Ransomware and Cybersecurity Preparedness

Michael Meline

MsIA, CISSP, CEH, CFE, PCIP, TNCA, C)DFE, ACE, CIPM, CIPP/E, ISO/IEC 27001 Auditor, CMMC Provisional Assessor

mike@cyberselfdefense.com

CYBER® SELF-DEFENSE

Springbrook

First – The Basics – What is Ransomware?

❑ What is Ransomware?

  ○ It’s a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.

  ○ It encrypts your files so you cannot use them with the highest grade of encryption.

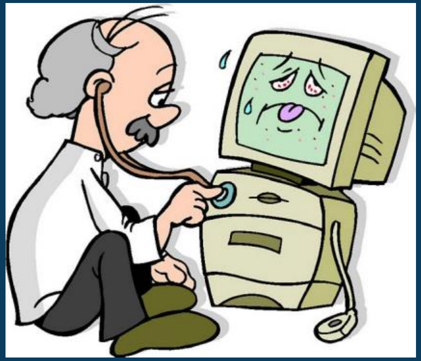
❑ Who is infected?

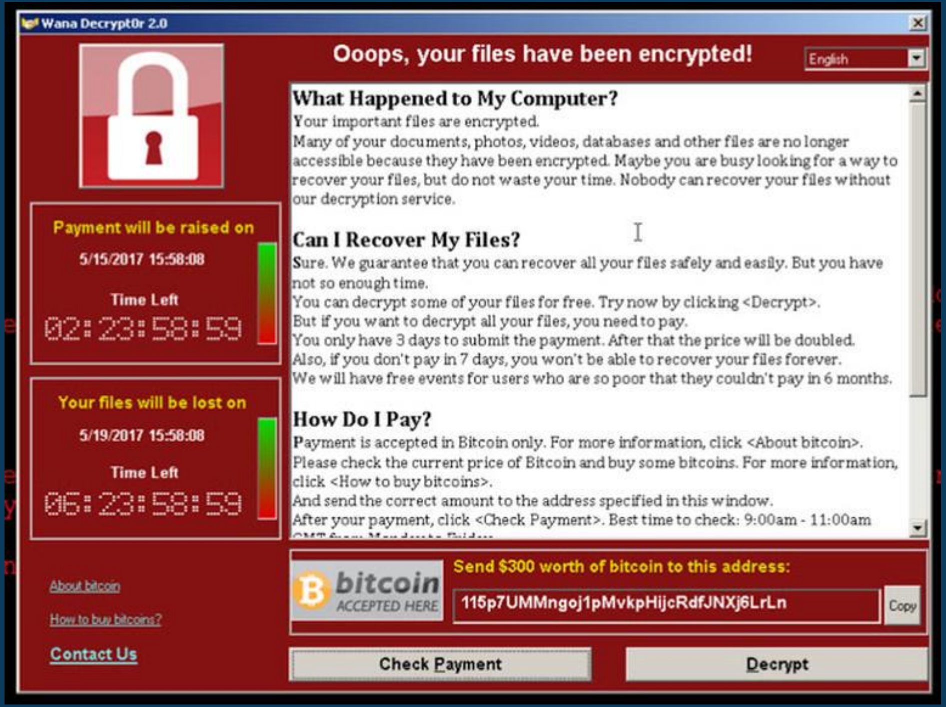
  ○ Everyone can be a victim.

❑ How is it Spread?

  ○ Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

  ○ Using a laptop on a public WIFI network.





Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

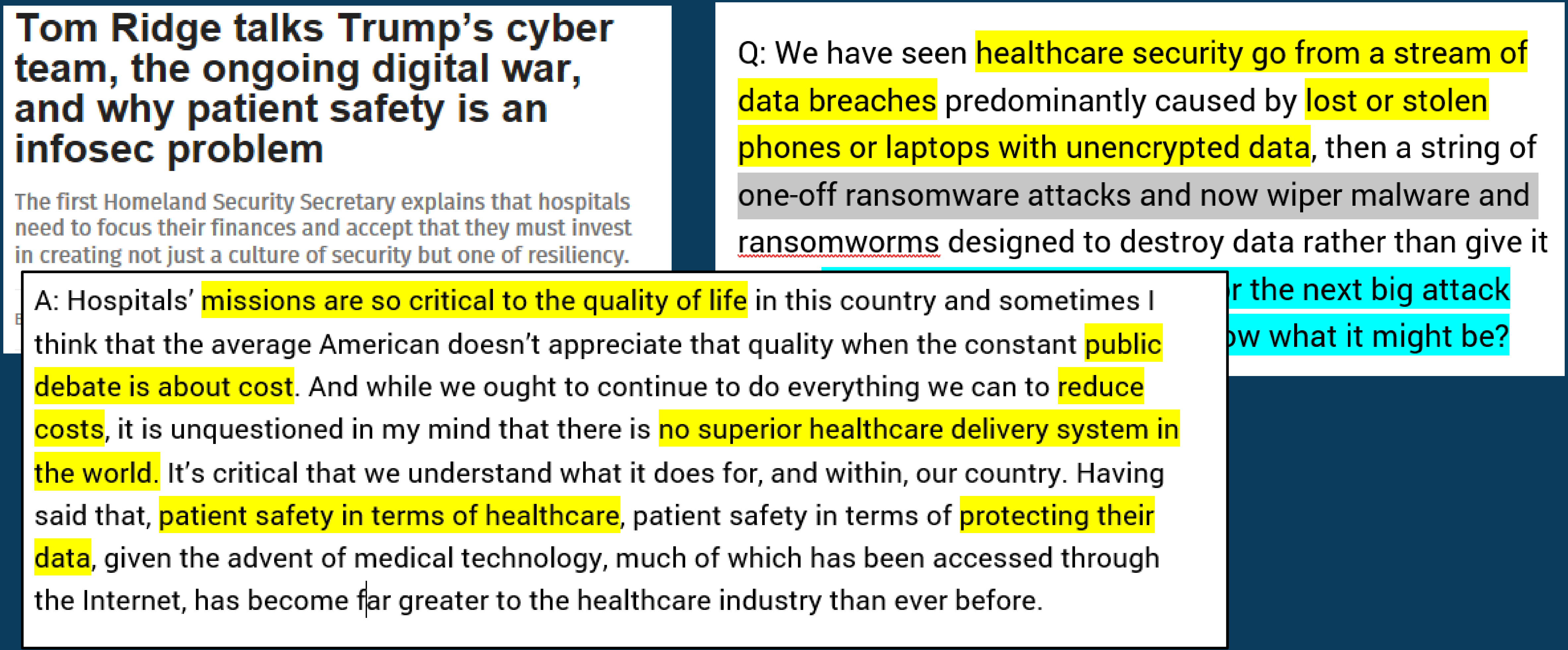
Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Why You and Why Now?

- ❑ Ransomware criminals are looking for:
  - ○ Targets that cannot accept a sustained period of no computer access.
  - ○ May have “personal information” thereby triggering a duty to provide public notice.
  - ○ Having the ability to pay a ransom.
- ❑ This is a bit of a random event
  - ○ Local government, retailers, hospitals and banks have all been attacked.
  - ○ Much of the ransomware is sent out, onto the internet, with hopes that it will find a victim.

Complacency – We Have Never Had a Problem - Yet



Tom Ridge talks Trump's cyber team, the ongoing digital war, and why patient safety is an infosec problem

The first Homeland Security Secretary explains that hospitals need to focus their finances and accept that they must invest in creating not just a culture of security but one of resiliency.

