Fortanix®

WHITEPAPER

CISO Guide:

The Digital Transformation of Data Security

Prioritization of Data Security in the Cybersecurity Programs

According to Gartner, Cybersecurity budgets grew at 12% CAGR in 2018 but are projected to slow to only 7% growth by 2023[1]. Going forward, selecting the cybersecurity projects that deliver the highest risk reduction for the most impactful security incidents will be critical to the success of cybersecurity programs. Major trends including migration to public cloud, the expansion of Software as a Service (SaaS) application delivery, the increasing cost of data breaches, proliferating privacy regulations and the importance of data analytics all point to data security as an increasingly important part of cybersecurity programs, particularly relative to traditional spending on endpoint, perimeter and network-based security controls that are becoming less effective.

Data breaches are the best example illustrating why a data-centric approach to cybersecurity is required. When an organization suffers a data breach, it costs the average business in the United States $8.19 Million[2] with some breaches costing up $4 Billion (Epsilon)[3] . While there are many ways to prevent and mitigate data breaches, the single most effective factor decreasing the cost of a data breach is the extensive use of encryption[4].

Around the world, more than one hundred countries on six continents have implemented data privacy regulations. One of the first and most notable is General Data Protection Regulations (GDPR) in the European Union, which has already resulted in fines up to the $210 Million penalty for British Airways[5]. The California Consumer Privacy Act (CCPA) went into effect on January 1st, 2020 and carries stiff penalties for lost records of up to $750 per consumer per incident, which could amount to hundreds of millions of dollars for larger breaches. Data security technologies such as encryption and tokenization of Personally Identifiable Information (PII) are the most effective mechanism for avoiding these costly penalties.

> “This means that a data breach involving a million consumers, of which there have been many, could cost hundreds of millions of dollars in penalties per breach. However, there is an important caveat: fines cannot be levied if the data that has been disclosed, accessed, or stolen is encrypted or redacted. The fines only apply to nonencrypted information. With this encryption provision, it’s clear that encryption provides the best defense against any fines that might be levied for violations of data breaches under CCPA. Encrypted data that is stolen remains unintelligible, protecting the identity and personal information of its owner and mitigating risk for the business.”
>
> *— California Consumer Privacy Act (CCPA) Compliance Guide*
> *Enterprise Strategy Group*

ESG
Enterprise Strategy Group

GET THE REPORT

[1] https://www.gartner.com/document/3980890?ref=solrAll&refval=246543855

[2] 2019 Cost of a Data Breach Report Ponemon Institute

[3] https://www.eweek.com/security/epsilon-data-breach-to-cost-billions-in-worst-case-scenario

[4] 2019 Cost of a Data Breach Report Ponemon Institute, Page 39

[5] https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/

Leading the Digital Transformation of Data Security

> Information is the oil of the 21st century, and analytics is the combustion engine[6].
>
> *—Peter Sondergaard*
> *Senior Vice President and Global Head Research*
> *Gartner*

Across almost every industry, businesses are embarking on digital transformation initiatives to gain competitive advantage, improve customer experience, and increase profitability. In some cases, this means using technology to create a new business model, digitizing records, or leveraging artificial intelligence to improve products. Regardless of the industry, data is at the center of digital transformation and the ability to secure it is an integral part of digital transformation projects. Similarly, it is possible to apply a digital transformation approach to data security itself by using some of the same principles and strategies.

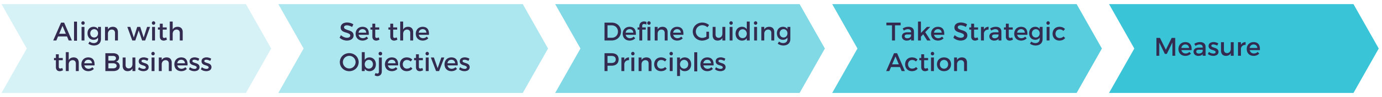
Data protection and data privacy are the cornerstones of trust between businesses and their clients. Encryption and managing the keys to the kingdom are critical components to maintaining that trust, preventing data breaches, and avoiding regulatory penalties. However, the technology used to manage encryption is often antiquated and based on twenty-year-old hardware security module (HSM) technology that doesn't interoperate well with public cloud or new APIs, slowing digital transformation.

