

# Holding Vendors Accountable for IoT Security Through New Federal Legislation

By Bob Hunter, CEO




# AlphaGuardian™

Securing the Industrial Internet of Things

# Bob Hunter Key Background Points

- [Principal Author "Data Center OT Cybersecurity" Chapter for the 2021 Data Center Handbook by Wiley & Sons](#)
- [Co-Author of Lawfare & Brookings Institution Paper "The SolarWinds Hack Can Directly Affect Control Systems."](#)
- **Founded NetBrowser Communications in 1996**
  - *Created the first Data Center Infrastructure Management (DCIM) system*
  - *Customers included AT&T, Charles Schwab and Merrill Lynch*
- **Founded TrendPoint Systems in 2001**
  - *Created the first branch-circuit smart meter which included waveform capture*
  - *Customers included the FAA, Facebook & Twitter*
- **Founded [AlphaGuardian Networks](#) in 2014**
  - *Providing NIST-compliant cybersecurity systems*
  - *First systems for integrated NIST Confidentiality, Integrity and Availability protection*

# The Problem Every Government Agency Faces

- 
- IT data systems rely on critical IoT to provide the power and cooling to keep information flowing.
  - IoT power and cooling systems use 20<sup>th</sup> Century communications protocols that are unsecured against 21<sup>st</sup> Century attacks.
  - SolarWinds SNMP Management Systems were exploited using these vulnerable protocols by Russia to give Moscow access to key U.S. assets.
  - IoT vendors have taken the approach that either:
    - Their systems are not vulnerable and/or,
    - They are not responsible for the cybersecurity of their systems.

# IoT Communication Protocols are 20+ Years Old

## IoT Systems Are Highly Vulnerable to Cyberattack

### Standard IoT Communications Protocols include:

- **SNMPv1 and v2:** *“Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Disable legacy unencrypted protocols such as Telnet and SNMPv1 and v2...”*  
*U.S. Department of Homeland Security CISA - ICS 4/16/2018*
- *“SNMPv3 fails to provide its advertised security guarantees”*  
*...These vulnerabilities are implementation agnostic and demonstrate a fundamental flaw in the current protocol”*  
*- Dr. Patrick Trayor, Nigel Lawrence, Georgia Institute of Technology*
- **Modbus:** *“When the master sends a message to the field device, it needs to first authenticate the device from which it obtained the packet and then process the packet. The Modbus protocol lacks this ability and hence middle man attacks can easily take place in Mod* - *California Energy Commission*
- **BACnet:** *“Network security in BACnet is optional. The existing BACnet Network Security architecture is based on the 56-bit DES cryptographic standard and needs to be updated to meet the needs of today’s security requirements.”*  
*- BACnet Secure Working Group*

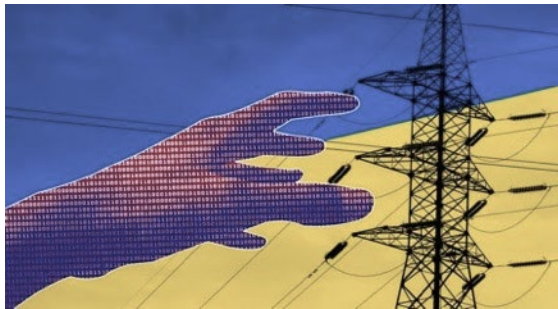


# The Significance of the Cybersecurity Problem

## Attackers are Using Protocol Weaknesses to Attack Mission-Critical IoT



- The 2020 SolarWinds SNMP Management Console attack is widespread across critical U.S. government and Fortune 500 company assets. This attack has been severe at many agencies and vendors. – [Fedscoop](#)



