






# Building Systems Overlooked. Under Secured.

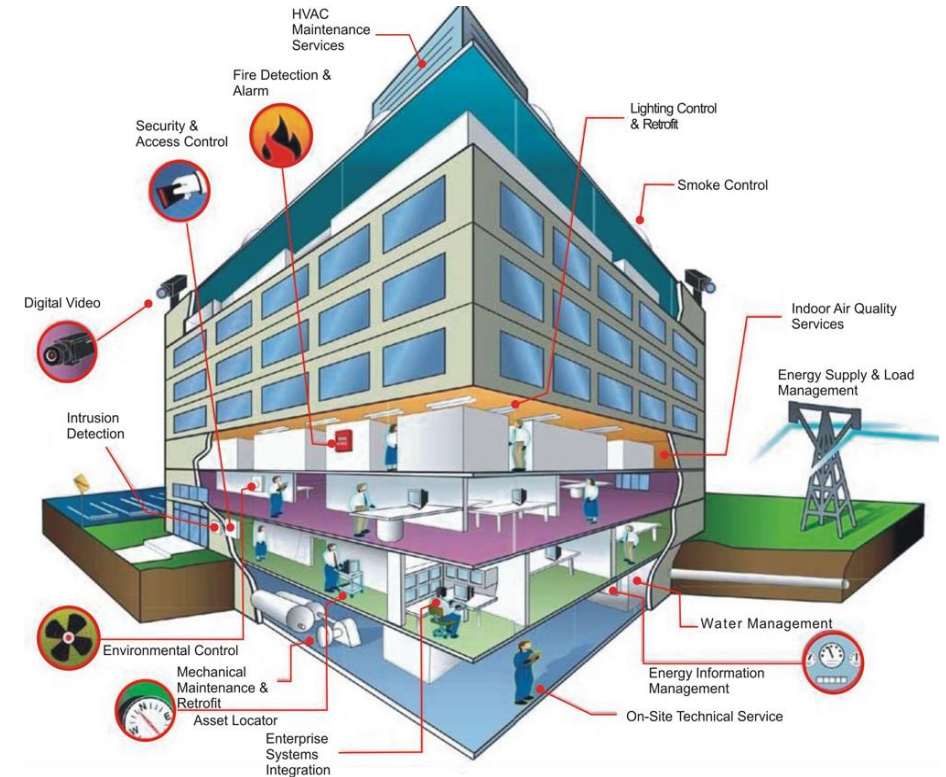
Dr. Joel Rakow, Fortium Partners, Cybersecurity and Building Systems



# As Much as Your CIO Wants to Help...

## 3 Key Points for Today:

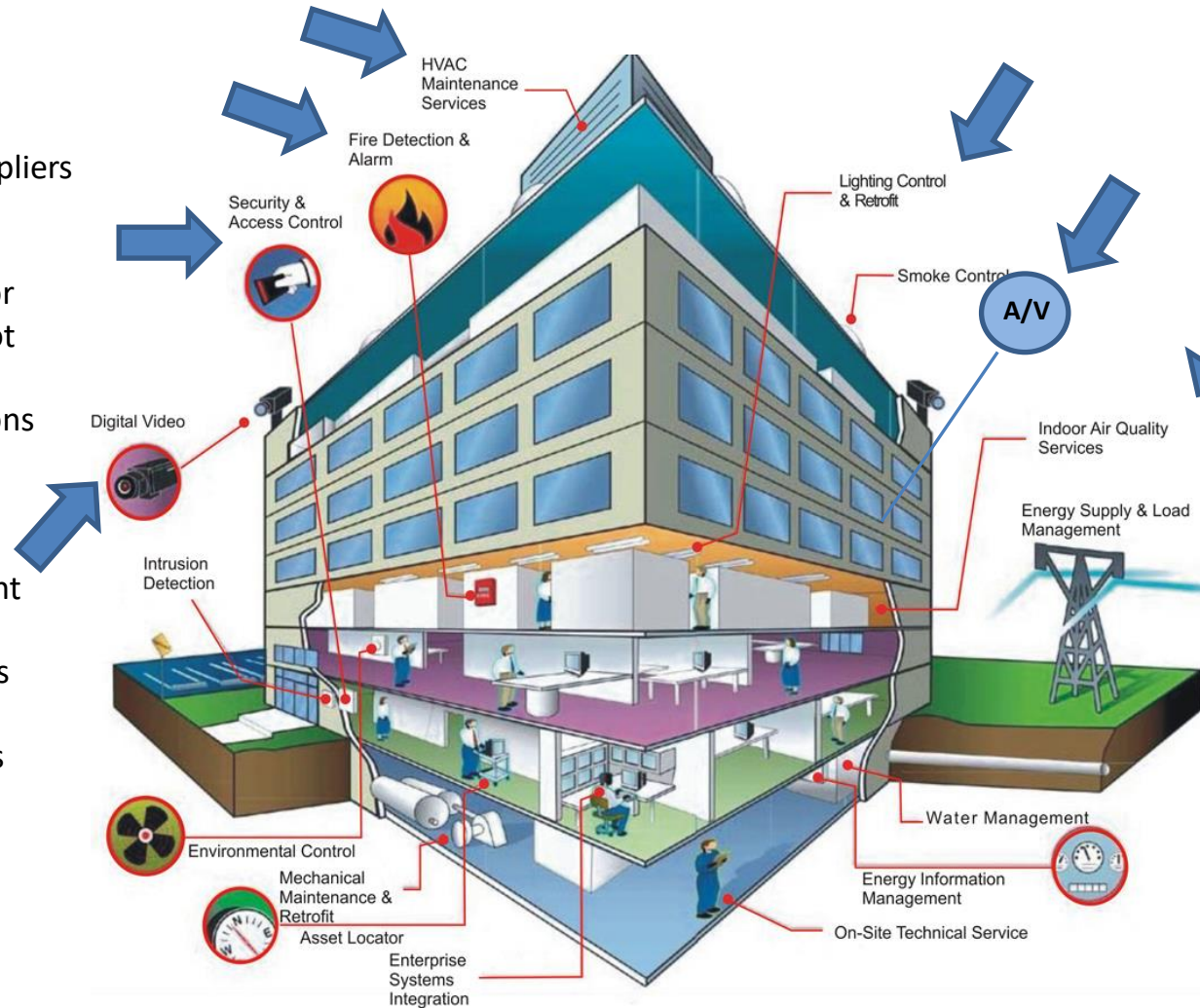
-  1. Vulnerabilities and Breaches Reside Outside and Beyond IT's Ethernet Networks
-  2. These Breaches are often the Points of Entry – Not the Point of Attack or Exploit!
-  3. Contracts Trump Standards When Managing 3<sup>rd</sup> Party Building System Suppliers



