Privacy Risk Study 2018:
Privacy law compliance and litigation deemed significant risk factors
Executive summary

The U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose potential risk factors, including exposure to cybersecurity threats and violations of consumer privacy laws. The IAPP's third annual study of these disclosures (part of Form 10-K) of 150 publicly traded companies shows that – like last year – effectively 100 percent identified concerns about cyberattacks in their 2017 10-K reports. New this year is a significantly higher concern about risks of legal action from privacy law violations, which jumped nearly 20 percent over last year.

Although concerns about malicious outsiders causing data breaches and taking other actions against corporate cybersecurity remained the primary threat reported by companies, more companies also acknowledged data risks posed by other actors. Companies were much more likely to acknowledge the risk of potential employee error, equipment failure, and information loss/misuse by third party vendors than in prior years.

Loss of personal information was again the highest reported data risk, with 85 percent acknowledging it, while risks of losing intellectual property fell slightly to 31 percent. Additionally, concern about losing payment card data has more than doubled over last year (up 15 percent, to 31 percent).

The most important take-away from this year’s results, however, is the dramatic rise in companies reporting risks of privacy-related legal action, both regulatory action (up to 80 percent, from 63 percent) and civil litigation (up to 78 percent, from 52 percent last year). Consistent with this, reported concerns about legal compliance have also risen significantly, with three out of four companies now listing compliance with current U.S. privacy laws as a business risk, and nearly half citing compliance risks with non-U.S. privacy laws. More than one-quarter of surveyed companies (28 percent) specifically named the European Union’s General Data Protection Regulation as a compliance issue.

Interestingly, however, concern about new privacy regulations fell from 51 percent in 2017 to 36 percent in this year’s reports. This may prove short-sighted for global companies, however, because even though GDPR is now in effect, several new privacy laws have already come online since May 2018, including in California and Brazil, while India and others are poised to adopt privacy legislation as well.

The largest reported post-breach business cost and harm remains damage to reputation (90 percent). Although concern about financial losses (84 percent), business disruption (83 percent), and remediation expenses (65 percent) have all remained roughly the same as last year, concern about data breaches causing a loss in sales has risen 13 points to 62 percent. The number of corporations expressing concern that the handling of a data breach will distract senior management has almost quadrupled – up to 34 percent, from 9 percent last year. Additionally, concern about passing costs on to the consumer and losses exceeding insurance have also risen.

Lastly, consistent with the rise in compliance and loss of credit card data seen elsewhere, concerns about legal penalties and damages (now 85 percent) and specific credit card-related liability (now 10 percent) have also risen over last year.

Sample, representative language by selected companies, pulled from their actual 2017 10-K reports, can be found in this report's Annex.
Privacy law compliance and litigation deemed significant risk factors

Understanding risk is vital to the operation of a mature privacy program. Many privacy laws around the world, including the EU’s General Data Protection Regulation, are essentially exercises in risk assessment. What is the appropriate protection and policy, privacy pros are constantly asked, for a given data set? The answer to this question demands risk assessment.

More broadly, as privacy leaders look to get budget allocation and to make return on investment arguments for growing their programs, they must make compelling arguments about how much response is appropriate for how much risk to the business.

There is, however, relatively little for privacy professionals to benchmark against. What do other organizations deem risky? As we start to get guidance in this area from the likes of the EU’s European Data Protection Board and the National Institute of Standards and Technology, the IAPP has also endeavored to use our Westin Research Center to provide information organizations can use to assess their own programs.

From the “Assessing Mobile App Data Privacy Risk” research, which crowdsourced privacy risk surrounding many common data types, to our annual IAPP-EY Governance Report, where we report out difficulty scores for common compliance tasks, we are looking to build useful data sets by which you can check your own work.

Now in its third year, the IAPP’s “Privacy Risk Study” has become a key tool in the privacy risk-assessment toolbox. Because the U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose potential risk factors, so that investors are well informed, we are able to see how some of the world’s most successful companies, likely endowed with substantial risk-assessment operations, view the digital-risk landscape.

Their reports include exposure to cybersecurity threats and violations of consumer privacy laws, among other “digital risk.” For the past three years, the IAPP Westin Research Center has studied these disclosures (part of Form 10-K) released by the 150 largest publicly traded companies and trends are clearly starting to crystalize. Without question, companies are beginning to take privacy regulation more seriously, and they are much more aware of the risk posed by consumer-generated privacy litigation. At the same time, traditional digital threats, like the fear of losing intellectual property, seem less potentially onerous to America’s biggest companies.

