SEC ADOPTS INTERPRETIVE GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES

On 21 February, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

The guidance stresses that companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors. The SEC also encourages companies to consider adopting specific policies restricting executive trading in shares while a hack is being investigated and before it is disclosed. The SEC, in unanimously approving the additional guidance, said it would promote “clearer and more robust disclosure” by companies facing cybersecurity issues.

According to Reuters, the new guidance will mean an increase in information disclosed on cyber-attacks and risks. “This essentially creates a mandatory new disclosure category - cyber security risks and incidents,” said Spencer Feldman, an attorney with Olshan Frome Wolosky LLP. Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP said the SEC guidance “makes clear that it doesn’t want a repeat of the Equifax situation.”

According to the SEC’s statement, “we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation
which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

We remind companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.”

Read more: the full guidance from the SEC is available here.

“However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.”

US COMMODITY FUTURES TRADING COMMISSION (CFTC) BRINGS CYBERSECURITY ENFORCEMENT ACTION

The U.S. Commodity Futures Trading Commission (CFTC) issued on February 12, 2018 an Order filing and simultaneously settling charges against AMP Global Clearing LLC (AMP), a registered Futures Commission Merchant since 2010, for its failure between June 21, 2016 and April 17, 2017 to supervise diligently the implementation of critical provisions in AMP’s information systems security program (ISSP). As a result of this failure, a significant amount of AMP’s customers’ records and information were left unprotected for nearly ten months. In April 2017, as a result of this failure, a third party unaffiliated with AMP (Third Party) accessed AMP’s information technology network and copied approximately 97,000 files, which included customers’ records and information, including personally identifiable information. The Third Party thereafter contacted federal authorities about securing the copied information and subsequently informed AMP that the copied information had been secured and was no longer in the Third Party’s possession.

James McDonald, the CFTC’s Director of Enforcement, commented: “Entities entrusted with sensitive information must work diligently to protect that information. That’s not only good business, but when it comes to registrants in our markets, it’s the law. As this case shows, the CFTC will work hard to ensure regulated entities live up to that responsibility, which has taken on increasing importance as cyber threats extend across our financial system.”

Specifically, the Order finds that AMP failed to supervise its IT Provider’s implementation of ISSP provisions it was delegated with implementing under AMP’s supervision, including identifying and performing risk assessments of access routes into AMP’s network, performing quarterly network risk assessments to identify vulnerabilities, maintaining strict firewall rules, and detecting unauthorized activity on the network. This failure left a significant amount of AMP’s customers’ records and information vulnerable to cyber-exploitation for nearly ten months, until the Third Party accessed AMP’s network.
The Order finds that the vulnerability in AMP’s network involved an open access route in a network attached storage device (NASD). Three successive quarterly network risk assessments failed to identify this vulnerability. Indeed, the Order finds that, before the Third Party accessed the NASD’s contents, the media had reported three other incidents of unauthorized access of NASDs used by organizations other than AMP, including some from the same manufacturer of AMP’s NASD. Yet AMP did not detect the vulnerability until its network was accessed and customer records and information compromised.

The Order requires AMP to pay a $100,000 civil monetary penalty and cease and desist from violating the CFTC regulation governing diligent supervision. The Order further requires AMP to provide two written follow-up reports within one-year of entry of the Order to the CFTC verifying AMP’s ongoing efforts to maintain and strengthen the security of its network and its compliance with its ISSP’s requirements.


“Entities entrusted with sensitive information must work diligently to protect that information. That’s not only good business, but when it comes to registrants in our markets, it’s the law”.

SINGAPORE TO INTRODUCE A NEW MANDATORY BREACH NOTIFICATION REGIME

On February 1, 2018, Singapore’s Personal Data Protection Commission (PDPC) released its response to feedback received from a public consultation launched in July 2017 on “Approaches to Managing Personal Data in the Digital Economy.” The PDPC sought views on the relevance of other bases for collecting, using and disclosing personal data under the Personal Data Protection Act (PDPA), namely the proposed “Notification of Purpose” and “Legal or Business Purpose” approaches. The PDPC also proposed a mandatory data breach notification regime for notification of data breaches to PDPC and affected individuals under the PDPA. These proposals are part of the PDPC’s review of the PDPA.

The PDPC considers that notifying individuals of the purpose (“Notification of Purpose”) can be an appropriate basis for an organization to collect, use and disclose personal data where the collection, use or disclosure of personal data is not expected to have any adverse impact on the individuals. The PDPC intends to incorporate the Notification of Purpose as part of the consent framework under the PDPA, so that, in parallel to the existing actual consent (i.e. express consent) and the deemed consent (i.e. inferred by the conduct of the individual), a new opt-out approach would be made available where an individual is (i) notified of the purposes of the collection, use or disclosure of his personal data; (ii) provided a reasonable time period to opt out but (iii) does not opt out within the time period. Under this approach, an organization would have to conduct a risk and impact assessment, such as a data protection impact assessment (DPIA), which should be documented, in order to ascertain whether the intended collection, use or disclosure is likely to have an adverse impact on the individual. The PDPC further clarified that it would not be possible to rely on this new Notification of Purpose approach for direct marketing purposes or for purposes that are likely to have an adverse impact or consequences from the individual (express consent of the individual would be needed in those cases). The PDPC will issue guidelines as to what would be considered “not likely to have any adverse impact”.
The PDPC further states that it will not specify how organizations are to notify individuals: it is up to the organizations to determine the most appropriate way of doing so based on their specific circumstances, and to ensure they take reasonable steps to inform individuals of the purposes and how they may opt out. The PDPC indicates that it will provide further guidance on circumstances where large volumes of personal data are instantaneously and seamlessly collected (e.g. data collected by sensors).

