TIA QuEST Forum
Telecommunications Industry Association
TECHNICAL BULLETIN
TIAonline.org / @TIAonline

How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Aligns with the Findings and Recommendations of IBM Security's Cost of a Data Breach 2021 Report

July 29, 2022

Executive Summary

IBM Security, leveraging research by the Ponemon Institute and data from 537 real-world cyber-attacks, has produced an annual *Cost of a Data Breach Report* (the "Report") for 17 consecutive years. It has become a leading benchmark for the cybersecurity industry.

The Report touches upon many factors that helps organizations mitigate the rising cost of data breaches. It provides analysis and key metrics on cyber-attacks of various types and the resulting costs to impacted organizations. This year's Report states that data breach costs have risen to an average of $4.24M USD, the highest average cost in the history of the report.[1] Additionally, the average time to identify and contain a breach is the highest in the history of the report.

This TIA Technical Bulletin provides an overview of the findings and recommendations of the Report and how the TIA QuEST Forum's SCS 9001 Supply Chain Security Standard aligns with the findings and recommendations of the Report and can play a useful role in mitigating cyber-attacks.

[1] As stated within the Report, it is a global report, combining results from 537 organizations across 17 countries and regions, and 17 industries to provide global averages.

Introduction to the Telecommunications Industry Association (TIA)

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents more than 400 global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs, standards development, and business performance solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI) and is active in developing and promoting international standards.

TIA QuEST Forum brings together companies from around the world who manufacture, deploy and operate cutting edge networks, to develop process-based industry standards and tools to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA's QuEST Forum community built and maintains the ICT industry's most prominent quality standard – TL 9000. As part of our commitment to ensuring global networks are reliable, trusted and secure, TIA QuEST Forum has released the "SCS 9001 Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry and benchmarks performance to drive continuous improvement. This standard provides value to network operators of all types and developers and manufacturers of products and services used within those networks.

How SCS 9001 Aligns with Findings of IBM's Cost of a Data Breach Report

2021 Report Finding	TIA QuEST Forum SCS 9001 Alignment
Regulatory Compliance Failures Out of a selection of 25 cost factors that either increase or mitigate data breach costs, compliance failures was the top failure that increased costs.	SCS 9001 requires that organizations document their security policies and that they are reviewed at least annually for effectiveness and adherence with all relevant legal, statutory, and / or regulatory compliance obligations.
Initial Attack Vectors A variety of attack vectors were identified with a review of and costs experienced by the victimized organizations. Examples include compromised credentials, phishing attacks, 3rd party software vulnerabilities, lost data / device, physical security compromise and malicious insider activities.	SCS 9001 has defined processes and specific controls and measurables that address all of these attack vectors. Certification to SCS 9001 would be beneficial in helping to alleviate the potential of these attacks and the costs incurred if any were successful.
Zero Trust Architecture The Report finds that organizations who have deployed or are in the process of deploying a ZTA experience costs of breaches 42% less than those who do not. The Report further notes that only 35% of respondents have deployed or plan on implementing a ZTA.	SCS 9001 requires that organizations develop a plan to deploy a network architecture based on Zero Trust principles such as described in NIST SP 800-20 and that the plan be considered a living document, reviewed, and updated at least annually.
Incident Response The time to detect and contain incidents rose to the highest level recorded since the inception of the Report.	SCS 9001 requires that organizations establish Incident Management, Incident Response, and Incident Reporting processes, that such processes are tested, and that employees are properly trained in their execution.
Compliance Failures Organizations with frequent compliance failures experience over 50% higher costs associated with breaches.	SCS 9001 requires that organizations establish Security Policies that are reviewed at least annually to ensure its continuing adherence to corporate security strategy and applicability to legal, statutory, and / or regulatory compliance obligations.
Encryption Organizations using a high level of encryption experience nearly 30% reduction in costs associated with breaches.	SCS 9001 requires that organizations establish a NIST FIPS cryptography standard – or equivalent – as well as Cryptographic Control and Access Control Policies to protect all device types and data assets both at rest and in transit.

Security Automation Security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of incidents and intrusion attempts. The Report further finds that largest gap of cost exposure of any of the attack vectors for organizations who have deployed security automation, versus those who have not.	SCS 9001 requires that organizations deeply instrument their operations in areas such as monitoring asset access, creating logs of administrative actions, network traffic, and automated equipment identification be used as a method of connection authentication, amongst other requirements.
Remote Work Organizations with remote workers experience nearly 25% higher cost and 10% longer time to resolve cyber-attacks.	SCS 9001 requires that organizations establish a Workspace Policy covering remote work and system access, assurance through multi-factor authentication, and that remote sessions are actively monitored.

How SCS 9001 Aligns with Recommendations of IBM's Cost of a Data Breach Report

The Report provides seven specific recommendations to help minimize the financial impacts of a data breach. The table which follows lists the recommendations along with the strong alignment of SCS 9001.

2021 Report Recommendation	TIA QuEST Forum SCS 9001 Alignment
Invest in security orchestration, automation and response (SOAR) to help improve detection and response times.	SCS 9001 requires extensive environment monitoring to detect anomalous behaviors within network sessions and user activity.
Adopt a zero-trust security model to help prevent unauthorized access to sensitive data.	SCS 9001 requires that a ZTA implementation plan be established, and progress assessed at least annually.
Stress test your incident response plan to increase cyber resilience.	SCS 9001 requires that the organization establish an Incident Response process and that it be tested at least annually.
Use tools that help protect and monitor endpoints and remote employees.	SCS 9001 promotes modern tooling to monitor endpoints including the ability to update and wipe sensitive data.

Invest in governance, risk management and compliance programs.	SCS 9001 can be an effective global standard in achieving the goals of the referenced programs.
Embrace an open security architecture and minimize the complexity of IT and security environments.	SCS 9001 offers controls to enable open architectures and promotes leverage of advance tooling and regular tests to ensure security goals are met, including that of suppliers.
Protect sensitive data in cloud environments using policy and encryption.	SCS 9001 defines Access Control Policies for all assets with encryption of data in transit and at rest and that inter-process communications across network boundaries be protected.

Questions? Want more information about TIA QuEST Forum's SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

References

- NIST NISTIR 8276:
  Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (nist.gov)
- U.S. Government BEAD Program
  Broadband Equity, Access, and Deployment (BEAD) Program | BroadbandUSA (doc.gov)
- BEAD Program Notice of Funding Opportunity (NOFO)
  BEAD NOFO.pdf (doc.gov)