Further, companies increasingly note the risks posed by employees and vendors, who have access to personal data and therefore present greater risk as privacy regulations are put into place with heightened penalties.

One thing has not changed, however: Above all else, these companies make clear that the ultimate harm they fear is damage to their brands.
Methodology

Under the 1934 Securities Exchange Act, companies must file yearly reports with the Securities Exchange Commission (SEC) containing various information, including financials. Since financial years often coincide with the calendar year, most 10-Ks are filed on December 31, although some are filed at other times throughout the year. The agenda items are governed by statute and SEC regulation, which requires them to use a common numbering system. The IAPP reviews Item 1A, in which the company summarizes its views of the major risk factors facing it (and thus its investors) in the coming year.

This year, the Westin Research Center reviewed the Item 1A section of 150 form 10-K filings of corporations ranked the largest in Fortune by revenue. Companies represented in our study reflect a wide variety of industry sectors, the largest of which are banking, finance and insurance (collectively 17 percent); retail (15 percent); and technology (12 percent). We coded the privacy and cybersecurity risks in each 10-K report into categories of each of the following sections: vulnerabilities to the data; types of information at risk; concerns about privacy-related legal actions and privacy-related compliance challenges; and mention of harms (privacy-related business costs). We also identified passages to include in the annex as representative sample language.

One limitation to our methodology is that more than one researcher was involved in coding the answers, which may involve variations in data input.
Fear of information loss by third parties (vendors) has risen 17 percent over last year.

Cybersecurity remains king, but privacy concerns are rising

Like last year, hacks and cyberattacks were the most commonly identified privacy and data protection risk. Every company but two identified malicious actions by outsiders as a concern, and the two hold-outs (a railway and a bank holding company) didn’t mention any cyber vulnerabilities.

Concern over other vulnerabilities has grown significantly over the past year. In particular, companies were almost 13 percent more likely than last year to acknowledge that employee error or malfeasance presents a risk to data and systems, and information technology system failure was cited as a vulnerability 11 percent more often this year.

However, the most significant change was greater acknowledgement of the potential for information loss or misuse by third parties (typically, vendors), which has increased 17 percent over our 2017 study. Privacy and cybersecurity laws and regulations — including in the health and financial services sectors, but also now under GDPR — require vetting and contractual risk-sharing with third parties that have access to personal data, and this seems to have at last caught the attention of most public companies.

---

### Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacks/Cyber attacks</td>
<td>0.00%</td>
<td>98.67%</td>
</tr>
<tr>
<td>Employee error/malfeasance</td>
<td>1.00%</td>
<td>5.67%</td>
</tr>
<tr>
<td>Information loss or misuse by business partners, vendors, or other third parties</td>
<td>25.00%</td>
<td>52.67%</td>
</tr>
<tr>
<td>IT system failure (specifically no bad actor)</td>
<td>42.00%</td>
<td>80.67%</td>
</tr>
<tr>
<td>No mention of vulnerabilities</td>
<td>0.67%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Other</td>
<td>4.00%</td>
<td>12.00%</td>
</tr>
</tbody>
</table>

* Darker shades represent 2017 data, lighter shades represent 2016.
The growth in mobile banking and new payment players may be fueling worry over payment card vulnerability.

PII remains highest information concern, but PCI data is gaining

Losing the personal information of customers and employees remains the top-reported information loss risk, looming over other types of important business data including proprietary and confidential information, and even intellectual property. Concern over loss of proprietary and confidential business information has risen marginally over last year, while concern about loss of IP fell slightly.

Meanwhile, concern about the loss of payment card information has more than doubled from last year — up to 31 percent from 15 percent. Companies are rightly identifying credit card information as one of the most attractive types of data they possess, given its ready use in identity theft. This growth in concern likely also extends from the burgeoning popularity of omnichannel retail strategies and the importance of credit card data to an omnichannel system. We should expect to see a stronger push for PCI DSS compliance, and compliance verification, as companies attempt to avoid additional penalties in case of a breach. Additionally, we might see better credit card data destruction and storage habits to mitigate the risk.

