White paper:

The double edge sword: Data protection and data enablement in the age of “everything online”.

Occamlabs.com

Occam Labs

02

INTRODUCTION

Organizations today accumulate enormous amounts of complex information from an increasing number of sources.

Data is one of the most valuable assets an organization has, created, compiled, collected, stored and disseminated in everything from day-to-day operations to regulatory compliance.

The amount of data that organizations collect and process is exponentially growing. IDC Research predicted that the volume of digital data will expand at a compound annual growth rate of 42% over the decade of 2010 to 2020.

With so much data in circulation there is always a risk of a data leak or breach, exposing confidential information to unauthorized parties.

The reasons for how data breaches happen might sometimes be traced back to intentional attacks against a weak security perimeter. However, it can just as easily result from human error, flaws in a company's nformation infrastructure or a scope creep in business intelligence.

03

According to Risk Based Security, the first six months of 2019 saw more than 3,800 publicly disclosed breaches exposing 4.1 billion compromised records, with one of the biggest data breaches so far in 2020 from Marriott hotels that potentially affected over 5 million customers.

Adopting a data-centric approach means organizations see data as a vital component in their interaction with customers and other key stake-holders. It is critical to competing in what today is a data-driven economy.

However, as the amount of accessible data rapidly increases, organizations have been forced to address the regulatory and operational demands that come with the circulation of personal customer,employee and partner data both inside and outside of their organizations.

As companies grow, staying compliant in a world of evolving privacy regulations adds new layers of complexity to doing business. Extracting value from the data collected whilst ensuring security and regulatory compliance are a challenge for an organization of any size.

04

An effective data governance strategy forms the foundation of an organization’s approach to protecting the privacy of personal data under the General Data Protection Regulation (GDPR), the recent data privacy law released by the European Union.

The GDPR, or General Data Protection Regulation, came into force in May 2018, and represents a comprehensive regime for the regulation of data privacy and the flow of personal information. The requirements apply to personal data of any individual EU resident that is used by any person, group, company or government agency located anywhere in the world.

What is GDPR?

GDPR applies to almost every type of personal information about an individual, including their name, address, bank details, social networking content, medical information and computer IP address.

The GDPR strengthens existing rights and provides for rights for individuals who are in the EU to control thecollection, storage, processing and use of their personal data.

It lays out specific requirements for organizations that control and process such data, which fall under the umbrella of data governance. For example, GDPR requires all organizations to report a data breach to the ICO within 72 hours and notify affected customers without undue delay.

There are severe financial penalties to those companies that do not comply with these regulations. The largest fine to date under the GDPR was $57 million for Google.

With the emergence of stricter regulations regarding consumer privacy and data rights, companies have to be more diligent about managing data.

€55,955,871

Fines paid by companies in the European Economic Area for GDPR non-compliance in 1 year European Data Protection Board, 2019

Consumers, employees and partners v. data leaks - why is it hard to do it right?

Despite the implementation of the GDPR and high-profile data breaches serving as a reminder of what is at stake, many organizations still need to do more to enhance their privacy and data governance.

Data breaches and other considerations of data privacy have become a common occurrence in today's digital reality.

Small businesses in the UK are the target of an estimated 65,000 attempted cyber-attacks every day, according to figures from a study from Hiscox a specialist insurer.

According to Hiscox, almost one in three (30%) UK small businesses suffered a cyber breach – equivalent to over 4,500 successful attacks per day or one every 19 seconds.

Indirect costs such as damage to reputation, the impact of losing customers and difficulty attracting future customers, remains unmeasured but is expected to have a significant impact.

Massive cybersecurity breaches have become almost commonplace from Facebook to British Airways, all regularly grabbing national headlines.

