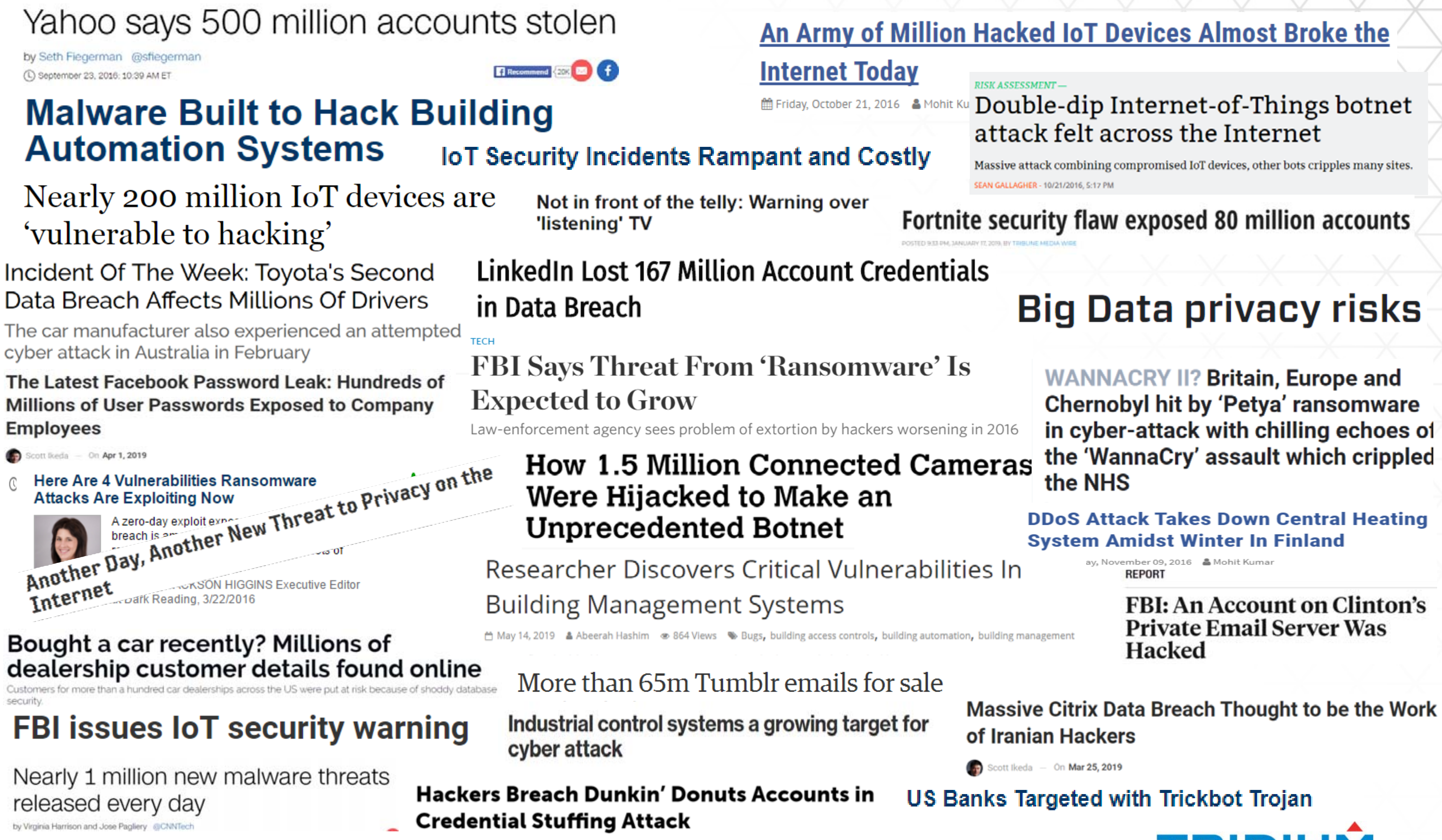
Cybersecurity Considerations in Smart Buildings

Kevin T. Smith, Tridium

You Really Shouldn’t Be Surprised..



Yahoo says 500 million accounts stolen

by Seth Fiegerman @sfiegerman

September 23, 2016: 10:39 AM ET

Malware Built to Hack Building Automation Systems

IoT Security Incidents Rampant and Costly

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Friday, October 21, 2016 Mohit Ku

RISK ASSESSMENT —

Double-dip Internet-of-Things botnet attack felt across the Internet

Massive attack combining compromised IoT devices, other bots cripples many sites.

SEAN GALLAGHER - 10/21/2016, 5:17 PM

Nearly 200 million IoT devices are ‘vulnerable to hacking’

Not in front of the telly: Warning over 'listening' TV

Fortnite security flaw exposed 80 million accounts

POSTED 9:33 PM, JANUARY 17, 2019, BY TRIBUNE MEDIA WIRE

Incident Of The Week: Toyota's Second Data Breach Affects Millions Of Drivers

The car manufacturer also experienced an attempted cyber attack in Australia in February

LinkedIn Lost 167 Million Account Credentials in Data Breach

Big Data privacy risks

TECH

FBI Says Threat From ‘Ransomware’ Is Expected to Grow

Law-enforcement agency sees problem of extortion by hackers worsening in 2016

The Latest Facebook Password Leak: Hundreds of Millions of User Passwords Exposed to Company Employees

Scott Ikeda — On Apr 1, 2019

WANNACRY II? Britain, Europe and Chernobyl hit by ‘Petya’ ransomware in cyber-attack with chilling echoes of the ‘WannaCry’ assault which crippled the NHS

Here Are 4 Vulnerabilities Ransomware Attacks Are Exploiting Now

A zero-day exploit exp… breach is a… …ts of

…KSON HIGGINS Executive Editor …Dark Reading, 3/22/2016

Another Day, Another New Threat to Privacy on the Internet

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

…ay, November 09, 2016 Mohit Kumar

Researcher Discovers Critical Vulnerabilities In Building Management Systems

May 14, 2019 Abeerah Hashim 864 Views Bugs, building access controls, building automation, building management

REPORT

FBI: An Account on Clinton’s Private Email Server Was Hacked

Bought a car recently? Millions of dealership customer details found online

Customers for more than a hundred car dealerships across the US were put at risk because of shoddy database security.