Loss of Protected Information

* Darker shades represent 2017 data, lighter shades represent 2016.
Concern about privacy law compliance and legal action has spiked

One of the most important outcomes of this year’s privacy risk study — and perhaps of greatest note to privacy professionals — is a significant increase in disclosed concerns about compliance with privacy regulations and laws.

Nearly three in four companies now express concern about compliance with U.S. privacy laws, and nearly half about non-U.S. privacy laws, as a risk factor for investors to consider. As expected, we saw many more companies — 28 percent in this year’s survey compared to just 11 percent last year — specifically mention concern about GDPR compliance in their Form 10-K. Meanwhile, the number of companies reporting no concerns about privacy compliance has fallen from 41 percent to just 19 percent.

One interesting outlier to the disclosed privacy law compliance risks is that far fewer companies expressed concern about “new” privacy laws and regulations than prior years — falling from 51 percent in 2017 to 36 percent this year. This may reflect the fact that GDPR was much closer to implementation this December than last — no longer “new” — but it suggests a blindness to the rapid growth in privacy and data protection laws globally, including the surprise California Consumer Privacy Act passed just a few months ago.

Concern about adverse legal action arising out of data privacy and security issues has increased across the board. Regulatory enforcement action remains the largest single concern, reported this year by four in five companies. Concern about civil actions and litigation has seen a surge as a risk factor, up from 52 percent to 78 percent.

Consistent with these results, the number of businesses expressing no concern about legal consequences has dropped to just 9 percent.

Risk of Legal Actions

![Bar chart showing the risk of legal actions across surveyed 10-Ks.]

* Darker shades represent 2017 data, lighter shades represent 2016.
Brand Reputation Remains Top Post-Breach Risk, but Concern About Penalties is Rising

In their Form 10-K reports, companies not only describe what their vulnerabilities are, they also tell the SEC and potential investors what business harms might result from those outcomes. If the worst should happen — a data breach or other privacy violation — harm to brand and reputation remains far and away the most-recognized business risk (named by 90 percent of companies, similar to last year’s 95 percent). The levels of concern about general financial losses, disruption of business, and remediation expenses are all roughly the same as last year, too.

Privacy Law Compliance Challenges I

* Darker shades represent 2017 data, lighter shades represent 2016.
Consistent with increased concern over privacy legal actions, companies are also much more likely to report risk of legal damages and regulatory penalties.

One area of increased concern is the risk of legal damages and regulatory penalties. Nearly 85 percent of companies in this year’s survey reported it as a risk factor, compared to 69 percent last year. This follows from the overall sensitivity to regulatory enforcement action and civil litigation for privacy harms. Companies also reported a corresponding uptick in risks of liability exceeding insurance coverage (32 percent this year over 22 percent in 2017’s report). Because the Form 10-K filings we reviewed were all prepared in advance of the California Consumer Privacy Act’s passage this summer, we may see even more concern about risks of legal damages next year due to CCPA’s private right of action for data breach.

Concern about loss of sales and reduced purchases due to a cyberattack also rose 24 percent. This reflects both the increasingly crucial role of online retail in the average corporation’s portfolio and increased worry about distributed denial of service (DDoS) attacks. Many corporations directly named DDoS attacks as a business risk. We may see a renewed push to invest in web monitoring software and other DDoS identification and remediation technology.
Finally, we observed that nearly three times as many companies acknowledged that personal information breaches and mishandling may involve significant management time and resources, distracting from core business goals. This signals a long-awaited general awareness on the part of senior management about the devastating impacts of a data breach on a business and the large amount of work required to alleviate it.

Business Costs and Harms I

- General financial losses/reduced profit
- Ability to conduct business operations/system downtime
- Reduced purchases/Loss of sales
- Harm to reputation/brand/customer trust
- Remediation expenses (system upgrades, customer notification, mitigation)
- Legal damages and regulatory penalties

* Darker shades represent 2017 data, lighter shades represent 2016.

Business Costs and Harms II

- Liability may exceed insurance coverage
- Expenditure of management time and resources, distraction
- Liability to payment card issuers and merchant banks
- Increased costs passed to customer
- None. No mention of privacy-related costs
- Other

* Darker shades represent 2017 data, lighter shades represent 2016.
Conclusion

This year’s study demonstrates a growing acknowledgement among publicly traded U.S. companies of the importance of sound privacy and data security practices to reduce business risks. Not only did they affirm that mishandled personal data can lead to reputational harm, we also found increased concerns about privacy legal compliance and regulatory action this year. The EU’s GDPR — coming online in May 2018 — likely played a factor in that result.