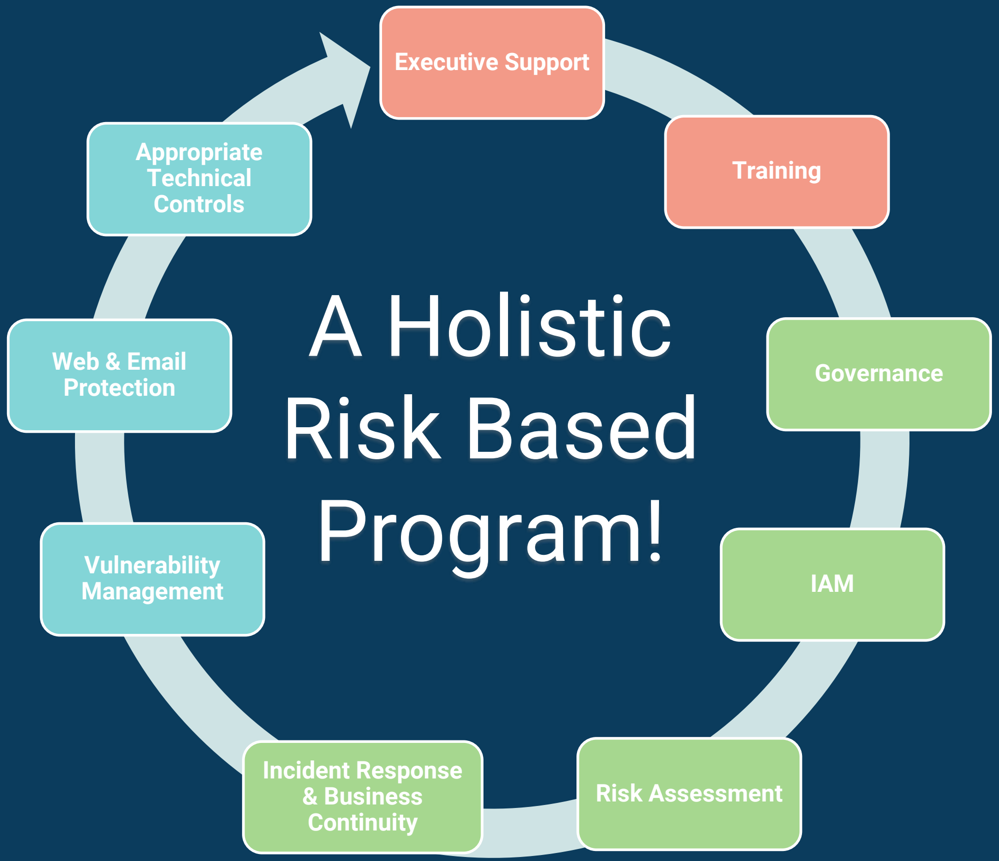
Q: We have seen healthcare security go from a stream of data breaches predominantly caused by lost or stolen phones or laptops with unencrypted data, then a string of one-off ransomware attacks and now wiper malware and ransomworms designed to destroy data rather than give it

r the next big attack

ow what it might be?

A: Hospitals' missions are so critical to the quality of life in this country and sometimes I think that the average American doesn't appreciate that quality when the constant public debate is about cost. And while we ought to continue to do everything we can to reduce costs, it is unquestioned in my mind that there is no superior healthcare delivery system in the world. It's critical that we understand what it does for, and within, our country. Having said that, patient safety in terms of healthcare, patient safety in terms of protecting their data, given the advent of medical technology, much of which has been accessed through the Internet, has become far greater to the healthcare industry than ever before.

THE NEW SCHOOL OF CYBERSECURITY



A Holistic Risk Based Program!

PEOPLE PROCESS

TECHNOLOGY

- ❑ **Executive Support** – Security is an agency problem!
- ❑ **Training** – Users are first line defense and your greatest vulnerability.
- ❑ **IAM**-Identity and Access Management. Ensure that access is appropriate.
- ❑ **Governance**– Set the expectation with the agency.
- ❑ **Risk Management** – Your strategic plan.
- ❑ **Incident Response & Business Continuity** – Because it's not if, it's when. Are you ready?
- ❑ **Vulnerability Management** – Before you can prevent, you must identify.
- ❑ **Web & Email Protection** – The most common means of cyber attack is against people and this requires diligent controls.
- ❑ **Technical Controls** – Always refer to your Risk Assessment.

Prevention

- ❑ **No Open Shares**
  - o These are corporate drives that allow everyone access. There should be no shared drives that allow “everyone” access. You should ensure that all folders allow only the people who need access to the folder have access.
- ❑ **Ensure that system admins log in as their normal (non-administrative) user and elevate privileges, as necessary.**
  - o Admins should avoid logging in as their administrative accounts to only those situations that REQUIRE this type of access.
- ❑ **Limit or block access to social media sites like Facebook, gambling sites, and anything that could be construed as pornography.**