FORRESTER®

> Justify your budget by your investments' impact on security maturity and value.
> The size of your budget says nothing about how well you spend those resources and whether
> your investments are lifting your security posture in a meaningful way.
> By assessing and measuring security maturity, S&R pros can better define and measure success.
> Prioritizing investments based on security maturity returns will focus your investment
> in the right areas and at the right level of investment required.
> Building your business case on value will also provide a more balanced
> approach than solely focusing on potential breach costs.
>
> *—The State of Data Security and Privacy, 2020, Forrester*

DOWNLOAD THE REPORT

Leading a Data Security Transformation



Align with the Business → Set the Objectives → Define Guiding Principles → Take Strategic Action → Measure

Align with the Business

The first step in a Digital Security Transformation is to identify business initiatives and align the data security program with those initiatives. It's often difficult for the information security organization and leadership to gain the trust of business leaders and gain support for strategic initiatives that are purely information security driven, particularly if it means changing behavior. The most effective method to break down the barriers and garner support for your data security program is to look for opportunities to align with existing strategic business initiatives already underway. Start by having conversations with the business leaders and understanding their business objectives, the security and regulatory challenges they face, and try to uncover ways that information security can help them move forward. As you learn more about the business, look for ways to use security technology to unlock new business opportunities that your colleagues might not be aware of. For example, the concept of privacy preserving analytics makes it possible to share confidential data with third-parties, apply machine learning models, and produce essential business insights without exposing that data to the other party or violating privacy regulations.

Set the Objectives

As with all business initiatives, the data security program needs measurable objectives to guide and motivate the team working to achieve the goals. It is important that the objectives be simple, measurable, and visible to both the information security team and business leadership. The fewer and simpler the objective, the more powerful it will be in driving behavior. Before setting the objectives you should perform a careful assessment of what outcome will reduce risk the most for your organization. This could be a process such as data classification or a security control such as implementing encryption. For data security, increasing the percentage of sensitive data encrypted from 50% to 100% is an example of a simple yet highly impactful objective that can be measured.

Define Guiding Principles

Once you have identified objectives, it is helpful to define and document guiding principles for your organization that will shape the implementation of your data security program. While the principles may vary by organization, there are certainly some that are being adopted widely by leading organizations. For example, the implementation of public cloud data security will be highly dependent on your cloud strategy and percentage of sensitive data or workloads running in public cloud. A tech company that is cloud-native and has standardized on a single public cloud provider will have very different guiding principles for a data security program than a financial institution with a small percentage of its total data in public cloud. In a recent Gartner survey of public cloud users, 81% of respondents said they are working with two or more cloud providers[7]. For a financial institution that is early in its journey to cloud and plans to operate in multiple public clouds, the guiding principles might include that data security should be agnostic to the cloud provider and support a multi-cloud architecture.

Take Strategic Action

When launching your data security initiative, it is critical to identify and execute strategic actions to start the process and build momentum for the program. Lay out the vision for your initiatives and then take bold and visible action that will move you towards achieving your objectives. Going back to our example of a Financial institution, their strategic action might be to create a data classification framework and determine the security controls required for each level of classification.

Measure

Creating metrics and measuring progress towards the set objectives is critical to sustaining a successful data security program. We discussed above an objective of increasing the percentage of sensitive data that is secured using encryption. So, let's say the objective is to encrypt 100% of data that is classified as sensitive, wherever it resides. First, you must build a data classification system to identify sensitive data. Then, you must have the ability to tag and monitor sensitive data. Finally, you must be able to implement an encryption security control that can secure the sensitive data and report on which data is encrypted. Then, you might want sub-metrics to measure the percentage of data encrypted in public cloud, SaaS applications, and on-premises separately to guide your implementation steps.

