Cyber Security Plan
Why you need one and How to Create One.

Joseph Fishel
AA. BSBA, MBA, CBET
OwnerThe Fishel Group LLC

MDEXPO
SoCal • October 11-13, 2022

Quotes

- If you Fail to Plan, You are Planning to Fail.
  Benjamin Franklin

- A Plan isn't a Plan unless it has Identifiable Goals and a Time Line, Otherwise it is only an idea
  Fortune from a fortune cookie

Why you need a Cyber Security Plan

- Provides Guidance or direction for:
  - Procurement of New Equipment Requirements
  - Identifies procedures should an attack take place to be followed
  - Helps identify who does what and when
  - Helps prepare ahead of time to prevent attacks

What is the Difference between an IT/IS Cyber Plan the Plan from an HTM Plan?

- IT/IS equipment is primarily the same manufacture for Servers, Laptops, Computers, etc.
- IT/IS equipment can have OS upgrades and Patches pushed to them
- Applications such as Word, Excel, EPIC are standardized
- Clinical Equipment has different Apps, Operating Systems, Different Patch levels

Components of a Cybersecurity Plan

Components of a Cybersecurity Plan

- Get the Basics of Security In Order. ...
- Collaborate with Internal Stakeholders. ...
- Work Within a Framework. ...
- Be Aware of Threat Intelligence. ...
- Understand Regulatory Factors and General Liability. ...
- Conduct a Thorough Risk Assessment. ...
- Undertake Incident Response Planning.

Get the Basics of Security In Order.

- Standardize and Publish Secure ways of Putting Medical Devices on the Network
- Develop a standard for Purchasing Requirements
- Identify the medical equipment and who covers it.
- What tools are going to be used?
- What data will you collect?

Collaborate with Internal Stakeholders

- IT/IS
- IT/IS Cyber
- Risk
- Clinical Engineering/Biomed/HTM
- Legal

Identify who does what and when

IT/IS Roles

- IT/IS
  - Has Tools for Identifying issues on the Network
  - Determines requirements for Hard Wired and Wireless Networking
  - Identifies and implements various protocols to put things on the network.

IT/IS Cyber

- Identifies Vulnerabilities, Attacks, Attempts etc.
- Sets the bar for minimum requirements
- Works with HTM/Biomed/Clinical Engineering to insure things are Segmented

Risk

- Can help determine what the Risk is
- Can help identify time lines for Reporting.
- Risk can help implement change and rules
- Risk can give Weight to the polices based on Risk and Liability.
- When a breach occurs they are the primary ones to respond, HIPPA, FDA, Joint Commission etc.

Clinical Engineering/Biomed/HTM

- You are the Subject Matter Experts
- You Own the Plan
- Putting Devices on the Network, Patching, Identifying new equipment for purchase.

Legal

- If a vulnerability occurs Legal will need to be involved with representing the facility.
- They can help put in Flags so that when the Flags occur they are notified s that they aren’t caught unaware.

Work Within a Framework. ...

- Pick a Framework or Standard to Use
- Compare the standard to existing practices
- Use the Framework to develop a cross walk from requirements to existing policies and procedures
- Use the crosswalk to determine level of Compliance

Be Aware of Threat Intelligence

- You have to know what the threats are to identify your vulnerabilities
- IT/IS usually have the latest threats.
- IT/IS has tools to identify possible attacks and infections
- IOT is a tool that can Assist in identifying threats
- Manufactures as well as FDA and ECRI issue Notices

Conduct a Thorough Risk Assessment. ...

- Use your CMMS to run lists based on OS/Patch levels and any other type of cyber identifier.
- Ask IT/IS what tools they have that can identify vulnerabilities
- Have IT/IS run an assessment with their tools
- Develop Fields in Your CMMS that will assist in identifying which devices have a certain vulnerability

Undertake Incident Response Planning

- Determine what needs to be done should an infection occurs
- Identify who does what and when IT/IS, Risk, HTM
- Identify various scenarios based on degrees of severity.

