# Beyond Compliance: Building 360-Degree Cyber Resilience for Society

28 AUGUST 2026

**Burak Baran**

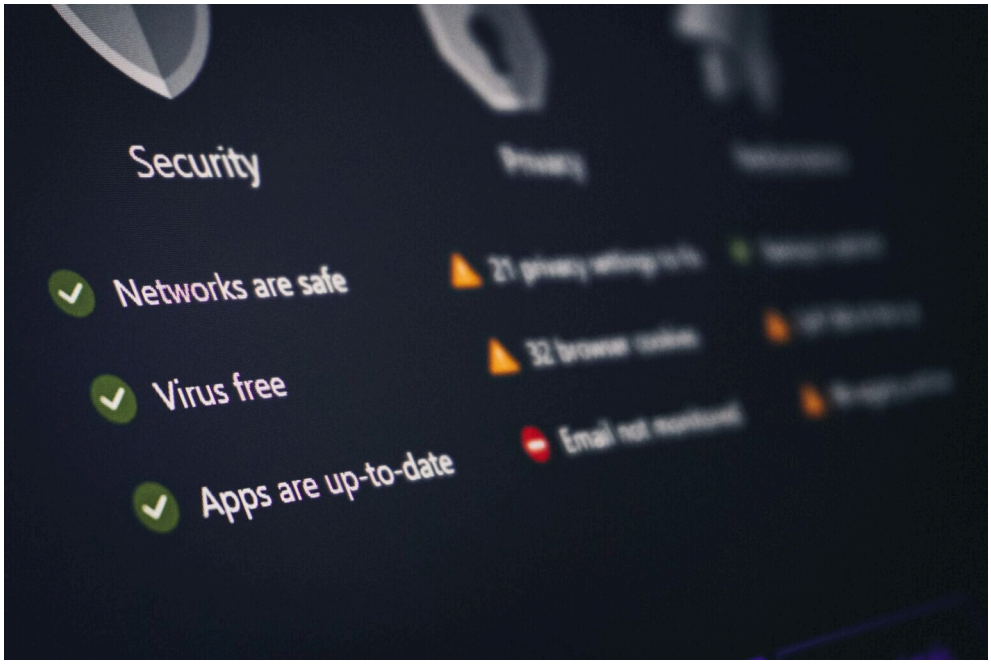


Photo by Zulfugar Karimov on Unsplash

Cybersecurity is no longer measured by the capability to prevent attacks. We now face cyber threats, evolving technologies, expanding regulatory obligations, and campaigns threatening critical infrastructure and supply chains. Governments and regulators are therefore introducing stricter frameworks.

Compliance used to be an exercise through meeting requirements and passing audits. That is no longer enough. Regulations place importance on risk management, preparedness, resilience and accountability. Continuity is essential, but no longer sufficient. An organisation's failure can extend beyond its own systems. If an energy provider or transportation company suffers an attack, consequences can escalate.

This shift has given rise to a 360-degree resilience, an approach that shifts beyond prevention to preparedness, response, recovery and improvement. Governments cannot always expect organisations to inter-

nalise risks independently, so they establish minimum expectations to ensure accountability.

Compliance is no longer about ticking boxes or passing audits. Organisations and institutions are expected to understand why regulations exist and apply them in a way that follows their rules and intended purpose.

### Understanding today's regulatory landscape

European governments introduced binding frameworks that establish minimum requirements for cybersecurity and resilience in public and private sectors. While each addresses different aspects of cyber risk, they share the common aim of strengthening governance, protecting infrastructure, improving operational resilience and ensuring continuity.

The General Data Protection Regulation (GDPR) forms the foundation of the EU's data protection framework. It governs how organisations collect, process, store and transfer personal information, while requiring appropriate security measures, breach reporting within 72 hours and organisational accountability.

Network and Information Security 2 Directive (NIS2) expands the original NIS Directive to sectors including energy, transportation, healthcare, banking and public administration. It introduces stricter obligations for risk management, incident reporting, continuity and accountability.