More than 65m Tumblr emails for sale

FBI issues IoT security warning

Industrial control systems a growing target for cyber attack

Massive Citrix Data Breach Thought to be the Work of Iranian Hackers

Scott Ikeda — On Mar 25, 2019

Nearly 1 million new malware threats released every day

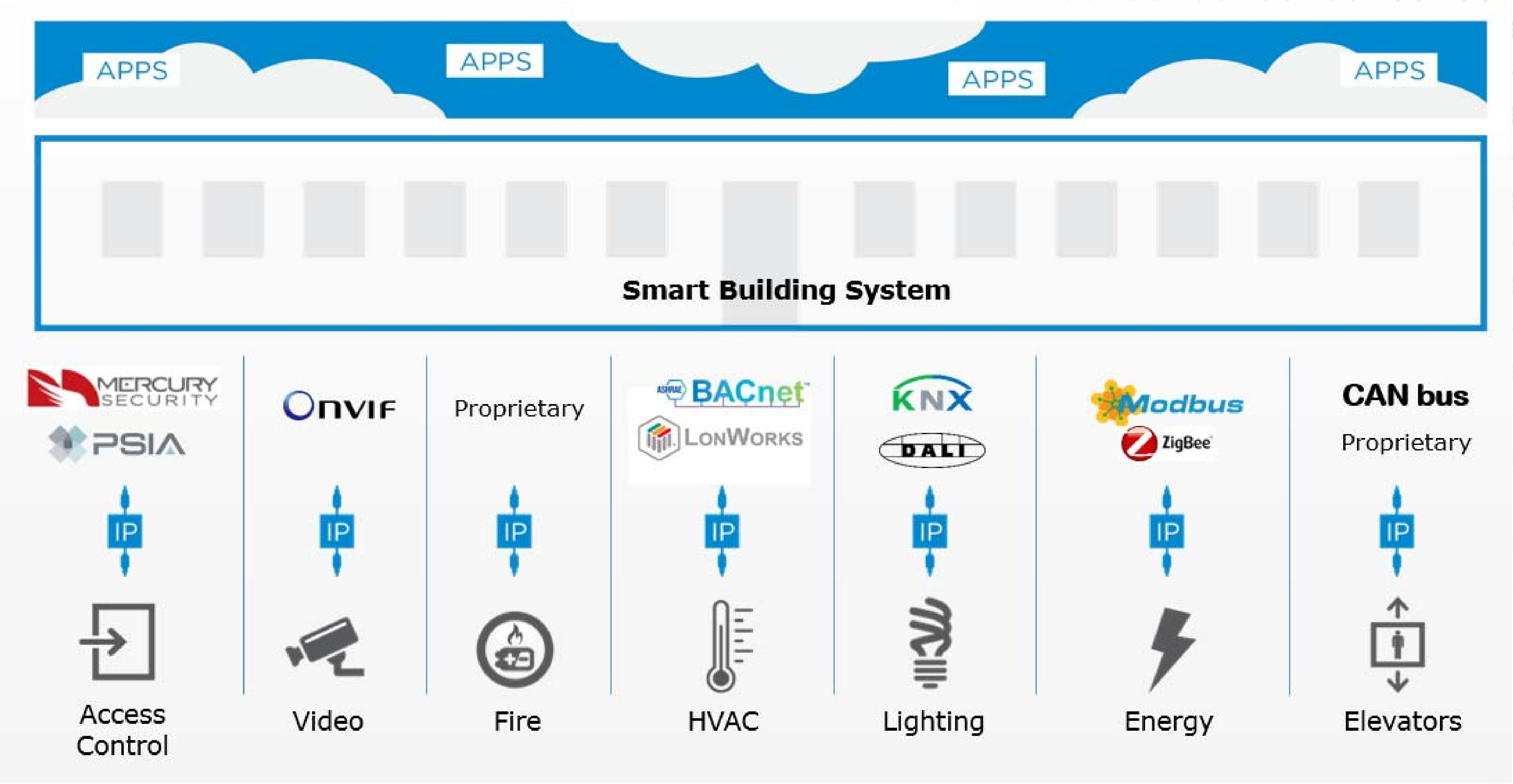
by Virginia Harrison and Jose Pagliery @CNNTech