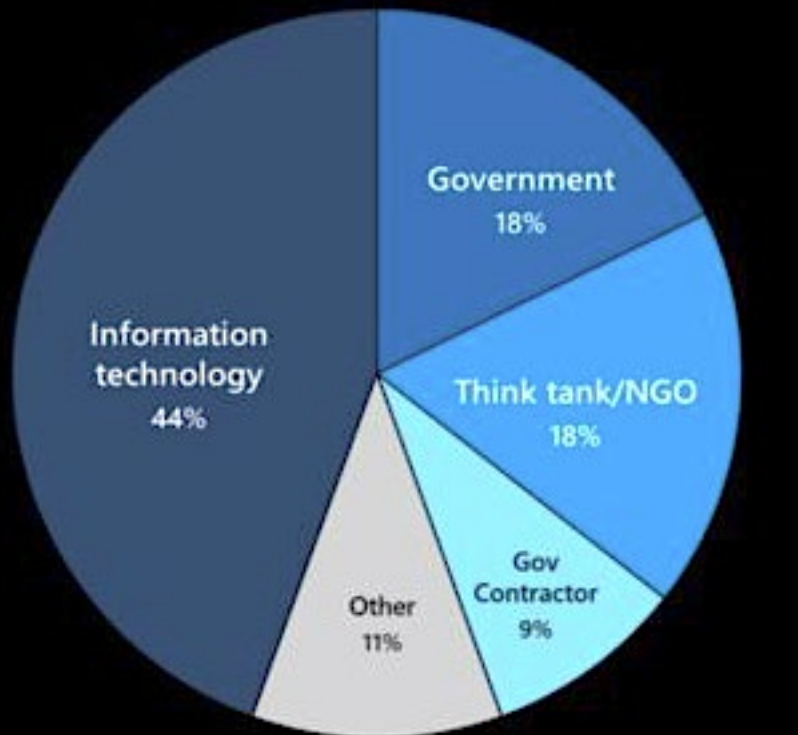
- The Russian attack on a Ukrainian power plant targeted a control room UPS SNMP-card to completely immobilize the controls. They then opened the master breakers, shutting-off power to nearly 250,000 people. – [Wired Magazine](#)



- The Staminus cloud attack used a Rack Power Distribution Unit as a backdoor to attack database servers. Information was stolen using the PDU as the vehicle. – [Krebs on Security](#)

# The Significance of the SolarWinds Attack

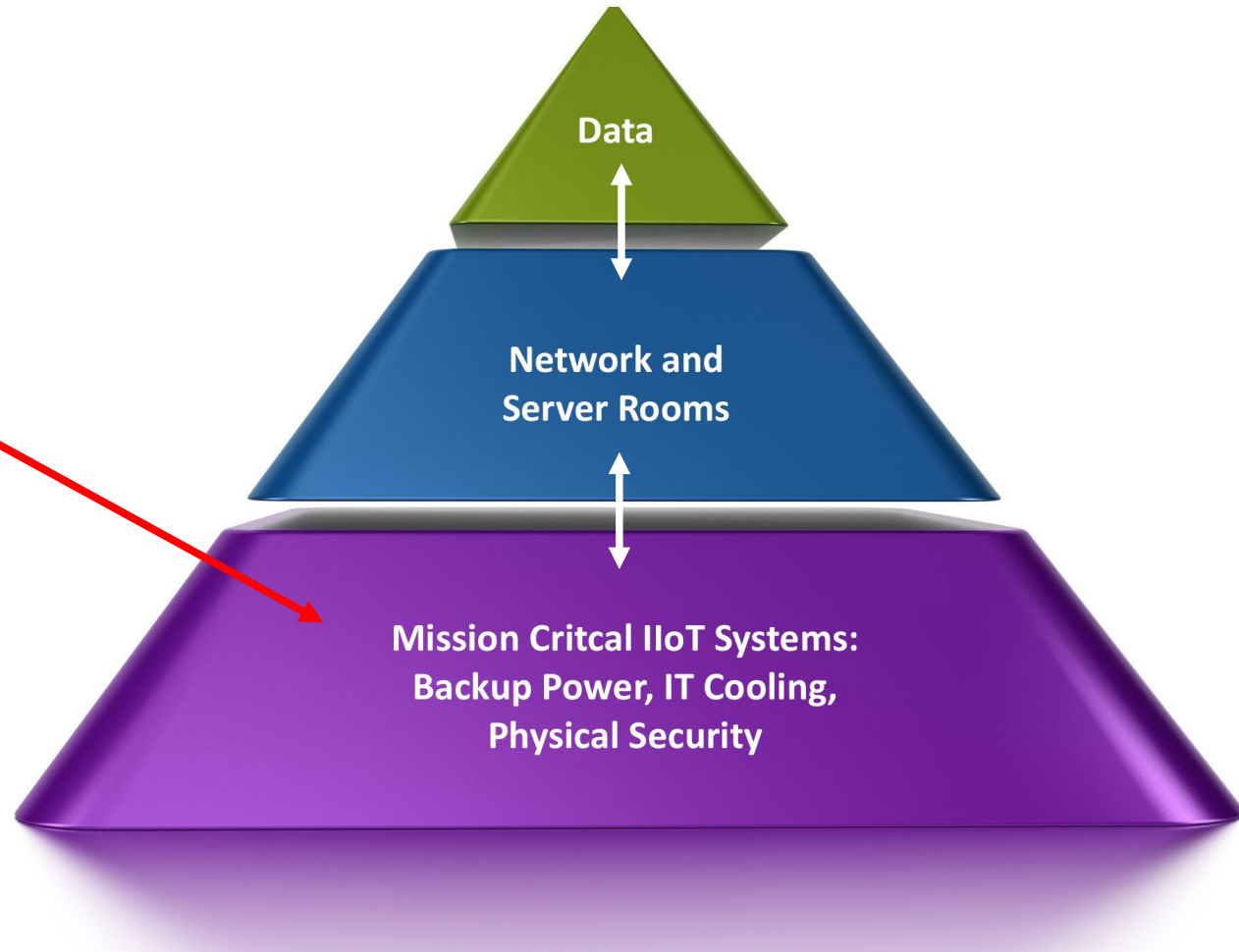
## Many Government Agencies and Contractors Have Been Under Attack



