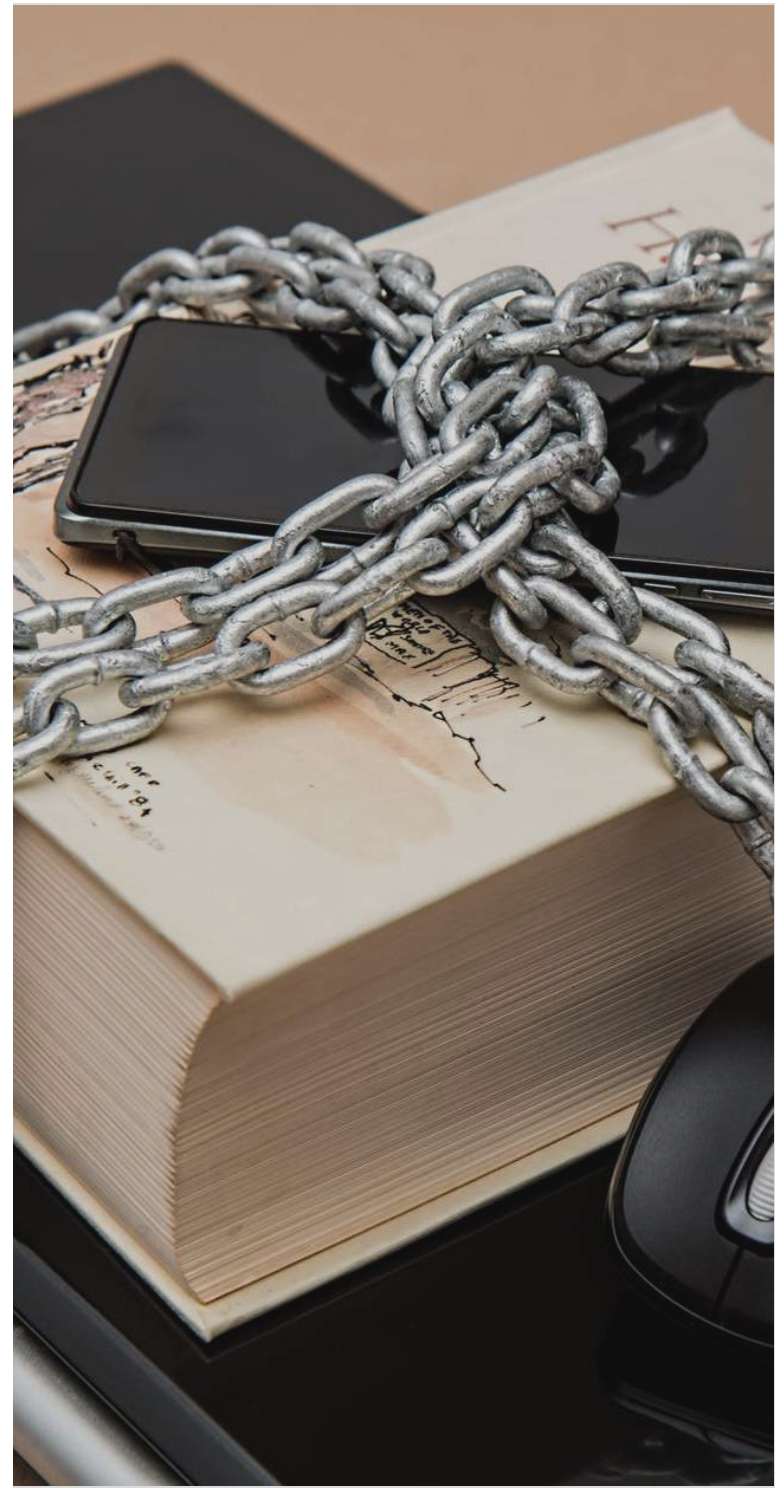
Third-Party Risk in Standards & Regulations

BLACK KITE

Executive Summary



In today's ever-changing environment, businesses rely on third-parties to help drive their core-activities. This dependence makes third parties, sometimes referred to as "suppliers" or "vendors", an organic part of business processes.

Recent breaches affecting Amca, CenturyLink, Capital One, Facebook, and Twitter all originated from a third-party website or platform supplier. These breaches cause thousands, and in some cases millions, of records to be exposed.

A recent survey conducted by the Ponemon Institute reveals that 59% of organizations have experienced one or more data breaches caused by a third party, costing an average of $7.5 million to remediate.

The cost of these breaches sometimes involve engaging forensic experts, hiring a law firm, offering victims identity protection services, as well as reputation damage and regulation fines, which in turn may add up to millions of dollars.

This financial burden could be devastating to small and medium businesses, putting some firms out of business. With record-breaking GDPR fines due to third party breaches, whether it is a part of the due-diligence process or a malicious third party script, it is time to take a closer look at regulations from a third-party perspective.

TABLE OF CONTENTS

Putting into Practice: Third Parties by Regulations & Standards

Although the term “third-parties” differs in each regulation, more or less the obligations remain the same. Whether it be “service providers”, “vendors” or “just another business I am selling consumer data” (as in CCPA), these third parties are potentially the weakest security link in a company's cyber ecosystem.

Here, we dig into the most prevalent security regulations to derive the business’ liabilities on a third-party scale.

NIST 800-53 and Cyber Security Framework

NIST 800-53 and Cyber Security Framework

NIST released two industry standards to drive security requirements around supply-chain (a.k.a third-party) management.

NIST 800-53

NIST 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" sets out guidelines and controls for protecting the government's sensitive information as well as citizens' personal information from information security and cyber attacks. It aims to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA). The controls (operational, technical, and management safeguards) and guidelines are evolving in accordance with changes in the information and cybersecurity landscape, as well as shifts in infrastructures and business models. However, the ultimate goal remains the same: To maintain the integrity, confidentiality, and security of federal information systems.

Currently draft publication is released for revision 5.
Some important changes in this revision are:

- Integrating privacy controls into the control set
- Scoping controls to be used by different interest groups such as systems, engineers, software developers, enterprise architects; and mission/business owners
- Integration with different risk management and cybersecurity approaches such as NIST Cyber Security Framework
- Incorporating new controls based on threat intelligence

How NIST views Third Parties

NIST views supply chain risk management as a critical organizational function. Organizational assets need to be protected throughout the system development life cycle. A standardized process needs to be addressed with respect to supply-chain risk of information systems and system components. Another important process is to educate the acquisition workforce on threats, risk, and required security controls.

