The Road to verifiable Cybersecurity

May 2021

GPI USA

The Challenge: Increased demand for proven cybersecurity & data privacy

In the Energy Industry

E&E NEWS

<< Back to E&E News index page.

CYBERSECURITY

Huge federal hack ripples across energy industry

Christian Vasquez, E&E News reporter

Published: Thursday, December 17, 2020

Four days after a sweeping hack of government and private-sector computer networks came to light, U.S. electric utility companies are struggling to assess the fallout. Electric transmission lines are pictured. Chris Hunkeler/Flickr

Electric utilities are grappling with the fallout from one of the most significant cyber intrusions in years, as the far-reaching impact of a sophisticated hacking campaign comes into sharper focus.

Four days after the supply chain cyberattack on IT service provider SolarWinds was revealed, details on its global victims — from federal agencies to oil and electricity companies — are still emerging (***Energywire***, Dec. 15).

The SolarWinds software hijacked by suspected Russia-linked hackers was widely used by U.S. power providers, experts say, leaving many companies scrambling to find out if they're affected by the breach. And sources say a simple software update or patch won't erase the threat from the "Sunburst" malware: Organizations targeted by the hackers will likely have additional malware installed that could be difficult to find.

"Any organization that says, 'Yep, we got it solved. It's all good,' in the next 90 days: I would respectfully disagree," said Jim Guinn, global managing director for cybersecurity in energy, chemicals, utilities and mining at Accenture.

Healthcare … & beyond

NEWS

Hackers post detailed patient medical records from two hospitals to the dark web

SECURITY

Hackers post detailed patient medical records from two hospitals to the dark web

The files, which number in at least the tens of thousands, includes patients' personal identifying information.

HEALTH IT SECURITY

xtelligent HEALTHCARE MEDIA

Home News Features Interviews

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

Learn more about Data Encryption in our White Paper Library

Case studies, webcasts, eBooks and white papers all available now!

HEALTH IT SECURITY

VIEW NOW

LATEST HEALTH DATA BREACHES NEWS

Ransomware Hits Scripps Health, Disrupting Critical Care, Online Portal

Scripps Health is operating under EHR downtime and diverting some critical care after a ransomware attack over the weekend; a third-party incident, employee error, phishing, email hacks, and another Netgain victim complete this week's breach roundup.

CSO UNITED STATES | DIGITAL MAGAZINE | EVENTS | NEWSLETTERS | RESOURCE LIBRARY | IDG TECH(TALK) COMMUNITY

Home > Security > Critical Infrastructure

NEWS ANALYSIS

US bulk energy providers must now report attempted breaches

US bulk energy providers must now report attempted breaches as well as successful breaches. Guidance is murky over what constitutes an "attempted" breach.

By Cynthia Brumfield

CSO | JAN 11, 2021 12:13 PM PST

The Questions to Answer

- Is our security posture appropriate to meet our requitement & risks? – IDENTIFY
- Are we protected from reasonably-expected threats? – PROTECT
- Do we have appropriate situational awareness to detect an incident – DETECT
- Do we have trained people and tested processes to respond to an incident – RESPOND
- Can we recover and sustain key business operations if an incident happened? - RECOVER

Are we secure?

The Common Sense response

The Top 10 basic Steps for Detection & Response

1) Hire an independent firm to conduct an email and network threat assessment

2) Bolster access controls

3) Implement stronger audit controls

4) Ensure 24 x 7x 365 monitoring of your network with advanced intrusion detection systems (IDS)

5) Make top-down personnel education a priority for everyone (from the Board of Directors, to the C-Suite, managers and employees)

6) Create an internal and external crisis communications plan

7) Implement cyber insurance claims preparedness and adequate coverage

8) Create an incident response plan

9) Conduct periodic incident response exercises and simulations to test your response capabilities

10) Develop and test a Business Continuity Plan (BCP) and Disaster Recovery (DR) plan

Cybersecurity

Understanding, managing, controlling and mitigating risk to the organization's critical assets

Top Frameworks to ensure continuous controls

- HIPAA/HITECH
- **ISO27001**
- SOC 2
- NIST SP800-53
- COBIT
- PCI-DS
- **HITRUST CSF**
- NIST 800-171
- **CMMC** : DoD first, other federal contractors later..