# Common Operational Technology (OT)

## What a CIO Might See:

- Director of Facilities
- Building System Suppliers
- Systems IT Cannot Monitor or Manage
- 55 Considerations for Products they Do Not Know
- Manual Configurations
- Back Doors to the Network
- Default Passwords
- A Single User Account
- Privileged Users
- Firmware downloads sites
- Cyber Vulnerabilities



a.k.a

- “Building Systems”  
(before connecting to the Internet.)
- “Building IoT”
- “Smart Buildings”

## Key Watch Words:

- Improvements
- Enhancements
- Efficiencies



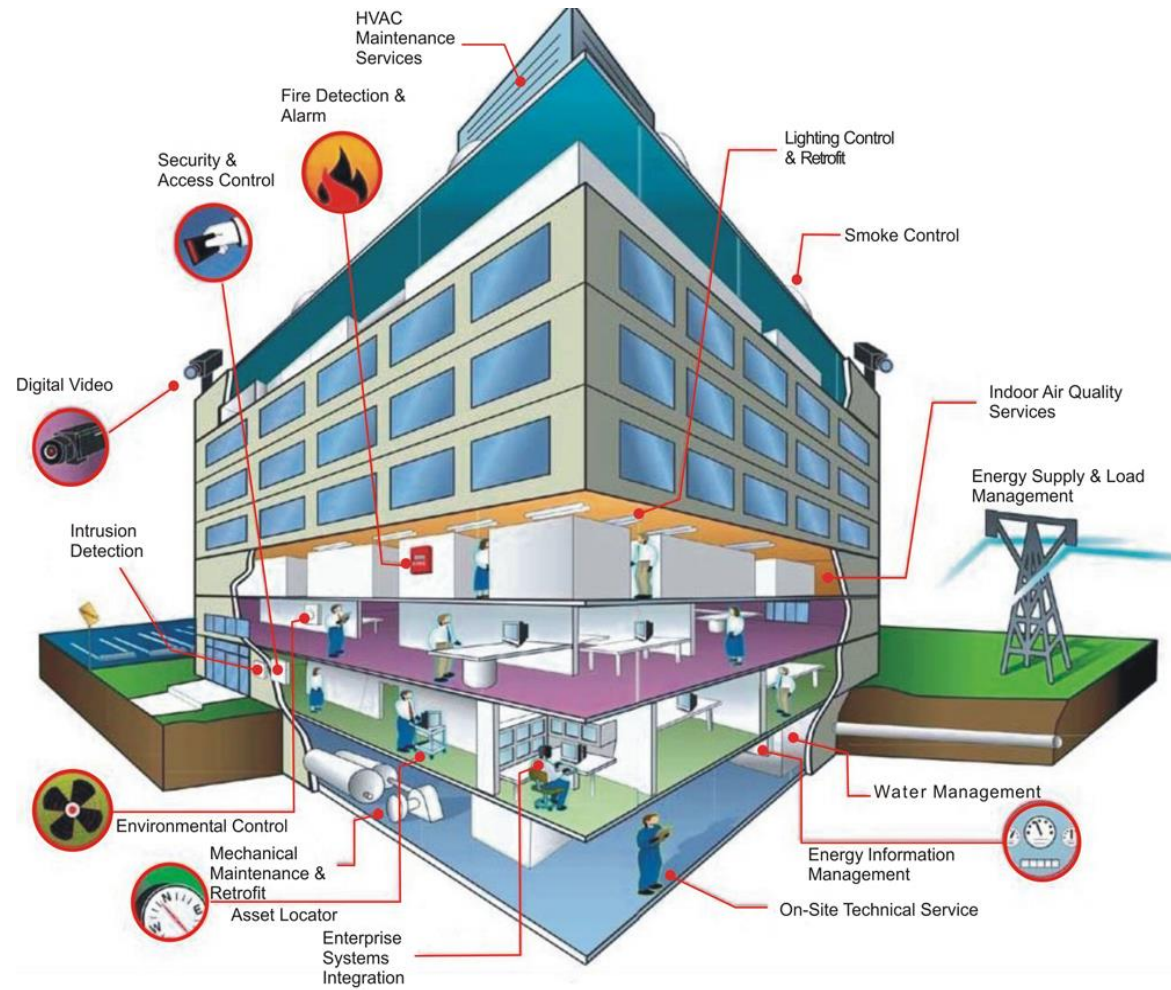
# Communication

## Hardened, Secured or Unsecured?

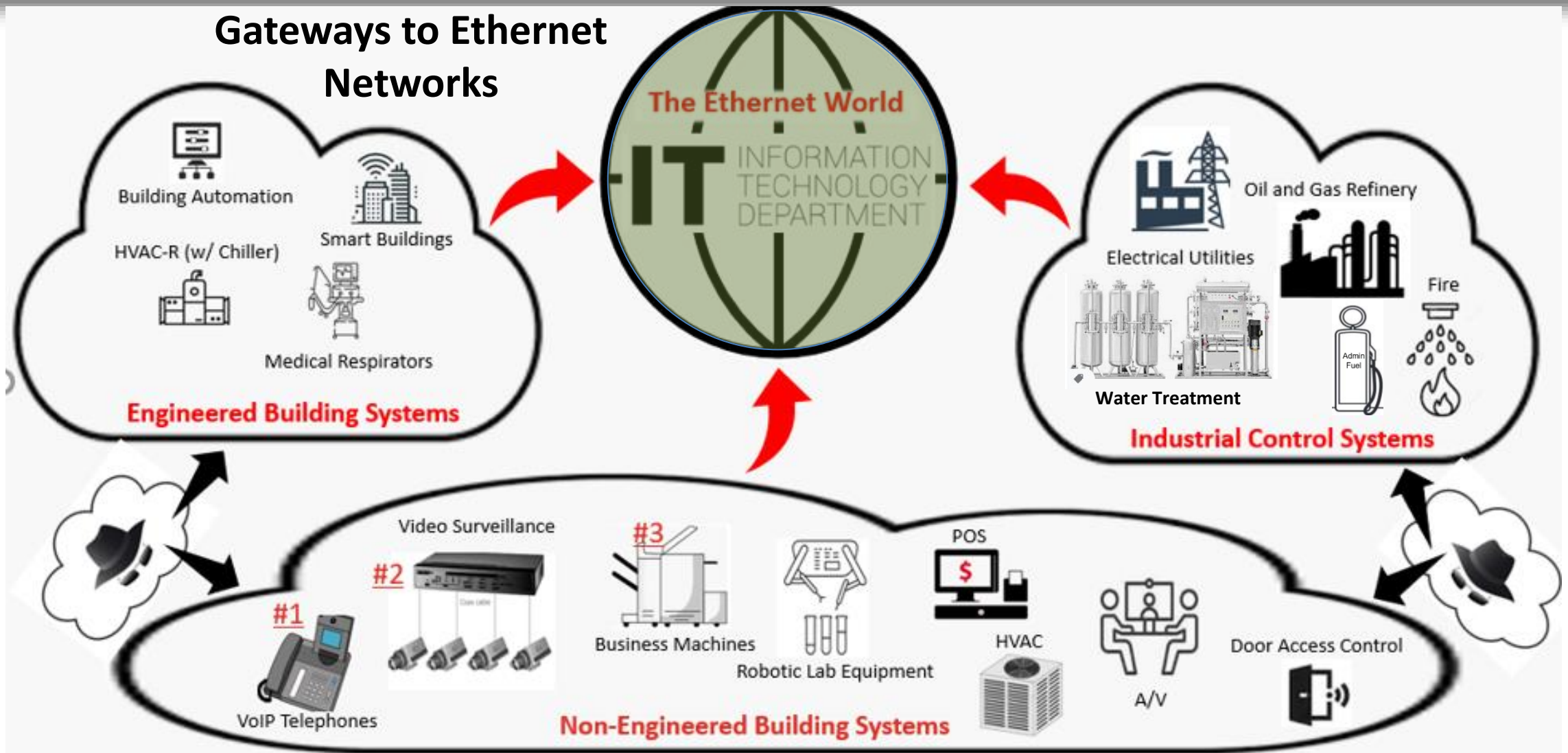
- Serial
- IP
- Analog-to-Digital Converters
- **Sensors**
- Radio
- LoRaWAN
- Ethernet