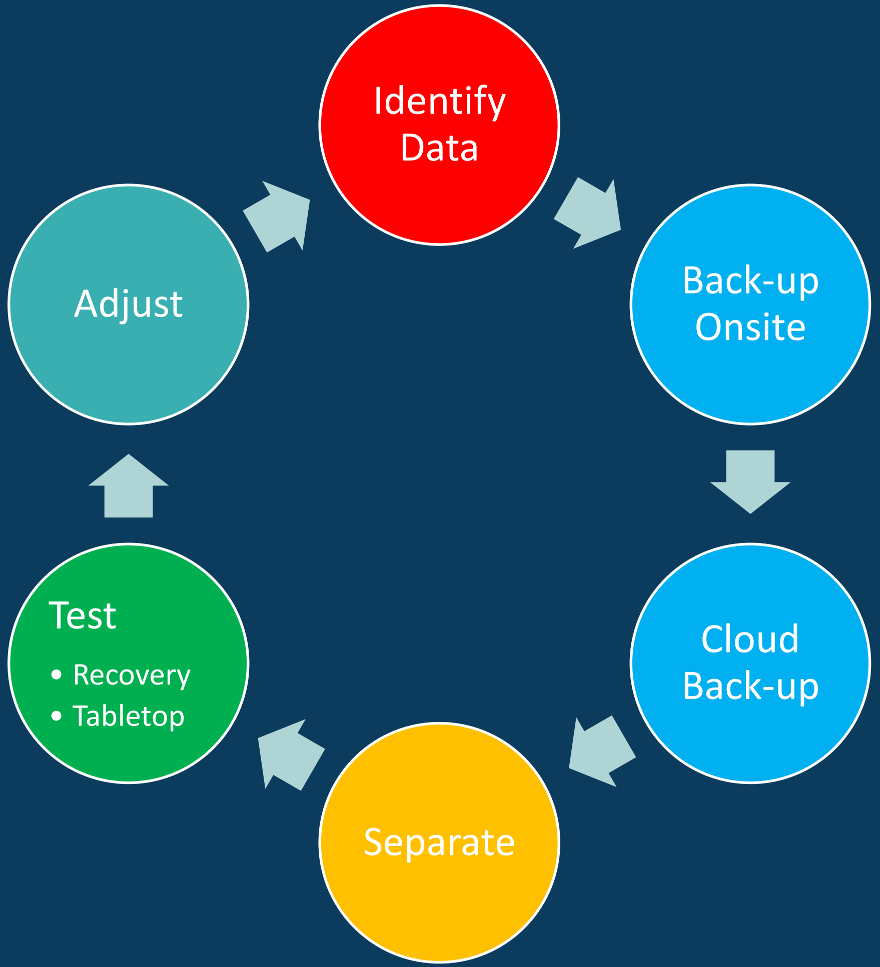
Prevention

- ❑ **Block or limit access to publicly-facing remote desktop protocols and other administrative access.**
- ❑ **Keep systems up-to-date!**
- ❑ **Check your Vendors!!**
- ❑ **Governance; Policies/Procedures/Plans**
- ❑ **Use STRONG PASSPHRASES;**
  - ○ **“CyberSelf_Defenseismygo2company4cybersecurity!”**
- ❑ **Train your employees for success; IN PERSON.**
  - ○ DO NOT CLICK!
  - ○ https://www.virustotal.com/gui/home/url
  - ○ Tabletops
- ❑ **Web and Email Proxies**
- ❑ **Antivirus**
  - ○ https://www.av-comparatives.org/

Prevention

❑ **Back-ups**

- ○ Have solid, **tested** backups of everything that is important to you. DO NOT RELY ON THIRD PARTY VENDORS!!!
- ○ Ensure that these back-ups are **kept isolated** from production systems.
- ○ Ensure that these back-ups **do not allow access (login)** with your normal account.
- ○ **Take back-ups offline** when not using them.
- ○ Ensure that when recovered, the back-ups are not infected.
- ○ Back up operating systems and anything else necessary for YOUR success; snapshots are excellent.
- ○ **Build a strategy, test it often, and correct, as necessary**.



Prevention

- ❑ **Firewalls**
  - ○ Enable the system firewall to properly protect the system. Surprisingly, many companies shut their system firewalls off, as this is a line of defense that is effective add no additional cost for the protection it provides.
  - ○ NEXTGen Firewalls
- ❑ **Use application whitelisting.**
  - ○ This methodology gives you the ability to allow only approved applications.
  - ○ Allowing only approved applications ensures that users cannot run inappropriate programs.
  - ○ This methodology is even more important if your organization has outdated and unsupported systems, like Windows XP, on the network.
- ❑ **Remove local administrative rights from end users.**
  - ○ Require them to get IT/Security approval for all software that is installed

DO YOU KNOW YOUR RISK APPETITE?
DO YOU UNDERSTAND YOUR RISK?

