Data Discovery : The Foundation of Any Compliance or Regulatory Obligation

GROUND LABS

Introduction

In 2017, The Economist claimed that data is now the most valuable asset in the world, surpassing oil as the most profitable commodity. Data giants like Facebook, Microsoft, Alphabet (Google's parent company), Amazon, and Apple are among the most valued companies in the world. While Amazon accounts for about 50% of all dollars spent online, almost all digital advertising dollars spent in America go to Facebook and Google.

So why are these companies so highly valued? It's not only because they are technologically revolutionary 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, or anything relevant to that user's provided 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.

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 and 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.

When new data regulations are inevitably introduced in the future, the security of the organization will already be designed to be robust and withstand future security regulations. This will ultimately satisfy the trust of the customer since there will be less of a chance of a major data breach.

Therefore, companies need to be acutely aware of how their data is managed. Both large and small organizations 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

2 The Situation

In 2020, **cyber security is a $173 billion market**, with projections to grow to $270 billion by 2026. Data is at the core of this, as almost every sector handles, collects, and stores data on their servers, desktops, cloud, and more. But what happens after this data is stored? Without the correct safeguards in place, your customers' valuable data may be susceptible to a breach. In fact, as of July 2020, there have been **540 publicly reported data breaches** reported in the last 6 months alone.

Most breaches originate at endpoints, with credentials being the most popular breach entry point. This can mostly 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 to risk

Access accounts not being maintained, resulting in orphaned accounts

With numerous ways for breaches to occur, **Ponemon Institute** estimates that the average cost of a data breach for U.S. companies is $8.19 million, a 130% increase from estimates in 2006. Additionally, enterprise companies 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. However, data breaches can affect every industry, including healthcare, retail, casino/online gaming, government, telecommunications, transportation, QSA, and enterprise.

In 2020, the onset of the COVID-19 pandemic and the subsequent increase in the need for remote work has caused business leaders to be faced with a tough predicament: trading a potential health threat for a potential security threat. For both employer and employee, working from home instead of in a secure office environment is a new feat. Before the threat of COVID-19, it was mostly businesses as usual. Now, tens of millions of remote workers' identities and the security of their devices are at risk. Consequently, cybersecurity in this "new normal" has become a priority.

Whether it's a worldwide pandemic or an operating system change, data security needs to be both stringent and dynamic to withstand any change to the working environment.

3 Consumer Trust

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

So why are these companies so highly valued? Let's look at how some major businesses have handled data breaches. Everyone is 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 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.

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. Marriott was faced with a whopping fine of $126 million. Inevitably, this breach caused a large sum of customers to feel angry, concerned, and ultimately wanting to not hand over their information to Marriott in the future. Additionally, a well-known airline is now facing fines for up to $183M due to a data breach that occurred in 2018.

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

According to the Center for Victim Research, approximately 7-10% of people in the U.S. experience identity fraud each year. More than 20% of these individuals experience multiple occurrences of fraud. Therefore, consumers are increasingly becoming 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.

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%).

Building customer trust is advantageous to not only gain but also retain business. According to a recent study, 83% of U.S. consumers say that they would stop spending at a business for several months immediately following a security breach. That's why an organization's foundation of this trust should start with your employee's security practices. Since around 99% of 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, 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.

4 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**, 194 countries worldwide have implemented legislation to secure the protection of data and privacy. Major regulations encompass laws relating to e-transactions, data protection privacy, cybercrime, and consumer protection. Irrespective of where you live, compliance is growing and it can't be ignored. Just as California has led the way with vehicle **emission standards** and the rest of the country has followed, the same can be expected of the California Consumer Privacy Act (**CCPA**).

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 only 20% of businesses believe they are GDPR compliant. Established in Europe in 2018 and meant to regulate how companies handle personal data, privacy, and consent, these regulations were designed to reflect our ever-evolving world and the increasing risks that come along with it. Additionally, these regulations stipulate that organizations need to alert customers and regulators within 72 hours of a discovered data breach.

Perhaps unsurprisingly, the number of GDPR compliant organizations has decreased since its initial introduction two years ago as businesses large and small have struggled to adhere to these regulations. Many cite their legacy IT systems as a major obstacle; 38% of those surveyed claim their IT landscape isn't equipped to handle the complexities of GDPR. Additionally, 36% of respondents believe GDPR requirements are too complex to implement. The financial burden of aligning with GDPR is another major obstacle for organizations to overcome.

While adhering to GDPR and other security regulations may be expensive for organizations, the risk of a data breach, tarnishing company reputation, and losing 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. It helps to establish customer trust at the onset, therefore boosting customer trust and 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-complying organizations, were more likely to be using cloud platforms (84% vs. 73%), data encryption (70% vs. 55%), robotic process automation (35% vs. 27%), and industrialized data retention (20% vs. 15%).

A newer piece of privacy legislation, the California Consumer Privacy Act (**CCPA**), which was enforced on July 1, 2020, also had companies scrambling to meet its requirements. While GDPR laid the groundwork, only a small portion of businesses surveyed said they were going to be compliant with CCPA ahead of the enforcement date. In fact, in the most recent **Global Privacy Benchmark Survey**, more than 20% of respondents reported that they were either somewhat unlikely to be, very unlikely to be, or don't know if they will be fully compliant with CCPA by July 1st, 2020.

One challenge many respondents cited was having manual processes in place, rather than automation. Automation helps simplify data privacy while using data to drive business growth. While this is a more efficient way of handling security processes, it is a more advanced methodology that some businesses are not yet equipped for.

One example of a new security risk is the COVID-19 pandemic and the increase in remote workforces. Working remotely has caused many companies to introduce new communication avenues that also have an increased security risk: video conferencing and collaboration tools. In this "new normal," 22% of respondents indicated that personal device security while working remotely has added a great deal of risk to their business.

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 a "new normal" looks like.

5 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 then 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 sensitive or regulated data to securely protect or remove it. This has become a priority for enterprise businesses in trying to get compliant-ready. After auditing their data, this discovery allows security teams to protect and ensure the confidentiality and availability of the protected, sensitive 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 helps aid this challenge by identifying a company's data in full and making sure it is securely maintained with best practices and controls in place.

The benefits of data discovery and context-aware security can help save a company from a 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 security 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 your security practices.

6 Staying Secure and Compliant

With multiple government regulations as well as internal company practices to maintain and manage security threats, it's clear that 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 personal data and how imperative it is to protect it.

7 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, it's even more 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 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 using your internal resources.
5. Implement orchestration to get the entire team involved. Make them accountable for ownership of their data.
6. Be brave, be bold, and modify security practices when necessary.

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

Enterprise Recon

GDPR Compliance Solutions

CCPA Compliance Solutions

Ready to learn more about how to use data discovery to maintain compliance?

Request a demo today!