We also found increased worry about credit card data and a more encompassing view of the impact data breaches have on the bottom line. Based on these findings, we expect to see greater emphasis on compliance, data privacy insurance, and indemnification clauses and other liability-shifting measures in vendor contracts, and closer due diligence of employees and third-party providers. We also predict continued, significant growth in demand for privacy and security professionals to help mitigate business risks.
Following are excerpts from 2017 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. The completed forms can be found at www.sec.gov/edgar.

Technology

“Despite our cybersecurity measures (including employee and third-party training, monitoring of networks and systems, patching, maintenance, and backup of systems and data), the Company’s information technology networks and infrastructure may still be vulnerable to damage, disruptions or shutdowns due to attacks by hackers, breaches, employee error or malfeasance, power outages, computer viruses, telecommunication or utility failures, systems failures, service or cloud provider breaches, natural disasters or other catastrophic events.”

~

“We also could be required to spend significant financial and other resources to remedy the damage caused by a security breach, including to repair or replace networks and information technology systems, liability for stolen information, increased cybersecurity protection costs, litigation expense and increased insurance premiums.”

~

“The Company’s business requires it to use and store confidential information, including, among other things, personally identifiable information (‘PII’) with respect to the Company’s customers and employees. The Company devotes significant resources to network and data security, including through the use of encryption and other security measures intended to protect its systems and data. But these measures cannot provide absolute security, and losses or unauthorized access to or releases of confidential information may still occur, which could materially adversely affect the Company’s reputation, financial condition and operating results.”
“Data protection authorities may assert that our collection, use, and management of customer data is inconsistent with their laws and regulations. Legislative or regulatory action relating cybersecurity requirements may increase the costs to develop, implement, or secure our products and services. Legislative or regulatory action could also emerge in the area of AI, increasing costs or restricting opportunity. Applying these laws and regulations to our business is often unclear, subject to change over time, and sometimes may conflict from jurisdiction to jurisdiction. Additionally, these laws and governments’ approach to their enforcement, and our products and services, are continuing to evolve. Compliance with these types of regulation may involve significant costs or require changes in products or business practices that result in reduced revenue. Noncompliance could result in the imposition of penalties or orders we stop the alleged noncompliant activity.”

~

“Adversaries tend to focus their efforts on the most popular operating systems, programs, and services, including many of ours, and we expect that to continue. Adversaries that acquire user account information at other companies can use that information to compromise our users’ accounts where accounts share the same attributes like passwords. Inadequate account security practices may also result in unauthorized access. We are also increasingly incorporating open source software into our products. There may be vulnerabilities in open source software that may make our products susceptible to cyberattacks.

To defend against security threats to our internal IT systems, our cloud-based services, and our customers’ systems, we must continuously engineer more secure products and services, enhance security and reliability features, improve the deployment of software updates to address security vulnerabilities in our own products as well as those provided by others, develop mitigation technologies that help to secure customers from attacks even when software updates are not deployed, maintain the digital security infrastructure that protects the integrity of our network, products, and services, and provide customers security tools such as firewalls and anti-virus software and information about the need to deploy security measures and the impact of doing so.”

~

“Government authorities can sometimes require us to produce customer or user data in response to valid legal orders. In the U.S. and elsewhere, we advocate for transparency concerning these requests and appropriate limitations on government authority to compel disclosure. Despite our efforts to protect customer and user data, perceptions that the collection, use, and retention of personal information is not satisfactorily protected could inhibit sales of our products or services, and could limit adoption of our cloud-based solutions by consumers, businesses, and government entities.”
“We are building AI into many of our offerings and we expect this element of our business to grow. We envision a future in which AI operating in our devices, applications, and the cloud helps our customers be more productive in their work and personal lives. As with many disruptive innovations, AI presents risks and challenges that could affect its adoption, and therefore our business. AI algorithms may be flawed. Datasets may be insufficient or contain biased information. Inappropriate or controversial data practices by the Company or others could impair the acceptance of AI solutions. These deficiencies could undermine the decisions, predictions, or analysis AI applications produce, subjecting us to competitive harm, legal liability, and brand or reputational harm. Some AI scenarios present ethical issues. If we enable or offer AI solutions that are controversial because of their impact on human rights, privacy, employment, or other social issues, we may experience brand or reputational harm.”

