Digital River®

WARNING: Your Brand May be at Risk

Protect your data and maintain compliance in an ever-changing ecommerce environment

CONTENTS

Executive Summary

When it comes to global ecommerce, advancements in modern technology have allowed brands—both big and small—to connect directly with consumers in ways like never before. While this has provided unprecedented access to goods from far reaches of the globe, it has exposed brands to a myriad of malicious and fraudulent data activity and cyber threats. In turn, hundreds of data-related laws have been created worldwide to protect consumers and their personal information.

As technology advances at a dizzying speed, governments and businesses alike are scrambling to create and abide by stronger legal safeguards to protect their citizens. Today approximately 109 of the 195 countries in the world have some form of data protection laws in place.[1] While the reach around the globe increases, the number of compliance laws increase—making running a global business more complex than ever before.

It's imperative for global ecommerce businesses to understand the ever-changing international landscape of cyber security and data protection laws. Any vulnerabilities or missteps with fraud or compliance disciplines can have huge consequences. And while it does require resources to prepare for a data-related disaster and to comply with global regulations, these costs are minuscule compared to the damage that can ensue if a business is unaware or unprepared. Fines, investigations, negative media attention, revenue loss and brand depreciation are all scary and real consequences.

The Rising Cost of Cyber Threats and Data Breaches

Experts agree: the costs associated with potential data breaches are now a consistent cost of doing business, as the threat of cybercrime is widely considered to be a permanent risk. On average, the total cost of a single data breach rose from $3.8 million in 2015 to $4 million in 2016.[3]

$4M

The Average Cost of a Single Data Breach

Breaches, investigations and fines

No executive wants the negative attention, clean up costs, government investigations and fines that are likely to follow a data breach. Worse than the time and money required to clean up after a breach is withstanding the assault that follows loyal customers, shareholders and employees catching wind of a breach, regulatory investigations, massive fines and/or possibly a class-action lawsuit. The fallout is damaging and may have lasting effects. Loss of consumer confidence is particularly distressing as it can cause significant revenue loss, forcing executives to make difficult decisions.

To give you an idea of how costly data breaches can be, below are some infamous examples:

- In 2013, cyber thieves siphoned information from more than 1 billion Yahoo accounts, including users' email addresses, scrambled account passwords and dates of birth. The data breach is the largest from a single site in history, according to a database of other hacking incidents. At the time, it was feared the criminals would use the information to go after more sensitive personal data elsewhere online. In August 2016, the hackers were discovered trying to sell 200 million Yahoo accounts, which would have been the second-largest single breach.[16] The result: Verizon's $4.8 billion acquisition deal with Yahoo has been placed on hold, perhaps indefinitely, as the Securities and Exchanges Commission (SEC) in the U.S. investigates.
- In October 2015, Britain's TalkTalk Telecom Group sustained a cyber attack that breached a portion of its customer records, which eventually led to 101,000 lost customers and costs totaling £60 million—the equivalent of $79.8 million.[4] This is double the amount that was originally predicted by the company which was £30-£35 million ($39.9 - $46.6 million).
- In April 2016, the Personal Data Protection Commission (PDPC) in Singapore imposed a financial penalty of S$50,000 ($37,000) on a karaoke chain, K Box Entertainment Group, after a September 2014 data breach that exposed the personal data of 317,000 of its members. In addition, the IT vendor in charge of K Box's content management system, Finantech Holding, was also fined S$10,000 ($7,400) for failing to have proper and adequate protective measures in place to prevent such a breach.[5]
- Also in April 2016, and more widely known, was when the Central American law firm Mossack Fonseca confirmed it was the target of the largest data breach in history. Now known as The Panama Papers, more than 40 years of data was stolen, including 4.8 million emails, 3 million database format files, 2.2 million PDFs, 1.1 million images and 320,000 text documents.[6] The damages in this story continue to amass as various governmental agencies, representing dozens of countries around the globe, continue their investigations.
- In June 2016, the U.S. Securities and Exchange Commission (SEC) fined Morgan Stanley $1 million for failing to properly protect customer information. According to the SEC, Morgan Stanley did not have the policies and procedures in place to prevent an ex-employee from accessing and transferring data related to approximately 730,000 accounts to a personal server, which was then hacked by a third party.[7]

