NDIA

National DEFENSE

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) OUTLOOK

SPECIAL REPORT

CMMC: An Introduction

New rules and regulations are common occurrences for the defense industry. Despite perennial promises from politicians that they want to cut red tape, the acquisition laws are ever-changing.

But perhaps no other recent regulation has caused more consternation among defense contractors than the Cybersecurity Maturity Model Certification (CMMC).

The bottom line is fairly straightforward: comply with standards designed to mitigate cybersecurity breaches or you will not be able to do business with the Defense Department.

The deadline to comply for all contractors is 2026, but for some companies with cutting edge technologies, that deadline is coming much quicker.

Already a cottage industry surrounding CMMC is springing up.

There will be auditors known as CMMC Third Party Assessment Organizations (C3PAOs), who will be in charge of certifying that a contractor is complying — and charging fees to do so. Along with consultants who are eager to advise clients on how to pass their inspections — and they won't be working for free, either.

The question now is how big of a financial burden will this be on small businesses?

Katie Arrington, chief information security officer in the office of the undersecretary of defense for acquisition and sustainment and the Defense Department's point person on CMMC, said recently that she expected 7,500 contractors to be compliant by next year.

It's a start, but with some estimated 300,000 members of the defense industrial base, there is a long way to go.

This eBook, produced by *National Defense* magazine staff, will help answer some of the commonly asked questions about this new, important regulation.

Stew Magnuson
Editor in Chief
National Defense

iStock photo

Table of Contents


BlueVoyant®
Prepare for CMMC with
BlueVoyant Cybersecurity
The DOD will soon implement a new assessment process for all Contractors and Subcontractors to ensure Controlled Unclassified Information is adequately protected. Are you ready?
We can help you with Cybersecurity Maturity Model Certification.
Learn more at www.bluevoyant.com/cmmc
For sales: contact@bluevoyant.com | 646-586-9914

CMMC: The Necessity and Reasons for Compliance

BY HAWK CARLISLE

For decades, the National Defense Industrial Association and its members have worked hard to ensure U.S. and allied warfighters enjoy decisive advantage across the spectrum of conflict. American innovation is at the heart of delivering this advantage.

These innovations, however, are increasingly under threat as China systematically steals our intellectual property. With the advent of 5G technology, they are preparing to conduct their theft on a previously unimaginable scale, leading U.S. decision-makers to develop and implement bipartisan policies to counter these aggressive, illegal actions.

Despite high levels of partisanship in Washington, the Chinese threat to American IP is one area where the administration and Congress agree and are acting to defend our national security. These actions, however, could dramatically impact the health and size of the defense industrial base.

The Cybersecurity Maturity Model Certification (CMMC) is one of the administration's most public efforts to thwart the loss of IP to China and Chinese companies. The Pentagon released CMMC v1.0 in January. It contains requirements to enhance cyber fortifications across the defense contracting community by rolling out "pass/fail" standards impacting the industrial base from primes down to the smallest subcontractor.

Starting in October, beginning with select high-impact contracts with cutting edge technology, prime and subcontracting companies lacking CMMC certification at the level defined by the contract will be ineligible to compete. By 2026, all Defense Department contracts will contain CMMC requirements.

NDIA will continue to work closely with the department, the CMMC accreditation body and our members to ensure a smooth rollout of this critical emerging requirement.

Less discussed but likely more impactful are congressional actions to directly mitigate China's threat. In the 2019 National Defense Authorization Act, Congress took the dramatic step of banning government procurement of products from Chinese companies Huawei, ZTE and their affiliates. Congress has seen evidence these two telecommunication companies — and clearly many more — operate as extensions of the Chinese Communist Party, allowing the nation to spy on communications and collect data stored on networks containing Huawei and ZTE components. Congressional concern recently intensified when representatives learned Huawei can also covertly access mobile networks through back doors meant for law enforcement.

The congressional ban — contained in Section 889 of the fiscal year 2019 NDAA — has two parts: a U.S. government agency prohibition against purchasing any telecommunication products containing Huawei or ZTE components after August 2019, and a U.S. government agency prohibition against purchasing any products from any companies that use Huawei or ZTE equipment or components within their internal systems as of Aug. 13, 2020. The Pentagon has been granted a temporary waiver for the latter prohibition until Sept. 30.

The government is currently trying to implement the first part, which has proven difficult. The second, however, poses a significantly more complicated set of challenges. It stretches

iStock illustration

far beyond government procured products and services, requiring insight into and potential oversight of the way U.S. and non-U.S. companies conduct business more broadly, in order to protect and defend U.S. interests. This policy that has significant potential for disruption hinges on predatory Huawei and ZTE business strategies.

After stealing American and allied IP they file for Chinese patents, providing them with cutting edge technology without the associated research and development costs. Huawei and ZTE pass their "savings" onto customers, creating a dependency on their low-cost products and components. This strategy leads to broad penetration of the international business market and throughout the U.S. and allied defense industrial bases.

The Pentagon, which recently held a public meeting to obtain industry input on the potential impact of the more stringent second requirement, is designing rules outlining implementation. A strict reading of the statute requires the department to demand companies large and small to replace current equipment and internal systems to qualify for Defense Department contracts and business. This demand will ripple through existing and emerging contracts, impacting everyone from the largest multinational contractors down to companies receiving prime contracts under small business set-asides.

When the second part takes effect, companies with Huawei and ZTE equipment or components in their government offerings face significant disruption as they seek alternatives.

Compliance with CMMC and the two parts of Section 889 will come at a cost to both industry and government. Companies will require resources, personnel and money to secure networks against penetration and exploitation. And the department's imperative to "go faster" on innovative programs will likely run into the competing imperative of protecting the IP that drives innovation.

Thus, collaboration across government and industry is critical in developing effective barriers to cyber threats at the lowest possible cost to U.S. and allied contractors.

NDIA supports the bipartisan congressional and administration policies requiring protection of America's most valuable natural resource — our creativity. The association will ensure our members have a voice during the discussions that help define emerging policies and will provide background and compliance updates at NDIA.org/CMMC.

Additionally, NDIA will continue to act as an honest broker, convening events to drive collaboration and working with policymakers to craft regulations without inadvertently imposing requirements that drive costs without benefit. ND

Retired Air Force Gen. Hawk Carlisle is president and CEO of NDIA.

iStock illustration

CMMC FREQUENTLY ASKED QUESTIONS

Corbin Evans, principal director of strategic programs at the National Defense Industrial Association, has emerged as one of the leading experts on the CMMC outside the government.

He has held a series of NDIA members-only webinars, where he seeks to clarify the knowns and unknowns of the law as the rules are being sorted out by the Pentagon. The following are some questions that have emerged from his first two webinars.

