EBOOK

Data Privacy in 2019

How to Protect Consumer Data in the Age of Information Sharing

Norman Ford

Norman Ford, VP Compliance Products, Skillsoft Compliance

skillsoft compliance

In late 2018, a global hotel chain announced that personal information for as many as 500 million guests may have been compromised in a security breach of its reservation database. The year before, a major U.S. credit reporting agency revealed that 146 million accounts were exposed. Those are the more recent major data breaches that U.S. companies have experienced, but they're not even the largest—nor the most expensive. Ponemon Institute, which has been measuring the cost of data breaches since 2005, estimates that a breach involving one million records could cost $39.49 million in detection and escalation, post-breach response (including fines), notification, and lost business. At 50 million records, the total cost could be as high as $350 million.[1] In the first 11 months of 2018 alone, there were 1,138 data breaches in the U.S., with more 561 million records exposed.[2]

Unsurprisingly, this issue has caught the attention of regulators, and recent legislation, such as the European Union's General Data Protection Regulation (GDPR), has increased liability and complexity for companies that hold customer data. Unfortunately, many organizations still fail to fully understand the scope of the problem. While 65 percent of C-suite executives believe their cybersecurity strategy is well-positioned, just 17 percent of these strategies are considered at the highest level.[3]

One reason for this gap may be that if a company hasn't experienced a breach, leadership might incorrectly assume their defenses are adequate. But another reason might be borne of a common misperception: that IT alone is responsible for safeguarding sensitive data. However, privacy isn't just an IT issue. While technology solutions are critical, people are often the weakest link in an organization's cyber defenses. Consider that 28 percent of attacks involve internal actors, yet many employees do not receive any form of cybersecurity training.[4] The solution, then, is a comprehensive program of awareness, education and training to facilitate each member of the organization's participation in a comprehensive data privacy strategy.

Personal info of **500 million guests** exposed by global hotel chain in 2018

146 million records exposed by U.S. credit bureau in 2017

= $350m

Ponemon Institute estimates the cost of a data breach of **50 million records at $350 million**

28% of attacks involve an internal actor, yet many employees don't receive any cybersecurity training.

1 "2018 Cost of a Data Breach Study." Ponemon Institute, 2018.
2 "ITRC Data Breach Reports." Identity Theft Resource Center, November 30, 2018.
3 "Securing the C-Suite: Cybersecurity Perspectives from the Boardroom and C-suite." IBM, 2016.
4 "2018 Data Breach Investigations Report." Verizon.

THE DATA PRIVACY PARADOX

Data has become one of the most valuable assets a company can hold—essential to business models that include marketing and customer service. And wary as they are, customers now expect the convenience that comes with data sharing. A 2017 study by Stanford University and MIT found that most undergraduates were willing to provide three friends' email addresses in exchange for a free pizza.[5] At the same time, however, consumers expect that their data will be protected. A study by the Identity Theft Resource Center revealed that 75 percent of consumers say they would not buy a product from a company—no matter how great the products are—if they don't trust the company to protect their data.[6] Breaches, therefore, can result not only in regulatory fines, but even more costly response and reputational damage. In 2018, the average total cost of a data breach reached $3.86 million, an increase of 6.4 percent over 2017.[7]

IMPLICATIONS FOR THE ORGANIZATION

Clearly, "out of sight, out of mind" is not an effective data privacy strategy. Instead, organizations must engage employees at every level to protect their customers' private data.

Corporate leadership. Boards, CEOs, and other members of the C-suite must put data privacy on the agenda and make it a part of their company culture, executive meetings, and all-hands meetings. Without support at the highest levels of management, any program is bound to struggle. In a study by email provider Mimecast, nearly 40 percent of executives said their CEOs themselves were a cybersecurity weak link.[8] One of the most important considerations is to integrate data privacy into strategy. Organizations need to set priorities to ensure that business models and processes do not conflict with data privacy goals.