Complementing NIS2, the Critical Entities Resilience (CER) Directive focuses on keeping critical infrastructure operational during disruptions. It covers various sectors, requiring risk assessments, resilience measures, continuity planning and preparedness. CER shows the shift toward 360-degree resilience and how critical entities must protect their IT environments and the services that are essential.

The Cyber Resilience Act (CRA) addresses cybersecurity from a product perspective. It establishes requirements for hardware and software products sold in the EU. It requires manufacturers to integrate security throughout the product, addressing vulnerabilities and adopt secure-by-design principles.

In the financial sector, Digital Operational Resilience Act (DORA) establishes a framework for Information and Communications Technology (ICT) risk management. It requires ICT risk management, resilience testing, third-party monitoring and significant incident reporting.

Together, all of the mentioned frameworks represent a shift towards proactive governance, embedding security, resilience and risk management into everyday operations.

### Compliance vs. security

Compliance concerns how good an organisation follows requirements, while security focuses on protecting systems, networks, data and assets. Compliance establishes the minimum; security is a continuous process. An organisation can therefore comply with regulations and remain insecure.

Traditionally, organisations treated compliance as the primary aim of cybersecurity, focusing on passing audits and implementing measures. While those measures reduced risk they didn't really protect them against modern threats. Attackers don't research whether organizations passed an audit or not; they exploit vulnerabilities, weak governance and human error.

For example The Marriott data breach has shown the limitations of a compliance-oriented approach. Even with having security measures up to the standards, weaknesses in its systems remained unaddressed, allowing attackers to exploit vulnerabilities and remain undetected. The UK Information Commissioner's Office concluded that several weaknesses could have been identified using only standard tools.

Modern frameworks treat compliance as the foundation of cybersecurity. This distinction is important especially for resilience. Continuity may restore operations, but may fail to consider how disruption affects the society. As a result, organizations must understand not only what regulations require, but why those requirements exist and which risks they aim to address.

**Leadership and governance in the regulatory era**

Cybersecurity has become a national security concern, hence responsibility has expanded to governments, institutions and authorities. Effective cyber resilience requires strategic decision-making, coordination and governance. Governments should develop strategies, establish frameworks, coordinate incident responses, allocate resources and cooperate with infrastructure operators.

Good governance also requires collaboration. Much of a country's infrastructure is operated by private entities. As a result, governments need partnerships that enable information sharing, coordinated responses and joint planning.

Cyber resilience is a measure of state capacity. Governments that invest in leadership, coordination and adaptive governance are to withstand disruptions, protect citizens and maintain public trust.

**Building a 360-degree resilience strategy**

Building cyber resilience at the state level requires a departure from traditional approaches to preparedness, response, recovery, and adaptation. Since no government can guarantee full protection against cyberattacks, states must instead focus on ensuring that critical systems remain operational.

A 360-degree resilience strategy takes a whole-of-system and whole-of-society perspective. For corporations, resilience doesn't stop at organisational boundaries; they must understand how a disruption in their services could affect suppliers, customers and wider systems. From a

state perspective, resilience means anticipating threats, maintaining operations, restoring services and learning from past incidents.

Strategies now integrate cybersecurity into national security, economic planning and public governance. New strategies include protecting critical infrastructure, improving incident response, investing cybersecurity and developing coordination mechanisms between actors.

Preparedness requires governments to conduct risk analysis, national strategies, crisis procedures and exercices. States must restore services, investigate incidents, strengthen measures and adapt policies to emerging threats.

## 6. Concluding Remarks

Cybersecurity is a fundamental problem of national security, stability, governance and resilience. Critical services depend on private infrastructure, meaning a company's failure can have consequences in the whole society.

This makes the distinction between business continuity and 360-degree resilience more important than ever. Business continuity focus on keeping an organisation functional, while 360-degree resilience considers how disruption affects wider society through a whole-of-society perspective.

The future of cybersecurity should be understood through comprehensive resilience. Organisations must ask whether they can anticipate, withstand, respond to, recover from and adapt to disruptions while limiting consequences for the systems and society that depend on them.

The objective of 360-degree resilience is not simply to keep business running; it is to keep society functioning.