EXECUTIVE SUMMARY

The U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose in their Form 10-K submissions potential risk factors to investors. Beginning in 2017, the IAPP studied these disclosures to assess not just whether companies have been disclosing personal data processing practices and privacy regulations as a risk, but also increasingly what business harms the organizations faced for getting privacy wrong.

In this year’s study, the IAPP’s Westin Research team focused on six key industry sectors and reviewed the privacy risk disclosures published by representative companies in each sector. The industry sectors we chose to focus on are business-to-consumer technology, business-to-business technology, banking and finance, traditionally brick-and-mortar retail, pharmaceuticals and health services, and health insurance.

Although each industry sector perceives privacy and security risks through a particular lens, there were clear trends across all sectors:

- The sudden and unexpected shift to working from home due to the COVID-19 pandemic created new and additional information security risks for firms.
- Although cybersecurity concerns have always been the top privacy-related disclosed risk, a significant number of 10-K disclosures emphasized the sophistication and unpredictability of cyberthreats today, including the high potential for a ransomware incident.
- Companies are now fully aware of how interconnected their information systems are with those of their business partners and tech vendors, leading to enhanced security and privacy risks.
- New and proposed privacy regulations in the U.S. and around the world create uncertainty, which creates compliance cost and risk.
- And finally, even existing privacy regulations, like the EU General Data Protection Regulation, are sufficiently dynamic and complex that compliance remains a moving target — especially, in 2021, for personal data transfers from the European Union.
This report is organized as follows: We summarize the privacy risk disclosure essence for each selected industry sector, based on our reading of the representative companies' most recent Form 10-K risk disclosures. We signal their collective concern for each of the following categories of risk: breach/cyberattack; sectoral privacy legal compliance; comprehensive privacy law compliance; payment card industry standards compliance; and risks to core revenue from consumer behavior tied to privacy, such as breach of trust or harm to brand. More information about these measures can be found in the key on this page.

Finally, for each industry sector, we illustrate the key points with selected quotes from certain risk disclosures and longer clips from those that were either standouts in their phrasing or illustrative of the industry’s view on privacy, generally.

Companies are now fully aware of how interconnected their information systems are with those of their business partners and tech vendors, leading to enhanced security and privacy risks.

---

**Privacy Risk Categories**

Privacy risk disclosures in 6 major industry sectors

We identify six privacy risk categories common across industries: Breach/cyberattack resulting in disclosure of personal data; compliance with sectoral privacy laws (e.g., the U.S. Health Insurance Portability and Accountability Act); compliance with comprehensive privacy laws (e.g., the GDPR and California Consumer Privacy Act); compliance with the PCI standards; risk of private litigation or regulatory enforcement action resulting in damages, fines or other sanctions; and risk to core revenue based on consumer privacy preferences (e.g., harm to reputation or brand, inability to use consumer data for analytics).
Risk disclosures published in 2021 were written with the COVID-19 pandemic very much on everyone’s mind. For many B2C tech companies, business thrived. But remote work created its own risks, with employees potentially in insecure environments, using new technology and unable to react as rapidly to security incidents.

As more jurisdictions begin to adopt and implement comprehensive privacy laws, B2C tech companies are finding themselves navigating uncertain compliance waters. Their risk disclosures frequently mention the number of new U.S. state comprehensive privacy laws that have passed or been proposed and note their stringent enforcement.

Many firms mention the direct correlation between privacy laws and changes to their fundamental business models’ reliance on collection and use of personal data, including selling of data for targeted advertisements, which generates a large part of their revenues. Other limitations include those related to data storage, deletion and localization, all of which are considered to directly impact success of the business.

They also note the uncertainty of a changing regulatory environment creates inherent risk, as compliance is always elusive. For example, companies like Facebook and Alphabet (Google) emphasize in their 10-K disclosures the high costs of compliance with comprehensive privacy laws, including trying to address different requirement across a variety of jurisdictions. Coupled with increasing enforcement frequency, the variation in regulatory requirements causes uncertainty. Companies need to allocate significant resources to compliance because they are unsure how to comply with the patchwork of laws to avoid regulatory action and private litigation.

