ASHB
Association for Smarter Homes & Buildings

Intelligent Buildings Council (IBC)

Webinar/Meeting will commence 12:05pm ET

Thursday, February 27, 2025 | 12 NOON – 1:30 PM (ET)

IBC Chair: Bob Allan (NAVCO Inc.)

Vice-Chair: Harsha Chandrashekar (Honeywell International Inc.)

Vice-Chair: Robert Lane (Robert H. Lane and Associates Inc.)

Vice-Chair: Chris Larry (exp US Services Inc.)

Connect to what's next™
www.ashb.com

Agenda
Marta Klopotowska (ASHB)

1. Call to Order, Welcome, Introductions, About IBC
2. Administrative
3. Research Update
4. Keynote: **Cybersecurity Best Practices – Safeguarding Your Network and Building Systems** - Brad Bonfiglio, Schneider Electric
5. ASHB Podcast
6. ASHB Whitepapers & Research Library
7. ASHB Journal
8. New Business
9. Announcements
10. Adjournment

1. Call to Order, Welcome, Introductions, About the IBC
Bob Allan (NAVCO, Inc.)

IBC Chair
Bob Allan
Vice President of Sales,
East Region
NAVCO, Inc.

NAVCO

IBC Vice-Chair
Harsha Chandrashekar
Product Approvals &
Regulatory Leader
Honeywell International

Honeywell

IBC Vice-Chair
Robert Lane
President & Managing
Partner, Robert H. Lane
and Associates Inc.

Lane
TRUSTED ADVISORS

IBC Vice-Chair
Chris Larry
Director of Energy
Engineering
Exp US Services Inc.

exp.

The ASHB Intelligent Buildings Council works to strengthen the large building automation industry through innovative technology-driven research projects. The Council was established in 2001 by ASHB to specifically review opportunities, take strategic action, and monitor initiatives that relate to integrated systems and automation in the large building sector. The Council's projects promote the next generation of smart building technologies and incorporate a holistic approach that optimizes building performance and savings. www.ashb.com/ibc ,

2. Administrative

Bob Allan (NAVCO, Inc.)

Approval of IBC Minutes
November 7, 2024

www.ashb.com/ibc

3. Research Update
Harsha Chandrashekar (Honeywell International Inc.)

ASHB
Association for Smarter Homes & Buildings

2025 Smart Building
Trends & Technology Adoption

LANDMARK RESEARCH PROJECT

BELIMO DAIKIN DELTA DISTECH CONTROLS
DWYEROMEGA EBTRON a measurable difference! Functional Devices, Inc. Honeywell Johnson Controls
Schneider Electric SIEMENS Southwire TRANE

2025 IBC Landmark Research
Smart Building Trends & Technology Adoption

Funders

BELIMO DAIKIN DELTA DISTECH CONTROLS

DWYEROMEGA EBTRON a measurable difference! Functional Devices, Inc. Honeywell Johnson Controls

Schneider Electric SIEMENS Southwire TRANE

Contact admin@ashb.com to obtain research findings and to join as a funder.