- “From a software engineering perspective, this is the largest and most sophisticated attack the world has ever seen... Certainly more than 1,000 engineers were used to create this Malware”.  
– Brad Smith, President of Microsoft
- IT, Government and Government Contractors were heavily hit in these attacks. These attacks are continuing because Malware was placed deep into the recesses of equipment like IoT systems that have no antivirus software within them.

# IT Support Systems are a Gold Mine

An attack on any IoT system can give full access to IT Systems and Data



# New Federal Agency IoT Cybersecurity Law

## Internet of Things Cybersecurity Act of 2020 Requires the following:

“The Director of the Institute shall develop and publish under section 20 of the **National Institute of Standards and Technology Act** (15 U.S.C. 278g-3) standards and guidelines for the Federal Government on the appropriate use and management by agencies of **Internet of Things devices owned or controlled** by an agency **and connected to information systems owned or controlled by an agency**, including minimum information security requirements for managing cybersecurity risks associated with such device.”

- **Focus is IoT systems that support IT.** For typical facilities this includes all power and cooling systems that support your network closets, server rooms, lab rooms and any data centers on the property
- All IoT devices connected to IT systems owned or controlled by a Federal Agency must conform to NIST standards by September 4<sup>th</sup>, 2021



# New Cybersecurity Executive Order

## Biden Executive Order of May 12, 2021

"The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))."

- Focus is IoT in data centers and cloud systems. Biden Executive Order requires **FULL NIST Compliance** and is a “Dramatic Game Change” – Chris Krebs, former US CISA Chief
- This EO directly affects ALL IoT Systems that support IT including:
  - Uninterruptible Power Supplies (UPSs)
  - Power Distribution Units (PDUs)
  - Computer Room Air Conditioners and Air Handlers (CRAC & CRAH)
  - Building Management Systems (BMS)
  - Data Center Infrastructure Management Systems (DCIM)