“[T]he changes in our work environment as a result of the COVID-19 pandemic could impact the security of our systems, as well as our ability to protect against attacks and detect and respond to them quickly. The rapid adoption of some third-party services designed to enable the transition to a remote workforce also may introduce security risk that is not fully mitigated prior to the use of these services.”

— Facebook
**SURVEY SPOTLIGHT**

**UBER**

The GDPR further provides that EU member states may institute additional laws and regulations impacting the processing of personal data, including (i) special categories of personal data (e.g., racial or ethnic origin, political opinions, and religious or philosophical beliefs) and (ii) profiling of individuals and automated individual decision-making. Such additional laws and regulations could limit our ability to use and share personal or other data, thereby increasing our costs and harming our business and financial condition.

Other jurisdictions outside the EU are similarly introducing or enhancing privacy and data security laws, rules, and regulations, which will increase our compliance costs and the risks associated with noncompliance. For example, the California Consumer Privacy Act ("CCPA"), which provides new privacy rights for consumers and new operational requirements for businesses, went into effect in January 2020. … Brazil provides another example, having passed the General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or LGPD) in 2018, which is now in effect.

Additionally, we are subject to laws, rules, and regulations regarding cross-border transfers of personal data, including laws relating to transfer of personal data outside the EEA. … If we cannot rely on existing mechanisms for transferring personal data from the EEA, the United Kingdom, or other jurisdictions, we may be unable to transfer personal data of Drivers, consumers, or employees in those regions, which could have an adverse effect on our business, financial condition, and operating results.

**B2C tech firms also realize that cybersecurity risks and data breaches are not only growing in frequency, but the methods of attack are also more sophisticated than ever.** Their disclosures note the potential for reputational harm as a core concern, equally damaging to their financial position as the risk of managing a breach response, private litigation or regulatory enforcement. To that end, the companies disclosed they could suffer reputational harm not merely from an actual incident, but as well from merely a public perception of inadequate data security.
B2B tech companies have long known that data security is a core product differentiator. As privacy by design has gone from niche idea to regulatory requirement, supporting their business customers’ privacy compliance obligations is also a major feature of the top B2B tech firms’ platforms. These firms were the most likely among all the reviewed industries to mention compliance risk for the widest number of domestic and international privacy and data protection laws.

For newcomers like Zoom, which rocketed into everyone’s homes in 2020, crafting a risk disclosure that comprehensively and accurately describes all the possible data risks is undoubtedly a significant challenge. Working from home forced many companies to rapidly digitize their workflows, driving up demand for B2B tech services. But with greater dependence on B2B services came more bad actors and greater consequences to service downtime, especially when both the platform providers and customers alike lack fully redundant systems.

Significant attention is paid to the uncertainty created by the 2020 “Schrems II” decision that invalidated the existing Privacy Shield framework between the EU and U.S. In addition, Brexit also introduced privacy law compliance uncertainty, and companies noted in their risk disclosures that lack of regulatory clarity leads to high compliance costs.

Like all other industries, B2B tech firms rely heavily on data to drive business strategy. The firms disclosed government regulation could force them to change their data-handling practices and frustrate their prior investments in data analysis, especially artificial intelligence. They also note that several jurisdictions, including China, are enacting data localization practices that may further complicate operations.

“The Company’s investment in gaining insights from data is becoming central to the value of the services we deliver to customers, our operational efficiency and key opportunities in monetization, customer perceptions of quality, and operational efficiency. Our ability to use data in this way may be constrained by regulatory developments that impede realizing the expected return from this investment.”

— Microsoft
SURVEY SPOTLIGHT

ZOOM

Interruptions, delays or outages in service from our co-located data centers and a variety of other factors, including increased usage stemming from the COVID-19 pandemic, would impair the delivery of our services, require us to issue credits or pay penalties, and harm our business. …

The actual or perceived failure by us, our customers, partners or vendors to comply with stringent and evolving privacy, data protection and information security laws, regulations, standards, policies and contractual obligations could harm our reputation and business or subject us to significant fines and liability. …

*Increased usage of our services, novel uses of our services, and additional awareness of Zoom and our brand stemming from the COVID-19 pandemic could make it more difficult for us to comply with our contractual obligations,* our policies, our publications, our certifications, our documentation, standards, regulations, and applicable laws related to privacy, data protection, and information security, and has and could result in greater public scrutiny of, press related to, or a negative perception of our privacy, data protection, and information security practices. …

We expect EU regulators to aggressively enforce EU laws prohibiting data transfers to the U.S. and other countries without a legally sound transfer mechanism, and it (is possible) that EU regulators could prevent Zoom from transferring any personal data out of the EU to certain countries like the U.S.