Hackers Breach Dunkin’ Donuts Accounts in Credential Stuffing Attack

US Banks Targeted with Trickbot Trojan

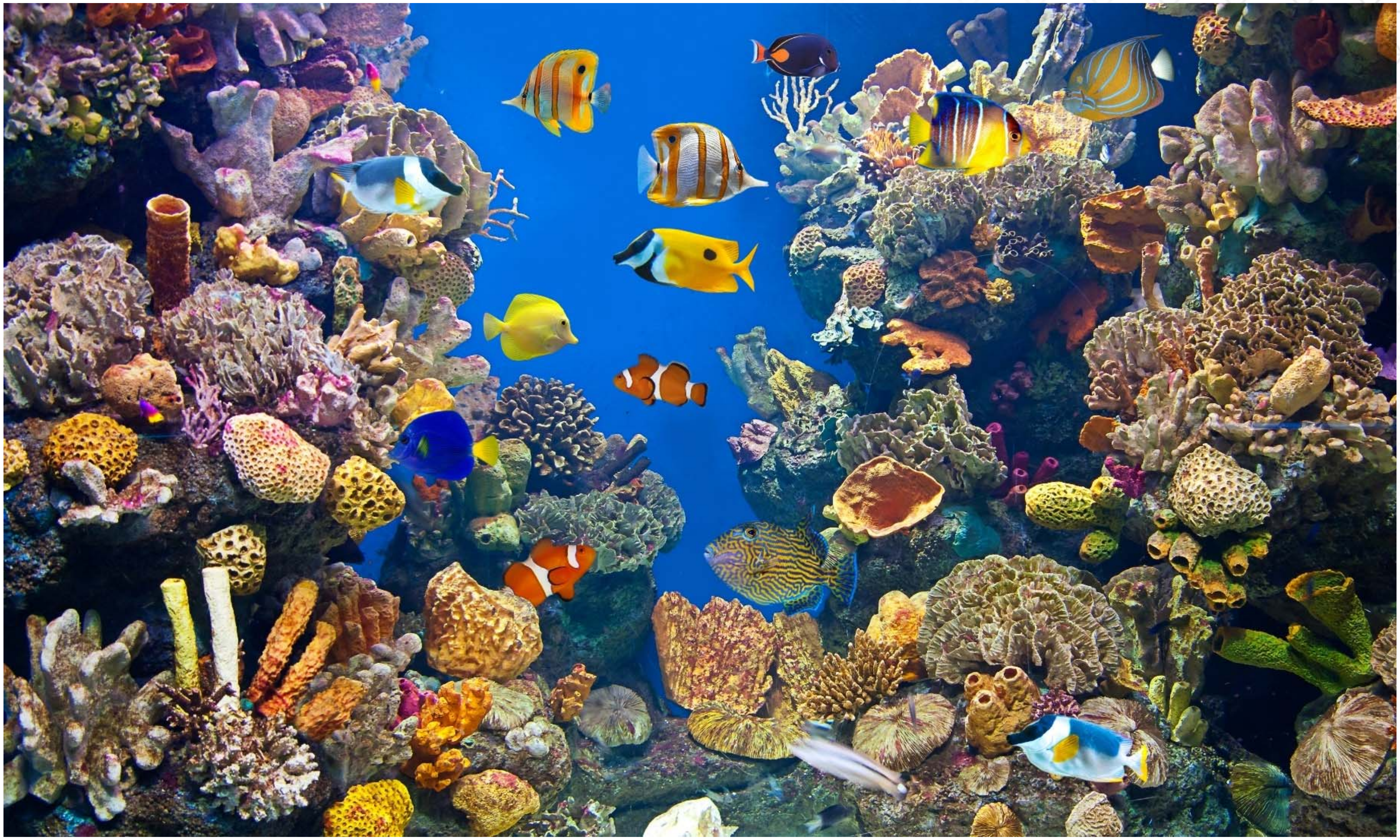
TRIDIUM

The Evolution of Intelligent Buildings



TRIDIUM

The Impending Edge Cyber Storm

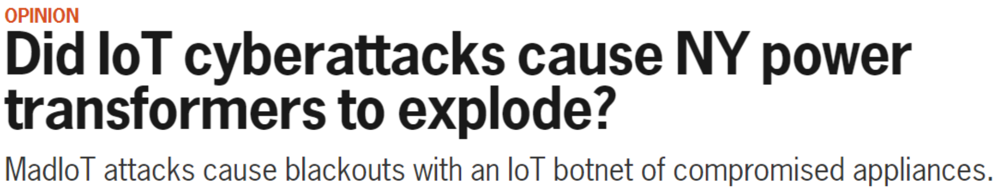


TRIDIUM

Agenda

- Understanding the Threats
- Defending Against the Threats
- Best Practices

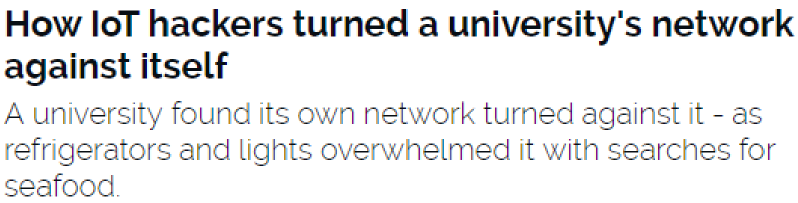
The Cyber-Physical Appeal to Hackers



OPINION

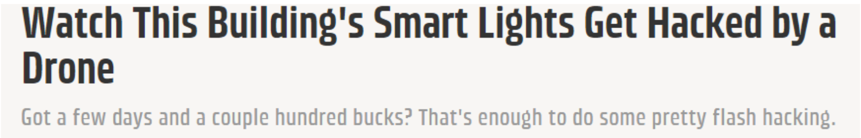
Did IoT cyberattacks cause NY power transformers to explode?

MadIoT attacks cause blackouts with an IoT botnet of compromised appliances.



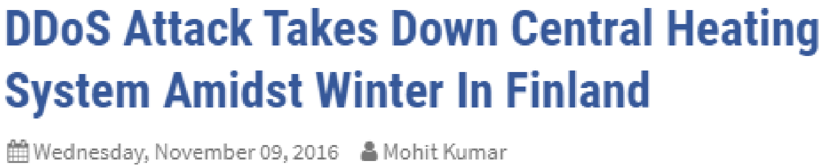
How IoT hackers turned a university's network against itself

A university found its own network turned against it - as refrigerators and lights overwhelmed it with searches for seafood.



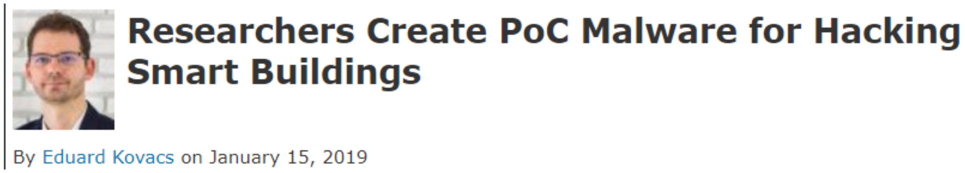
Watch This Building's Smart Lights Get Hacked by a Drone

Got a few days and a couple hundred bucks? That's enough to do some pretty flash hacking.



DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

Wednesday, November 09, 2016 Mohit Kumar



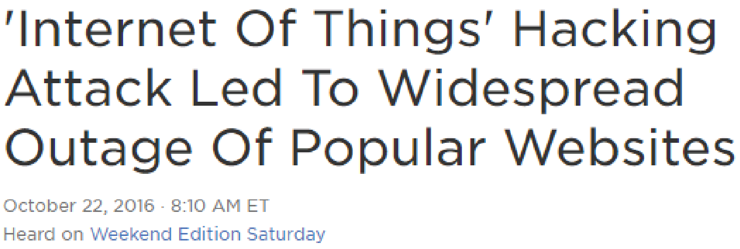
Researchers Create PoC Malware for Hacking Smart Buildings

By Eduard Kovacs on January 15, 2019

Tucson digital traffic sign hacked, July 2015

#internetOfthingsIWantToHack

> *“If your industrial control system is connected to the Internet, it has almost a 100 percent guarantee to be hacked the first day.”*
>
> — E. Kaspersky, founder, Kaspersky Lab



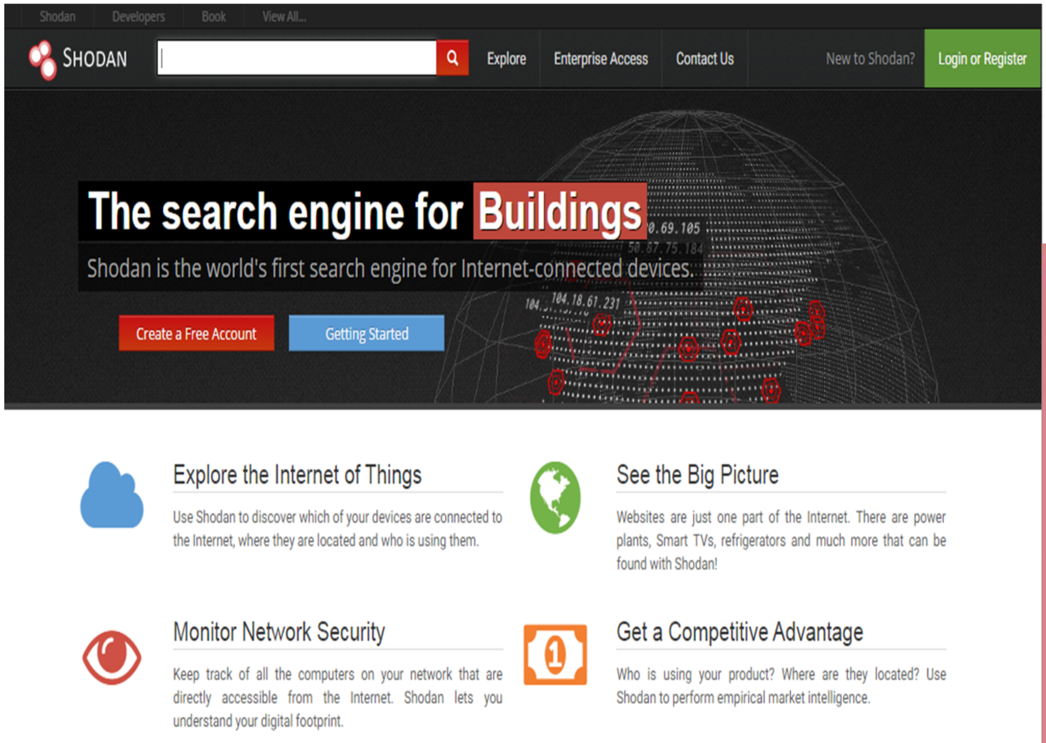
'Internet Of Things' Hacking Attack Led To Widespread Outage Of Popular Websites

October 22, 2016 · 8:10 AM ET

Heard on Weekend Edition Saturday

Shodan and Other “Hacker Friendly” Sites

They can find you…



The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

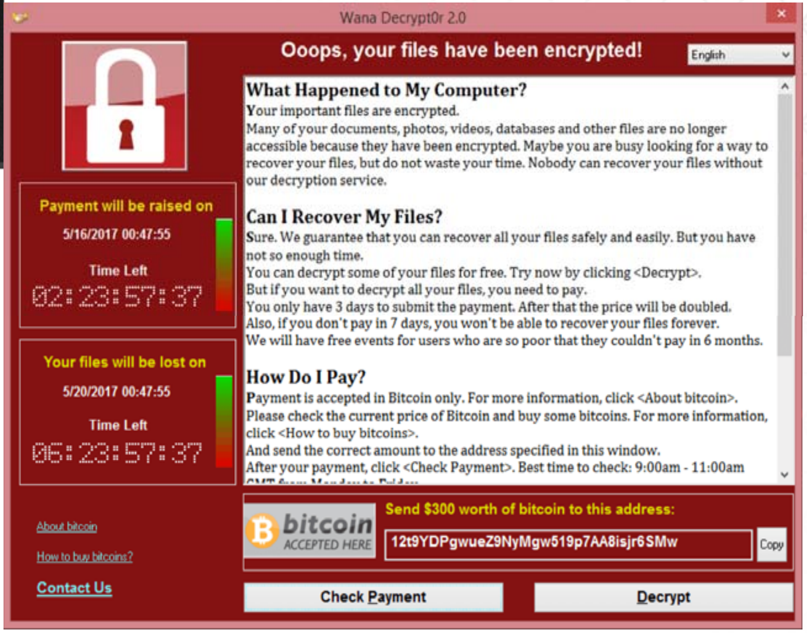
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

And ruin your day.