# What are the NIST Cybersecurity Standards?



The NIST Standards are the Security Triad:  
**C. I. A.**

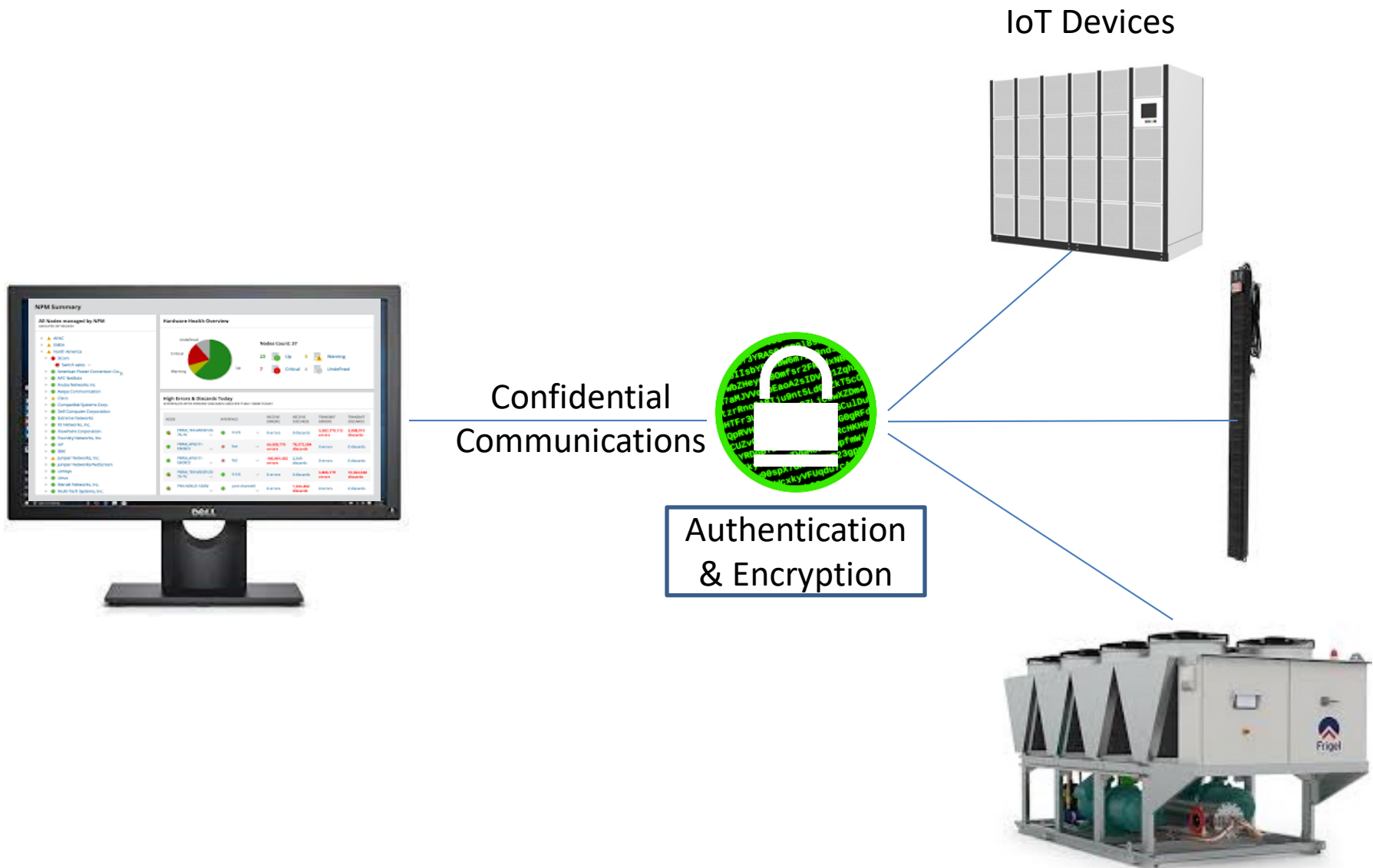
- ❖ **Confidentiality** – All data must be encrypted from point-to-point
- ❖ **Integrity** – Must ensure that all IoT data is accurate and timely
- ❖ **Availability** – Must ensure uptime of all IoT system components

# Confidentiality

## **NIST defines Confidentiality as follows:**

- *“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.”*
- *IS THE LOGIN AND DATA TRANSFERRED SECURED BY ENCRYPTION?*
- To keep data confidential, each device must offer the following:
  - ✓ Provide an encrypted authentication means to ensure that any connection is made by an authorized source
  - ✓ Provide encryption of all data to and from the device

