The GDPR Domino Effect on U.S. State Legislation for Data Security

7 Guidelines to Help You Navigate the Impending Compliance Obstacles
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Introduction</td>
</tr>
<tr>
<td>04</td>
<td>Third Party Access: Who’s Looking at Your Data</td>
</tr>
<tr>
<td>05</td>
<td>GDPR has Created a Domino Effect of U.S. Regulation</td>
</tr>
<tr>
<td>06</td>
<td>Government and Industry Have a Ways to Go for Data Security Excellence</td>
</tr>
<tr>
<td>07</td>
<td>Best Practice SIEM Gives You a Cyber Fighting Chance</td>
</tr>
<tr>
<td>09</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
Introduction

The European Union’s General Data Protection Regulation (GDPR) was enacted in May 2018. Since then, many states within the U.S. have been following the EU’s lead with their own version of citizens’ data protection and privacy legislation. Until recently, corporate (i.e. sales and marketing) attitudes towards mass data collection have been the more the merrier. Now with the GDPR and U.S. states’ legislation enactments, for the first time ever there are much harsher punitive damages enforceable by law for the mishandling of consumer data. With the GDPR, no matter where your business or data resides, if you collect Personally Identifiable Information, or PII, of a European citizen, you must comply with the regulation. Similarly, with the California Consumer Privacy Act\(^1\), effective in January 2020, even if your business is incorporated outside of the state you must comply if your database contains California citizens’ PII.

In 2005, the state of North Carolina enacted the North Carolina Identity Theft Protection Act\(^2\) which strengthened security measures for its citizens’ personal information and gave consumers more tools to fight theft of their information. In 2019, state legislators reintroduced even tougher legislation to protect against identity theft. The Act to Strengthen Identity Theft Practices has requirements more similar to the GDPR\(^3\). Now, consider 50 U.S. states enacting PII security laws that your organization will have to understand and manage. Having to understand each states’ different stipulations for their respective citizens’ for PII security is going to be overwhelming.

This paper addresses the genesis of these U.S. states’ consumer data protection laws, some commonalities of this legislation, and finally best-practices for maintaining good security posture across your enterprise that will give your organization its best chance for reducing risk of data breaches and achieving compliance with data protection and privacy policies globally and locally.

---

\(^1\) https://www.caprivacy.org/

\(^2\) https://ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_76/Article_2A.html

\(^3\) https://www.jdsupra.com/legalnews/a-bipartisan-proposal-to-beef-up-north-73529/
Third Party Access: Who’s Looking at Your Data

Currently, third-party access to our personal data is the price we pay for receiving useful services the internet provides, and it is a price we are happy to pay – until recently that is. With each data breach scandal that makes headlines, the consumer becomes increasingly weary of the unadulterated access we’ve so willingly (or rather ignorantly) allowed corporations (and hackers)! And, with more and more of our daily lives taking place online, our entire digital identity is accessible to the services we rely on to communicate, access banking accounts, make purchases, receive educations, and access our own healthcare information. The latter arguably being the most robust cache of PII.

The recent Facebook Cambridge Analytica scandal sparked an ethical debate and public wake-up call over the scale and power behind this widespread, unwanted data collection. And while Big Data hoarding is certainly a threat to our privacy, it’s also a threat to our pocketbook. With more and more purchasing happening online, unprotected credit-card data is wildly abundant on the internet and cyber-criminals are taking advantage of this. The 2018 Experian “Global Fraud and Identity Report” revealed that 63 percent of businesses surveyed had the same or more fraud losses in the past 12 months.

The GDPR was just the start. After the GDPR went live in May 2018, 11 U.S. states launched data protection laws to safeguard the PII of their residents, and more are coming this year and next. Additionally, in November of 2018, President Donald Trump signed into law the Cybersecurity Infrastructure Security Agency Act of 2018. This act establishes the Cybersecurity and Infrastructure Security Agency (CISA). CISA is responsible for protecting the Nation’s critical infrastructure from physical and cyber threats, a mission that requires effective coordination and collaboration among a broad spectrum of government and private sector organizations. The onus to protect this data, however, no longer solely falls on the shoulders of IT departments.