~

“From time to time, we encounter intrusions or unauthorized access to our network, products, services, or infrastructure. To date, none have resulted in any material adverse impact to our business or operations. Such incidents, whether or not successful, could result in our incurring significant costs related to, for example, rebuilding internal systems, writing down inventory value, implementing additional threat protection measures, providing modifications to our products and services, defending against litigation, responding to regulatory inquiries or actions, paying damages, providing customers with incentives to maintain the business relationship, or taking other remedial steps with respect to third parties. In addition, these threats are constantly evolving, thereby increasing the difficulty of successfully defending against them or implementing adequate preventative measures. While we seek to detect and investigate all unauthorized attempts and attacks against our network, products, and services, and to prevent their recurrence where practicable through changes to our internal processes and tools and/or changes or updates to our products and services, we remain potentially vulnerable to additional known or unknown threats. In some instances, we, our customers, and the users of our products and services may be unaware of an incident or its magnitude and effects.”

~

“Security vulnerabilities may exist with respect to our processors and other products as well as the operating systems and workloads running on them. Mitigation techniques designed to address these security vulnerabilities, including software and firmware updates or other preventative measures, may not operate as intended or effectively resolve these vulnerabilities. In addition, we may be required to rely on third parties, including hardware, software, and services vendors, as well as end users, to develop and deploy mitigation techniques, and the effectiveness of mitigation techniques may depend solely or in part on the actions of these third parties. Security vulnerabilities and/or mitigation techniques,
including software and firmware updates, may result in adverse performance, reboots, system instability, data loss or corruption, unpredictable system behavior, or the misappropriation of data by third parties, which could adversely impact our business and harm our reputation.”

~

“A side-channel exploit is a type of security vulnerability that has recently received attention as a result of the variants referred to as ‘Spectre’ and ‘Meltdown.’ Information on these variants was prematurely reported publicly before mitigation techniques to address all vulnerabilities were made widely available, and certain of the mitigation techniques did not operate as intended. To date, we do not expect a material financial impact to our business or operations from these security vulnerabilities. ... The recent publicity regarding side-channel exploits may also result in increased attempts by third parties to identify additional variants. We will continue to reassess whether or not we expect to be exposed to a loss that could be material.”

~

“Our digital content offerings depend in part on effective digital rights management technology to control access to digital content. If the digital rights management technology that we use is compromised or otherwise malfunctions, we could be subject to claims, and content providers may be unwilling to include their content in our service.”

Pharmaceuticals

“We also have outsourced significant elements of our operations to third parties, including significant elements of our information technology infrastructure and, as a result, we are managing many independent vendor relationships with third parties who may or could have access to our confidential information.”

~

“We operate dispensing pharmacies, call centers, data centers and corporate facilities that depend on the security and stability of our technology infrastructure. Our technology infrastructure could be disrupted by any number of events including a general failure of the technology, security breach, malfunction of business process or a disaster or other catastrophic event. Such disruptions could, temporarily or indefinitely, significantly reduce, or partially or totally eliminate our ability to process and dispense prescriptions and provide products and services to our clients and members. Any such service disruption at these facilities or to this infrastructure or our failure to implement adequate business continuity and disaster recovery strategies could have a material adverse effect on our business and results of operations.”
Banking/Finance

“There have been a number of highly publicized cases involving financial services companies, consumer-based companies, governmental agencies and other organizations reporting the unauthorized disclosure of client, customer or other confidential information in recent years.”

“Third parties with which the Company does business, as well as retailers, data aggregators and other third parties with which [Company’s] customers do business, can also be sources of operational risk to [Company]. This is particularly the case where activities of customers or those third parties are beyond [Company’s] security and control systems, including through the use of the internet, personal smart phones and other mobile devices or services.”

“[Company] has also been the target of significant distributed denial-of-service attacks which are intended to disrupt online banking services.”

“A cyber attack could occur and persist for an extended period of time without detection. We expect that any investigation of a cyber attack would be inherently unpredictable and that it would take time before the completion of any investigation and before there is availability of full and reliable information. During such time we would not necessarily know the extent of the harm or how best to remediate it, and certain errors or actions could be repeated or compounded before they are discovered and remediated. In addition, announcing that a cyber attack has occurred increases the risk of additional cyber attacks, and preparing for this elevated risk can delay the announcement of a cyber attack. All or any of these challenges could further increase the costs and consequences of a cyber attack.”