ACCESS CONTROL

APPLICATIONS

ENCRYPTION

DROPBOX
GOOGLE DRIVE

VENDOR MANAGEMENT

SIEM

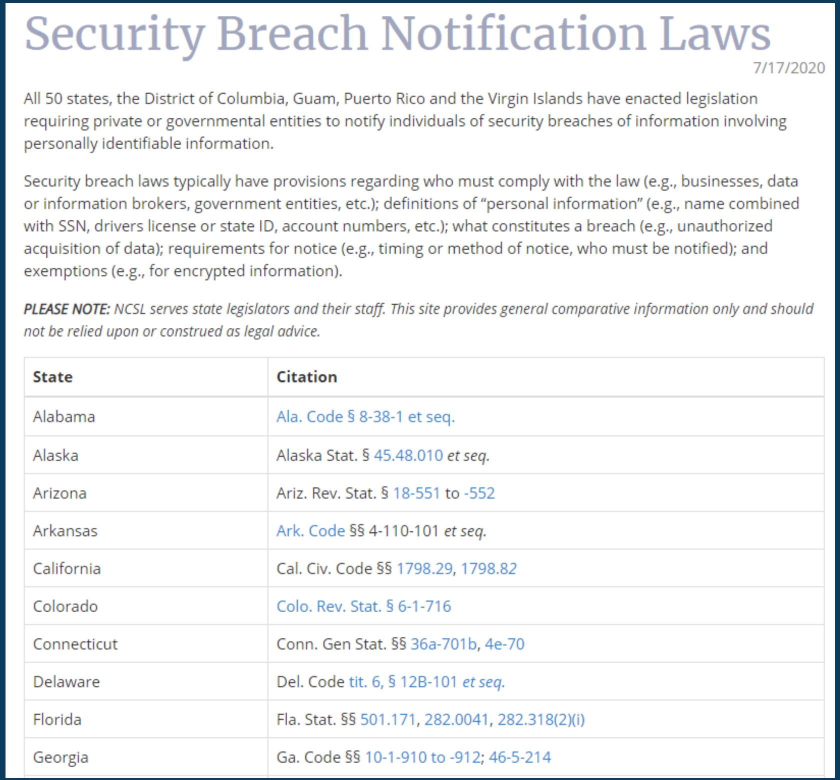
WHAT TECHNOLOGIES DO I PURCHASE?

WEBMAIL

BACK-UPS

Cyber Attack – Immediate Actions

- ❑ Assemble the right team
  - Cyber security expert
  - Legal
  - Incident command
  - Perhaps PIO
- ❑ Move to restore the system quickly
  - Operational issue
  - Cost issue
- ❑ Manage the incident
  - Communicate with employees, the commission, law enforcement, the insurance companies and maybe the public
- ❑ Determine if there has been a release of "personal information"
  - This will require notification
    - ❖ Employee data
    - ❖ Public/Patient data
- ❑ Protect the system from future assaults



Security Breach Notification Laws

7/17/2020

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

PLEASE NOTE: *NCSL serves state legislators and their staff. This site provides general comparative information only and should not be relied upon or construed as legal advice.*

State	Citation
Alabama	Ala. Code § 8-38-1 et seq.
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-551 to -552
Arkansas	Ark. Code §§ 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910 to -912; 46-5-214

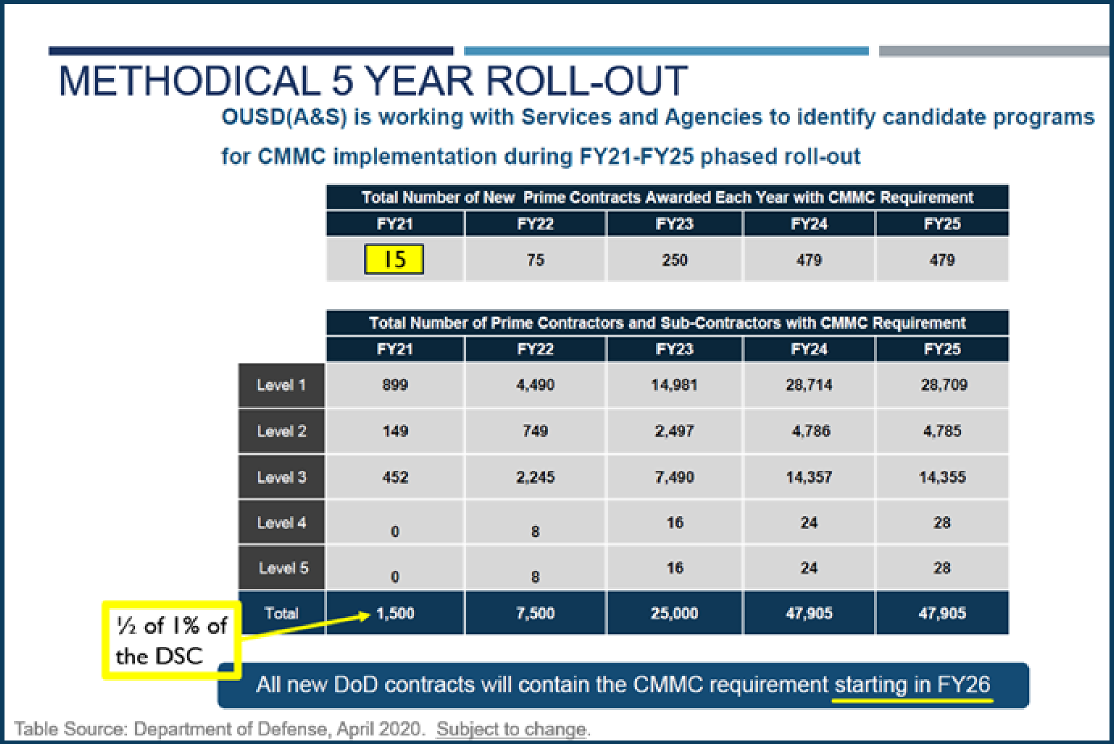
https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