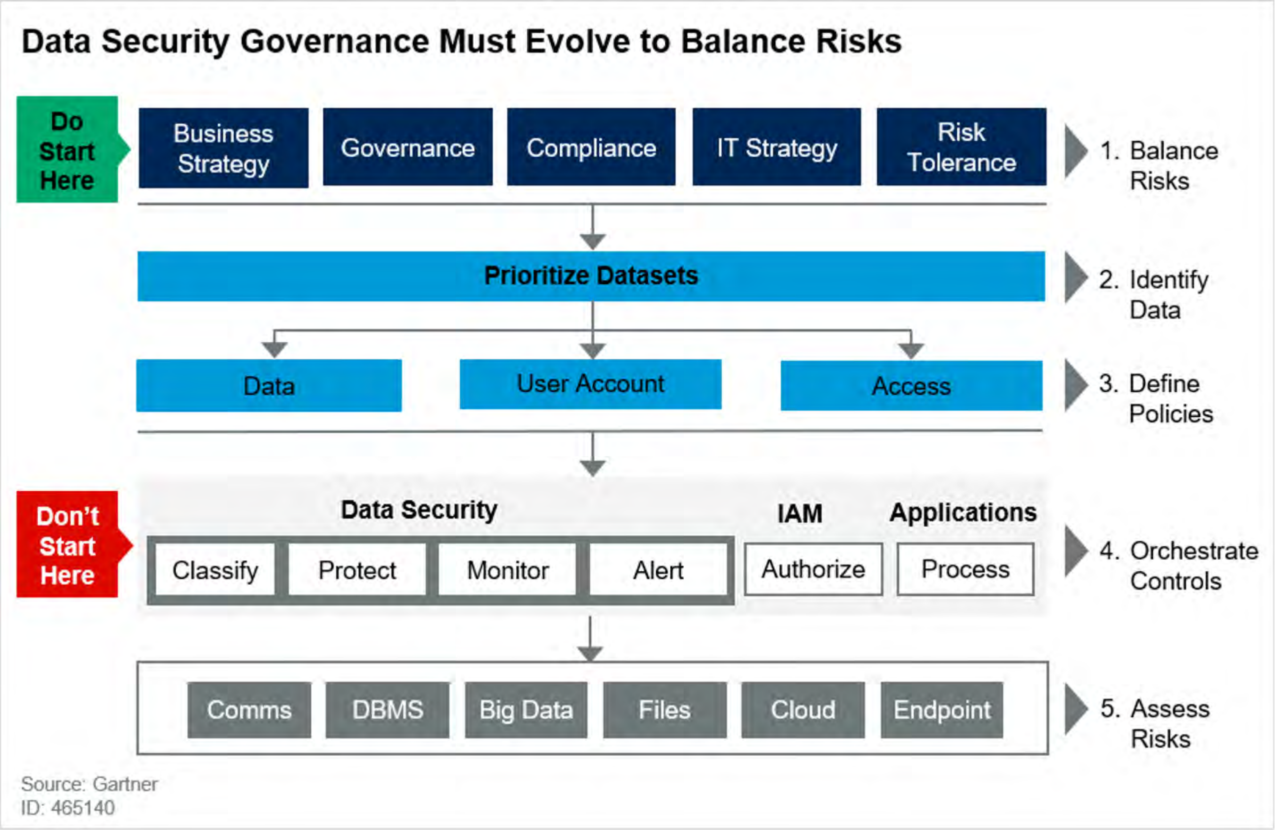
[7] https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy/

Implementing Your Data Security Program

> The opportunities to use data are growing exponentially, but so too are the business and financial risks. Security and risk management leaders should use the data security governance framework to mitigate business risks caused by security threats, data residency and privacy issues.
>
> *—Gartner ID G00465140*

Picking a Data Security Framework

When implementing a data security program, it is recommended to adopt or customize an existing framework to meet your needs. If you are a Gartner client, consider the "The Gartner Data Security Governance (DSG) Framework"[8]. One of the strengths of this framework is that it emphasizes starting with balancing business risk with the business value of data rather than starting from the security control mindset that is common in the information security industry. Gartner advocates starting by understanding your business strategy, the compliance constraints, the overall IT strategy and risk tolerance rather than jumping right into traditional security controls such as encryption or data loss prevention.