3. Research Update
Greg Walker (ASHB)

Annual BACS Market Sizing
North America

Automated Logic

Carrier

BELIMO

Delta Controls

Distech Controls

Honeywell

Johnson Controls

Schneider Electric

SIEMENS

4. Keynote
Robert Lane (Robert H. Lane & Associates Inc.)

Keynote Speaker

Brad Bonfiglio - Global Power & Energy Research Director

Schneider Electric

Cybersecurity Best Practices – Safeguarding Your Network and Building Systems

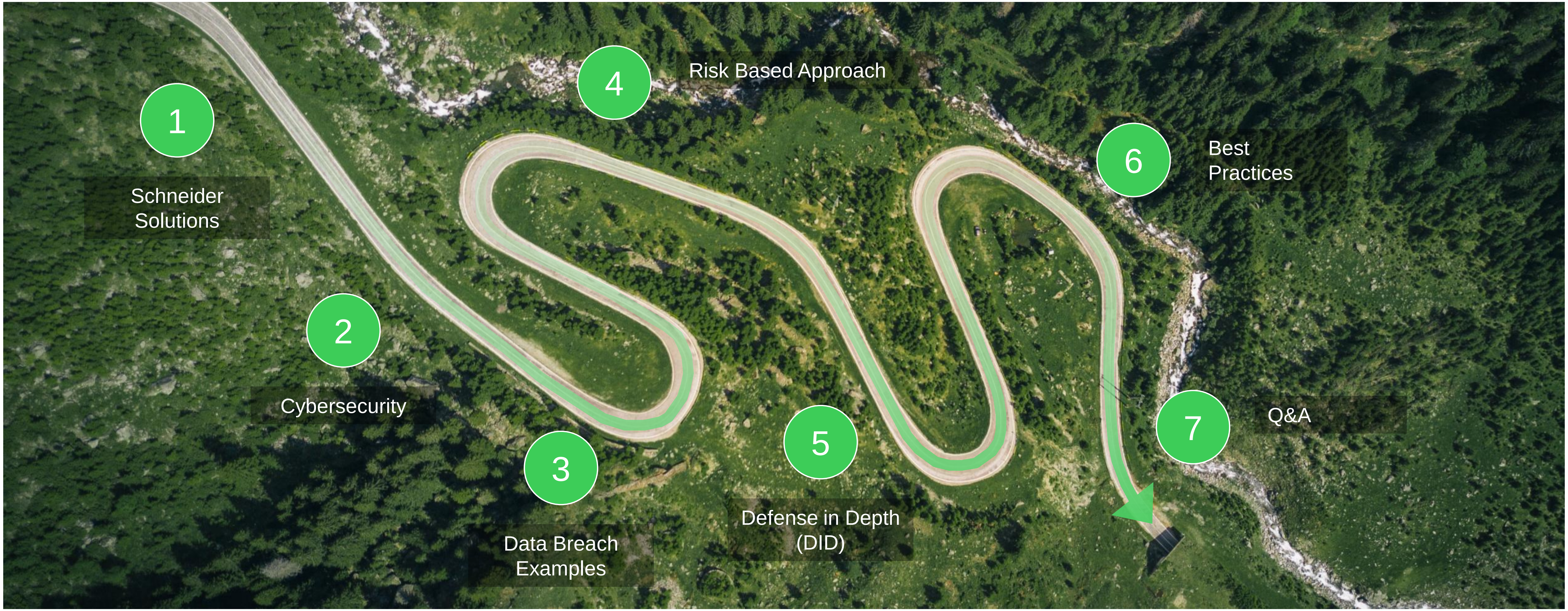
Cybersecurity Best Practices – Safeguarding Your Network and Building Systems