a.k.a

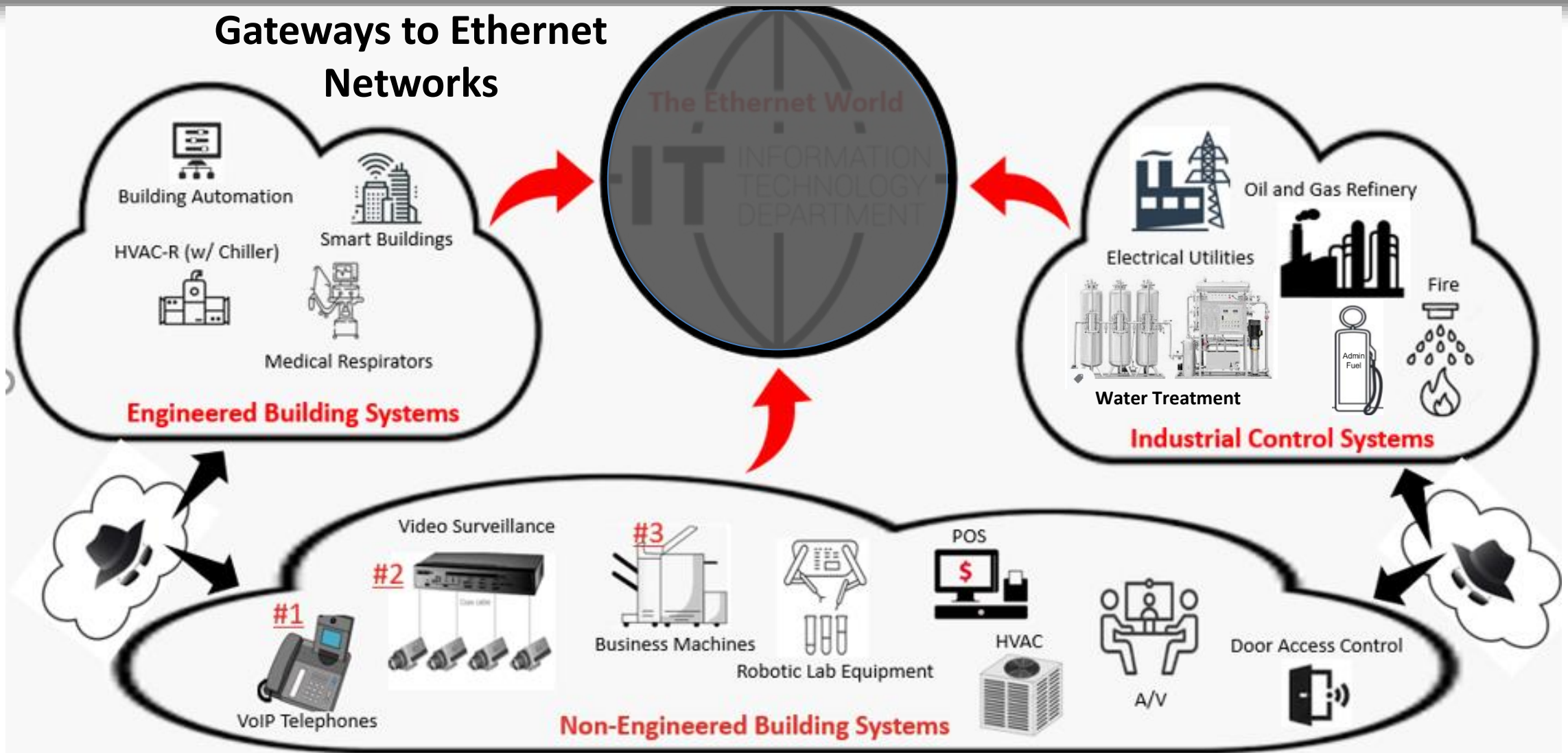
- “Building Systems”  
(before connecting to the Internet.)
- “Building IoT”
- “Smart Buildings”