Like fire, a data breach must be contained quickly

If a breach is not identified and contained immediately, costs will escalate quickly. On average, it takes 201 days to identify a breach and an additional 70 days to contain it.[3] In the event of such an emergency, efficient deployment of a predefined incident response plan is necessary for immediate response and damage control. Shockingly, 70% of U.S. security executives say they currently do not have an incident response plan in place.[3]

In the absence of an incident plan, many companies today are leveraging an incident response team, which have been known to save companies considerable money—on average up to $400,000.[3] An incident response team is responsible for time-sensitive activities such as incident forensics, communications and legal expenditures. They are also extremely knowledgeable in regard to regulatory mandates. These activities account for 59% of the cost incurred during a data breach and require great skill and expertise to execute flawlessly. In addition to creating an incident response plan, it's important to develop and enact a business continuity management (BCM) process, which can help you locate and contain a breach in less time. Companies with BCMs in place discovered breaches 52 days earlier, and contained the threat 36 days faster.[3]

When it comes to two of the nastiest words in ecommerce, "data breach"—time is not only money, it's a brand's entire reputation.

Ongoing threats and the importance of internal audits

There was a time when large global corporations were confident that they had the infrastructure and processes in place to protect their systems. But the number of high profile hacks, such as the one on Sony Pictures Entertainment Inc., have technology executives paying more attention to their internal controls. Sony servers were attacked with a vengeance by North Korean hackers who were angered by the studio's release of a comedy that depicted the fictional assassination of their real-life leader. The hackers released sensitive emails from employees, deleted massive amounts of data, stole employee data, and pirated and distributed a series of yet-to-be-released movies. In addition to significant revenue loss, embarrassment and the costs associated with containing and resolving the data breach, Sony agreed to pay up to $8 million to resolve a lawsuit from its employees over the stolen data.[8]

Large corporations are not the only targets these days; a growing number of small and midsized businesses (SMBs) are being besieged as well. No company should feel safe or complacent in today's ecommerce environment.

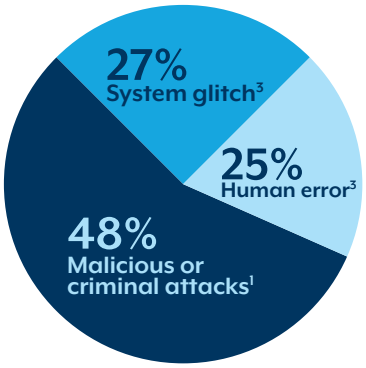
A cost-effective way to protect data privacy is to partner with an accountable service provider that has the experience, processes and procedures in place and will perform regular audits on the effectiveness of these processes. Data breaches are a very real threat and companies need to take the necessary steps to limit risk.

70%

Of U.S. Security Executives Say They Don't Have Incident Response Plans in Place

What causes a data breach?

The Ponemon Institute LLC conducted the 2016 Cost of Data Breach Study. Global Analysis. The study determined the following causes:



If you prefer to tackle data privacy yourself, be prepared for a long and arduous course. Here are just a few questions to ask yourself:

Infrastructure

Do you have a data privacy or information security team? Whom have you appointed to monitor how privacy risks are handled? What gaps exist?

Processes

How do you collect, analyze, store and share client data? What about employee information? Have you mapped the flow of all personal data? What controls are in place to ensure compliance?

Training and testing

How much training has been delivered to your employees? Do your employees know and understand their roles in data security compliance? How often do you conduct training? How do you test your employees' knowledge related to privacy risks?

Auditing

Is data privacy embedded within your regular audit processes? What mechanisms are in place to ensure the information is obtained and processed legally? How do you ensure the information is accurate?