Evans will be hosting a third NDIA members-only talk online on Sept. 24.

Q. How do you know what CMMC level you should be in?

A. Short answer: we don't know yet. Longer answer: if you handle controlled unclassified information (CUI), you are likely CMMC Level 3 or higher. If no CUI, then you are likely Level 1. CMMC Levels 4/5 will likely only be for a handful of companies.

Q. I was recently approached by a company that is stating that they are conducting CMMC Level 3 pre-assessments for companies all over the country. They are implying that they are one of the companies that will be certified assessors. Have these assessors or instructors been chosen yet? Or should we be leery of companies making these claims?

A. No assessors have been chosen yet. There are a lot of companies in the marketplace that are seeking to provide consulting services and may even seek to be assessors once the CMMC Accreditation Body has that program stood up.

At this point in time it not necessary to seek out consulting services, as it is still unknown when any individual company will need to be CMMC compliant, but it is a potentially prudent business practice to start to build a better understanding of where your business's current practices might fit within the CMMC program.

Q. What level will require manufacturers to certify that all of their machine tools on their shop floor are cybersecure?

A. It is likely that this requirement will start at Level 3. It depends on the amount of information that is being pushed to or housed by the machines on your shop floor.

Q. Will each contractor have an overall, organization-wide CMMC level on top of CMMC levels for independent information systems within the organization?

A. We're still waiting for more details from DoD on this question. Companies will likely have the option to bring the whole or parts of their internal system up to the CMMC level required by one or more contracts.

One note on this: it may be more expensive to bring your entire system up to CMMC Level 3 than it would be to just enclave the data for that particular contract to achieve the required certification.

Q. Does CUI include technical data used by manufacturers?

A. Yes. The definition of CUI continues to be developed by DoD, but technical data is exactly the type of data the CMMC program is designed to protect.

Q. Does CMMC also apply to Federal Acquisition Regulation 12 (commercial contracts)?

A. At this point we don't know exactly what the bounds of the CMMC program are, but we do know that the program does not intend to apply to commercial-off-the-shelf products based on public statements by the DoD program leads and by the FAQs posted on the DoD CMMC site.

Q. Assuming you are already using or in the process of implementing NIST 800-171 controls and are Defense Federal Acquisition Regulation Supplemental (DFARS) compliant, should you not be well on the way to CMMC?

A. Yes! If you have implemented all of the requirements under the NIST 171 standard, you are very close to being compliant with CMMC Level 3.

Q. Level 1 should be low cost. But I am getting quotes for $50,000 just to assess what we need to do. What should we actually expect the cost to reach Level 1 to be?

A. The actual costs of implementing the 17 practices associated with Level 1 are low. Consulting services may vary in cost.

Q. For academic organizations that are part of a defense industry team, have standalone work agreements with U.S. government defense offices, and/or a Federally Funded Research and Development Center/University Affiliated Research Center, do they have the same CMMC certification requirements as defense industry partners?

A. Educational institutions and FFRDCs that are funded through the DoD will likely be required to be part of the CMMC program. What level and the process for certification remains unclear.

Q. Do you have insight as to how CMMC will address pre-award certification of certain high security networks that will be purpose-built for contracts as called for in RFPs?

A. The CMMC program is intended to require pre-award certification. To be awarded a contract containing the CMMC requirements, you must meet, and be certified to the required CMMC level prior to award. This will also be the case for Levels 4 and 5.

Q. For companies that utilize a diverse supply chain, what assumptions should be made to help plan for required CMMC levels? Is there guidance on what type of information would be considered CUI that would help determine if suppliers would need to be ready for Level 1 or Level 3?

A. The easiest answer is if you flow down CUI to suppliers, they will need to be at least Level 3. If you have suppliers that do not receive CUI — keeping in mind the current issues with the definition of CUI — you can assume they will only need to be Level 1.

Q. Will the cost of the certification by the CMMC Third Party Assessor Organization be standardized or will they be up to them to set the price?

A. This is not set in stone yet, but the CMMC-AB has made previous statements that they plan to allow the "market" to set prices for certification, so we expect them to vary across C3PAOs.

iStock illustration

Q. For C3PAO certifications for assessments, is that only for auditing or also doing a security assessment?

A. The CMMC-AB is still creating guidance on this issue, but its members have made statements that they do not want to allow companies to provide both security consulting and certifying services for the same company.

Q. Would accounting firms that do work for contractors need to be CMMC compliant?

A. Yes.

Q. Is there a place to get a definitive answer on which CMMC level you will need?

A. No.

Q. As subcontractors, how do we know what level we should be targeting?

A. If CUI, then Level 3. If no CUI, then Level 1. There will likely only be very few subs at Levels 4 and 5.

Q. How does the CMMC affect current DoD contracts that we have already been awarded?

A. There will be some block changes to current contracts but we know the majority of current contracts will remain unchanged until 2026.

Q. We are a parts distributor and approved vendor for the Defense Logistics Agency. Do we need to get CMMC?

A. Yes.

Q. If the prime contractor is required to have a high CMMC rating — say Level 4 or 5 — will all subcontractors have to have the same rating of a 4 or 5 or could they possibly only need a 2 or 3?

A. There is no requirement that all subs have the same level as the prime contractor. It is likely that the subs will have lower CMMC levels than the prime because they are receiving less — or no — CUI.

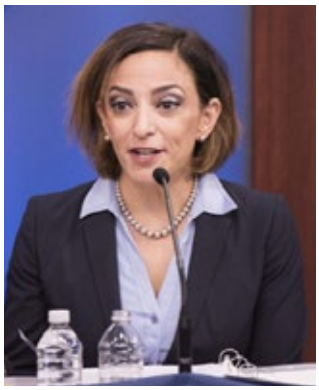
Q. Does an organization have to retain their initial certification level for a predetermined amount of time? If their security posture improves can the organization get recertified at any point in time?

A. Initial certifications will be good for three years. It is unclear at this time what the process will be for receiving a change in your certification during those three years. More to come on this from the CMMC-Accreditation Body. ND

Katie Arrington: In Her Own Words

Katie Arrington, chief information security officer at the office of the undersecretary of defense for acquisition and sustainment, is the Defense Department point person for all things Cybersecurity Maturity Model Certification.

She recently spoke with the general manager of cybersecurity consultant Celerium, Tommy McDowell, during a webinar where she answered several pressing questions. Her statements have been edited for clarity and brevity.



What is CMMC?

At the very, very highest level it is a maturity model based on critical thinking for a company to do their utmost best A: to protect themselves; B: to protect the national security interests of work that they may be doing.

