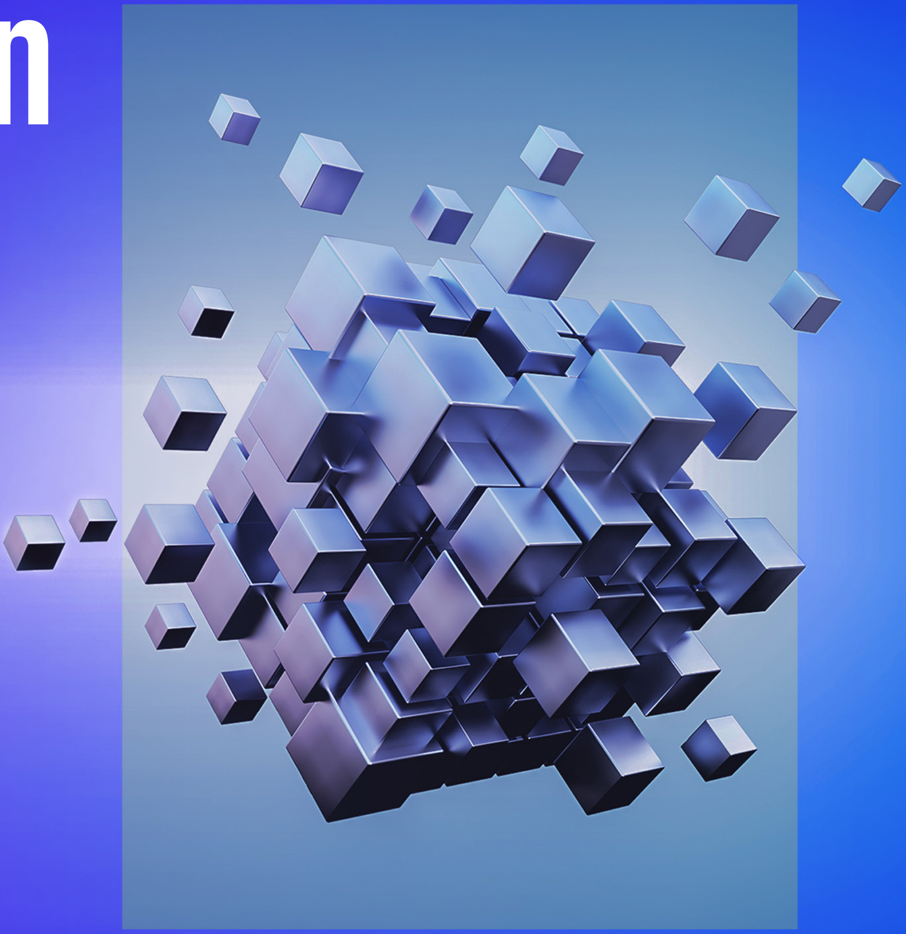
KPMG

Digital transformation accelerates the need for data protection



2023

kpmg.com

Contents

Introduction

Digital transformation leverages digital technology to improve businesses, enhance value, innovate, and develop capabilities to adapt to ever-changing circumstances. The need to remain competitive in this rapidly evolving environment has led organizations across the globe to embark on digital transformation journeys. This trend is heavily correlated with increasing amounts of data, on-premises and in the cloud, without adequate protections. The rapid transformation has opened many opportunities for attackers with malicious intent to gain unauthorized access or control of data, dramatically impacting digital transformation investments and brand value. Business leaders must ensure that they are embedding data protection into their digital transformation strategy.

Pitfalls of not having proper data protection strategies in place:

A data protection strategy sets forth an organization's goals, objectives, and approach to managing the personal and confidential data they capture, store, and process to run their business. The approach defined in the data protection strategy would include all the reasonable measures and actions to protect data in the organization. A data protection strategy aims to safeguard business-critical data, regulated data, and sensitive personal data. Organizations design their data protection strategies to prevent threat actors from gaining unauthorized access to data and preventing data misuse.

An organization's data protection strategy and approach will vary according to the industry, size, risk appetite, and nature of personal or sensitive data. Risk appetite plays a key role in defining the data protection strategy and controls that an organization should implement. A low-risk appetite would generally lead to having more and stricter controls in place to manage the data. Conversely, an organization with a high-risk appetite may choose not to expend efforts to design and implement a robust data protection strategy.

A failure to implement a data protection strategy often leads to the compromise of business-critical or sensitive personal information that the organization stores and processes. Failure to implement an adequate data protection strategy can lead to various tangible and intangible costs that can impact organizations across industries and sizes:

- The staggering costs of data breaches: The tangible cost of a data breach can be crippling to an organization. The average cost of a data breach in the U.S. in 2022 was $9.44 million. The average global total cost has increased by 12.7 percent in the last two years.[1] This cost is the highest it has ever been and is projected to continue rising. These costs include forensic investigations, notifying users, credit monitoring services, and fines.
- Legal repercussions: Failing to comply with data protection regulations can expose the organization to legal ramifications. The consequences could include

[1] IBM web site, Cost of a Data Breach, 2022.

financial penalties, compensation for damages, suspension of activities in the region, additional audits, legal actions, and imprisonment depending upon violation.