The actual or perceived failure by us, our customers, partners or vendors to comply with stringent and evolving privacy, data protection and information security laws, regulations, standards, policies and contractual obligations could harm our reputation and business or subject us to significant fines and liability.
During the COVID-19 pandemic, the Company has experienced increased information security risks, primarily as a result of the increase in work-from-home arrangements. These risks may increase in the future as the Company continues to increase its mobile- and internet-based product offerings and expands its internal usage of web-based products and applications.

— US Bancorp
Although the top publicly traded companies in the financial services sector are still the big banks, their industry is far from static. Innovation in cryptocurrency, peer-to-peer payments, buy-now-pay-later mechanisms, AI, robotics, mobile applications and data aggregation are among the many forces driving rapid change and creating heightened privacy and security risks for customers and investors.

Banks have been heavily regulated at the state and federal level for many years and for many business functions, including privacy, while the up-start financial technologies have so far mostly avoided costly compliance obligations. And yet as banks find themselves increasingly integrated with and reliant on a variety of third parties for conducting their core businesses, and as comprehensive privacy laws emerge, data privacy and security risks increase for all players, and compliance obligations affect the entire supply chain.

In addition to vulnerability from cyberattack — to themselves or one of their partners — financial institutions report risks from failure to comply with the GDPR and CCPA, as amended by the California Privacy Rights Act. As with the B2C and B2C tech firms, confusion over personal data transfers from the EU is also listed among the regulatory compliance risks facing banks.

“We … face indirect technology, cybersecurity and operational risks relating to the … third parties (including their downstream service providers) … upon whom we rely to facilitate or enable our business activities or upon whom our customers rely. Such third parties … include financial counterparties, financial data aggregators, financial intermediaries, … vendors, regulators, providers of critical infrastructure, … and retailers for whom we process transactions.”

— Bank of America
US BANCORP

In the United States, several states have recently enacted consumer privacy laws that impose compliance obligations with respect to personal information. In particular, the California Consumer Privacy Act (the “CCPA”) imposes significant requirements on covered companies with respect to consumer data privacy rights. In November 2020, voters in the State of California approved the California Privacy Rights Act (“CPRA”) … Compliance with the CCPA, the CPRA after it becomes effective, and other state statutes, common law, or regulations designed to protect consumer, employee or applicant personal data could potentially require substantive technology infrastructure and process changes across many of the Company’s businesses. Noncompliance with the CCPA, CPRA, or similar laws and regulations could lead to substantial regulatory fines and penalties, damages from private causes of action, and/or reputational harm.…

The July 2020 decision by the Court of Justice of the European Union relating to transfers of personal data outside of the European Union ("Schrems II") may impact the Company’s operations and ability to transfer personal data out of the European Union or may require additional compliance programs. … Schrems II and subsequent guidance from the European Commission and European Union Data Protection Board could result in substantial costs of compliance and failure to adhere to the guidance may subject the Company to fines or regulatory oversight.

The July 2020 decision by the Court of Justice of the European Union relating to transfers of personal data outside of the European Union ("Schrems II") may impact the Company’s operations and ability to transfer personal data out of the European Union or may require additional compliance programs.
Our digital platforms, which are increasingly important to our business and continue to grow in complexity and scope, and the systems on which they run, including those applications and systems in our acquired eCommerce businesses, are regularly subject to cyberattacks.

— Walmart
The pandemic drove people to online shopping and home improvement projects, favoring the retailers built to respond. It also created risks to business operations due to the increased use of remote work infrastructure. At least one retailer we surveyed disclosed that some of its own systems and those of its third-party service providers experienced security breaches during the pandemic, although they “did not have a material adverse (effect) on operating results.”

“In certain circumstances, our contracts with payment card processors and payment card networks … require us to adhere to payment card network rules which could make us liable … if information in connection with payment cards and payment card transactions … is compromised.”