# Where Improvements are Needed



# Who Keeps the Bad Guys Out?

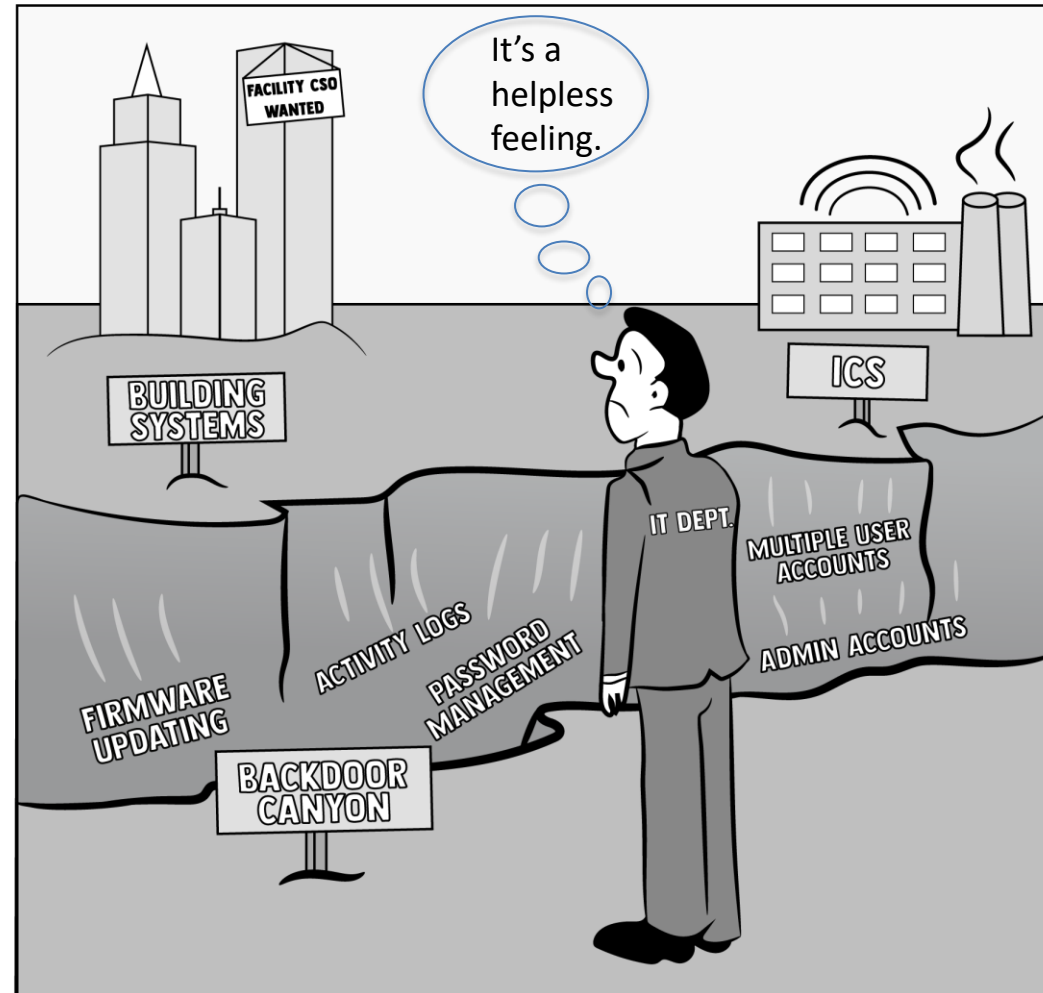




# As Much as Your CIO Wants to Help...

## OT Lacks:

- Interoperability with IT
- Security-Design Consideration
- Network Security for “Out-of-Band” Devices and Components



Ethernet vs. Serial  
Data Streams

Out of Band  
Plague IT's  
Ethernet  
Systems with  
Malware

# As Much as Your CIO Wants to Help...



## Point #1

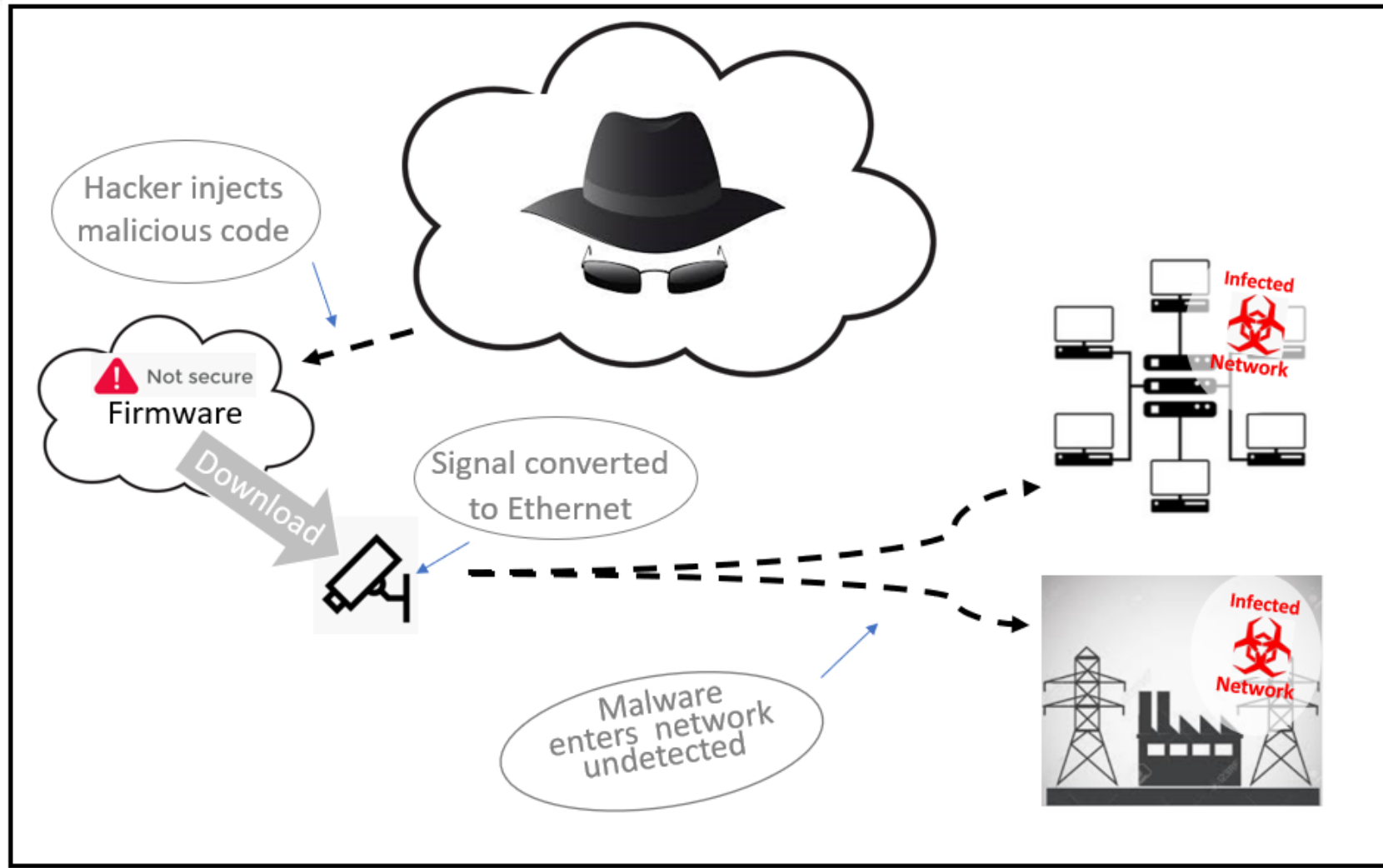
Vulnerabilities and Breaches Occur Outside and Beyond Your Ethernet Networks





# Attacks Starting Outside IT or “Out of Ethernet Band”

A Pre-Ethernet  
Attack



Research  
**eset**

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

**FORTIUM**  
Partners

# More Clear View with 2019 & 2020 Research Reports

Links to  
Research  
Available  
Upon  
Request



1

**A Clearer Understanding of Building Systems and Cybersecurity.** Approximately 60% of successful cyber attacks on U.S. public companies found their initial point of entry through building systems, as reported by The Harvard Business Review.<sup>1</sup> The top 3 points of entry for successful cyber attacks perpetrated by nation states on 1,400 publicly-traded U.S. companies were: VoIP telephone systems; Video Surveillance Systems; and, Business Machines<sup>1</sup>



