Privacy Risk Study 2017:
PII Remains Top Information Risk
Privacy Compliance Concerns Rise
Executive summary

The U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose potential risk factors, including cybersecurity concerns. The IAPP’s second annual study of the disclosure statements of 150 publicly traded companies shows that 100 percent of these companies identify cyber attacks in their 2016 10-K reports as current and ongoing risks, up from 86 percent in reports filed in 2015.

Losing customers’ or employees’ personally identifiable information (PII) remains first among disclosed information-related risks (87 percent). Moreover, for those companies disclosing privacy risk, reputational harm is the greatest consequence of concern (95 percent), far more than risk of remediation expenses (66 percent) and legal damages or regulatory penalties (69 percent).

Despite the fear of reputational harm, only 9 percent of companies specifically mention concern over compliance with state data breach laws and regulations. Indeed, companies continue to discuss compliance-related risks in only general terms, with 53 percent of companies citing general compliance with existing U.S. data privacy laws and 37 percent identifying compliance with non-U.S. regulations as risks to their investors. These numbers stand in stark contrast to the 10 percent that specifically mention HIPAA/HI-TECH compliance and less than 6 percent that specifically mention the U.S.-EU data transfer mechanism known as Privacy Shield.

Although more than half of the 150 surveyed disclosure statements mention the introduction of new privacy laws and legal standards as a risk, only about one in 10 (11 percent) specifically name the EU’s forthcoming General Data Protection Regulation as a compliance risk. While these numbers do represent a slight uptick from last year’s findings, we might anticipate more mention of the GDPR in next year’s report due to the GDPR’s May 2018 implementation deadline.

In this study’s Annex we include sample language used by selected companies in various industries to help you identify the emerging nomenclature of privacy risks.
Methodology

Pursuant to U.S. securities laws, companies that issue securities are required to file with the SEC annual reports that include a “Form 10-K.” Companies generally file 10-Ks shortly after the close of their fiscal year, typically December 31. Among the items to be disclosed on Form 10-K are the most significant factors that make the securities offered by the company speculative or risky to investors.

This year, the Westin Research Center analyzed the Form 10-K disclosures filed at the end of 2016 by 150 companies ranked in Fortune Magazine’s top 200 U.S. companies based on revenue. We categorized the risk disclosures made by these companies based upon their perceived privacy or security threats; the type of information companies felt was the most vulnerable; the companies’ legal concerns arising from cyber or privacy risks; and the possible business harms associated with these privacy and security risks.

We made some changes in our methodology from last year’s inaugural survey to facilitate analysis of singular items, such as the General Data Protection Regulation, and to allow for the use of percentages rather than raw numbers. The changed methodology does not always allow direct comparisons between this year’s and last year’s data, especially as the study pertains to compliance concerns, but should facilitate comparisons for future reports.

One limitation to our methodology is that more than one researcher was involved in the research, which could lead to variations in data input. We attempted to calibrate our methods and analysis, and the results were sufficiently consistent that we feel the error rate for this concern is rather low.
100 percent of companies report cyber attacks or hacking as a current and ongoing risk to investors

Once again, cyber attacks top the list of information-related threats to companies. Each company whose 10-Ks we reviewed reported cyber attacks, hacking or other malicious acts targeting information networks and systems as current and ongoing threats, up 14 percent from last year (and now it can’t go any higher), making it clear that data privacy and information security is an unavoidable concern, regardless of industry.

Following cyber attacks, the next greatest concern for companies is information loss or misuse by business partners or other third parties (69 percent). This represents a 22 percent increase over last year’s findings, reinforcing the importance of vendor management and the difficulty of ensuring that data processors and business partners practice sound security and privacy practices. Finally, following closely behind third-party negligence, companies have identified general IT system failures (63 percent) and employee error or malfeasance (53 percent) as major threats to their businesses. This last category may represent a bit of vulnerability blindness: Many studies show employee error as the leading cause of data breaches.
A cyber attack or other malicious incident can damage systems, but the biggest risk companies disclose is the loss of customers’ or employees’ personal information (PII) (88 percent), ahead of the loss of proprietary and confidential business information (71 percent) and far ahead of losing intellectual property (34 percent). Although losing IP through cyber espionage puts companies at a disadvantage relative to their competitors, it does not necessarily expose them to liability, damage to reputation, or loss of consumer trust like a breach of PII.