ISO vs SOC2 vs NIST vs HITRUST vs CMMC

SOC 2

- 5 Trust Principles: Security, Availability, Processing, Integrity, Confidentiality & Privacy
- Compliance : prove controls have been implemented

ISO 27001

- Development and maintenance of an Information Management System – Risk based
- Compliance relies on risk assessment, identification and implementation of security controls and effectiveness review regularly

NIST

- Best practices set for federal agencies – Control-based
- Compliance relies on risk assessment, identification and implementation of security controls and effectiveness review regularly

HITRUST

- Designed for the Healthcare industry. Combines from various NIST and ISO controls

CMMC

- Designed to safeguard controlled unclassified information
- Practices are based on a level (1-5) specified in the contract
- More technical in nature, include situational awareness & maintenance

4 Steps

1. Define security objectives, business areas to cover
2. Gap Analysis
3. Identify appropriate security controls an implement (inc. documentation-SOP, and review/improvement process)
4. Audit

Steps to an Audit-Ready Cybersecurity & Privacy Program

1. Develop a targeted Vision, Mission & Strategy

- How the security program contributes to the organization success?

2. Adopt Cybersecurity & privacy principles

- Which law, regulations & contracts are driving compliance needs?

3. Develop policies, standards and procedures to support the principles

- Well designed documentation is foundational

4. Identify target maturity state

- What right looks like (people, process, technologies)

5. Implement Appropriate Controls to achieve the desired maturity

- Using People, Processes, Technologies

6. Use controls to assess risk & maturity across the business

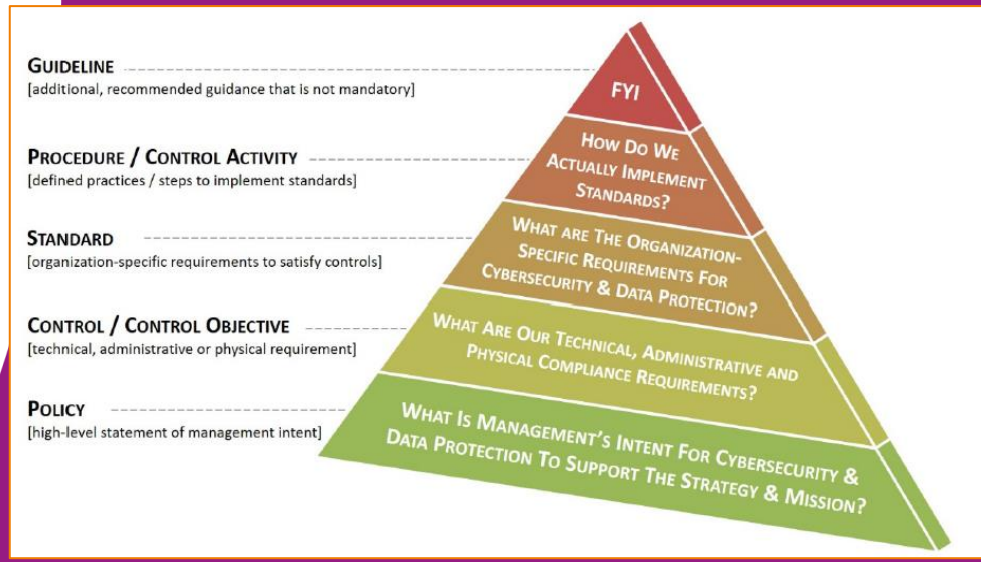
- A cybersecurity risk assessment is the process of identifying and analyzing information assets, threats, vulnerabilities and incident impact in order to guide security strategy.

