# Cybersecurity Risks and the Cybersecurity Maturity Model

Loren Wagner
lwagner@centracomm.net

CENTRACOMM
Trusted to secure and manage hybrid networks.

**Loren Wagner**
Director of Risk
lwagner@centracomm.net

Loren is actively engaged in helping organizations become more secure and compliant by performing risk assessments and advisory services based on the NIST Cybersecurity Framework, NIST SP 800-171, and the DoD's Cybersecurity Maturity Model Certification (CMMC) program. Loren is a designated CMMC Registered Practitioner.

Prior to joining CentraComm, Loren held global senior management positions for a major manufacturer in information security, networking, and data center operations. Loren is a respected expert in his field and has presented papers and provided dozens of presentations to organizations regarding risk mitigation, cybersecurity & information technology.  Loren has a Doctorate in Information Assurance from the University of Fairfax, an MBA from The University of Findlay and a Certificate in Security Management from the National Defense University. A part-time lecturer at the University of Findlay for more than 20 years, he played a major role in the development of their Information Assurance Program.

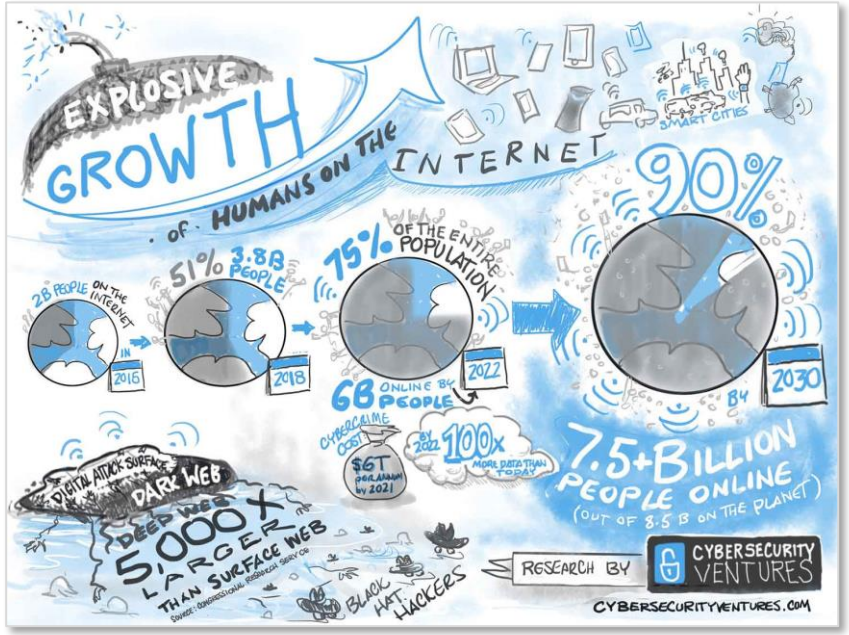
# Agenda

- Part 1
  - Threat Overview
  - Practical Tips
  - Cybersecurity Take-Aways & Action Steps
- Part 2
  - Cybersecurity Maturity Model Certification (CMMC) Introduction
  - NIST Interim Rule & Supplier Performance Risk System (SPRS)
  - CMMC Updates
  - NIST 800-171 Implementation

# The Daily Barrage

Practically every day, we see news articles or receive alerts relating to another organization falling victim to a ransomware attack or this season's scam.

- Ransomware
  - Kaseya
  - Colonial Pipeline
  - Solarwinds
  - Microsoft Exchange
- Payment Scams
  - Business Payments
  - Unemployment
  - Delivery Scams
  - IRS




CENTRACOMM

# What If This Were To Happen To My Company?

- Am I completely helpless and unable to defend against these business-impacting events?
- If there are steps to avoid becoming a victim, what are they?

# What Are the Stats Telling Us?

- As of Q1 2021 average ransomware payment=$220,298. Up 43% since Q4 2020. - Coveware
- Most affected clients experienced *3 to 14 days of downtime*. – NinjaRMM
- According to RSA Security, *the future* of this growing threat will include not just a lockdown on integral files and folders, but access to networks and accounts. - RSA Security


CENTRACOMM

# The Totality of Loses

What Can a Small Business Do To Prevent Becoming One of These Statistics?

**By Victim Loss**

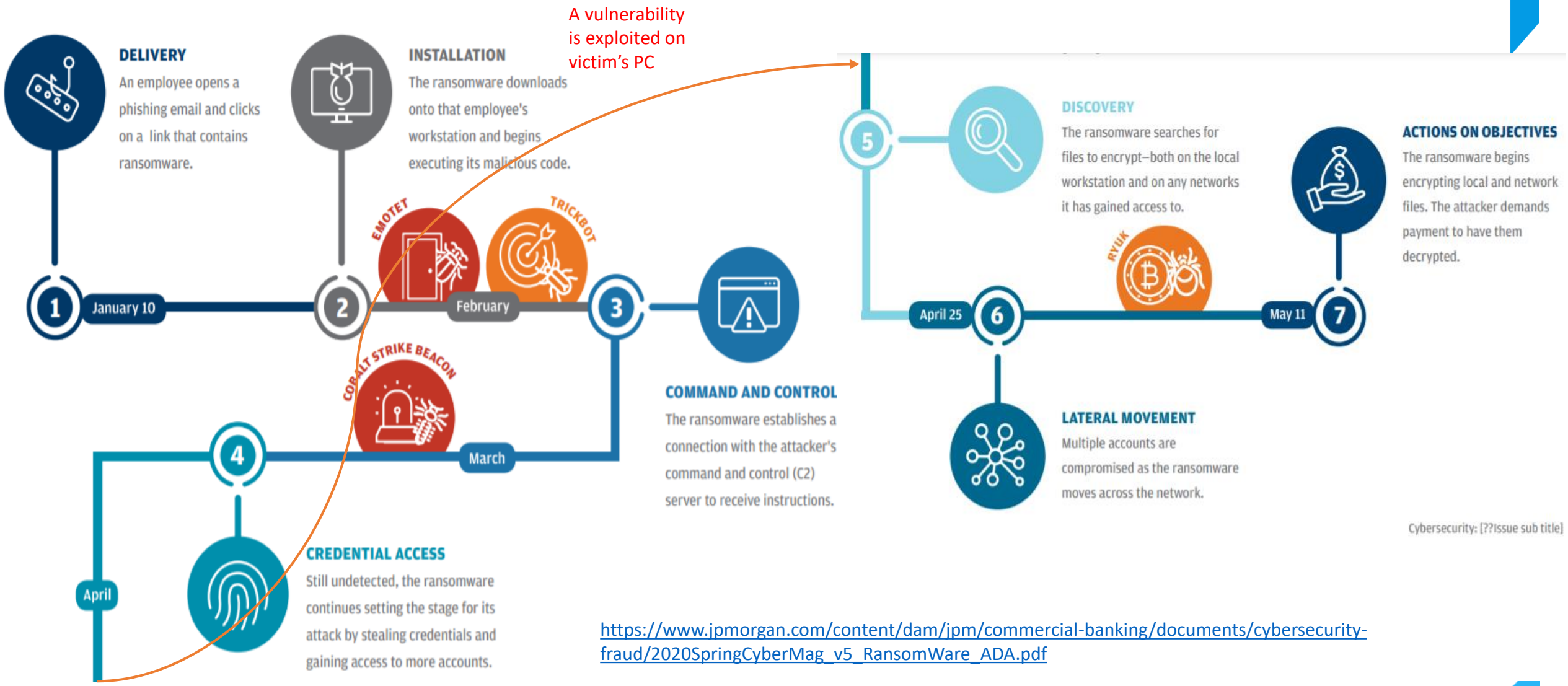
| Crime Type | Loss | Crime Type | Loss |
|---|---|---|---|
| BEC/EAC | $1,866,642,107 | Overpayment | $51,039,922 |
| Confidence Fraud/Romance | $600,249,821 | Ransomware | **$29,157,405 |
| Investment | $336,469,000 | Health Care Related | $29,042,515 |
| Non-Payment/Non-Delivery | $265,011,249 | Civil Matter | $24,915,958 |
| Identity Theft | $219,484,699 | Misrepresentation | $19,707,242 |
| Spoofing | $216,513,728 | Malware/Scareware/Virus | $6,904,054 |
| Real Estate/Rental | $213,196,082 | Harassment/Threats Violence | $6,547,449 |
| Personal Data Breach | $194,473,055 | IPR/Copyright/Counterfeit | $5,910,617 |
| Tech Support | $146,477,709 | Charity | $4,428,766 |
| Credit Card Fraud | $129,820,792 | Gambling | $3,961,508 |
| Corporate Data Breach | $128,916,648 | Re-shipping | $3,095,265 |
| Government Impersonation | $109,938,030 | Crimes Against Children | $660,044 |
| Other | $101,523,082 | Denial of Service/TDos | $512,127 |
| Advanced Fee | $83,215,405 | Hacktivist | $50 |
| Extortion | $70,935,939 | Terrorism | $0 |
| Employment | $62,314,015 | | |
| Lottery/Sweepstakes/Inheritance | $61,111,319 | | |
| Phishing/Vishing/Smishing/Pharming | $54,241,075 | | |