Most of the supply-chain related controls are listed under System and Services Acquisition Policy and Procedures of NIST 800-53 and in particular SA-12 controls.

Organizations can leverage these controls to:

- reduce the likelihood of unauthorized modifications at each stage in the supply chain
- protect information systems and information-system components, prior to taking delivery of such systems/components

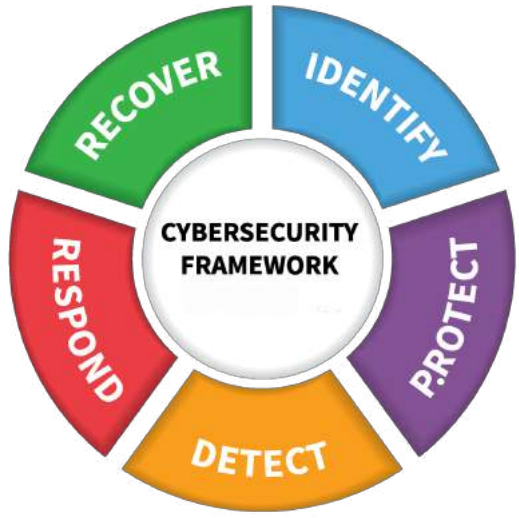
NIST Supply-Chain Risk Management in a Nutshell

1. Employ organization-defined tailored acquisition strategies, for the purchase of the information system and/or system component
2. Conduct a supplier review prior to entering into a contractual agreement
3. Employ security safeguards to limit harm from potential adversaries
4. Conduct an assessment of the information system, system component, or information system service prior to selection, acceptance, or update
5. Use open-source intelligence analysis (inc. OSINT) of suppliers and potential suppliers of the information system
6. Employ at least one: organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing

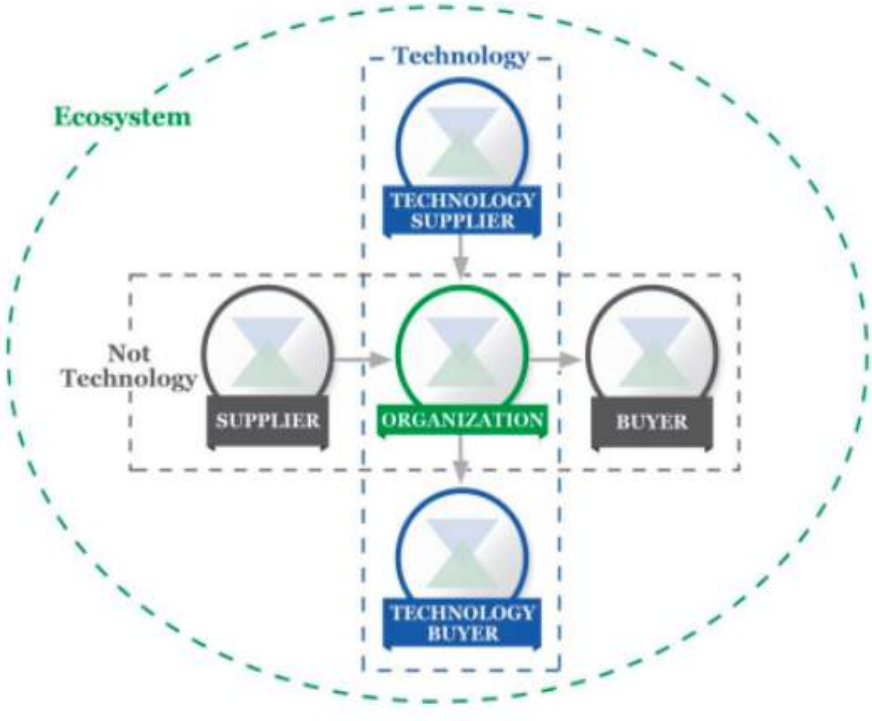
NIST CSF

In April 2018, NIST updated its cybersecurity framework, clarifying and enhancing some of its requirements. An important part of the update is on expanding the Cyber Supply Chain Risk Management process and the additional section, Buying Decision.

This framework can be seen as a common language aiming to improve "risk and cybersecurity communications", both internally and across stakeholders. It is an inclusive framework that can be used across many businesses and domains.



The framework simplifies cybersecurity functionalities within an organization by narrowing down to five functionalities; Identify, Protect, Detect, Respond and Recover, following similar steps to that of NIST SP 800-53. Section 3.3, Communicating Cybersecurity Requirements with Stakeholders, explains how to use the framework to manage supply chain risk. These are high-level abstractions in the management of the cyber-security programs.



Cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization. Organizations can communicate through the Current Profile or Target Profile to express cybersecurity state/requirements with their existing or prospective suppliers. Most of the supplier-related actions are contained in the Identify (Supply-Chain Risk Management) Functionality.

Things to Consider in NIST Supply-Chain Risk Management:

- Determining cybersecurity requirements for suppliers
- Enacting cybersecurity requirements through a formal agreement (e.g., contracts)
- Communicating to suppliers how those cybersecurity requirements will be verified and validated
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies
- Governing and managing the above activities

Click here to assess your suppliers'/third-parties' compliance as part of NIST supplier risk assessment!

Using NIST CSF and FAIR together

NIST has formally published FAIR (Factor Analysis of Information Risk) as an Informative Reference to the NIST CSF, in the sections covering risk analysis and risk management. Most of the time, there is a presumption that the maturity frameworks models are either the same as, or similar enough to a risk analysis model so that one could be chosen over the other. However, FAIR should be considered a complementary standard to frameworks in particular for conducting risk management efforts.

Both NIST CSF and FAIR fulfill different purposes. Organizations can focus their efforts on NIST CSF controls to increase cyber security posture. Which controls will increase the security most and effectively could be answered by FAIR.

Using FAIR and a quantitative risk analysis companies can understand how to prioritize NIST CSF's risk reduction activities based on a financial risk assessment. The relationship between FAIR and NIST CSF has been set for IDENTIFY (ID) > Risk Assessment (ID.RA) and IDENTIFY (ID) > Risk Management Strategy (ID.RM) elements of the "Identify" functionalities of NIST CSF in defining risk parameters, risk components and translating Quantitative Results into Qualitative Statements.