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

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.

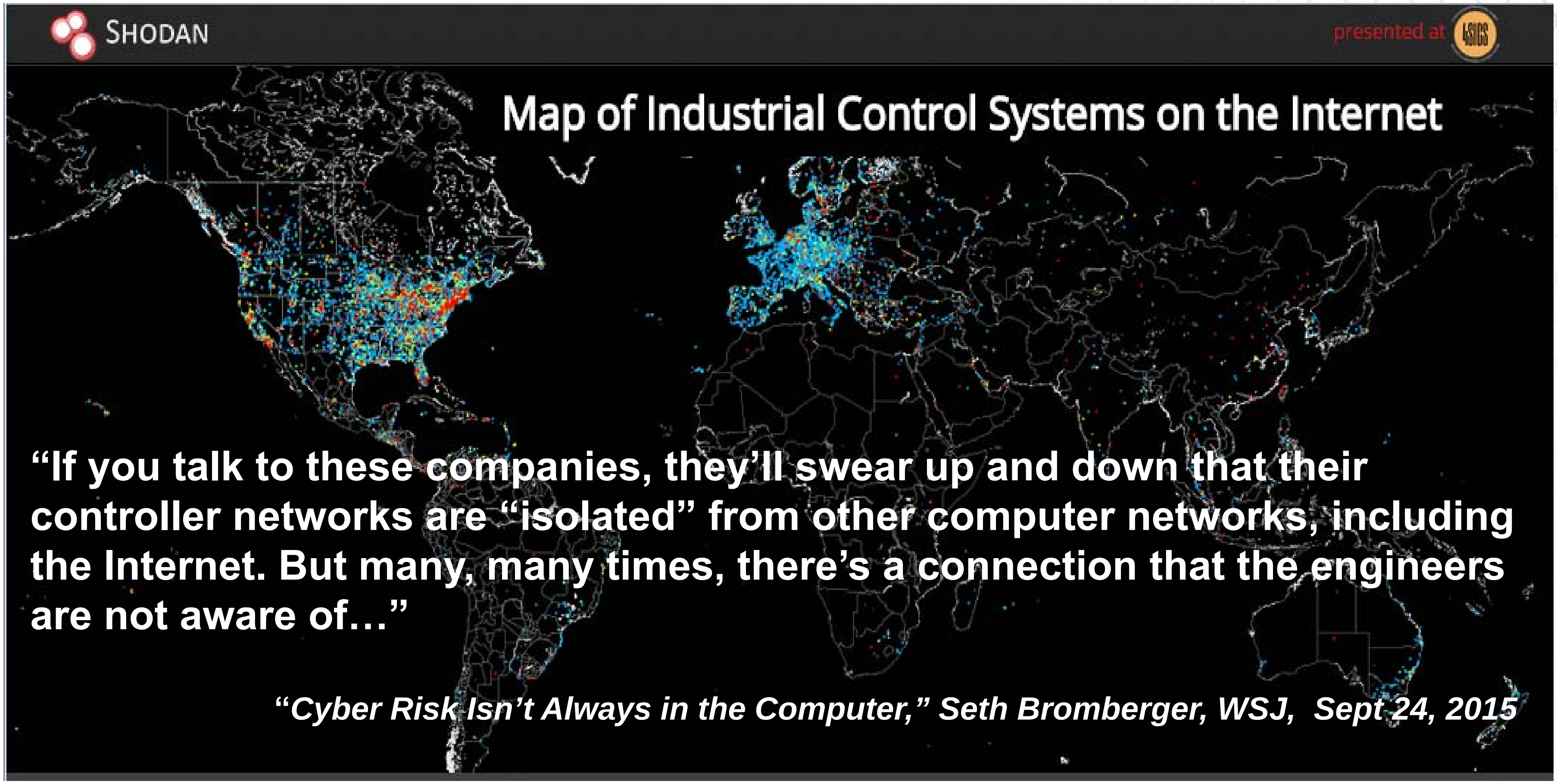
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

TRIDIUM

Control Systems Exposed



"If you talk to these companies, they'll swear up and down that their controller networks are "isolated" from other computer networks, including the Internet. But many, many times, there's a connection that the engineers are not aware of…"