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

CENTRACOMM

# The 7 Stages of Ransomware Attacks

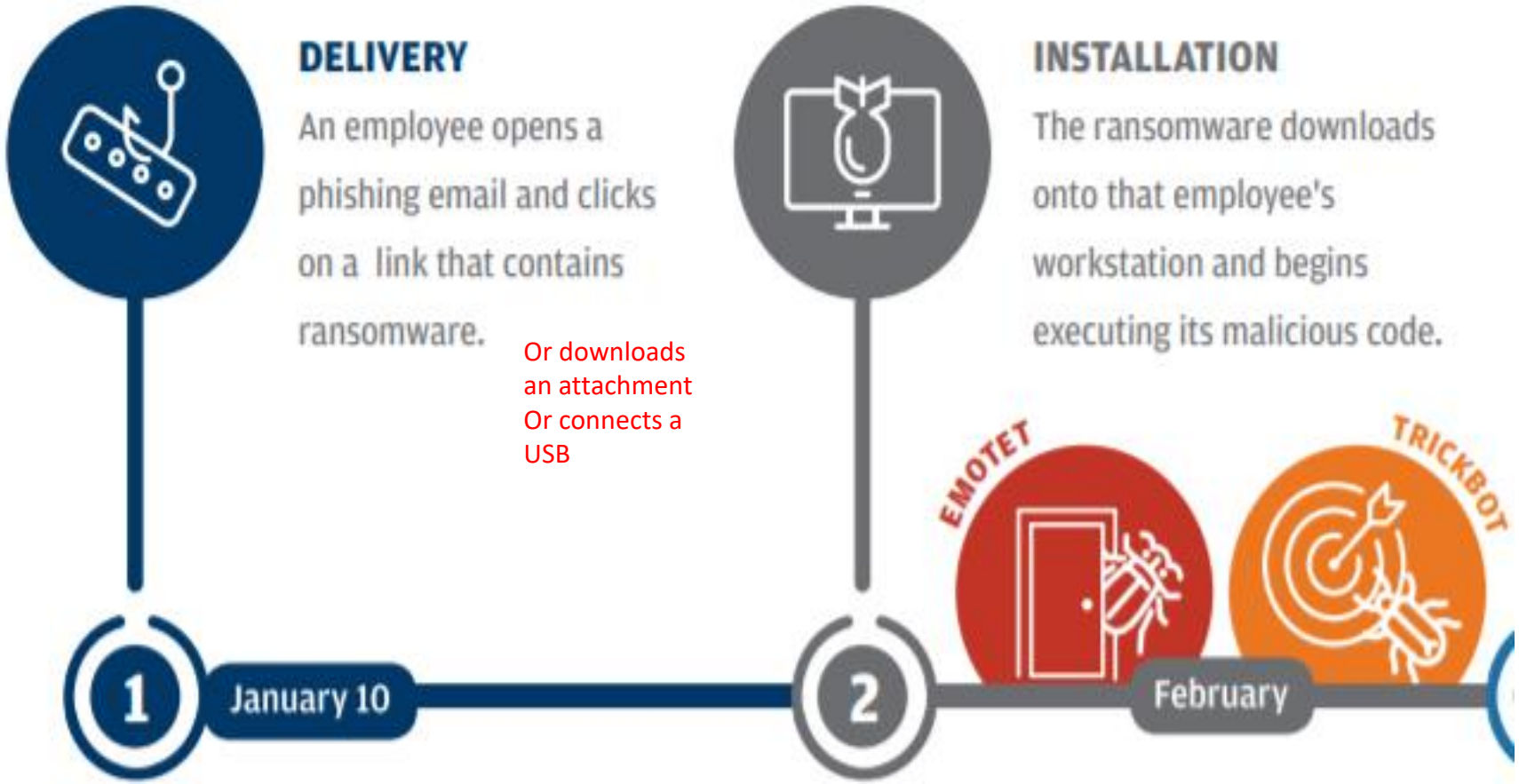



Cybersecurity: [??Issue sub title]

https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/cybersecurity-fraud/2020SpringCyberMag_v5_RansomWare_ADA.pdf

# Breaking Down The Threat

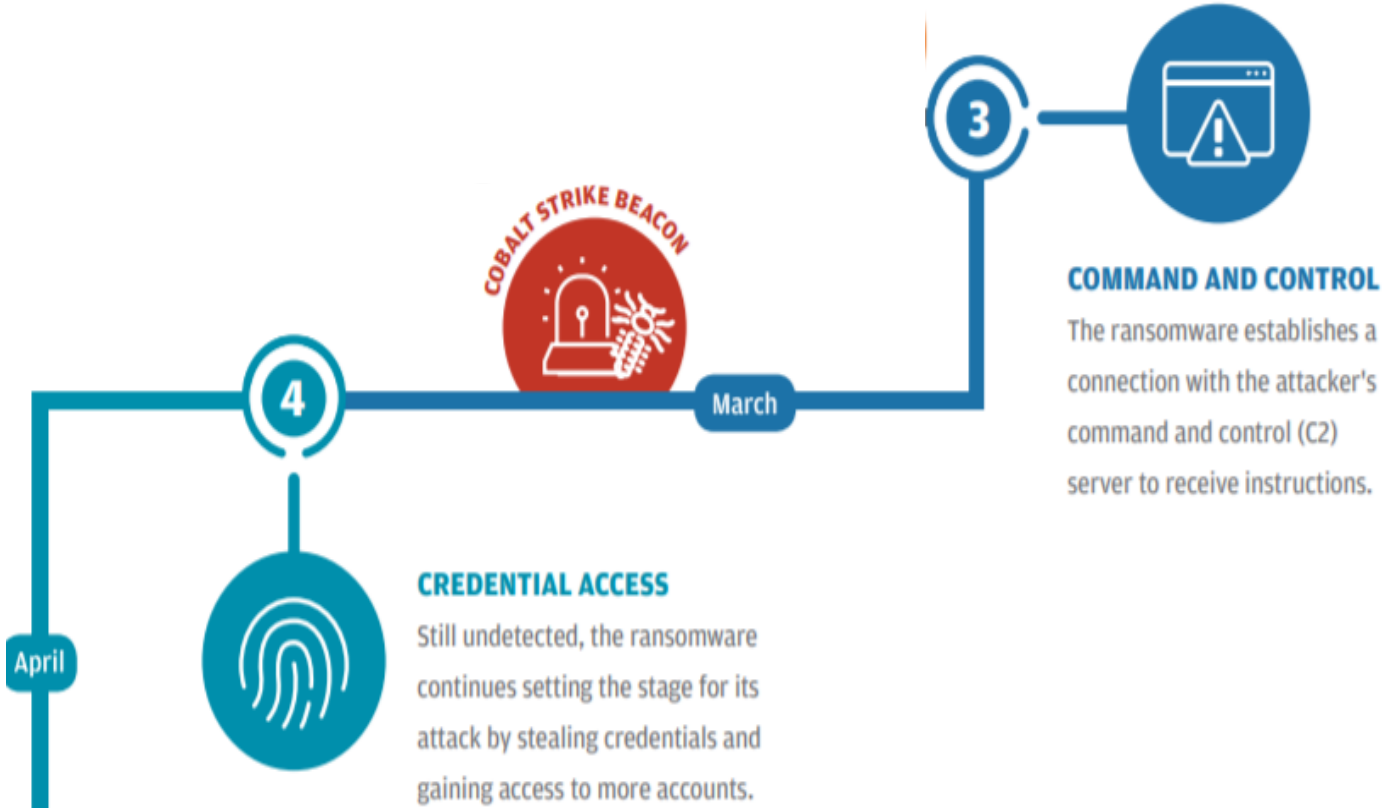
A vulnerability is exploited on victim's PC




https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/cybersecurity-fraud/2020SpringCyberMag_v5_RansomWare_ADA.pdf

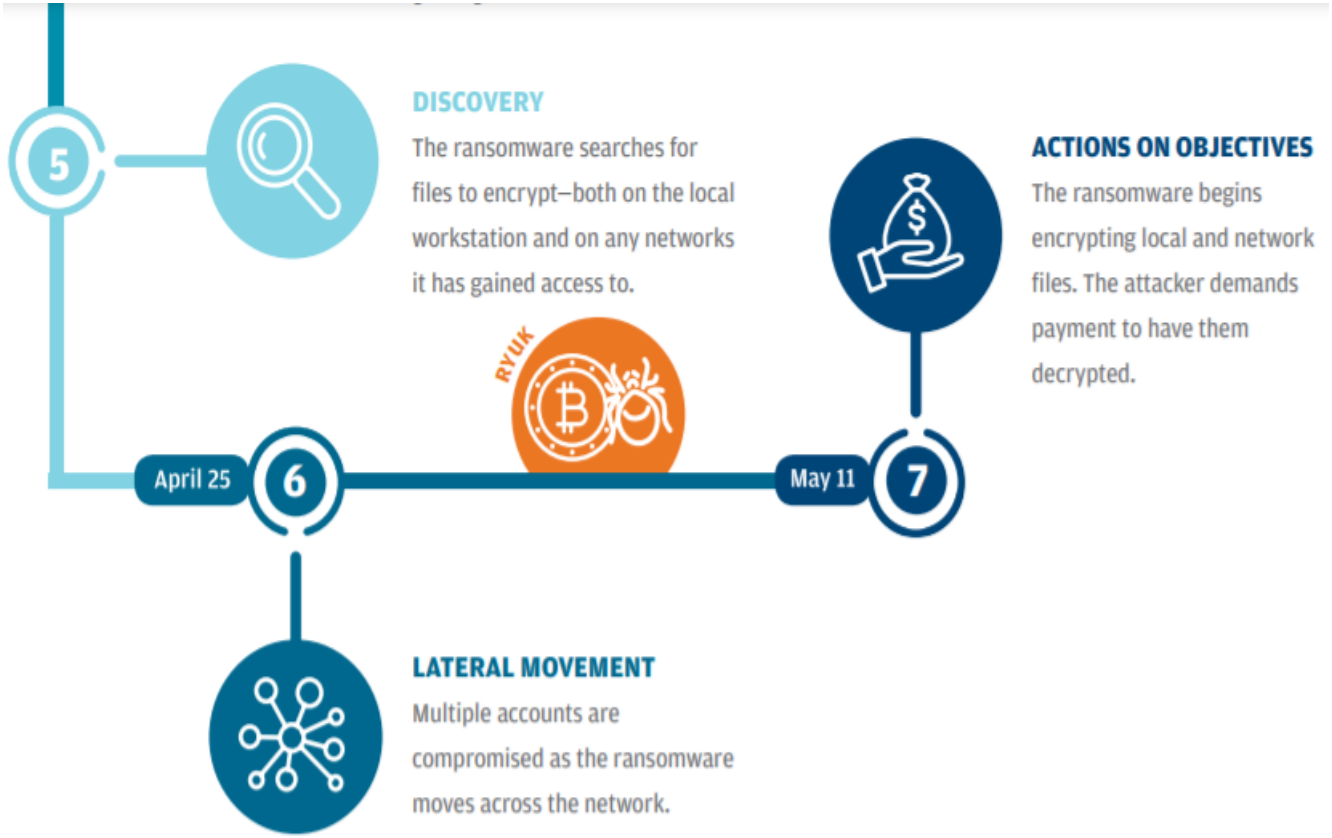
CENTRACOMM

# Breaking Down The Threat




https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/cybersecurity-fraud/2020SpringCyberMag_v5_RansomWare_ADA.pdf