It's based on maturity of companies, their critical thinking about cybersecurity. It is not a checklist. … We are all moving to a maturity model because not all security risks are equal, right? We needed to have a tailorable, scalable, repeatable process that we could implement throughout the entirety of the DoD supply chain, which is about 300,000 [companies]. … We have people that are creating, selling and manufacturing boots. We also have people creating technology for hypersonics. We couldn't give one standard to everybody in the [defense industrial base] to get to this level of security, because it was unattainable. We couldn't afford it. And we would put companies out of business.

It needed to be based on maturity and it needed to be scalable so that we can say, "All right, yes, it's important that everybody has cybersecurity."

How that is accomplished…

There are 17 foundational tools or controls in Level 1. You should be doing [them] at home. You should be doing it in every single business that you have. These are 17 practices that create good cyber hygiene. They're basics. They're things equal to brushing your teeth and taking a shower. They're the things you should do every single day continuously to maintain good hygiene.

The maturity model is built on five levels. So, Level 1 is good cyber hygiene.

Level 2 is when you start to actually put processes in place in your organization to ensure cybersecurity. You implement it into a handbook. You create certain things and processes within a company to ensure good cyber posture.

Level 3 is the instantiation of what is in the [National Institute of Standards and Technology Special Publication 800-171]. It's 110 controls that if you have a Defense Federal Acquisition Regulation ruling in your contract — DFARS rule 252.204.7012 — and you are transmitting or touching controlled unclassified information, you are attesting to the federal government that you are actually doing those 110 controls. That's where policy dictates cybersecurity.

In the CMMC model, we added 20 additional controls into Level 3. … Those you will see in Level 4 and 5 in the CMMC. Those are going to be used on about 0.06 percent of our defense contracts. So they're very exquisite, very specialized, very expert controls — things like a 24-hour-a-day security operations center, a SOC.

But Level 3 is the main crux of it as it supports the Special Publication 800-171. We are working through the rule change right now. That DFAR rule currently says that you need to attest that you are compliant to the NIST 800-17. The new DFAR rule says that you are compliant to the CMMC level requirement in the contract that you're executing. So, we needed to make it scalable. We needed to make it a maturity model. So that's where we are. And we're going through the rule change process right now.

When this all begins…

Here's my challenge point: The cart before the horse, the chicken before the egg, I kind of live in that world. Until the rule change is all the way through the process, I can't require it to be in a contract. I can't require it to be in a [request for proposals]. …

We are not the controlling body doing that. … We've done the interagency coordination and adjudication of comments. The DFAR rule is getting ready to be released for public comment. There will be a 60-day period where the public can comment on the model on anything that they want. And then after that, we'll ensure we've adjudicated all those comments and concerns, and then they will publish the rule. It will go into effect 30 days after it's published, and then you will actually start seeing it in RFPs. So, I'm still in the mindset of the October [2020] timeframe, September-October timeframe. We're entering July-August for the 60-day period. Then the 30-day period is September-October, and then you'll start seeing it in RFPs.

On foreign contractors' obligations…

We have been talking to, specifically, allied partners in the F-35 program and how each of those individual countries will be able to adopt the CMMC because it will be a requirement in our DoD contracts. Therefore, if you're doing work in one of those countries, you're going to have to get certified. …

We're having those conversations around the world in real time, because it's a DoD contract. You must make it fair and equitable. If I asked a U.S. contractor to do it then I have to have my allied nation partners doing the same type of work on those types of contracts to get the same certifications.

On prime contractors and their role in compliance with subcontractors…

Defense Dept. photo

The creation of the model was to ensure the independence of the small businesses. I worked at a large prime. I also owned and operated my own nontraditional startup, and the capability to let me chart my own path was really important. And I wanted to maintain that integrity for small businesses. So, if we gave it to the prime to validate and certify, there is a chance that bad things could happen, right? You never want to set the ground for that. So, we have created a model that a small business can go and get certified at whatever level they want to achieve.

On big primes sharing threat intelligence with their partners…

Absolutely they're supposed to be doing that now. That's part of the contract — the prime-sub relationship is they're supposed to be disseminating threat information. It's not a perfect system. I think the [Information Sharing and Analysis Centers] personally are an amazing opportunity to transmit threat information through the channels. I work with them every day.

I think that one of the things that we have been talking about is if we required — or we urged — primes to join the ISAC of the sector that they were in and give that information to their supply chain so that they can get it directly — create a direct feed to get threat intel. … The ability to disseminate threat information is key. … We do need to get better at finding new ways to actually get that information out.

On the role of the CMMC auditors…

The company, or small business, is creating a fiduciary relationship with their CMMC auditor. That auditor has the obligation once they've submitted that your system is certified to be at this level. When big events like the Windows 10 update comes … you're going to hear it from your primes. You're also going to hear it from your CMMC auditor: "Have you done this patch? I need to see verification." Because it's only then where we actually would be able to create the critical thinking about, "OK, when I get this patch information, what do I need to do? How will it really affect my networks? Do I need to run a test before I do the patch? … The CMMC is a step to get there, but that auditing and feedback loop is going to be essential.

On the importance of small businesses needing cyber protection…

You say, "I only am a small business and there's no way China even knows I'm here." Oh, they know. They've been watching you for a long time. China, Russia, North Korea, Iran. They don't want us to succeed and they are absolutely watching you. And they are absolutely creating a pathway to take you out. So, get protected. The CMMC is a tool to use in your toolkit to protect your company, to protect your IP and ensure your opportunity will be there in the future.

The last part that I'll add on this is that we in the Department of Defense write contracts, we create programs, we create policy. You are the doers, you're the executors, you're the heart of the program, right? We don't live without you and you don't live without us. The industrial base is deeply entrenched into our fabric as military policy. We don't live, we don't function, we cannot provide the national security without our industrial base. It's up to all of us to get good about this right now.

Her predictions for the next year…

I think that 12 months from now, if you've been paying attention to all the fun stuff, there's something called the National Cyber Solarium report. That is something that was a spin-off of the National Cyber Strategy. In the report it said that the United States needed a national cyber certification program, and that it should be built on the DoD CMMC model. The next part of that report was in section 4.4.4 of the National Cyber Solarium report. They said that we need … to include cybersecurity requirements, maturity and your threats as part of your SEC filings.

I think 12 months from now, we'll have worked through the pathfinders and the pilot program. We will be rocking and rolling. An estimated 7,500 companies will be certified in 2021. That doesn't seem like a lot. But if you think about the interconnectivity of the DIB, it's a certification that's good for all DoD contracts for three years. The 7,500 in the first year is huge and it only continues up. I think that in five years from now it's part of a national standard, it's part of how we do business. ND

EDITED BY STEW MAGNUSON AND MANDY MAYFIELD

iStock illustration

Undetected, Forgotten Hardware May Pose CMMC Issues

BY YASMIN TADJDEH

The defense industry is gearing up for audits as the Pentagon's highly anticipated set of new cybersecurity standards begin to be implemented this summer. However, undetected hardware and software on company networks may pose challenges.

