WE ARE KMS

Manage Your Cyber Risk Webinar
9.9.21

KANSAS MANUFACTURING SOLUTIONS

Trusted Advisors for Growth

www.weareKMS.com

WEBINAR HOUSEKEEPING

- Everyone attending the webinar is muted. To ask a question, type your question in the Q/A text box on your GoToWebinar panel.
- We will ask as many questions as we can at the end of the presentation.
- This webinar is being recorded. The link to the recording will be included in a follow-up email being distributed tomorrow.
- Please check our website **www.wearekms.com** frequently for new webinars and events.

KANSAS MANUFACTURING SOLUTIONS
Trusted Advisors for Growth

WE ARE KMS

Kansas Manufacturing Solutions exists to help small to mid-size manufacturers in Kansas compete and grow.

From trusted advisor to vocal advocate for manufacturing in Kansas, we are working to help you be successful by providing value proven solutions to increase your competitiveness in the domestic and global markets.

KANSAS MANUFACTURING SOLUTIONS
Trusted Advisors for Growth

Manage Your Cyber Risk Webinar

Raja Paranjothi
Principal at Oread Risk & Advisory

Mike Gutierrez
Director of Client Integrations at PayIt

KANSAS MANUFACTURING SOLUTIONS
Trusted Advisors for Growth

KMS Meeting
September 2021

Introduction

Michael Gutierrez

- 15+ years IT/Manufacturing/Business Experience
- Director of Client Integrations - PayIt
- Former Director of IT - Safe Fleet
- https://www.linkedin.com/in/msg390/

System HelpDesk

Jenny Davison <j.davison@qub.ac.uk>

Sent: Thu 12/12/2013 1:51 p.m.

To: Jenny Davison

You have reached the storage limit on your mailbox. Please visit the below link to restore your email access.

http://wb-admins2.phpform.com.us/f/d2e17444cf1

System HelpDesk Copyright © 2013 # • • ALL RIGHTS RESERVED

See more about: Jenny Davison.

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]

Sent: Monday, September 25, 2017 1:39 PM

To:

Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify..

Verify Now

Microsoft Security Assistant

Microsoft office365 Team! ©2017 All Rights Reserved

MSSP Alert (blog)

Mailto Ransomware Attacks Michigan State

Michigan State University (MSU) recently suffered a Ma
attack, though the overall impact of the attack has not b

2 hours ago

STATE

Texas transporta
ransomware atta

ZDNet

Thousands of enterprise systems infecte
Mockingbird malware gang

Researchers say Blue Mockingbird attacks public-fa
ASP.NET apps that use ... The Mac malware most li

6 days ago

Bloomberg Law

INSIGHT: Ransomware Attacks Compound (

INSIGHT: Ransomware Attacks Compound Covid-19 Bus
Marshall L. Miller. May 19, 2020, 8:01 AM. Listen. Cyberc
the ...

2 weeks ago

NATIONAL SECURITY

What We Know About The Ransomware Attack On A Critical U.S. Pipeline

Updated May 10, 2021 · 8:29 PM ET

SCOTT NEUMAN

Fuel tanks are seen at a Colonial Pipeline Co. delivery point Monday in Baltimore. The company's pipeline was hit with a major ransomware attack last week.

Jim Watson/AFP via Getty Images

2 weeks ago

ributors; Hackers

ed data files belonging to
k that reportedly ...

ets Enterprise Servers Then

of patient ransomware attacks that
ing. A Java-based ransomware ...

cond Time in 2020

are attack against Toll
that extends across ...

Results in Data

had fallen victim to a
he Magellan ...

09/29/18

D-Day

About Safe Fleet

- 14 Locations US/Canada
  - 750MM ARR
  - 500 Users
  - 1,110 Devices
  - Hybrid Network
  - 10 people total in IT
- No major cyber incidents

09/29/18 Events

- 6 AM - Call received from IT Lead in NC
- All servers were inaccessible
- Evidence of ransomware attack
- Received two more calls from other locations same issue was happening
- Spun up entire team with emergency conference line

“We need to stop the bleeding, proceed with taking everything offline”

- Michael Gutierrez

Initial Investigation

- Confirmed we have been hit by a ransomware attack
- All domain controllers, file servers, databases, erp system encrypted
- All on-site and off-site backups wiped/destroyed

RyukReadMe.txt - Notepad

File Edit Format View Help

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation.
More than a year ago, world experts recognized the impossibility of deciphering by any means except the original decoder.
No decryption software is available in the public.
Antiviruse companies, researchers, IT specialists, and no other persons cant help you encrypt the data.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT DELETE readme files.