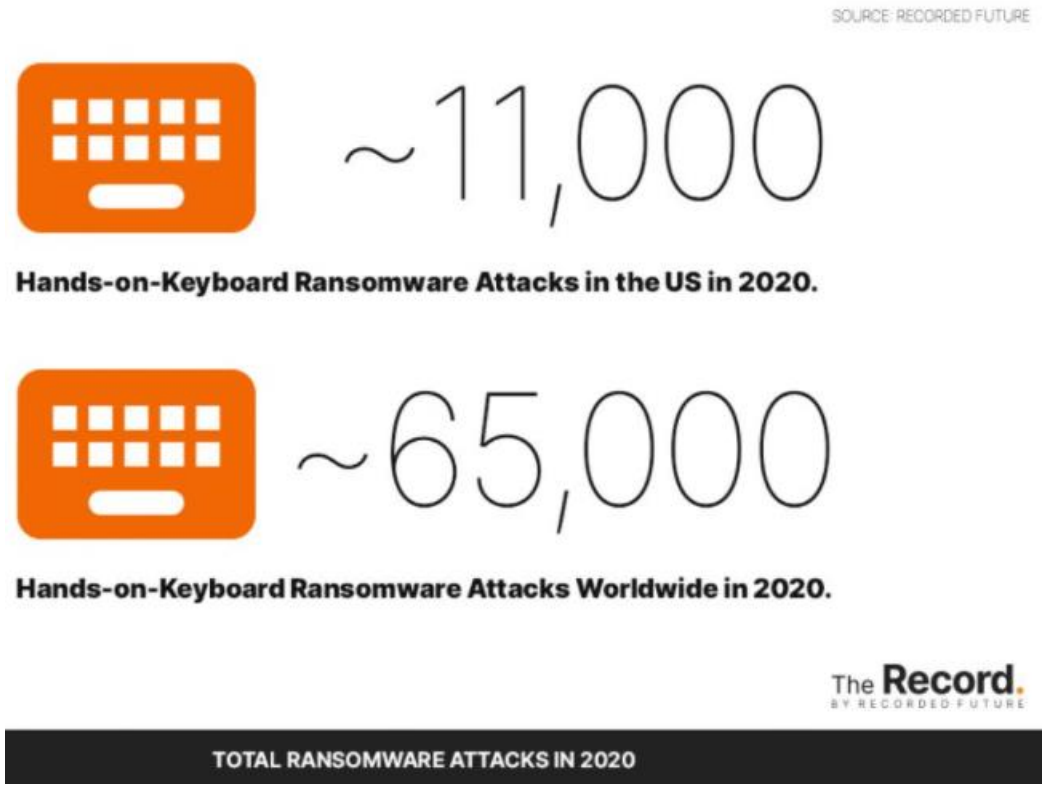
# Breaking Down The Threat




https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/cybersecurity-fraud/2020SpringCyberMag_v5_RansomWare_ADA.pdf

CENTRACOMM

# Ransomware Attacks in 2020




[The Record by Recorded Future]

CENTRACOMM

# The Answer: Practice Cybersecurity Hygiene

## Where Quality Counts!

Almost all successful attacks take advantage of conditions that could reasonably be described as “poor cyber hygiene.”

- **It isn’t unusual to see attacks taking advantage of vulnerabilities that have been fixed 3-4 years ago!**


*Tony Sager is a Senior Vice President and Chief Evangelist for CIS (The Center for Internet Security). In this role, he leads the development of the CIS Controls, a worldwide consensus project to find and support technical best practices in cybersecurity, August 2020.

# Minimize Vulnerabilities To Minimize The Threat!


CENTRACOMM

# Cybersecurity Technical Statistics

- 57% of data breaches are attributed to **poor patch management**. - study conducted by the Ponemon Institute
- 74% of data breaches start with **privileged credential abuse**. – Columbus, L., Feb. 26, 2019
- 93% percent of cloud deployment **configuration errors** have contributed to more than 200 breaches over the past two years. – Jaffee, L., August 4, 2020


CENTRACOMM

# Technical Cybersecurity Hygiene

“Relatively simple, well-defined actions:

- Patching Known Vulnerabilities
- Management of Privileges
- Proper Configuration Management

can provide significant value - but not a complete cure - for many cyber health problems.” – T Sager, August 2020

# Patching Considerations of Known Vulnerabilities

Operating Systems:
- Microsoft Windows
- Apple OS

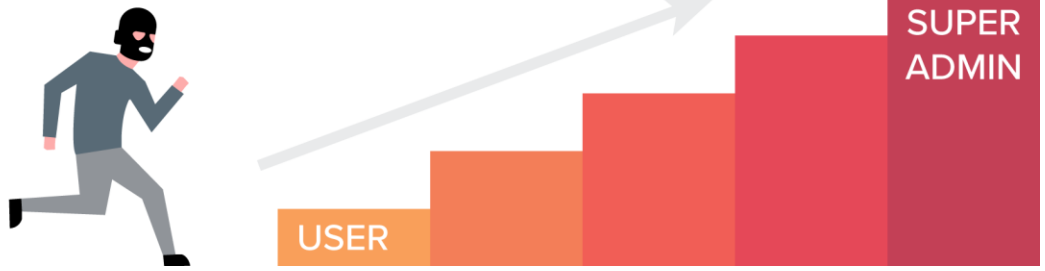
Applications:
- Adobe Products
- Browsers
- ITunes
- Java
- Microsoft Office Products

Older, unused products

# Management of Privileges:  Proper Credentials

Follow the concept of “least privilege”.

- Do not use Privileged Accounts when not needed.
- Do not use an Administrative Account if not needed for the task.
- PC & Laptop accounts often are created with Admin Privilege – remove this access
- Such access is particularly dangerous when surfing the web



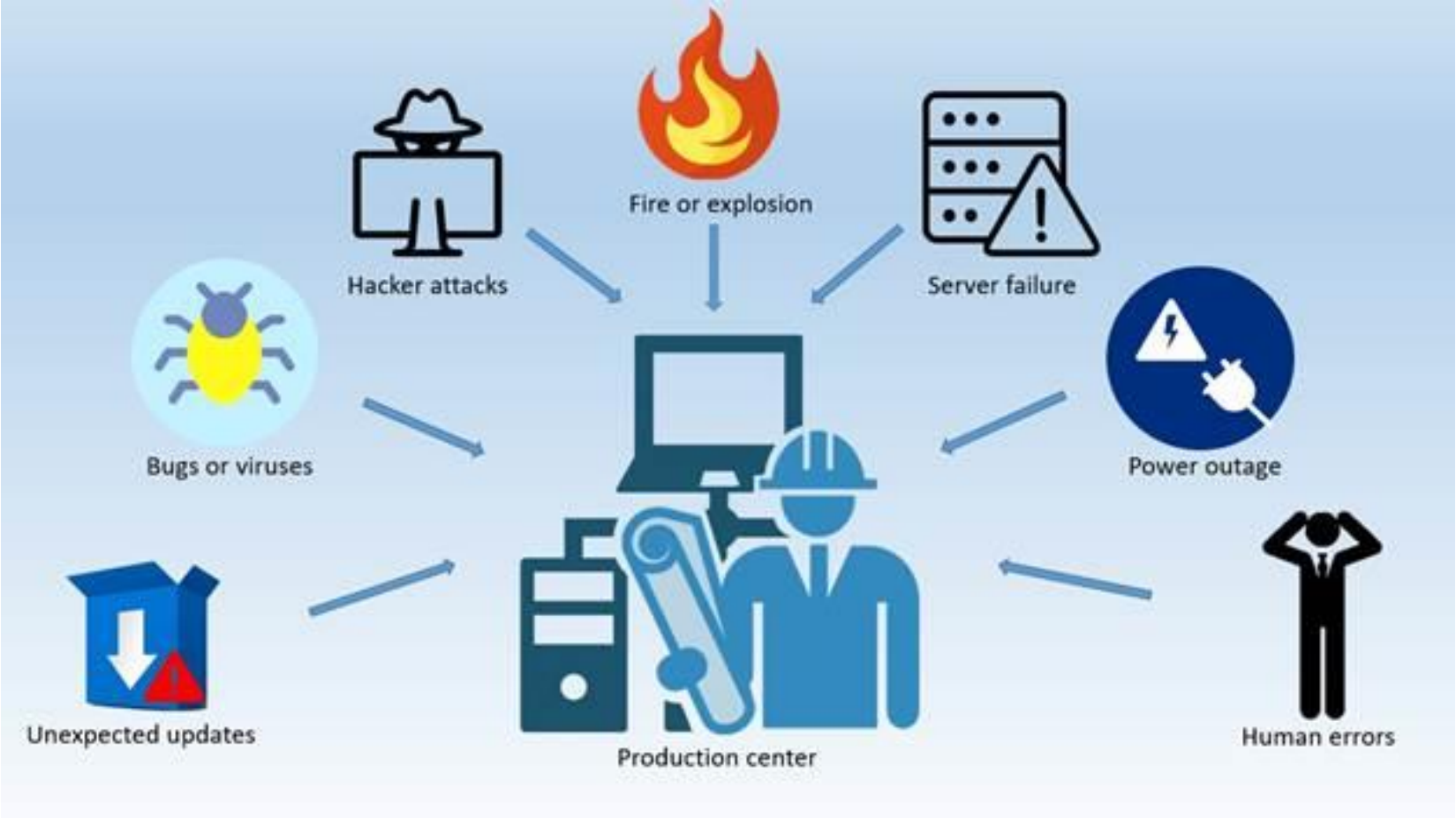
# Proper Configuration Management

Often PCs, Laptops, & Servers are run with installations out of the box:

- Remove default accounts that are not needed
- Change default passwords
- Use Windows Firewall
- Use Windows A/V

