Matt Santos,
Analyst and CMMC Services Consultant

Email a CMMC professional
cmmc@bv.com

The Cost of Cybersecurity and Policy Implications (CMMC)

According to the National Institute of Standards and Technology (NIST), a cybersecurity incident is a violation of "an explicit or implied security policy." Incidents are further segmented into cyberattacks and data breaches, which include attempts to access systems without authorization, unauthorized changes to software, and many others.

Overall, according to a report by the Council of Economic Advisors, it is estimated that cybersecurity incidents cost the American economy between $57 billion and $109 billion in 2016. Especially in recent years, cybersecurity issues have become more prominent. According to CNN Business, as recently as August 2021, T-Mobile suffered a breach in which over 40 million people were affected. Names, birthdates, Social Security Numbers, and other sensitive information were compromised during the breach. Besides the reputational damage, the company also saw its stock drop about 5% between August 13 and August 26.

Some areas where cybersecurity has become increasingly worrisome are those related to governments and nation-state attacks. According to CBS News, as recently as June 2021, a private company called iConstituent was targeted by ransomware. The company provides a newsletter service that U.S. lawmakers use to reach out to constituents, and nearly 60 offices in the United States Congress were targeted.

According to Business Insider, perhaps one of the most relevant incidents occurred in 2020 - when hackers breached the systems of Solar Winds, which is a large information technology firm in Texas. Hackers added malicious code into Solar Winds' software systems, which consequently affected thousands of people, companies, and government entities. The breach not only targeted companies such as Microsoft, Deloitte, Intel, and Cisco - but also affected the United States government. More specifically, the targets of the cyber-attack included the Pentagon, the Department of Homeland Security, the Department of State, the National Nuclear Security Administration, the Department of Energy, and the Department of Treasury.

Cyber capabilities are constantly evolving and are becoming more prominent in both national security and international relations. Dr. Michael McGuire, a senior lecturer in Criminology at the University of Surrey, wrote a report titled "Nation States, Cyberconflict, and the Web of Profit." He stated in his report that "the result of the trends highlighted in these findings is something entirely novel; a merging of traditional international relations with the cybercrime economy and the tools and techniques which now drive the digital underground." As a result, organizations, especially government entities, need to become more proactive in their cybersecurity efforts. With cybersecurity incidents becoming a more important issue during this era of rapidly evolving technology, especially incidents that are nation-state related, the United States government has taken notice and has sought to implement more stringent cybersecurity policies.

As highlighted in the Office of the Under Secretary of Defense for Acquisition & Sustainment, in January 2020, to combat the rise in cybersecurity incidences, the United States Department of Defense (DoD) issued initial guidelines for Cybersecurity Maturity Model Certification (CMMC)." It is a series of processes and practices that serve as a cybersecurity framework for those in the Defense Industrial Base (DIB). Federal contractors and sub-contractors will need a certain level of CMMC to bid and execute federal contracts. Although the CMMC framework builds upon NIST SP 800-171, the CMMC framework has additional requirements and cannot be achieved through self-certification (must be certified by a C3PAO).

In response to the DoD's new CMMC framework, Black & Veatch Management Consulting, LLC, has achieved accreditation as a Registered Provider Organization (RPO) from the CMMC Accreditation Body and has launched a new CMMC offering. Combining its nearly 20+ years of experience in cybersecurity with an expert team of CMMC – AB Registered Practitioners and Certified CMMC Professionals, Black & Veatch is best suited to assist your organization in preparing for your Level 1 – 3 CMMC assessment.

Sources

- Council of Economic Advisors
- CNN Business
- CBS News
- Business Insider
- Nation States, Cyberconflict, and the Web of Profit
- Office of the Under Secretary of Defense for Acquisition & Sustainment

Learn more at

innovate.bv.com/cybersecurity

BLACK & VEATCH
MANAGEMENT CONSULTING