Course / Module 1: What is Data Security / Common Data Security Pitfalls

Previous Next

Pitfall 1: Failure to move beyond compliance

Bookmark this page

Compliance doesn’t necessarily equal security. Organizations that focus their limited security resources to comply with an audit or certification can become complacent. Many large data breaches have happened in organizations that were fully compliant on paper. The following examples show how focusing solely on compliance can diminish effective security:

- Incomplete coverage: Enterprises often scramble to address data-base misconfigurations and outdated access polices prior to an annual audit. Vulnerability and risk assessments should be ongoing activities.
- Minimal effort: Many businesses adopt data security solutions just to fulfil legal or business partner requirements. This mindset of “let’s implement a minimum standard and get back to business” can work against good security practices. Effective data security is a marathon not a sprint.
- Fading urgency: Businesses can become complacent towards managing controls when regulations, such as the Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR), mature. While, over time, leaders can be less considerate about the privacy, security and protection of regulated data, the risks and costs associated with noncompliance remain.
- Omission of unregulated data: Assets such as intellectual property, can put your organization at risk if lost or shared with unauthorized personnel. Focusing solely on compliance can result in security organizations overlooking and under protecting valuable data.

Solution: Recognize and accept that compliance is a starting point, not the goal Data security organizations must establish strategic programs that consistently protect their business’ critical data, as opposed to simply responding to compliance requirements. Data security and protection programs should include these core practices:

- Discover and classify your sensitive data across on-premises and cloud data stores.
- Assess risk with contextual insights and analytics.
- Protect sensitive data through encryption and flexible access policies.
- Monitor data access and usage patterns to quickly uncover suspicious activity.
- Respond to threats in real time.
- Simplify compliance and its reporting.

The final element can include legal liabilities related to regulatory compliance, possible losses a business can suffer and the potential costs of those losses beyond noncompliance fines. Ultimately, you should think holistically about the risk and value of the data you seek to secure.

Previous Next