Only 15 percent of companies specifically identify as a risk the loss of payment card information and just one in 10 specifically mention “protected health information.” These terms are prevalent in U.S. data breach and health care law. As GDPR compliance becomes a more pressing risk factor for U.S. multinationals in Fortune’s top rankings, it will be interesting to see whether data other than PII is more or less often mentioned in 10-K risk disclosures.
Compliance and enforcement concerns

Only 63 percent of companies mention the risk of regulatory enforcement actions following a breach.

Although 100 percent of surveyed U.S. companies are warning investors about the risk of a data breach, only 63 percent of companies mention the risk of regulatory enforcement actions following a breach, and just over half – 52 percent – mention the risk of civil litigation or class action lawsuits. A negligible number mention the potential for criminal liability due to exposing personal data in a breach.

Risk of Legal Actions

- Regulatory enforcement action: 63.33%
- Civil actions/litigation, generally: 52.00%
- Criminal actions: 6.00%
- None (No mention of legal actions): 23.33%

Number of surveyed 10-Ks listing this threat

0 25 50 75 100 125 150

- 63.33%
- 52.00%
- 6.00%
- 23.33%
Companies are not universally concerned about compliance with privacy laws, either. To the extent legal compliance is mentioned, it is done in a general rather than specific manner: 51 percent of surveyed 10-Ks mention as an investor risk compliance with existing U.S. privacy laws in general, and 35 percent identify compliance with non-U.S. laws and regulations in general.

Just over half – 51 percent – mention that new privacy laws and legal standards may be a risk, but only 11 percent of companies mention the implementation of the GDPR specifically. This does indicate a slightly greater awareness of GDPR over the 2016 report, but we predict the reports being written and filed now – to be covered in next year’s survey – are much more likely to reflect concerns over the GDPR’s hefty penalties for non-compliance.
Brand and reputation most vulnerable in breach

So, if companies are not warning investors about regulatory enforcement, privacy law compliance concerns, or class action litigation following a data breach, what are the risks? For the second year, the results could not be more clear: Harm to brand or reputation is the top risk following a data loss incident, as reported by 95 percent of the surveyed companies. Just over eight in 10 mention general financial losses as a risk flowing from the data disclosure, including from lost sales.

Brand damage due to loss of PII in a breach significantly outweighs concerns about legal and regulatory penalties (69 percent) or the costs of remediation (65 percent). Of course, with the GDPR calling for regulatory enforcement penalties up to 4 percent of global revenue, regulatory penalties could be a more prominent risk disclosed in future 10-K reports.

Another major risk from a cyber attack or related harm to an IT network is system downtime, reported by 88 percent of companies. Finally, almost one in four companies mention that a severe data loss incident could exceed insurance coverage, and 10 percent mention expenditure of management time and resources to respond to the incident as a risk to their business and bottom line.
Conclusion

In this second annual look at privacy risk disclosures in SEC Form 10-K filings by publicly traded companies in the U.S., we find that businesses continue to be motivated to protect their PII primarily by risks of reputational harm and loss of consumer confidence. It will be important to monitor whether future breaches and changing international regulatory landscapes begin to change the way companies in the U.S. view their risks from mishandling personal data.
ANNEX

Following are excerpts from 2016 10-K risk disclosures relating to information privacy concerns. We selected them for comprehensiveness, industry, global perspective, and in some cases use of language that might be instructive or illustrative for others who have to review or prepare these reports. They have been edited for length, relevance and company identity. These forms can be found at www.sec.gov/edgar.

Global Retail Sector

The unauthorized access, use, theft or destruction of customer or employee personal, financial or other data or of Company's proprietary or confidential information that is stored in our information systems or by third parties on our behalf could impact our reputation and brand and expose us to potential liability and loss of revenues.

Our information technology systems, such as those we use for our point-of-sale, web and mobile platforms, including online and mobile payment systems and rewards programs, and for administrative functions, including human resources, payroll, accounting and internal and external communications, as well as the information technology systems of our third party business partners and service providers, can contain personal, financial or other information that is entrusted to us by our customers and employees.

