US Treasury Highlights Risks to Financial Institutions for Facilitating Ransomware Payments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) both released advisories regarding the role of financial intermediaries in ransomware payments.

On October 1, 2020, the U.S. Department of the Treasury released two advisories aimed at combating ransomware attacks and identifying the risks of facilitating ransomware payments. Ransomware attacks are those in which an attacker seizes control of a victim's computer system (often by encrypting the data used by that system) and threatens to delete, damage or release the information unless the victim pays a ransom dictated by the attacker. The advisories come as ransomware attacks have increased amid the COVID-19 pandemic, particularly involving those in the government, financial, education and health care sectors.

OFAC Advisory

OFAC's "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments"[1] highlights the risks to financial institutions and other companies of facilitating ransomware payments on behalf of victims of ransomware attacks. The advisory emphasizes that paying such demands may create a sanctions risk to the institution and may, as a practical matter, encourage future ransomware attacks.

Accordingly, OFAC has designated ransomware attackers and entities that facilitate ransomware transactions under its cyber-related sanctions programs. Under the International Emergency Economic Powers Act and the Trading with the Enemy Act, U.S. persons are prohibited from transacting with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List, as well as other blocked persons and persons covered by comprehensive embargoes on jurisdictions. By designating these attackers and entities under its sanctions program, OFAC has made it possible for financial institutions that engage with ransomware attackers and payment facilitators to be found to have violated that program.

[1] A copy of the advisory is available here.

When determining its response to a violation of the sanctions program, OFAC will look to the company's sanctions compliance program. In the advisory, OFAC recommends that financial institutions (including those entities that engage with victims of ransomware attacks) implement a risk-based compliance program that accounts for the risks of making ransomware payments to sanctioned entities. The advisory also encourages companies to report ransomware attacks to law enforcement and cooperate during and after the attack, as OFAC will consider these actions as mitigating factors when determining enforcement outcomes.

Beyond the potential sanctions violation, the advisory identifies several issues with individuals and companies paying ransoms to sanctioned actors, stating ransomware payments:

- can be used to fund activities that present national security threats;
- may lead to future attacks; and
- do not guarantee that the victims will recover the impacted data.

FinCEN Advisory

FinCEN's "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments"[2] highlights the role of financial intermediaries in payments of ransomware attacks, identifies trends in ransomware tactics and outlines red flags that companies can use to identify likely ransomware payments.

The advisory warns that ransomware operations are becoming more sophisticated, and attackers are increasingly targeting larger enterprises and demanding higher ransoms as a result. Attackers also are working together to launch more complex and effective attacks, as well as using "fileless" ransomware, through which malicious code is written directly into a computer's memory. The advisory also highlights an increase in the use of double extortion schemes, in which attackers exfiltrate and encrypt sensitive data and demand a ransom to both recover the data and prevent the attacker from sharing or selling the data. Additionally, attackers are increasingly demanding payment in anonymity-enhanced cryptocurrencies, which use mixing and cryptographic enhancements to further reduce the transparency of ransomware payments.

FinCEN's advisory notes that ransomware payments often involve converting payments into a cryptocurrency and then transferring that currency to criminal-controlled accounts (often through a series of intermediary steps and organizations intended to obscure the payment and the attackers' identities). The advisory goes on to state that, depending on the facts and circumstances involved, this activity could constitute money transmission, and that entities engaged in money services business activities (such as money transmission) are required to register with FinCEN as a money services business. Such organizations would then be subject to enforcement under FinCEN and are subject to Bank Secrecy Act obligations, including filing suspicious activity reports (SARs) when appropriate.

