AmTrust FINANCIAL

What is the GDPR?

The Impact on the Insurance Industry and Small Businesses in the U.S.

Table of Contents

04 What is the GDPR?

05 How Does the GDPR Impact the U.S. and Small Businesses?

06 Policy Checklist

07 California Consumer Privacy Act

08 GDPR Impact on Insurance Industry

09 GDPR and Cyber Liability Insurance

10 Definition of Terms in GDPR

12 Key GDPR Actions

13 Sources

In early 2018, people started receiving updated privacy notification emails from their financial institutions, personal email companies, social media accounts and any other business that collects and uses personal data. If you regularly receive newsletters from certain companies, you also might have received emails asking you to re-subscribe to these newsletters or other marketing emails.

All of these notifications were sent because of the privacy policies implemented by the European Union's (EU) GDPR that went into effect in spring of 2018. U.S. businesses might not think that it matters to them, but in truth, it impacts every business, both small and large, in the country.

Join us for a look into the GDPR, what it is, and how it impacts small businesses, including the insurance industry, in the United States.

What is the GDPR?

On May 25, 2018, the European Union enacted the General Data Protection Regulation (GDPR), a comprehensive data privacy law. The law, which is an update to the outdated 1995 Data Protection Directive, reflects the need for privacy laws relevant to today's technology. The GDPR's goal is to reduce the myriad of individual EU country data protection laws into one standard. Although this has been achieved to a certain extent, there are laws which individual countries have passed which may include requirements beyond the scope of GDPR. For example, Germany has specific laws, which depending on how they are interpreted, may require the personal identifiable information (PII) of German citizens to remain in Germany.

One of the purposes of the GDPR is to bridge a perceived gap between the EU's fundamental right to privacy and the routine collection and use of personal data in our increasingly digitalized economy. It places more requirements on organizations that process and collect personal data with an emphasis on accountability and evidencing compliance, while strengthening the individual's rights. The GDPR is viewed as a model for updating privacy laws around the world. In fact, California has passed a wide-reaching privacy law that will go into effect in 2020.

The GDPR's goal is to reduce the myriad of individual EU country data protection laws into one standard.

GDPR - An overview

Increased Fines
4% of global turnover or €20,000,000

Opt-in Consent
Clear, no opt-out, use data only as agreed

Breach Notification
72 hours to regulators, users "without delay"

Territorial Scope
Organizations with data on EU individuals

Joint Liability
Data controllers and processors

Right to Removal
Users are in charge

Removes Ambiguity
28 laws become one

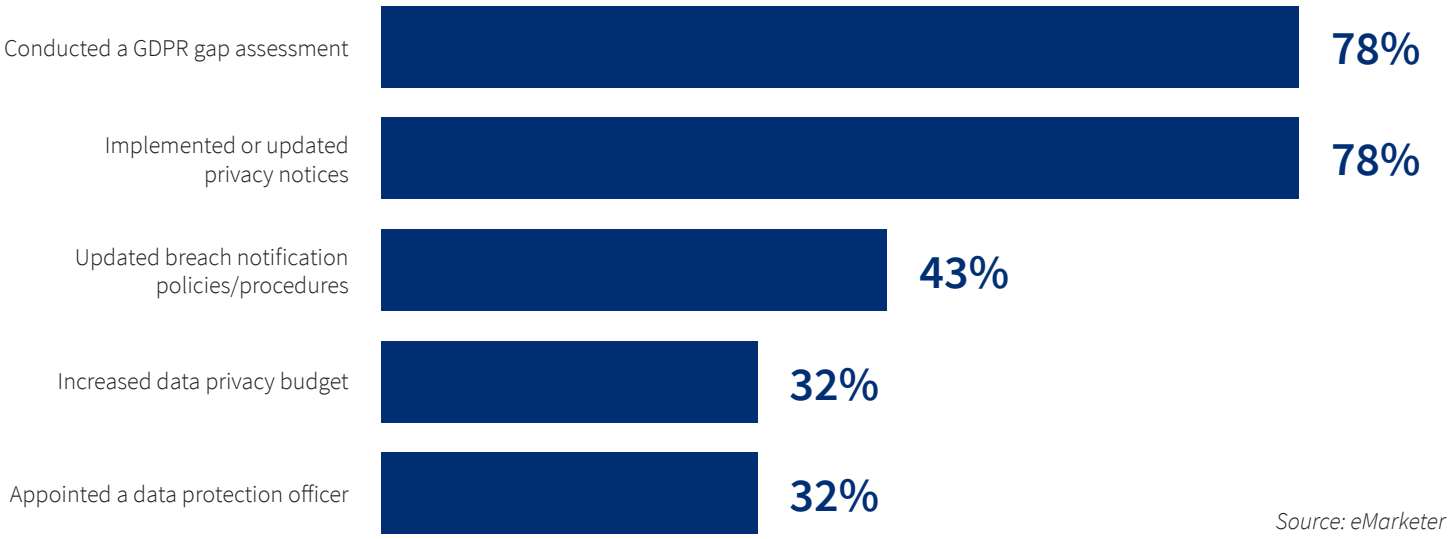
Data Transfer
Data keeps privacy rights as it moves globally