Data Security Governance Must Evolve to Balance Risks

Source: Gartner
ID: 465140

[8] https://www.gartner.com/en/documents/3978381

The National Institute of Standards and Technology (NIST) also provides an extensive cyber security framework for improving critical infrastructure that includes a data security program[9]. While broader than the Gartner DSG, the NIST framework does emphasize a risk assessment approach. In the most recent revision of the framework (1.1), supply chain relationships were added as a key risk to assess, a change which has many data security implications. The table below shows some of the categories and subcategories of the NIST framework that are relevant to data security programs.

Category	Subcategory
DATA SECURITY (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
	PR.DS-2: Data-in-transit is protected
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition **PR.DS-4:** Adequate capacity to ensure availability is maintained **PR.DS-5:** Protections against data leaks are implemented
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
	PR.DS-7: The development and testing environment(s) are separate from the production environment
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

Implementing the Framework

Whichever framework you select, performing a business risk assessment, identifying and prioritizing data assets, defining policy for data access, and implementing data security controls are common themes that are essential regardless of the framework.

Business Risk Assessment

> "Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for delivery of services achieving their organizational objectives and can express this as their risk tolerance."
>
> *—NIST Cybersecurity Policy Framework*

Reducing business risk should be the primary objective of data security programs. To reduce business risk, organizations first need to document the risks through an assessment process that identifies threats, then assigns a probability and estimates the impact of the risk occurring. Once all the known risks are documented they can be prioritized based on the combination of the probability of occurrence and the potential impact. Let's calculate the risk of a data breach as an example. When an organization suffers a data breach, it costs the average business in the United States $8.19 Million[10] with some breaches costing up to $4 Billion (Epsilon)[11]. The likelihood of experiencing a data breach has increased for each of the past five years and in 2019 was 14.8%. This means that the average business has a total risk of $1.21 Million per year ($8.19M x 14.8%).

[9] https://www.nist.gov/cyberframework

[10] 2019 Cost of a Data Breach Report Ponemon Institute

[11] https://www.eweek.com/security/epsilon-data-breach-to-cost-billions-in-worst-case-scenario

Another example would be the risk of financial penalties of data privacy regulations. First, you would identify all the data privacy regulations that apply to your organization and then calculate the risk of non-compliance. For businesses operating in California, the California Consumer Privacy Act (CCPA) went into effect on January 1st, 2020 and carries stiff penalties for lost records of up to $750 per consumer per incident – a potential penalty of hundreds of millions of dollars for larger breaches. There is a high probability of being fined that would be much more probable than a data breach. For this example, we will estimate a 30% probability of a regulatory penalty on an incident that impacts 100,000 customers. At a cost of $750 per consumer, that would be a financial risk of $2.25 million ($750 x 100,000 consumers X 30% Probability).

Data Classification

> “As business risks continue to evolve, Data Security Governance (DSG) provides a continuous reassessment and prioritization of risks. SRM leaders should engage closely with business stakeholders to address the size of the challenges faced, and that can start with a data discovery and mapping phase.”
>
> *—Gartner ID G00465140*

After completing a business risk assessment, it is important to classify data according to the business risk before determining policies and security controls to protect that data. This process starts with a data classification system similar to how the government would classify data as unclassified, sensitive but classified, confidential, secret, and top secret. The corporate equivalent often involves the four levels of public, internal, confidential, and restricted data. Then, business leaders assign all data to a level that will dictate policies and access controls implemented by the IT organization.