The advisory outlines 10 instances that signal to financial institutions that ransomware activity has occurred:

- Malicious activity can be discovered through IT enterprise activity, including log files, network traffic or file information.
- Customers identify that payments are in response to ransomware activity when opening a new account or interacting with the financial institution.
- The address the customer uses to transact has been linked to ransomware strains or payments.
- A transaction occurs between an organization and a digital forensics and incident response company (DFIR), or a cyber insurance company (CIC).
- A DFIR or CIC customer sends an amount to a convertible virtual currency (CVC) exchange in the same amount recently received from a customer company.
- During onboarding, a customer is not knowledgeable about CVC but later purchases CVC.
- A customer makes a large CVC transaction with no history of CVC transactions.
- A customer appears to be using liquidity to execute large, offsetting transactions between CVCs without identifying itself to the CVC exchanger or registering as a money transmitter.
- A customer uses a CVC exchanger or money services business in a high-risk jurisdiction without adequate anti-money laundering and countering financing of terrorism regulations.
- A customer makes multiple trades between multiple CVCs in a short period without any apparent related purpose.

[2] A copy of the advisory is available here.

The advisory also provides information on how financial intermediaries can file SARs related to ransomware attacks.

Key Takeaways

Organizations faced with a ransomware attack are in a difficult position. It is tempting for them to pay the requested ransom rather than incur the time and expense necessary to recover its data and systems if and when the attacker makes good on its threats. As the OFAC advisory makes clear, however, companies that decide to pay the ransom may find themselves running afoul of U.S. sanctions laws, and in any event may simply encourage future attacks by the same or different attackers. The FinCEN advisory, in turn, reminds financial institutions that enable ransomware payments that they may have a duty to file SARs with respect to such activity, while also providing practical suggestions on how financial institutions might identify such payments taking place through their systems.

Return to Table of Contents

Israeli Privacy Protection Authority Determines EU-US Privacy Shield is No Longer a Valid Data Transfer Mechanism

The Privacy Protection Authority of Israel (PPA) announced that the EU-U.S. Privacy Shield is no longer a valid mechanism through which data can be transferred from Israel to the U.S.

On September 29, 2020, the PPA announced that the Privacy Shield arrangement previously negotiated between the United States and the EU would no longer be deemed a valid mechanism for transmitting personal information from Israel to the U.S. This announcement, published in a position letter,[3] was made approximately two months after the EU's invalidation of the Privacy Shield in the *Schrems II* decision, and further complicates the data privacy landscape for companies that seek to transfer personal information across jurisdictional lines.[4]

Impact of *Schrems II*

Israel's privacy regulations piggyback off of the EU's General Data Protection Regulation (GDPR) by allowing the transfer of personal information from Israel to countries that receive personal information from EU member states using mechanisms permitted by the GDPR.

Prior to *Schrems II*, companies in the U.S. could rely on the Privacy Shield as a self-certification mechanism for data transfers from the European Economic Area (EEA) to the U.S. The Privacy Shield (in addition to the European Commission Standard Contractual Clauses) was a data transfer mechanism that addressed the perceived inadequacy of U.S. privacy laws when viewed under the European Commission's privacy standards. On July 16, 2020, the Court of Justice of the European Union (CJEU) struck down the Privacy Shield in its ruling in *Schrems II*, arguing that there were limitations on the protection of personal data under U.S. law, and that U.S. authorities' access and use of EEA data were disproportionate and without effective redress mechanisms in place for data subjects.

Under Israeli law, the Privacy Shield also was an approved framework for transferring personal data from the country to the U.S. After *Schrems II*, Israel initially continued to acknowledge the validity of the Privacy Shield. The PPA's position letter has changed that policy, so companies must now rely on other data transfer mechanisms permitted under the Israeli privacy regulations, including through contractual arrangements.

Israel is yet another country that has followed the EU's decision to invalidate the Privacy Shield. Similarly, in early September, the Swiss federal data protection and information commissioner concluded that the Swiss-U.S. Privacy Shield regime did not adequately protect data transferred to the U.S. from Switzerland.[5]

Key Takeaways

It is unclear which — if any — countries would continue to allow the transfers of personal information to the U.S. under the Privacy Shield, though it is very clear that the framework is becoming less useful to multinational operations. Therefore, companies should not rely solely on the Privacy Shield as a means for authorizing international data transfers and should examine alternate methods.

Return to Table of Contents

[3] The position letter is available in Hebrew here.