Good Quality Control

# Don’t Forget: Data Backups & Testing



# Social Engineering

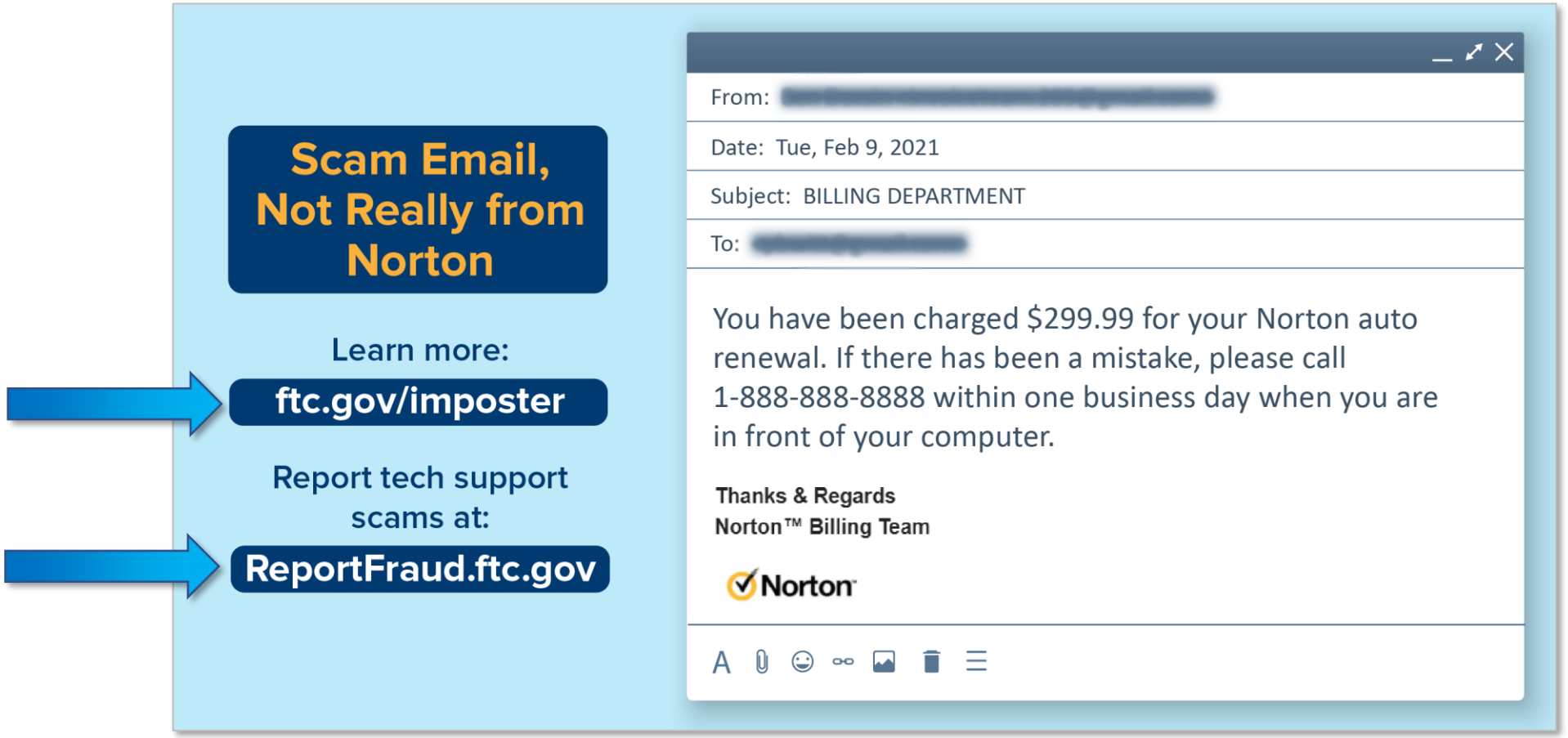
Psychological manipulation of people into performing actions or divulging confidential information.  A type of “confidence trick” for the purpose of information gathering, fraud, or system access.

# Social Engineering: Phishing

Phishing - An Internet scam designed to trick the recipient into revealing credit card, passwords, social security numbers and other company and/or personal information to individuals, businesses, and/or nation states who intend to use them for fraudulent purposes.

- Contains a link or graphic to be clicked
- Contains a malicious download or attachment
- Asks you to pay a bill online
- Request verification of information
- Ask urgently for help
- Claims that you have unemployment benefits
- Other

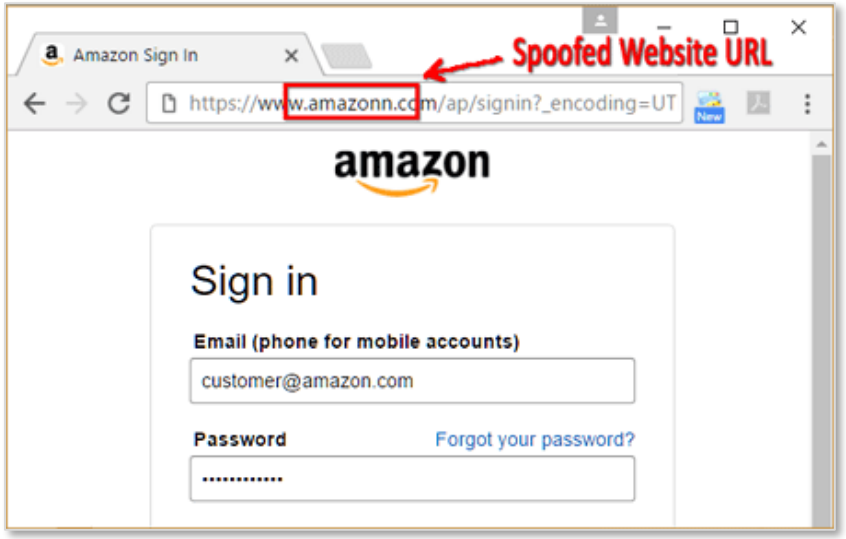
# Email Phishing



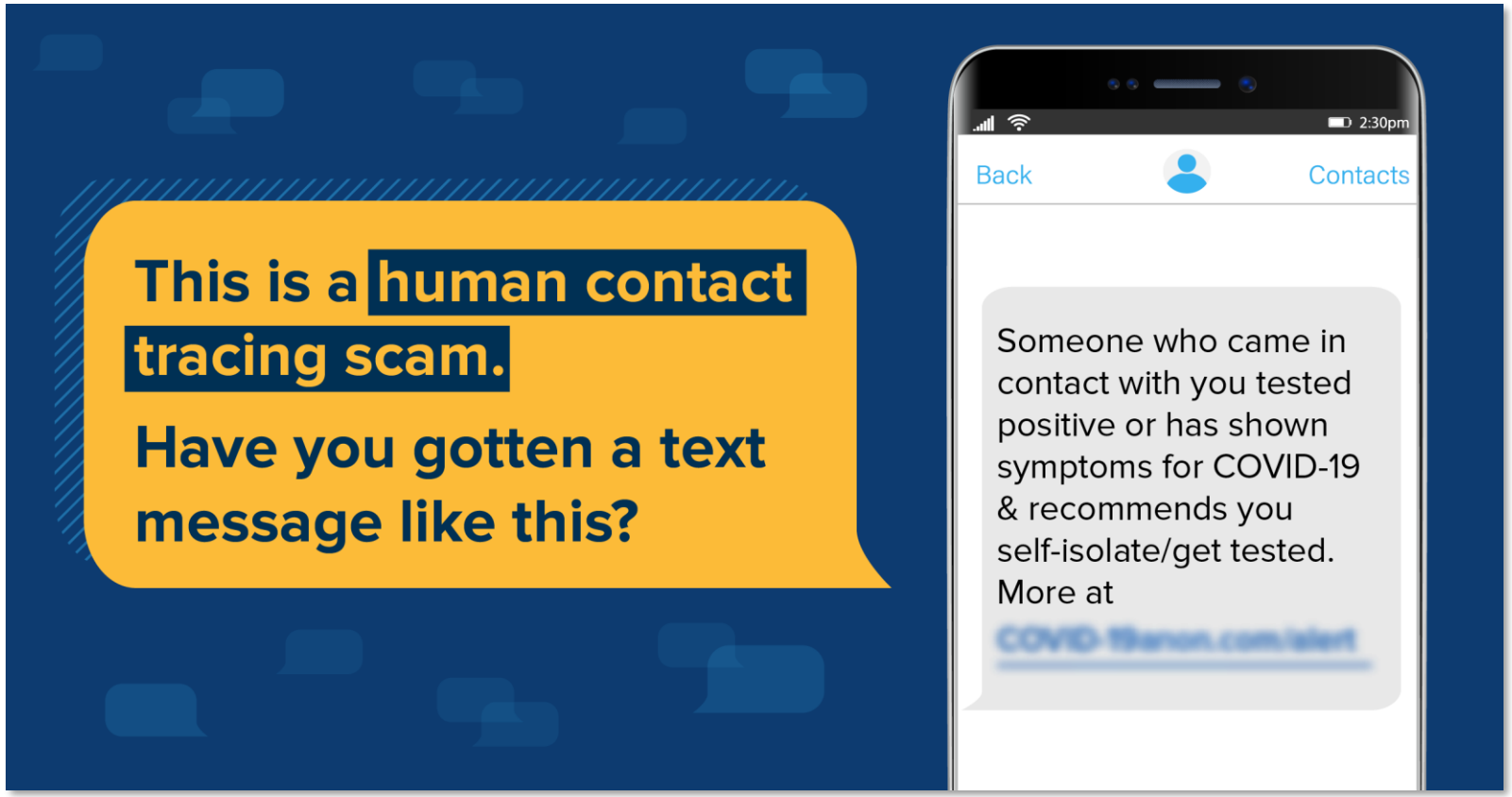

CENTRACOMM

# Website Phishing

A phishing website (sometimes called a "spoofed" site) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website. You could even land on a phishing site by mistyping a URL.