A New Era of Data Protection

Privacy Shield

For the past 15 years, U.S. and EU companies have followed the Safe Harbor agreement, which governed the flow of data from Europe to the United States. This agreement allowed companies to transfer and store the data of EU citizens on U.S. servers if the U.S.-based company stated they were complying with the EU data protection standards. This changed greatly when Edward Snowden, the former U.S. National Security Agency contractor, claimed that U.S. intelligence agencies tapped into commercial internet servers to perform mass surveillance.

In October 2015, the Safe Harbor agreement was declared invalid by the Court of Justice of the European Union (CJEU) and was replaced with the EU-U.S. Privacy Shield, which was released in February, 2016 with the final text issued in July, 2016. Developed by the European Commission and the U.S Department of Commerce, the Privacy Shield's enforceable protection requirements monitor and enforce the laws that protect Europeans' personal data.

The EU is leading the world on enforcement

The EU's 28 data protection authorities allowed a three-month grace period during which U.S. companies were required to bring their data transfers in line with the EU law. During the grace period, the Data Protection Authority (DPA) of Schleswig-Holstein warned that it would issue fines of up to 300,000—the equivalent of $336,810—for the unlawful transfer of personal data.

While most of the companies were compliant through their use of "standard contractual clauses" (SCCs), not all passed the test. On June 6, 2016 the DPA of Hamburg announced that it was issuing fines to three U.S. companies for the unlawful transfer of data from Germany to the U.S. Although each company could have been charged 300,000 ($336,810), the fines were reduced because the companies moved to SCCs during the process. Ultimately, the DPA levied fines on the offending businesses.

What's changed with the Privacy Shield?

On July 12, 2016 the European Commission officially adopted the EU-U.S. Privacy Shield and ushered in a new era of data protection for residents of the EU. Key changes include:

Stricter data limitations

Companies must now delete personal data that no longer serves the purpose for which it was originally collected and retain data for only as long as it's needed.

More detailed privacy statements

How do you collect, analyze, store and share client data? What about employee information? Have you mapped the flow of all personal data? What controls are in place to ensure compliance?

Tighter transfer rules

Data transfers to third-party vendors may only be performed for a limited time for the collection purposes that have been previously provided to the individual. This means additional contractual obligations with service providers and other third parties, and additional oversight by the U.S. Department of Commerce.

More transparent government access

Under the Privacy Shield, the U.S. government commits that access to personal data for national security purposes will be for specific instances, with limits and oversight, and not part of a mass surveillance.

Annual review for compliance

The European Commission and the U.S. Department of Commerce will review the process each year to ensure no barriers exist within the process and will conduct random audits to ensure compliance.

As of August 1, 2016, U.S. companies can apply to the U.S. Department of Commerce for certification under the Privacy Shield. As of this document's publication, Standard Contractual Clauses are still an acceptable data transfer mechanism, but may be more challenging than certification under the Privacy Shield.

Your next steps towards data protection:

1. Develop a strong and consistent privacy policy.
2. Secure your user's personal data.
3. Review all data management processes.
4. Develop and implement a data management program that meets the Privacy Shield requirements.
5. Review your data-sharing contracts with all third parties to ensure compliance with the Privacy Shield.
6. Develop a process to respond to privacy-related complaints.

GDPR enforcement begins in May 2018

New year, new privacy law

In January 2012, the European Commission drew a line in the sand as to what were the best ways to protect the privacy of EU residents. It announced a more comprehensive regulation that more closely aligns with the technology-driven nature of the culture today. Known as the General Data Protection Regulation (GDPR), the law reflects the need for increased privacy for the residents of the 28 EU member states. The GDPR replaces the 20-year-old Data Protection Directive, which was open to interpretation among the EU's individual member states.

The new regulation was officially adopted in April 2016, and enforcement will begin in May 2018, after a two-year transition period. The GDPR requires EU and non-EU organizations that process the personal data of EU residents to institute stricter controls, change processes and possibly even hire additional staff.

To fully understand the GDPR, it's important to note some of the new definitions:

Personal data

Any information relating to an identified or identifiable natural person ("data subject"). The GDPR also states that personal data includes online identifiers and location data such as IP addresses,cookie identifiers and unique device IDs, and all must be protected.