Policies and Data Access

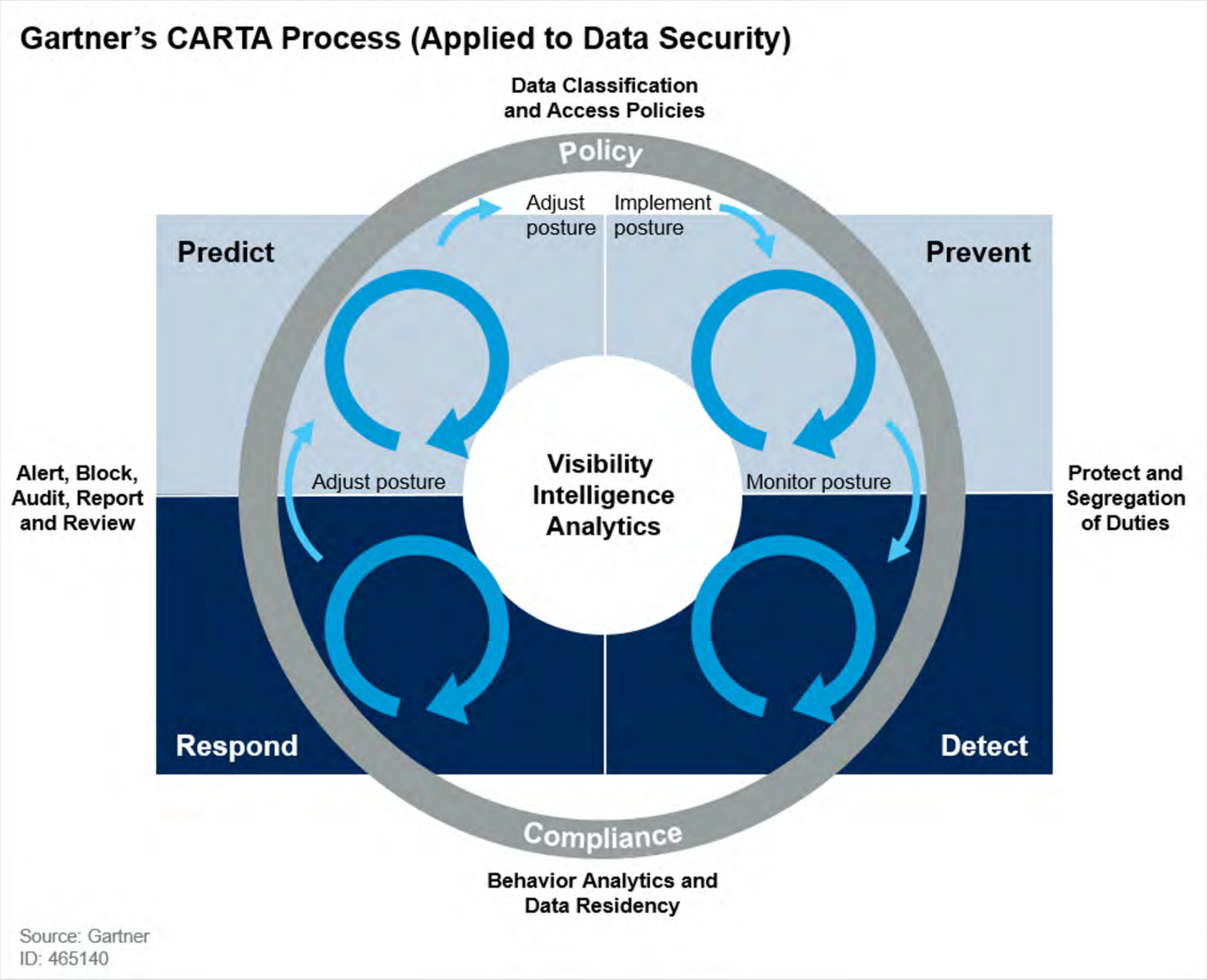
> “Create a companywide handling matrix for the different levels that are required. This is another area where clear communication is critical. The matrix format not only lets the reader quickly find the intersection of the situation and classification they are looking for, but also promotes a clear visual understanding of the differences in data treatment depending on classification.”
>
> *—Gartner ID G00344316*