Earlier this year, the Defense Department unveiled new rules — known as the Cybersecurity Maturity Model Certification version 1.0 — aimed at compelling the defense industrial base to better protect its networks and controlled unclassified information against cyberattacks and theft by competitors such as China. The rules will eventually be baked into contracts, and the Pentagon wants to include them in requests for information as early as this summer on pathfinder programs.

Audits will be conducted by third-party assessment organizations, known as C3PAOs. Auditors will be trained and approved by a new accreditation body.

As companies seek to comply with CMMC — which features different standards depending on the nature of the work being done, with Level 1 standards being the least demanding and Level 5 the most burdensome — they should be aware of undetected devices on their networks that could pose risks to their certifications, said Katherine Gronberg, vice president of government affairs at Forescout Technologies, a San Jose, California-based security firm.

"On average we can go into a company in any sector and find about 30 to 40 percent more devices than they knew about," she said.

Since last summer, Forescout has worked with about three dozen medium and large defense companies as they prepare for CMMC audits. During assessments, Forescout discovered numerous issues that could complicate compliance with the cybersecurity rules.

During one contractor's assessment, Forescout discovered two smart speaker devices placed in sensitive locations, five unknown or previously unidentified wireless devices and wireless access points, instances of unknown or high-risk software platforms on the network, and other issues.

Worryingly, it found 27 instances of Kaspersky software and Kaspersky-furnished files on the network of the contractor, according to Forescout. Kaspersky is Russian-made security software that is banned by the U.S. government for civilian and defense agencies.

Other policy violations the firm discovered included two examples of networks believed to be air-gapped, or closed, but shown by Forescout to be accessible remotely, according to the company. This could have occurred by accident or because of poor design.

Forescout's goal is to "make people understand that tools that they have for identifying devices are usually inadequate," Gronberg said.

When it comes to reaching CMMC compliance, a defense contractor's visibility into its network will be critical, she said.

"If you have … all of these reporting requirements under

iStock illustration

CMMC, do you want to be doing it for only 70 percent of your environments?" she asked. "You're not going to have very good reporting if you're only reporting on the assets that you know about today. You've got to have a really comprehensive way to discover all of those."

The devices that represent a risk for a defense company may differ substantially from a financial services company, Gronberg noted.

"We called out Kaspersky for example," she said. Kaspersky is "a widely commercially available tool that if you're in another sector might be fine. … But in the defense sector — and certainly for the federal agencies themselves — they're not allowed to have that."

Chinese-made products could also be problematic for many defense companies, she noted.

Not having an accurate count of networked devices is not limited to the defense industry, she added. Forescout is part of the Department of Homeland Security's Continuous Diagnostics and Mitigation program, a sprawling effort that is meant to reduce cyber risk and provide visibility across the civilian agencies throughout the federal government.

"We're not the only tool delivering in that program, but we're the ones who went to the networks to detect all the hardware," Gronberg said. "When we did that, on average, the program discovered 75 percent more assets than the federal agencies knew about. That's a lot."

Once a company improves its ability to discover assets, it needs to be better about classifying them from a security standpoint. "Knowing that something is there is important, but it's only the first step of importance," she added.

Meanwhile, while the COVID-19 pandemic may cause some Pentagon program delays, CMMC is still on track, said Katie Arrington, chief information security officer at the office of the undersecretary of defense for acquisition and sustainment.

"We're having to retool some of the training because the actual inspections … have to happen," she said in April. "The actual audit has to be done on site."

The Pentagon is working on ways around that, she said during a webinar.

"We're still on track," she said. "We're still doing the pathfinders. We're working through those. We're still on target to release some initial RFIs in June with the CMMC in it so we can all kind of get a feel for it."

CMMC requirements are expected to be included in pathfinder program requests for proposals later this year.

Speaking during another webinar hosted by Bloomberg Government, Arrington said potential delays of a couple of weeks would be insignificant to the broader initiative.

"A two-week push on something is not going to … have a massive impact to our rollout of this," she said. "Maybe we'll have a two-, three-week slip on actually doing the first audits, the pathfinders, but nothing of significance."

Auditors may have to wear masks or social distance while conducting their work, she added. ND

CMMC Regulations on The Way Despite Pandemic

BY CONNIE LEE

The Defense Department's new high-profile cybersecurity regulations are on schedule for implementation this year despite potential setbacks from the COVID-19 pandemic.

Katie Arrington, chief information security officer at the office of the undersecretary of defense for acquisition and sustainment, said the Pentagon will begin rolling out the Cybersecurity Maturity Model Certification version 1.0 rules this year.

The requirements are part of the Defense Department's push to protect industrial base networks and controlled unclassified information from cyberattacks. The CMMC rules will require contractors to be certified by third-party auditors, which will ensure that companies are adhering to certain standards. Organizations will be required to meet different levels of security requirements depending on the type of work they are doing, with Level 1 being the lightest and Level 5 the most stringent.

Acquisition officials unveiled their roadmap for implementation in January, before the COVID-19 pandemic roiled U.S. society and industry. The plans included releasing solicitations with CMMC requirements baked in for pathfinder programs this year.

"We are on track to do that," Arrington said during a Project Spectrum webinar in May. "We're still on target to release some initial [requests for information] in June. … Stay tuned, but the work hasn't stopped and we're still doing our absolute best to stay on track." Project Spectrum is intended to help small businesses improve their cybersecurity and is supported by the Defense Department's Office of Small Business Programs.

The biggest challenge presented by COVID-19 includes figuring out how to conduct third-party audits of companies' cybersecurity readiness, she noted. Auditors are required to perform on-site visits to assess compliance.

"We're trying to figure out ways around that," Arrington said.

During a webinar hosted by Bloomberg Government, Arrington said auditors may need to "find a new way of doing business" to adjust to COVID-19 safety concerns. This will include wearing personal protective equipment while visiting companies.

"I think that you'll wear a mask, and you'll maintain some social distancing and you'll be able to do the audit," she said. "Just like

iStock illustration

the cable guy today — they come into your home, or they meet you, they wear a mask and we respect each other's personal space to ensure safety for all."

There could potentially be a two- to three-week delay on carrying out the first round of audits due to coronavirus, she noted. However, the potential schedule slip is expected to be "nothing of significance," she added.

"Of course, COVID-19 is … impacting every aspect of our life," she said. "But a two-week push on something is not going to have a massive impact to our rollout of this. … I don't think it's going to be anything impactful to the schedule."

Defense contractors should still expect to see new CMMC requirements in requests for proposals issued in November, Arrington noted, but the Pentagon plans to help companies adapt.