Pseudonymous data

Data that has been subjected to technological enhancements such as key coding or encryption. While it can't directly identify an individual without additional information, it's still considered to be personal data and is subject to the GDPR rules.

Personal data breach

A security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Data controller

An organization or individual with the authority to decide how and why information about data subjects is processed.

Data processor

The person or entity that processes personal data on behalf of the controller.

What can you expect?

Check with your legal counsel to discuss the specifics of how this new law impacts your business within the EU.

Greater enforcement and bigger fines

Regulators are prepared to issue fines for noncompliance and—according to the legal parameters of the regulations—can issue fines of up to 4% of the enterprise's annual global turnover, or up to 20 million euros—whichever is higher.

Increased oversight

Companies will be held accountable for how they control and process personal data of EU residents, and some businesses may be required to appoint a Data Protection Officer to oversee processes and ensure compliance.

Defined time to notify authority of data breaches

When a personal data breach occurs, the data controller must notify the proper supervisory authority within 72 hours from the time you learn of the breach.

Stronger consent guidelines

The implications of making the switch from one-time payments to recurring billing cycles is not to be underestimated. New technology, business processes and revenue management practices are needed to support such a shift.

Data portability

The GDPR rules strengthen an individual's rights to control his/her data by allowing the individual to transfer his/her data from one organization (or service provider) to another in a structured, commonly used and machine-readable format. This means that individuals have the right to request a copy of their personal data to hand over to a potential competitor.

Right to erasure

The GDPR extends EU residents' protection to also include areas of ecommerce.The European Court of Justice believes that the data a company stores is ultimately that company's responsibility to keep secure and protected. In specific circumstances outlined in Article 17 of the GDPR, an individual may request that their personal data be erased.

For example, under Article 17, controllers must erase personal data "without undue delay, if the data is no longer needed, the data subject objects to the processing, or the processing was unlawful." If your company cannot or does not erase a customer's data within one month, you could face stiff penalties of up to 4% of annual worldwide turnover from the preceding financial year or 20 million euros (approximately US$22,426,480), whichever is greater.[17]

What if you use a third party to store the personal data? As a data controller and/or processor, you are legally bound and must ensure that your third party is following the letter of the law.

Compliance Standards for Securing Private Data

Are hackers stealing personal data to uncover financial information, or the opposite? The motivations of the intruder(s) can range greatly. Whether it is greed, boredom, revenge or any other motivating factor, keeping financial information safe is just as important as protecting personal data. Governments worldwide are getting serious about data protection and enacting their own laws, including data localization laws, that require data collected in a particular country to be stored or processed within that country for privacy and security reasons. The countries with data localization laws are currently Russia, Canada, Germany, Indonesia, China and South Korea.[14] The new laws only add to the complex and ever-changing nature of cross-border business.

Financial data standards

Following the accounting scandals of Enron, Tyco and Worldcom that cost investors billions of dollars in the late 1990s, U.S. Congress passed legislation known as Sarbanes Oxley in 2002. The law was created to increase standards for reporting corporate financials. Today, an auditing standard known as the Statement on Standards for Attestation Engagements (SSAE) 16 is an essential part of new vendor selection criteria for service organizations handling sensitive financial data. SSAE 16 is essentially a snapshot of an organization's day-to-day controls over financial data. Although SSAE 16 is an American standard, it mirrors the international standards of the ISAE 3402.

Credit card data standards

Short for Payment Card Industry Data Security Standard, PCI DSS is the standard for storing, processing and transmitting credit card data. If your company stores, processes, or transmits cardholder data, you are a target for criminals looking to steal and use personal financial data. Financial fraud is a serious problem and PCI DSS compliance and certification can be an overwhelming task if you choose to tackle it on your own. Most companies outsource their card processing to third-party specialists who have the expertise needed and proper controls in place to maintain compliance.