The next step is to create policies for data access and use that builds on your data classification levels. You can use a matrix of policies by category as shown in the table below that defines how each classification category of data should be treated. For example, personally identifiable information (PII) for customers will likely be treated as “restricted” data that would need to be encrypted throughout the data lifecycle, labelled as PII, only accessible to the applications and users that require access and never transmitted outside the organization through email.

	Public	Internal	Confidential	Restricted
Storage Policies				
Labeling Policies				
Access Control				
...				

Implement Data Security Controls

> “In this context, CARTA can be used to select the data security controls as a cyclical process that should be applied to each dataset pervasively for its evaluated lifetime.”
>
> *—Gartner ID G00465140*


Gartner’s CARTA Process (Applied to Data Security)
Data Classification and Access Policies
Policy
Adjust posture
Implement posture
Predict
Prevent
Alert, Block, Audit, Report and Review
Adjust posture
Visibility Intelligence Analytics
Monitor posture
Protect and Segregation of Duties
Respond
Detect
Compliance
Behavior Analytics and Data Residency

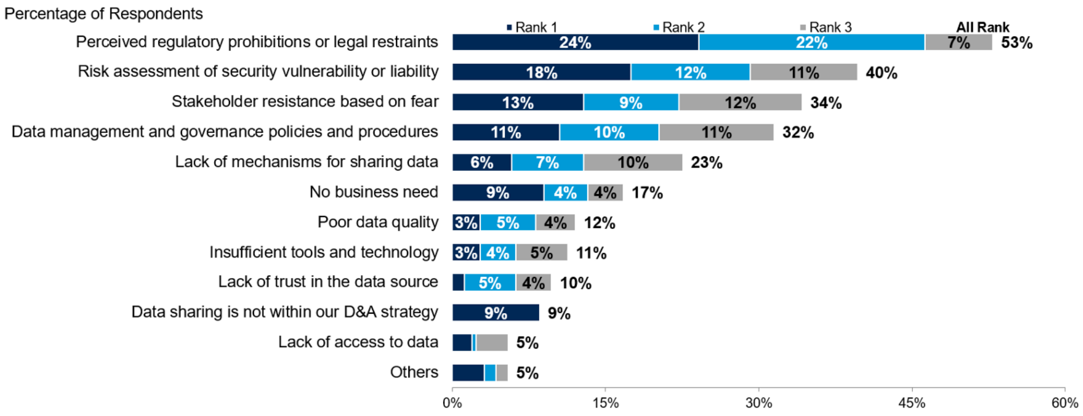
Source: Gartner
ID: 465140

While implementing security controls is where information security professional will feel most comfortable, make sure the controls you select are designed to minimize the business risks you identified earlier in the process and to secure the data that you prioritized for protection. Gartner uses a process called continuous adaptive risk and trust assessment (CARTA) to select the appropriate security controls. Those controls are broken down into technologies that prevent, detect, respond and predict threats. Going back to our personally identifiable information (PII) example, preventative security controls would include technologies such as encryption or tokenization of PII. Detection-based technologies might monitor for unauthorized access to the data or encryption keys. Responsive technologies might include automatically revoking an encryption key if a compromise was detected. Predictive technologies can analyze audit logs and risk assessment to identify gaps in controls or policies.

