Cybersecurity Compliance: A view from the trenches

Sam Morthland
February 26, 2020
Overview

• A bit of history
• Notes from the Field
• CMMC 1.0 Released – Now What
• Recommendations for Businesses
Cybersecurity Compliance

A bit about us…

• Veteran Owned Small Business, established in 2011, previous DOD cybersecurity and intelligence members

• Payment Card Industry (PCI) - Qualified Security Assessor (QSA)
  • 1 of 147 US-based Assessors

• Federal Risk and Authorization Management Program (FedRAMP) accredited Third Party Assessment Organizations (3PAO)
  • Accredited by American Association for Laboratory Accreditation (A2LA) to ISO/IEC 17020:2012, Requirements for bodies performing inspection
  • 1 of 38 Federally approved FedRamp 3PAOs

• 8 years of serving the financial, commercial and Federal markets
Cybersecurity Compliance

A bit of History…

- DFARS 252.204-7012 (Final Rule Oct 2016)
  - All DOD contractors to be compliant to NIST 800-171; **NLT 31 Dec 2017**
  - Self Attestation of compliance - Required documents: SSP and POAM

- US Navy Sea Dragon Breach – Jul 2018

- MITRE’s “Deliver Uncompromised” - Aug 2018

- Geurts Memo – Sep 2018
  - Imposing enhanced security controls on “critical” Navy programs

- Mar 2019 - The Office of the Assistant Secretary of Defense for Acquisition began the process of creating the Cybersecurity Maturity Model Certification (CMMC)

- Jul 2019 - Defense Contract Management Agency (DCMA) assessing contractor compliance with DFARS Clause 252.204-7012 and NIST SP 800-171 as part of review of contractor purchase systems

- Sep 2019 - Navy Marine Corps Acquisition Regulation Supplement (NMCARS) changes to make cybersecurity compliance as a “material requirement”
  - KOs consider the **right to reduce or suspend** progress payments for contractor noncompliance
  - Reinforces, that “A contractor MUST make their SSP available to the contracting officer within 30 days of contract award and be ready to host the contracting officer for a review of the SSP at the contractor’s facility.”

- Jan 2020 – CMMC 1.0 released, to be implemented thru 2025
Cybersecurity Compliance

**Reality Check Report**

- Developed May 2019 report from incident response and assessment data from the previous 2 years
  - Provided an assessor’s view of compliance in the DIB
- Provided a snapshot of compliance and identified areas for DIB companies to focus efforts and resources
- No companies were 100% compliant
UNFORTUNATELY IN A YEAR VERY LITTLE HAS CHANGED!
Most Companies still fail to implement 16 controls
Larger issues with implementing NIST SP 800-171

• Misunderstanding the controls
  • Many IT personnel are fully engaged in support of the availability of the network. Seeking to discern meanings from government policies tends to be low on their list of priorities

• Cultural issues
  • Security is not seen as a profit driver – significant additional costs
  • Security requires change – changing people’s access levels

• Cloud Services
  • Enable centralized storage of documents in a secure environment – BUT minimally secure regarding outside access, requires additional controls
  • Many cloud services in use are not FedRAMP Moderate baseline compliant
Cybersecurity Compliance

Any Company Vulnerable to Attack

• Electronic Warfare Associates (EWA) suffered a ransomware infection in Jan 2020
  • a 40-year-old a well-known US government contractor
  • Among the systems that had data encrypted during the incident were the company's web servers.
• Signs of the incident are still visible online
  • Encrypted files and ransom notes were still cached in Google search results, even a week after the company took down the impacted web servers
Cybersecurity Compliance

**Incident Response Findings**

- In most cases, 800-171 controls would have prevented a breach or significantly reduced the impact.

- In particular,
  - Lack of MFA (3.5.3)
  - Untrained users (3.2.1)
  - Poor patch management (3.11.3)
  - Lack of Audit Logs (3.3.1)
Cybersecurity Compliance

**CMMC 1.0 Released – Now What?**

- Standard out, more to follow
- Companies clamoring to get certified – waiting on auditors
- Companies want to be auditors – waiting on certification program
- Some companies just now understanding existing requirements of FAR 52.204-21 or DFARS 252.204-7012
- Some companies still unaware of need for compliance
  - “We don’t have any CUI...whatever that is”
  - Disconnect from Privacy Act and other PII protection regulations
Cybersecurity Compliance

Why is this important to Small/Medium Businesses

• Protect what you have built
• Comply with existing contracts - DFARS 252.204-7012, etc.
  • Avoid violation of False Claims Act
• Prevent catastrophic losses due to:
  • Theft of data (IP, CUI) or encryption of all company data due to ransomware
  • Loss of reputation with customer (1 to 6 rule, amplified with social media)
  • Financial loss (reimbursement, remediation, lost revenue, additional security)
  • Operational disruption (loss of data, stand-down during remediation)
  • Legal ramifications (FCA claims, PII claims, etc.)
• Average Cost of a Breach in 2019, company >500: $2.74 million*

(*Cost of a Data Breach Report, IBM Security, Jan 2020)
Cybersecurity Compliance

Recommendations for Businesses

• Find your SSP and complete actions in POAMs to comply with 800-171r2
  • Best preparation for CMMC in Oct 2020

• Budget for cybersecurity
  • Labor, Vulnerability Scans, Pen Tests, internal/external audits

• Ensure cybersecurity is a team effort – Admin, Intel, Ops, and IT
  • Put your Cybersecurity Support POC on speed dial

• Run your Incident Response Plan w/Key Players – desktop exercise

• Treat Cybersecurity like you do ISO – C-Suite led, monthly metric reviews, documentation reviews, internal audits

"An ounce of prevention is worth a pound of cure."
Benjamin Franklin
Cybersecurity Compliance

Sam Morthland
Partner & Chief Financial Officer
sam.morthland@sera-brynn.com
703-988-5764