— Walmart

The retail sector’s risk disclosures have traditionally been slightly less focused than other industries regarding comprehensive privacy legislation — especially outside the U.S. — but the sector remains very concerned about meeting PCI security standards and the risks of cyberattack to systems and data. The retail sector also makes heavy use of “loyalty” cards and associated personal data, which are vulnerable to low adoption rates or abandonment if customers lose confidence in the firms’ information security.

In a competitive field, interruptions in business operations can drive fickle customers to other retailers. The industry players noted that relying on digital platforms to reach customers and conduct transactions is paramount to survival but also poses heightened risk to data breach and system failure. Like the other industries, the retail companies we studied noted that cybersecurity concerns are growing in their complexity as bad actors use increasingly more sophisticated tactics and technique.

Although the retailers mentioned privacy law compliance, it was not covered as extensively in this sector. To the extent mentioned, the companies pointed out privacy laws are constantly evolving and compliance involves significant expense.
HOME DEPOT

Our business depends on our customers’ willingness to entrust us with their personal information. Events that adversely affect that trust, including inadequate disclosure to our customers of our uses of their information or failing to keep our information technology systems and our customers’ sensitive information secure from significant attack, theft, damage, loss or unauthorized disclosure or access, whether as a result of our action or inaction (including human error or malfeasance) or that of our service providers or other third parties, could adversely affect our brand and reputation.

Further, the regulatory environment related to data privacy and cybersecurity is constantly changing, with new and increasingly rigorous requirements applicable to our business. The implementation of these requirements has also become more complex. Maintaining our compliance with those requirements, including recently enacted state consumer privacy laws, may require significant effort and cost, require changes to our business practices, and limit our ability to obtain data used to provide a personalized customer experience. In addition, failure to comply with applicable requirements could subject us to fines, sanctions, governmental investigations, lawsuits or reputational damage.

The regulatory environment related to data privacy and cybersecurity is constantly changing .... The implementation of these requirements has also become more complex. Maintaining our compliance with those requirements ... may require significant effort and cost, require changes to our business practices, and limit our ability to obtain data used to provide a personalized customer experience.
We have outsourced significant elements of our operations, including significant elements of our information technology infrastructure and, as a result, we manage relationships with many third-party vendors who may or could have access to our confidential information. The size and complexity of our information technology and information security systems, and those of our third-party vendors (and the large amounts of confidential information that is present on them), make such systems potentially vulnerable to service interruptions or to security breaches from inadvertent or intentional actions by our employees or vendors, or malicious attackers.

— Johnson & Johnson
Pharmaceutical companies host extremely sensitive personal information associated with human clinical trials and must constantly be vigilant against intellectual property theft. Accordingly and predictably, they are highly attuned to the risks of cyberattack to the extent intrusion exposes proprietary data.

Information systems were made vulnerable as the pandemic drove more employees to work from home. To combat these risks, the companies have purchased cyber liability insurance and invested in their digital infrastructure. However, even with these measures, companies such as McKesson and Pfizer note cyberattacks are increasing in sophistication.

The companies surveyed cite their increased dependence on cloud platforms and new technologies as a cause for the increased information security risks. In addition, information systems were made vulnerable as the pandemic drove more employees to work from home. To combat these risks, the companies have purchased cyber liability insurance and invested in their digital infrastructure. However, even with these measures, companies such as McKesson and Pfizer note cyberattacks are increasing in sophistication and whether the companies can effectively prevent incidents or mitigate the damage is uncertain. There are costs associated with system repair and risks of litigation. In addition, reputational damage is still a major concern after any potential system downtime stemming from a security incident.

The level of sophistication in each company’s disclosure of risk related to data protection laws varied through the companies we surveyed. Most of the companies mentioned the GDPR and CCPA when referring to risks related to government regulation of privacy. They also noted risks related to the growing number of jurisdictions adopting comprehensive privacy laws and the associated uncertainty created by a potentially vigorous enforcement environment.