Our information technology systems also contain Company proprietary and other confidential information related to our business, such as business plans, product development initiatives and designs. Similar to many other retail companies and because of the prominence of our brand, we have experienced frequent attempts to compromise our information technology systems. To the extent we or a third party were to experience a material breach of our or such third party's information technology systems that result in the unauthorized access, theft, use or destruction of customers’ or employees’ data or that of the Company stored in such systems, including through cyber-attacks or other external or internal methods, it could result in a material loss of revenues from the potential adverse impact to our reputation and brand, our ability to retain or attract new customers and the potential disruption to our business and plans. Such security breaches also could result in a violation of applicable U.S. and international privacy and other laws, and subject us to private consumer or securities litigation and governmental investigations.
and proceedings, any of which could result in our exposure to material civil or criminal liability. For example, the European Union adopted a new regulation that becomes effective in May 2018, called the General Data Protection Regulation (“GDPR”), which requires companies to meet new requirements regarding the handling of personal data, including its use, protection and the ability of persons whose data is stored to correct or delete such data about themselves. Failure to meet GDPR requirements could result in penalties of up to 4% of worldwide revenue. Our reputation and brand and our ability to attract new customers could also be adversely impacted if we fail, or are perceived to have failed, to properly respond to these incidents.

Significant capital investments and other expenditures could be required to remedy the problem and prevent future breaches, including costs associated with additional security technologies, personnel, experts and credit monitoring services for those whose data has been breached. These costs, which could be material, could adversely impact our results of operations in the period in which they are incurred and may not meaningfully limit the success of future attempts to breach our information technology systems.

Media or other reports of existing or perceived security vulnerabilities in our systems or those of our third party business partners or service providers, even if no breach has been attempted or has occurred, can also adversely impact our brand and reputation and materially impact our business. Additionally, the techniques and sophistication used to conduct cyber-attacks and breaches of information technology systems, as well as the sources and targets of these attacks, change frequently and are often not recognized until such attacks are launched or have been in place for a period of time. We continue to make significant investments in technology, third party services and personnel to develop and implement systems and processes that are designed to anticipate cyber-attacks and to prevent or minimize breaches of our information technology systems or data loss, but these security measures cannot provide assurance that we will be successful in preventing such breaches or data loss.

**Energy Sector**

Cyberattacks targeting Company’s process control networks or other digital infrastructure could have a material adverse impact on the company’s business and results of operations. There are numerous and evolving risks to cybersecurity and privacy from cyber threat actors, including criminal hackers, state-sponsored intrusions, industrial espionage and employee malfeasance. Although Company devotes significant resources to prevent unwanted intrusions and to protect its systems and data, the company has experienced and will continue to experience cyber incidents of varying degrees in the conduct of its business. Cyber threat actors could compromise the company’s
process control networks or other critical systems and infrastructure, resulting in disruptions to its business operations, injury to people, harm to the environment or assets, access to its financial reporting systems, or loss, misuse or corruption of critical data and proprietary information, including intellectual property, business information and that of its employees, customers, partners and other third parties. Cyber events could result in significant financial losses, legal or regulatory violations, reputational harm, and legal liability and could ultimately have a material adverse effect on the company’s business and results of operations.

Software/Technology Services Sector

Our industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users’ data. Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. In addition, computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future. As a result of our prominence, we believe that we are a particularly attractive target for such breaches and attacks. Such attacks may cause interruptions to the services we provide, degrade the user experience, cause users to lose confidence and trust in our products, or result in financial harm to us. Our efforts to protect our company data or the information we receive may also be unsuccessful due to software bugs or other technical malfunctions; employee, contractor, or vendor error or malfeasance; government surveillance; or other threats that evolve. In addition, third parties may attempt to fraudulently induce employees or users to disclose information in order to gain access to our data or our users’ data. Although we have developed systems and processes that are designed to protect our data and user data, to prevent data loss, and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security.

In addition, some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Company. We provide limited information to such third parties based on the scope of services provided to us. However, if these third parties or developers fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users’ data may be improperly accessed, used, or disclosed.
Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

Financial Sector

A failure to protect our computer systems, networks and information, and our clients’ information, against cyber attacks and similar threats could impair our ability to conduct our businesses, result in the disclosure, theft or destruction of confidential information, damage our reputation and cause losses.

Our operations rely on the secure processing, storage and transmission of confidential and other information in our computer systems and networks. There have been several highly publicized cases involving financial services companies, consumer-based companies and other organizations reporting the unauthorized disclosure of client, customer or other confidential information in recent years, as well as cyber attacks involving the dissemination, theft and destruction of corporate information or other assets, as a result of failure to follow procedures by employees or contractors or as a result of actions by third parties, including actions by foreign governments. There have also been several highly publicized cases where hackers have requested “ransom” payments in exchange for not disclosing customer information.