Human Resources. HR plays a critical role in spreading the gospel of data privacy. First, of course, HR is a repository for private employee information. It also needs to coordinate training for all employees, so they understand what information requires protection and how to recognize ways in which malicious actors use social engineering to gain access to it.

of consumers won't buy products from a company they don't trust to protect their data

$3.86 million

The average cost of a data breach in 2018

Almost **40%** of execs name their CEOs as the weakest cybersecurity link

5 "Pizza over privacy? Stanford economist examines a paradox of the digital age." May Wong, Stanford News, August 3, 2017.
6 "New Survey Finds Deep Consumer Anxiety Over Data Privacy and Security." IBM, April 16, 2018.
7 "2018 Cost of a Data Breach Study." Ponemon Institute, 2018.
8 "The State of Email Security." Mimecast, 2018.

Legal. The role of the legal department is to communicate the legal implications of failing to meet private data security requirements and expectations.

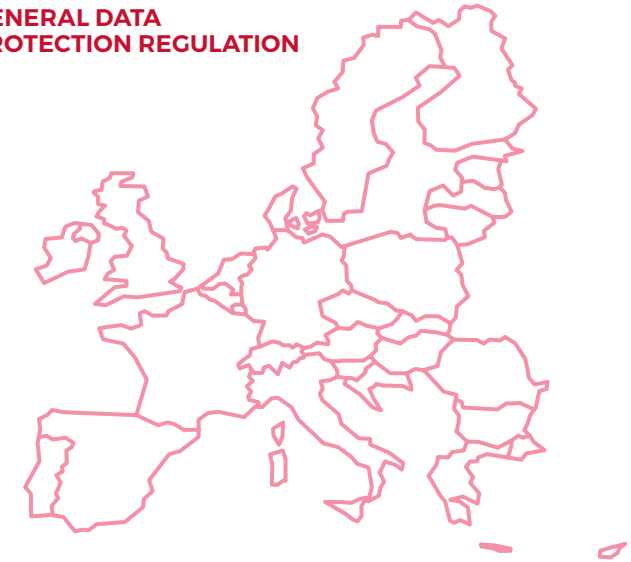
Compliance. The risk management and/or compliance teams are central to establishing data governance policies and procedures. This group needs to communicate specific regulatory requirements in all jurisdictions across the organization.

DATA PRIVACY REGULATIONS

As anxiety about data privacy rises, governments around the globe have responded with regulations that give consumers greater control over their own data and establish complex rules about how organizations hold and share such data. Here's a quick look at some of the most significant recent regulations:

General Data Protection Regulation (GDPR). In 2016, the European Union enacted the most sweeping and comprehensive consumer data protection regulation to date. GDPR, which became effective in May 2018, applies to any company that has customers in the EU, which means that most global companies must adhere to it. Primary among the many requirements that GDPR imposes is the "right to be forgotten" (i.e., have one's data removed completely) and data portability (the ability to download one's data in a readable format and reuse), both of which impose high technological hurdles for companies to achieve. But the law also includes stipulations on general data governance and corporate accountability. Adding to the complexity, the regulation itself comprises 99 dense articles and is descriptive rather than proscriptive. The articles focus more on goals than procedures, making it more difficult to comply with than more straightforward standards, such as the Payment Card Industry Data Security Standard (PCI DSS). What's not in dispute are the high costs of non-compliance: GDPR imposes fines as high as €20 million (about US$23 million as of this writing) or 4 percent of the organization's annual global revenue, whichever is greater.

GENERAL DATA PROTECTION REGULATION



GDPR requires the **"right to be forgotten"** and data portability

GDPR imposes fines as **high as $23 million or 4%** of the offending company's annual revenue—whichever is greater

Brazil's General Data Privacy Law (LGPD). Brazil's legislation, which will become effective in February 2020, closely mirrors GDPR, while imposing shorter deadlines for companies to comply with consumer requests and broadening the range of companies affected to include even small businesses. Non-compliance could result in fines amounting to 2 percent of gross sales or a maximum sum of R$50 million per infringement (approximately US$12.9 million.)

LGDP fines can reach **2% of a company's gross sales or $12.9 million** per infringement

BRAZIL GENERAL DATA PRIVACY LAW

California Consumer Privacy Act (CCPA). California's latest data privacy legislation, which goes into effect in January 2020, is the most comprehensive data privacy law in the U.S. and applies to any company with customers residing in California. Similar to GDPR, CCPA gives California residents the right to request the deletion of personal information and to opt out of the sale of personal information. The law also provides users the right to data portability. Perhaps the most significant aspect of CCPA is its broad definition of "personal data," which includes not only a consumer's personal identifying information (PII), but also geolocation, biometric data, internet browsing history, psychometric data, and inferences a company might make about the consumer.