To confirm our honest intentions.Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
2 files we unlock for free

To get info (decrypt your files) contact us at
LindaMccann@protonmail.com
or
LindaMccann@tutanota.com

You will receive btc address for payment in the reply letter

Ryuk

No system is safe

Next Steps

- Briefed Senior Leadership on situation
- Continued Investigation on what could be done internally
- Filed a claim with insurance vendor
- Third party Cyber Incident firm contacted

Incident Response

- Incident firm determined this was a new type of cyber intrusion coupled with ransomware (emotet)
- No one has seen a decryption key before through common channels
- All efforts to attempt to undo the damage failed
- Began mitigation process
  - Upgraded malware/antivirus
  - Running information scans to collect data.
- Setup conference room to be a war room

Incident Response (cont.)

- It was decided to use contact the attackers and get the ransom amount for decryption key
- Simultaneous effort to attempt to undo the work of the attack after systems were cleaned
- Created and implemented plan to get offline systems in place to operate the businesses and ship product

Attackers Responded

- Ransom ask was to send 50 bitcoins
- 50 bitcoins = $500,000
- 72 hours to send the funds

Regroup

- Decided to acquire the bitcoin in case we were going to pay the ransom
- Continued effort to figure out if we could crack the code and clean/decrypt systems
- Sent notice to attackers we were going to pay ransom

Critical Path

- Get the files decrypted
- Pulling 12+ hour days
  - Cleaning and mitigating networks
  - Some computers had to be completed wiped and started over
  - All windows 7 machines retired and ordered replacements
  - Continued effort on trying to decrypt files ourselves

Less than 24 hours left...

- Discovered way to clean off systems that had the payload installed on the system but files were not decrypted
- However, all efforts to decrypt data failed
- Final approval to send bitcoin was approved by executive management
- Ready to send

BUT THEN……..

Hope

- A copy of the exact ransomware/decryption key was acquired by a contact in the FBI
- Never been tested or validated
- On the clock to the deadline
- Let the testing begin!