"Cyber Risk Isn't Always in the Computer," Seth Bromberger, WSJ, Sept 24, 2015

Defending Against the Threats: Organizational Best Practices

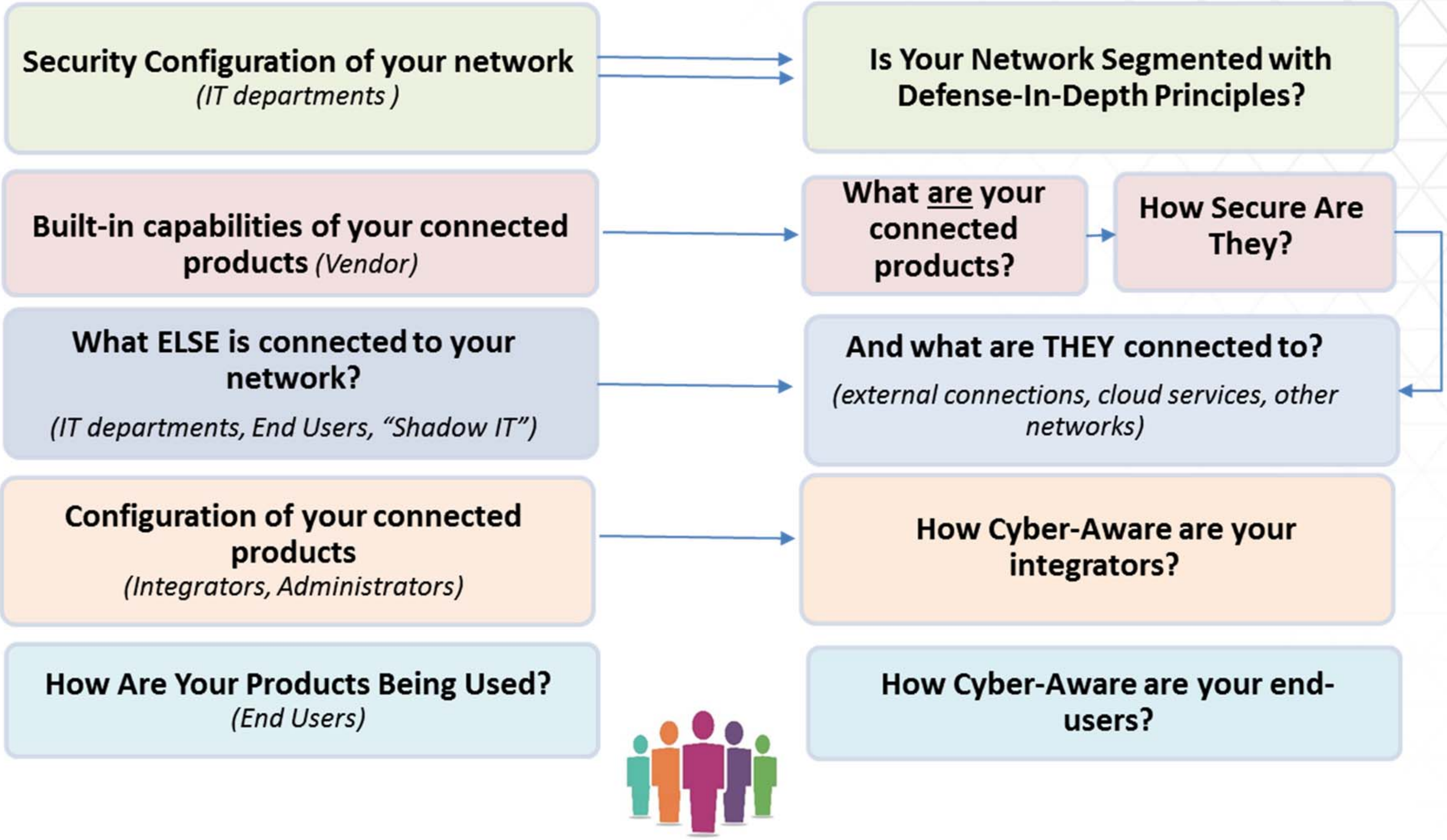
TRIDIUM

People, Processes & Technology

- Security isn't just an "IT thing"
- Policies and procedures are critical
  - Patch management
  - Proper use of IT systems
  - Proper use of building control systems
  - Procedures for incident response
- Communicate: Make sure users understand/respect the cyber threat and follow organizational security policies
- Educate: Teach them how to follow the correct procedures
- Enforce: Make sure everyone knows that Cybersecurity is a priority from the top down in your organization & enforce good behavior through technical controls where possible.

Policies
Procedures
User awareness
Best practices

An Organizational, Holistic View



Security Configuration of your network *(IT departments)*

Is Your Network Segmented with Defense-In-Depth Principles?

Built-in capabilities of your connected products *(Vendor)*

What are your connected products?

How Secure Are They?

What ELSE is connected to your network? *(IT departments, End Users, “Shadow IT”)*

And what are THEY connected to? *(external connections, cloud services, other networks)*

Configuration of your connected products *(Integrators, Administrators)*

How Cyber-Aware are your integrators?

How Are Your Products Being Used? *(End Users)*

How Cyber-Aware are your end-users?

If you think *technology* can solve your security problems, then you don't understand the *problems* and you don't understand the *technology*. *-Bruce Schneier*

Who’s Involved in Security?

Product Supplier (PS)

Integration Provider (IP)

Asset Owner (AO)

Asset Operator (AOP)

Maintenance Provider (MP)

Service Provider (SP)

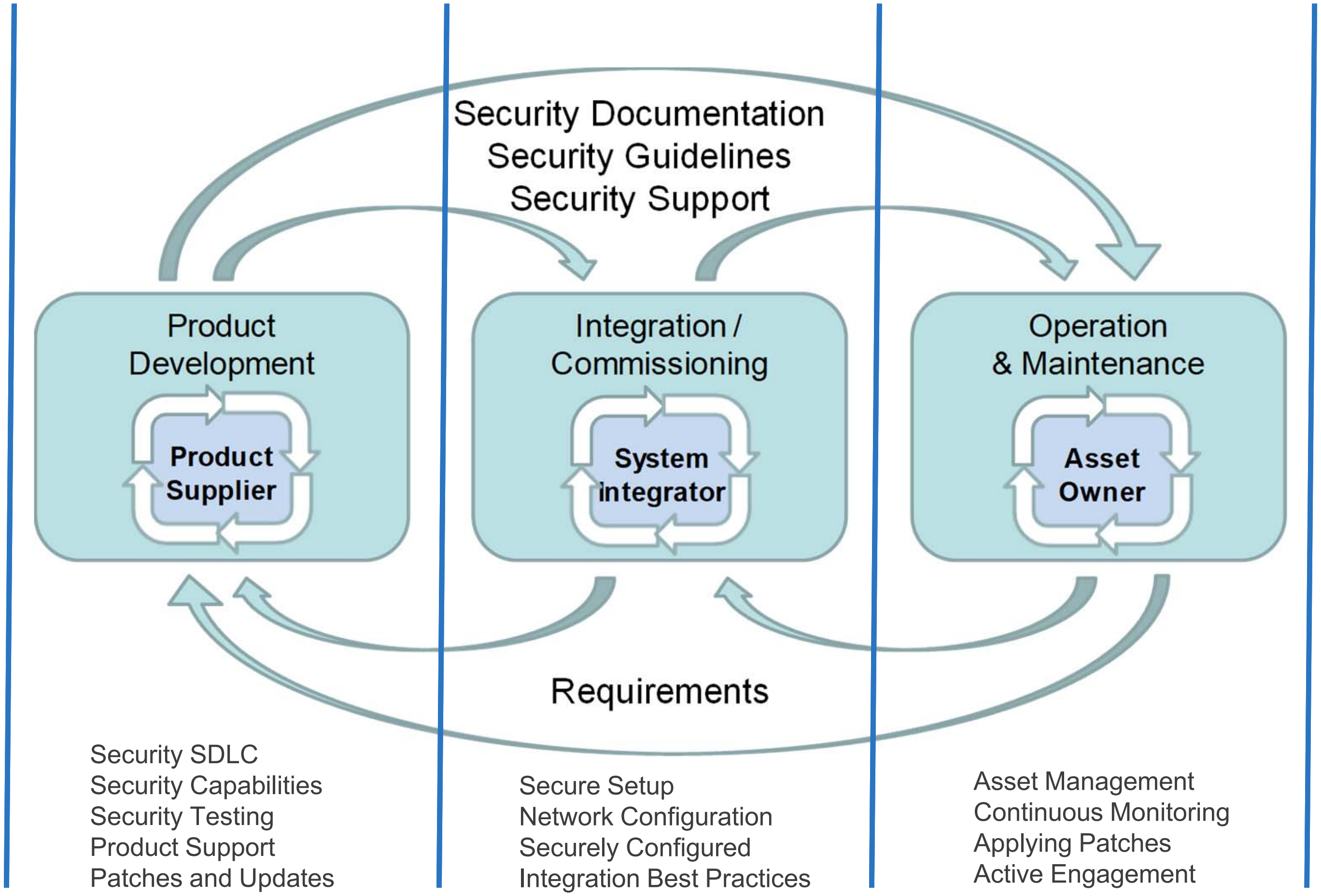
System Operator (SO)

Regulatory Authority (RA)

Compliance Authority (CA)

Principal Roles (from ISA 62443-1-1)

Lifecycles and Swim Lanes



Security Documentation
Security Guidelines
Security Support

Product Development

Product Supplier

Integration / Commissioning

System Integrator

Operation & Maintenance

Asset Owner

Requirements

Security SDLC
Security Capabilities
Security Testing
Product Support
Patches and Updates

Secure Setup
Network Configuration
Securely Configured
Integration Best Practices

Asset Management
Continuous Monitoring
Applying Patches
Active Engagement

OT and IT Need to Work Together

TRIDIUM

Periodic Risk Assessments – What are your assets & risks?

- Understand your organization's appetite for risk & determine a risk threshold, re CVSS score
- Identify the electronic assets you wish to protect & document security requirements re: confidentiality, integrity, availability
- Engage an independent security team to assess threats and potential vulnerabilities for your network & those assets
- Follow up with action items
- Do this on a periodic basis – assets change, requirements change.