NIST CSF Elements		Relationship		FAIR Item
ID.RM	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Functional	superset of	C13G - 4.2.4 - Translating Quantitative Results into Qualitative Statements
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	Functional	superset of	C13G - 4.2.3 - Capacity and Tolerance for Loss
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	Functional	superset of	C13G - 4.2.4 - Translating Quantitative Results into Qualitative Statements

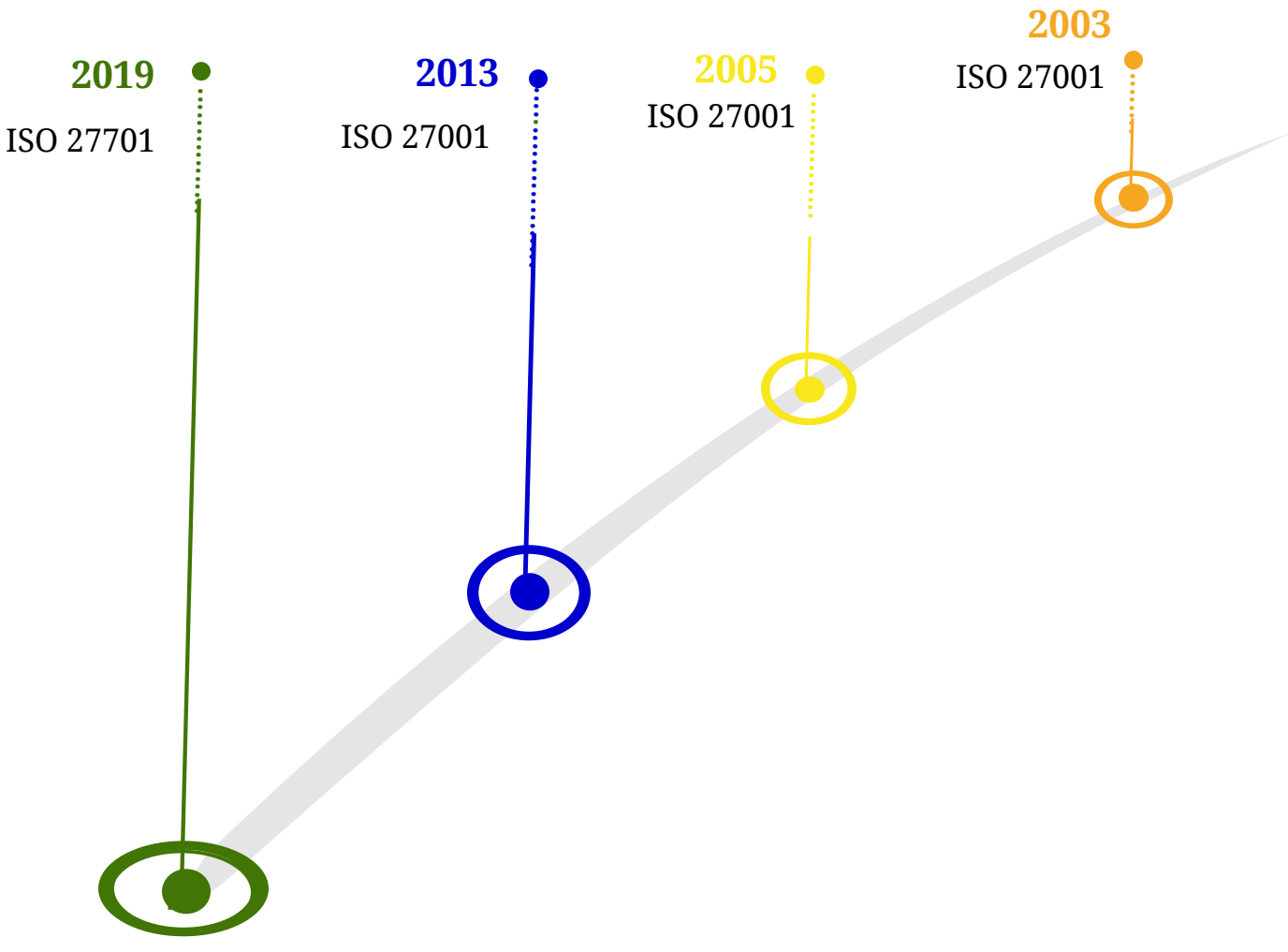
Relation between NIST CSF ID.RM and FAIR,
https://csrc.nist.gov/projects/cybersecurity-framework/informative-reference-catalog/details/4

ISO 27001
and
ISO 27701

ISO 27001

ISO/IEC 27001 (some only write ISO 27001) is an international standard created by ISO and IEC jointly to standardize information security best practices. The standard takes a risk-based approach in determining threats and risks to an organization, eventually leading to the selection of 114 controls in 14 different categories. Compliance to ISO 27001 standard provides benefits to an organization to better manage their IT systems with those control items.

Besides, organizations that meet ISO 27001 requirements can be certified after an audit. The standard was updated in 2017 with cosmetic changes.



Do third parties/ suppliers have to comply ISO 27001 standards?

Yes. ISO/IEC 27001, Section A15, has five measures (aka "controls") for Supplier Relationships. Based on these control items, third party compliance can be checked in 5 dimensions.

- Create an information security policy for supplier
- Agree on Infosec requirements for mitigating the risks associated with supplier's access to company assets
- Make the supplier sign a contractual agreement to ensure that there will not be any misconceptions in future (the organization can have "a right to audit", force "legal and regulatory requirements,", and oblige a supplier to " periodically deliver an independent report on controls", etc)

Use BLACK KITE reports to generate a supplier (third-party) security report

- Cover requirements addressing InfoSec risks associated with ICT services and product supply chain (i.e. propagation of security practices through supply-chain, if suppliers subcontract for parts of the products or services)
- Monitor and review supplier services to ensure the supplier adheres to the terms and conditions per the agreement
- Manage change to supplier services such as the update of information security policy, use of new technologies/tools, changes to a physical location, improvised services, etc.

How does BLACK KITE help your organization continuously monitor your suppliers?

ISO 27701

Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

ISO/IEC 27701:2019 is a privacy extension to ISO 27001, aiming to enhance ISMS with additional requirements regarding the protection of personal data. Both EU GDPR, and several other privacy laws coming into effect globally, ISO 27701 aims to elaborate on what these requirements should be on the technical and organizational level.

How does ISO 27701 map to GDPR?

GDPR foresees a certification mechanism in Article 42 for organizations to prove their compliance, although no such mechanism is currently in place. Certification ISO 27001 and to its privacy extension 27701, is a way to demonstrate compliance to stakeholders.