Hope

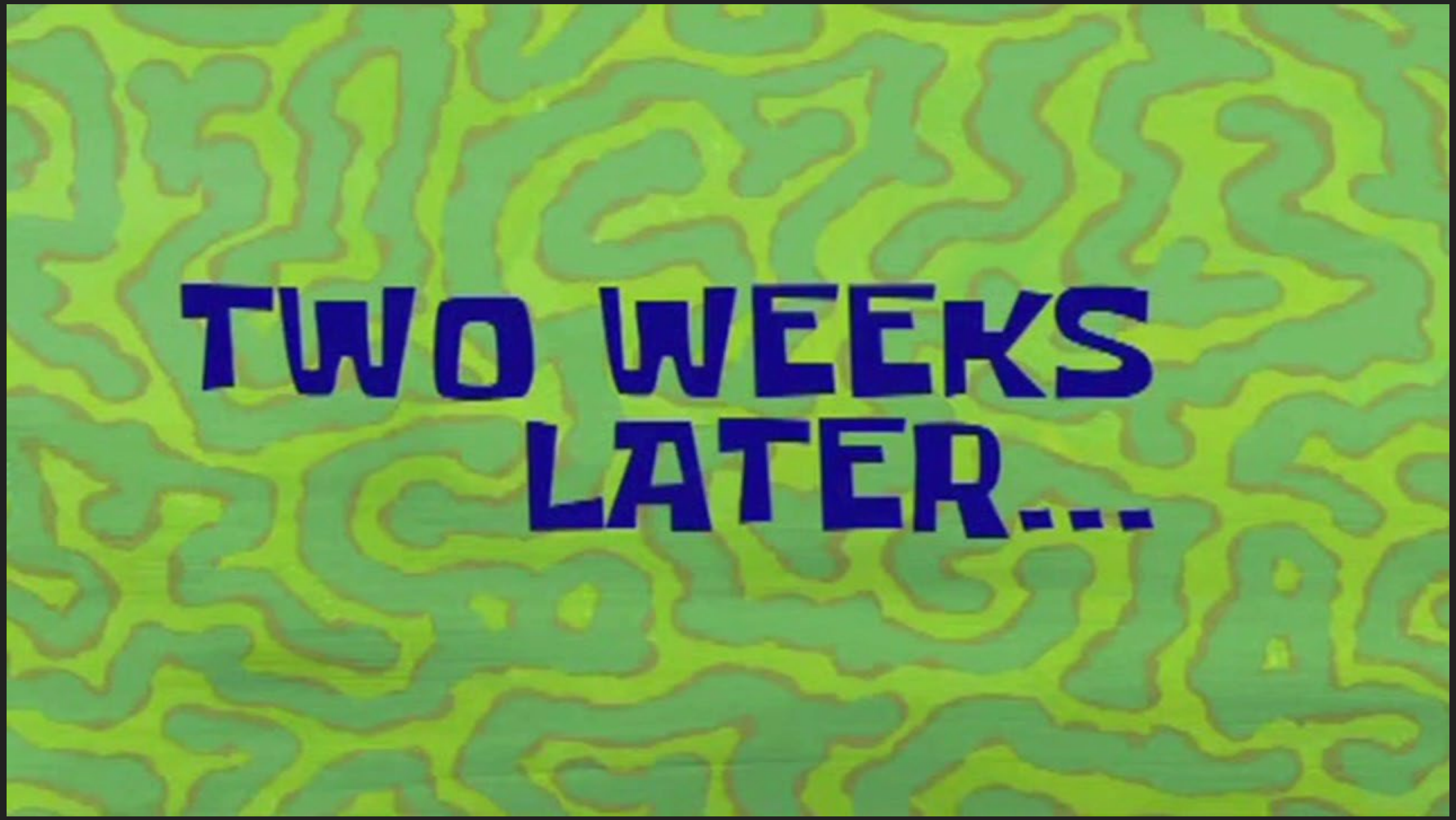
- After about three hours…
- No luck in running the decryption successfully
- Decided to take a chance and ask for an extension with the attackers
- They accepted and gave us another 24 hours
- Continued to work to see if the decryption program working

11th hour

- After another 8 hours of work…
- The decryption program is working
- Decided not to pay the attackers the ransom
- Now some of the real work begins...

Let the decryption begin...

- Good news - program works great
- Bad news - decryption works one file at a time.
- Terabytes of data to decrypted across 100+ servers
- Average server taking 8 hours to fully decrypt


TWO WEEKS
LATER...

Fast Forward...

- Decryption of servers still in progress
- Started hardening of the network

10/27/18

The New Normal

Summary

The Good

- Great response by the team to address the issue
- Impact the business during the crisis was manageable
- No data was exfiltrated from the network
- No data loss to the company

The Bad

- Hit with a large wide scale attack that took the entire network down.
- Spent the next 30 days trying to recover the network
- The lost cost to the business was about $1.5 MM after insurance claim

Lessoned Learned

- Always prepare for the worst
- Don’t be afraid to leverage the expertise
- Get involved
- Prep the business what the cost is for cyber security
- Consider a cyber security insurance policy
- Consider a managed services agreement
- Test, Test, Test

Thanks!

Contact me:

Michael Gutierrez

mgutierrez@mikegutierrez.com

OREAD RISK & ADVISORY, LLC

Kansas Manufacturing Solutions

Manage Your Cyber Risk

September 9, 2021

Agenda

1. Supply Chain Attacks
2. Security Frameworks
3. Practices to implement
4. CMMC Overview
5. CMMC-AB Update

Appendix

- Appendix A: CMMC Practice Areas, & Standards
- Appendix B: BIOs

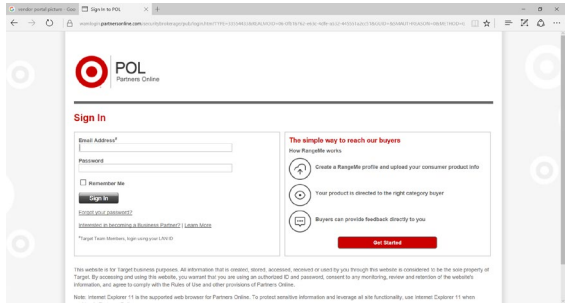
OREAD RISK & ADVISORY

Supply Chain Attacks

Cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers

Example attacks include Target, SolarWinds, etc.