We are regularly the target of attempted cyber attacks, including denial-of-service attacks, and must continuously monitor and develop our systems to protect our technology infrastructure and data from misappropriation or corruption. We may face an increasing number of attempted cyber attacks as we expand our mobile- and other internet-based products and services, as well as our usage of mobile and cloud technologies and as we provide more of these services to a greater number of retail clients. In addition, due to our interconnectivity with third-party vendors, central agents, exchanges, clearing houses and other financial institutions, we could be adversely impacted if any of them is subject to a successful cyber attack or other information security event.

Despite our efforts to ensure the integrity of our systems and information, we may not be able to anticipate, detect or implement effective preventive measures against all cyber threats, especially because the techniques used are increasingly sophisticated, change frequently and are often not recognized until launched. Cyber attacks can originate from a variety of sources, including third parties who are affiliated with foreign governments or are involved with organized crime or terrorist organizations. Third parties may also attempt to place individuals within the firm or induce employees, clients or other users
of our systems to disclose sensitive information or provide access to our data or that of our clients, and these types of risks may be difficult to detect or prevent.

Although we take protective measures and endeavor to modify them as circumstances warrant, our computer systems, software and networks may be vulnerable to unauthorized access, misuse, computer viruses or other malicious code and other events that could have a security impact. Due to the complexity and interconnectedness of our systems, the process of enhancing our protective measures can itself create a risk of systems disruptions and security issues.

If one or more of such events occur, this potentially could jeopardize our or our clients’ or counterparties’ confidential and other information processed and stored in, and transmitted through, our computer systems and networks, or otherwise cause interruptions or malfunctions in our, our clients’, our counterparties’ or third parties’ operations, which could impact their ability to transact with us or otherwise result in significant losses or reputational damage.

Healthcare Products and Services Sector

If we or our business associates that handle certain information on our behalf fail to comply with requirements relating to patient privacy and information security, among other things, our reputation and business operations could be materially adversely affected.

The collection, maintenance, use, disclosure and disposal of individually identifiable information or data, including PHI and payment cardholder data, by our businesses are regulated at the federal and state levels, and in some cases are subject to contractual requirements. Despite the privacy and security measures we have in place to ensure compliance with applicable laws, regulations and contractual requirements, our facilities and systems, and those of our third party vendors and service providers, are vulnerable to privacy and security incidents including, but not limited to, computer hacking, breaches, acts of vandalism or theft, computer viruses or other forms of cyber-attack, misplaced or lost data, programming and/or human errors or other similar events. …

A party, whether internal or external, that is able to circumvent our security systems could, among other things, misappropriate or misuse sensitive or confidential information (including but not limited to PHI, payment cardholder data and other member information), user information or other proprietary information, cause significant interruptions in our operations and cause all
or portions of our internal operating systems or website to be unavailable. Internal or external parties may attempt to circumvent our security systems, and we have in the past, and expect that we will in the future, experience external attacks on our network, including, without limitation, reconnaissance probes, denial of service attempts, malicious software attacks, including without limitation attacks intended to render our internal operating systems unavailable, and phishing attacks. We have expended significant resources to protect against such attacks, detect if and when attacks occur, respond to these attempted attacks and recover the enterprise to regular operations, and we expect to continue to do so in the future. Any reductions in the availability of our website or our internal operating systems could impair our ability to conduct our business and adversely impact our members and employees during the occurrence of any such incident.

Because the techniques used to circumvent security systems can be highly sophisticated and change frequently, often are not recognized until launched against a target and may originate from less regulated and remote areas around the world, we may be unable to proactively address all possible techniques or implement adequate preventive measures for all situations. Recent, well-publicized attacks on prominent companies, including in our industry, have resulted in the theft of significant amounts of sensitive and personal information and demonstrate the sophistication of the perpetrators. These attacks have generated national security risks that are being engaged by the federal government, which further illustrates the magnitude of the threat posed to companies across the nation.

Noncompliance with any privacy laws or data security laws or any security incident or breach involving the misappropriation, loss or other unauthorized use or disclosure of sensitive or confidential member information, whether by us, one of our business associates or another third party, could have a material adverse effect on our business, reputation, financial condition and results of operations, including but not limited to: material fines and penalties; compensatory, special, punitive, and statutory damages; litigation; consent orders regarding our privacy and security practices; requirements that we provide notices, credit monitoring services and/or credit restoration services or other relevant services to impacted individuals; adverse actions against our licenses to do business; and injunctive relief. Additionally, the costs incurred to remediate any data security or privacy incident could be substantial.