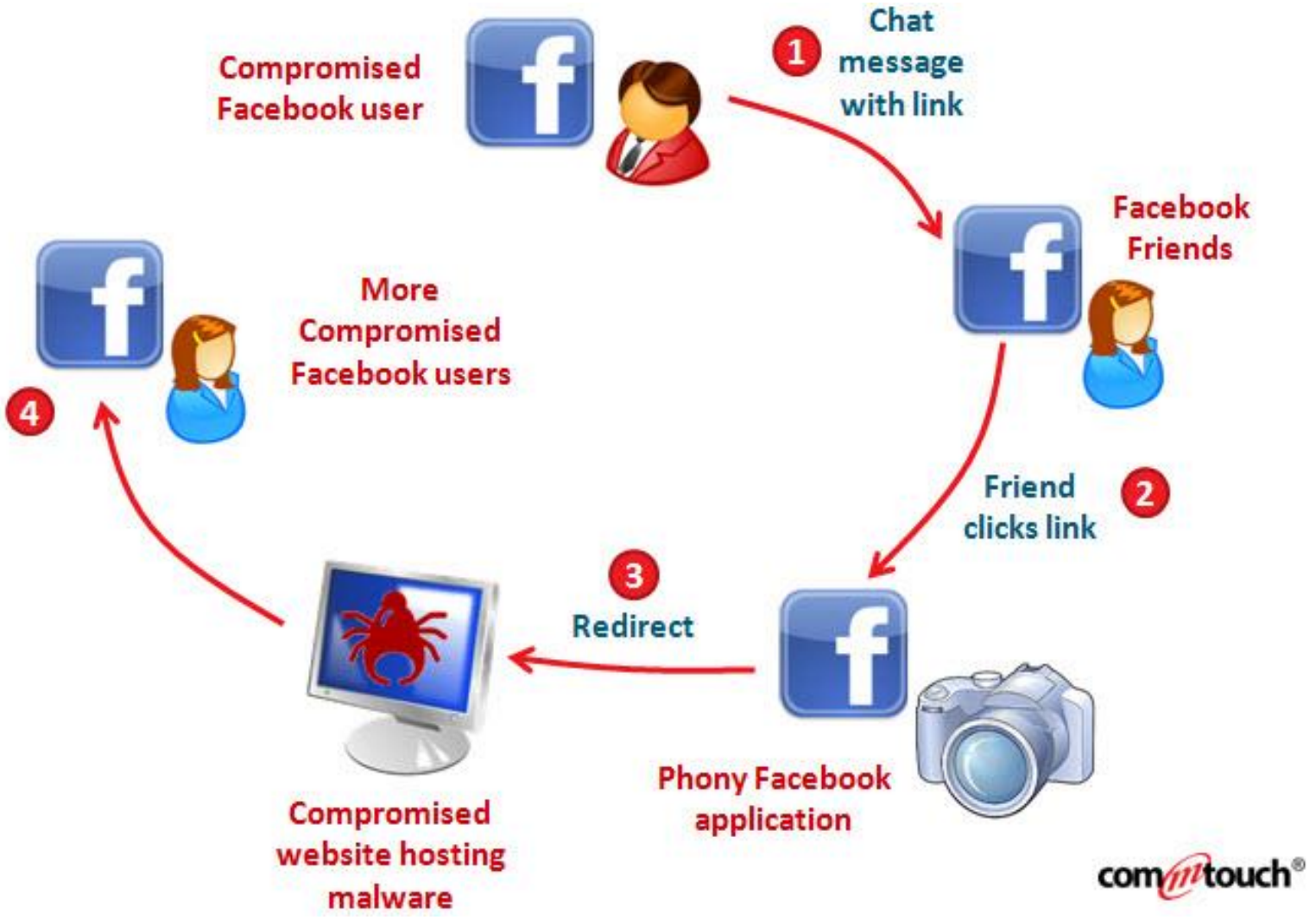

# Text Messaging Phishing



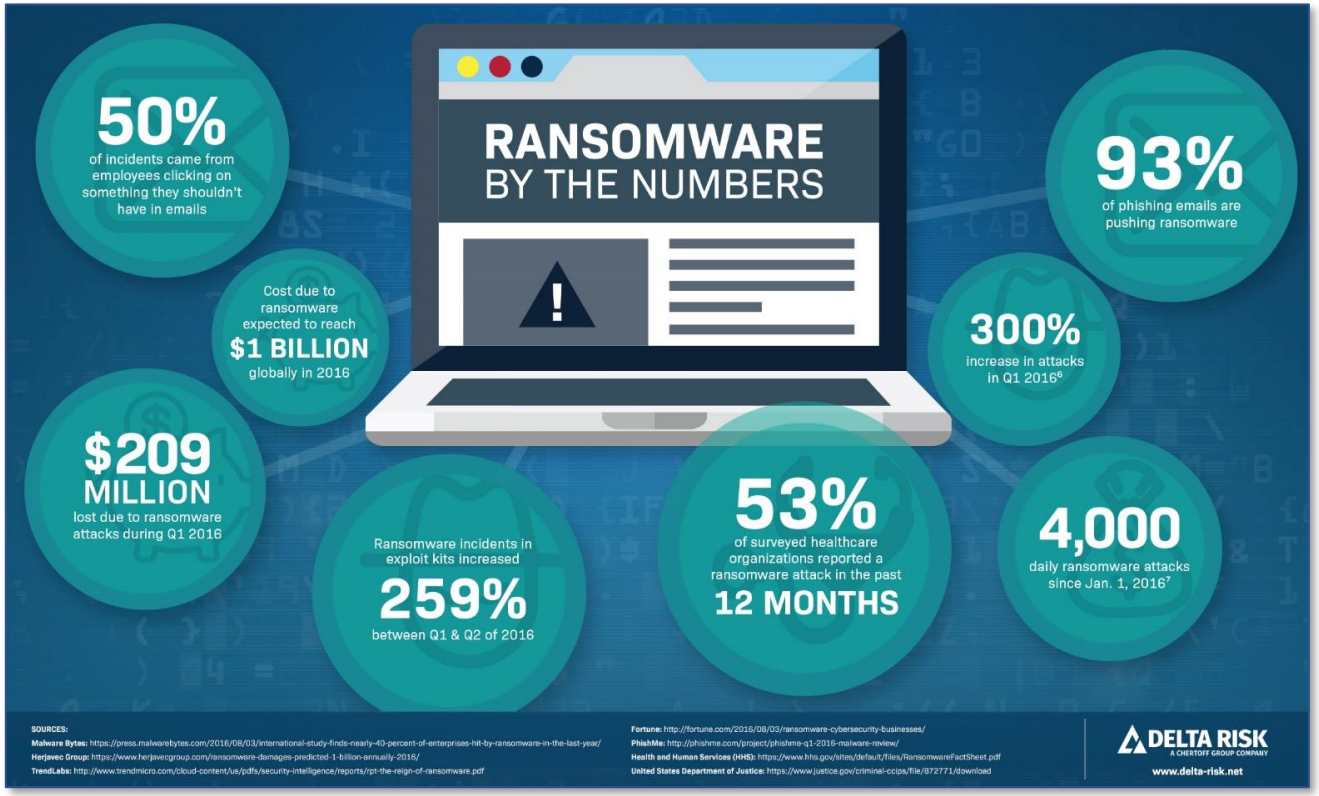

Federal: https://reportfraud.ftc.gov/

Ohio: https://www.ohioattorneygeneral.gov/About-AG/Contact/Report-A-Scam

# Social Media Phishing: Facebook



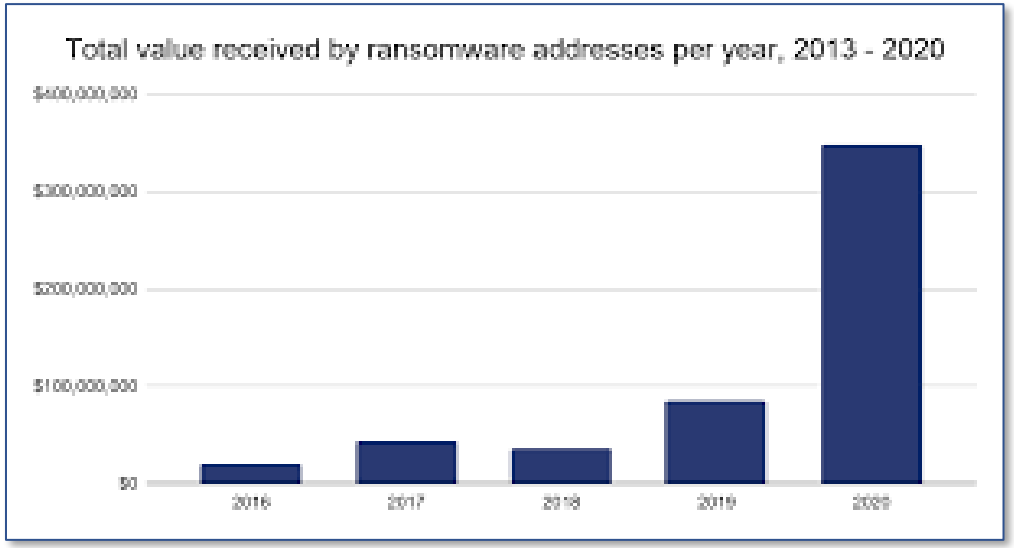
# Your Business Could Become a Statistic





# Ransomware $ Demands Continue to Grow

- The highest ransom demanded from hackers has more than doubled:
  - 2019 - $19.3 million
  - 2020 - $38.6 million
  - 2021 - $70 million
- The highest ransom actually paid to hackers:
  - 2019 - $6.4 million
  - 2020 - $12.9 million in 2020*
  - 2021 - TBD




Zdmnet: https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/

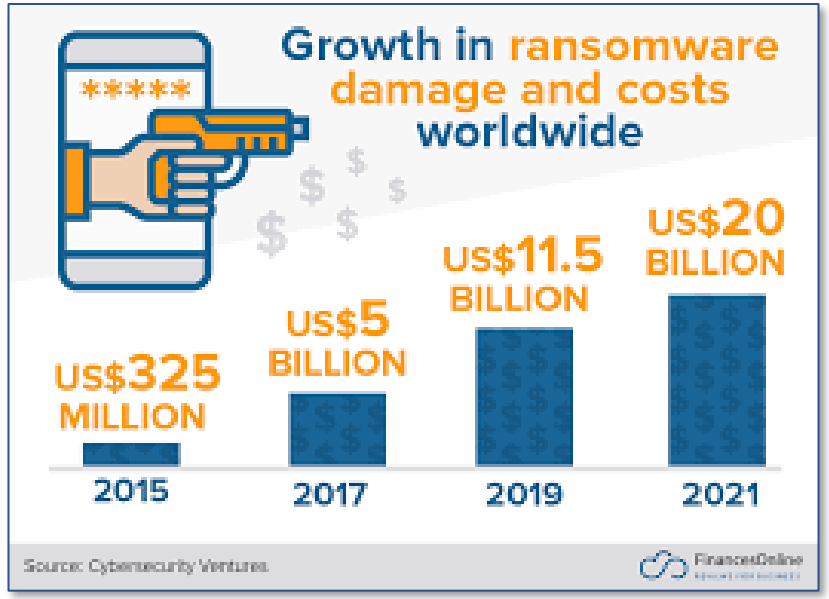
* iTWire - Palo Alto Networks 2021 Ransomware Threat Report: average ransom payment almost tripled