Common Enforcement
Authorities will be strict

Collective Redress
Class Action Lawsuits from individuals

How Does the GDPR Impact the U.S. and Small Businesses?

What steps have companies in the United States taken to comply with GDPR?



Source: eMarketer

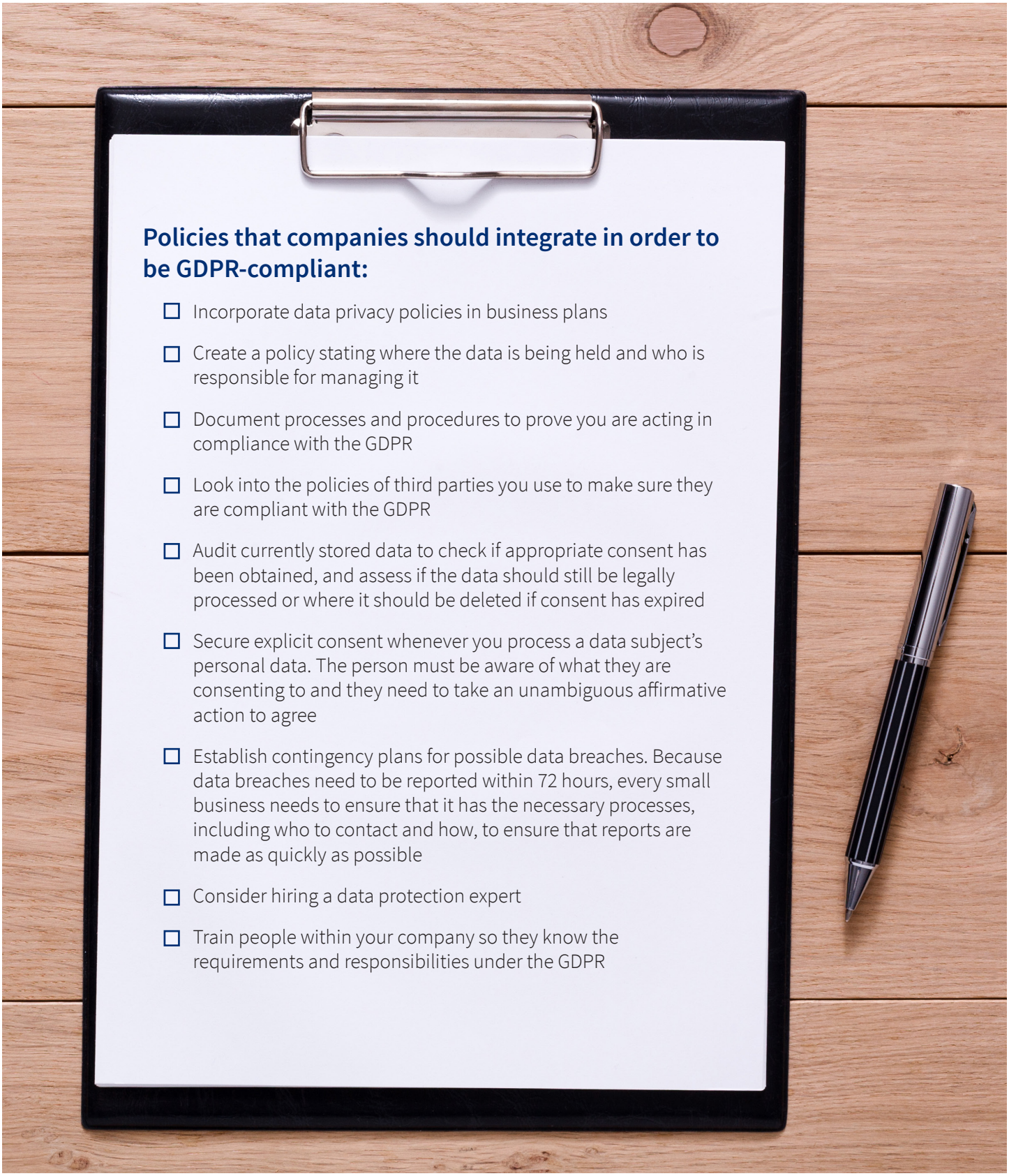
Starting in spring 2018, international companies sent out a variety of notices about their data privacy initiatives. Users received privacy updates from credit card companies, saw privacy notices from their social media accounts, received emails asking them to re-subscribe to a company's marketing emails or viewed "cookie collection" notifications on their favorite websites. The emails and notifications were consequences of the privacy policies implemented by the GDPR.

