A SPECIAL EXCERPT FROM
THE AMAZON.COM BESTSELLING BOOK

THE COMPLIANCE FORMULA

Successful Strategies Of CMMC Compliant Companies

CHAPTER 6

WHAT IS YOUR CYBER-HYGIENE SCORE?

FIND OUT IF YOU'RE DOING GREAT OR ARE IN DANGER, AND WHERE TO START

BY DAVID LUFT,
CEO – LDD Consulting

Becoming a United States Government contractor is a lucrative proposition, but it also comes with a great deal more red tape than working in the private sector. If you want to win contracts with the Department of Defense, then the complexity climbs higher, as it should. Could you imagine handling DoD information without requirements on how to protect it? Even if you aren't working directly with the DoD, but you're a subcontractor or anywhere in the supply chain, you too are required to be Cybersecurity Maturity Model Certification (CMMC) compliant.

While a cyber-hygiene score sounds like something your dentist made up to get you to brush more, it's a vital and honest assessment of your company's readiness to handle cyberthreats and can measure how you stand up to CMMC compliance. It's about following procedures and steps to keep your network and

information safe. Much like your personal hygiene, it's based on discipline and consistency. If you make it part of your everyday life, it will become mechanical, and you won't have to wonder where you stand – it will just be a part of your routine.

CORE CYBER-HYGIENE STRATEGIES

So, you've decided to go after those DoD contracts, and you want to know where you stand. Let's get started by reviewing what I call core cyber-hygiene strategies and then we'll dive deeper into them. These are the things that need to be put in place to ensure a reputable cyber-hygiene score. They include:

- Core Security and Access Controls (including firewalls, antivirus, and backups)
- Employee Training and Personnel Security
- Monitoring, Maintenance and Configuration Management
- Policies and Procedures
- Security Assessments, Auditing, and Accountability
- Incident Response
- Risk Management (including subcontractors)

CORE SECURITY AND ACCESS CONTROL

Core security and access controls are big categories. They encompass your systems and network security, but also physical security and access to your facilities. I know some of your eyes just glazed over a bit, but stick with me because this stuff is important, and I'll try to address it with the assumption that you have little-to-zero knowledge of networking and technology.

First, let's talk about authentication and authorization. Authentication means verifying that you are who you say you are. We accomplish this with individual network credentials with secure passwords that prove you are the person you claim to be. Authorization means accepting your credentials from authentication, but then determining what you can do. To break

these down to non-technical examples, we'll look at it in the context of physical security. When you start a new job and you get a badge with your picture on it, that allows people to see that your face matches your badge, so that's authentication and identity. Later that day, you're roaming the building and you see a door with a badge reader on it. You decide to look inside, but you're not allowed to enter that room – when your badge is scanned, you are denied entry. That is authorization.

Firewalls are a lot like locks on doors but apply to your network and computers. Firewall rules determine WHO can get to WHAT resources on your network. They can be physical pieces of equipment or, if you're a small operation, they may just be software that's embedded in your router, which is what connects you to the Internet. Firewalls work with allow-and-deny rules. Older firewalls used Internet protocol addresses as the WHO, but many of the modern options can even allow/deny based on your network credentials. The WHAT refers to other computers or equipment on the network. If you have a server with data that shouldn't be accessible by everyone, then by default you deny all traffic to it, then put in rules that allow only specific persons or computers to get to that machine.

Another important part of this category is virus and malware detection and prevention. Ninety-five percent of cybersecurity breaches are a result of human error. This is often because someone clicks a link in an email they shouldn't or opens a document from email or a website they don't recognize. While antivirus and zero trust software can't stop all incidents, they will prevent many of them. Although it's not enough just to have these features, you should keep them updated with the latest virus definitions, because the bad guys are constantly finding new ways to exploit your systems.[1]

Now that your network has firewalls, you know the identity of the people on your network and you have up-to-date antivirus

1. Cybint (December 23, 2020), "15 Alarming Cyber Security Facts and Stats." https://www.cybintsolutions.com/cyber-security-facts-stats/

software installed, you need to make sure you have backups, and you can restore them. Ideally, you back up every computer and device on your network, but you must, at a minimum, have regular backups of your important systems. Imagine the fallout when you've been working on a major project for weeks and your system suffers a catastrophic failure. This could be your laptop or a database on one of your servers. Either way, it's going to be a terrible day, but your day will get much worse if you don't have backups of the critical data.