CENTRACOMM

# Ransomware As A Service (RaaS)

Satan RaaS Platform:

- Dark Web
- Launch Customizable Ransomware Attacks
- Wide Scale
- Minimal to No Technical Skills
- Subscription Based
- Launch Individual Attacks on Their Given Targets
- 30% of Their Cut to the Creators




Cerber: Banner Ads and Forum Postings on the Dark Web

https://www.theneweconomy.com/technology/raas-satans-business-model
https://www.sciencedirect.com/science/article/pii/S0167404820300468

CENTRACOMM

# Cybersecurity Action Steps:  Ransomware

Be Prepared for a Ransomware Attack:

- Determine Your Risk Tolerance
- Discuss How Many Days You Can Afford to Be Down
- What Are the Best- and Worst-Case Scenarios
- Run Scenarios If Ransom is Paid and Not Paid
  - Note: Paying Ransoms increasingly contentious
- Understand Bitcoin
- Prepare a Business Continuity Plan
- Have Backups
- Know Who Are the Members of Your “Go-To” Team
  - Develop an incident response plan

# Cybersecurity Action Steps: Technical & Human

Talk with Your Technical Support about:

- Patching Known Vulnerabilities
- Management of Privileges
- Proper Configuration Management
- Tested Backups
- Business Continuity

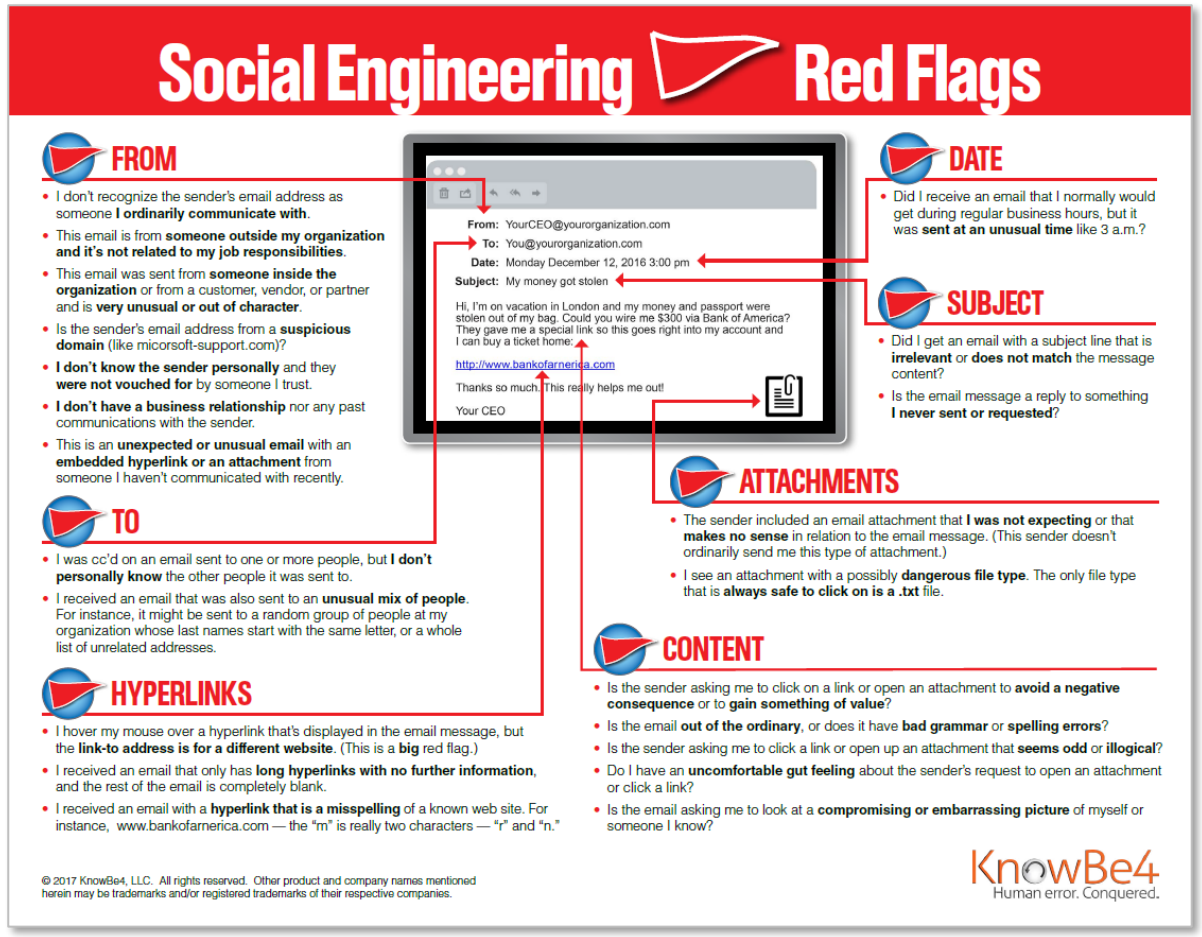
Increase Your Awareness of Social Engineering Tactics:

- CEO/BEC Fraud
- Web Site Phishing
- Social Media Phishing
- Text Phishing
- Email Phishing
- Report Fraud to the FTC and/or Ohio Attorney General
  - https://reportfraud.ftc.gov/
  - https://www.ohioattorneygeneral.gov/About-AG/Contact/Report-A-Scam

# Don’t Forget: Training & Awareness


CENTRACOMM

# Email Phishing Red Flags




https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf

CENTRACOMM

# End of Part 1 – Cybersecurity Hygiene

CENTRACOMM

# Introducing the CMMC

- Cybersecurity Maturity Model Certification
- ***All companies*** conducting business with the DoD, including subcontractors, must be certified by a third-party assessor organization (C3PAO)
- Five designated maturity levels ranging from “Basic Cybersecurity Hygiene” to “Advanced.”
- ***Guaranteed loss of business if certification not met!***


https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

# The New Frontier

- Accreditation Body established January 2020.
- Setting the standards, process and requirements for
  - Assessors becoming certified
  - Organizations becoming an accredited C3PAO
    Third Party Assessment Organizations
  - Registered Practitioners
  - Registered Provider Organization


https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

# CMMC Model Structure

17 Capability Domains

| | | |
|---|---|---|
| Access Control (AC) | Incident Response (IR) | Risk Management (RM) |
| Asset Management (AM) | Maintenance (MA) | Security Assessment (CA) |
| Awareness and Training (AT) | Media Protection (MP) | Situational Awareness (SA) |
| Audit and Accountability (AU) | Personnel Security (PS) | System and Communication Protection (SC) |
| Configuration Management (CM) | Physical Protection (PE) | System and Information Integrity (SI) |
| Identification & Authentication (IA) | Recovery (RE) | |

# CMMC Practices Per Level

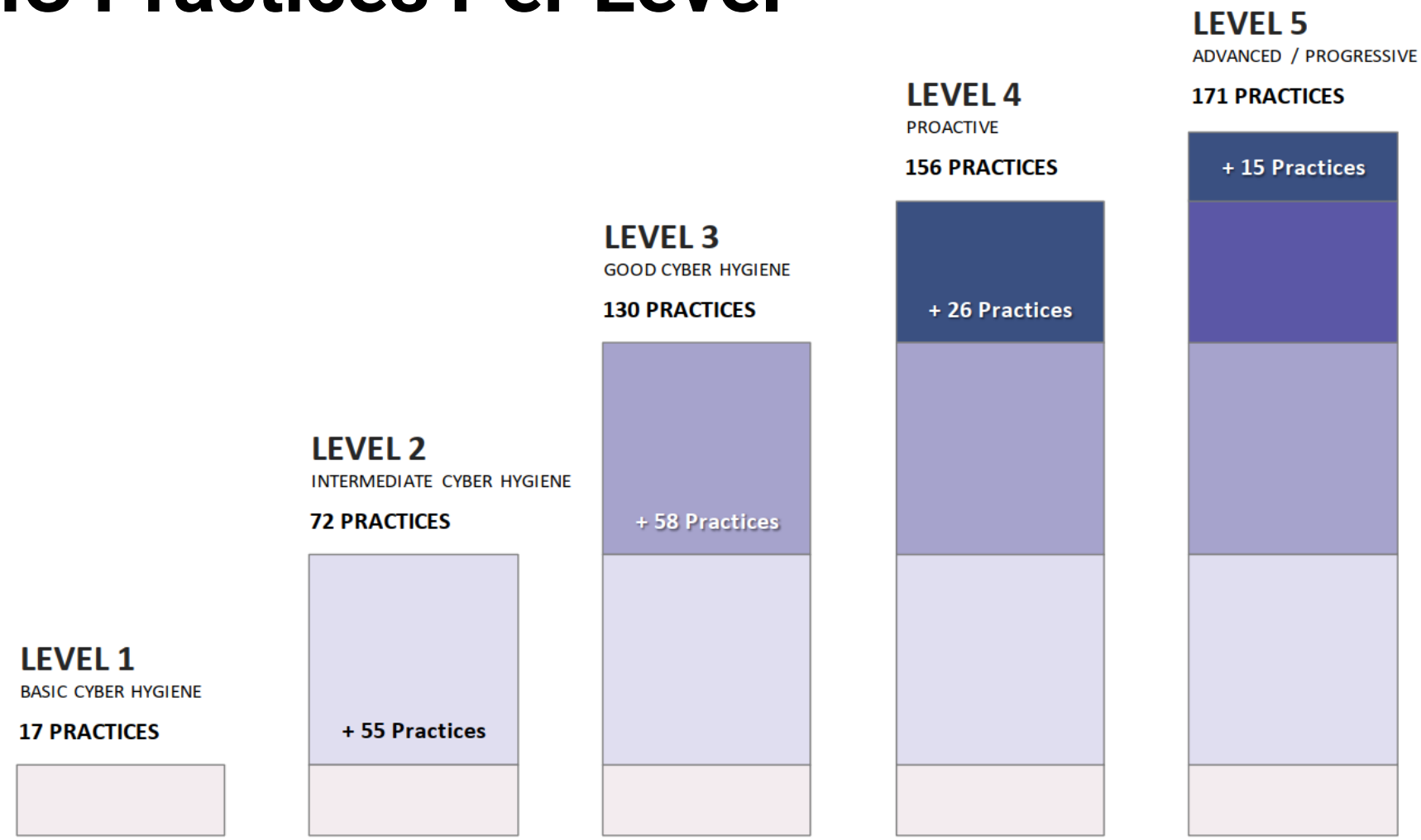
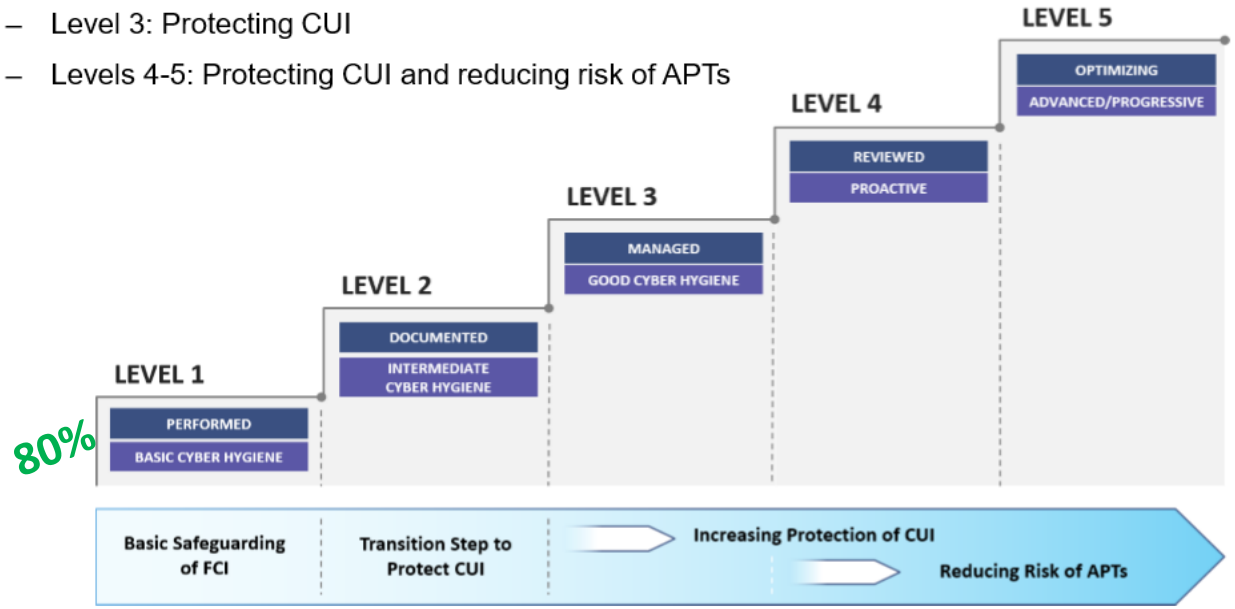



