WHY THE ICT INDUSTRY SHOULD PREEMPT GOVERNMENT MANDATES FOR QUALITY AND SECURITY STANDARDS

The CrowdStrike outage of 2024 highlighted significant vulnerabilities in the information and communications technology (ICT) industry, exposing just how devastating a single quality failure can be. This incident caused widespread disruptions across critical infrastructure systems, affecting airlines, hospitals, banks, and government agencies. While the outage wasn't the result of a security breach, it shared several hallmarks of a cyber incident or a DDoS attack, including widespread system crashes, service disruptions across critical industries, and a prolonged recovery period that left organizations vulnerable and scrambling to restore operations.

As ICT service providers and their solutions partners evaluate this incident and create their plans to prevent quality and security issues from arising in the future, two options are emerging. They can either follow a proactive, industry-led approach like the telecommunications industry did in the 1990s or wait for government mandates to dictate quality and security requirements. In this article, we'll explore these two options.

To learn more about how quality frameworks like TL 9000 can help mitigate future outages and drive resilience across today's ICT systems, read our white paper on the 2024 CrowdStrike incident.

THE TWO APPROACHES TO QUALITY AND SECURITY: INDUSTRY-LED VS. GOVERNMENT-MANDATED STANDARDS

As the ICT industry looks for ways to prevent the next CrowdStrike incident, we see two distinct paths forward. One is a proactive approach, where providers collaborate to establish, maintain, and enforce their own quality and security standards. The other path relies on government mandates, where external regulations dictate how ICT organizations must operate to combat risk. Understanding how these approaches differ offers valuable lessons for today's ICT leaders.

THE TELECOMMUNICATIONS INDUSTRY'S PROACTIVE MODEL

In response to rapid growth and innovation in the 1990s, telecom providers faced new challenges as traditional circuit-switched networks rapidly evolved to support advanced services like dial-up Internet, enhanced voice features, and emerging digital communication technologies. This surge in innovation introduced new complexities and quality risks that threatened service reliability.

Rather than waiting for regulatory pressure, the industry collaborated to proactively implement the TL 9000 standard. This effort led to significant measurable improvements in the telecommunications industry that continue today. For example, according to data from TIA QuEst Forum:

- Major problem reports for edge routers declined by 90%
- Defective software fixes for edge routers dropped from 4.5% to 0.2%
- Hardware return rates improved by up to 90% for WLAN base station equipment
- Software fix quality improved by approximately 90% for wireline software
- Smartphone return rates dropped by 35%

By acting decisively before government mandates were introduced, telecom providers shaped their own quality standards, maintained control over implementation, and tailored standards to their specific operational requirements.

THE GOVERNMENT-MANDATED APPROACH

While the telecommunications industry proactively addressed quality concerns through collaboration and self-regulation, the ICT sector may find itself facing increasing external pressure. Governments worldwide are beginning to mandate security frameworks across a range of critical services – including ICT– due to growing cyber threats and infrastructure vulnerabilities:

- In the United States, Congress is investigating the 2024 Salt Typhoon cyberattacks and discussing potential actions with agencies like the FCC to implement stricter regulations. While formal mandates have yet to be enacted, the heightened scrutiny suggests that new cybersecurity requirements could soon become inevitable for ICT providers.
- Standards such as CISA's Cybersecurity Framework and the NIST SP 800 Series are becoming foundational for securing ICT services.
- Government-funded programs like the BEAD NOFO (Broadband Equity, Access, and Deployment Notice of Funding Opportunity) in the United States are coupling cybersecurity requirements with grant applications, signaling that future funding may increasingly be tied to compliance with certain security standards.

- The European Union's NIS2 Directive expands cybersecurity requirements across essential sectors, including energy, transportation, banking, financial market infrastructures, drinking water, healthcare, and digital infrastructure.
- Costa Rica has become the first country in Latin America to mandate that vendors certify to the SCS 9001 Supply Chain Security standard and other security frameworks, following a series of cyberattacks in 2022 that compromised critical infrastructure.

THE CHALLENGES OF GOVERNMENT-MANDATED APPROACHES

There are several issues with following a government-mandated approach to quality and security standards for mission-critical ICT services. The first is time: it can take years for governments to create and implement policies, and those policies can change as administrations come and go. While the ICT industry waits, the risks of the next incident only increase – and so, too, does the potential for reputational damage, economic losses, and security issues.

Control is another factor: government mandates don't always accommodate the business and service realities of the companies being regulated. This can lead to quality standards that are either ineffective or impractical to follow. Finally, there's the issue of competitive advantage. Since government regulations tend to vary from one country to another, the likelihood is high that there will be inconsistencies and gaps with government-mandated standards that leave some providers or vendors in a stronger position than others.

A DEFINING MOMENT FOR ICT TO LEAD ON QUALITY AND SECURITY

With so much innovation happening in the ICT sector, the time for an industry-led approach to quality and security is now. New and unproven suppliers seemingly enter the market every day. Networks are undergoing tremendous change as disaggregated architectures and software-defined approaches become commonplace. And device proliferation continues as the Internet of Things (IoT) and mobile technologies move from nice-to-have commodities to strategic infrastructure components. Much like the telecommunication bubble of the 1990s, all this innovation creates the potential for security and quality issues that can significantly impact mission-critical ICT services.

The telecom industry's successful adoption of TL 9000 provides a clear model for the ICT sector to follow today. TIA QuEST Forum offers ICT providers the tools they need to manage both quality and security end-to-end – on their own terms. With the TL 9000 quality standard and the SCS 9001 framework for addressing cybersecurity and supply chain risks, the ICT industry can lead the way to reducing risk, while gaining:

- **Control over compliance:** Voluntary adoption allows ICT suppliers to implement standards on their terms, avoiding rushed responses to government-imposed regulations.
- **Stronger supplier relationships:** Requiring adherence to consistent quality standards across partners instills consistency and quality within the ICT supply chain.
- **Competitive advantage:** Early adopters position themselves as ICT industry leaders, earning trust from customers and regulators.

Learn More Today

For an in-depth analysis on how the right quality framework can help prevent future ICT disruptions, be sure to read the full white paper here. If you're ready to take proactive steps and get started with TL 9000 or SCS 9001 certification, or if you'd like to get involved and help shape the future of ICT quality and security standards, contact us today at membership@tiaonline.org.