"We understand this is a big cultural shift and we want to ensure that we're doing everything we can to bring our small business partners right along with us," she said at the annual Special Operations Forces Industry Conference, which was held virtually in May by the National Defense Industrial Association due to safety concerns about COVID-19.

"We are working on different plans and strategies to help."

For instance, contractors bidding on a program may not need to have their CMMC certifications until the time of contract award, she noted.

"As we release the RFIs, we'll have the certified and trained auditors who will be able to go out to industry and certify companies at the level of maturity required for the work that they're bidding on," she said.

Corbin Evans, director of regulatory policy at NDIA, said the Defense Department has yet to recruit, train and certify auditors.

"It does seem like they're getting close" to doing that, he said. "Once they start up that process, we'll start to get a better idea of how long that certification is going to take.

"At this point in time, I think it's safe to say mid- to late summer is probably a good estimation for when those auditors will likely start to go out into the field, although that may be a little on the early side," he added.

Meanwhile, the Defense Federal Acquisition Regulation Supplement 252.204-7012 is undergoing a rule change, Arrington noted. This will be completed in October. DFARS 252.204-7012 and National Institute of Standards and Technology Special Publication 800-171 are the current regulations for storing, transmitting and processing defense information.

"You will not see the CMMC in any Department of Defense contracts or RFPs until the rule change is completed," Arrington said.

Evans said the Pentagon is changing the Defense Federal Acquisition Regulation in accordance with CMMC. The department has developed a draft rule requiring that CMMC regulations be attached to future contracts.

"This process is a little bit more formalized," he said.

To pass the rule, officials will first need to have a public meeting to gather feedback from stakeholders and outside parties including NDIA, Evans noted. However, this process may be affected by the inability to gather large crowds in public spaces due to COVID-19 restrictions.

They "have started to have conversations around delays in that process because of the limitations on their ability to have a public meeting," he said. "The rule-making process is potentially stalled because of the fact that they can't do a public meeting."

The new rules will still take time to implement because they cannot be inserted into an active contract, Arrington noted.

"We have to go through an acquisition cycle," she said. "Most of our acquisition contract strategies are one base year plus four option years. So if you're on a contract today that is not due to come out for recompete for three years, you are not going to be required to get a CMMC certification if you're bidding only on that work for the next few years."

By 2026, all Pentagon contracts will require CMMC certification, according to officials.

The majority of companies will need to achieve CMMC Level 1 certifications, Arrington said. Prime contractors will likely need to meet higher levels than subcontractors.

"Most of you … just need to get the Level 1 which is simple things like access controls and passwords and making sure you have antivirus software on your computers and that you're actually updating them and you have a way to download patches if needed," she said.

Evans said that he is "cautiously optimistic" that CMMC will continue to stay on track despite COVID-19. Although some Defense Department programs may be experiencing delays of up to 60 to 90 days, CMMC is one of the department's high priorities, he noted.

"It is plausible that they're kind of allocating resources internally to prioritize keeping CMMC implementation on track," he said.

Stuart Itkin, vice president of product management and marketing at Exostar, a Herndon, Virginia-based supply chain management company, said members of the defense industrial

iStock illustration

base are already working on bolstering their cybersecurity practices to prepare for the new rules and stop intellectual property theft.

"Some suppliers are looking at it from a risk perspective and they understand that the intellectual property, the [controlled unclassified information] that is being exfiltrated — that is being stolen — actually belongs to them," he said. "They are the ones that are experiencing the loss."

In May, Exostar released a cybersecurity tool geared toward helping companies score their existing policies and procedures, he said. The firm is not charging customers to use its tool to reach the first level of CMMC certification, he noted.

Implementing CMMC regulations is intended to help companies reduce the risk of losing their IP, he said. The United States has been working to deter adversaries such as China from stealing information from defense contractors.

"Compliance is intended to be a proxy for security," he said. "Implementing those practices or implementing those regulations should reduce the risk … of IP loss."

The increase in teleworking due to COVID-19 has highlighted the need for companies to review their policies to ensure employees are following safe cybersecurity practices from home, he noted.

"The teleworking has had a real impact on expanding the attack surface that adversaries look at," he said. It is "exposing vulnerabilities that may not have been as apparent as in the past. … One of the things that we've emphasized to organizations is that they look and they review their work-from-home policies."

Evans said improving cybersecurity practices in advance of the CMMC rollout may help companies stave off a potential increase in cyber threats as contractors continue teleworking.

"That's going to help them not only prepare for the CMMC adoption down the road, but also allow them to thwart some of those increased number of threats as … their workforce is more dispersed," he said.

Arrington encouraged industry to get a head start on meeting the new requirements, noting that companies can download the model and begin implementing some practices that would help them meet Level 1 standards.

"Waiting isn't an option for any of us," she said. "This is just a … when life gives you lemons, make lemonade" situation.

However, meeting these requirements may be more difficult for smaller businesses that are already hurting economically from the pandemic, Evans noted. The Small Business Administration and other government agencies are in discussions about potentially providing financial assistance for certification, he said.

"There are the financial constraints that are likely affecting small businesses that may inhibit their ability to make cyber-related investments at this point in time," he said. ND

New Cybersecurity Standards Pose Challenges For Small Businesses

BY JON HARPER

The Defense Department in late January released its highly anticipated new set of cybersecurity standards that companies must eventually adhere to if they want to do business with the Pentagon. But important issues have yet to be resolved, including how much it will cost contractors to comply.

Cybersecurity Maturity Model Certification version 1.0, or CMMC, is an effort to prod the defense industrial base to better protect its networks and controlled unclassified information against cyberattacks and theft by competitors such as China.

The lower tier of the supply chain is of particular concern.

"Adversaries know that in today's great power competition environment, information and technology are both key cornerstones [of national security], and attacking a sub-tier supplier is far more appealing than a prime," Undersecretary of Defense for Acquisition and Sustainment Ellen Lord told reporters at the Pentagon during a briefing about the new model. "We know that the adversary looks at our most vulnerable link, which is usually six, seven, eight levels down."

CMMC combines multiple cybersecurity frameworks, including NIST Special Publication 800-171, into one unified set of benchmarks. The specific standards that must be met will depend on the program and specific work that a company will be doing, said Katie Arrington, chief information security officer in the acquisition and sustainment office.

"Cybersecurity is not one-size-fits-all."

The Level 1 standards will be the least demanding and Level 5 the most burdensome.

Level 1 will be focused on "basic cyber hygiene" practices such as using anti-virus software and regularly changing passwords. Level 2 will require "intermediate cyber hygiene" and serve as a stepping stone to Level 3, where the bar will be much higher.

"It's a big move from Level 1 to Level 3," Arrington said. "You're moving from 17 to over 110 controls."