**Figure 5. CMMC Practices Per Level**

# CMMC

## Summary

- **CMMC establishes cybersecurity as a foundation for future DoD acquisitions**
- **CMMC levels align with the following focus:**
  - Level 1: Basic safeguarding of FCI
  - Level 2: Transition step to protect CUI
  - Level 3: Protecting CUI
  - Levels 4-5: Protecting CUI and reducing risk of APTs




DISTRIBUTION A. Approved for public release



CENTRACOMM

# CMMC – Important Terms

- FCI – Federal Contract Information
  - “Information not intended for public release. It is provided by or generated by for the Government under a contract to develop or deliver a product or service to the Government.  FCI does not include information provided by the Government to the public.” - Reference: Federal Acquisition Regulation 52.204-21 Basic Safeguarding of Covered Contractor Information

- CUI – Controlled Unclassified Information
  - CUI is sensitive (but not classified) information that the U.S Government wants to keep private. Examples are weapons test data or information about military personnel.
  - The National Archives (archives.gov) maintains a list of the categories of information that are considered CUI.
  - Defense Contractors are required to safeguard CUI on their networks according to DFARS 252.204-7012.

https://www.cmmcaudit.org/cmmc-glossary-terms-and-definitions-whos-who-in-cmmc/

# DFARS Regulation

- Defense Federal Acquisition (DFARS)
  - Regulation Supplement 252.204-7012
- Required as of December 31, 2017
- Applies to ALL businesses in the Defense Industrial Base
  - That handle Controlled Unclassified Information (CUI)
- Potential Loss of Business if Regulation Not Met
- Relies on self-assessment

# Am I Required to Implement NIST SP 800-171?

- Yes, if your business retains or processes Controlled Unclassified Information (CUI)
- What tells me if I am handling CUI data?
  - Look at your contract(s)

# Contract Example

## ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 15

| 1. CONTRACT/PURCH ORDER/AGREEMENT NO. | 2. DELIVERY ORDER/CALL NO. | 3. DATE OF ORDER/CALL (YYYYMMMMDD) | 4. REQUISITION/PURCH REQUEST NO. | 5. PRIORITY |
|---|---|---|---|---|

| 16. TYPE OF ORDER | | | |
|---|---|---|---|
| | DELIVERY/ CALL | | This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract. |
| | PURCHASE | X | Reference your Offer/Quote dated 2019 DEC 06, furnish the following on terms specified herein. |
| | | | ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME. |

NAME OF CONTRACTOR | SIGNATURE | TYPED NAME AND TITLE | DATE SIGNED (YYYYMMMDD)

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

| 18. ITEM NO. | 19. SCHEDULE OF SUPPLIES/SERVICES | 20. QUANTITY ORDERED/ ACCEPTED* | 21. UNIT | 22. UNIT PRICE | 23. AMOUNT |
|---|---|---|---|---|---|
| | THE AWARD CLAUSES ARE APPLICABLE AS INDICATED IN THE DLA MASTER SOLICITATION FOR AUTOMATED SIMPLIFIED ACQUISITIONS REVISION 60 (DECEMBER 9, 2019) WHICH CAN BE FOUND ON THE WEB AT https://www.dla.mil/Portals/104/Documents/J7Acquisition/Master_Solicitation_Revision-60_December-09-2019.pdf?ver=2019-12-09-144123-1 | 102 | SY | 31.16 | |

# Contract Example (cont)

## SECTION I - CONTRACT CLAUSES

**252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016) (DFARS)**

(c) FAR . This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

FAR: **https://www.acquisition.gov/?q=browsefar**

DFARS: **https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html**

DLAD: **http://www.dla.mil/HQ/Acquisition/Offers/DLAD.aspx**

***

# Contract Example (cont)

| CONTINUATION SHEET | REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE7M2-20-V-0443 | PAGE 3 OF 15 PAGES |
|---|---|---|

**SECTION B**

PR: 0082657895
SUPPLIES/SERVICES:

9320010199073

RA001: THIS DOCUMENT INCORPORATES TECHNICAL AND/OR QUALITY REQUIREMENTS (IDENTIFIED BY AN 'R' OR AN 'I' NUMBER) SET FORTH IN FULL TEXT IN THE DLA MASTER LIST OF TECHNICAL AND QUALITY REQUIREMENTS FOUND ON THE WEB AT:

http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx

# Contract Example (cont)

| CONTINUATION SHEET | REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE8E5-21-V-1828 | PAGE 7 OF 16 PAGES |
|---|---|---|

**SECTION I - CONTRACT CLAUSES (CONTINUED)**

**252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (JAN 2021) (DFARS)**

**252.204-7020 NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020) (DFARS)**

(a) *Definitions.*

"Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that --

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

CENTRACOMM

# DoD DFARS Regulation

- Protect confidential information
- Overall risk reduction
- Minimize opportunities for business disruption
- Decrease downtime potential
- Increase trust
  - With business partners & customers
- Increased awareness
  - Training & Awareness for ALL employees

# Process Effectiveness?

- Approximately 300,000 businesses in the Defense Industrial Base
- Estimated 10,000 businesses implemented all 110 of NIST 800-171 controls
- So…

