CENTRE
LAW & CONSULTING

Insights

How Mature Should My Cybersecurity Program Be?

By Brandon Graves

How Mature Should My Cybersecurity Program Be?

The Risks in Selecting the Wrong Cybersecurity Maturity Model Certification Level.

The Department of Defense's Cybersecurity Maturity Model Certification (CMMC) and related interim rules have focused government contractors' attention on cybersecurity. The time required to establish the certification program may give some organizations (at least those without cybersecurity obligations in their current government contracts) the impression that they have significant time to comply. But whether they know it or not, government contractors (and other private companies) are already subject to cybersecurity requirements separate and apart from their contractual obligations. Waiting to comply with the CMMC leaves organizations non-compliant with existing obligations.

Even organizations that reach certain CMMC Levels may not be compliant with their other obligations. Certifying a level of maturity lower than these obligations can create headaches, especially in the wake of a data breach. Organizations must understand the risks involved in obtaining the wrong level of certification

Common Law, Negligence, and Reasonable Security

The law on cybersecurity is far from fully developed. As the then California Attorney General Kamala Harris said in 2016, "[t]he legal obligation to secure information is contained in an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes." These obligations continue to expand. Specific industry sectors have their own cybersecurity requirements. Healthcare and financial services have two of the most well-known legal regimes, but they are not alone. The Federal Trade Commission (FTC) imposes cybersecurity requirements under section 5 of the FTC Act. Certain states impose requirements for organizations

that collect personal information. These requirements are explicit, but there are an ever-growing number of implicit requirements.

There are several sources of these implicit requirements. For instance, courts are beginning to recognize a common law duty of care to secure personal information, including that of employees. Also, enforcement authorities expect organizations to implement "basic" cybersecurity controls even in the absence of specific statutory or regulatory requirements.

> *"…enforcement authorities expect organizations to implement "basic" cybersecurity controls even in the absence of specific statutory or regulatory requirements."*

Common Law Obligations

First, common law negligence. Plaintiff's lawyers have become increasingly creative in pleading causes of action for cybersecurity breaches. They have also been diligent, and so while early negligence claims were typically dismissed under the economic loss doctrine or Article III standing grounds, some courts have relented in more recent cases.

For instance, plaintiffs in the class action suit against Equifax were able to get common law negligence claims, among others, past a motion to dismiss. Likewise, the Eleventh Circuit Court of Appeals determined that the FTC based its enforcement program on an underlying common law negligence theory (although it did not evaluate the actual existence of the duty of care). The exact contours of this duty are evolving and will continue to do so, as recent successes encourage plaintiff's lawyers to make additional claims.

Enforcement Authority Expectations

Second, enforcement authorities have said that they expect a certain level of cybersecurity even in the absence of an explicit requirement. Then AG Harris said that the Center for Internet Security's 20 Critical Security Controls "constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet."

The Federal Register notice for Federal Acquisition Regulation 52.204-21, Basic Safeguarding of Contractor Information Systems, characterized the requirements as "generally employed as part of the routine course of doing business." In response to concerns that the clause was too broad, the government stated that "this rule requires only the most basic level of safeguarding. . . ." and that a "prudent business person would employ this most basic level of safeguarding, even if not covered by this rule." These statements help enforcement authorities minimize the compliance burden for new rules, but they also indicate how enforcement authorities will view cybersecurity when investigating a breach. Plaintiffs will point to them in establishing a standard of care for negligence claims.

Any organization that collects personal information, including their employees', arguably has a legal duty to implement some level of cybersecurity. Even in the absence of an explicit legal obligation, enforcement authorities expect basic cybersecurity

protections. What these protections look like differs, but most enforcement authorities look for a "reasonable" level of cybersecurity, which they define based on the specific circumstances of the organization, and often in hindsight.

> *"Any organization that collects personal information, including their employees', arguably has a legal duty to implement some level of cybersecurity."*

What is Reasonable Security?

Most legal regimes do not provide specificity on what is required as far as cybersecurity (government contracting regulations being a notable exception). The field moves too fast for traditional rule making to keep pace. Organizations are always playing catchup to threat actors, who are constantly designing new means and methods to breach organizations' security.

To address this timing problem, many legal regimes require "reasonable security", or something roughly similar. Reasonableness is determined by the specific situation. For instance, under California law, businesses must tailor their efforts to the "nature of the information" they collect. The FTC looks more broadly, taking into account "the sensitivity and volume of consumer information it holds, the size and complexity of its operations, and the cost of tools available to reduce data security risks."

These inquiries are often conducted with the benefit of hindsight. FTC investigations are almost always conducted in the wake of a data breach, which casts doubt on an information security program. Target's 2014 data breach happened despite Target's compliance with the Payment Card Industry Data Security Standards, at least according to Target's Qualified Security Assessor. This assessment was not sufficient to protect Target from the legal consequences of its breach.