Your backups should be automated – not something you even have to think about daily. You should also have offline backups of your backup files. What does that mean? If your backups run to disk, you need to back up those backup files somewhere that can't be reached as easily. This can be to the cloud or external devices you unplug when not actively backing up. The reason: ransomware attacks don't only try to encrypt the files on your machines, they also try to find and encrypt your backup files. So, if you don't take the extra step, you won't be able to recover the backups to get your business up and running again. Restores are the other part of the equation – backups are useless if you can't restore them. You should test restoring your backups on a regular basis to avoid surprises. If a hacker wipes out important data and you can't restore it, your best option will be to update your résumé, because then it's too late.

EMPLOYEE TRAINING AND PERSONNEL SECURITY

Earlier we talked about antivirus software and how most cybersecurity breaches are the result of human error. The antivirus software can only do so much, as hackers are finding new ways to breach every day, and the software makers can't always keep up. All employees in your company need to have comprehensive cybersecurity training, regardless of their role. The importance of this training needs to rank as high as the human resource training we all take when starting a new job, and it also needs to be reinforced with ongoing training to keep

the concepts fresh in the minds of your employees and keep them abreast of new scams and attack types to be aware of.

Personnel security doesn't refer to having security to escort people to their cars at night, but to vetting employees based on conduct and character for positions with the government. This includes doing proper pre-employment screenings and terminating employees who violate conduct policies or show moral or ethical failings. It seeks to minimize risks posed by workers to the organization's assets.[2]

Personnel Security:
The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.[3]

MONITORING, MAINTENANCE AND CONFIGURATION MANAGEMENT

You've implemented some processes we've outlined, and now you need to monitor and maintain them. How will you know if something has changed or that you have operating systems or applications running outdated versions and what will you do to fix them? You need to monitor your systems and your physical space. CMMC Level 1 requires escorting visitors and monitoring their activity, as well as managing physical devices like USB keys. For systems monitoring, you need to monitor your network and boundary systems. Implementing an intrusion detection system to alert you of network irregularities is also a good idea.

For maintenance, you can't dismiss this or "kick the can" further down the road. Outdated applications and operating systems don't get patches or upgrades released as often and are perfect targets

2. National Institute of Standards and Technology (June 2017), "An Introduction to Information Security." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

3. Computer Security Resource Center, Glossary. https://csrc.nist.gov/glossary/term/personnel_security

for hackers looking to exploit vulnerabilities. You also must have regular patching schedules to apply any security patches released by vendors. A security patch can be released because of a known issue that's already in the wild, but it could also be one that hasn't yet been discovered by hackers. If it's the latter, then hackers are learning about it when the patch gets released and they'll start working to exploit it, so the sooner you apply it, the better.

Configuration management refers to storing and knowing the state of your systems. There are many software packages out there that can help with this, but its job is to look for changes to a system, and it can even be told to restore it anytime it finds a deviation. The basic principle here is that you need to know what your system is supposed to look like, know when it's changed and who changed it.

POLICIES AND PROCEDURES

Your employees can't follow policies and procedures that aren't known and documented. Even less strict frameworks, like HIPAA and Sarbanes–Oxley, require you to have these documented, so you know it's going to be necessary if you work for the government. I won't dive into everything that should be included in those policies and procedures, but you must have them, and everyone in your company should know their location and contents. It's even a good idea to request that employees read and acknowledge them every year.

SECURITY ASSESSMENTS AND AUDITS

The security assessments are a bedrock of CMMC compliance. Most businesses will outsource these assessments to a company like LDD Consulting, which specializes in this type of work. The time invested and level of effort to perform these tasks internally will be exponentially harder for the uninitiated. The results of the assessments tell the government if you can maintain your compliance. If you choose to self-assess, which will be allowed for

some companies in CMMC 2.0, make sure you report accurately and honestly, or you could be in violation of the False Claims Act.