Small businesses need to engage in the same way as their larger counterparts to ensure sensitive data is protected to be compliant with the GDPR.

Any small business which processes the personal data of people within the EU is subject to the GDPR, no matter where in the world the business is based. It is important to note that the GDPR applies to people within the EU, but not necessarily to EU citizens.

The GDPR applies to all data directly or indirectly related to an identifiable person in the EU that is processed by an individual, company or organization. This means that any company using the data of EU subjects, even if this company is stationed outside the EU, will need to comply with new ways of protecting data related to identifying information, IP address, cookies, health, genetic or biometric data, racial or ethnic data and sexual orientation.

Any company using the data of EU subjects, even if this company is stationed outside the EU, will need to comply with new ways of protecting data related to identifying information, IP address, cookies, health, genetic or biometric data, racial or ethnic data and sexual orientation.



Policies that companies should integrate in order to be GDPR-compliant:

- ☐ Incorporate data privacy policies in business plans
- ☐ Create a policy stating where the data is being held and who is responsible for managing it
- ☐ Document processes and procedures to prove you are acting in compliance with the GDPR
- ☐ Look into the policies of third parties you use to make sure they are compliant with the GDPR
- ☐ Audit currently stored data to check if appropriate consent has been obtained, and assess if the data should still be legally processed or where it should be deleted if consent has expired
- ☐ Secure explicit consent whenever you process a data subject's personal data. The person must be aware of what they are consenting to and they need to take an unambiguous affirmative action to agree
- ☐ Establish contingency plans for possible data breaches. Because data breaches need to be reported within 72 hours, every small business needs to ensure that it has the necessary processes, including who to contact and how, to ensure that reports are made as quickly as possible
- ☐ Consider hiring a data protection expert
- ☐ Train people within your company so they know the requirements and responsibilities under the GDPR

California Consumer Privacy Act

California recently passed a sweeping consumer privacy law that might force significant changes on companies that deal in personal data. This landmark policy, similar to the EU's GDPR, could be the most stringent data protection regime in the U.S.

The new law, California Consumer Privacy Act A.B. 375, gives California residents an assortment of new privacy rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. The law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information and access the personal information in a "readily useable format" that enables the easy transfer of the data to third parties.

The law, which is set to go into effect in 2020, technically applies only to California residents, however it will most likely have much broader implications. Most national companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some California customers. Organizations will have to either reform their global data protection and data rights infrastructures to comply with California's law or institute a patchwork data regime in which Californians are treated one way and everyone else another. The penalties from not complying with the law costs companies up to $7,500 per violation.

GDPR Impact on Insurance Industry

Cavalier attitudes towards the protection of sensitive data and the unauthorized transfer of private information will find the GDPR to be punishing and dissuasive - in short it will no longer be tolerated, at least in California and the EU.

Ian Thorton-Trump, Head of Cyber Security for AmTrust International

The GDPR is both a challenge and an opportunity for the insurance industry. It has raised customer awareness for the protection of personal data. However, all insurance organizations do not use personal data in the same way or for the same purposes.