Corbin Evans, director of regulatory policy at the National Defense Industrial Association, said Level 3 is what the Pentagon expects a plurality of the defense industrial base to achieve. NDIA was in close communication with the department and provided feedback on CMMC drafts that were circulated prior to the release of version 1.0.

Standards for Levels 4 and 5 are even more stringent and will be imposed on "very critical technology companies" working with the most sensitive information, Arrington noted.

Third-party assessors, known as C3PAOs, will be trained and approved by a new accreditation body. They will have to certify that a company has met the CMMC standards before it can win contracts.

The new model will be phased in over the next five years to give contractors time to adjust.

"Obviously this is a complicated rollout for industry and we're being realistic in terms of making sure we have pathfinder projects, and then we implement it and learn, get the feedback and go on," Lord said.

By fiscal year 2026, all new Defense Department contracts will contain CMMC requirements that companies must meet to win the award.

However, the new requirements will be included in requests for proposals for about 10 pathfinder projects in the September timeframe. The pathfinders are expected to impact about 150 contractors per contract — a total of 1,500, Arrington said.

Evans said it could be challenging to get that many contractors CMMC certified by then.

"We think the implementation of this, especially putting RFPs into place by the October '20 timeframe, is going to be a real uphill battle," he said. "It's our understanding that your average Level 3 certification will take between three or four business days just to conduct the on-the-ground inspection. … There's going to be a lot of effort required for us to get to that number."

In the coming years, companies trying to get up to speed may be in for a rude awakening, experts say.

The consulting firm Tier 1 Cyber in November conducted a survey of 150 government contractors and released a report titled, "Cybersecurity Preparedness: Perception vs. Reality."

"Our survey discovered that respondents had a false sense of their cybersecurity preparedness," said the study. "Nevertheless, 27 percent of respondents admitted they are unprepared for a cyber breach."

Lord noted that the Pentagon conducted extensive outreach to industry and other stakeholders before it issued the new CMMC standards. However, 58 percent of contractors surveyed were unfamiliar with the initiative, according to the Tier 1 Cyber study.

"Despite the massive impact CMMC will have on all government contractors, … our DoD survey participants were largely unaware of CMMC," the report said. "In fact, only a quarter could correctly identify the acronym."

The poll also highlighted industry concerns about the supply chain.

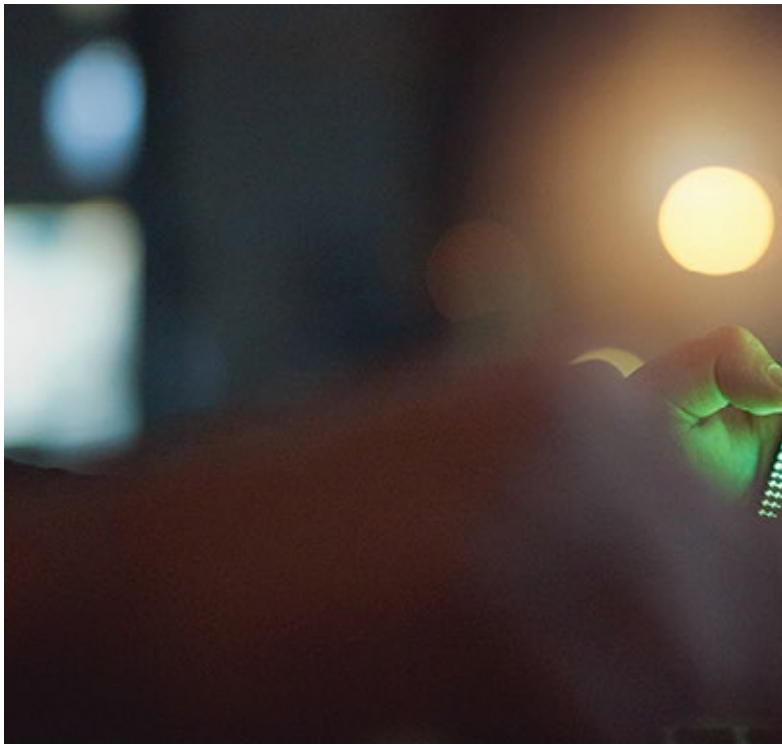
"Only 12 percent of DoD contractors were confident in the cybersecurity of their vendors," the report said. "The vast majority expressed no confidence, reservations, or not enough knowledge."

NDIA, in partnership with the supply chain performance management firm Verify, has been conducting its own industry survey, which examines the hurdles that many companies will have to overcome to become CMMC compliant.

More than 40 percent of about 300 respondents thus far, said they only have between one and 10 individuals dedicated to information technology, and 10 percent didn't have a dedicated IT professional at all, according to Evans.

That is "certainly a worrisome response there because … it's going to be difficult to comply with CMMC without at least one dedicated IT professional on your team," he said.

About 44 percent of respondents said they were still working to meet the NIST 800-171 requirements — which are expected to be part of Level 3 CMMC standards. Forty-one percent said their cyber incident response plan was a work in progress, and only 20 percent said they have an incident response plan in place. A sizeable number also said they haven't been flowing down robust cybersecurity requirements to their subcontractors, Evans noted.



"That speaks to where folks are … [and] the floor that they're kind of operating on," he said. "We can assume that that subcontracting base is operating on a pretty low foundation, as far as their level of cyber controls they have in place currently. So they're probably going to see a large delta in the amount of work that they need to do just to get up to CMMC compliance, but also the costs associated with that."

A number of factors will affect the price tag, including where companies stand now with their cybersecurity and the level they are trying to reach.

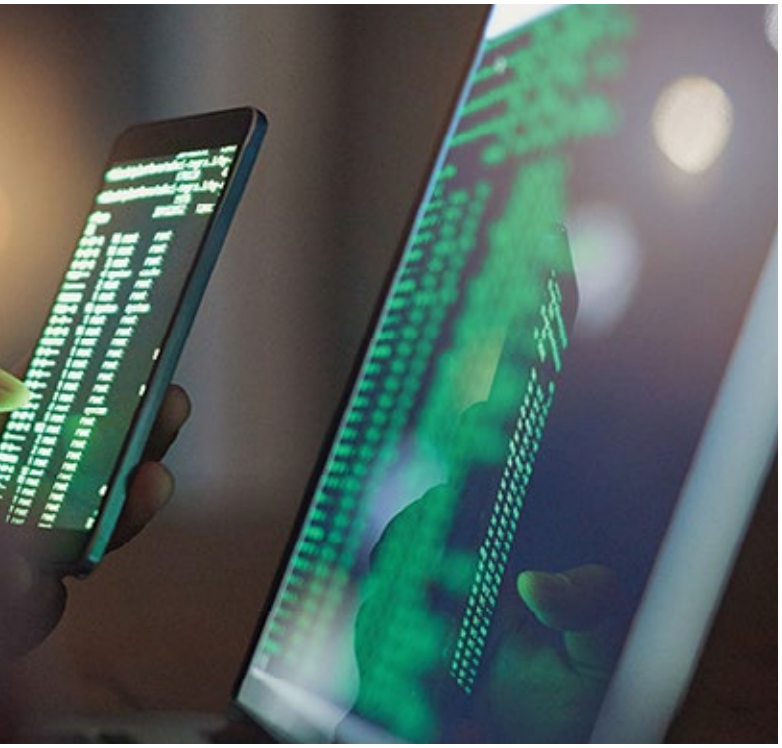
"If I'm a small business looking to get CMMC, let's say Level 3 compliant, and I'm starting at a foundation of essentially zero, I think the costs are going to come in a few different camps," Evans said.