“Cybersecurity risks for banking organizations have significantly increased in recent years in part because of the proliferation of new technologies, and the use of the Internet and telecommunications technologies to conduct financial transactions. For example, cybersecurity risks may increase in the future as we continue to increase our mobile-payment and other internet-based product offerings and expand our internal usage of web-based products and applications. In addition, cybersecurity risks have significantly increased in recent years in part due to the increased sophistication and activities of organized crime groups, hackers, terrorist organizations, hostile foreign governments, disgruntled employees or vendors, activists and other external parties, including those involved in corporate espionage. Even the most advanced internal control environment may...
be vulnerable to compromise. Targeted social engineering attacks are becoming more sophisticated and are extremely difficult to prevent. The techniques used by bad actors change frequently, may not be recognized until launched and may not be recognized until well after a breach has occurred. Additionally, the existence of cyber attacks or security breaches at third parties with access to our data, such as vendors, may not be disclosed to us in a timely manner.”

“Examples of regulatory changes that have resulted in increased compliance risks and costs include (i) ... [the Fed’s] ‘total loss absorbing capacity’ ... (ii) the Volcker Rule, ... and (iii) a proliferation of laws relating to the limitation of cross-border data movement, including data localization and protection and privacy laws, which can conflict with or increase compliance complexity with respect to anti-money laundering laws.”

Construction

“The amount of insurance coverage we maintain may be inadequate to cover claims or liabilities relating to a cybersecurity attack.”

“We are bound by our client and other contracts, as well as our own business practices, to protect confidential and proprietary information (whether it be ours or a third party’s information entrusted to us) from disclosure.”

Aerospace and Defense

“Due to the evolving nature of these security threats and the national security aspects of much of the data we protect, the impact of any future incident cannot be predicted.”

“Furthermore, there has been heightened legislative and regulatory focus on data security in the U.S. and abroad (particularly in the European Union through the General Data Protection Regulation that will go into effect in May 2018). Substantial changes in applicable regulations may require us to make costly changes to our systems.”
“Cybersecurity incidents aimed at the software imbedded in our products could lead to third party claims that our product failures have caused a similar range of damages to our customers, and this risk is enhanced by the increasingly connected nature of our products.”

Travel/Hospitality

“This regulatory environment is increasingly challenging and may present material obligations and risks to our business, including significantly expanded compliance burdens, costs and enforcement risks.”

“The Company will continue its efforts to meet its privacy and data security obligations; however, it is possible that certain new obligations may be difficult to meet and could increase the Company’s costs.”

Telecommunications

“There are also bills pending in both the U.S. House of Representatives and Senate that could impose new privacy and data security obligations. We cannot predict whether any of these efforts will be successful or preempted, or how new legislation and regulations, if any, would affect our business.”

“System redundancy may be ineffective or inadequate, and the Company’s disaster recovery planning may not be sufficient to cover everything that could happen.”

“Moreover, our increasing presence in the IoT industry with offerings of telematics products and services, including vehicle telematics, could also increase our exposure to potential costs and expenses and reputational harm in the event of cyber attacks impacting these products or services.”
“Despite our best attempts to maintain adherence to information privacy and security best practices as well as compliance with applicable laws, rules and contractual requirements, our facilities and systems, and those of our third party service providers, may be vulnerable to privacy or security breaches, acts of vandalism or theft, malware or other forms of cyber-attack, misplaced or lost data including paper or electronic media, programming and/or human errors or other similar events.”

“Many foreign data privacy regulations (including the General Data Protection Regulation (GDPR), which becomes effective in the European Union on May 25, 2018) are more stringent than those in the United States.”

“The collection, maintenance, protection, use, transmission, disclosure and disposal of protected personal information are 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. For example, the HITECH amendments to HIPAA imposed further restrictions on our ability to collect, disclose and use protected personal information and imposed additional compliance requirements on our business.