Supplier Relationships on ISO27701 Perpective

- Specify in agreements with suppliers whether personal information is shared
- Agree on minimum technical and organizational measures that the supplier needs to meet
- Consider each party and respective obligations including the customers, suppliers, suppliers' third-parties in the agreements
- Make sure agreements call for audited compliance (6.12.1.2)

General Data Regulation Protection

General Data Regulation Protection

GDPR came into effect as of May 2018, with an extended territorial scope and stricter fines. The fines are as high as 20 million Euros or 4% of annual global turnover, whichever is the higher. With this in mind, companies are scrutinizing their security measures.

Under the new rules, a company, independent of geographical location, is subject to GDPR, if it processes EU citizen's personal data. The definition of personal data is broad, however, this data could either be in the form of a simple name-surname, an e-mail, a payment data, or even a cookie data.

What does GDPR say about third-parties?

GDPR clearly states that all businesses and their third-parties are jointly responsible for protecting the user data. The third-parties come in two forms: either as a "joint-controller" or as a "data processor", each having different responsibilities vis a vis person a.k.a data subjects.

GDPR not only requires businesses themselves to implement GDPR-compliant technical and organizational measures, but also selects third-parties according to their level of security-compliance.

Check Your Third-Parties' Risks and Level of GDPR Compliance

It is an industry fact that businesses must conduct risk assessments a.k.a a Personal data Impact Assessment (PIA) to comply with GDPR. Often overlooked, third-parties are also recursively liable for this assessment. With a clear requirement in Article 28(1) saying “the controller shall use only processors providing sufficient guarantees to

implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this regulation and ensure the protection of the rights of the data subject." It is now the businesses' responsibility to check whether their third parties are providing sufficient guarantees.

The Relation between Fines and Third Parties

From May 2018 – March 2020, the Data Protection Authorities imposed a total of 231 fines and sanctions. With the addition of GDPR, the number of fines and costs associated has increased drastically. Although this spike demonstrates increased accountability, the total number of fines issued remains low in comparison to the 144,000 complaints submitted. As filed complaints and fines continue to pile up, it is not surprising the top-two fines are due to third-party related breaches.

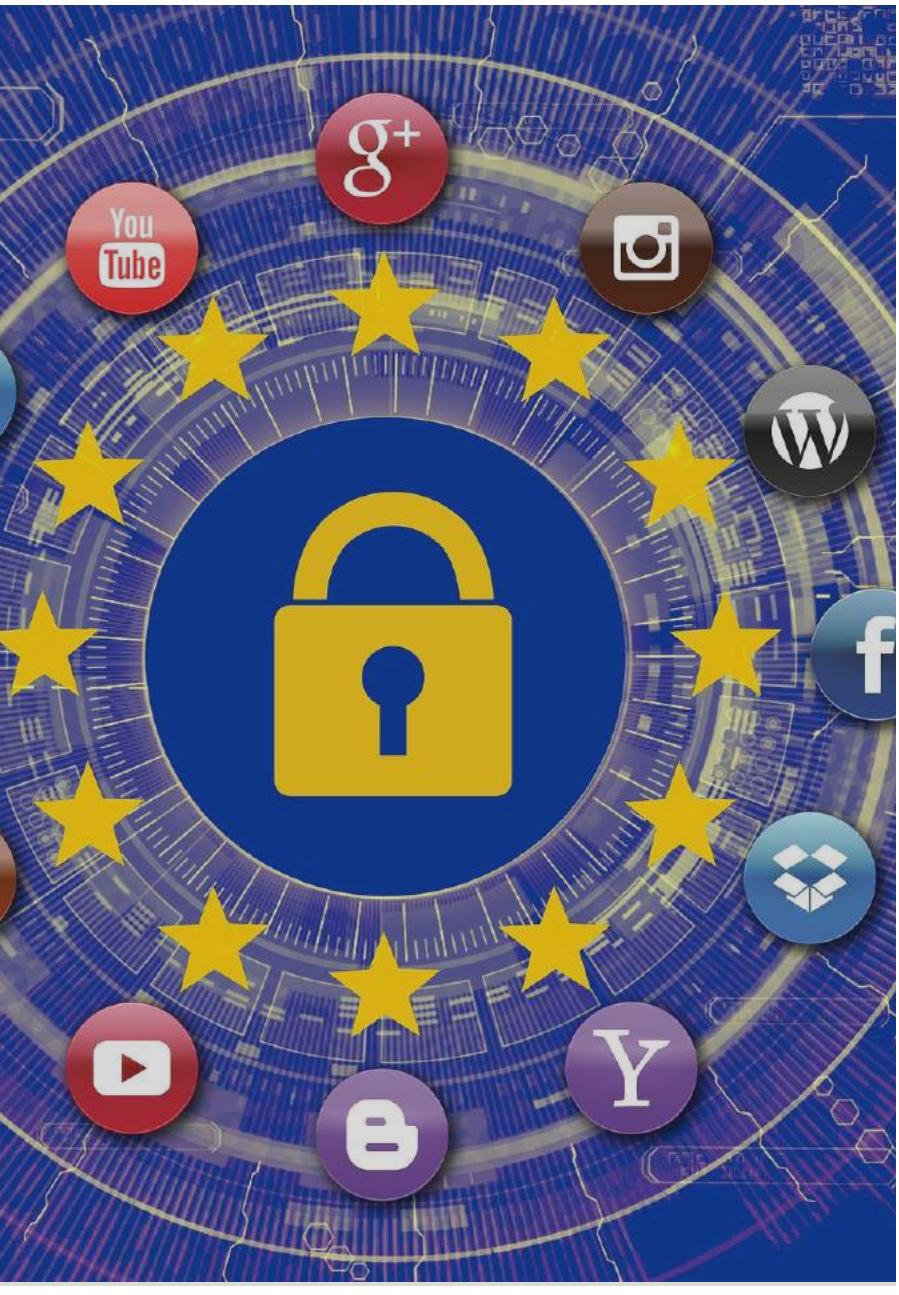
Company	Fine
British Airways	204,600,000 €
Marriott International	110,390,200 €
Google Inc	50,000,000 €
TIM	27,800,000 €
Austrian Post	18,000,000 €
Deutsche Wohnen SE	14,500,000 €
1&1 Telecom GmbH	27,800,000 €
Eni Gas e Luce	8,500,000 €
Google LLC	7,000,000 €
Eni Gas e Luce	3,000,000 €

Top Ten fines given under GDPR
https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

As the largest skimming community, Magecart hackers conducted the British-Airways data breach by leveraging a third-party library. The Magecart community used an unauthorized insertion of a third party JavaScript code. Through this fraudulent code, the attackers harvested details of approximately 500,000 customers.