[4] For more on the *Schrems II* decision, please see our July 2020 update here.

[5] For more on the Swiss decision, please see our September 2020 update here.

CJEU Finds Belgian, French and UK Mass Surveillance Laws Incompatible with EEA Law

On October 6, 2020, the CJEU concluded that mass surveillance laws in Belgium, France and the U.K. are invalid because they conflict with European Economic Area (EEA) laws, which may have potential significant implications for the U.K. as it approaches the end of the Brexit transition period at the end of 2020.

Background

Certain EU member states' national security laws require telecommunications services providers (TSPs) to collect and retain certain communications data, such as users' traffic and location data. Such data, which is collected indiscriminately and concerns all users of telecommunications services, can then be analyzed by national intelligence agencies for national security purposes, including by cross-checking the data with other databases held by those agencies. Privacy activist groups in Belgium, France and the U.K. brought claims challenging the legality of the countries' so-called "mass surveillance" laws. The CJEU joined the cases of *Ordre des barreaux francophones et germanophone and others* from Belgium,[6] *La Quadrature du Net and Others* from France,[7] and *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* from the U.K.,[8] (collectively, *La Quadrature du Net and Others*). The national courts in each case referred separate legal questions to the CJEU, the details of which are discussed below.

Does the ePrivacy Directive Apply?

The CJEU decided that the mass data retention and collection practices of member states for national security purposes must comply with EEA law, including the GDPR and the ePrivacy Directive. Article 1(3) of the ePrivacy Directive excludes matters that relate to public security, defense or state security from its scope.

However, the CJEU stated that this exclusion relates to activities of the state itself, while Article 3 of the ePrivacy Directive makes clear that the directive regulates the activities of TSPs. Therefore, the national laws in question fall within the scope of the ePrivacy Directive.

Are National Surveillance Laws Incompatible With EEA Law?

Article 5(1) of the ePrivacy Directive states that member states shall "ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services," and "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications" of such data. Consequently, the CJEU found that users of telecommunications services are entitled to expect that their communications (and data relating to their communications) remain anonymous and not be recorded, unless they agree otherwise.

Article 15(1) of the ePrivacy Directive allows member states to introduce an exemption to Article 5(1) where such exemption constitutes a "necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences." This exemption allows member states to introduce measures that provide for the retention of data on one of the relevant national security grounds.

However, the CJEU was clear that such an exemption cannot become the rule. The scope of Article 15(1) also must take into account the Charter of Fundamental Rights, including the Article 7 right to privacy. Any exemption to Article 5(1), including in relation to Article 15(1), must be limited to what is strictly necessary, and should "lay down clear and precise rules governing the scope and application of the measure in question," imposing minimum safeguards so as to ensure that the individual has sufficient guarantees that their personal data will be protected from the risk of abuse.

The CJEU found that the "general and indiscriminate" data retention measures under the national laws could not be said to be limited to what is strictly necessary. This does not mean that national surveillance agencies are prohibited in all circumstances from accessing individuals' communications data, such as the traffic and location data in this case. However, any access by national surveillance agencies to such data must be done on the basis of objective criteria that defines the circumstances and conditions under which such access may be granted. The sheer volume of data presents the risk of abuse and unlawful access, according to the CJEU.

Therefore, the CJEU concluded that national laws that require TSPs (on a general and indiscriminate basis) to collect and retain traffic and location data, and transmit the same to national intelligence agencies, are incompatible with EEA law.