One is the hiring of outside consultants to help contractors reach the required security level.

"That knowledge is going to be hard for you to come by just being a small business owner or small business leader," Evans said. Firms will also need dedicated IT staff in-house to keep up with the requirements.

Additionally, there are subscription services that are required for compliance with a number of these controls, such as active encryption software, he noted. Those will impose a continual cost on companies that need to keep their protections up to date.

Contractors will also have to pay to have their cybersecurity



iStock illustration

systems inspected and certified by the third-party assessors. "That one is an unknown as to how much that's actually going to cost," Evans said.

The certifications are expected to be valid for three years before they must be renewed.

Becoming CMMC compliant could be more expensive than the Pentagon anticipated, Evans said, and it remains to be seen who will ultimately bear the cost — contractors or the government.

"Initially they had a number that was in the low thousands [of dollars] to get CMMC compliant," Evans said. "I can tell you that from my conversations with NDIA members that have implemented NIST 171 up to the full 110 controls — so essentially getting themselves Level 3 compliant — they're looking at about $250,000 to do that."

Some firms could opt not to do business with the Pentagon rather than shell out large sums of money to meet the new standards, especially if they have a customer base in the commercial sector, Evans said.

"If not handled carefully and … brought to small businesses in a way that can usher them through the program in a way that they can absorb the costs — whether it be over time or some sort of cost sharing or reimbursement mechanism with the department — we think [CMMC] will chase them out of the defense marketplace," he added.

The Pentagon is working on ways to ensure that complying with the new rules won't be cost prohibitive, Lord noted.

"One of my biggest concerns is implementing CMMC for small and medium businesses because that's where a large part of innovation comes from," she said. "We need small and medium businesses in our defense industrial base and we need to retain them."

Prime contractors have come up with ideas about how to more cost effectively accredit lower-tier suppliers that they work with, including ways to streamline the certification process, she noted.

But nobody can sidestep compliance.

"We understand that CMMC could be a burden to small companies particularly, and we will continue to work to minimize impact — but not at the cost of national security," Lord said.

Evans said primes will likely have an easier time meeting the requirements because they already have relatively robust security systems in place and extensive in-house IT expertise. However, no one is getting away scot-free, he noted.

"The primes and these traditional actors are typically going to enter at the Level 4 or Level 5 level of CMMC, which is going to be quite a bit more onerous and expensive to comply with most likely than even what they're currently doing now," he said. "The delta between Level 3 and Level 5 is going to be pretty large in terms of costs and complexities of controls."

Level 5 would be an exclusive club, Evans said. "I've not heard of any company having that level of robust security on their unclassified systems."

However, for some firms and individuals CMMC could provide a financial windfall, as 300,000 contractors in the defense industrial base move to come into compliance with the new standards and get certified.

"It's certainly a good time to be a cyber consultant or a cybersecurity expert in this space," Evans said. "A lot of NDIA members have reached out to us that offer these services.

"So we know that they're certainly out there, and I think they're going to be very useful to companies. That's going to be a pretty lucrative business to be in as companies kind of go through this initial adoption period over the next four or five years."

Lord said a number of firms are interested in being third-party assessors, but the department had not yet officially determined who is qualified.

CMMC is expected to evolve over time, as indicated by the Pentagon's referral to the recent release as version 1.0.

"Since this is a big, complex issue, I think we're going to see kind of some trial and error," Evans said. "I'm sure there will be some missteps in the coming year on both the part of the department and industry, … so I think there will be some changes there."

Lord said industry associations like NDIA will play a key role as intermediaries between the Pentagon and contractors as CMMC is rolled out.

"The role that we look to continue to play is … to transmit what's coming out of DoD, translate it for our membership, ensure that they know what's going on and they know what requirements they will be expected to comply with," Evans said.

Also, the association will look for the downsides and communicate unintended consequences to the Defense Department. "What's the cost piece? Are there companies that are actually going out of business or leaving the defense marketplace as a result?" ND

How to Avoid the Ransomware Onslaught

BY DAVID E. KITCHEN AND ANTHONY P. VALACH

Ransomware is among the most common and persistent threats faced by organizations of all sizes.

The ransomware threat landscape worsened in several significant ways through 2019 and into the current year, according to BakerHostetler's 2020 Data Security Incident Response Report. Average demands increased more than tenfold and all industry segments saw growth in attack frequency, with stark increases seen by education and government entities.

Several threat actor groups began exfiltrating sensitive data from victims as an additional means to extort a payment, the report noted.

The average ransom paid in 2018 was $28,920 and the largest payment $250,000. But that figure jumped to $302,539 the following year and the largest payment was $5.6 million, the latest report stated.

Questions had arisen in years past as to why ransomware demands seemed relatively low. By deploying ransomware, the threat actors were crippling a company's ability to function but would often settle for a five-figure payoff, while the victims were losing hundreds of thousands or millions of dollars a day due to the business interruption.

Whatever the reasons, threat actors changed their approach, and 2019 was the year they were ready to increase the stakes. This year has only seen these trends continue.

A primary reason for the demand increase stems from the rise of dedicated ransomware variants that are deployed by various groups with unique and identifiable tactics, techniques and procedures.

For example, the Ryuk attackers most often gain entry through a phishing email when victims click on a malicious link or attachment, which downloads malware — TrickBot, Emotet, Mimikatz — used to collect system credentials. The perpetrators then move laterally across the environment to encrypt as many systems as possible.

Often different groups will work in parallel, with one group exploiting vulnerabilities to gain entry and then selling the access to a second group specializing in inflicting as much encryption damage as possible. The Ryuk attackers were particularly adept in 2019 at steadily increasing demands month over month in an effort to test a victim's maximum price points.

A second example is the Sodinokibi attackers, also known as REvil, which frequently target information technology managed service providers. Once the group compromises the provider's remote management tools, they quickly move to as many downstream customer systems as possible and encrypt the systems of dozens or even hundreds of victims in one swoop.