---

7 https://www.dhs.gov/CISA
GDPR has Created a Domino Effect of Regulation

In a recent Ponemon/IBM survey\(^8\) of what CISOs worried about in 2018, “lack of competent inhouse IT staff” was the number one concern. There is a serious discrepancy between the vastness of an organization’s cyber-security capability compared to the level of cyber-security awareness their employees receive during onboarding and then retain. IT cannot go at this alone, for they are understaffed and so overwhelmed fighting IT complexity, security is most times a back-burner item. IT and Business departments, for security’s sake, must work together now more than ever integrating data and intellectual property security standard operating procedures when onboarding new employees. We must now include HR departments and department leaders in setting data security policies. And most importantly, implementing continuing education to shrink the employee security gap in the workplace.

This security gap could have a serious effect on the bottom line for any business, and now that government security mandates (laws!) are in full force, the stakes for noncompliance are even higher. Another recent Ponemon/IBM study\(^9\) shows that data breaches are larger, costlier, and take longer to discover year after year. This new states’ legislation will certainly amplify the ramifications for cyber breaches in the years to come and organizations like yours will now have to navigate an incoming maze of differing data privacy laws from every direction. Additionally, a large cost component of a data breach is the work to become compliant after the infraction.

The U.S. Federal Government Has Joined the Fray

We are staring down the barrel of unprecedented legislation for data security at the state level. In turn, the Trump administration’s cybersecurity directive appears to be a reaction to the states’ legislation; clearly the GDPR has created a domino effect of regulation for U.S. consumers for increased PII protection. For consumers in the U.S., this is great news. For businesses and IT leaders in the Fortune 1000, where siloed work environments and IT complexity reign supreme, the news should be worrisome.

Surprisingly, one executive in the enterprise has taken on a bigger role in technology spending and data collection, and s/he is not from the IT department. The Chief Marketing Officer is now set to outspend the CIO in technology for the first time since this data was collected.\(^{10}\) Marketing budgets are expanding to accommodate the latest sales and marketing software products designed to accelerate and automate sales pipelines – CRM and Marketing Automation systems.

---

Government and Industry Have a Ways to Go for Data Security Excellence

A recent survey from Gartner\(^\text{11}\) revealed that CMOs are spending nearly one third of their budgets on this sales and marketing technology – the software tools that hold their customer and prospect PII. Large organizations are seeing the value that customer/prospect data brings to their revenue streams and will continue to invest more dollars in the years to come. Marketing Technology or MarTech purchases in 2018 were the largest marketing expense, far surpassing other categories.\(^\text{12}\) With CISOs worrying about employee negligence with data and non-technical resources handling more data, enterprises appear to be on a collision course for correction fueled by this newly enacted consumer data protection legislation.

Clearly, government and industry have a long way to go for data security correction in the enterprise. The 2018 IBM/Ponemon Research “Cost of a Data Breach Report”\(^\text{13}\) reveals some startling statistics about corporate data protection.

- The mean time to identify a breach was 197 days.
- The mean time to contain a breach was 69 days.
- The average total cost of a data breach was $3.86 million.
- If you were able to contain a breach in less than 30 days, you saved more than $1 million.

It is not uncommon for a Fortune 1000 company to invest six- or seven-figures (some, eight-figure) in cybercrime fighting technologies. How then is it possible that the average time to discover a breach – with all the tools and knowledge that companies invest – takes more than six months? The answer lies within these breached organizations’ ability to 1) create a single source of log information for enterprise security, 2) correlate events for security breach potential, and 3) generate real-time alerts from all IT systems of potential threat. Because of the heterogenous nature of network infrastructures and the differing human resources who use them, this is a nearly impossible task.

---

\(^{11}\) [https://www.gartner.com/smarterwithgartner/2017-2018-gartner-cmo-spend-survey/]
\(^{13}\) [https://www.ibm.com/security/data-breach]
Best Practice SIEM Gives You a Cyber Fighting Chance

There are, however, best practices for breaking through the silos of IT systems and the people who use them. Security Information and Event Management, or SIEM, systems were originally developed back in the mid-2000s on distributed computing systems. These systems have matured over the years to be very effective at collecting user and system event logs, correlating the log data and generating real-time alerts whenever a hint of malicious cyber activity occurs. The problem with these systems is they leave out the most valuable IT asset in Fortune 1000 or government enterprise, the mainframe.

To protect yourself from impending data protection and privacy legislation BMC suggests the following best practice guidelines to be applied across all systems, especially your mainframe where the most valuable PII lies.