[6] Case C-520/18

[7] Cases C-511/18 and C-512/18

[8] Case C-623/17

Key Takeaways

- **Brexit.** On January 1, 2021, the Brexit transition period will end and the U.K. will become a "third country" for the purposes of data transfers from the EEA to the U.K. under the GDPR. The smoothest transition for organizations transferring personal data between the EEA and the U.K. would be if the European Commission recognized the U.K. as providing "adequate" levels of data protection that are "essentially equivalent" to the GDPR. Such an adequacy decision would allow personal data to continue to flow freely between the EEA and the U.K. However, the CJEU's decision in *La Quadrature du Net and Others* means that the U.K.'s Regulation of Investigatory Powers Act 2000 is not compatible with EEA law. Organizations should therefore assume that the U.K. will not receive an adequacy decision from the European Commission before January 1, 2021, and implement alternative data transfers mechanisms to govern personal data transfers from the EEA to the U.K. The U.K. government has stated, however, that data transfers from the U.K. to the EEA will not be restricted.[9]
- ***Schrems II.*** The CJEU's decision comes three months after the *Schrems II* decision, in which the court invalidated the EU-U.S. Privacy Shield in part due to the indiscriminate access to personal data under U.S. surveillance programs. The *Schrems II* and *La Quadrature du Net and Others* decisions share a common concern: access to personal data by the state. In both cases, the CJEU's view is clear that mass surveillance is too blunt of a tool and national laws permitting indiscriminate access to personal data for national security purposes do not comply with EEA law.

Return to Table of Contents

California Attorney General Issues Proposed Modifications to CCPA Regulations

California Attorney General Xavier Becerra announced a series of proposed clarifications and other changes to the California Consumer Privacy Act (CCPA) regulations. The changes come less than two months after an initial set of implementing regulations.

On October 12, 2020, Mr. Becerra announced an unanticipated set of proposed modifications to the initial CCPA implementing regulations, merely two months after the initial regulations became effective on August 14, 2020. These proposed modifications are aimed at clarifying and refining requirements related to opt-out notices and processes, verifying authorized agent requests, and providing notices to minors. The deadline to submit written comments to the proposed regulatory modifications was October 28, 2020.

Background

Less than two months after approval of the initial set of CCPA implementing regulations put forth by the California Office of Administrative Law on August 14, 2020, the Mr. Becerra proposed new updates to the those regulations, seeking to provide clarifications in specific compliance areas. These latest proposals[10] follow the publication and approval of the initial set of regulations, which were the result of months of hearings, public notices and comment periods by the attorney general. The relatively short period of time between the start of finalization of the current regulations and release of the proposed modifications suggests that the attorney general may currently see broad noncompliance or misunderstanding of the regulations in certain areas. While most of the proposed modifications apply to businesses that sell personal information (under the CCPA's broad definition), the revisions also include important changes regarding businesses receiving requests from authorized agents.

Proposed Regulation Modifications

The proposed modifications include updates in four key areas: (1) offline opt-out notices; (2) consumer opt-out flow; (3) verification for authorized agent requests; and (4) notices to minors.

1. Offline Opt-Out Notices

The first modification concerns businesses that sell the personal information of consumers and collect personal information offline. The proposed updates would require such businesses to "provide notice by an offline method that facilitates consumers' awareness of their right to opt-out." The proposed language goes on to provide examples of where information is collected in-person at a brick-and-mortar store or over the phone. Where personal information is collected at a physical store, the proposed modifications advise either printing a paper form for the collection of personal information that includes the notice or posting physical signage in the area where the personal information is collected that directs consumers to the online notice. Where personal information is collected over the phone, the modifications advise providing the notice orally during the call where such information is collected.

[9] See the Information Commissioner's Office Brexit Frequently Asked Questions for more information.

[10] Text of Proposed Modifications.

2. Consumer Opt-Out Flow

The second modification also applies to covered businesses that sell personal information of consumers. The proposal would add a new subsection to the existing regulation to clarify that a business's opt-out submission process must be "easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out." Furthermore, the designated opt-out method cannot "use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out." The proposal also includes a number of illustrative examples of the types of actions it seeks to prevent, including:

- The business's process for consumers to submit a request to opt-out cannot require more steps than the process for a consumer to opt-in after having previously opted out. For an opt-out, the number of steps is measured from when the consumer clicks a "Do Not Sell My Personal Information" link until completion of the request, and the number of opt-in steps is measured from the consumer's first indication to the business of their interest to opt-in until completion of the request.
- A business cannot use confusing language when providing consumers the choice to opt-out (such as double-negatives).
- A business cannot require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request (unless otherwise permitted under the regulations).
- The business's process for consumers to opt-out cannot require the consumer to provide personal information that is unnecessary to implement the request.
- Once the consumer clicks the "Do Not Sell My Personal Information" link, the business cannot require the consumer to search or scroll through a privacy policy or similar document or webpage to locate the mechanism to submit an opt-out request.