Target Breach



OREAD RISK & ADVISORY

Security Frameworks

- NIST 800-171
- NIST CSF
- CIS
- PCI
- ISO 27001
- CMMC

What should we do?

- **Vendor Management**
  - Assess security and practices of vendor before contracting with them
  - Assess vendor on annual basis (security questionnaire, SOC report, etc.)
- **Security awareness training**
  - Annual training for employees
  - Email phishing exercises
- **Incident Response Management**
  - Develop an Incident Response Plan
  - Test the plan

What should we do? Cont'd

- **Access Account Management**
  - Password Settings
  - Implement MFA
  - Limit administrative access to a few personnel
  - Implement least privilege access
- **Data Recovery**
  - Establish and maintain a Data Recovery Process
  - Test Data Recovery
- **Penetration Testing**
  - Perform external pen tests annually
  - Perform internal scans of network

What should we do? Cont'd

- **Malware Defenses**
  - Implement an effective Anti-Malware solution
  - Make sure all employees PC's have the solution implemented with updates being made
- **Keep up to date on security news**
  - Cisa.gov (Cybersecurity & Infrastructure Security Agency)
  - krebsonsecurity
- **Internal Risk Assessment**
  - Assess yourself annually
  - Remediate any identified deficiencies

What should we do? Cont'd

- **Vulnerability Management**
  - Windows Updates
  - Software Updates
- **Data Protection**
  - Encrypt data at rest
  - Encrypt data in transit
  - Securely Dispose of data

OREAD RISK & ADVISORY, LLC

CMMC Readiness and Approach

CMMC Overview

OREAD RISK & ADVISORY

What is CMMC?

1. The **Cybersecurity Maturity Model Certification (CMMC)** is a new cybersecurity framework and accompanying certification by the US Department of Defense (DoD). The goal of the new CMMC compliance requirement is **to protect Federal Contract Information (FCI)** and **Controlled Unclassified Information (CUI).**

OREAD RISK & ADVISORY

What is CMMC Cont'd.?

2. This new umbrella standard includes requirements from NIST 800-171, the Federal Acquisition Requirements (FAR) document 52.204-21, and beyond. There are five levels of CMMC certification. Each level requires more practices and controls than the previous. Most organizations will have to comply with either Level 1 or Level 3. The **certification is valid for three years.**

What is CMMC Cont'd.?

3. Starting this year, contracts offered by the DoD might specify a level of the CMMC required to be awarded the contract. **By the end of 2025 all contracts will require a CMMC certification**. Unlike for the current NIST 800-171 requirements there will be **no self-assessment accepted**. Instead, the certification audit will be performed by Certified 3rd Party Assessor Organizations (C3PAO).

Who Needs CMMC?

1. Only contracts for Commercial off-the-shelf (COTS) products will be exempt from CMMC compliance requirements.

2. Any company and its subcontractors that bid on a DoD contract that contains **Federal Contract Information (FCI)** or **Controlled Unclassified Information (CUI)** will be required to be CMMC compliant.

Which Level of CMMC Will We Need?

The CMMC level mandated will be stated in the contract information. The majority of contracts will require a Level 1 or Level 3 certification.

As a general rule:

- If your company will receive exclusively FCI under the contract, then your will need CMMC Level 1 implementation and certification.
- However, if your organization will receive CUI in addition, then CMMC Level 3 will be required as a minimum.

When Will This Be Required?

The DoD **started rolling out** CMMC compliance requirements for new contracts **beginning of 2021.** The expectation is that by the **end of 2025 every active contract will have a CMMC level requirement** in place. Approximately 15 prime contractors and 1500 sub-contractors will have CMMC requirements in 2021.

