HCRS

Cybersecurity Checklist *for* All Business Owners

Best Practices & CMMC Compliance

Visit: HealthcareResolutionServices.com

Overview

Recent changes to the **Cybersecurity Maturity Model Certification (CMMC)** are likely to be adopted across multiple industries. In order to improve your data management and protection, we'd like to share how CMMC has evolved, 10 tips you can use to meet its requirements, and three main security best practices you can implement today.

Table of Contents

Key Takeaways

Current Cyber Threats and Ransomware

Ransomware and malware incidents are on the rise, and most healthcare organizations have already experienced some form of digital attack.

CMMC: Past and Present

The most recent updates for CMMC are meant to make the certification process easier to follow, while maintaining a fair and balanced series of requirements.

Steps to Cyber Resilience

If organizations want to be better protected against bad actors, they need to incorporate stronger passwords, secure data backups, and comprehensive incident response plans.

HCRS

Introduction

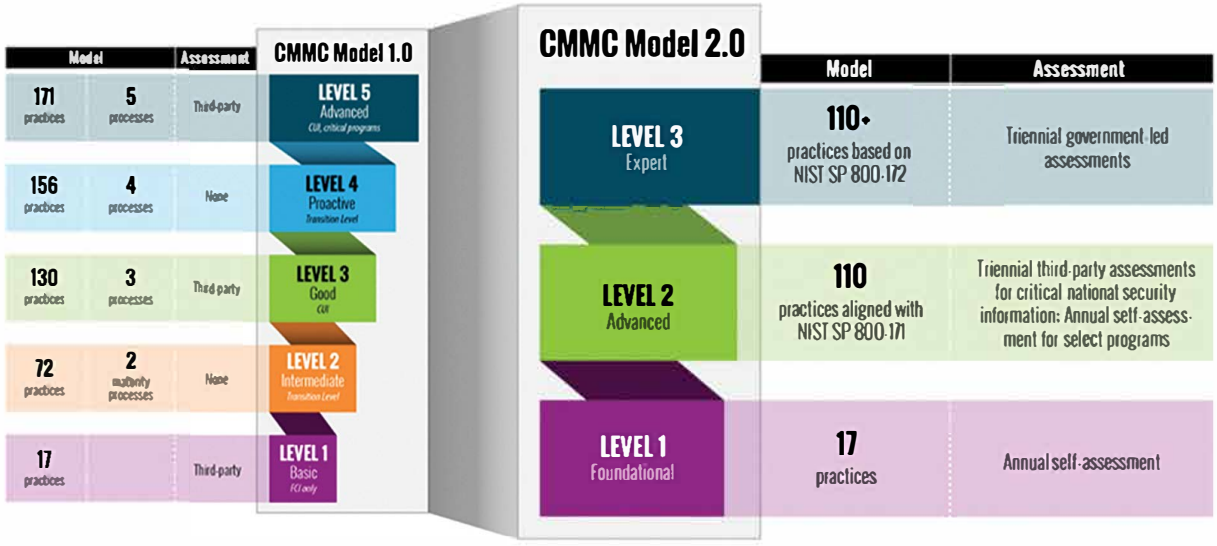
Seventy percent of cybersecurity professionals surveyed by HIMSS in 2020 reported a "significant security incident" had affected their organization, including phishing (57%) and ransomware (20%), while HHS notes that the average cost to resolve a ransomware attack is roughly $1.27 million. These incidents also risk an organization's reputation, client relationships, and — when it comes to government contracts — fines for noncompliance.

CMMC

History. CMMC's purpose is to verify that an organization has reached a certain cyber maturity through the completion of a third-party audit, rather than a self-assessment. CMMC 1.0 was originally five levels, each achieved by implementing specific practices and processes. A total of 171 practices were needed to reach Level 5.

Recent Changes. As of 2021, CMMC 2.0 is reorganized into three levels based on those original practices: 17 practices to reach Level 1, 110 for Level 2, and 110+ for Level 3. A practice is defined as a technical activity that can meet the capability needs for a specific cybersecurity domain.

KEY FEATURES OF CMMC 2.0



Source: Office of the Under Secretary of Defense. "About CMMC." www.acq.osd.mil/cmmc/about-us.html

Checklist: 10 Tips to Reach CMMC

- Invest 11-15% of annual revenue on IT and cybersecurity.
- Secure dedicated and credentialed cybersecurity resources.
- Schedule a free CMMC gap analysis.
- Seek cybersecurity liability insurance.
- Execute written cybersecurity policies and procedures.
- Document employee training on cybersecurity at initial hiring and annually thereafter.
- Know your state regulatory laws (pending and current cyber legislation), and their effective dates.
- Seek state funding for early adoption of cyber practices.
- Know what it means to self-attest and consequences for cyber breaches.
- Execute the following:
  - System Security Plan (SSP)
  - Plan of Action and Milestones (POA&Ms)
  - Supplier Performance Risk System (SPRS) score
  - Application for Level 1 compliance

Steps to Cyber Resilience

Password Length and Security. An eight-character password can be cracked in eight hours — even if it includes upper- and lowercase letters, numbers, and special characters. Adding two more characters extends that protection by at least five years. Discourage coworkers from sharing login credentials by adopting two-factor authentication, and remove any ghost accounts (active accounts that no longer have users) to close off vectors that could be compromised.

Secure Data Backups. Use *logical air gapping* to isolate on-site media hardware from your local network and the Internet. This protects hardware from outside access or ransomware. Data is only transferred through a secure networking port.

Comprehensive Incident Response Plan. This is required specifically per HIPAA, but can easily benefit any organization's capabilities for responding to a threat on their network. As HealthITSecurity explains, it should include "a data backup plan, a disaster recovery plan, and an emergency mode operation plan, among other administrative safeguards."

Industry Reports

2020 HIMSS Cybersecurity Survey
HHS Ransomware Trends 2021

About HCRS

Since 1998, HCRS has been helping customers meet their health information requirements thanks to our team of expert medical professionals, recruiters, trainers, and consultants. Headquartered in Columbia, Maryland, we've served customers at more than 100 Department of Defense and Veteran Affairs sites in more than 40 states across the U.S.

HCRS

Visit: HealthcareResolutionServices.com