A fine of £183.39 million ($230 million) was issued, and set a new record as the highest penalty to be issued from ICO under GDPR.

Holding second place in GDPR fines, the Marriott data breach became sensational the moment the hospitality giant announced the breach in November of 2018. Its Starwood guest reservations database was accessed in an unauthorized manner for four years, from 2014 until September of 2018. Around 383 million records - not guests- were involved in the incident, with multiple records associated.



Use Black Kite's FAIR Model to quantify your third-party personal data risk and leverage it in your decision-making process

Simple steps to meet third party GDPR compliance

- List all of your third-parties [you share personal data with] [either in the form of a "joint-controller" or "processor"]
- Revise terms of agreement /policies
- Restrict access to personal data on a need-to-know basis
- Run a third-party risk-assessment / (in GDPR called PIA)
- Keep records of third-party processing activities
- Make sure adherence to lawful basis or consent

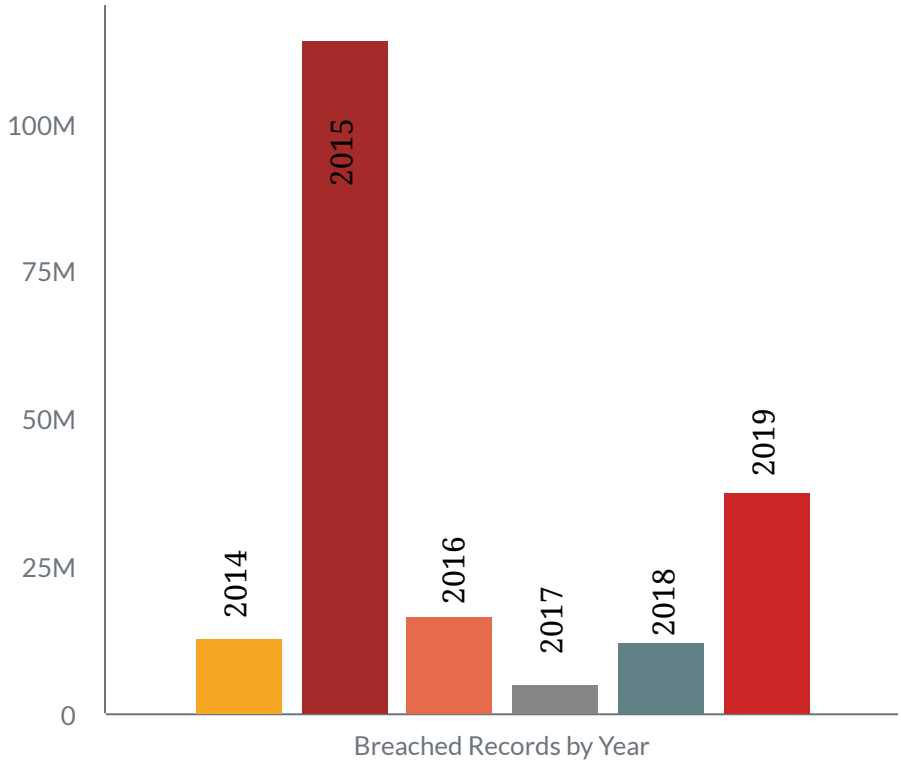
Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) aims to protect the health-related and personal information of individuals, including medical records, health insurance data, SSNs of patients, etc. This information is very valuable and profitable in the black market of the dark web.

No Good Year for HIPAA

2019 was not a good year for HIPAA with regard to breaches. 37.47% more records were breached in 2019 than 2018, increasing from 13,947,909 records in 2018 to 41,335,889 records in 2019. The Department of Health and Human Services' Office for Civil Rights (OCR) received 510 breach notifications, which compromised more than 500 records. This was a 196% increase from 2018. Third-party vendors and phishing attacks were behind most of these healthcare breach incidents.