When Will This Be Required? Cont'd

Although not every contract will require CMMC compliance right away, we highly recommend that companies who plan to bid on DoD contracts **start preparations for their CMMC certification now**. The early adopters of CMMC will have a clear competitive advantage – especially considering that implementation and certification could take several months and **certification is required at the time of contract award**. The sooner your organization meets CMMC compliance, the less competition it will face when bidding on new DoD contracts that require CMMC.

How Long Does It Take To Implement CMMC?

The implementation timeframe depends on these main factors:

- The level of certification are you required to comply with
- The current state of your NIST 800-171 implementation
- The size and scope of your system.

CMMC-AB Update

“Unifying 300k+ voices is a formidable challenge. Getting it right will involve trial, error, and error”

CMMC-AB August Town Hall

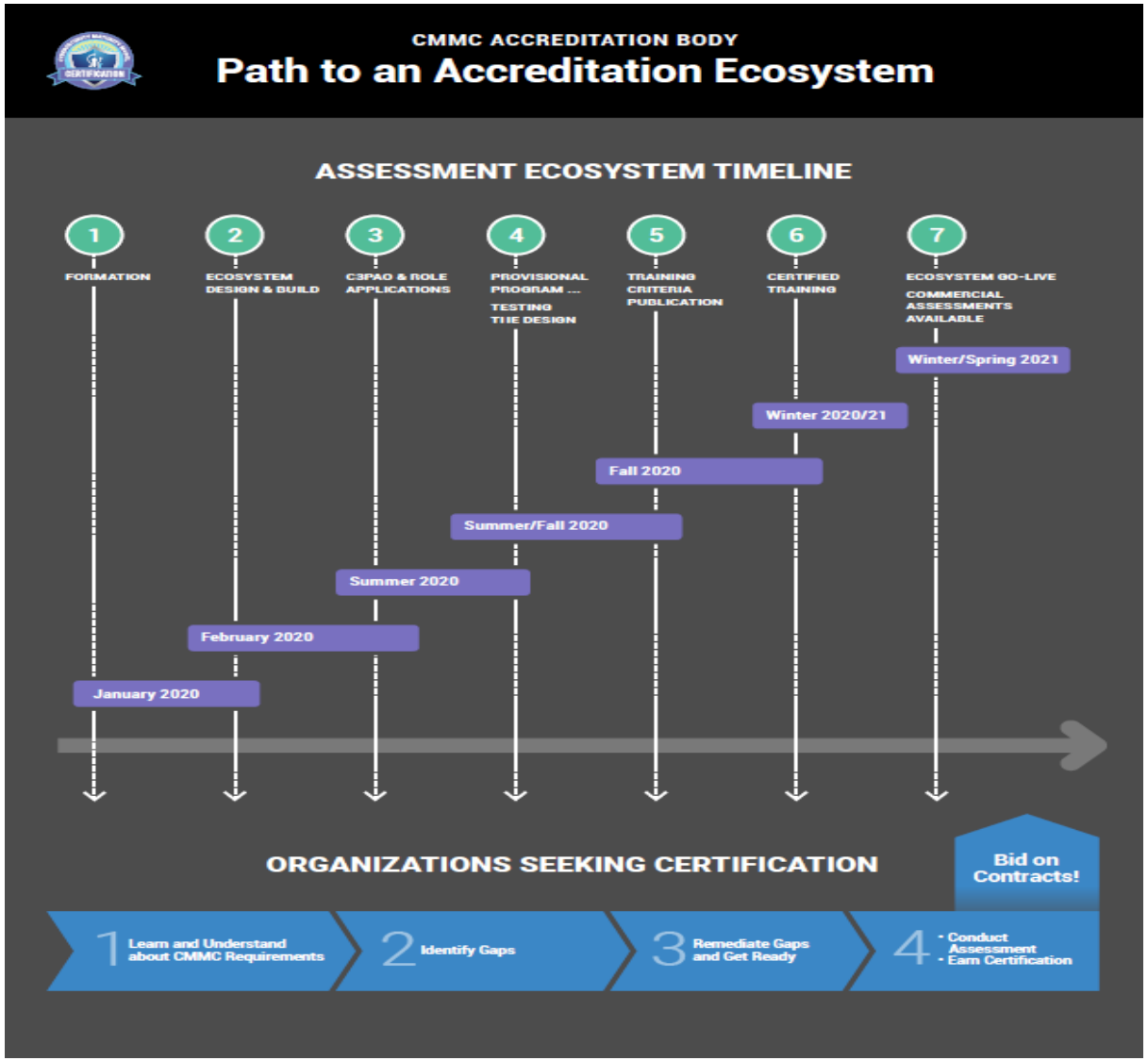
August

OREAD RISK & ADVISORY

CMMC-AB Update

1. Despite initial hiccups, CMMC-AB is building critical mass.
    a. Stakeholders agree CMMC is necessary
        i. Bipartisan support
    b. Infrastructure being built:
        i. Governing body formed
        ii. Assessor capabilities created
        iii. Training standards taking shape
        iv. Recognition audits will be virtual
2. Other USG departments likely will adopt CMMC standards.
3. DoD's message: "Begin now. Late adopters will struggle."
4. Obtain CMMC certification or become ineligible to bid on DoD contracts.

What We Should Do Now?
A Call to Action



1. Understand CMMC
2. Identify Gaps
3. Remediate Gaps
4. Schedule Assessment
5. Earn Certification
6. Bid On Contracts

OREAD RISK & ADVISORY

Appendix

OREAD RISK & ADVISORY

Appendix A: CMMC Practice Areas

CMMC Model v1.0 Number of Practices Per Source

CMMC Level	Total Number Practices Introduced per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B **	Other
Level 1	17	15*	17*	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11

CMMC Level 1 only addresses practices from FAR Clause 52.204-21