The PDPC recognizes that there are circumstances where organizations need to collect, use or disclose personal data without consent for a legitimate purpose, but they are not authorized to do so under the PDPA or other written laws, for example in relation to the sharing and use of personal data to detect and prevent fraudulent activities. Following the public consultation, the PDPC intends to provide for the collection, use or disclosure of personal data regardless of consent where it is necessary for a “legitimate interest”. The PDPC had originally proposed the concept of “legal or business approach”, however, in response to suggestions to instead use the term “Legitimate Interests” as adopted in the European General Data Protection Regulation (GDPR), the PDPC has now decided to opt for the concept of “legitimate interest”. The PDPC will provide clarification in guidelines on the purposes that fall in scope.

The PDPC intends to require a benefit to the public as a condition, and organizations would need to conduct a risk and impact assessment (such as a DPIA), which should be documented, in order to determine whether the benefits outweigh any foreseeable adverse impact to the individual. As an additional safeguard, the PDPC will require organizations to disclose their reliance on “legitimate interests” as a ground for collection use or disclosure, and make available a document justifying their reliance on “legitimate interests” and the business contact information of the person who is able to answer individuals’ questions about such collection, use or disclosure on behalf of the organization. In the event of complaints, the PDPC reserves the right to require organizations to disclose these assessments for the PDPC’s consideration.

A majority of responses received by the PDPC were supportive of the proposed mandatory breach notification regime. A breach notification would be required to affected individuals and to the PDPC if the breach is “likely to result in significant harm or impact to the individuals to whom the information relates”. A “significant scale” is needed for the breach to be eligible for notification, but the PDPC declined to prescribe a statutory threshold number of affected individuals. Notification to affected individuals would need to be done “as soon as practicable” and to the PDPC “as soon as practicable, no later than 72 hours”.

The PDPC intends to provide an assessment period of up to 30 days from the day the organization first becomes aware of the suspected breach to assess its eligibility for notification. The PDPC notes that this follows Australia’s notifiable data breach scheme, which allows organizations a 30-day assessment period for such breach. The organization would need to document steps taken in assessing the breach from the time it first becomes aware of it to demonstrate it has taken all reasonable and expeditious steps to assess the breach. Organizations may nevertheless choose to notify the PDPC of the suspected breach incident at any time during the assessment period in order to receive guidance from the PDPC where necessary. However, in any case, the PDPC stressed that the organization must notify the PDPC and affected individuals as soon as practicable (and in the case of the PDPC, within 72 hours) from the time the organization determines that the breach is eligible for reporting, regardless of whether it has fully utilized the 30-day assessment period.

Organizations will not be required to notify affected individuals of an eligible breach that is the subject of an ongoing or potential investigation under the law, if it is assessed that notifying affected individuals will compromise investigations or prejudice enforcement efforts under the law. Organizations that experience a loss of encrypted data that has been encrypted to a reasonable standard may be exempted from the requirement to notify affected individuals. An exception will also be introduced for organizations which have taken remedial actions to reduce the potential harm or impact to affected individuals. These exceptions do not however exempt
notifying the PDPC of eligible breaches. Where a data breach is committed by an employee acting in the course of his employment, the organization (not the employee) will be liable for the data breach under the PDPA and the organization will be responsible for complying with the data breach notifications under the PDPA. For data intermediaries processing personal data on behalf of and for the purposes of another organization, the 30-day assessment period to assess and establish the eligibility of the suspected breach commences from the time the data intermediary first becomes aware of the breach. The data intermediary would then have to notify the organization that it processes the personal data on behalf of without undue delay from the time it first becomes aware of the breach. Advisory guidelines will be issued by the PDPC to provide guidance for organizations in complying with the data breach notification requirements, including the considerations for assessing whether data breaches meet the criteria for notification, the time frame for notification and the types of information to be included in the breach notification to affected individuals and to the PDPC.

An organization must notify the relevant sectoral or law enforcement agency according to applicable legal or regulatory requirements, in addition to notifying the PDPC and affected individuals, in accordance with the applicable requirements in each case. In order to minimize the regulatory burden on organizations, they may adopt the same format of notification required for reporting to the other sectoral regulator or law enforcement agency for its breach notifications to the PDPC. Mechanisms for streamlining notifications to the PDPC and the relevant sectoral or law enforcement agencies will be further explored by the PDPC.

Read more: The PDPC's full response document (15 pages) is available here.