If you feel that you have the resources available to maintain your PCI DSS compliance in-house, be prepared for the increased workload. You will be required to:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly test and monitor networks
- Maintain an information security policy

New standards: Introducing PCI DSS 3.2

In April of 2016, the PCI Security Standards Council (PCI SSC) issued a new version of its data security standard to address current challenges and prevent threats. A noted change in PCI DSS 3.2 includes multifactor authentication as a requirement for any personnel with administrative access into environments handling card data. Previously this requirement applied only to remote access from untrusted networks.

Additional changes in PCI DSS 3.2 include:

Multi-factor authentication

PCI DSS 3.2 requires users with administrative access to use multi-factor authentication to access a Cardholder Data Environment (CDE).

Requirements for service providers

Service providers must demonstrate that they have a detection mechanism in place to respond to a failure with critical security controls, and they must conduct penetration tests on the segmentation of the network at least twice a year. In addition, quarterly checks must be completed to ensure that all personnel are following security policies and procedures. Lastly, the top executives from all service providers must demonstrate an understanding of PCI DSS compliance.

An extended migration period

Because of concerns associated with the transition away from SSL and TLS 1.0, the PCI Council pushed back the migration deadline to July 1, 2018. However, organizations must now have a secure offering as of June 30, 2016, and a formal Risk Mitigation and Migration Plan in place to meet the new deadline.

Know your compliance level

PCI compliance can be overwhelming and time consuming—it's not something to be taken lightly. Requirements and fines are based on your company's volume of Card Brand transactions over a period of 12 months. Below are the general merchant requirements as defined by Visa and MasterCard.

Level 1

Merchants processing more than 6 million transactions a year must complete an annual on-site assessment conducted by a qualified PCI assessor and undergo quarterly PCI scans administered by an Approved Scanning Vendor (ASV). Quarterly scans are used to check for vulnerabilities in operating systems, services and devices.

Level 2

Merchants who process 1 million to 6 million transactions a year are considered a Level 2. These companies are not required to undergo an on-site data security assessment but must complete an annual risk assessment with the appropriate Self-Assessment Questionnaire (SAQ). Quarterly PCI scans by an ASV are also required.

Level 3

Merchants who process 20,000 to 1 million e-commerce transactions a year are considered Level 3. Level 3 merchants must complete the annual risk assessment with the appropriate SAQ and conduct quarterly PCI scans, processed by an ASV.

Level 4

Any merchant that processes fewer than 20,000 ecommerce transactions a year is a Level 4 and must complete the appropriate SAQ. These smaller merchants also need to conduct quarterly PCI scans, processed by an ASV. Quarterly PCI scans are also required.

Fines for non-compliance can be as high as **$100,000** per month

Staying Ahead of Global Fraud

In a recent survey of international branded manufacturers and digital services providers, Forrester Consulting found that 58% of the respondents believed protecting their business against fraud was a top priority in their global ecommerce strategy.[9] Rightfully so, as according to the 2016 LexisNexis True Cost of Fraud report, the average number of successful fraudulent transactions grew by 32.1% in 2015 year over year. In addition, retailers reported an average of 236 prevented fraudulent transactions per month in 2015, an increase of 33.3% from 177 the year before.[10]

According to a 2014 survey by Ernst & Young, more than one in ten executives surveyed said that their company has experienced significant fraud in the two years prior.[11]

Also noted:

- Ten countries recorded a significant increase in fraud, including the United States (16% in 2014, up from 8% in 2012), China (8%, up from 4%), Japan (10%, up from 6%) and Russia (16%, up from 10%).
- In six countries, more than 25% of respondents reported experiencing significant fraud rates in the past two years. These included Egypt, with the highest level at 44%, as well as Germany and Norway at 26% each.

It seems that corruption is playing a significant role in the rising fraud rates globally. A 2014 survey by Ernst & Young showed that in 40% of the countries surveyed, more than half of the respondents said corruption was widespread, with that number rising to a staggering 80% for those surveyed in Egypt, Kenya and Nigeria.