7. Measure execution to identify improvement opportunities

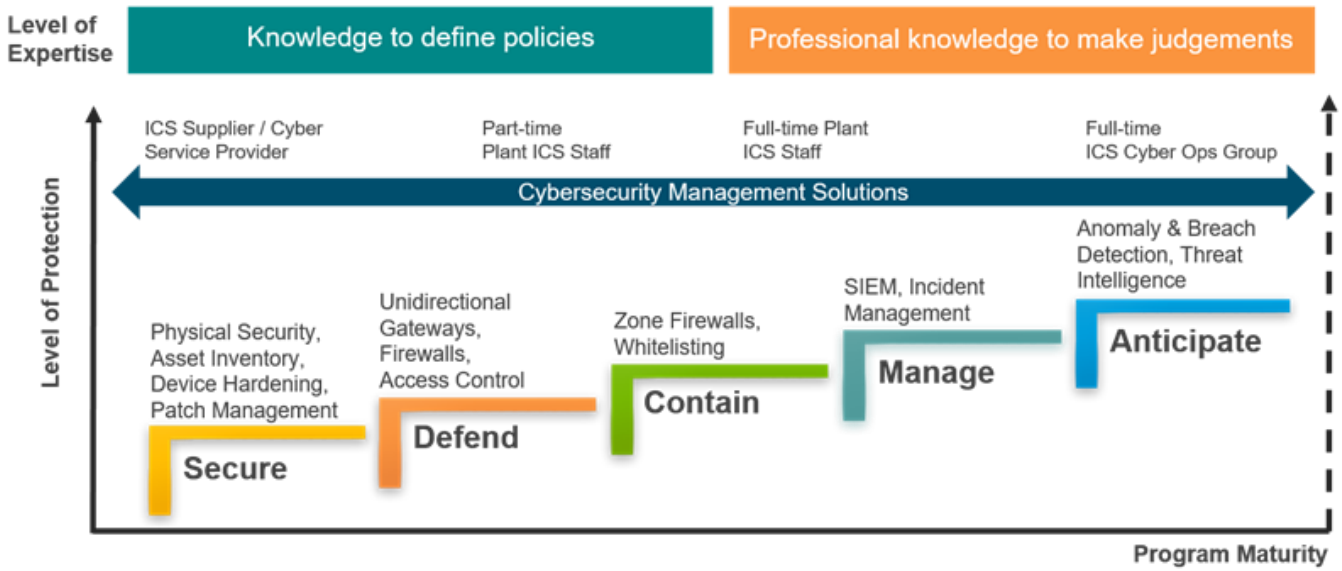
- Metrics, KPIs, trends,..

Cybersecurity

Understanding, managing, controlling and mitigating risk to the organization's critical assets

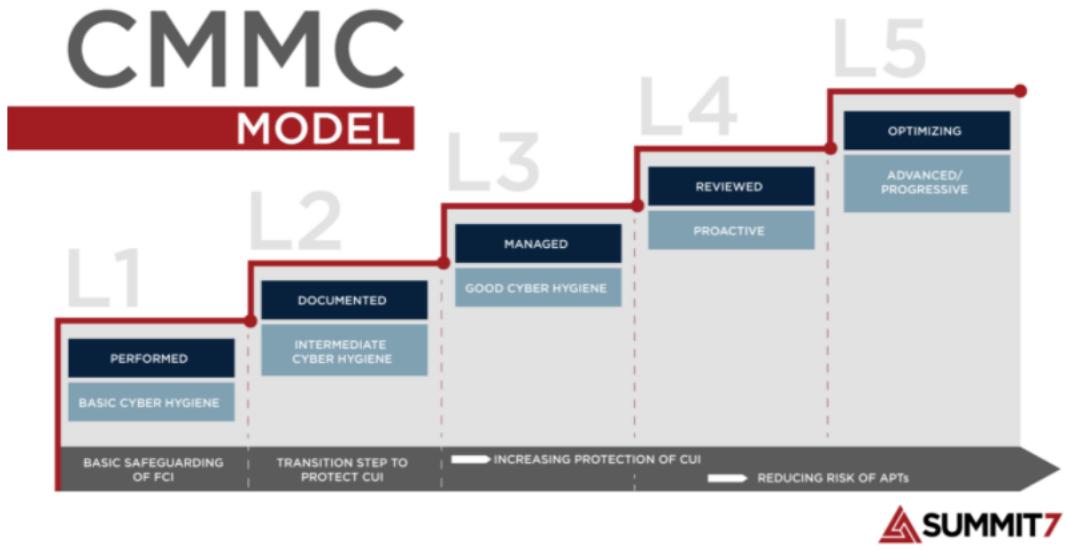


MATURITY MODELS



The 5 Levels of CMMC

- Level 1: 17 NIST 800-171 Requirements
- Level 2: 72 Practices (65 NIST 800-171 Requirements PLUS 7 Other Practices)
- Level 3: 130 Practices (110 NIST 800-171 Requirements PLUS 20 Other Practices)
- Level 4: 156 Practices (110 NIST 800-171 Requirements PLUS 46 Additional Practices)
- Level 5: 171 Practices (110 NIST 800-171 Requirements PLUS 61 Additional Practices)



SUMMIT7

CMM 0	CMM 1	CMM 2	CMM 3	CMM 4	CMM 5
Not Performed	Performed Informally	Planned & Tracked	Well Defined	Quantitatively Controlled	Continuously Improving
NEGLIGENT PRACTICES	*AD HOC PRACTICES*	*REQUIREMENTS-DRIVEN PRACTICES*	*ENTERPRISE-WIDE STANDARDIZATION*	*METRICS-DRIVEN PRACTICES*	*WORLD-CLASS PRACTICES*