1. Correlate event logs across all systems, mainframe and distributed. Combining event messages helps determine user or system behavioral patterns that might indicate threat. Intelligent correlation rules can identify anomalous and suspicious events which can be strong indicators of compromise.

2. Make sure all mainframe security event data is visible in your IT Security Operations Center. This will enable you to view event messages in a single version of security truth, providing a 360-degree perspective on threat activity in your infrastructure on both distributed and now mainframe systems.

3. Understand that your most valuable IT asset – the mainframe – is where the most sensitive PII and corporate IP is stored and managed. It is also the system that is often forgotten when developing cyber-security defense strategies in distributed systems. If your mainframe is not included in your SOC, you are missing the most critical chunk of user activity to monitor. On your mainframe, privileged users have the keys to the data kingdom. You must know their every move in real time.
4. Make sure you have real-time security visibility and alert notifications from your SIEM. Speed of reaction is critical to stemming data exfiltration during a security breach. It only takes a few minutes for terabytes of critical data to be exfiltrated from your network, so your security notification systems and response need to be as quick as up-to-the-second. Your approach to cyber defense should be “not if, but when.”

5. Involve your legal team now. They are aware of the GDPR and States’ laws concerning PII. Understand your breach scenarios so your teams understand the ramifications of breach law. Ask your legal team what you need to know about your organization’s cyber insurance. This will help you understand your threat scenarios and what is at stake.

6. Find the right vendor to address your specific security and compliance requirements. There are a host of solutions coming out now to help address these new regulations and increasing threats to cybersecurity. Understand your weaknesses and also that it takes a village and the right technology vendor to help you set and maintain cyber security compliance.

7. Define and practice your response plan to incident threats. Your mantra for data security should be “not if, but when,” which makes time to mitigate critical to stem data exfiltration. Many organizations install security systems and policies yet never practice response, making remediation slow and confused.

The key to maintaining IT security compliance in a new era of data privacy laws is to make sure everyone in the organization is involved in the effort to make your cyber security plan best practice. Everyone from the administrative assistant to the security guard to your legal team needs to be properly informed of the cost of a data breach (widescale job security could be at risk here) and then properly trained on how to secure data to SOPs. What’s more, it is also imperative to take a holistic approach when developing plans to protect your IT infrastructure. For event correlation – perhaps your biggest InfoSec ally – leaving Win/UNIX systems separated from your mainframe within your SOC is a mistake that may prove incredibly more costly than ever before with this new batch of legislation.

A recent high-profile breach from Ticketmaster UK spanned a both pre- and post-GDPR timeframe. Ticketmaster UK got off lucky because this was the first post-GDPR high-profile breach and the EU appears to have some leniency. At this writing, the EU case is still ongoing. However, a UK law firm has launched a $6.5 million class-action lawsuit against Ticketmaster US citing “multiple fraudulent transactions” since the breach. The fine could be as much as €17 million or as low as pre-GDPR amount of several hundred thousand. As of February 2019, 59,000 GDPR violations have been reported and 91 fines have been imposed, the highest of which was issued to Google at €50 million.

Your legal team should by now be aware of the legislation coming (if not already enacted) from your state. There is no time like the present to be ready for a breach. As we saw in Ticketmaster and Google post-legislation breach looks much worse than pre- so act now. The reality of what’s at stake punitively is starting to set in, and if you fail to act now you may soon be held accountable by any citizen questioning your data security practices – and now, many have the right to.
Conclusion

The rise of Big Data Analytics has helped organizations have unprecedented insight into their audiences’ purchasing behavior. This robust data and the analytics coming from it is now the main driving force behind business decisions, and that offers incredible value to an organization. However, as Spiderman fans are quick to point out, with great power comes great responsibility. It is critical to understand that this data is now mostly leveraged by non-technical, less security-conscious marketing resources in your organization. The days of massive data collection and management without strategic plans for its security are over, as governments begin to react to calls for greater data responsibility from the organizations that are benefiting from the privilege of consumer data insight. As with any other aspect of a healthy organization, agility and proactivity are key to overcoming the inevitable cyber security and compliance obstacles in front of us.

And it helps to always be thinking (of your breach potential) “it’s not if, but when.”

For more information
To learn more about BMC’s latest mainframe security product family, Automated Mainframe Intelligence (AMI), please visit bmc.com.