"Personal Data" under CCPA includes:

- Personal identifying information
- Geolocation
- Biometric data
- Internet browsing history
- Psychometric data

CALIFORNIA CONSUMER PRIVACY ACT

Colorado Protections for Consumer Data Privacy. Of more immediate concern for businesses is the extension of the Colorado Consumer Protection Act (CCPA), which went into effect in September 2018. The legislation expands three areas of the original law. First, it requires companies of all sizes to take all "reasonable" measures to protect PII they hold and to create a security plan explaining how customer data is handled and to set a procedure should a breach occur. However, the law leaves "reasonable" undefined, making it difficult to know if a plan is fully compliant. Second, companies experiencing a data breach must notify affected customers within 30 days. If more than 500 Coloradans are impacted, the business must also notify the state's attorney general. Finally, companies must develop and implement written policies governing the destruction of both paper and electronic records containing PII.

Companies must **notify affected customers within 30 days** of a data breach, under the Colorado Consumer Protection Act

COLORADO CONSUMER PROTECTION ACT

CREATING A COMPLIANCE CULTURE

Given the increasingly complex nationwide and worldwide regulatory landscape, a "check the box" approach to compliance will not work. There are simply too many overlapping rules across multiple jurisdictions to consider. Instead, organizations should establish a broad data privacy strategy including high information governance standards for themselves that meet or exceed regulations. Creating such a culture of compliance will not only avoid the risk of regulatory sanctions, costly reparations, and incalculable reputational damage, but also reap competitive advantage in terms of consumer trust.

Compliance culture is crucial as well because data security is not simply an IT responsibility. In fact, among the greatest risks to privacy and information security are employee actions. While bad actors certainly exist, even well-meaning but uninformed employees can cause a breach by falling for a phishing scam, inadvertently downloading malware, or clicking on a malicious link. Therefore, any training should encompass both broad data privacy concepts as well as specific requirements and cyber threats.

UNDERSTANDING DATA PRIVACY

Your organization's training should include basic data privacy concepts so that employees understand what is at stake for the company, its customers and employees themselves. Coverage should include these broad concepts:

What is protected information? Depending on your industry and their function, your employees may have access to several types of customer or employee personal information. Personal identifiable information (PII) is data that could be linked to a particular individual, such as a bank account number or social security number. Your training should distinguish PII from aggregate information that, while provided by customers and/or their actions, does not reveal any individual's identity. Examples include overall website traffic or compiled survey response statistics. In some cases, employees may have access to private health information (PHI), which may be considered a subset of PII. In the U.S., PHI is protected under the Healthcare Insurance Portability and Accountability Act (HIPAA).

What are the consequences of failure? Before getting into the specifics of how to protect private data from falling into the wrong hands, it's important to ensure that employees understand what's at stake. Have them consider how they would feel if their own personal information were mishandled. Explain the consequences to the organization of a breach—including loss of trust and reputation, liability costs, and revenue loss. Explain that if malicious actors gain

access to the company's networks they can install malware or ransomware, which could grind operations to a standstill.

Data mobility. All the security protocols in the world are of little help if a device, such as a laptop, isn't secured. As mobile devices, such as smart phones, tablets, and thumb drives proliferate, the chances that PII can fall into unauthorized hands increases. This is true whether their organization has a bring-your-own-device (BYOD) policy or not.

Data sharing. Employees must also understand when it is appropriate to share data and when it is not. Certainly, intra-office sharing of information between two authorized users is appropriate, but even in that case, they should use approved methods to maintain security.

Data retention policies. Finally, your employees should understand that in many cases, data should be destroyed after an appropriate retention period. Failure to do so can lead to costly legal liability in the form of lawsuits or regulatory infractions. While data retention policies can be automated to a certain degree, employees must understand why they should not circumvent such processes by, for example, downloading data onto their desktop computer.

ADDRESSING COMMON THREATS

When your employees have a good understanding of the reasons behind data security and what data to protect, you can then arm them with specific ways to combat breaches. Here are a few common threats that every employee should know how to thwart:

Phishing. It is a cybercrime in which cybercriminals pose as legitimate institutions using email, phone, or text to lure individuals into providing sensitive data. They can use this information to gain access to individual accounts or even entire networks. Your training should highlight the telltale signs of phishing, particularly look-alike links (e.g., google.com.fakeurl.com) that request information on web pages that imitate the official site. Users should also make sure they recognize the sender's email address and be particularly wary of attachments they did not request. Emphasize caution and encourage employees to reach out directly to the apparent sender by phone or separate email to confirm a message's validity.