The Challenges

- ❑ **Aging software systems**
  - o Windows 7 after 2019
  - o Old programs without updates
- ❑ **Inadequate network backup protection**
  - o Data backup on agency servers
  - o Data backup onto the world wide web
    - ❖ How safe is cloud based storage
- ❑ **Lack of prior planning and testing**
- ❑ **Poorly designed firewall**
- ❑ **No segregation of system administrative accounts and normal user account**
  - o Three sperate passwords for admin, backup and user
- ❑ **Personnel complacency**
  - o Using a public WIFI without a VPN (“But I just wanted to check my emails”)
  - o Facebook and web searching on agency computers (“But it was on my lunch break”)
  - o Opening unknown emails (“But I did not want to miss an important message”)
  - o Accountability (“Oops my bad I just violated the policy this one time”)
- ❑ **Porn sites**

Cybersecurity Maturity Model Certification (CMMC)

- The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices.
- AT THIS TIME; there are NO Companies and 100 individuals who can conduct certifications.
  - The current process
    - ✓ 2021 there will be 15 DOD contracts with certification requirements.
    - ✓ Certification will be required upon award.
    - ✓ CMMC-AB will ONLY allow companies submitting proposals to achieve certification.
    - ✓ C3PAOs are still being vetted.
    - ✓ MOST COMPANIES will only require ML1 Certification (roughly 300,000).
    - ✓ Certification lasts 3 years.
    - ✓ Provisional assessment may change; Delta assessment may be required.



METHODICAL 5 YEAR ROLL-OUT

OUSD(A&S) is working with Services and Agencies to identify candidate programs for CMMC implementation during FY21-FY25 phased roll-out

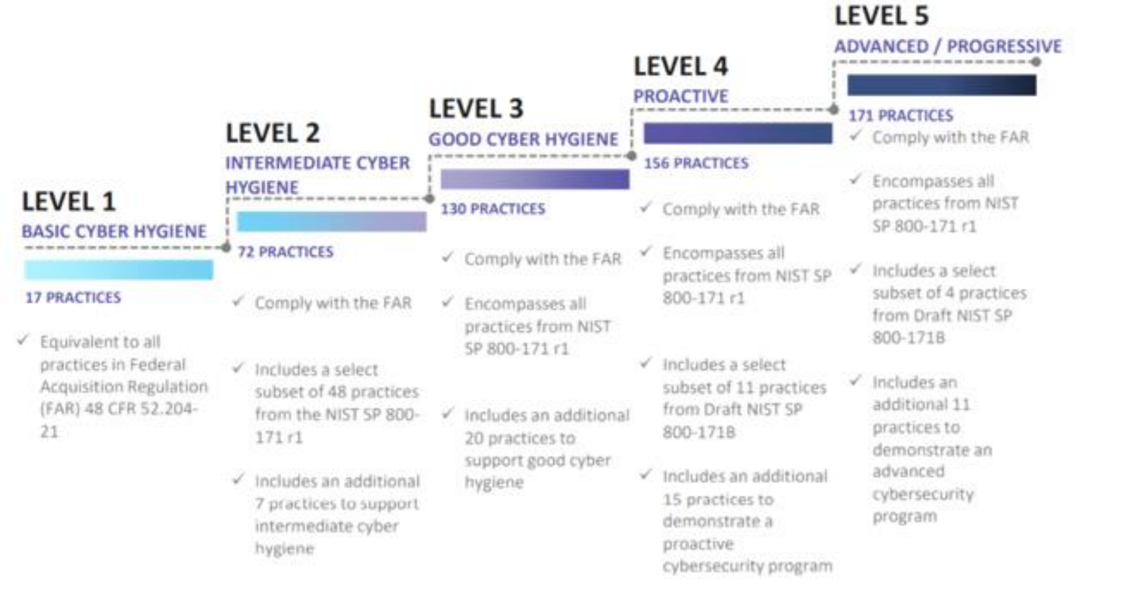
Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