Most enforcement authorities look for certain procedural steps when evaluating reasonableness. In the absence of a defined standard, enforcement authorities evaluate a company's diligence in determining what was reasonable. The signposts that enforcement authorities look for are evolving. For instance, the FTC has included in its recent consent decrees a requirement that organizations present their board or equivalent with the organization's written information security program, which is a higher level of oversight than previously required.

It is important for organizations to evaluate what their respective legal obligations are, as both what is reasonable and what enforcement authorities look for differs. But there are some commonalities. Many enforcement authorities expect a fulsome information security program, including an organization-wide risk assessment, an information security program briefed to the board or equivalent, and dedicated executive oversight. These process requirements indicate that an organization made a good faith effort to determine what was reasonable, even if in hindsight an organization's practices were insufficient to prevent a data breach.

Is the CMMC Reasonable for You?

The Department of Defense implemented the CMMC because contractors were not meeting existing contractual cybersecurity obligations. The CMMC process will eventually require third-party assessors to validate the maturity level of a contractor's cybersecurity program.

The CMMC assesses organizations under two broad categories: processes and practices. An organization's overall maturity level is the lower of its maturity level in these two categories. For instance, an organization with excellent practices (*e.g.*, it has implemented many advanced technical controls) but with little to no formal documentation would have the lowest level of maturity.

Under the current CMMC process, an organization's maturity level will not be made public, but the fact that an organization is certified will be. Much like other cybersecurity certifications (*e.g.,* PCI DSS), regulators, plaintiff's lawyers, and similar entities will demand the underlying work papers when they have the authority to do so (*e.g.*, in discovery). Ultimately, CMMC documentation may serve as roadmap for third parties seeking to prove that an organization lacked reasonable security. This is especially true for the Level 1 maturity level, which lacks the rigor that many enforcement authorities look for in a cybersecurity program.

CMMC Level 1 Certification

The current CMMC guidelines do not require a process assessment for the lowest level of maturity, assuming that processes are ad hoc. The assessed practices must only meet the FAR 52.204-21 requirements. These requirements are the "most basic level of safeguarding" as established in 2016. Technology has advanced significantly since then.

While minimum standards are appealing to subject organizations, the requirements for CMMC Level 1 are so low that meeting only those requirements could raise concerns about an organization's security program. First, the practice requirements established at Level 1 are below what many enforcement authorities expect today. Second, the process requirements are non-existent, when most enforcement authorities require systematic processes managed at an appropriate level within an organization.

CMMC Level 1 requires only the most basic security controls. These security controls may not be "reasonable" for the sensitivity of data that an organization collects. For instance, the CIS 20 includes training, penetration testing, and red team requirements, whereas the FAR clause is silent on these issues. Then AG Harris considered the CIS 20 as the minimum for any personal information; certifying to a lesser standard, especially in cases where more sensitive information is stored, could be problematic.

Next, many enforcement authorities would view an ad hoc security program as unreasonable, even though such a program is sufficient for CMMC Level 1. As an example, the FTC has included in its recent consent decrees a requirement that organizations present their board or equivalent with the organization's written information security program.

Organizations that seek CMMC Level 1 certification should ensure that the paperwork surrounding the process is clear that the assessor did not examine their entire

cybersecurity program, and only looked at the practices necessary for the organization to meet its DFARS requirements.

Higher Levels of Certification

The CMMC has 5 levels of maturity. Level 3 contains all requirements necessary for an organization to store, transmit, or process Controlled Unclassified Information. Level 2 bridges Level 1 and Level 3, while Levels 4 and 5 have requirements that attempt to mitigate the risk from Advanced Persistent Threats.

Organizations should examine the requirements of the CMMC level they are seeking and compare it against their other legal obligations. For instance, the Level 2 process requirements include practices and policies for the specific practice domains, but do not currently require an overarching security program. The Level 2 practices do contemplate basic risk assessments, but there is not a requirement to conduct periodic risk assessments of the type that the FTC has required in consent decrees. In short, Level 2 process requirements may not meet the requirements in other legal regimes.

This post has focused on some of the most generally applicable cybersecurity legal regimes, but some industry sectors have more specific requirements, such as financial services and healthcare. Organizations with these specific requirements should ensure that their CMMC Level requirements match on a line-by-line basis with their other obligations. Each enforcement regime has different priorities, and what may be critical control for one may not be for another.

Conclusion

The CMMC may be some organizations first introduction to formal cybersecurity requirements. Organizations need to ensure that they are not designing their cybersecurity programs to the CMMC maturity levels, since these levels likely do not represent an organization's full set of legal requirements. More practically, the CMMC requirements, especially at the lower levels, are unlikely to be sufficient to mitigate the threat of data breaches.

Organizations seeking CMMC certification should consider that effort as one part of a broader cybersecurity program that is compliant with an organization's full set of legal requirements, as well as appropriate to the organization's actual needs. A failure to do so could result in unwanted legal and technical risk.

CONTACT:

For more information or to connect with one of the Centre Law & Consulting team contact us at info@centrelawgroup.com or call (703) 288-2800.