“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 that there will continue to be new proposed laws, regulations and industry standards concerning privacy, data protection and information security in the European Union 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. For example, in May 2018, the European Union’s General Data Protection Regulation will overhaul data protection laws in the European Union. The new regulation will supersede current European Union data protection legislation, may impose more stringent European Union data protection requirements on us or our customers, and may prescribe greater penalties for noncompliance.”
“Through our ... business, we maintain a database of administrative and clinical data that is statistically de-identified in accordance with HIPAA standards. Noncompliance or findings of noncompliance with applicable laws, regulations or requirements, or the occurrence of any privacy or security breach involving the misappropriation, loss or other unauthorized disclosure of protected personal information, whether by us or by one of our third-party service providers, could have a material adverse effect on our reputation and business, including mandatory disclosure to the media, loss of existing or new customers, significant increases in the cost of managing and remediating privacy or security incidents and material fines, penalties and litigation awards, among other consequences, any of which could have a material and adverse effect on our results of operations, financial position and cash flows.”

~

“Among other things, we have experienced automated attempts to gain access to our public facing networks, brute force, SYN flood and distributed denial of service attacks, attempted malware infections, vulnerability scanning, ransomware attacks, spear-phishing campaigns, mass reconnaissance attempts, injection attempts, phishing, PHP injection and cross-site scripting. We also have seen an increase in attacks designed to obtain access to consumers’ accounts using illegally obtained demographic information.”

**Automotive**

“The Company relies on information technology systems, including the internet and other computer systems, which may be subject to disruptions during the process of upgrading or replacing software, databases or components; power outages; hardware failures; computer viruses; or outside parties attempting to disrupt the Company’s business or gain unauthorized access to the Company’s electronic data.”

~

“Despite security measures, we are at risk for interruptions, outages, and breaches of: (i) operational systems (including business, financial, accounting, product development, consumer receivables, data processing, or manufacturing processes); (ii) facility security systems; and/or (iii) in-vehicle systems or mobile devices. Such cyber incidents could materially disrupt operational systems; result in loss of trade secrets or other proprietary or competitively sensitive information; compromise the privacy of personal information of customers, employees, or others; jeopardize the security of our facilities; affect the performance of in-vehicle systems; and/or impact the safety of our vehicles.”
“Omni-channel retailing is rapidly evolving and we must keep pace with changing customer expectations and new developments by our competitors. Our customers are increasingly using computers, tablets, mobile phones, and other devices to comparison shop, determine product availability and complete purchases, as well as to provide immediate public reactions regarding various facets of our operations. We must compete by offering a consistent and convenient shopping experience for our customers regardless of the ultimate sales channel and by investing in, providing and maintaining digital tools for our customers that have the right features and are reliable and easy to use. If we are unable to make, improve, or develop relevant customer-facing technology in a timely manner that keeps pace with technological developments and dynamic customer expectations, our ability to compete and our results of operations could be materially and adversely affected. In addition, if our online activities or our other customer-facing technology systems do not function as designed, we may experience a loss of customer confidence, data security breaches, lost sales, or be exposed to fraudulent purchases, any of which could materially and adversely affect our business operations, reputation and results of operations.”

“We accept payments using a variety of methods, including cash, checks, credit and debit cards, our private label credit cards and gift cards, and we may offer new payment options over time, which may have information security risk implications. As a retailer accepting debit and credit cards for payment, we are subject to various industry data protection standards and protocols, such as payment network security operating guidelines and the Payment Card Industry Data Security Standard. We cannot be certain that the security measures we maintain to protect all of our information technology systems are able to prevent, contain or detect any cyber-attacks, cyber terrorism, or security breaches from known cyber-attacks or malware that may be developed in the future. To the extent that any cyber-attack or incursion in our or one of our third-party service provider’s information systems results in the loss, damage or misappropriation of information, we may be materially adversely affected by claims from customers, financial institutions, regulatory authorities, payment card networks and others. In certain circumstances, payment card association rules and obligations to which we are subject under our contracts with payment card processors make us liable to payment card issuers if information in connection with payment cards and payment card transactions that we hold is compromised, which liabilities could be substantial. In addition, the cost of complying with stricter and more complex data privacy, data collection and information security laws and standards could be significant to us.”
“Compliance with more rigorous privacy and information security laws and standards may result in significant expense due to increased investment in technology and the development of new operational processes.”

“...industry requirements, such as Generally Accepted Privacy Principles may be imposed on us by our contracts with our ... clients or other customers. Many of our businesses are also subject to the Payment Card Industry Data Security Standard, which is a security standard mandated by the credit card industry for the purpose of protecting credit card account data. These increasingly complex laws, regulations and industry requirements are subject to change and compliance with them may result in significant expenses associated with increased operational and compliance costs, particularly as we continue to collect and retain large amounts of information. To the extent that either we or our vendors with whom we share information are found to be out of compliance with applicable laws and regulations or experience a data security breach, we could be subject to additional litigation, regulatory risks and reputational harm.”