What about Equipment not on the network?

- Is it Vulnerable?
- Can it be protected?
- How can it be attacked?
- Can it be Patched?

IS IOT a Plan?

- IOT is an Application
- It only addresses devices on the network
- It identifies vulnerabilities.
- Can be linked to some CMMS programs to generate notices and create work orders.
- Can automatically update your CMMS for OS, IP Address, MFR, Model Serial Number

How to use the Plan to set rules

- Limit the number of files retained on your devices
- Rules about going out to Social Media from Medical Devices.
- Attaching Personal devices to Medical Equipment

Where Do Cyber Attacks Come From

- External over the Network
- Thumb drive’s/Laptops of Service providers.
- USB ports on the side of equipment
- Doesn’t have to be on the network, A kid could plug in a Phone, or tablet to charge.

What are you trying to Protect?

- Medical Devices for operability
- Stealing of PHI/PI
- Loosing Control of Equipment

How HIPPA Feeds Into the Program

- Loss of Data Triggers a Process
- Amount of Data lost can Generate a fine
- Bad Public relations

Joint Commission and a MEMP Plan

- Joint Commission is the standard
- MEMP manual is how you meet those standards
- A Crosswalk is often developed between the Standards and how you meet them

What is Needed to Develop a Cyber Policy and Procedure

- Pick a Standard to follow
- Identify the Stakeholders to include in creating the Plan
- Identify various Policy and Procedures currently in place with the Stakeholders.

Determine what Standard you are going to use

- ISO 27001 A common standard that requires auditing PCI DSS Payment Card Industry
- HIPPA Health Insurance Standard Hospitals Follow
- FINRA The standard that Banks follow
- GDPR European standard for General Data Protection
- NIST National Institute of Standards and Technology The standard the federal government follows.

Subcategory	Informative References	In-House Policy or Procedure	Rating	Date to be Completed By
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	Located in CMMS and identified as to what is on the network		
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	OS Platforms identified in CMMS and an inventory can be provided		
ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8	In the process of developing flows with IT		12/14/2022
ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9	50% identified in the process of developing with IT		11/19/2022

Score Card colors definition

	Policy or Procedure meets Criteria	100%
	Policy or Procedure meets some of the Criteria but needs more	80%
	There is something there but more is needed	50%
	There is no Policy or Procedure at this time	0%

Some Additional Standards

ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4: Governance and risk management processes address cybersecurity risks
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

Converting your Crossover

- Once your crossover is completed the actual document can start to be created
- List the Category and then list the applicable current Policy or Procedure
- For Missing Policies and Procedures insert the category for future development.
- Currently NIST has approximately 108 Standards

Cyber Policy and Procedure Document

- It will take Time to Create
- It is a Living Document
- As things change so will the document

How a CMMS can help

- When a Field is needed the field can be easily created
- Some examples of fields are Operating System, Version, Patch Level, Application, Application version, Microprocessor etc.
- Able to be searched or data mined
- If linked to an IOT work orders can be generated to correct or generate for a patch.
- Automatic Reports or algorithms can be created to annunciate a condition such as Contains PI/PHI and Can Not Locate (CNL)
- For all devices both on the network and not, this is a great place to consolidate information.

Draw backs

- Creating Fields and populating takes time.
- For existing devices it means going back to gather information to include those devices in being able to be reported on.
- Identifying information/fields up front before going back to collect.
- It will take time to Pull things together

Positives

- Pulls HTM Cyber Security into one program
- Identifies the different Roles of who does what and when
- Creates procedures for when something occurs
- Creates Proactive Procedures and plans to be implemented ahead of time.

Web Link to NIST

cyberframework@nist.gov

Questions?

Win $100 Simply By Posting Your Picture!

Take a picture

Post on social media using **#MDExpo**

The attendee who posts the most will win a $100 gift card!!