- Diminished brand value and loss of customers: Trust, whether from consumers or investors, is a key factor that keeps an organization running—40 percent of the U.S. general population say they don't trust companies to do the right thing and 13 percent don't even trust their employer.[2] A data breach or other loss of essential assets would likely have a negative impact on the value and confidence of a brand. The aftermath of a data breach may cause an organization to experience a decline in its reputation and a loss in revenue.
- Disruption of service: A cybersecurity attack on an organization's systems and data may also interrupt business operations. Depending on the severity of the attack, the investigation process can take up to a few months. In May 2017, the WannaCry ransomware attack served as a wake-up call to the devastating impacts of cyberattacks. Over 230,000 computers were infected by the worm across 150 countries in a single day. The resulting damage and cleanup costs were estimated at around $4 billion.[3] In April 2020, a ransomware attack impacted a large technology service provider's infrastructure supporting work from home. The organization lost roughly $50 million to $70 million in revenue for the quarter.[4]

It is important to remember that designing a good data protection strategy itself is not sufficient to prevent data breaches. The key lies in the execution of the strategy. Execution involves implementing the defined measures, putting in place methods to track the success of this implementation, and periodically evaluating the standards and controls.

[2] Lucas, Orson, et al., "Corporate data responsibility: Bridging the consumer gap," KPMG LLP, August 2021

[3] Latto, Nica, "What is Wannacry?," Avast, July 21, 2022

[4] "Cognizant Anticipates $50-70 Million Loss Following Ransomware Attack," Security Magazine, May 11, 2020

Evolving data protection landscape in the recent years

Today, organizations are modernizing their systems and processes with the use of technology. Digitization supports organizations to replace legacy processes, accelerate efficient workflows, enhance data collection, unlock business and customer insights, and increase profitability. Customers are helping drive organizations towards digital transformation with their desire for digital convenience, high-quality user experience, and virtual service requests.

The global banking industry has pivoted towards online and mobile banking service options to enhance product availability and user experience. Cash usage has been replaced with digital wallets. The use of chatbots and interactive voice response has become popular in insurance and government agencies to reduce customer wait times to address their complaints and concerns. Law enforcement and security guard services are enhancing their patrolling with high-tech products like 3D cameras and facial-recognition-based software for improved security. These innovations lead to the generation and collection of massive quantities of sensitive and critical data every second. This large data footprint has created a much larger attack surface for hackers to target internet-based systems and platforms.

There is an urgent need for organizations to proactively protect the confidentiality, integrity, and availability of their data. A strong data protection program enhances overall data security, safeguards organizational resources, and helps with recovery efforts. Proper data protection practices can reduce the devastating damage from data breaches and other cyberattacks.

The global pandemic has caused businesses to reconsider their strategy, vision, and operations. Organizations have rapidly adjusted to remote work patterns and sped up their digital transformation journeys to preserve business continuity. These changes, ranging from smaller projects to large technology transformations, resulted in numerous data protection challenges. Organizations faced issues like zoom-bombing, unauthorized social media usage, accessing company cloud storage on personal devices, or even unmanaged personal devices on the company network. The pandemic helped to advance digital transformation journeys, but data protection was not a consideration during the rapid transformation.

As organizations today adopt cloud-based services and undergo technological transformations such as the Internet of Things and robotic process automation, it becomes imperative to have proper data protection controls. Identity and access management (IAM) plays a crucial role in securing data in the cloud and from operational technologies. The increase in data breaches has emphasized the need for mature IAM programs as organizations upgrade to hybrid multicloud systems and start to leverage "Zero Trust" strategies. Organizations often lack proper knowledge of adapting to the paradigm shift and how to align their digital transformation journey and data protection strategy to a hybrid work environment.

Six steps to protect data

Organizations must implement sufficient data protection controls to ensure their data remains secure. Leading practices include securing confidential data using multifactor authentication, limiting access based on business needs combined with having defined access policies, enabling event logging, possessing native backup and restore capabilities, and properly implementing data encryption throughout the organization data-at-rest and in-transit. To protect sensitive data while still reinforcing collaboration and productivity, organizations should consider the following "Quick Wins":

01 Reshape and reorganize the operating model:

Updating an operating model calls for a holistic approach regarding people, processes, and technology. Arrange and classify the data by functions, tasks, and risks. It requires, in part, optimizing core processes with a focus on key data protection objectives and strategically integrating data protection technology solutions at an overall level into the updated operating models.