Communication habits. Even if your company has strict data-sharing policies and provides the appropriate technology to share data within and without the organization securely, employees may be tempted to circumvent them for convenience's sake. It is all too easy to send such information over insecure formats, such as email, chat, or social media, so it is imperative that employees understand the potential consequences of doing so. Additionally, they should understand who is authorized to receive PII, and how to ascertain the identity of the recipient.

Device security. It is crucial that employees understand that a lost or stolen device can expose their organization to enormous liability. They should avoid downloading sensitive information to mobile devices, and make sure they have adequate security in place, such as multi-factor authentication and the ability to wipe a device's data remotely.

ENGAGING TRAINING TO GO BEYOND "CHECKING THE BOX"

Shaping corporate culture means adjusting behavior and attitudes, which requires a sophisticated training approach. Establish that your training strategy leverages each of these important components:

Engage the whole organization. As we hope we've shown here, cybersecurity training is for everyone in your organization. Incorporate it into onboarding and annual review cycles for all your employees.

Structure training to maximize retention. Your training should break down into tangible learning objectives that are met through an engaging presentation of information, practice opportunities, and evaluation. Strategies including the use of practical examples, case studies, video scenarios, animation, and narration help to maximize engagement and retention.

Leverage brain science. Years of scientific research indicates that people need three things for an optimal learning experience: relevance, meaning, and emotion. Your courses should focus on the learner, incorporating real-world scenarios that foster a linkage between emotion and cognition.

CONCLUSION

Protecting data privacy grows more important by the day, as personal information becomes more valuable and hackers become more sophisticated. Cybersecurity awareness is now crucial for your entire workforce—not just IT. Data privacy training offers a unique opportunity for companies to go beyond regulatory compliance to develop a corporate culture that builds your organization's reputation as a trusted partner to its customers.

ABOUT THE AUTHOR

NORMAN FORD

As VP of Compliance Products, Norman Ford is responsible for the compliance product portfolio at Skillsoft. Prior to joining Skillsoft, Ford was Vice President of eLearning Products and Services and co-founder of GoTrain Corp. Ford has also served as Manager of Technical Assistance and Qualification for Lockheed Martin Energy Systems, where he was responsible for the development of training requirements and procedures and provided corporate subject matter expertise in regulatory and compliance issues. Norman Ford has over 30 years of experience in Conduct of Operations, Nuclear Operations, Training Drills, Qualification, Certification, Training Procedure and Technical Training issues while serving organizations including Lockheed Martin, the U.S. Department of Energy, and the U.S. Department of Defense (U.S. Navy).

Norman Ford
VP Compliance Products,
Skillsoft Compliance

skillsoft compliance

linkedin.com/company/skillsoft
facebook.com/skillsoft
twitter.com/skillsoft
skillsoftcompliance.com

US 866-757-3177
EMEA +44 (0)1276 401994
ASIA +65 6866 3789 (Singapore)
AU +61 2 8067 8663
FR +33 (0)1 83 64 04 10
DE +49 211 5407 0191
IN +91-22-44764695
NZ +64 (0)21 655032

ABOUT SKILLSOFT COMPLIANCE SOLUTIONS

Skillsoft Compliance Solutions provides ethics, risk mitigation, and workplace safety training tailored to meet an organization's unique, industry-specific requirements. With over 500 risk topics in 32 languages, Skillsoft offers one of the largest selections of compliance training to ensure organizations can effectively meet regulatory obligations and encourage the behavioral changes needed support a culture of compliance.

Developed in partnership with industry-leading compliance experts, courses are constructed on key instructional design principles, leveraging the latest brain science research to accelerate ethical and workplace safety practices across an organization. With Percipio Compliance, an advanced learning management system, Skillsoft delivers an engaging user experience along with the robust functionality necessary to manage complex training needs.

Through a comprehensive suite of training services and compliance-based learning solutions, Skillsoft Compliance Solutions helps businesses protect against risk and safeguard employees.