Presented by: Brad.Bonfiglio@se.com

Life Is On | Schneider Electric

Property of Schneider Electric

Cybersecurity journey



1 Schneider Solutions

2 Cybersecurity

3 Data Breach Examples

4 Risk Based Approach

5 Defense in Depth (DID)

6 Best Practices

7 Q&A

TIME

WORLD'S MOST SUSTAINABLE COMPANIES

IN PARTNERSHIP WITH statista

2024

World's most sustainable company is ready to go further, faster

EcoStruxure™
Innovation At Every Level

EcoStruxure Innovation At Every Level Building

SQUARE D™

BARBER COLMAN COMPANY

Wonderware®
by Schneider Electric

APC®
Legendary Reliability™

EcoStruxure Security Expert

AndoverControls
Controlling Tomorrow's World

PowerLogic®
Control the cost, quality and reliability of your utilities

AutoGrid

MGE
UPS SYSTEMS

EcoStruxure Access Expert

t.a.c®

invensys®

AVEVA®

VICONICS Beyond Comfort

VERIS INDUSTRIES™

Planon
Building Connections

RIB
running together

ASCO Power Technologies®

200+ Factory Certified System Integrators

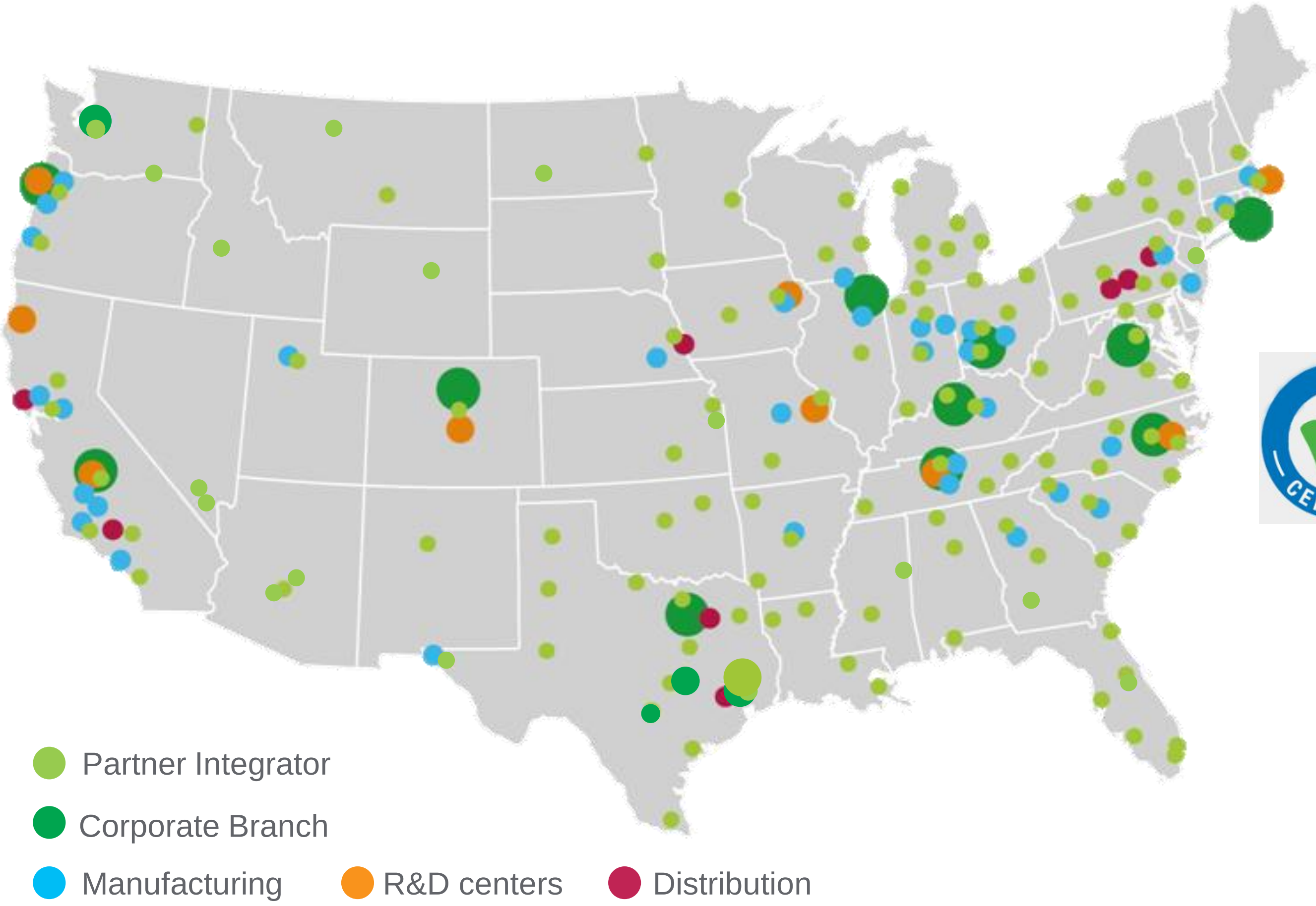
Specialization Certifications

Buildings

Data Center

Healthcare

Life Science



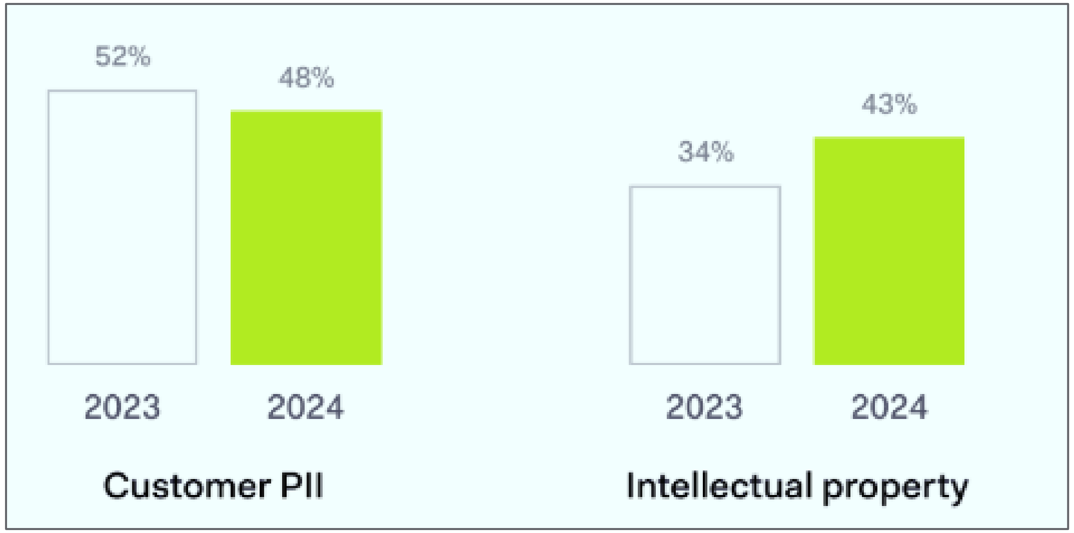
Cybersecurity breaches in building control systems or sensitive data can result in significant regulatory penalties, disrupt core operations, and **damage business reputations**, eroding consumer, employee, and investor trust.