02 Integrate Virtual Desktop Infrastructure (VDI):

VDI primarily enables users to log in without exposing organizational data to the user's device itself. This feature helps reduce data loss and helps minimize the risk of an unpatched or out-of-date device. VDIs are managed and updated centrally by the organization rather than relying upon end users and endpoint monitoring agents to keep their devices up-to-date and properly configured. Secure data access has become increasingly important as users gain access to organizational resources from private networks.

03 Protect data using data-oriented tools:

Utilize advanced technologies such as data discovery, data classification, and data loss prevention (DLP) to find and prevent data from being shared outside the organization. DLP tools are frequently considered stand-alone products, but many solutions you already own likely have DLP features organizations can leverage.

04 Conduct audits and stress tests at regular intervals

Periodic reviews and audits of your organization's data protection procedures and capabilities are essential. Technology is rapidly changing, and new threats are constantly emerging. It's critical to review and update current implementations to compare them with new technologies and safeguards that have been developed.

05 Leverage built-in security controls

The culture of security by design has helped software companies to embed security measures across their products. Evaluate what features exist across existing toolsets that can be leveraged to protect your data. Often, built-in security features can work better than separate solutions as these features are fully integrated into the product. Organizations should take inventory of existing solutions before exploring additional software solutions.

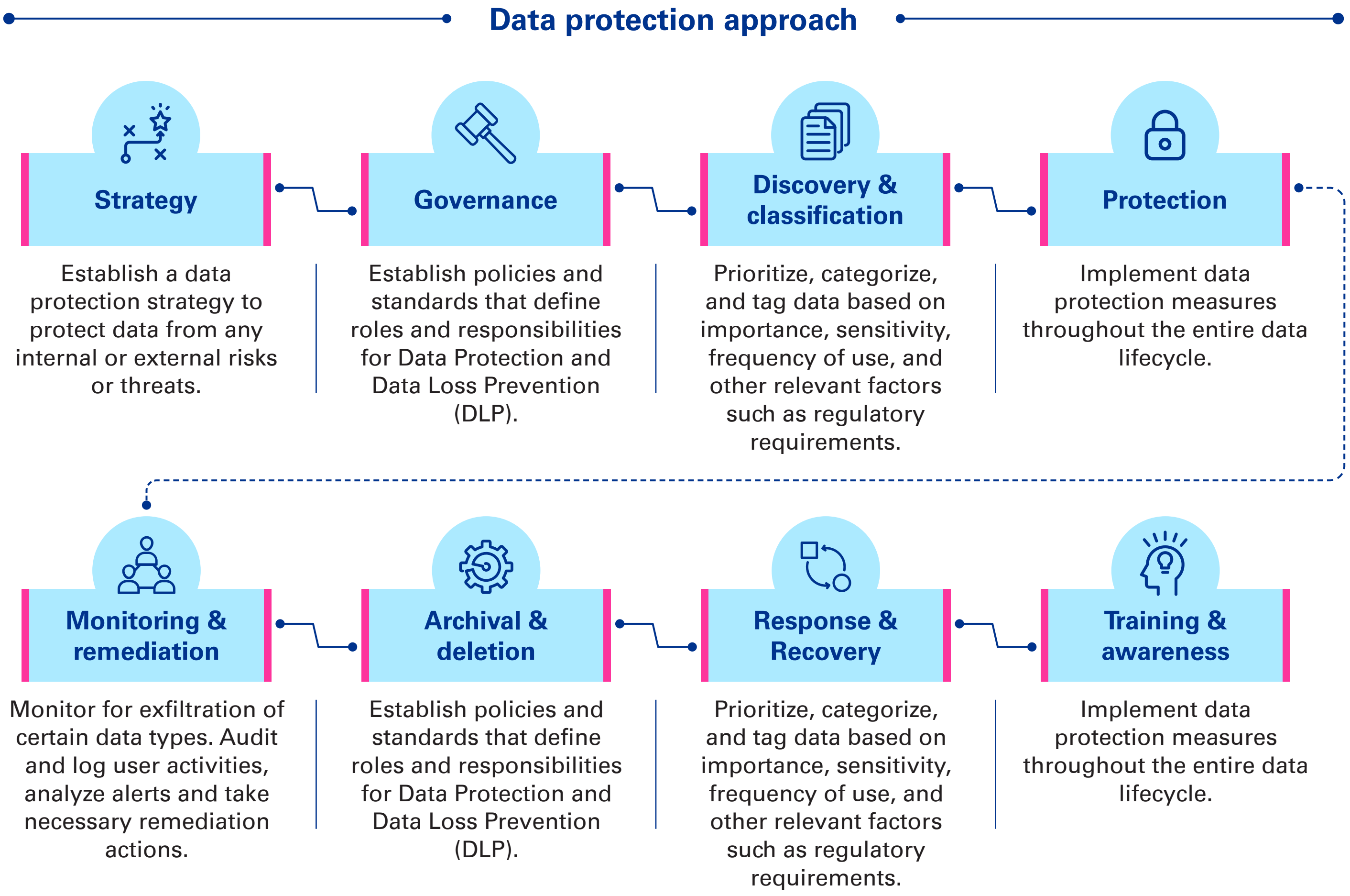
06 Incorporate separation of duties

Foster collaboration between system owners and the IAM team to ensure existing and future user roles incorporate separation of duties. Review job responsibilities to ensure one user cannot access multiple components within critical business processes. This can help protect business processes susceptible to misuse, abuse, or fraud.

Strengthen your data protection program

As you proceed with your digital transformation journey, your organization must integrate data protection throughout the process. Both your digital transformation and data protection journeys should be aligned with your organization's risk tolerance.

Enhancing your data protection program is often easier said than done, and organizations struggle to get started or take on too much at once. The KPMG data protection framework is a thorough solution to support the development, assessment, and enhancement of your data protection program to reduce the risk of data loss and ensure ongoing compliance with data protection legislation. The framework provides an in-depth, holistic, and cross-functional review of an organization's ability to protect its information assets. The eight high-level domains of the KPMG data protection approach are outlined below:



Data protection approach

Strategy

Establish a data protection strategy to protect data from any internal or external risks or threats.

Governance

Establish policies and standards that define roles and responsibilities for Data Protection and Data Loss Prevention (DLP).

Discovery & classification

Prioritize, categorize, and tag data based on importance, sensitivity, frequency of use, and other relevant factors such as regulatory requirements.

Protection