> *The False Claims Act (FCA), 31 U.S.C. §§ 3729–3733 was enacted in 1863 by a Congress concerned that suppliers of goods to the Union Army during the Civil War were defrauding the Army. The FCA provided that any person who knowingly submitted false claims to the government was liable for double the government's damages plus a penalty of $2,000 for each false claim.*[4]

Auditing has many contexts in the business world and even within the context of this book. You need to have auditing turned on for your systems, you need to audit your security controls regularly and you should even hire third-party companies to perform audits. Just as public companies are required to have financial audits, you need to have someone perform security audits. This may include hiring someone to do penetration testing, where someone tries to gain access to your systems with brute force or through known vulnerabilities. Some companies hire people to try social engineering campaigns to see if your employees will unwittingly give up private information that can game your security controls. Hiring ethical hackers to find soft spots in your company to gain entry is another example. One other part of auditing is that you should collect the logs from all your systems into a central location. This makes it easier to analyze them and makes it more difficult for hackers to clean up after themselves if they breach one of your systems.

INCIDENT RESPONSE

What happens if your business is hacked? Let's face it, in today's climate it's more like WHEN you're hacked. You need to have a response plan. Whether this is an internal process or through a partner, it's essential to know what you're going to do BEFORE

4. The United States Department of Justice, "The False Claims Act: A Primer." https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf

the breach occurs. If you're the victim of a ransomware attack, for example, and you don't have your incident response planned out, it could take weeks or even months before you're back to business as usual. That can cost your company a lot of money and likely damage your reputation. Sure, your reputation may take a minor hit just for being hacked, but it happens so frequently today that how you recover will be what gets the most attention. If you're back up and running in a day or two, it will show your resiliency.

RISK MANAGEMENT

For information system security, risk management means limiting the risk to an organization's operations and assets. As it applies to CMMC, any project handling Controlled Unclassified Information is expected to have a defined risk management approach. While the CMMC is not overly prescriptive in its details on what the approach should include, it's the culmination of all the items included in my core cyber-hygiene strategies we've been walking through. The buck doesn't stop with you though – if you are the prime contractor, this also applies to subcontractors in the supply chain. It is your responsibility to ensure your subcontractors also meet the requirements.

CONCLUSION

The road to a good cyber-hygiene score is difficult, but it's necessary for gaining CMMC compliance and scaling the mountain that is DoD contracting. The government needs private-sector contractors to unearth new ideas and innovate the next generation of concepts and designs to keep our country safe and keep us on the leading edge of technological advancements.

Keep in mind that the government knows this process is arduous and the price of admission is steep, and the contracts awarded allow for that burden. There are a lot of companies these days that offer their services to perform the assessments. At LDD Consulting, we take a different approach, as we know that

getting those results is just the beginning. As a company rooted in managed services, we don't just drop the assessment on your desk and move on to the next project. If you want our help with implementation, maintenance and the ongoing work needed to stay current, we'll roll up our sleeves and get our hands dirty. If you already have a trusted implementation contractor or team, that's fine as well. We strive to offer the best service and customer service, so we're here for any of your business needs.

About David

David Luft is the CEO of LDD Consulting. He founded the company in 2002 with Dina, his wife since 1992. LDD Consulting is a Managed Services Provider of IT services. The original focus of the company was on education and medical businesses because they're in environments that require compliance, security and automation and often don't have the internal resources to manage them. With the daily increase in cyberthreats, LDD Consulting has added cybersecurity and government compliance to its arsenal of offerings.

When David was in high school, his father told him he had to take a foreign language, so he signed up for Spanish. That didn't go so well, and he failed. His father still required him to take a foreign language and suggested computer programming, which in the early '80s was still very much foreign. After that, David was all in and never wanted to do anything else.

David was a Microsoft Certified Trainer and previously taught the Microsoft Certified Systems Engineer certification at the University of Phoenix, ITT Tech, and the University of New Mexico. He started working toward a Bachelor of Computer Science, but upon taking some psychology classes needed for his studies in artificial intelligence, he found he enjoyed the subject and finished with a Bachelor's in Psychology with a minor in Computer Science. He later completed his MBA with a focus on Information Technology.

David and Dina have two grown children they're extremely proud of, a son and a daughter. David credits Dina's positivity for their children growing up to be caring and giving people. They also have three grandchildren who they adore. When David isn't protecting companies from cyberthreats, he can often be found hiking or backpacking in the New Mexico high desert. He and Dina also love camping with their expanding family and get out on a boat any time the opportunity presents itself.

Contact LDD Consulting:

- Email: info@lddconsulting.com
- Web: https://lddconsulting.com
- Phone: 505-792-2375