CHANGING CONSUMER CONCEPTIONS OF PII DATA NECESSITATE EVENT CORRELATION, REAL-TIME ALERTS AND REHEARSED INCIDENT RESPONSE

Europe's Data Protection Directive emerged in 1995, just two years after the formation of the European Union (EU). It was designed almost a decade before Facebook and three years before Google – a time when ecommerce was just a blip on the radar and the internet had a total of 120,000 registered domain names. By 2016 that number had grown to 326.4 million, and the rapid pace of technological change meant we were living in a different world that demanded modernized data security regulations.

After four years of deliberation and design, the EU announced the General Data Protection Regulation (GDPR), a sweeping law governing the data security and privacy of European citizens. When the law came into force in May of 2018, it affected not just European businesses, but companies all over the world that had customers in Europe. It also had even broader implications by inspiring the creation of similar laws in the U.S. California led with the California Consumer Privacy Act (CCPA) in 2018, and a total of 25 states now have data protection laws. While more will surely follow, there's also the looming possibility of a federal law governing how companies treat the Personally Identifiable Information (PII) and other data of US citizens.

Why all the concern? Until recently, consumers have been all too happy to give away reams of Personally Identifiable Information or PII data without much concern for how it was being used. However, a slew of major data fumbles, from Facebook's Cambridge Analytica scandal to the

Equifax breach that exposed the financial records of 148 million people, have eroded public trust and pushed consumers to question how companies are defending sensitive PII.

The Year 2015 BC (Before Cambridge)

In 2015, the RAND Corporation set out to weigh public perception of high-profile data breaches. The "Customer Attitudes Toward Data Breach Notifications and Loss of Personal Information" study surveyed 2,038 individuals to determine how consumer behavior changes after breach notifications. While responses varied by demographic, a mere 11% of respondents indicated they would cease doing business with a company after a breach while 65% felt that their relationship with the company would continue unchanged.

With cybersecurity itself evolving at such a frantic pace, Ping Identity set out in 2018 to determine if customer perception might echo those changes. "Attitudes and Behavior in a Post-Breach Era" polled more than 3,000 consumers around the globe, and the results told a profound story. Almost half (49%) of those surveyed indicated that they wouldn't use a service or application that had recently been breached, and while 37% would, they would only do so if they had no other options for the service in question.

In the tumultuous world of corporate cybersecurity, one thing is perfectly clear – consumers are more conscious of their data than ever before. While they can welcome the passage of additional legislation to establish protections and penalties, the rash of U.S. state regulations on the horizon will continue to plague the Fortune 1000 enterprises that lose control of their data. With the costs of a breach – both to a company's reputation and its bottom line – climbing ever higher, CxOs must take the following steps to demonstrate an effective and clearly evident posture of cybersecurity defense.

1. **Use correlation to glean evidence from event logs**
   Correlation should occur on both distributed and mainframe systems, combining event messages and user activity to help determine the type of behavior that constitutes a threat. BMC AMI Security uses an intelligent correlation engine that automatically spots anomalous events events based on Indicators of Compromise developed by the world's leading mainframe hackers and alerts administrators
2. **Rely on solutions that provide insights in real time**
   It takes an unacceptable 279 days for the average organization to identify and contain a data breach, according to 2019 data from the Ponemon Institute. Enterprises aren't just failing to put a stop to cybercriminal activity – they're failing to see it going on in the first place. To amend the present state of affairs, organizations must rely on real-time threat reporting that happens automatically. With automated security solutions, administrators are notified the instant a cyberattack is spotted, enabling them to take immediate action according to the nature of the threat.
3. **Implement and practice an incident response plan**
   Many organizations mistakenly think their security procedures and policies adequately insulate them from the risk of a data breach, which means they're left scrambling to initiate a response when a breach inevitably occurs. When dealing with data exfiltration, seconds count, and having a plan in place might mitigate some of the fallout from a breach. The most advanced enterprises, however, are the ones that actually practice their incident response plans. As the cybersecurity landscape evolves, there are more threats than ever, and the most appropriate

response depends on the specific danger. For example, BMC AMI Security supports the ability to take a user ID and immediately search for all actions taken by a user to determine scope and depth of the damage versus companies who must sort through system data in batches with the hopes of piecing together what happened. Knowing what to do and practicing how to do it will allow for a relatively quick and painless remediation compared to the alternative.

Attitudes around data security are changing, and for good reason. As massive organizations demonstrate a careless approach to PII that jeopardizes the well-being of their customers, governments are responding with increased regulation. To win trust and conquer compliance obstacles, enterprises must implement forward-thinking solutions that bring their mainframe security practices into modernity. To access our in-depth report on cybersecurity legislation and the steps to achieve compliance, download our whitepaper today.