# Part of the Soft Underbelly of OT

## Top 3 targets of cyber attack

Provide initial point of entry

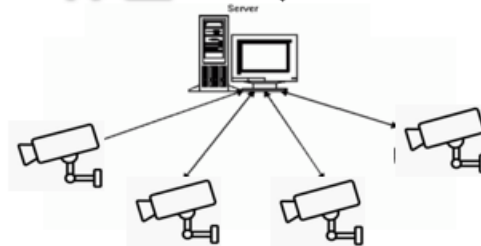
- Convert Sensor Signals from Analog to Digital
- Internet Connected
- Network Connected

#1



Voice-over-IP Telephones

#2



Video Surveillance Systems

#3



Business Machines



Links to  
Research  
Available  
Upon  
Request

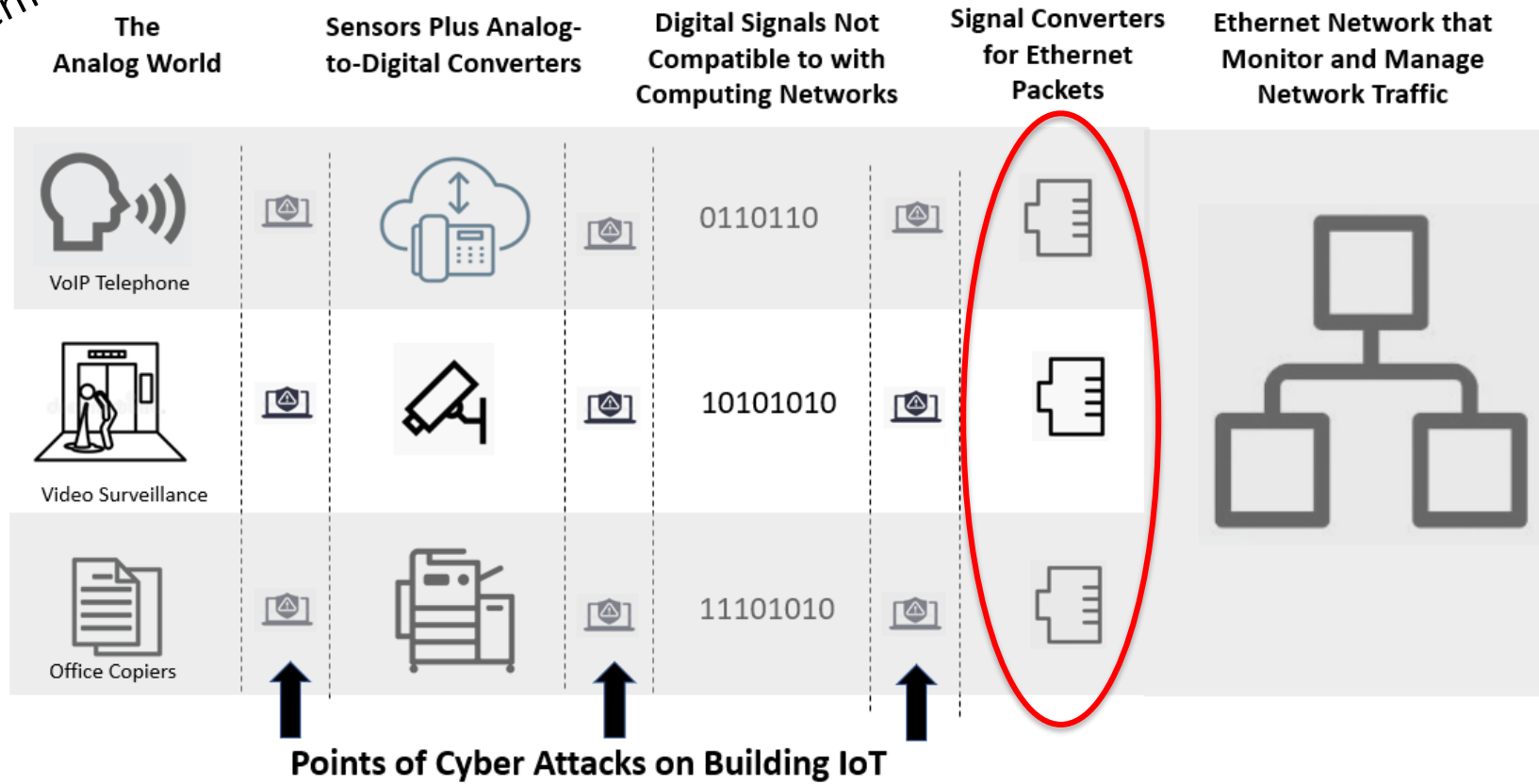




# Outside IT or “Out of Band”

## How Three Sensors Enable Attackers to Infect IT Systems and Go Undetected

A Pre-Ethernet  
Attacks

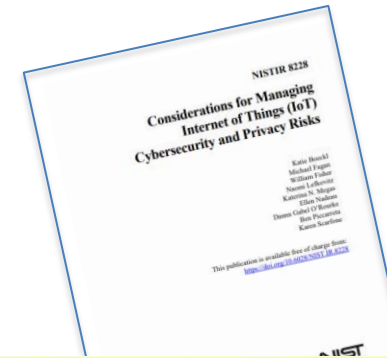


Research



Honeywell

# NIST Strikes Out – No Standard for IoT



2

**NIST Strikes Out Swinging at Building Systems.** NIST issued an Internal Report, 8228, stating they could not issue a cybersecurity standard for IoT systems and devices. (This includes Building Systems, sometimes referred to as legacy IoT). Instead of a standard, NIST issued as more than 50 considerations that must be applied to each type of IoT system and device. The reason given, by NIST, is there is a lack of interoperability between the platforms and tools used by substantially all IT departments to monitor and manage network-connected systems, and way too many IoT devices and systems require configurations performed manually or from non-IT platforms.