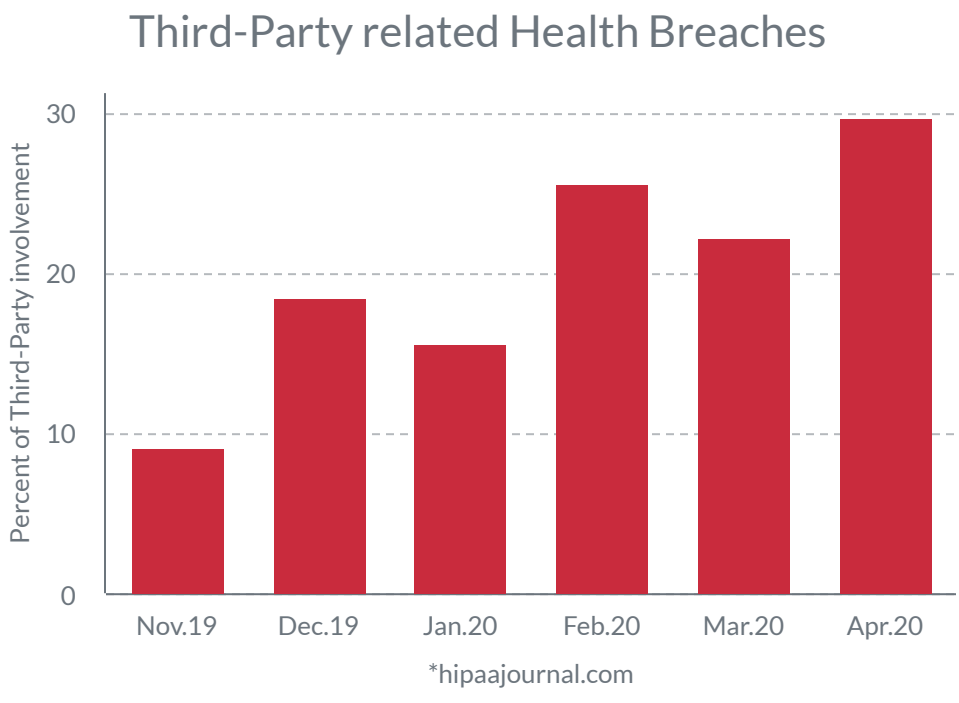
Breached Records by Year

* hipaajournal.com

Largest 2019 Data breach caused by a Third Party

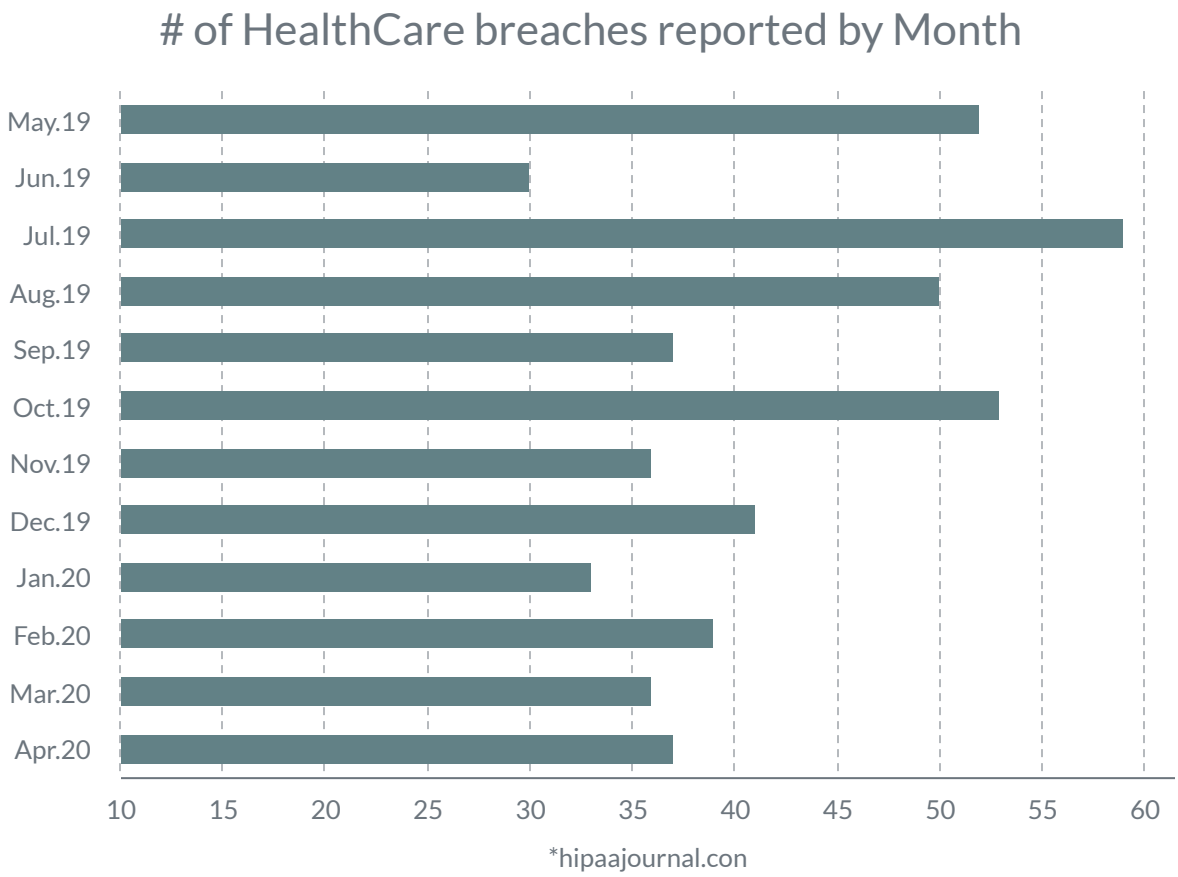
When we take a closer look at 2019 health data breaches, we see that third-party vendors working with healthcare providers account for about 23 percent of breaches.

When a third party a.k.a business associate experiences a data breach it does not always report the breach. Sometimes a breach is encountered by a third-party vendor and the healthcare entities working separately reveal the breaches, as was the case with the American Medical Collection Agency (AMCA), a collection agency used by several HIPAAs covered entities. Hackers gained access to AMCA systems in 2019 and stole sensitive customer/patient data.



The breach was the second-largest data breach in the healthcare sector ever documented, with only the 2015 data breach of Anthem Inc. impacting more people.

At least 24 organizations are known to have stolen data due to the hack. The breaches are ongoing as of April 2020, and 145 breaches have been reported to the OCR to date.



Third-Party Obligations Put into Practice

Under HIPAA, "covered entities" are individuals or entities transmitting protected health information for transactions for which the Health and Human Services Department has adopted standards. HIPAA Security Rule requires that covered entities are responsible for assessing the security readiness of their business associates. This includes the vendors and other third parties that are contracted with to receive, process, store or transmit PHI on behalf of the covered entity.

Ground rules for third-party management with HIPAA

- Business associates must enter into a HIPAA-compliant agreement with the covered entity before they are granted PHI, or access to systems containing PHI

- A covered entity can disclose protected health information (PHI) to a business associate under a written contract with certain assurances to comply with certain parts of the rule. This rule also applies to the subcontractor that business associates work with and has access to PHI data

- Business associates of covered entities must comply with the applicable requirements

- Business associates who fail to obey HIPAA rules may be directly liable for HIPAA penalties ranging from $114 to $57,0511 per infringement

Payment Card Industry Data Security Standard PCI-DSS

PCI-DSS

PCI-DSS is a Data Security Standard released by the Payment Card Industry (PCI) Security Standard Council to explain requirements and security assessment procedures of account data. The latest version (v 3.2.1) was released in May of 2018.

The standard is a baseline of security requirements for the protection of payment card data. It also includes validation procedures and guidance to help organizations understand the requirements.

The standard applies to the entire eco-system of the payment card industry including merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers to make cardholders safer.

Any breach of payment systems affects the entire payment ecosystem and consequences usually result in huge financial losses. Financial institutions that experience data breaches lose credibility and reliability.

Steps to prevent liabilities from third-party service providers

- Establish agreements with third parties. Agreements should be written clearly and should have references to PCI-DSS.
- Check PCI DSS requirements and determine which one of those should be met by the third party.
- Monitor the compliance of the third-party
- Prior to working with a third party, complete a risk assessment.

PCI DSS's Perspective on Third Parties

PCI DSS states that a service provider or a merchant may use a third-party for data storage, processing, or transmitting cardholder data or management of hardware/software components (routers, firewalls, databases, etc.). Third parties include Entities providing call center, E-commerce payment providers, E-commerce or mobile-application third parties, Managed firewall/router providers, Providers of maintenance services—for example, HVAC or cleaning.

