

DATA DISCOVERY

The Foundation of any Compliance or Regulatory Obligation








CONTENTS

Introduction	3
The Situation: Dispersed Data and Determined Cybercriminals	5
Consumer Trust	7
The New Regulatory Environment	9
Data Discovery As a Foundation	11
Staying Secure and Compliant	12
Implementing Data Security Moving Forward	13
Contact and Further Information	14

INTRODUCTION

The Value of Data

Data has become the most valuable asset in the world, surpassing oil as the most profitable commodity.

-  Every minute of the day,¹
-  5.7 million Google searches are conducted
-  65,000 photos are shared on Instagram
-  Consumers share \$304,000 on Venmo
-  \$283,000 is spent in transactions on Amazon

This is just a microscopic look at the flood of data in the possession of just a handful of companies.

In fact, data has become so massive and critical for business success that Gartner has named data and analytics as a **core organizational function**, with Chief Data Officers having the opportunity to increase consistent production of business value by a factor of 2.6x.²

Today, data giants like Facebook, Microsoft, Alphabet (Google's parent company), Amazon and Apple are among the most valued companies in the world. It's not only because they are technical revolutionaries in their own right, but because they have access to much of a user's most sensitive and personal information. This can include names, addresses, date of birth, phone numbers, political views, sexuality, health history, buying habits and intentions. With this information, websites can serve user-targeted ads for products, services and anything else relevant to that user's information. They get the ad revenue, and the ad buyer gets to hyper-target a potential new customer. It's a win-win for all, except for the user's information that can be compromised in the process.



The Data Opportunity Brings Repercussions

While big data and innovation can result in revolutionary technology and more efficient ways of doing business, it comes with an insurmountable security threat. Most companies have an abundance of unknown, hidden data stored on their workstations, servers and in the cloud. This lack of awareness poses a huge threat to security and makes them vulnerable to breach.



To make sure this type of information doesn't get into the wrong hands, companies need to start adopting the strict security regulations that will make them compliant with the law, as well as maintain their own security rules. While remaining in accordance with the law, organizations should not differentiate data based on regulatory standards. They should secure all personal and sensitive data based on the highest common denominator — the highest security standard.

As new data regulations continue to be introduced and amended, as evidenced by the evolution of the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), the security of the organization must be designed to be robust and withstand future regulatory change. This will ultimately satisfy customers and secure their trust, since there will be less chance of a major data breach.

Understanding Data Management

Companies, therefore, need to be acutely aware of how their data is managed. Organizations large and small need to be diligent in defining their processes regarding data privacy to ensure they abide by the regulatory obligations that apply to their business, as well as customers' expectations of security.



If data is not properly maintained and managed, organizations can face significant monetary and brand reputation consequences.

In this eBook we will discuss:

- How data plays an important role in businesses
- Building and maintaining consumer trust
- How government regulations keep businesses accountable
- Data discovery as a secure foundation
- Maintaining security into the future

THE SITUATION:

Dispersed Data and Determined Cybercriminals

Due in large part to the distributed, hybrid nature of the workforce brought about by COVID-19, cybersecurity investment has grown exponentially, with projections that the market will grow to \$270 billion by 2026.³ Data is at the core of this, as almost every sector handles, collects and stores data on their servers, desktops, cloud platforms and more. But what happens after this data is stored? Without the correct safeguards in place, huge volumes of valuable data may be susceptible to a breach.

By 2026
Cybersecurity
investment is
projected to
grow to
**\$270
billion**

Most breaches originate at endpoints, with use of stolen credentials being the most popular point of entry. This can stem from practices such as:



Not modifying default passwords for systems and hardware



Social engineering, including impersonation of someone calling the help desk



Using easy-to-guess passwords



Malware installing keylogging software on the system



**Phishing users
Sensitive data being stored outside of protected areas**



Sharing sensitive information across users and organizations without consideration of risk



Access accounts not being regularly reviewed, resulting in orphaned accounts

With numerous ways for breaches to occur, the Ponemon Institute estimates that the average cost of a data breach for US companies in 2021 was \$4.24 million, the highest average total cost in nearly 17 years. Additionally, the average cost was \$1.07 million higher in breaches where remote work was a factor.⁴

Additionally, enterprise organizations generally experience six instances of fraud within a 24 month period, according to a PwC study. The study also found that financial service firms are the primary target for breaches.⁵ However, data breaches can affect every industry, including healthcare, retail, casino/online gaming, government, telecommunications, transportation and enterprise.

Whether managing a dispersed, hybrid workforce or an operating system change, data security needs to be both stringent and dynamic to withstand any change to the working environment.