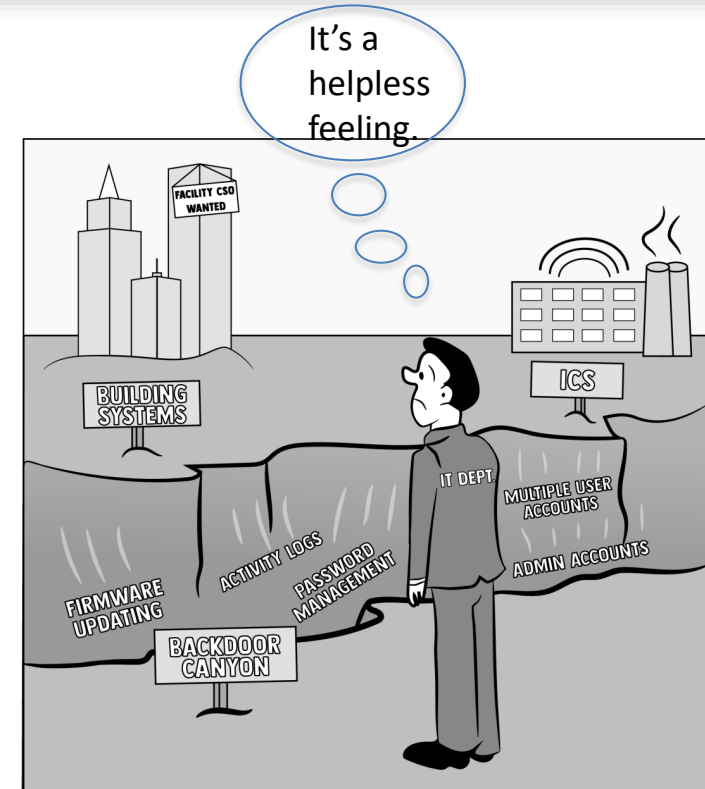
Other standards explicitly exclude all or certain non-Ethernet communications.

# As Much as Your CIO Wants to Help...



## Point #2

These Breaches are the  
Point of Entry – Not the  
Point of Attack or Exploit!





# Standards Are Good - Contracts Are Better

**Supply Contract**

A contract between \_\_\_\_\_

\_\_\_\_\_

and \_\_\_\_\_

\_\_\_\_\_

for \_\_\_\_\_

\_\_\_\_\_

Contents	Page
Part C1: Agreements and contract data	1
Form of Offer and Acceptance	1
Contract Data provided by the Purchaser	4
Contract Data provided by the Supplier	9
Part C2: Pricing Data	11
Part C3: Scope of Work	14
Conditions of Contract (available separately)	

Notes about this contract are printed in boxes like this one. They are not part of the contract.

© This contract contains copyright material from the New Engineering Contract system. The copyright material has been reproduced with permission of the Institution of Civil Engineers (London), and may not be reproduced other than in this document without the permission of the copyright holder's agent, Publishing Director, Thomas Telford Ltd, 1 Heron Quay, London E14 4JD. Telephone + 44 20 7987 6999, Fax + 44 20 7538 4101

Based on the  
NEC Engineering and Construction Contract 2nd Edition (November 1995),  
NEC Professional Services Contract 2nd Edition June 1998, and  
NEC Engineering and Construction Short Contract, 1st Edition July 1999



Our Installation Team

**Use Contracts to Secure the Systems Installed by Your Suppliers**

# Specify the Security You Deserve

## Exhibit A

### Building Systems Supply Contract

#### GOAL

Enable  
Secure  
Installation  
Projects

#### SYSTEM TYPE

-Access  
Control  
-Video  
Surveillance

#### MARKET

Passenger  
Rail Transit

#### STALWART SECURITY SYSTEMS

##### SECURITY SYSTEM INTEGRATOR

Cybersecurity attacks are a threat to every organization and Stalwart is committed to increasing your security with the work we do for you. This document shares with you the controls we employ to harden the system against cyber attack. We focus on controls applied at the device level. Network-level security is more the domain of your IT department and is not our mission with the Cybersecurity Hygiene. Upon request, we will be happy to adapt this protocol into a customized service-level agreement customized specifically for your organization.

##### Level 1: Single Location

At organizations with a single, individual locations, Stalwart provides the following:

- Assure data is backed up prior to modifying data
- Update Windows OS to most current version
- Enable automatic updates for OS (current version is always recommended)
- Change default passwords
- Implement hardened passwords (or password phrase)
- Store and deliver passwords on a password safe
- Check new devices for malware prior to connecting to your network
- Disable anonymous access to the application software
- Set time and date using the network clock
- Limit physical access to devices, including cameras, DVRs, controller for door access control, etc.
- Create separate end user accounts for administrators



JOEL.RAKOW@FORTIUM  
PARTNERS.COM



310 418 7322



WWW.LINKEDIN.COM/I  
N/JOEL-RAKOW-71741?