However, PCI DSS acknowledges that if a third-party is used, then there may be an impact on cardholder data ecosystem security. Therefore, they offer two options to third-party services to validate compliance. Third parties can either:

- Undergo an annual PCI DSS assessments on their own and provide evidence of compliance

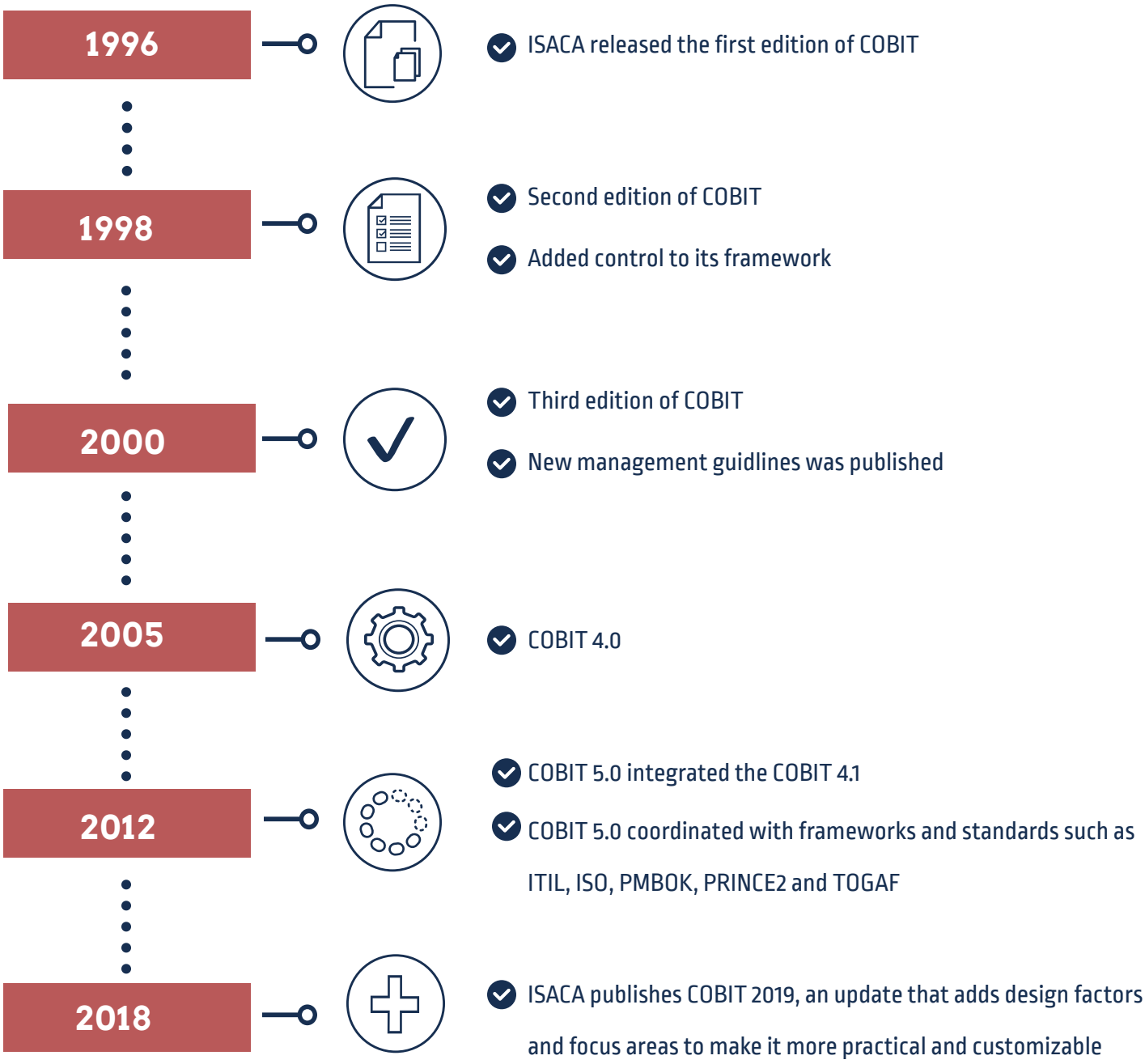
- Undergo assessments upon request of their customers and participate in their customer's PCI DSS reviews

Control Objectives for Information and Related Technologies
COBIT

COBIT

COBIT (Control Objectives for Information and Related Technologies) created by ISACA is an integrator framework many IT standards such as ISO 27001, COSO, ITIL, etc. It summarizes the key objectives of these guidance materials. Since the first version released in 1996, COBIT is well-accepted by an international material for enterprise IT management and governance with the framework, process descriptions, control objectives, management guidelines, and maturity models provided.

Since its release in 2012, COBIT 5 has become a good-practice framework for IT management and governance for enterprises. By following certain checkpoints in the framework, a company can create a good IT risk management process.



What COBIT's view on third-party risk?

One of the main sections in COBIT checkpoints is Delivery and Support (DS), where the second subsection (DS2) is all about how to manage third-party services. Here, third parties are defined as suppliers, vendors and partners. COBIT claims that control over the IT process of managing third parties can be achieved by:

- Identifying and categorizing supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

and is measured by:

- Number of user complaints due to contracted services
- Percent of major suppliers meeting clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring

COBIT explains how to manage third party relationships in DS section under four categories:

- Identification of all supplier relationships
- Supplier relationship management
- Supplier risk management
- Supplier performance monitoring

Steps to check COBIT-compliance

- Establish agreements with third parties (Agreements should be written clearly and should have references to COBIT)
- Check COBIT control points and determine which one of those should be met by the third party
- Monitor compliance of the third-party
- Prior to work with a third party, complete a risk assessment

California Consumer Privacy Act CCPA

CCPA

California Consumer Privacy Act (CCPA), signed into California State Law in June 2018 took effect as of January 2020. The bill aims to enhance the privacy rights of California residents in the U.S. According to this act, businesses are obliged to tell consumers what data it is collecting and gives consumers the right to say no to the sale of their personal information.

Consumer Rights in a Nutshell

CCPA gives several rights to the consumers. These include:

- Know what personal data is being collected about them
- Know whether their personal data is sold or disclosed and to whom
- Say no to the sale of personal data
- Access their personal data
- Request a business to delete any personal information about a consumer
- Not be discriminated against for their privacy choices

"Selling Data" Put into Practice: Third-Parties

According to CCPA, selling is, "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

This definition covers many more activities than selling data to another company for money. For example, a business collecting email info through its web site and making it available to third-parties is in the scope of selling data. This means relations need to be reviewed with third-parties according to the above definition (even if it does not involve a financial transaction).