A tip to avoid this: require vendors to implement multi-factor authentication to access an environment.

The Sodinokibi attackers often will make one very large demand for a tool to decrypt all customer systems, thereby leaving small customers at the mercy of the managed service providers to procure a tool.

Another reason that ransomware became an epidemic in 2019 was an increased focus by perpetrators on entities that traditionally have weaker security postures, particularly education and local government organizations. In past years, attackers frequently targeted large organizations, perhaps believing that they have greater capacity to pay demands.

Those organizations remain significant targets — manufacturing and professional services still lead all industry segments in attacks — however, many of these organizations have advanced cybersecurity and disaster recovery measures in place and did not pay the ransom.

Notably, across all business sizes, 73 percent of the organizations were able to restore systems without paying the ransom in 2019.

Attackers saw an opportunity to increase ransom demands as smaller and more diffuse organizations obtained cyber insurance and opened their network environments to remote access. These new victims often lacked necessary security measures such as endpoint monitoring, segregated backup systems, network segmentation and strong oversight of vendors with access to the environment, which allowed criminal groups to quickly cripple an organization, leaving no recourse but to pay the ransom in order for the business to survive.

Toward the tail end of 2019, several groups began a relatively new extortion tactic of stealing data from the environment to hedge against victims that were able to restore systems from backups. The first of these groups utilizes the Maze variant. But as the tactic has proved successful, many other groups — including Sodinokibi, Doppelpaymer, Nefilim, Snatch, Lockbit and others — have started to employ the same approach this year.

Extortion groups steal data they deem sensitive prior to deploying ransomware and then threaten to release the data to the public unless the victim pays a ransom, which is usually the same price as the ransomware demand. While the theft of personal information alone may trigger a notification obligation — both to individuals and to regulators — the threat of public humiliation introduces a new level of crisis.

A victim that does not pay the extortion demand — which itself is no guarantee of avoiding publication — is faced with conducting an investigation into an incident about which the public and regulators have already been loudly informed but for which the victim will not be able to provide meaningful answers for some time. These incidents may challenge relationships with key stakeholders such as customers, patients, shareholders and the public at large.

As reflected in the 2020 report, only 6 percent of ransomware incidents in 2019 resulted in unauthorized access or acquisition of data leading to notification obligations.

However, only six months into 2020, BakerHostetler has seen that percentage already jump several-fold and expects the trend to continue as attackers refine their tactics to obtain as much money as possible from their victims. The era of extortion is

here to stay.

The following are steps organizations can take now to avoid becoming a victim and to be better prepared to respond effectively to ransomware attacks.

First, avoid being phished. Most attacks start with an employee falling victim to a phishing email. Through phishing emails, attackers can obtain access to an organization's computer system or steal an employee's access credentials before deploying the ransomware. Conduct periodic phishing and security awareness training to help employees spot suspicious emails and avoid common social engineering tactics. Encourage employees to report suspicious emails to the IT team and express the importance of phishing vigilance throughout the organization. Look into using an email threat filter.

Next, use strong passwords. Attackers also exploit organizations with weak password policies. Require the use of strong passwords of sufficient length that must be changed periodically, prohibit reuse of passwords and implement a password management tool for employees.

Another tip: employ multi-factor authentication. The use of MFA — particularly for remote access to systems and email by employees — can lessen the risk of an attacker accessing your system or email accounts with stolen credentials. Multi-factor authentication creates an additional layer of authentication by requiring the employee to input a unique code before access is granted.

Next, secure remote access to company systems. In addition to establishing a foothold in the environment through a malicious link or an attachment in a phishing email, attackers frequently seek to connect to systems using remote desktop protocol before moving laterally within the system to deploy ransomware.

Adopt controls to restrict source internet provider addresses seeking remote access, including prohibiting connections from countries that are not essential for business operations. This can be done through hardening your firewall configuration, requiring the use of a third-party service to connect to your systems remotely, or by using a virtual private network.

Another recommendation: limit the use of domain administrator accounts. Many recent attacks have been preceded by compromise of credentials for a domain administrator account. Such accounts should be limited to select employees who need administrator permissions and, even for those employees, should not be used for normal work functions.

Administrators should have separate accounts to use for their non-administrative functions.

Also, maintain good access controls and the principle of least privilege. The greater the access a compromised employee's account has to different parts of an organization's network, the more easily ransomware can spread. A basic tenet of good cyber hygiene is to limit an employee's access to the minimum systems and files necessary to do his or her job.

It's also wise to segment the network. Attackers often move laterally to deploy ransomware to as many systems as possible. By identifying and segmenting critical data stores from systems accessible from the internet, an organization can limit the impact of an attack. Also requiring passwords with multi-factor authentication to move across environments may limit the scope of a ransomware attack.

Organizations should also ensure backups. The ones that have updated, intact and accessible backups secured and segmented from production systems are in a much better position to respond to and recover from a ransomware attack. Adopt and implement a procedure for the creation, updating and storage of on-site and off-site backups of all critical files and data. Be sure to include procedures for verifying and testing backups and for securing them so they are not impacted by the ransomware attack.

Another mistake is that firewalls are not configured properly. Many types of ransomware attempt to move laterally within systems using standard Windows operating system protocols, including server message block, to communicate between endpoints within a system. Ensure that Windows firewall policy is configured properly to restrict the scope of permitted communications between common endpoints. Attackers often exploit software vulnerabilities that could have been remedied by regular and timely deployment of the software developer's updates and patches.

In addition, periodically evaluate business continuity, disaster recovery and incident response plans to ensure they align with the current threat landscape. Consider yearly incident response tabletop exercises to test the organization's ability to timely and effectively respond to a security incident.

Another tip: enable appropriate security logging and retention to ensure forensic artifacts can be reviewed in the event of an incident. Often, default logging settings do not provide an organization enough information to investigate an incident. Also, ensure the logs are stored for a sufficient amount of time and are secure in the event of a system compromise.

Knowing daily business losses in the event systems are unavailable is also an important data point in an organization's ransom payment analysis. Paying a ransom is a business decision where the only leverage an organization has are time and the ability to restore from backups. Even if recovery from backups is possible, it may make business sense to pay a ransom if the losses exceed the demand.

Finally, deploy endpoint monitoring, which can detect system anomalies and malware, such as credential harvesting tools that often precede a ransomware attack.

Evaluate the current endpoint monitoring solution, and determine whether it should be upgraded to properly protect against the current malware and ransomware threats. ND

David E. Kitchen is a partner and Anthony P. Valach counsel at the law firm of BakerHostetler. The views expressed in this article are those of the authors and not necessarily those of BakerHostetler or its clients.