3. Verification of Authorized Agent Requests

This proposed modification edits existing language concerning a business's processing of consumer requests submitted through authorized agents, which impacts all businesses subject to the CCPA. Importantly, this clarification distinguishes between what a business may require of the submitting authorized agent and what it may require of the consumer who is making the request.

First, the proposal confirms that the business may require the submitting authorized agent (as opposed to the consumer) to provide proof of the consumer's signed authorization to submit the request. Second, the proposal would maintain the right of a business to directly contact the consumer to confirm (1) the consumer's identity or (2) the authority of the agent to submit the request associated with that consumer. As a result, upon approval of this regulatory modification, businesses may wish to explicitly require all authorized agents to include such signed consumer approvals as a part of their request submission process to minimize the number of necessary follow-up interactions for each request.

4. Notices to Minors

The final proposed change impacts businesses that sell the personal information of minors and updates existing regulatory language. This modification would clarify that a business selling the personal information of minors under 13 and/or from 13 to 15 years old must include descriptions of its compliance procedures with certain CCPA requirements in its privacy policy. One possible interpretation and source of misunderstanding in the current language is that such disclosures are only required where the business sells the personal information of minors in both age groups.

Key Takeaways

Mr. Becerra's focus on these specific issues at this time suggests that the businesses that the attorney general's office has analyzed thus far may have had a variety of unsatisfactory interpretations of the current requirements of the CCPA, such that further clarification was necessary in these modifications. Businesses would be well-served to consider how they would account for these proposed modifications if they went into effect, especially those businesses that determine they "sell" personal information. With Californians set to vote on Proposition 24, the proposed California Privacy Rights Act of 2020 on November 3, 2020, and with certain temporary CCPA compliance exceptions to expire on January 1, 2021, businesses must remain vigilant in tracking CCPA developments over the coming months as statutory obligations and regulatory enforcement measures continue to evolve.

Return to Table of Contents

Privacy & Cybersecurity Update

British Airways Fined £20 Million for 2018 Data Breach

On October 16, 2020, the U.K.'s Information Commissioner's Office (ICO) issued a penalty notice to British Airways (BA) under the GDPR following a 2018 cybersecurity attack that compromised the credit card details of over 400,000 customers. The £20 million penalty is a significant decrease from the £183 million penalty initially proposed under the ICO's earlier notice of intent (NOI) issued in July 2019.

Background

Prior to the attack, BA had been providing remote access credentials to its network to a third-party provider of cargo services. In 2018, an attacker was able to obtain these credentials and gain undetected access to BA's internal systems, which did not require multi-factor authentication. The attacker was able to locate unencrypted cardholder data, which it then redirected to an external third-party domain controlled by the attacker, a process known as "skimming," affecting what BA estimated to be 430,000 data subjects. BA's logging of the unencrypted cardholder data was not intentional, but the result of human error. After a two-month period, the breach was detected by a third party. BA immediately contained the vulnerability and notified the ICO and affected customers. Following the issue of the NOI and multiple rounds of negotiations with BA, the ICO issued its final penalty notice of £20 million.

Breach of the GDPR

The ICO's penalty notice was issued in regards to BA's failure to comply with its obligations under:

- **Article 5(1)(f) of the GDPR**, which requires organizations to process data in a manner that ensures appropriate security of that data, using appropriate technical and organizational measures; and
- **Article 32 of the GDPR**, which requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the relevant risk.

The ICO referred to these provisions of the GPDR by comparing the adequacy and appropriateness of BA's data security measures against the risks that the company knew of or could have reasonably foreseen. Based on this approach, the ICO found that BA had failed to ensure appropriate security for its processing of personal data and that the attack could have been prevented, or at least mitigated, if the company had implemented appropriate measures.