CMMC Level 3 includes all of the practices from NIST SP 800-171r1 as well as others

CMMC Levels 4 and 5 incorporate a subset of the practices from Draft NIST SP 800-171B plus others

Additional sources, such as the UK Cyber Essentials and Australia Cyber Security Centre Essential Eight Maturity Model, were also considered and are referenced in the model

Appendix A: CMMC Practice Areas By Level

Domains	Capabilities	Tot. Practices per Domain	Practices per Level				
			Level 1	Level 2	Level 3	Level 4	Level 5
Access Control	4	26	4	10	8	3	1
Asset Mgmt.	1	2	0	0	1	1	0
Audit & Accountability	4	14	0	4	7	2	1
Awareness & Trng.	2	5	0	2	1	2	0
Configuration Management	2	11	0	6	3	1	1
Identify and Authorization	1	11	2	5	4	0	0
Incident Response	5	13	0	5	2	2	4
Maintenance	1	6	0	4	2	0	0
Media Protection	4	8	1	3	4	0	0
Personnel Security	2	2	0	2	0	0	0
Physical Protection	1	6	4	1	1	0	0
Recovery	1	4	0	2	1	0	1
Risk Management	2	12	0	3	3	4	2
Security Assessment	3	8	0	3	2	3	0
Situational Awareness	1	3	0	0	1	2	0
Sys and Comms Protection	2	27	2	2	15	5	3
Systems and Info Security	4	13	4	3	3	1	2
		Total Practices per Level	**17**	**55**	**58**	**26**	**15**

CMMC Standards

Carnegie Mellon University

- CERT Resilience Management Model (CERT RMM) v1.2

ACQUISITION.GOV

- FAR Clause 52.204-21

ISO International Organization for Standardization

- ISO 27001, ISO 27032

National Cyber Security Centre
a part of GCHQ

- UK Cyber Essentials

NIST

- NIST SP 800-171 Rev 1
- Draft NIST SP 800-171B
- NIST Framework for Improving Cybersecurity (CSF) v1.1

- CMMC Model v1.2

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

- Australia Cyber Security Centre Essential Eight Maturity Model

CIS Center for Internet Security®

- CIS Controls v7.1

AIA
AEROSPACE INDUSTRIES ASSOCIATION

- AIA NAS9933

OREAD RISK & ADVISORY

Appendix B: Bio - Raja Paranjothi

Raja is currently a Principal with Oread Risk & Advisory, a Risk Consulting and Attestation firm. Raja has over 20 years of experience providing client and consulting services with expertise in IT Security, Risk Assessments, HIPAA assessments, PCI, IT audits, IT Governance and Compliance and SOC reports.