TRIDIUM

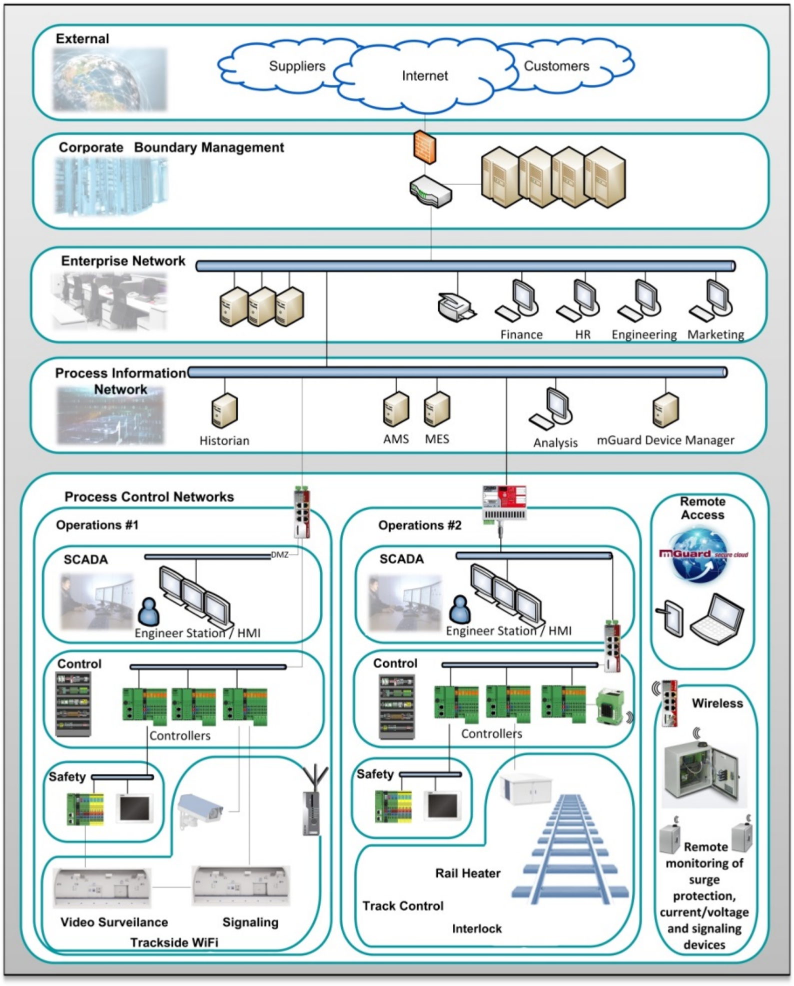
Product Manufacturers –

Enforce Good Behavior through Technology Controls

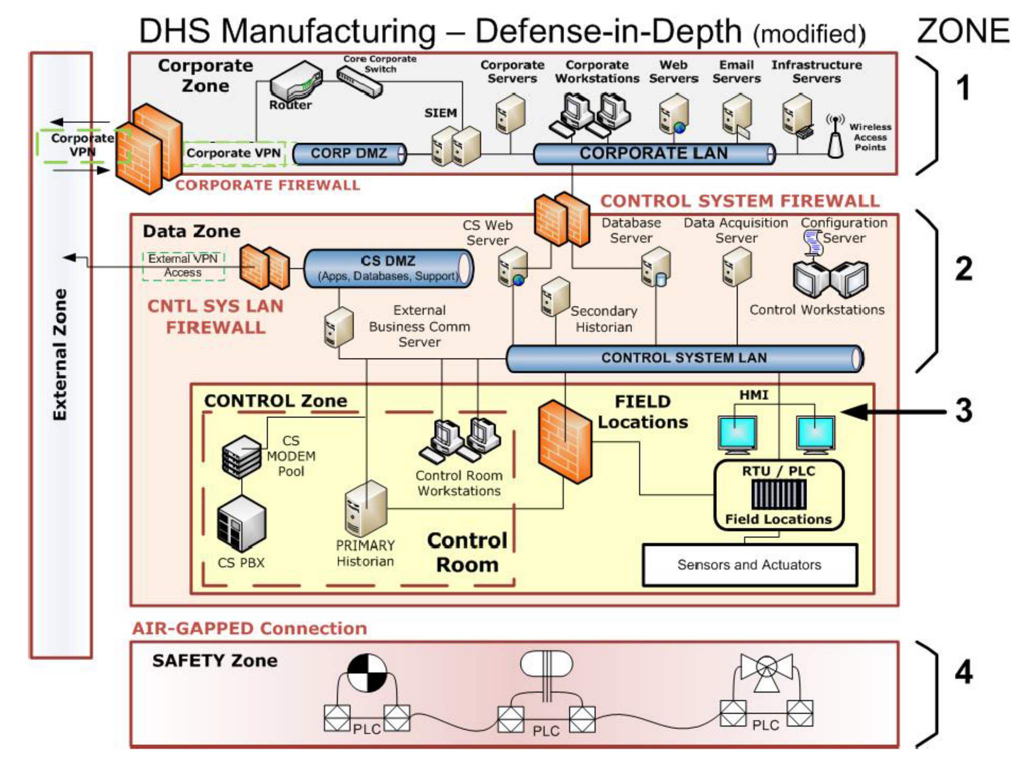
One of our Key Cybersecurity principles at Tridium is to **make security easier for end-users:**

- **“Secure by Default”**
  - Forcing default credential changes immediately upon commissioning
  - Strongest authentication mechanism by default
  - Enforcement of strong passwords
  - Encrypted communications (FoXS and HTTPS)
- **Role-based Access Control**
  - Make user management easier with Role-Based Abstractions (vs. fine-grained permissions)
- **Do the Right Thing By Default, regardless of configuration:**
  - Encryption of Sensitive Information at Rest
  - Sandboxing of third-party code
  - Digitally-signed code, validated for integrity and source at run-time
  - Secure Boot
- **Customer Education**
  - Security Guides, Hardening Guides
  - Podcasts, Whitepapers, Presentations on Security Best Practices

Networking: Defense-In-Depth



From Rashid, Coladonato, Schaeffer, *"Maintaining Data Integrity from Creation to Collection to Consumption in an Infrastructure Environment"*



Patch Management is Critical

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

https://www.us-cert.gov

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

https://ics-cert.us-cert.gov/

- Organizations such as US-CERT and ICS-CERT provide a great service internationally, reporting vulnerabilities in hardware and software
- Many advisories affect millions of devices
- Vendors release security patches and updates, and these organizations point you to where to get them
- *Any* unpatched system on your network can be an attacker’s avenue into your organization

TIP: NIST SP 800-40r3 Provides Guidance for Patch Management for Your Organization that can be helpful for all building systems (control systems, edge devices, etc.) .