How to become CCPA-Compliant when sharing data with Third Parties?

For businesses processing California residents' personal data and sharing with third parties, there are several steps to be compliant with CCPA.

- Train your employees
- Derive a data map
- Start listing all your service providers and third-parties.
    - Conduct a due diligence process
    - Identify which parties are decision-makers in agreements (e.g, analysis of whether the disclosure is a sale), etc..
- Provide privacy policy and notice
- Do not forget to include "Purpose of sharing data"
- Establish a process for consumers to request access, disclosure, deletion, or optout
- Post "Do Not Sell My Personal Information" link on the website

Shield Act of New York

SHIELD ACT OF NEW YORK

The Stop Hacks and Improve Electronic Data Security Act – which is known as the SHIELD Act – is an expansion of the New York state's existing data breach law. It aims to protect residents of New York for private information exposure due to data breaches. The law required companies to adopt cybersecurity programs and reduce risks of a data breaches by March 21, 2020. The act also required reporting of data breaches to the state attorney general as of Oct. 23 2019. If the disclosed data is health-related, then companies must take a step further and report the breach to federal authorities as well.

What kind of Information?

There are two kinds of information mentioned in the law:

- **Personal Info:** Any information regarding a natural person, for ex: name, number, other identifiers
- **Private information:** Specific information regarding a natural person such as a Social Security number, credit card number, and unencrypted biometric information.

Things to Consider on the Third-Party Dimension

There is a clear requirement in the Act saying that a business is compliant if it

“Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
(6) adjusts the security program in light of business changes”

The act also refers to continuous risk monitoring both internally and externally as per third-party.

What steps are needed to become SHIELD-Compliant?

The act comes with some criteria for compliance. Three types of safeguards, namely Administrative, Physical and Technical are defined in the law. The security requirements include:

- Training employees to coordinate cybersecurity program
- Working with SHIELD-compliant third-party service providers
- Performing cyber security risk assessment in various domains and processes including network, software design, information processing, transmission and storage
- Applying physical and procedural safeguards
- Monitoring the effectiveness of the cybersecurity program
- Updating the program periodically in response to need in business changes

Online Trust Alliance
OTA

OTA 2017

IoT Trust Framework, developed by Online Trust Alliance (OTA), sets out the principles for securing IoT devices used in homes (such as television, children toys), business, and health (e.g. fitness devices). The framework targets the whole lifecycle of an IoT device and its data, from manufacturing, to shipment and operation phase.

The framework provides some vertical and horizontal requirements regarding the device security and data privacy. The horizontal requirements include:

- comprehensive disclosures prior to product purchase
- data collection, usage and sharing policies
- terms and conditions of post warranty security patching
- the need to have security updates
- recommendations for manufacturers to enhance transparency and communication.

Vendors and Other Third-Party Service Providers

The framework sets clear requirements for vendor and other third-party relationships. As many products coming to market rely on third-party components and software, there is no way other than performing continuous supply chain security and privacy risk assessments for third-parties.

Steps to become OTA-Compliant in an ecosystem of Third-Parties are:

- Maintaining an inventory for any third-party/open source code and/or components.
- Maintaining a “bill of materials” for third-party software libraries, firmware, and hardware including device, mobile and cloud services
- Sticking to lawful basis or consumers’ affirmative consent when sharing personal data with third parties
- Ensuring that third-party service providers adhere to regulations and the same policies, and
- Conducting third-party security and privacy risk assessment program.

BLACK KITE'S COMPLIANCE CHECK

Regulations recommend monitoring third party vendors and conducting a risk assessment. A risk assessment can be done in an old-school questionnaire method. Unfortunately, some third parties are not completely honest in responding in the fear that the results will affect the relationship, questions might not cover all the risks, and the answers will be scoped with the third party's knowledge on the Information Security infrastructure.

Black Kite correlates cyber risk findings to industry standards and best practices. The classification allows a business to measure the compliance level of any company or a third party for different regulations and standards including NIST 800-53, NIST 800-171, NIST CSF, CIS CSC-20, ISO27001, PCI-DSS, HIPAA, COBIT, OTA GDPR, and Shared Assessments. Even prior to working with a third party, its compliance level to these regulations can easily be checked with Black Kite Cyber Risk Assessment.

HOW IT WORKS

Black Kite classifies the findings into NIST 800-53 Control Family, FIPS-200 Area, NIST 800-37 Process Step. The findings of the cyber risk assessment allow for the prediction of the compliance level of the target company in terms of different regulations including NIST 800-53, NIST 800-171, NIST CSF, ISO27001, PCI-DSS, OTA, HIPAA, and GDPR. The prediction is not a replacement of a regular compliance assessment, but it is a baseline to start working with. Black Kite's shared responsibility platform also allows users to update the compliance level of their organization after the estimated level. Finally, Black Kite has a unique cross-walking capability to calculate the compliance level of a standard based on the input given from another standard.

Say a company works with a number of different vendors, each bound to different regulations. All that company needs to do is to request an upload for the NIST 800-53 compliance report to our system. Black Kite's algorithm can then estimate the compliance level of other regulations such as PCI-DSS, HIPAA, COBIT, and GDPR, saving time both on the vendor and the company side.

FINANCIAL IMPACT OF NON-COMPLIANCE

It is a common dream for a company's compliance team to convey security and non-compliance concerns to the board-level in the right language. Although grade-based scoring together with benchmarking and trending performance means a lot for the technical teams, concerns and the level of severity might be "lost in translation" when expressing the results to management. The FAIR module acts as a powerful enabler for quantifying the risk sought in every regulation and standard.

Using an extensive database of sector-specific data, such as breached data, likelihood statistics, and previous regulation fines, allows companies to adjust the parameters and fine-tune possible financial loss.

About Black Kite

Black Kite (formerly known as NormShield) automates cyber risk results so you can make better business decisions. The average total cost of a data breach has risen to $3.92M Globally and $8.19M in the United States (IBM). Black Kite gives you the tools to make risk-based decisions with a high-quality data platform that does the work for you.

Black Kite correlates platform findings to industry standards and best practices. The cross-correlation capability measures the compliance level of a target company based on the standard input, saving time, and effort for both the company and vendor. The classification allows you to measure the compliance level of any company for different regulations and standards including NIST 800-53, NIST-CSF, NIST 800-171, CSC, ISO27001, PCI-DSS, HIPAA, GDPR, and Shared Assessments.

Learn more at www.blackkitetech.com