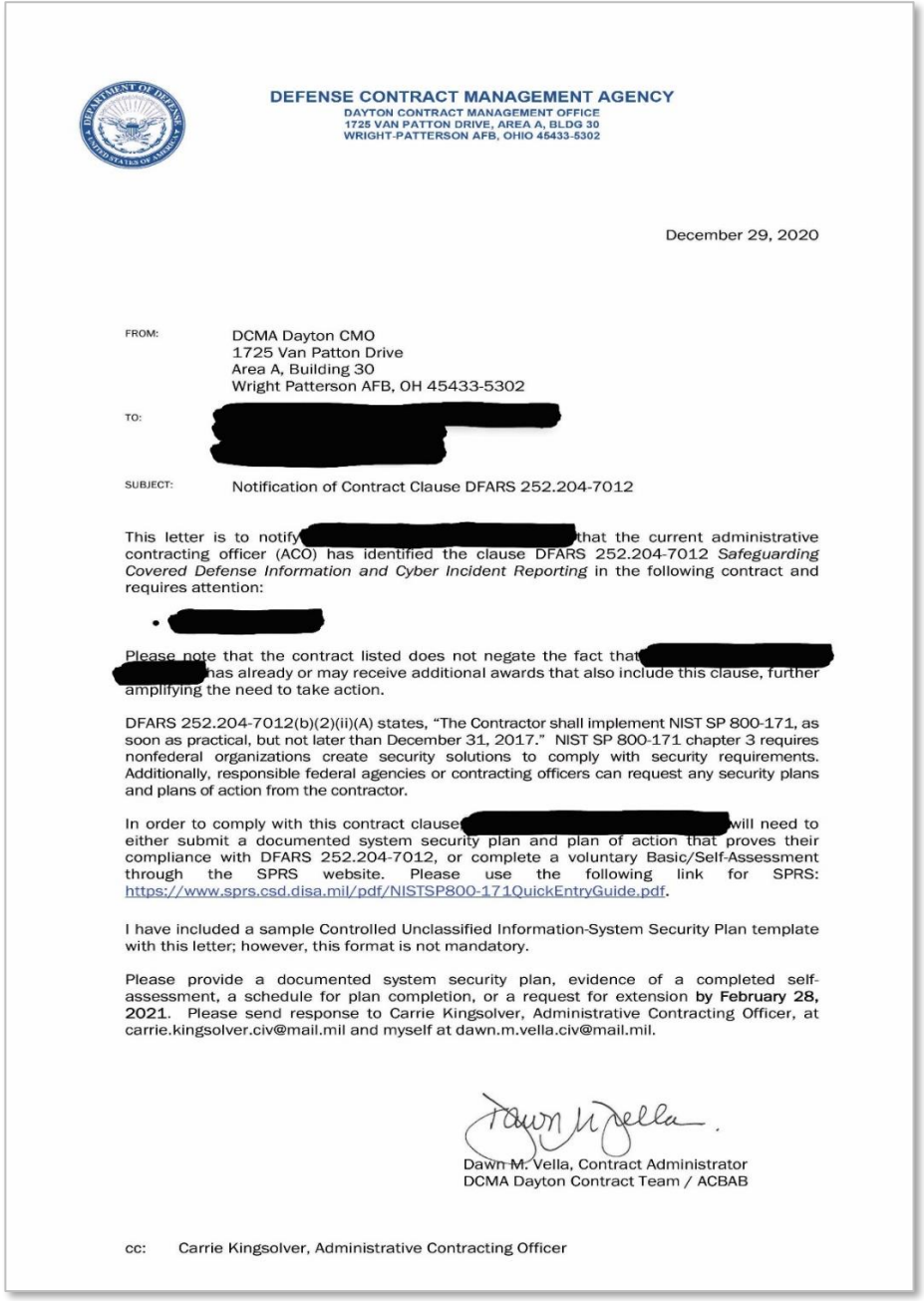
# New DoD DFARS Interim Regulation

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to mailto:webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

# Example



DEFENSE CONTRACT MANAGEMENT AGENCY
DAYTON CONTRACT MANAGEMENT OFFICE
1725 VAN PATTON DRIVE, AREA A, BLDG 30
WRIGHT-PATTERSON AFB, OHIO 45433-5302

December 29, 2020

FROM: DCMA Dayton CMO
1725 Van Patton Drive
Area A, Building 30
Wright Patterson AFB, OH 45433-5302

TO: [redacted]

SUBJECT: Notification of Contract Clause DFARS 252.204-7012

This letter is to notify [redacted] that the current administrative contracting officer (ACO) has identified the clause DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* in the following contract and requires attention:

- [redacted]

Please note that the contract listed does not negate the fact that [redacted] has already or may receive additional awards that also include this clause, further amplifying the need to take action.

DFARS 252.204-7012(b)(2)(ii)(A) states, "The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017." NIST SP 800-171 chapter 3 requires nonfederal organizations create security solutions to comply with security requirements. Additionally, responsible federal agencies or contracting officers can request any security plans and plans of action from the contractor.

In order to comply with this contract clause [redacted] will need to either submit a documented system security plan and plan of action that proves their compliance with DFARS 252.204-7012, or complete a voluntary Basic/Self-Assessment through the SPRS website. Please use the following link for SPRS: https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf.

I have included a sample Controlled Unclassified Information-System Security Plan template with this letter; however, this format is not mandatory.

Please provide a documented system security plan, evidence of a completed self-assessment, a schedule for plan completion, or a request for extension **by February 28, 2021**. Please send response to Carrie Kingsolver, Administrative Contracting Officer, at carrie.kingsolver.civ@mail.mil and myself at dawn.m.vella.civ@mail.mil.

Dawn M. Vella, Contract Administrator
DCMA Dayton Contract Team / ACBAB

cc: Carrie Kingsolver, Administrative Contracting Officer

CENTRACOMM

SUBJECT: Notification of Contract Clause DFARS 252.204-7012

This letter is to notify [redacted] that the current administrative contracting officer (ACO) has identified the clause DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* in the following contract and requires attention:

- [redacted]

Please note that the contract listed does not negate the fact that [redacted] has already or may receive additional awards that also include this clause, further amplifying the need to take action.

DFARS 252.204-7012(b)(2)(ii)(A) states, "The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017." NIST SP 800-171 chapter 3 requires nonfederal organizations create security solutions to comply with security requirements. Additionally, responsible federal agencies or contracting officers can request any security plans and plans of action from the contractor.

In order to comply with this contract clause, [redacted] will need to either submit a documented system security plan and plan of action that proves their compliance with DFARS 252.204-7012, or complete a voluntary Basic/Self-Assessment through the SPRS website. Please use the following link for SPRS: https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf.

I have included a sample Controlled Unclassified Information-System Security Plan template with this letter; however, this format is not mandatory.

Please provide a documented system security plan, evidence of a completed self-assessment, a schedule for plan completion, or a request for extension **by February 28, 2021**. Please send response to Carrie Kingsolver, Administrative Contracting Officer, at carrie.kingsolver.civ@mail.mil and myself at dawn.m.vella.civ@mail.mil.

# Supplier Performance Risk System (SPRS)

"...is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)

SPRS supports DoD Acquisition Professionals with meeting acquisition regulatory and policy requirements by providing:

- ✓ On-time delivery scores and quality classifications (DFARS 213.106-2)
- ✓ Price, Item and Supplier procurement risk data and assessments
- ✓ Company exclusion status (debarments, suspensions, etc.)
- ✓ **NIST SP 800-171 Assessment results**
- ✓ National Security System Restricted List
- ✓ Supply chain illumination


CENTRACOMM

# Potential Liability

- For the first time, a district court has held that **a contractor's failure to comply with a US government contract's cybersecurity requirements** can expose a company to False Claims Act liability – a significant and harrowing finding for government contractors. (applies to NIST 800-171)
- In reaching its decision, the court concluded that the **nondisclosures could be "material,"** as required to establish liability under the False Claims Act, because the government might not have awarded the contracts if it had known the extent of the noncompliance.
- Periodic assessments are a must. A one-time assessment of your company's cybersecurity compliance is insufficient. **This is a rapidly changing area, and periodic assessments are critical to ensuring compliance.** You must assume a minimum of Level 1

https://www.dlapiper.com/en/us/insights/publications/2019/05/court-finds-that-failure-to-comply-with-cybersecurity-obligations/

# CMMC Updates

CENTRACOMM

# State of Assessments & Roles

- Are there organizations certified to do certification assessment?
  - Yes, two authorized C3PAOs, visit the CMMC-AB Marketplace for a listing
  - https://cmmcab.org/marketplace/?search_category=headline&q=&search_method=contains&cat=38
- When will the CMMC-AB certification process start?
  - No assessments currently being completed by C3PAOs
  - No trained Certification Assessors
  - Perhaps starting in 2nd half of 2021
- What about organizations that can provide risk assessments and help us get ready for certification?
  - Registered Practitioners & Registered Provider Organizations are available today
  - Also listed in the Marketplace

# Assessment Concerns

- Results of some industry studies suggest that CMMC compliance may come with an expensive cost, burden and possible bottlenecks.
- Another anticipated obstacle in CMMC compliance is the possible bottleneck in the process. Under the interim rule, the 300,000 contractors supporting the DOD would need to undergo the assessment.
- The “Strengthening national security and supply chain resiliency by improving DOD cybersecurity certification” report involving 108 manufacturers… found that 24 percent, or nearly one in every five, companies said they might be forced out of the supply chain due to expensive compliance costs.

https://www.govconwire.com/2021/06/cmmc-compliance-will-come-with-expensive-costs-burdens-and-possible-bottlenecks/

# Recommendations

- Focus on NIST 800-171 implementation now
- Reference NIST 800-171 Rev 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- Use NIST 800-171a - Assessing Security Requirements for Controlled Unclassified Information https://csrc.nist.gov/publications/detail/sp/800-171a/final
- Perform a self-assessment
  - ***Third-party assistance recommended***
  - Refer to the ***DoD Assessment Methodology***
- Enter your SPRS score
- Work towards incremental improvements
- Update your SPRS score
- **If you haven't started, get going!**

# YOUR QUESTIONS?

CENTRACOMM

# CentraComm Overview

Founded in 2001, CentraComm is an IT cybersecurity, network infrastructure, and compliance provider that operates as an extension of your IT department:

- Provides IT risk, managed, and professional services supporting customer's business goals and strategic business technology initiatives
- Has around-the-clock engineering team and value-added services that deliver peace of mind for customers
- Utilizes top technology supported by industry-certified, top-level talent
- Has two Data Centers supporting Co-Location, Disaster Recovery, etc.
- Supports Fortune 50, educational institutions, and small to medium-sized businesses allowing them to innovate efficiently, be compliant, and remain secure

# Thank You!

Visit us at www.centracomm.net
Contact me at lwagner@centracomm.net

CENTRACOMM

# References


How to Stay Smart & Secure in a Connected World
By Tony Sager - Aug 19, 2020 5:16 am PDT
https://www.csoonline.com/article/3571743/cleaning-up-a-definition-of-basic-cyber-hygiene.html

Servicenow study conducted by the Ponemon Institute

74% Of Data Breaches Start With Privileged Credential Abuse
Louis Columbus - Feb 26, 2019,08:47am EST
https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/#533943063ce4

Misconfigured servers contributed to more than 200 cloud breaches
Larry Jaffee - August 4, 2020
https://www.scmagazine.com/featured/cloud-misconfigurations-contributed-to-more-than-200-breaches/

Small Business Playbook
Cyberattacks now cost companies $200,000 on average, putting many out of business
Scott Steinberg - Oct 13 201910:30 AM EDT Updated Mon, Mar 9 202011:37 AM EDT
https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Palo Alto Networks 2021 Ransomware Threat Report: average ransom payment almost tripled
Alex Zaharov-Reutt - Thursday, 18 March 2021 23:20
iTWire - Palo Alto Networks 2021 Ransomware Threat Report: average ransom payment almost tripled

# References


NIST 800-171 Rev 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST 800-171a - Assessing Security Requirements for Controlled Unclassified Information https://csrc.nist.gov/publications/detail/sp/800-171a/final

***DoD Assessment Methodology***

https://www.govconwire.com/2021/06/cmmc-compliance-will-come-with-expensive-costs-burdens-and-possible-bottlenecks/

https://www.dlapiper.com/en/us/insights/publications/2019/05/court-finds-that-failure-to-comply-with-cybersecurity-obligations/

Federal Acquisition Regulation 52.204-21 Basic Safeguarding of Covered Contractor Information

The National Archives (archives.gov) maintains a list of the categories of information that are considered CUI.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf