Governance + Compliance
Issue 3 | April 2023

Tech revolution

The magazine of the
Chartered Governance Institute UK & Ireland

9 772051 265233 02
UK £8.99

Cybersecurity misconceptions

Organisations often mistakenly think that cybersecurity regulations are there to protect them when in fact they are there to protect the data.

JORDAN DURHAM
SECURITY OPERATIONS PRODUCT SPECIALIST, ECLECTICIQ

As the world becomes increasingly interconnected and reliant on digital systems and applications, cybersecurity has become a critical concern for organisations. To address this concern and prevent a 'wild west' scenario, governments, industry think tanks and regulatory bodies have developed cybersecurity compliance standards to help organisations achieve the highest levels of resilience.

Although these standards have been widely adopted, there is a common misconception that they are there to protect organisations when, in fact, they are about protecting the data. The rising level of cyber threats calls for the development of a more comprehensive and dynamic cyber resilience strategy, applicable to the whole business.

The end goal of compliance standards

Organisations must follow compliance standards to perform certain activities, and these may vary between locations. If you hold patient data in the USA, you must be **HIPAA** compliant; to perform card payment transactions, you must be **PCI-DSS** compliant; to store or transfer the personal data of **EU** citizens within or out of the EU, you must be **GDPR** compliant.

Data is the core focus of these standards, with organisational or user-based protection coming as a by-product of the controls placed around it.

Assumed breach versus breach prevention

As our dependence on informational systems increased exponentially over the last two decades, our approach to protecting these systems had to change. Cybersecurity teams now operate under an 'assumed breach' methodology that replaced the previously used 'breach prevention' methodology.

Adopting the 'assumed breach' method forces you to consider potential scenarios for when you will be breached – because you will be – ahead of time, not after the event. As part of this methodology, you need to be cognisant of what could happen to your business-critical resources post-breach, including data – usually considered one of the most valuable.

Any organisation dealing with sensitive or standards-controlled data needs to prepare for a data-breach scenario and assess the potential impact on the organisation, its staff and stakeholders, including partners and customers. This is often thought of as a self-protection strategy but, again, data protection remains front of mind. Corporate self-protection is simply a by-product.

Adopting an 'assumed breach' mindset offers many benefits. It requires senior management to develop greater situational awareness of their business functions, the relationships between the different departments and the way data is being communicated and stored. These efforts go beyond any compliance control. When you are eventually breached, your ability to identify, contain and respond appropriately will save you, not your successful compliance audit.

A proactive cyber defence strategy

In the world of cybersecurity, nothing stays still. This also applies to the regulatory standards that govern cybersecurity practices. Emerging technologies and the inventiveness of malicious actors demand constant review and improvement of regulations. As data becomes more and more valuable so will the protections and controls around it.

However, experience shows that cybersecurity standards are usually updated by regulators every five or six years, which does not allow them to keep up with the fast-paced change of technology and malpractices.

The cause for this delay is that regulators need to build frameworks which can be widely adopted and which account for the majority of threats faced by their subscribers. To offset this lack of regulatory flexibility, organisations must take the necessary time to research, test and then implement controls.

A little discussed side-effect of this long review cycle is that if one of the core controls is proven to be easily breached, then any organisation adhering to that control becomes an easier target for malicious actors. In these situations, quick changes are required by the end organisations to patch the controls and maintain security and compliance. However, these can often leave unintended gaps because of hurried fixes. An example of this could be moving a public-facing webserver behind a newly implemented firewall with next-generation security technologies but, if this hasn't yet been moved into full production and is running a vulnerable software version, that can leave it open to exploitation.

By implementing different methods of control, regulators can break the cycle of technology vendors focusing on check-box solutions which solve the controls outlined in popular frameworks. Such is the requirement for fulfilling these compliance obligations, more holistic cybersecurity programs are overlooked by organisations as there are only so many hours in the day and pounds in the budget.

Dynamic controls

Regulators have the power to drive the cybersecurity industry forward by implementing controls that are designed to be updated on a regular basis and by updating these individual controls rather than the whole standard. Dynamic controls implemented by companies in addition to compliance standards can provide an extra layer of protection in a way that allows for greater flexibility and adaptability to the surge of new technology innovations and malware threats.

Companies need to go the extra mile to make sure data is protected, not by simply ticking the 'compliance' box but by developing situational awareness around their cyber vulnerabilities through the implementation of appropriate cyber threat intelligence tools.