3 Data Compliance Challenges and How to Beat Them

If HIPAA, GDPR, NIST, and CFAA have failed to confuse you, wait until CCPA and NYPA enter the scene. The alphabet soup of information privacy laws can feel like a minefield in the business landscape. And with technology evolving rapidly, data compliance challenges continue to increase in complexity. However, with careful planning, you can rise above these challenges.

According to a 2018 report by the Ponemon Institute, the average cost of a data breach ranged from $2.2 million to $6.9 million. In addition to fines, businesses found non-compliant face lawsuits, remediation costs and audits. Perhaps more damaging, they stand to lose both revenue and reputation.

Many factors contribute to compliance complexity. But the proliferation of bring your own device (BYOD) policies and the Internet of Things (IoT) pose unique data compliance challenges. At the same time, organizations continue to wrestle with email vulnerabilities and the human element. Hurdling these challenges can help make privacy manageable.

1. BYOD Policy Enforcement

Many organizations have adopted BYOD policies in recent years, citing an increase in productivity and job satisfaction. However, this practice puts data security in the hands of individuals and increases the risk of a breach. At one point, lost or stolen devices accounted for 68 percent of all healthcare data breaches.

Fortunately, organizations are learning that a few critical steps help to curb the data compliance challenges posed by mobile devices:

- Enforce strict password policies for all mobile devices.
- Ensure that mobile devices use up-to-date virus protection and encryption.
- Use mobile device management (MDM), taking care to obtain employee consent before installing MDM services on their devices. A quality MDM system allows you to specify devices that can access the network. It also allows you to remotely wipe a lost or stolen device.

2. Internet of Things (IoT) Vulnerabilities

The IoT has transformed business, delivering huge benefits to manufacturing, retail and other industries. Factories save money with predictive equipment maintenance. Remote health monitoring helps save lives and cure diseases. However, with those benefits come risks.

For instance, a breach at a POS terminal that processes credit card payments could expose sensitive credit card information. Likewise, a hacker who gains entry to connected equipment in a factory can access trade secrets or even take control of machinery. Alarmingly, the Ponemon Institute reports that 26 percent of companies experienced IoT-related data breaches.

To mitigate risk, organizations should take inventory of all IoT devices connected to the network, including those that belong to vendors. Change default credentials on those devices to employ strong passwords and quickly deploy any patches. Where possible, put IoT devices into a separate area of the network to limit access.

3. Unruly Email

Hardly a newcomer to the list of data compliance challenges, email holds a firm spot on the list of information security vulnerabilities. In fact, email-related data breaches appear to be on the rise, particularly in healthcare.

As an example, Verity Health System in California suffered three email hacking incidents in a three-month period over the last year. Hackers potentially gained access to health information on over 14,000 patients, just from a single attachment.

As a necessary first step, ensure encryption of all data, both in transit and at rest. Know the retention regulations that apply to your industry and set automatic archival and deletion accordingly. Finally, cover the human factor. Set email filters to guard against accidental sending of sensitive information, and educate employees on email policies.

Meeting Data Compliance Challenges Makes Good Business Sense

Untangling and complying with the intricacies of the various privacy laws can present a formidable challenge. At the same time, the steps you take to protect sensitive information also offer key business benefits. From enhanced cyber-security and data governance to increased client trust, you will recognize clear returns on your investment.

With a wealth of experience in information governance and cyber-security, the experts at Messaging Architects can guide you through the minefield of data compliance challenges.