The ICO reached its conclusion after reviewing the technical and organizational measures BA implemented and the measures the agency believed it should have implemented. The ICO emphasized that there was publicly available guidance that clearly warned of, and suggested strategies to mitigate, the actions eventually taken by the attacker. Such mitigation strategies included using multi-factor authentication, whitelisting, blacklisting, least privilege access and IPSec VPN. BA's failure to implement such strategies came alongside its failure to carry out rigorous testing, as well as internal penetration tests, manual code reviews and logging measures. In addition, BA used hardcoded passwords, which are generally seen as problematic and widely advised against. Taken cumulatively, the ICO considered that BA had failed to implement appropriate measures and was therefore in breach of its GDPR obligations.

Penalty Assessment

Making clear that the figure in the NOI was not the starting point for its assessment of the penalty amount, the ICO's penalty calculation focused on the penalty for breach itself, any aggravating and/or mitigating factors, and the economic impact of COVID-19.

- **Penalty for the breach.** As discussed above, BA could have implemented various measures to ensure that personal data was processed securely. The ICO noted that BA's failure to implement such measures affected over 400,000 data subjects, many of whom have suffered anxiety and distress as a result. Additionally, the breach may never have been detected had it not been discovered by a third party. The ICO concluded that the breach flowed entirely from BA's negligence and that a company of its stature should have been aware it may be targeted. Taken together, an initial penalty of £30 million was deemed appropriate.
- **Mitigating factors.** The ICO noted no aggravating factors in making its ruling. BA's immediate implementation of measures to minimize the damage, prompt notification to data subjects and the ICO, and its cooperation throughout the process were all considered mitigating factors. In addition, customers were reimbursed and provided with free credit monitoring, and remedial technical measures were introduced following the attack. Interestingly, the ICO also considered that this incident may raise individuals' awareness of cybersecurity risks at BA and may have an adverse effect on the company's brand and reputation. These mitigating factors led the ICO to reduce the initial penalty sum by 20%.
- **COVID-19.** In light of the pandemic's significant economic impact on the aviation industry, the ICO reduced the penalty by a further £4 million to reach a final penalty of £20 million.

Additional Claims

In addition to the £20 million fine, BA is facing a civil claim from the affected data subjects. The case is not likely to be heard until late 2021 at the earliest, as the cutoff date for affected data subjects to join the group litigation is April 2021. Given the lack of precedent for such privacy group litigation claims, the potential damages that could stem from the claim are uncertain.

Key Takeaways

The BA case presents a number of key lessons for companies operating in the U.K. under GDPR:

- **Take note of available guidance and perform testing.** Throughout its penalty notice, the ICO referred to BA's failure to follow publicly available cybersecurity guidance, such as the ICO's own guidance and that of other bodies, such as the U.K.'s National Cyber Security Centre and the U.S. National Institute for Standards and Technology. Companies should regularly review their internal cybersecurity processes and standards against prevailing cybersecurity best practices. They also should perform regular penetration tests and vulnerability assessments to verify the organization's cybersecurity robustness, and promptly address any remediation actions resulting from such tests or assessments. In line with the GDPR's accountability principle, companies should document their cybersecurity reviews.
- **Data protection training.** BA customers' cardholder data was accessed because it was unencrypted due to human error. It may not be possible to eliminate human error, but organizations can take steps to minimize their occurrence. Employees that receive regular data protection training, both in general and specific to their role, are more likely to be aware of data protection risks. Organizations should keep training logs in place, and such training should occur at least on an annual basis.
- **Prompt notification and cooperation.** The ICO noted that BA "acted promptly" and "cooperated fully with [its] investigation and has taken that into account." Regardless the amount of the potential fine at stake, organizations should consider fully cooperating with the relevant supervisory authority. Failure to do so may be considered an aggravating factor in calculating any applicable penalties and fines.