# Encryption for each IoT Device's Data





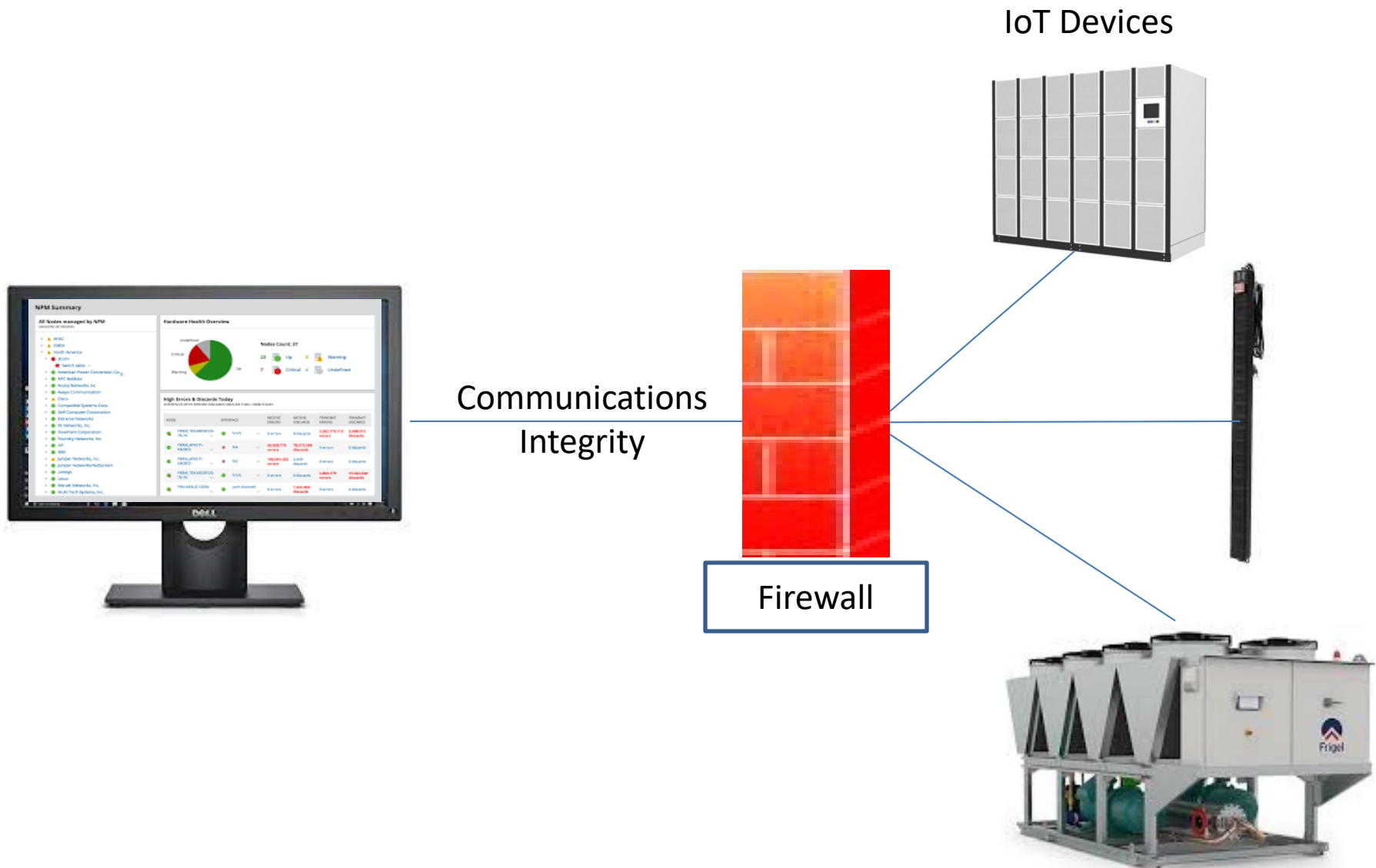


# Integrity

## **NIST defines Integrity as follows:**

- “Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.”
- *IS THE DATA RECEIVED FROM ITS INTENDED SOURCE AND UNALTERED?*
- To ensure data integrity, each device must offer the following:
  - ✓ The ability to instantly identify a data value that may have been modified or altered for quick response to potential issues
  - ✓ The ability to determine the origin of each data packet and to reject any data packet of unknown origin.

