DATA PROTECTION WORLD FORUM

CREATING AND CURATING ENGAGED GRC MARKET PLACES

Aptible

Compliance in the Age of the Cloud

CONTENTS

“The companies that do the best job on managing a user’s privacy will be the companies that ultimately are the most successful.”

- Fred Wilson

Every era has its defining business risk.

And as more and more data breaches hit the headlines, it's clear that now and forevermore, data security and compliance risks will result in serious financial repercussions and loss of customer trust.

THE EMERGENCE & GROWTH OF CLOUD TECHNOLOGY

Data security and compliance have always been important but previously, compliance did not have the high profile it does today. As cloud technology has been more widely adopted (especially public and hybrid cloud), data and security have taken center stage, as it is clear that they are integral to operating successfully in the cloud.

While cloud technology may appear to be a relatively recent innovation, it actually dates back farther than many of us know. Its origins lie in the 1950s, when computer scientist John McCarthy, who came up with the term "artificial intelligence", devised a theory resembling cloud computing as we know it today. It was too expensive and perhaps somewhat 'clunky' to use back then, as it was connected by cables. But with the arrival of mobile internet devices, the idea could be reapplied.

Unsurprisingly, cloud technology has taken off, given that it can offer businesses flexibility, lower costs, and greater efficiency. The overall hosting, storage, and computing cloud services market was estimated to be worth $126 billion in 2017 and is forecast to grow to $163 billion in 2021.

Chas Ballew, Co-founder and CEO, Aptible in his own words:

"The explosion of cloud services has made it possible to start automating a lot of security work. The cloud has also made it possible for businesses to grow – to unbelievable levels of impact and economic size."

And the cloud market shows no signs of slowing down: recent figures by Gartner indicated that the SaaS market is expected to grow to $104.7 billion worldwide in 2020.

DATA SECURITY & COMPLIANCE – THE CHALLENGES

As use of cloud technology has burgeoned, the focus on compliance has magnified, at a time when it has also become more complex and more difficult to manage.

One issue is the sheer volume of data created and consumed nowadays, which is unlikely to reduce: recent research by IDC shows that the total amount of data globally is expected to reach a massive 59 zettabytes (one zettabyte equals one sextillion bytes) in 2020.

This is partly attributed to the number of people working from home during the coronavirus pandemic and an increase in video consumption. The price of Zoom's shares skyrocketed from $73 per share in January of 2020 to over $240 in June. This is greatly attributed to the social distancing measures taken during COVID-19, the enforcement of remote work, and the new reliance on platforms that enable remote communications and collaboration.

High volumes of data can present a headache when it comes to collecting, organizing, and managing, as well as keeping it secure and compliant. Keeping track of it all can be challenging, particularly if a wide and ever-growing range of disparate SaaS tools is involved. For instance, compliance, security, sales, engineering, and other functions across the business might all have separate tools (think Jira, GitHub, HR software, etc.) that don't communicate with each other. The ongoing addition of new tools can make it harder, too. Storing data across a number of locations and a range of SaaS companies also complicates compliance management – fragmenting evidence collection and slowing down audits. In addition, there are many other compliance 'pain points', for all involved in making it work, such as manual compliance checks, user access reviews, and monitoring of controls. These are typically handled across a variety of formats, such as email and spreadsheets, to name just a few.

There's the big picture to consider too. While security and compliance is obviously a very high priority, attending to it effectively can slow down a company's ambitions and ability to achieve other goals. That risk of distraction has to be weighed against the risk of falling behind on making necessary changes to security requirements.

At the same time, the workload of compliance departments increasing as they are being called on more and more to help with the sales process. Because customers care more about compliance than ever before, proof of compliance and security posture is required in order to close the deal. Therefore the sales team will call on the compliance resources to provide proof such as audit reports, NDAs, data privacy regulations, and more.

Chas Ballew, in his own words:

"Compliance and business growth have become more intertwined than ever, and for more and more companies. When we talk to directors of GRC and other security leads at B2B SaaS companies, we hear that they're spending 30 or 40% of their time on helping to build trust with large customers. They also say that they're helping the sales team to grow the business, business by demonstrating their compliance 'posture' to their customers. And the demand for this is higher than ever."