Our Installation Team

Encourage (and perhaps help) your suppliers prepare to harden and/or secure what they sell and install

# Make It Easy for Suppliers' To Improve

## Let Your Suppliers Know



March 31, 2021  
RE: Cybersecurity and Your Built Space

Dear \_\_\_\_\_:

Cybersecurity is an important and increasing concern to our organization's stakeholders. We ask for your participation in our security efforts by hardening the building systems you supply and service for us.

In addition to any of your other security practices, we request that your organization prepare an affirmative statement of the specific security controls that, effective 6 months from the date of this letter, your field services teams will provide when performing installation, service and maintenance work on systems and devices that connect with our computing network. This statement will become your Cybersecurity Hygiene for services you perform for our organization.

In connection with your Cybersecurity Hygiene, we expect reasonable assurance, from your senior management, that your organization:

- Prepares and enables field and technical personnel to deploy the security controls that make up your Hygiene
- Agrees to include your Hygiene's security controls in your statement of work or as an addendum to applicable contracts
- Will respond to IT security questionnaires we submit to you with your Hygiene
- Will record device and relevant security information in the BuiltSpace software platform we provide for this purpose
- Will use reasonable business efforts to update your security controls (Hygiene) from time to time, but no less than once per year

We acknowledge that cybersecurity is a relatively complex concern and that you rely on any of the following:

- The free use of the Secure Controls Framework (<https://www.securecontrolsframework.com/>);
- The free NIST 8228 Internal Report (<https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf>);
- The fee-based, full-service NeverCry Cyber Defense for Building Systems provided by Fortium Partners. You can contact Fortium Partners through my office, or directly via Dr. Joel Rakow ([joel.rakow@fortiumpartners.com](mailto:joel.rakow@fortiumpartners.com)), 310 418 7322)
- A third-party service provider of your choosing

**Important Action Item:** We request a written notice, within 15 days, of your intentions regarding this matter. We expect that you will complete the Cybersecurity Hygiene and related activities within the next six months.

We appreciate the relationship between our two organizations, and we look forward to continuing our work together, as we respond to today's pressing cybersecurity concerns.

Feel free to contact me should you have any questions.

Respectfully,

Director of Facilities



Our Installation Team

## Allow 6 Month Advance Notice Consider a Cost-Sharing Program



# Potential Requirements for Each Supplier

## Terms You Should Require:

- A Specific Cybersecurity Controls
- 20 15-Minute Sessions of Orientation and Coaching on Each Control Delivered to Technicians
- Tone-at-the-Top Meeting with Senior Management
- Mutual Agreement on Contract Language

## Optional Terms:

- Guidance on Solutions:
  - Software-Defined Networks
  - Perimeter-Defined Networks
  - Encrypted Wireless Mesh Networks
  - Other
- Period Cybersecurity Meetings
- Software Platform for Tracking OT Devices & Systems
- Fixed-Fee Pricing (includes securing systems provided)



Our Installation Team

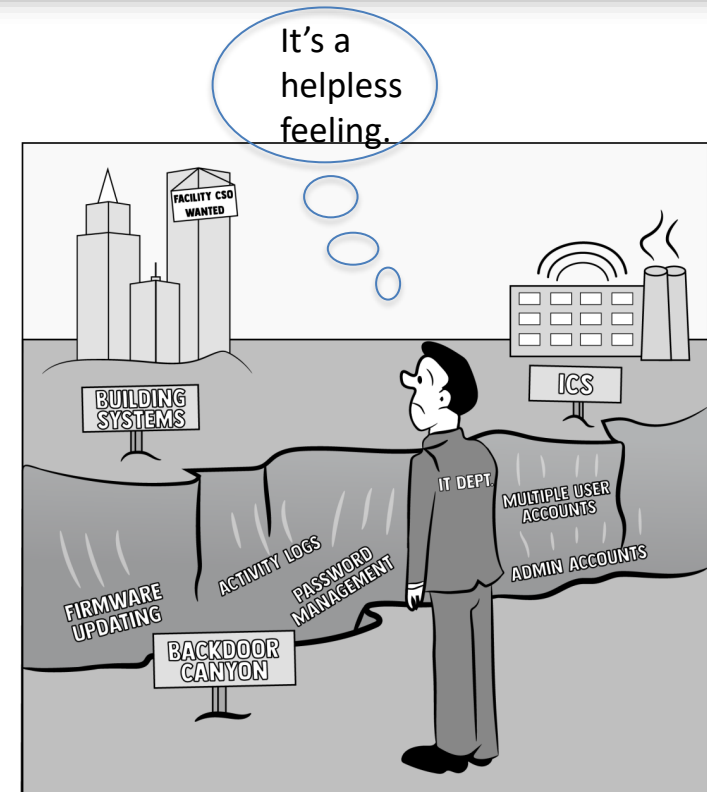
**Point Them to a 3<sup>rd</sup> Party Resource, If They Need One**

# As Much as Your CIO Wants to Help...



## Point #3

Contracts Trump Standards  
When Managing 3<sup>rd</sup> Party  
System Suppliers



# Q&A



???



Dr. Joel Rakow, Fortium Partners, Cybersecurity and Building Systems  
[joel.rakow@fortiumpartners.com](mailto:joel.rakow@fortiumpartners.com)  
310 418 7322

Links to  
Research  
Available  
Upon  
Request