“[O]n October 1, 2015, the payment card industry shifted liability for certain transactions to retailers who are not able to accept Europay, MasterCard, Visa (EMV) transactions. We completed the implementation of the EMV technology for our supermarket transactions, and have a plan in place to complete implementation for our fuel centers prior to the liability shift for fuel centers, which will occur in 2020.”

“We accept payments using a variety of methods, including cash, checks, credit and debit cards, PayPal, our private label credit cards, an installment loan program, trade credit, and gift cards, and we may offer new payment options over time. ... The payment methods that we offer also subject us to potential fraud and theft by criminals, who are becoming increasingly more sophisticated, seeking to obtain unauthorized access to or exploit weaknesses that may exist in the payment systems.”

“Access to the Internet from computers, tablets, smart phones and other mobile communication devices has empowered our customers and changed the way they shop and how we interact with them. Our websites, including [], are a sales channel for our products, and are also a method of making product, project and other relevant information available to our customers that impacts our in-store sales. Additionally, we have multiple affiliated websites and mobile apps through which we seek to inspire, inform, cross-sell, establish online communities among and
otherwise interact with our customers. Performance issues with these customer-facing technology systems, including temporary outages caused by distributed denial of service, ransomware or other cyber-attacks, or a complete failure of one or more of them without a disaster recovery plan that can be quickly implemented, could quickly destroy the positive benefits they provide to our home improvement business and negatively affect our customers’ perceptions of the Company as a reliable online vendor and source of information about home improvement products and services.”

Insurance

“The area of cybersecurity has also come under increased scrutiny by insurance regulators. On March 1, 2017, New York’s cybersecurity regulation for financial services institutions, including banking and insurance entities, became effective, and on October 24, 2017, the NAIC adopted the Insurance Data Security Model Law, which, if adopted as state legislation, would establish standards for data security and for the investigation of and notification of insurance commissioners of cybersecurity events.”

“There has been increased scrutiny, including from U.S. state and federal regulators, regarding the use of ‘big data’ techniques such as price optimization. We cannot predict what, if any, actions may be taken with regard to ‘big data,’ but any inquiries could cause reputational harm and any limitations could have a material impact on our business, financial condition and results of operations.”

Energy

“Threat sources continue to seek to exploit potential vulnerabilities in the electric and natural gas utility industry associated with protection of sensitive and confidential information, grid infrastructure and other energy infrastructures, and such attacks and disruptions, both physical and cyber, are becoming increasingly sophisticated and dynamic.”

“…[N]o cybersecurity or emergency recovery processes is failsafe, and if our safeguards fail or our data or technology infrastructure is compromised, the safety and efficiency of our operations could be materially harmed, our reputation could suffer, and we could be subject us to additional costs, liabilities, and costly legal challenges, including those involving privacy of customer data.”
Trucking & Courier Services

“In addition, the provision of service to our customers and the operation of our networks and systems involve the storage and transmission of significant amounts of proprietary information and sensitive or confidential data, including personal information of customers, employees and others. To conduct our operations, we regularly move data across national borders, and consequently we are subject to a variety of continuously evolving and developing laws and regulations in the United States and abroad regarding privacy, data protection and data security. The scope of the laws that may be applicable to us is often uncertain and may be conflicting, particularly with respect to foreign laws. For example, the European Union’s General Data Protection Regulation (‘GDPR’), which greatly increases the jurisdictional reach of European Union law and adds a broad array of requirements for handling personal data, including the public disclosure of significant data breaches, becomes effective in May 2018. Other countries have enacted or are enacting data localization laws that require data to stay within their borders. All of these evolving compliance and operational requirements impose significant costs that are likely to increase over time.”

Chemicals

“The Company has designed and implemented internal controls to restrict access to and distribution of its intellectual property. Despite these precautions, the Company’s intellectual property is vulnerable to unauthorized access through employee error or actions, theft and cybersecurity incidents, and other security breaches. When unauthorized access and use or counterfeit products are discovered, the Company reports such situations to governmental authorities for investigation, as appropriate, and takes measures to mitigate any potential impact. Protecting intellectual property related to biotechnology is particularly challenging because theft is difficult to detect and biotechnology can be self-replicating. Accordingly, the impact of such theft can be significant.”