½ of 1% of the DSC

All new DoD contracts will contain the CMMC requirement starting in FY26

Table Source: Department of Defense, April 2020. Subject to change.



LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
✓ Comply with the FAR
✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
✓ Includes an additional 7 practices to support intermediate cyber hygiene

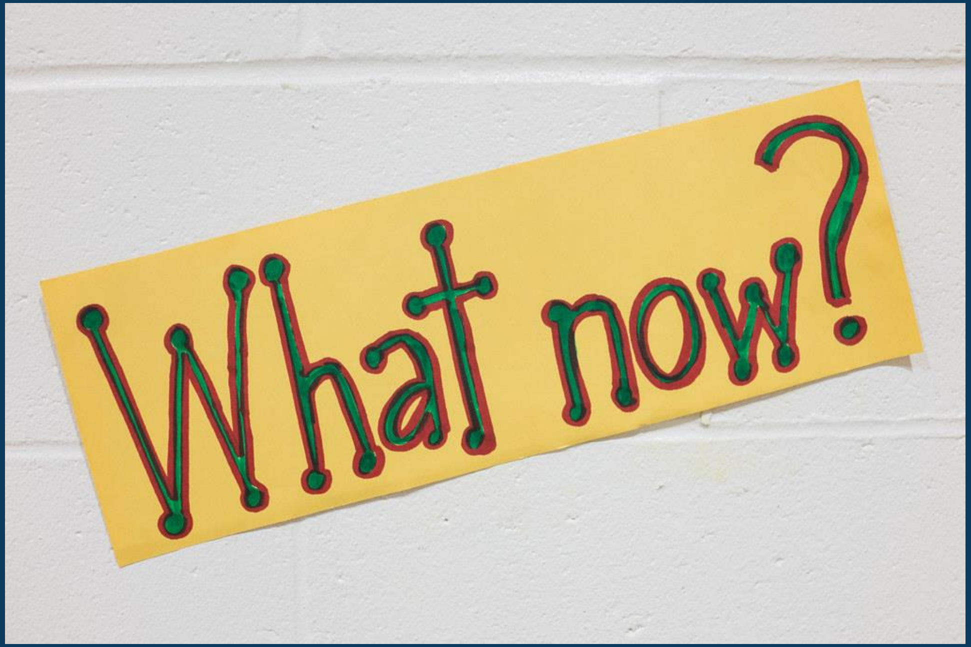
LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE
156 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
✓ Comply with the FAR
✓ Encompasses all practices from NIST SP 800-171 r1
✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

What should I do, after this meeting?

- ❑ Immediate actions – today
  - ○ Plan for this with your IT consultant.
  - ○ Ask the question: in the event of an attack, what will we do?
  - ○ Plan – operations for two weeks without computers.
  - ○ Determine if your systems and your backup servers or cloud storage are hardened against an attack.
  - ○ Train your staff to avoid risky behaviors.
  - ○ Make sure your insurance policies contain coverage for a cyber attack.
  - ○ Conduct a Risk Assessment.



Thank You

Michael Meline

MsIA, CISSP, CEH, CFE, PCIP, TNCA, C)DFE, ACE, CIPM, CIPP/E, ISO/IEC 27001 Auditor, CMMC Provisional Assessor

p. (208) 277-8857 | (866) CYBER-96
e. mike@cyberselfdefense.com
w. www.cyberselfdefense.com

CYBER®
SELF-DEFENSE

Springbrook

CISSP® CIPM CIPP E SDVOSB CMMC-AB PROVISIONAL ASSESSOR