Protection against Ransomware

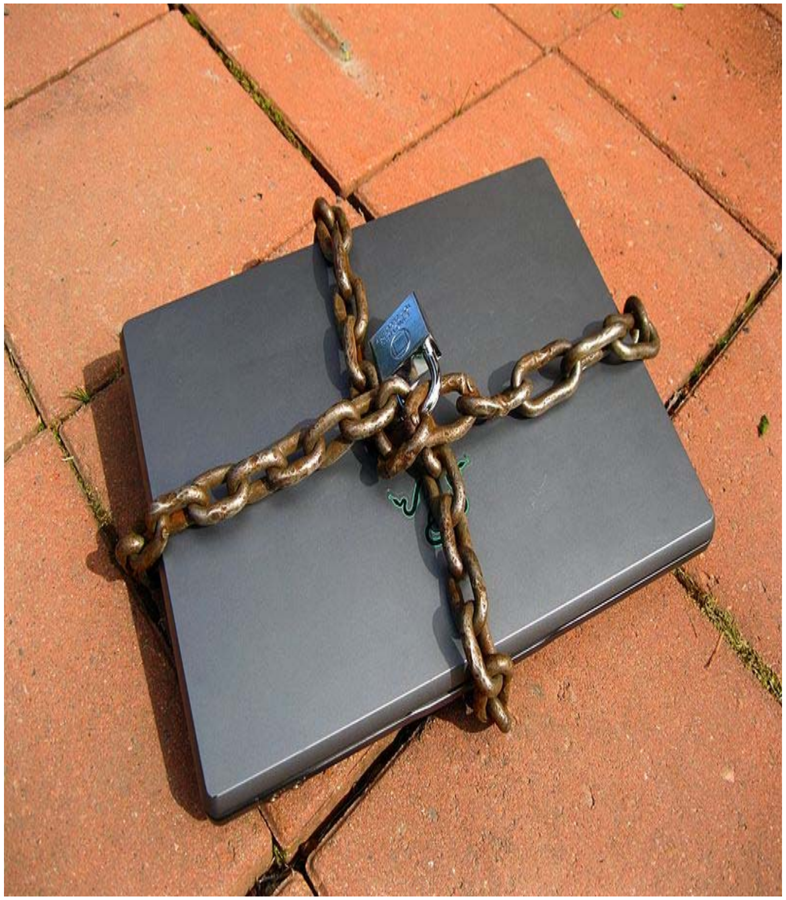


*Image – Santeri Viinamake, Creative Commons

1. Educate your people on the safe use of IT assets and the dangers of ransomware
2. Use anti-virus software on your systems and keep them up to date
3. Do periodic, scheduled backups of your systems
4. If you have a supervisory system (ex: Niagara Supervisor), treat it as mission-critical infrastructure, which means it shouldn't be a "web surfing" or "email checking" machine

Wireless Communications

- Vulnerabilities with Wireless Protocols & Insecure Configuration of Wireless Protocols have brought significant impacts and challenges
  - Notoriously weak Wired Equivalency Privacy (WEP) & its quick attempt at a replacement, WiFi Protected Access (WPA)
  - WPA2 and KRACK (2017/2018)
  - Insecure Configurations
- Countermeasures
  - Complementing Wifi protocols with other security protocols (ex: JACE8000 – all communications encrypted with TLS, over an encrypted Wifi tunnel (if one fails, confidentiality still exists)
  - Complementing Wifi protocols with other security infrastructure (802.1x, RADIUS, etc.)
  - Or.. Stick to wired..

Cryptography / Encryption Standards

- Symmetric (Secret Key) Crypto – used for encrypting data
- Asymmetric (Private/Public Key) Cryptography – very large keys, used for key exchange of symmetric keys
- Ciphers are broken every day & become obsolete – check!
  - What is effective today may not be tomorrow.
  - NIST recommends AES 256 (Symmetric) & RSA 2048 (Asymm)
- Ciphers are best when Perfect Forward Secrecy is used
- TLS can be used for providing a lot of goodness:
  - provides confidentiality & integrity
  - can prevent man-in-the middle and many other attacks
  - can provide non-repudiated assurance of both parties when using mutually-authentication (2-way TLS) with digital certificates
  - Watch for weak ciphers & downgrade possibilities where weaknesses can be exploited
  - Watch for implementations with known vulnerabilities.
- VPN tunnels (using various protocols – IPSEC) can be very effective, and much like TLS, watch your implementations, ciphers.

People forget Physical Security

- Even if you have great network security, secure products, it really doesn't matter if someone can gain physical access to your control systems and edge devices.
- Remember that many successful cyberattacks can also begin with a physical one
- Remember that malware can also be introduced through USB drives