Keeping up with the stipulations of the regulatory environment is also crucial, as this has been the source of far-reaching compliance changes, including GDPR, in Europe, in 2018. More recently, the introduction of the California Consumer Privacy Act (CCPA) has demonstrated just how serious an issue compliance is today. And earlier this year, the Court of Justice of the European Union issued a judgment which invalidated Privacy Shield, affecting companies in both the European Union and the United States.

Policies move and change constantly, and being able to adjust quickly is of benefit both to business continuity and maintaining customer trust.

As if all of this (growth of data, adoption of new SaaS tools, new regulation, and time constraints) were not enough to contend with, all of these challenges are taking place in an an environment where maintaining customer trust is non-negotiable. As far back as 2013, Boston Consulting Group research showed that in every generation and in most countries, consumers were five to ten times more likely to share personal data with an organization if they trusted that the data would not be used to harm them.

As rock-solid security and compliance has become simultaneously more pressing and more complex to handle, the cost of security failures has rocketed, in terms of the cost of fines and the price of losing hard-won customer trust. To put it more succinctly: data security and compliance can make or break a company and its reputation.

Companies sharing their data with third-party providers need to be able to trust that it will be used in a way that meets compliance standards, et a 2019 survey revealed that nearly half (44%) of all firms surveyed had suffered a substantial data breach because of a third-party vendor. Compliance teams have their work cut out for them.

Chas Ballew, in his own words:

"Our customers report that putting the information the customer needs, to be able to buy their cloud services, in their hands as soon as possible saves time, and is one of the most effective things they can do."

THE COST OF COMPLIANCE & DATA BREACHES

The fact that data breaches are almost inevitable does not make it any more palatable. Aside from the detriment suffered to the brand, and the loss of customer trust, there are serious financial repercussions.

According to the Identity Theft Resource Center, a number of household names, such as Yahoo, Equifax and Marriott Hotels (Starwood) have exposed significant volumes of customer data in the last few years. In the case of Yahoo, the number of customers affected ran to billions – and resulted in the eyewatering cost of $117.5 million, to settle a class-action lawsuit in relation to how it handled communications around the various hacks it experienced. But it's not just the big corporates which have suffered. In 2017, it was reported that information on nearly 200 million US voters was publicly accessible for nearly two weeks, on the server of Deep Root Analytics, a marketing company hired by the Republican National Committee. Not only did this information include phone numbers and birth dates; it also contained details of voters' political views.

While businesses and public-sector organizations are counting the cost of data breaches, vast sums of money are flowing in the direction of the cyber criminals responsible, with billions of dollars lining their pockets from ransom demands.

HOW TO IMPROVE COMPLIANCE IN THE AGE OF THE CLOUD

Data breaches aside, it's clear that businesses have their work cut out to remain compliant, following the move to the cloud: the problems, dilemmas and challenges are many and wide-ranging. But it doesn't have to be a complex and time-consuming task – and the goals of staying compliant, reaching business-growth ambitions and maintaining customer trust are not incompatible. So, how can organizations achieve these goals?

Here are a few practical takeaways:

01 | Make effective use of automation to reduce manual tasks, which frees the team to focus on strategic projects;

02 | Improve integration of the various tools used across the company, so that there is one single 'point of truth';

03 | Arm sales teams with the ability to easily access the compliance evidence they need;

04 | Ensure compliance is discussed early on in discussions with potential customers, to speed up the sales cycle.

Third-party cloud service providers can also put themselves in better position to attract customers (and earn their trust) by ensuring that they have the appropriate compliance certifications (SOC 2, ISO 27001, HIPAA, PCI, etc.). Signs that a business has gone to the effort to achieve certification can be reassuring to (if not outright required by) customers.

After all, as technology venture capitalist Fred Wilson points out, excellence in handling data is a route to competitive advantage. Therefore, companies who can demonstrate a strong commitment to security and compliance can build customer trust and grow their business.

To sum up, for organizations that have ambitious growth goals, it might be time to invest in a high-quality compliance program that will help take their business to a new level, and which could also provide them with the tools to be more effective than their peers.

Chas Ballew, in his own words:

"I do strongly believe that the most competitive businesses and those that will win, will effectively be the businesses that use compliance to fuel their growth, to shorten their sales cycles, to close deals faster and to close bigger deals. These are the ones that are going to out-muscle their competition."