Achieving Cyber Compliance

About the Document

This document describes the regulatory imperatives for implementing cyber compliance capabilities. In addition, it includes fundamental questions IT organizations must be able to answer to achieve cyber compliance (i.e., the integration of trade compliance controls into IT systems). These questions are informed by regulatory requirements and regulator expectations (as expressed through Consent Agreement requirements and published guidelines).

Acknowledgements

On October 27, 2015, the author had the pleasure of moderating the *IT Security & Export Compliance: Staying Current with Evolving Threats* panel at SIA's Fall Conference. The panel consisted of Gary Stanley (President at Global Legal Services), John Landwehr (VP & Public Sector CTO at Adobe), and Jonathan Priganc (Manager, International Trade Compliance-IT at UTC Aerospace Systems)[1], each a thought leader and accomplished professional in their respective fields. The hours of discussions preparing for the panel, and the panel itself, inspired the writing of this paper.

Gary Stanley's legal insights into the cyber compliance considerations of the DFARS, ITAR and EAR were extremely informative. The DFARS insights included in this paper are based on Gary's original research, which was delivered in the panel presentation. John Landwehr's observations regarding today's cutting-edge data protection practices, techniques and technologies provided insight into the future of cyber compliance. Jonathan Priganc's extensive hands-on experience provided practical, real-world insights into how a large and complex Aerospace and Defense company is implementing cutting-edge cyber compliance controls. The level of professionalism and dedication demonstrated by the panelist was exceptional, as were their inputs. Each panelist has earned the author's highest endorsement.

[1] Since this white paper was initially drafted, Jonathan Priganc has joined the TCEngine Team.

Trends in Cyber Compliance

U.S. regulatory enforcement activities are trending towards cyber compliance. Recent updates to the Defense Federal Acquisition Regulation Supplement (DFARS) (1) include requirements for *Safeguarding Unclassified Controlled Technical Information* (78 Fed. Reg. 69,273) and (2) revise DoD Defense Industrial Base Cybersecurity Activities Regulation (80 Fed. Reg. 59581) to mandate reporting of cyber incidents. DFARS 204.7301 defines a cyber incident as, "*actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.*"

From the perspective of US export regulations, export control requirements have always applied to "Technical Data," whether the data exists in hard-copy or electronic format. However, US export enforcement and compliance efforts have traditionally focused on controlling exports resulting from physical access (e.g. foreign person employees, foreign person visitors, etc.) and physical transfers (e.g. shipments, hand-carries, etc.).

As business operations evolved to become globally-networked and information-driven, organizations' export compliance programs remained focused on the physical domain. Thus, many organizations have yet to implement adequate cyber compliance programs. As a result, these organizations are regularly discovering and voluntarily reporting cyber compliance incidents to the US Department of State Directorate of Defense Trade Controls (DDTC), the U.S. regulator responsible for the International Traffic in Arms Regulations (ITAR).

In response to the increasing trend in cyber compliance incidents, DDTC has begun including cyber compliance requirements in punitive actions known as Consent Agreements. To summarize Consent Agreement cyber compliance mandates, DDTC requires companies to implement capabilities for identifying, controlling and tracking regulated information in IT networks and systems. Although not codified in regulation, these requirements represent DDTC's cyber compliance expectations.

Achieving Cyber Compliance

In simple terms, achieving cyber compliance requires organizations develop capabilities to identify what data is subject to what regulations and implement controls governing the location, access and transfer of regulated data. Answers to the following questions indicate an organization's cyber compliance capabilities and gaps.

1. **Export Control Program** – does your organization have the ability to readily identify:
    - **a.** Export control requirements, and
    - **b.** Export control standard work?
2. **Business Landscape Management** - does your organization have the ability to readily identify:
    - **a.** Legal Entities,
    - **b.** Management Structure, and
    - **c.** Organizational Structure?
3. **Infrastructure** – does your organization have the ability to readily identify:
    a. The companies that own, operate and service your IT infrastructure, to include the cloud and Disaster Recovery, and

   b. The geographic location, to include country, where the IT infrastructure is located?
4. **Networks** – does your organization have the ability to readily identify:
   a. The networks on which infrastructure resources reside, and
   b. The processes by which new infrastructure, applications and users are being provisioned/de-provisioned in the network(s)?
5. **Applications** – does your organization have the ability identify:
   a. The applications containing regulated data and the infrastructure on which it resides, to include network file drives, email, collaboration suites (e.g. SharePoint), Customer Relationship Management (CRM), Product Lifecycle Management (PLM), Software Development Lifecycle (SDLC), Enterprise Resource Planning (ERP), Supplier Relationship Management (SRM), Manufacturing Execution Systems (MES), Quality Assurance Systems (QAS), etc.?
6. **Administration** – does your organization have the ability to identify:
   a. The personnel who administer infrastructure, networks and applications, to include identity attributes such as employer, geographic location, citizenship, etc.?
7. **Users** – does your organization have the ability to identify:
   a. Employees who have access to infrastructure, networks, and applications,
   b. Contractors who have access to infrastructure, networks and applications, and
   c. External Business Partner personnel who have access to infrastructure, networks and applications?
8. **Data** – does your organization have the ability to identify:
   a. What data is subject to regulatory control,
   b. When data is regulated, the specific jurisdiction, classification and marking controls to which the data is subject, and
   c. To identify data and the related regulatory controls for both structured and unstructured data?
9. **Authorizations** – does your organization have the ability to identify:
   a. Applicable authorizations (e.g. internal policies, DSP-5s, TAAs, etc.) that define compliant location, access and transfer criteria?
10. **Integrated Controls** – does your organization have the ability to identify:
   a. Authorized regulated data creation and storage locations (infrastructure, networks and applications),
   b. Compliant user access control mechanisms (infrastructure, network, application and data-level),
   c. Compliant administrator access control mechanisms (infrastructure, network, application and data-level), and
   d. Authorized regulated data transfer mechanisms (e.g. encrypted email, authenticated portal, etc.)?

Conclusion

The world in which we operate is globally-networked and information-driven. Organizations and regulators have not traditionally focused on cyber compliance considerations and requirements. The growing trend in cyber incidents is prompting both organizations and regulators to focus on implementation of cyber compliance controls. To achieve cyber compliance, organizations must implement capabilities to compliantly manage infrastructure, networks, applications, administrators, users, data, authorizations, and implement integrated cyber compliance controls.

About the Author

Matt Henson is a Trade Compliance professional who has spent his career working at the intersection of global commerce, international trade regulations, and Information Technology (IT). He specializes in cyber compliance (i.e., the integration of trade compliance controls into IT systems). Matt may be reached at matt.henson@TCEngine.com.