Unlocking Business Opportunities Through Data Security

> “By 2021, in 75% of large enterprises, the office of the CDO will be seen as a mission-critical function comparable to IT, business operations, HR and finance.”
>
> *—Gartner ID G00467120*

While most cybersecurity focus is on risk reduction, the CISO and information security leaders are playing more important roles in unlocking the business potential of data. With the emergence of the Chief Data Officer (CDO) role, there is an increasing focus on commercializing or monetizing business data, much of which is sensitive. The CISO and information security organization can become an enabling resource when implementing data analytics and sharing initiatives led by the CDO. According to Gartner’s Fifth Annual CDO survey in 2019, the biggest challenges in sharing data externally are privacy issues that can be solved by the information security team.

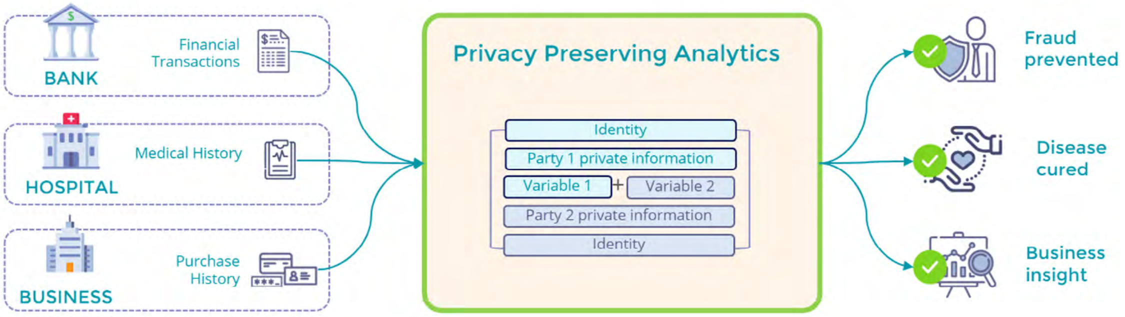


Most important challenges to sharing data externally

n = 257 Those sharing or exchanging data externally (Q12), excluding “unsure”
Q14B. What do you see as the top challenges to sharing or exchanging externally?
Source: Gartner’s Fifth Annual CDO Survey (2019)
Values less than 3% not shown

With the advent of big data, machine learning and analytics, the ability to share data has the potential to discover drugs that cure diseases, eliminate financial fraud, and unlock business insights that transform industries. However, organizations such as hospitals, financial institutions, and businesses are rightfully prohibited by privacy regulations from sharing this powerful data. Advances in encryption, trusted execution environments (TEEs) and analytics now make it possible to protect privacy while sharing private data, unlocking and advancing new learning.

Privacy preserving analytics can be applied to any case in which multiple parties have private data that needs to be combined and analyzed without exposing the underlying data or machine learning models to any of the other parties.



Conclusion

Businesses are re-inventing themselves through digital transformation initiatives. It is important for information security organization to undergo a similar transformation to become more strategic to the business. Major trends including migration to public cloud, the expansion of Software as a Service (SaaS) application delivery, the increasing cost of data breaches, proliferating privacy regulations, and the importance of data analytics require that data security be at the top of every CISOs priority list. CISOs should begin by leading a transformation of their data security program that puts in place a strategic approach to mitigating risk and aligning with business objectives. Then, information security organizations should implement data security controls designed to prevent, detect, respond to, and predict threats. As organization place a higher priority on monetizing data analytics and sharing, CISOs should look for opportunities to help CDOs remove regulatory, privacy and security obstacles using technologies such as privacy preserving analytics.

About Fortanix

Fortanix unlocks the power of organizations' most valuable data by securing it throughout its lifecycle, on premises and in the cloud. Fortanix provides unique deterministic security by encrypting applications and data everywhere – at rest, in motion, and in use with its Runtime Encryption® technology built upon Intel® SGX. Fortanix secures F100 customers worldwide and powers IBM Data Shield and Equinix SmartKey™ HSM-as-a-service. Fortanix is venture backed and headquartered in Mountain View, Calif.
For more information, see https://fortanix.com/.