In 2021 the
average cost
of a data
breach for US
companies was

**\$4.24
million**

CONSUMER TRUST

Businesses should maintain proper security precautions not only to protect their data but also to appease and instill trustworthiness with their customers. If customers don't believe a company's security measures are sufficient, the company is at risk of losing potential and existing customers.

Let's look at how some major businesses have handled data breaches.

FACEBOOK:

Most people are familiar with the infamous Facebook data breach that occurred in 2018 where the personal information of over 29 million user accounts was compromised. Not only did Facebook, now known as Meta, see a loss of \$13 billion in value, but as a result of the breach, about half of social media users view Facebook more negatively and one-third said they would use the platform less often.⁶ Adding to the reputational damage, Meta was recently fined \$18.6 million for violating the European Union's privacy regulations by failing to prevent data breaches on Facebook.⁷

LOSS

\$13billion

FINE

\$18.6million

REPUTATION

1/2 of all users negative

MARRIOT-STARWOOD:

Then there was the Marriott-Starwood data breach where one of their registration systems exposed millions of customer records, including credit card and passport numbers.⁸ Marriott was faced with a whopping fine of \$126 million.⁹ Inevitably this breach caused a large sum of customers to feel angry, concerned and ultimately wanting not to hand over their information to Marriott in the future.

FINE

\$126million

REPUTATION

Customers angry / unwilling to give information in future

We assume global brands are on top of compliance and security but, similar to smaller organizations, they are still susceptible to issues. Therefore, the need for a solid foundation of training, data governance and security measures are as relevant as ever.

According to the Center for Victim Research,¹⁰ approximately 7–10% of people in the US experience identity fraud each year. More than 20% of these individuals experience multiple occurrences of fraud. Therefore, consumers are becoming increasingly distrusting of organizations handling their data. PwC reports that just 25% of survey respondents believe most companies handle their sensitive data properly. Consequently, 87% of respondents said they would take their business elsewhere if they did not trust a company to handle their information.¹¹

While only 10% of consumers believe they have complete control over their data, consumers' trust in organizations varies by industry. Hospitals and banks are the most trusted organizations (42%), while healthcare providers are a close second (39%). Marketing and advertising companies (3%), along with startups are the least trusted (5%).

...an organization's foundation of this trust should start with employees' security practices

Building customer trust is advantageous to not only gain but also retain business. According to a recent study, 83% of US consumers say that they would stop spending at a business for several months immediately following a security breach.¹² That's why an organization's foundation of this trust should start with employees' security practices. Since most targeted cyberattacks rely on users to activate them, an employee's cybersecurity habits are important to be wary of. Their use of devices, password strength and protection, and general awareness of safety measures can have a direct effect on their corporation's security environment.

If a data breach does occur, there is a real possibility that some loyal customers will be lost because of it. However, it is possible to rebound with the expectation that the company will make real security improvements moving forward. Some measures likely to resonate with consumers are compensation for the victims, a detailed explanation of the breach and a specific description of new privacy policies. Most importantly, consumers expect transparency from a company and the assurance a breach will not happen again.

7-10%
of people in the
US experience
identity fraud
each year

only
10%
of consumers
believe they
have complete
control over
their data

83%
of US
consumers
would stop
spending at a
business for
several months
following a
security breach

THE NEW REGULATORY ENVIRONMENT

While proper security measures and protections should be established at the corporate level, there are many government policies now in place which mandate higher levels of security regulation. According to the United Nations, 137 out of 194 countries worldwide have implemented legislation to secure the protection of data and privacy.¹³ Major regulations encompass laws relating to e-transactions, data protection privacy, cybercrime and consumer protection. Irrespective of where you live, regulation is growing and it can't be ignored.



**137/194 countries
have data and
privacy legislation**



Compliance regulations will continue to grow and your business needs to prepare.

While the majority of countries have regulations in place, studies have found that confusion is serving as a barrier to compliance. For example, close to half of business leaders and marketers (42%) only know “some things” about GDPR, with 29% saying they know very little. Worryingly, 19% said that they knew nothing at all.¹⁴ Established in Europe in 2018 and aiming to regulate how companies handle personal data, privacy and consent, the regulation was designed to reflect our ever-evolving world and the increasing risks that come along with it. Additionally, the GDPR stipulates that organizations need to alert customers and regulators within 72 hours of discovering a data breach.