Insurance companies often need to process sensitive personal data to underwrite risks and provide claims handling and other insurance related services. Much of the personal data that insurers hold about individuals is sensitive in nature, particularly information about a person's health or medical treatment. These "special categories" of personal data cannot be processed unless the individual has given explicit consent to that processing, or in certain other limited circumstances, none of which readily apply to the insurance industry.

The GDPR and California's new law strengthens an individual's rights to access and protect their personal data. These include a right for the individual to request that their data be deleted (the right to erasure), a right to object to processing and the right to data portability – in electronic form. This means that a policyholder could request a copy of all data that their insurer holds about them in a commonly-used and machine readable format, so they can provide it to their new insurer. Also, individuals must be informed about any automated decision-making processes in the insurer's privacy notice. Individuals will also have the right to object to automated decision-making, meaning that the insurer must have a non-automated alternative.

Another impact of the GDPR on the insurance industry is how insurance companies and agents market their services. The GDPR introduced new restrictions on direct marketing for all businesses, including insurance. The most significant of these is that an "opt-out" mechanism, such as pre-ticketed boxes, are no longer a valid method of obtaining consent from individuals. Data subjects must provide their full consent to be included on any type of email marketing lists. In addition, new restrictions on electronic direct marketing are expected to be introduced later in the year, when the European Parliament passes the new ePrivacy Regulation.

A resident of the EU, data collected or processed outside of their home country must have protections compliant with the GDPR. Even insurers with no operations or presence in the EU are subject to the GDPR to the extent that they offer services to individuals located in the EU.

All insurance organizations do not use personal data in the same way or for the same purposes.

Insurers with no operations or presence in the EU are subject to the GDPR to the extent that they offer services to individuals located in the EU.

GDPR and Cyber Liability Insurance

Most general liability policies don't deal with cyber perils or are non-specific when it comes to damage from cyber-attacks. It's important to identify the level of risk an organization is faced with online and mitigate that risk accordingly.

Ian Thorton-Trump, Head of Cyber Security for AmTrust International

Every employer faces the reality that they may be the target of a network security or privacy breach. A cybersecurity or privacy breach can jeopardize credibility and cost small businesses thousands of dollars (or more) in damages. A data breach can impact an organization in many ways including: decline in customer service, lost client and proprietary data, business interruption, loss of reputation, etc. Plus, add in the costs of potential GDPR violation fines and the costs from a data breach could become an existential threat to continued business operations.

According to NetDiligence's Cyber Claims Study, the total cost of cyber and privacy-related claims topped $114 million in 2016. Personally identifiable information was the most reported data breach, with credit and payment card information being one of the most frequently stolen pieces of data. Maintaining cyber liability insurance will help keep companies operational after an attack.

The GDPR regulations spotlight the importance of privacy. This privacy extends to the systems which collect, store, process and transmit data. Cyber privacy can include both personally identifying information or non-identifying information which when aggregated can be used to identify - like a user's behavior on a website and cookie information.

The GDPR requires that an organization notify data protection regulators and affected individuals about any data breach which is likely to result in a privacy risk to affected individuals. Notification significantly increases the costs of responding to a data breach, as well as the chances that affected individuals will make claims against the controller. The GDPR empowers data subjects to seek restitution in the form of class action lawsuits.

An important component of the GDPR requires organizations to announce data breaches publically, within 72 hours of the internal knowledge of the breach. An example of this requirement was recently displayed by the disclosure of the Marriott-Starwood data breach of over 500 million guest records dating back to 2014. The data breach was discovered internally by Marriott in late November 2018. The company released information about the breach within 72 hours after the breach's discovery. It has yet to be determined if the company will also be given a large fine under the GDPR.

Cyber liability insurance augments and supports the business's efforts to recover in the event of a cyber-attack. It will provide access to expert resources and financial support through investigation, notification, recovery and post-recovery activates related to a data breach event.

An important component of the GDPR requires organizations to announce data breaches publically, within 72 hours of the internal knowledge of the breach.

Definition of Terms in GDPR

The GDPR has a variety of terms that might not be familiar to you, but they are important to know as data privacy laws continue to evolve in the U.S.