Implement data protection measures throughout the entire data lifecycle.

Monitoring & remediation

Monitor for exfiltration of certain data types. Audit and log user activities, analyze alerts and take necessary remediation actions.

Archival & deletion

Establish policies and standards that define roles and responsibilities for Data Protection and Data Loss Prevention (DLP).

Response & Recovery

Prioritize, categorize, and tag data based on importance, sensitivity, frequency of use, and other relevant factors such as regulatory requirements.

Training & awareness

Implement data protection measures throughout the entire data lifecycle.

Digital transformation is reshaping our lives, from the proliferation of data being created to increased data processing to gain business insights, employees working from remote locations, migration of data to the cloud, and the rapid adoption of the Internet of Things. Organizations are presented with various digital transformation opportunities, but these opportunities also come with challenges. As companies continue to undergo digital transformation, their attacks surface and data exposure increases, further highlighting the need for data protection. The legacy approach towards data protection may not meet the data protection needs of a modern organization.

How KPMG can help you

KPMG has closely worked with many high-end clients from all over the world throughout their digital transformation and data protection journey. Together, we have achieved remarkable success. We offer a complete range of data protection capabilities, including data discovery, classification, and DLP implementations. We provide a broad spectrum of services—including strategy, design, wide-ranging execution, and delivery—to assist you in your digital transformation. Furthermore, we work with various software tools, giving us distinct insights into what data protection capabilities they possess, how they bridge various gaps, and what systems are appropriate for an organization's use cases.

KPMG can assist you in protecting your most sensitive data regardless of your organization's maturity level, whether you are just beginning to digitize records, move data and services to the cloud, or are far along in your digital transformation journey. We can help you align your data protection strategy with your business needs and organizational risk tolerance by conducting impact assessments, establishing target operating models, creating transformation road maps, and developing business cases to highlight potential advantages.

Contact us

For more information on establishing or enhancing your data protection posture, whether your technologies are on-premises, in the cloud, or both, please go to our website or contact one of our professionals below:

Michael D. Gomez
Principal, Advisory
Cyber Security Services
T: 202-999-9383
E: michaelgomez@kpmg.com

Venoth Lal
Director, Advisory
Cyber Security Services
T: 214-840-4297
E: venothlal@kpmg.com

Elizabeth C. McConnell
Senior Associate, Advisory
Cyber Security Services
T: 404-222-7227
E: elizabethmcconnell@kpmg.com

Oindrila Mazumdar
Associate Manager, Advisory
Cyber & Governance
KPMG in India
T: 898-139-2089
E: oindrilam@kpmg.com

Orson B Lucas
Principal, Advisory
Cyber Security Services
T: 813-301-2025
E: olucas@kpmg.com

Andrew Ludwiczak
Manager, Advisory
Cyber Security Services
T: 415-361-0795
E: aludwiczak@kpmg.com

Pallavi Malap
Manager, Advisory
Cyber & Governance
KPMG in India
T: 823-714-9892
E: pallavisunilm@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.