Perhaps unsurprisingly, the number of GDPR compliant organizations has decreased since its initial introduction, as businesses large and small have struggled to adhere to its requirements. Two primary concerns for business leaders and marketers when managing GDPR compliance are the complexity of sourcing compliant technology solutions (19%) and the challenges related to securing legacy software (17%). Legacy IT systems continue to be a major barrier to achieving compliance, with many believing their IT landscape isn't equipped to handle the complexities of GDPR. Additionally, it's common for many business leaders to blame the financial burden of aligning with GDPR as another primary roadblock to achieving true compliance.

19%
of business
leaders said
they knew
nothing
about GDPR

While adhering to GDPR and other regulations may be expensive for organizations, the risk of a data breach, tarnished company reputation and loss of consumer trust is far greater and ultimately more costly. The Capgemini survey found that 92% of business executives believed being GDPR compliant made them stand out from their competitors.¹⁵ It helps to establish customer trust at the onset, thereby boosting overall revenue.

The survey also found that respondents felt as though the requirements had helped improve IT systems and cybersecurity practices throughout the organization. There is a clear gap in technology adoption between compliant organizations and those lagging behind. Organizations compliant with GDPR, in comparison with non-compliant organizations, were more likely to be using:

	GDPR-COMPLIANT	NON-COMPLIANT
Organization more likely to use:		
Cloud platforms	84%	73%
Data Encryption	70%	55%
Robotic Process Automation	35%	27%
Industrialise data retention	20%	15%

The COVID-19 pandemic and the increase in remote workforces has made compliance even more challenging, given the distributed nature of hybrid work. Working remotely has caused many companies to introduce new communication channels that come with an increased security risk — video conferencing and collaboration tools. For instance, 22% of respondents in the TrustArc Global Privacy Benchmark Survey indicated that personal device security while working remotely has added a great deal of risk to their business.¹⁶



As uncontrollable and unexpected occurrences happen, it's important to continually revise legislation. We need to ensure organizations are prioritizing security risk and protecting their consumer's sensitive data in any configuration of what "normal" looks like.

DATA DISCOVERY AS A FOUNDATION

When it comes to making business and security decisions, business executives should be wary of what the data says versus what the Executive may assume to be true. Many business owners fear that faulty or incomplete data can lead to poor decisions, and a moderate dose of skepticism of data is healthy. This, however, often leads to an assumption model, which is geared more towards human instinct and a basic knowledge of “how to do things” as opposed to what the data strictly says. While human thought can be valuable when it comes to business practices, executives shouldn’t be solely reliant on unverified hypotheses when building a security strategy.



One of the biggest intelligence trends in recent years, data discovery, involves identifying and locating critical, sensitive or regulated data to securely protect or remove it.¹⁷ This has become a priority for enterprise businesses in getting compliant-ready. After auditing their data, this discovery process allows security teams to protect and ensure the confidentiality and availability of their most valuable data.



For companies who operate remotely or within the cloud where file sharing is the norm, this is especially important. In an environment where there are multiple devices, applications and databases being used, maintaining the security of valuable information can be a challenge. Data discovery aids in this challenge by identifying a company’s data in full, offering visibility and ensuring it is securely maintained with best practice controls in place.

The benefits of data discovery and context-aware security¹⁸ can help save a company from major data catastrophe. Coined by Gartner in 2012 while cloud computing was growing exponentially, context-aware security is defined as being “**able to cope with emerging threats and evolving business requirements for greater openness.**” When a company becomes fully aware of factors such as file types, sensitivity, user, location, security teams and the solutions they implement, they can make much more effective security decisions across various use cases.

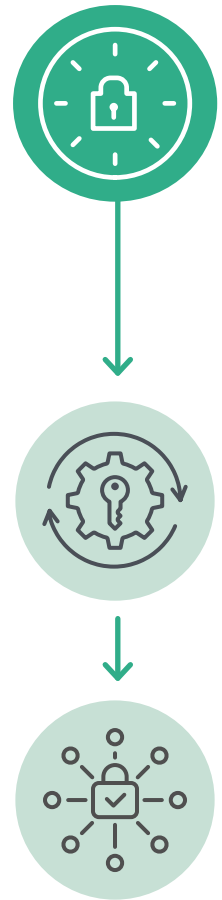
Once adopted, data discovery and context-aware security will be ever-evolving practices for an organization to maintain the security measures they have built. It’s important to set up a standard operating procedure and remain consistent across the organization in these practices.

STAYING SECURE AND COMPLIANT

With multiple government regulations as well as internal company practices to maintain and manage security threats, it's clear that the demand for good security never stops. While data discovery can become a part of a company's routine practice, it's important to think about the long term.