People Are Often the Weakest Link

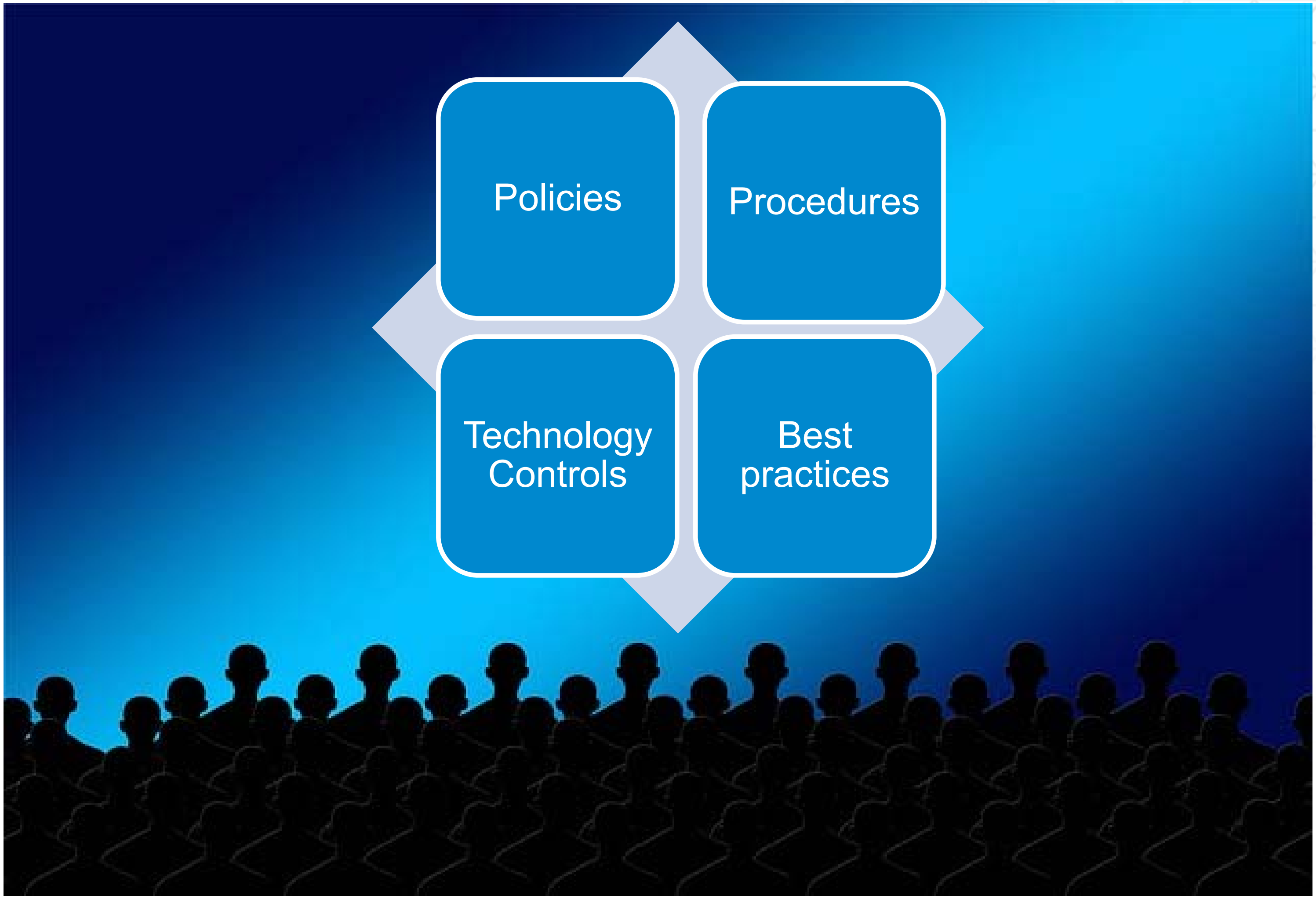
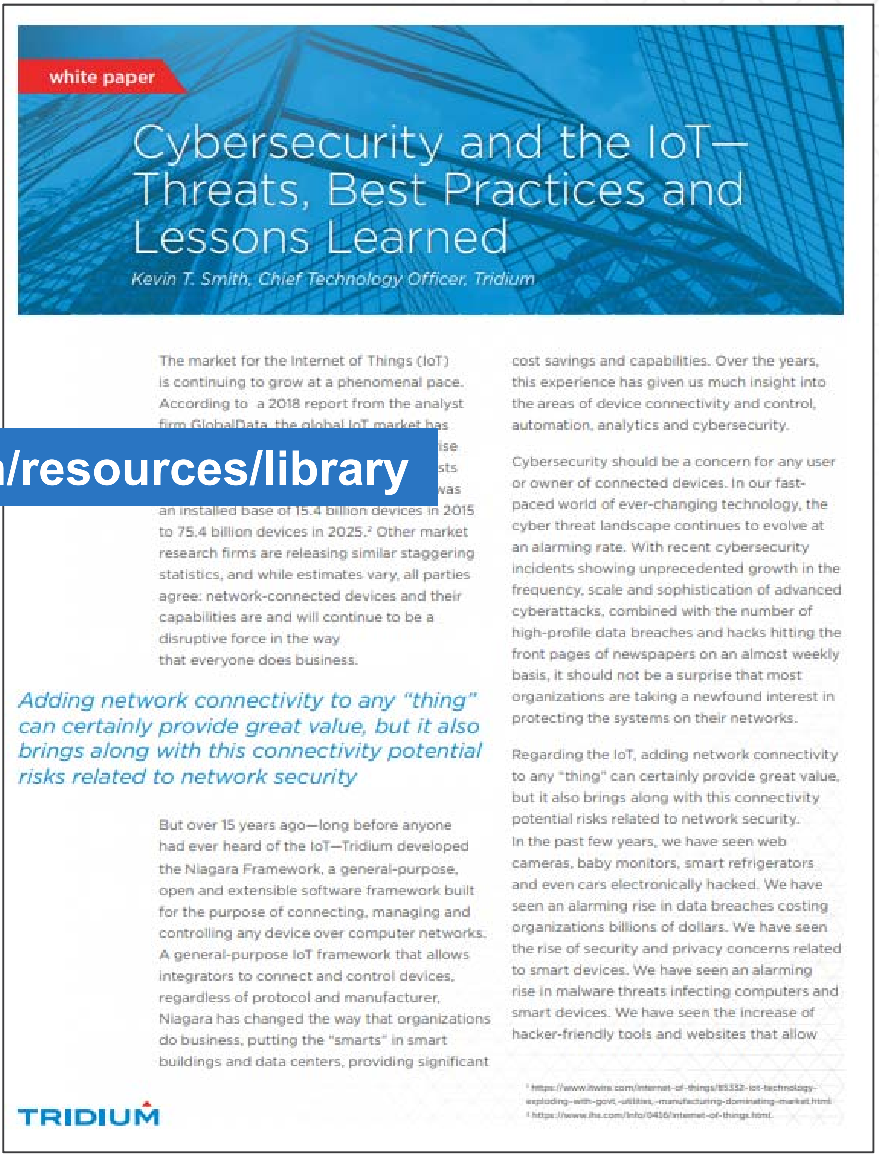


Image: Pixabay.com, available through Creative Commons CCO.

People are the most critical aspect of your building's security.

Resources	Where to find it
"Maintaining Data Integrity from Creation to Collection to Consumption in an Infrastructure Environment" by H. Rashid, M. Coladonato, & D. Schaeffer	http://rd.phoenixcon.com/aspapps/GWIS/splashproc/mediaDLs/287/Maintaining_Data_Integrity_from_Creation_to_Collection_to_Consumption_Final.pdf
NIST SP 800-50: *Building an Information Technology Security Awareness and Training Program*	http://www.nist.gov/
NIST SP 800-82: *Guide to Industrial Control Systems (ICS) Security*	http://www.nist.gov/
NIST SP 800-61: *Computer Incident Security Handling Guide*	http://www.nist.gov/
ICS CERT – *"Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies"*	https://ics-cert.us-cert.gov
ICS-CERT – *"Developing an Industrial Control Systems Cybersecurity Incident Response Plan"*	https://ics-cert.us-cert.gov
ICS-CERT – *"Remote Access for Industrial Control Systems"*	https://ics-cert.us-cert.gov
Niagara 4 & AX Hardening Guides	https://www.tridium.com/en/resources/library
Tridium Security Bulletins	https://www.tridium.com/en/resources/library
Niagara Smart Building Guide Specification	https://www.tridium.com/en/resources/library

Additional resources



white paper

Cybersecurity and the IoT—Threats, Best Practices and Lessons Learned

Kevin T. Smith, Chief Technology Officer, Tridium

The market for the Internet of Things (IoT) is continuing to grow at a phenomenal pace. According to a 2018 report from the analyst firm GlobalData, the global IoT market has
ise
sts
was
an installed base of 15.4 billion devices in 2015 to 75.4 billion devices in 2025.[2] Other market research firms are releasing similar staggering statistics, and while estimates vary, all parties agree: network-connected devices and their capabilities are and will continue to be a disruptive force in the way that everyone does business.

Adding network connectivity to any "thing" can certainly provide great value, but it also brings along with this connectivity potential risks related to network security

But over 15 years ago—long before anyone had ever heard of the IoT—Tridium developed the Niagara Framework, a general-purpose, open and extensible software framework built for the purpose of connecting, managing and controlling any device over computer networks. A general-purpose IoT framework that allows integrators to connect and control devices, regardless of protocol and manufacturer, Niagara has changed the way that organizations do business, putting the "smarts" in smart buildings and data centers, providing significant cost savings and capabilities. Over the years, this experience has given us much insight into the areas of device connectivity and control, automation, analytics and cybersecurity.

Cybersecurity should be a concern for any user or owner of connected devices. In our fast-paced world of ever-changing technology, the cyber threat landscape continues to evolve at an alarming rate. With recent cybersecurity incidents showing unprecedented growth in the frequency, scale and sophistication of advanced cyberattacks, combined with the number of high-profile data breaches and hacks hitting the front pages of newspapers on an almost weekly basis, it should not be a surprise that most organizations are taking a newfound interest in protecting the systems on their networks.

Regarding the IoT, adding network connectivity to any "thing" can certainly provide great value, but it also brings along with this connectivity potential risks related to network security. In the past few years, we have seen web cameras, baby monitors, smart refrigerators and even cars electronically hacked. We have seen an alarming rise in data breaches costing organizations billions of dollars. We have seen the rise of security and privacy concerns related to smart devices. We have seen an alarming rise in malware threats infecting computers and smart devices. We have seen the increase of hacker-friendly tools and websites that allow

[1] https://www.itwire.com/internet-of-things/85332-iot-technology-exploding-with-govt,-utilities,-manufacturing-dominating-market.html
[2] https://www.ihs.com/info/0416/internet-of-things.html

https://Tridium.com/en/resources/library

Thank You!

Kevin T. Smith, CISSP, CSSLP

ksmith@tridium.com

TRIDIUM