IN OTHER NEWS:

- Research: A Strong Privacy Policy Can Save Your Company Millions
- An Ai That Reads Privacy Policies So That You Don't Have To
- Yahoo's Brazil Unit Must Return Over Emails Stored Abroad

Research: A Strong Privacy Policy Can Save Your Company Millions

Read this article to understand how and why companies need to revise current privacy policies. In doing so, you are not only potentially saving your company from harm, but helping them down the line with their customer experience.

"Firms can use data privacy practices to protect themselves from the spillover effects of competitor’s privacy failures, but their efforts to do so need to be meaningful”.

Read the full article here: https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions

AN AI THAT READS PRIVACY POLICIES SO THAT YOU DON'T HAVE TO

This article covers a new technology which aims to make to make privacy policies easy to understand by everyone. As the article states (and we are definitely well aware): “those millions upon millions of words are produced for
the benefit of their authors, not readers”. One study from 2016 showed that people will agree to anything: 98% of the study’s participants didn’t realize that the policy for a fake social networking site gave all their personal information to the NSA and even required them to give up their first born child. A new technology aims at solving this problem. In about 30 seconds, the technology can read the policy and extract a readable summary, which would include things like: where the data can be send, opt out options, and data sharing.

Read the full article here: https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/

Yahoo’s Brazil Unit Must Return Over Emails Stored Abroad

Brazils top court ordered Yahoo Inc. to return emails that are stored abroad, and if they fail to do so they will be fined $15,000 daily.

Read the full article here: https://www.bna.com/yahoo-brazil-unit-n57982088614/

UPCOMING EVENTS

Internet of Things National Institute

Format: In-Person
Location: Crowell & Moring LLP
Date: May 9-10, 2018
Credits: 13.25 General CLE Credit Hours, 1.00 Ethics/Professionalism CLE Credit Hours

The Internet of Things (IOT) is defined as billions of vehicles, buildings, process control devices, wearables, medical devices, drones, consumer/business products, mobile phones, tablets, and other “smart” objects that are wirelessly connecting to and communicating with each other. This new top law practice area is raising unprecedented legal and liability issues.

As one of the most transformative and fast-paced technology developments in recent years, IoT will require businesses, policymakers, and lawyers (M&A, IP, competition, litigation, health law, IT/outsourcing, and privacy/cybersecurity) to identify and address the escalating legal risks of doing business in a connected world.

Attend this institute to:

- Discover why corporate, law firm, government, university, and other attendees gave the last two IoT Institutes rave reviews, calling it “magical,” “eye-opening,” with “rock star” speakers, and overall “a grand slam.”
- Gain insights and practical guidance on the latest legal, legislative, regulatory, and liability issues of the IoT transformation—a game-changer for businesses, policymakers, and lawyers that’s generating hundreds of billions of dollars in spending globally.
- Explore need-to-know IoT hot topics: big data/privacy, cybersecurity, litigation/mitigation, cloud/artificial intelligence, connected healthcare, ethics, global IoT product development and sales, insurance risk allocation, and homeland/national security.
- Get great value: Two (2) days of CLE credit (including ethics), including three (3) keynotes packed with compelling perspectives. There will also be opportunities for networking.
EDITORS

Paul Lanois - Mr Lanois is a global privacy, data protection and information security professional and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at conferences across Europe, Asia and the United States. He was named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. He was also recognized as a leading lawyer in The Legal 500's GC Powerlist. He has been recognized as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C).

Nathan M. Barotz - Mr. Barotz has been in the private practice of law for over 25 years. A graduate of Duke University (cum laude) and the George Washington University Law School, Mr. Barotz originally developed a focus on health care law which in the last ten years has led to his strong interest the rapidly developing body of law governing IoT, cybersecurity and privacy. For the last five years, Mr. Barotz has served in the role of general counsel and compliance and privacy officer for companies utilizing telemedicine technology in post-acute patient treatment and currently serves in that role for HomeSleep, LLC, a company which specializes in diagnostic testing for sleep apnea. Mr. Barotz is a member of the New York State and Connecticut State Bars, the United States District Court Bars, Southern District and Eastern District of New York and has received his CIPP/US certification from the International Association of Privacy Professionals.

Tamara Lev - Ms. Lev is a Data Privacy attorney, specializing in: data security, information security, and regulatory compliance. She assists her clients with diligence and care, while identifying potential privacy vulnerabilities and conducting information security risk assessments. Tamara is a law graduate from Ono Academic College with a LLB in Law. She is a Fordham Law School graduate with a LLM in Intellectual Property and Information Technology. Tamara is a member of the State Bar of New York.

THOUGHTS? COMMENTS?

We are always looking to make this newsletter better, as such, we hope you like the new format of the newsletter. As always, comments and suggestions are always welcome. You can send your feedback to paulanocom@aol.com.

You are currently subscribed to the American Bar Association's E-Privacy Law Committee mailing list. Your e-mail address will only be used within the ABA and its entities. We do not sell or rent e-mail addresses to anyone outside the ABA.

Update your profile | Unsubscribe | Privacy Policy

American Bar Association: 321 North Clark Street | Chicago, IL 60654 | 800-285-2221
Copyright © 2018 ABA, All Rights Reserved.