Return to Table of Contents

Cyber Insurance Market Continues To Mature and Expand, Recent Survey Finds

A survey conducted by insurance companies PartnerRe and Advisen shows that the cyber insurance market has continued to expand and mature, signifying an increased focus on the threat of cyberattacks for companies of all sizes.

Insurance companies PartnerRe and Advisen recently published a report summarizing the results of their seventh annual joint survey of cyber insurance market trends, revealing that the cyber insurance market has continued to mature and expand in 2020, while also identifying certain key marketplace trends.[11] This year's survey was conducted during the second quarter of 2020 and polled 260 cyber insurance brokers and 190 cyber underwriters from around the world.

Continuing with the trend identified in last year's report, the manufacturing/industrial sector brought in the most new-to-market buyers of standalone cyber insurance, with 49% of respondents identifying the field as among the top three sectors with new-to-market buyers. The professional services sector took second place (43%) followed by the financial services/insurance sector (32%). Interestingly, the health care sector, which took the top spot in 2018, fell to fourth place (31%). According to the report, this "suggest[s] higher levels of cyber insurance penetration have now been reached in this industry known as a frequent target for data breach[es]."

Another continued trend revealed in the survey is the strong demand for cyber-related business interruption coverage, which respondents identified as the most requested cyber coverage (68%). In a change from last year, respondents identified cyber extortion/ransom coverage as the second-most requested coverage (61%) (replacing funds transfer fraud/social engineering coverage, which slid to the number three spot this year (53%)), which the report attributes to the increased prevalence and notoriety of costly ransomware attacks over the last year. The majority of respondents (60%) also reported insureds' frequent interest in higher limits at renewal, though the report indicated that such interest may have plateaued.

[11] The report is available here.

Consistent with last year's results, respondents identified the top two drivers of new cyber insurance sales as news of cyber-related losses experienced by others (66%) and the organization itself experiencing a cyber-related loss (62%). The third-place driver — up from fifth place in last year's report — is demand by board members or senior management (42%), which "signal[s] a new trend of increasing awareness of the [cyber] risks faced by organizations," according to the report.

As in previous years, the primary obstacles to cyber insurance sales reportedly are (1) organizations not understanding exposures (70%), (2) organizations not understanding coverage (51%) and (3) cost (50%). Other obstacles identified by respondents include differing policy forms and coverages in the market, the application process, scope of coverage and capacity constraints.

When asked about the GDPR, the majority of respondents (78%) agreed that it would "not have much of an impact until there are headline losses and legal precedent." The majority of respondents (77%) also agreed that the GDPR has not "significantly impacted pricing" for cyber insurance, though 43% of respondents did report that the GDPR has "significantly impacted policy wordings." Respondents also predicted that the impact of the CCPA on cyber sales would be similar to that of the GDPR.

Another continued trend is an increasingly competitive marketplace, with 63% of respondents stating that overall competition has increased, due at least in part to new marketplace entrants. Notably, that figure fell sharply from 86% and 90% in 2019 and 2018, respectively, signaling that competition may be leveling off. Respondents also reported increased competition substantially more for small/mid-size accounts (72%) than for large/national accounts (54%). In addition, the majority of broker respondents reported increased market consistency in both cyber insurance pricing (61%) and coverage (72%).

However, the report notes that there has been a trend toward higher pricing, with broker respondents reporting rate increases between 5% to 10%. Those respondents generally agreed that rate hikes were driven by increases in claim costs, particularly for ransomware claims. Nonetheless, respondents indicated that industry competition has compelled insurers to curb cost increases and offer expanded coverage.

Key Takeaways

As the report indicates, businesses across a range of industries increasingly are turning to cyber insurance as one component of their risk management plans. This demand is due to many factors, including increased awareness of cyber risks, with competition among insurers continuing to spur coverage expansion while containing cost increases. However, the longevity and trajectory of these trends remain to be seen, as the market is showing signs of maturation and insurers must manage loss frequency and severity in this ever-evolving environment.

Return to Table of Contents

Privacy & Cybersecurity Update

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