Prior to starting Oread Risk & Advisory:

Raja directed a $1.3 million Business and Technology Risk Services practice in the Kansas City office of CBIZ & Mayer Hoffman McCann. Responsibilities include developing new business and client relationships, managing SOC engagements, IT Audits, PCI reviews, Internal Audits, SOX and IT Risk & Security engagements. Client industries include Technology, Banking and Financial Services and Retail.

Raja as a Senior Consultant within the Enterprise Risk Services practice of Deloitte & Touche, managed IT control assessment engagements and teams for Fortune 1000 clients to identify potential risks in process and information technology controls for general computer control compliance within corporate audits, SAS70s and Sarbanes-Oxley 404 attestations. Client industries include Retail, Government, Utilities, Banking and Financial services.

.

CERTIFICATION
CISA – Certified Information Systems Auditor

PROFESSIONAL ASSOCIATION
ISACA
ISC2

EDUCATION
B.S Business Administration & Accounting
M.S. Accounting and Management Information Systems
University of Kansas

OREAD RISK & ADVISORY

Appendix B: Bio - Dan Carter

Dan Carter is responsible for the management consulting practice of Policy Solutions. Dan guides senior management with a business-oriented, delivery-focused perspective that enables organizations to achieve strategic, risk, and transformational objectives. He is actively involved with the business development, client delivery, resource management and thought leadership to clients. Dan specializes in strategy, policy, process, and execution of strategic growth for the Fortune 100, large, midsize, and small companies across a broad range of industries.

Management consulting expertise and impact : corporate development, globalization, growth, innovation, information technology, operations, organizational design, post-merger integration, risk, strategy, sustainability, transformation, and turnaround.

Prior to Policy Solutions, Dan developed a management consulting practice for CBIZ MHM (the eighth largest accounting firm in the U.S as well as advisory role across several industry sectors. Earlier in his career, he served in management and technology consulting roles including: Sprint's finance business intelligence capabilities, National Association of Insurance Commissioners (NAIC) multi year re-engineering of its core systems; and as Arthur Andersen's liaison in building the North Central system capabilities of the Resolution Trust Corporation. He has presented at several forums including Society of Actuaries, CIO Exchange, IIA, ISACA, and industry specific conferences.

Industries served: data and cyber security, electronic commerce, energy, financial services, state & and federal government, healthcare, hospitality, high tech, insurance, InsurTech, manufacturing, not-for-profit, private equity, real estate, renewables and environment, retail, sustainable mobile eco-system, telecommunications, transportation, & venture capital.

Dan also served as Chapter Director for the COO Forum, a professional development association of Second-in-Command Executives: Chief Operating Officers, Operating CFOs, General Managers, Divisional Presidents, Operating CIOs, and Executive Vice Presidents.

CERTIFICATION
R2:2013 Auditor
ISO14001:2004 Auditor
ISO14001:2015 Auditor

PROFESSIONAL ASSOCIATION
2008 to Present, Council Member
Gerson Lehrman Group (GLG)

2009 to 2015, Chapter Director:
COO Forum

2012, Moderator, CIO Exchange

2011 Co-Chair Greater Kansas Chamber of Commerce "Innovation Conference"

Greater Kansas City Chamber of Commerce "Innovation Conference 2010: The Application of Innovation" Moderator and Planning Committee

Greater Kansas City Chamber of Commerce "Innovation Conference 2009: Innovation in Turbulent Times" Planning Committee

Publication, Ingram's Magazine
July 2004 "The Future is Now" – Sprint Arena

EDUCATION
B.S. Business Administration/Accounting
Pensacola Christian College

OREAD RISK & ADVISORY

Questions?

OREAD RISK & ADVISORY

FINISHING UP

- This webinar has been recorded. A link to the webinar replay and a PDF of the presentation deck will be included in a follow-up email to you tomorrow.
- KMS is offering Kansas manufacturers a no-cost cybersecurity readiness review and gap analysis. Visit www.wearekms.com/kms-connect-cybersecurity-readiness-review to request yours.

- Send additional questions to Phil@wearekms.com.

KANSAS MANUFACTURING SOLUTIONS
Trusted Advisors for Growth