Although only Merck referred to the “Schrems II” decision, the pharmaceutical companies are concerned with risks related to third-party data transfers, now ubiquitous in an industry reliant on digital infrastructure. Some are also aware of the growing complexity and demands of data sharing regulations in the EU and their potential impact on proprietary research data.
**MERCK**

The Company is subject to a significant number of privacy and data protection laws and regulations globally, many of which place restrictions on the Company’s ability to transfer, access and use personal data across its business. The legislative and regulatory landscape for privacy and data protection continues to evolve. There has been increased attention to privacy and data protection issues in both developed and emerging markets with the potential to (directly affect) the Company’s business. ...

Failure to comply with the requirements of the GDPR and the related national data protection laws of the EU Member States may result in significant monetary fines and other administrative penalties as well as civil liability claims from individuals whose personal data was processed. Data protection authorities from the different EU Member States may still implement certain variations, enforce the GDPR and national data protection laws differently, and introduce additional national regulations and guidelines, which adds to the complexity of processing personal data in the EU. ...

*There is, moreover, a growing trend towards required public disclosure of clinical trial data in the EU which adds to the complexity of obligations relating to processing health data from clinical trials.* Failing to comply with these obligations could lead to government enforcement actions and significant penalties against the Company, harm to its reputation, and adversely impact its business and operating results.
The health insurance sector has faced HIPAA regulation for many years. This year’s risk disclosures provide considerable detail regarding the very real risks of cyberattack, as well as potential for federal, state or international enforcement of privacy laws.

Like the other sectors, insurance is heavily data driven. Some of this personal data is collected from customers, but other data is generated through analytics. What is more, aggregated data is shared frequently with others, including pharmaceutical manufacturers, as well as data aggregators and analysts. At each step, the data is vulnerable to accidental or malicious acts that could result in unauthorized access or disclosure. These risks magnify as the industry grows in its interdependence on third parties and its digitization of systems.

Several of the risk disclosures mentioned prior cyber incidents resulting in significant internal if not governmental investigations, some of which are ongoing.

This year’s risk disclosures provide considerable detail regarding the very real risks of cyberattack, as well as potential for federal, state or international enforcement of privacy laws.

**UNIVERSITY HEALTH GROUP**

The collection, maintenance, protection, use, transmission, disclosure and disposal of protected personal information is regulated at the federal, state, international and industry levels and requirements are imposed on us by contracts with customers. These laws, rules and requirements are subject to change. Compliance with new privacy and security laws, regulations and requirements may result in increased operating costs, and may constrain or require us to alter our business model or operations.

Internationally, many of the jurisdictions in which we operate have established their own data security and privacy legal framework with which we or our customers must comply. We expect there will continue to be new proposed laws, regulations and industry standards concerning privacy, data protection and information security in the European Union, Brazil, Chile, India and other jurisdictions, and we cannot yet determine the impacts such future laws, regulations and standards may have on our businesses or the businesses of our customers.
The HITECH Act …granted enforcement authority to states' Attorneys General in addition to the HHS Office for Civil Rights. It is possible that Congress may enact additional legislation in the future to increase the amount or application of penalties and to create a private right of action under HIPAA, which could entitle patients to seek monetary damages for violations of the privacy rules.

— Centene Corporation
Privacy and breach risk disclosures

The “IAPP-EY Annual Privacy Governance Report 2021” revealed half of publicly traded companies surveyed disclose privacy-related risks in financial notices, disclosures, shareholder communications or annual reports. In these disclosures, 63% of respondents noted both privacy law compliance and data breach risks are disclosed, and 13% disclosed only privacy risks.

From the “IAPP-EY Annual Privacy Governance Report 2021”

Privacy risks communicated
(Base: Publicly traded)
- Yes, 48%
- No, 19%
- Unsure, 33%

What is communicated
(Base: Privacy items disclosed)
- Both compliance and breach-related, 65%
- Only data breach-related, 14%
- Only privacy compliance-related, 13%
- Unsure, 0%
- Neither, 8%
Risk disclosure predictions for 2022

“Many companies will categorize privacy and data protection as an environmental, social, and governance (ESG) matter, underscoring ‘the role that data privacy plays in boosting corporate reputation.’”

— Bloomberg 2021 study of 8-K and 10-K risk disclosures

“There will be increased focus on Europe and international privacy law compliance, even if companies have not started doing business in those regions yet. Many companies will be adding at least one risk factor to address China’s Personal Information Protection Law (PIPL).”

— Boris Segalis and Jacqueline Klosek, Goodwin