# Integrity for each IoT Device's Data

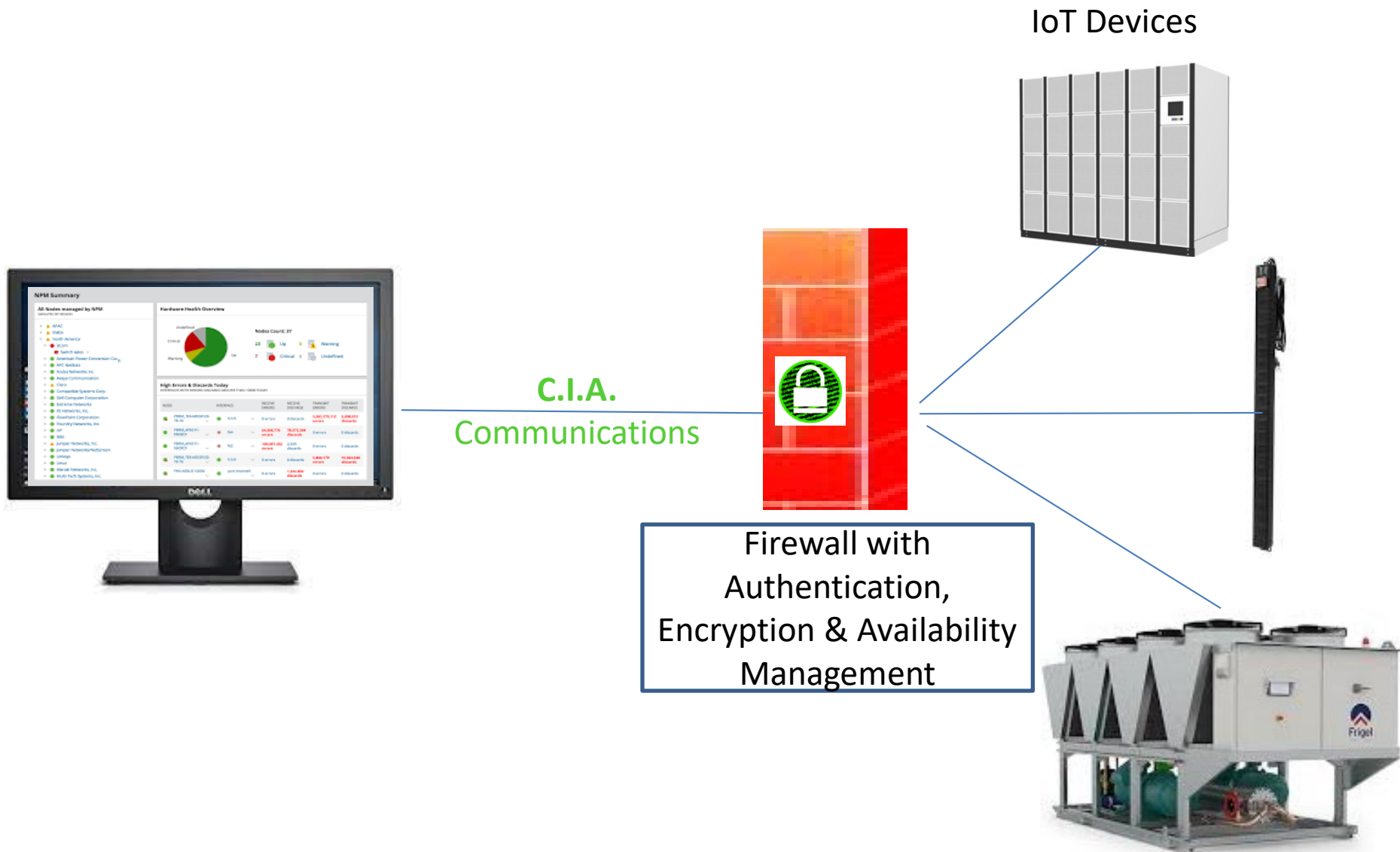


# Availability

## **NIST defines Availability as follows:**

- “Ensuring timely and reliable access to and use of information.”
- *ARE THE SYSTEMS FULLY AVAILABLE?*
- To keep data available each device must offer the following:
  - ✓ The ability to instantly determine if the device is non-responsive
  - ✓ The ability to gather data as quickly and reliably as possible

# Putting it All Together: IoT C.I.A.





# Summary

## **You now have a great legal toolset to use to stop cyber breaches**

- ✓ IoT 2020 and Biden Cybersecurity EO
- ✓ They give you the power and authority to demand cybersecure IoT/OT systems
- ✓ You no longer need to rely on your supply chain vendors to “do their best” to help you stay cybersecure. If any of their devices use SNMP or Modbus, the vendor supplying those products **MUST** provide you with a security device or system to secure the device and its communications.

**You now have the authority to better control your IoT device cybersecurity.**



# AlphaGuardian™

**AlphaGuardian Networks, LLC**

111 Deerwood Road, suite 200  
San Ramon, CA. 94583  
(925) 421-0050  
(888) 990-ALPHA

Principal Contact: Bob Hunter  
[bhunter@alphaguardian.net](mailto:bhunter@alphaguardian.net)