Personal Identifiable Information (PII)

The GDPR explicitly directs organizations to protect personal identifiable information (PII) of all "data subjects" of the European Union and United Kingdom. Personal data means information relating to an identified or identifiable natural person. A person can be identified from information such as an ID number, location data, online identifier (like an IP or MAC address) or other specific factors.

The protection of the PII data (and penalties associated with data breach of it) are rights held by the "data subject" and are enforceable inside and outside of the European Union and United Kingdom. The GDPR requires evidence of the protection measures a business has in place as PII data is collected, processed, stored or transmitted. The law also requires the specific consent of "data subjects" for a business to collect, process, store or transmit their data.

Data Subjects

The GDPR defines PII data as any information relating to a "data subject." A data subject is "an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The GDPR further defines the data subject as a resident of the European Union and United Kingdom. In some circumstances, such as a Canadian living in the European Union or United Kingdom, the protections of the GDPR would be extended to that data subject's PII information. Additionally, it's important to understand that the GDPR's protections extend the rights of European Union and United Kingdom residents outside the region.

Right to Access

Right to access gives the data subject indisputable rights (as in they can't be waived) to the PII data held by an enterprise. If a data subject requests access to their data, the law requires a response from the enterprise that includes all PII data for the subject. Additionally, the data must be transferred to the subject in an electronic format. Right to be forgotten, or right of erasure, allows data subjects to demand that enterprises delete their PII, stop transferring their data and even keep third parties from processing their data.

Data Portability

Data portability enforces the requirement for enterprises to provide the data subject with a copy of his or her data in a format that allows for easy use by another enterprise. When providing PII data, an enterprise must redact the PII of individuals other than the person requesting the data.

Consent

The GDPR requires that subjects give explicit consent for the collection, processing, storage and transmission of the PII data. Under the GDPR, consent must be freely given, specific and informed. Additionally, GDPR requires that a data subject reviews a statement and signifies via explicit action to their agreement to the collection, processing, storage or transmission of that subject's PII data.

Enforcement

When it comes to enforcement, each country has its own privacy and information office. These are collectively known as the GDPR Supervisory Authorities (SA), also known as Data Protection Authorities (DPA). These groups are "national authorities tasked with the protection of data and privacy, as well as with monitoring and enforcing the data protection regulations within the European Union and United Kingdom."

On the organizational level, the GDPR requires an enterprise, especially an international one, to designate a representative to be the point of contact for the country's SA. The position known as the Data Protection Officer (DPO), reviews an enterprise's operations to ensure they don't violate the GDPR. A key responsibility of the DPO is to conduct a Privacy Impact Assessment (PIA). During a PIA, the DPO oversees an analysis of the PII data held by an enterprise as well as their security policies, allowing them to reduce the overall risk of a PII breach.

Fines and Consequences

Violations of the GDPR requirements can come from many sources, from data subject complaints to large scale data breaches due to cybersecurity issues. Companies are just beginning to feel the wrath of consequences for violating the GDPR. Authorities can impose material fines up to €20,000,000 or 4 percent annual worldwide revenue, whichever is higher, for serious violations to the GDPR. Just recently, the CNIL, a French data protection watchdog, issued a $57 million fine to Google saying the company failed to comply with the GDPR when new Android users set up a new phone and during the phone onboarding process.

Key GDPR Actions

Organizations need to stay updated on changes to the EU law as well as the possibility of data privacy laws in the U.S. Businesses need to make sure they are prepared and protected when dealing with data privacy.

To summarize, businesses need to follow key GDPR actions:

- **Have a plan for GDPR Compliance**
- **Don't collect data you can't justify collecting**
- **The courts/regulator will decide**
- **Use a practical documented approach**
- **Your data, is your responsibility**

Protect Your Business

As mentioned earlier, cyber liability insurance provides a variety of services to address the modern day risks and threats of business identity theft and data breach. For more information about cyber liability coverage in the time of data privacy, contact AmTrust Financial Services or your AmTrust-appointed agent.

Sources:

https://gdpr-info.eu/

https://gdpr-info.eu/issues/fines-penalties/

https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

https://www.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html

https://amtrustfinancial.com/

https://amtrustfinancial.com/small-business-insurance/cyber-liability