Security automation will help ease security operations related tasks. An automated system can execute more menial tasks without human intervention. Some manual processes security automation can perform include monitoring and detection, data enrichment, incident response, user permissions and business continuity. Ultimately, automation will save both time and company resources so employees can focus more on strategic ways to approach security or other value-add projects.

Security orchestration would be the next logical step in building out a compliant, sustainable security plan. A method for connecting security tools and integrating disparate security systems, security orchestration can streamline security processes. While automation tools can save time, they need to be interconnected to be effective in the long run. Orchestration helps establish more encompassing processes and workflows that get the entire business involved, not just the security team. Once all employees are responsible for the organization's security, they will become more aware of critical, sensitive and regulated data and how imperative it is to protect it.



IMPLEMENTING DATA SECURITY MOVING FORWARD

Data protection should be of the utmost importance for any company. Not only is it crucial to comply with government regulation to avoid fines and penalties, but it's also important to maintain your customer's trust and brand's reputation. This is why internal security practices, such as data discovery and context-aware security, should be your company's main focus. One data breach can be detrimental for years to come.



Companies should follow these general guidelines when they start to build out a sustainable security program:

- 1 > Don't rely on assumptions or what you think to be true about your business. Start clean.
- 2 > Follow an evidence-based approach by conducting a data discovery audit across every piece of data in every location.
- 3 > Build your compliance and security program around your data discovery. You need concrete evidence to justify your plan.
- 4 > Once created, automate that discovery process so that it happens continuously without impacting on internal resources.
- 5 > Implement orchestration to get the entire team involved. Make them accountable for ownership of their data.
- 6 > Review your security practices often and modify them when necessary.

When it comes to data security, the relationship between customer and company is symbiotic. If a customer entrusts their private sensitive information to your company, it is in your company's best interest to protect it. If you have adequate measures in place, you will likely avoid a security breach and keep your customers both satisfied and loyal.





GROUND LABS

Established in 2007 and trusted by more than 4,500 companies in 85 countries, Ground Labs offers award-winning data discovery and management solutions for all industry sectors.

www.groundlabs.com

CONTACT:

US **+1 737 212 8111**
UK **+44 203 137 9898**
Ireland **+353 1 903 9162**
Australia **+612 8459 7092**
Asia **+65 3133 3133**

Email **info@groundlabs.com**



ENTERPRISE RECON

Data made visible with GLASS Technology™
Fast and accurate discovery, management and remediation solutions built for business

groundlabs.com/enterprise-recon ►



CARD RECON

Don't let payment card data catch you out
PCI DSS data discovery and remediation solutions trusted by QSAs

groundlabs.com/card-recon ►

Further Resources

GDPR Compliance & Data Discovery Solutions

groundlabs.com/compliance/gdpr ►

CCPA Compliance Software

groundlabs.com/compliance/ccpa ►

Endnotes

- 1 <https://web-assets.domo.com/blog/wp-content/uploads/2021/09/data-never-sleeps-9.0-1200px-1.png>
- 2 <https://www.gartner.com/smarterwithgartner/gartner-top-10-data-and-analytics-trends-for-2021>
- 3 <https://www.forbes.com/sites/louiscolombus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#61d0d9d5381d>
- 4 <https://www.ibm.com/reports/data-breach>
- 5 <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>
- 6 <https://themanifest.com/social-media/blog/facebook-after-cambridge-analytica-data-breach>
- 7 <https://www.pymnts.com/meta/2022/meta-fined-18-6m-over-facebook-data-breach/>
- 8 <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>
- 9 <https://www.wsj.com/articles/marriott-take-126-million-charge-related-to-data-breach-11565040121>
- 10 <https://victimresearch.org/>
- 11 <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/cyber-and-privacy-innovation-institute.html>
- 12 <https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security>
- 13 <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- 14 https://www.einnews.com/pr_news/565578308/new-survey-report-highlights-increased-impact-of-gdpr-on-marketers
- 15 <https://www.capgemini.com/us-en/news/championing-data-protection-and-privacy-report/>
- 16 <https://trustarc.com/blog/2020/06/17/highlights-2020-global-privacy-benchmark-survey/>
- 17 <https://www.groundlabs.com/>
- 18 <https://www.techopedia.com/definition/31013/context-aware-security>

COPYRIGHT NOTICE

© 2022 Ground Labs. All Rights Reserved. The Ground Labs name and logo and all other names, logos and slogans identifying Ground Labs products and services are trademarks and service marks or registered trademarks and service marks of Ground Labs Pte Ltd and its affiliates in Singapore and/or other countries. All other trademarks and service marks are the property of their respective owners.

DOCUMENT LAST UPDATED:
DECEMBER 2022