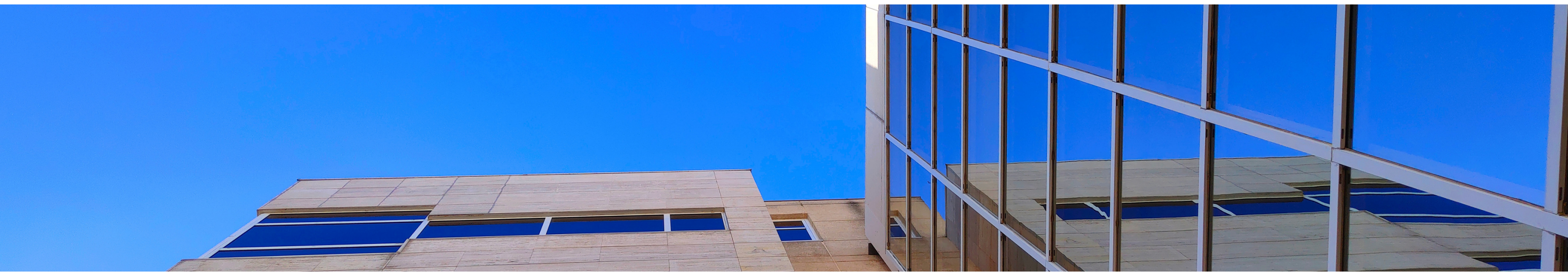
But, for all of the attention generated by these incidents, many organizations still struggle to comprehend the regulatory and compliance risks of a data leak and fail to prepare adequately.

Most alarming of all, is that the majority (56%) of those who've suffered a breach, are the victim of multiple leaks,
as a result of changing processes and technology too slowly or not at all.

According to Accenture's 2019 Cost of Cybercrime Study, "Humans are still the weakest link'', as human error is often at fault for exposing sensitive information or undermining internal security practices.

Governance frameworks and teams must work hard on empowering data driven decisions while making sure the right balance is struck, and limiting the risk of employees having access to too much data.

At a time when cyber criminals are adapting their attack methods.
They are targeting the human factor through increased ransomware, phishing and social engineering attacks to gain entry.



What is Data Governance?

An organization needs a secure data pipeline that enables them to retrieve and share data, all the while protecting its sensitivity. In addition business leaders need to clarify the policies and standards required to ensure effective and secure data management, data sharing and access across the organization.

Data governance refers to the policies, processes and people involved in managing and protecting data. Data governance is a key enabler, maximizing reliability and minimizing vulnerabilities within an organization.

An important goal of a data governance program is to protect the needs of data stakeholders – individuals or groups who could affect or be affected by the data.

These include those who create data, those who use data and those who set rules and requirements for data.

A fundamental factor in how successful businesses will fare in meeting GDPR and other data compliance requirements is the robustness of their ongoing practice of data governance.

$3.86M

2020 Average Total
Cost of a Data breach:
$3.86M
The Ponemon Institute

Data governance is not only about GDPR

There is more to data governance than just processes and practices. It's important to keep in mind the guiding principles on which data governance is founded. These include: integrity, transparency, auditability, accountability, stewardship, standardisation and change management.

To achieve success as a company, you must be able to identify the source of your data and trust it. Trusting your data implies validating and monitoring its quality as you apply it in your business processes.

Data quality is vital to mitigate regulatory compliance risk, but also to engage customers and stakeholders, optimize the outcome of key business initiatives, and apply analytics to inform daily decisions and long-term strategy.

04

Data governance is a key enabler, maximizing reliability and minimizing vulnerabilities to your organization.

Your teams need secure data pipelines that enable them to retrieve and share data, all the while protecting its sensitivity. In addition, business leaders need to establish, maintain and audit the policies and standards required to ensure effective data management across the organization.

Protect your data, envision the change, scale your insights.

OUR CONTRIBUTION:

OccamLabs can help you champion a data driven culture with easy but secure access to quality information and reap the following benefits:

Help develop your data governance model and roll it out across your organization for stronger data adoption, through training and collaboration.

Help you implement data lineage and distribution tracing product spanning across the entire organization. Resulting in a 360 view of the data-stakeholder match.

Support the creation of a decision support trail to couple key business events with key data in history, for more transparency and readability of business decisions throughout history.

Arm you with audit tools and methodologies of your data environment and inform on potential scope creeps or vulnerabilities of existing systems and processes, reducing your exposure to inside or outside led data leaks.

Get in touch at info@occamlabs.io and obtain a free data governance diagnostic

Book a free consultation:
Info@occamlabs.io