The data speaks volumes for the current fraud landscape, where it appears that the more the good guys do to prevent fraud, the better the bad guys get at committing the crime. Criminals are getting smarter, which translates into more complex attacks that cause greater damage. Remember the negative headlines involving U.S. retail giant Target? In 2013, hackers broke into the company's network and accessed private data, affecting 70 million customers. Between 2013 and 2014, the breach cost Target its reputation and more than $162 million in expenses that were not covered by insurance.[12]

Roles and Responsibilities Within the C-Suite

Chief Executive Officer (CEO)

Responsible for the entire company, its employees and possibly the shareholders, the CEO must fully understand the implications that uncontrolled fraud or a significant data breach could have on their company. They must understand the impact of the latest global laws and hire the right people—or the right business partners—to manage the company's compliance initiatives so that they are able to focus on more strategic initiatives to grow the business. Critical missteps or poor leadership in these areas could be devastating to the ongoing life of the business and to their career.

Chief Financial Officer (CFO)

Plays a critical role in the fraud and risk management chain. The CFO must understand the risks entirely and have processes in place to mitigate those risks. According to a 2014 survey by Ernst & Young, only 41% of CFOs view cybercrime as a concern.[11]

Chief Technology Officer (CTO) & Chief Information Officer (CIO)

The General Data Protection Regulation (GDPR) and the EU-U.S. Privacy Shield have a direct impact on these and all other C-Suite roles. Compliance with new data protection laws are likely to be expensive as you refine processes, address technical issues and commit sufficient time and resources to ensure that the personal information of EU residents is protected.

In light of the new challenges of running a global business, the C-Suite is expanding and welcoming new positions like the Chief Privacy Officer to their ranks. Today many multinational corporations are defining roles for Chief Privacy Officer or Chief Data Privacy Officer that ensure compliance with all global data protection laws and regulations on a day-to-day basis.

Conclusion

Data breaches and compliance failures—these are the types of threats that induce stress and rob business executives of valuable sleep. While expanding into global markets can have big rewards, it also comes with countless risks. You can have the best technology in the world powering your ecommerce, but it means nothing if your business is forced to dissolve for failing to have the correct processes in place to comply with industry rules or local laws.

Any vulnerabilities or missteps in global fraud and compliance disciplines can have huge consequences. You can't put a price tag on these areas of global commerce, but having the right processes in place can deliver huge savings and peace of mind.

We're all-in, fully committed to each facet of your ecommerce business. Contact us today.

E: info@digitalriver.com | US: +1 800 598 7450 | UK: +44 (0) 845 603 5070 | TW: + 886 2 8173 1711

Digital River®

digitalriver.com

1 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529
2 http://www.lexology.com/library/detail.aspx?g=5e4a3ef5-5f8d-41ca-91e8-1320513ca659
3 2016 Cost of Data Breach Study: Global Report; Benchmark research sponsored by IBM. Independently conducted by Ponemon Institute LLC, June 2016
4 https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave
5 http://news.asiaone.com/news/singapore/k-box-challenger-metro-among-11-companies-fined-and- warned-breaching-personal-data
6 http://www.computerworld.com/article/3052218/security/the-massive-panama-papers-data-leak-explained.html
7 http://www.bloomberg.com/news/articles/2016-06-08/morgan-stanley-to-pay-sec-fine-tied-to-adviser-s-data-breach
8 http://www.reuters.com/article/us-sony-cyberattack-lawsuit-idUSKCN0SE2JI20151020
9 Accelerate Global Growth While Reducing Risk; February 2015 thought leadership paper commissioned by Digital River and conducted by Forrester Consulting
10 http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx
11 http://www.ey.com/Publication/vwLUAssets/Overcoming_compliance_fatigue/$FILE/13th%20GLOBAL%20FRAUD%20SURVEY%20FINAL%20low%20res.pdf
12 https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/
13 http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VcJZlvlVhBc
14 The 2017 Data Privacy and Cybersecurity Update", Lisa J. Sotto, Hunton & Williams LLP
15 https://www.bloomberg.com/gadfly/articles/2016-12-15/yahoo-s-cyberfail-could-cut-1-billion-from-verizon-deal
16 http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html
17 See Article 83, http://eur-lex.europa.eu/eli/reg/2016/679/oj.