Adopting a new approach to designing and managing intelligent building control systems is key.

Data Breaches Update

2024 was one of the worst years yet on the cybersecurity front.

Average data breach is now cost $4.9M and Ransomware is $5.2M

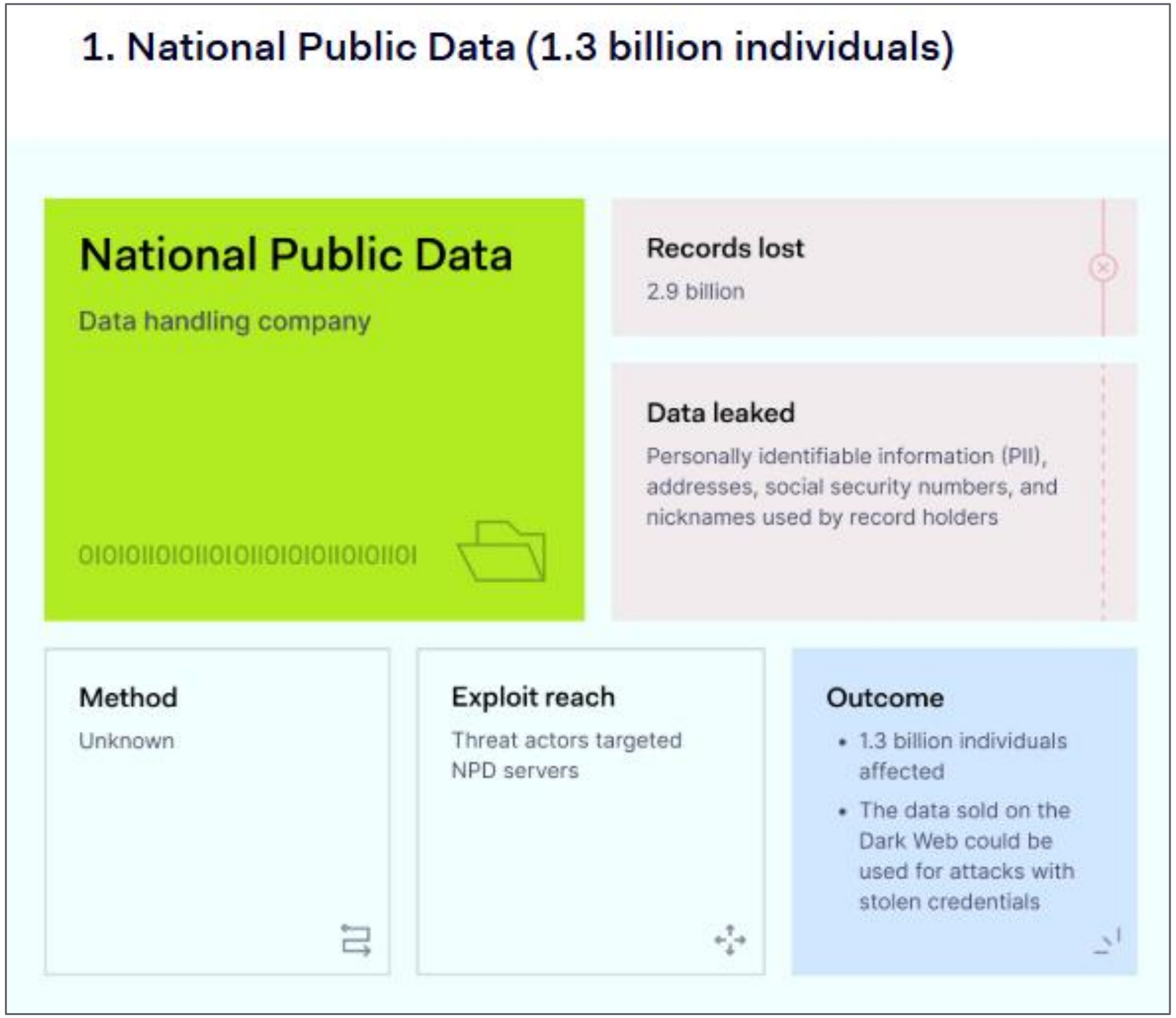


NordLayer Trends & Statistics “Biggest data breaches of 2024” Dec. 16, 2024
https://nordlayer.com/blog/data-breaches-in-2024/

2024 Largest Data Breach

1.3 billion personal addresses, Social Security Numbers, and records.

Method – Unknown



1. National Public Data (1.3 billion individuals)

National Public Data

Data handling company

01010110101101010110101010110101101

Records lost

2.9 billion

Data leaked

Personally identifiable information (PII), addresses, social security numbers, and nicknames used by record holders

Method

Unknown

Exploit reach

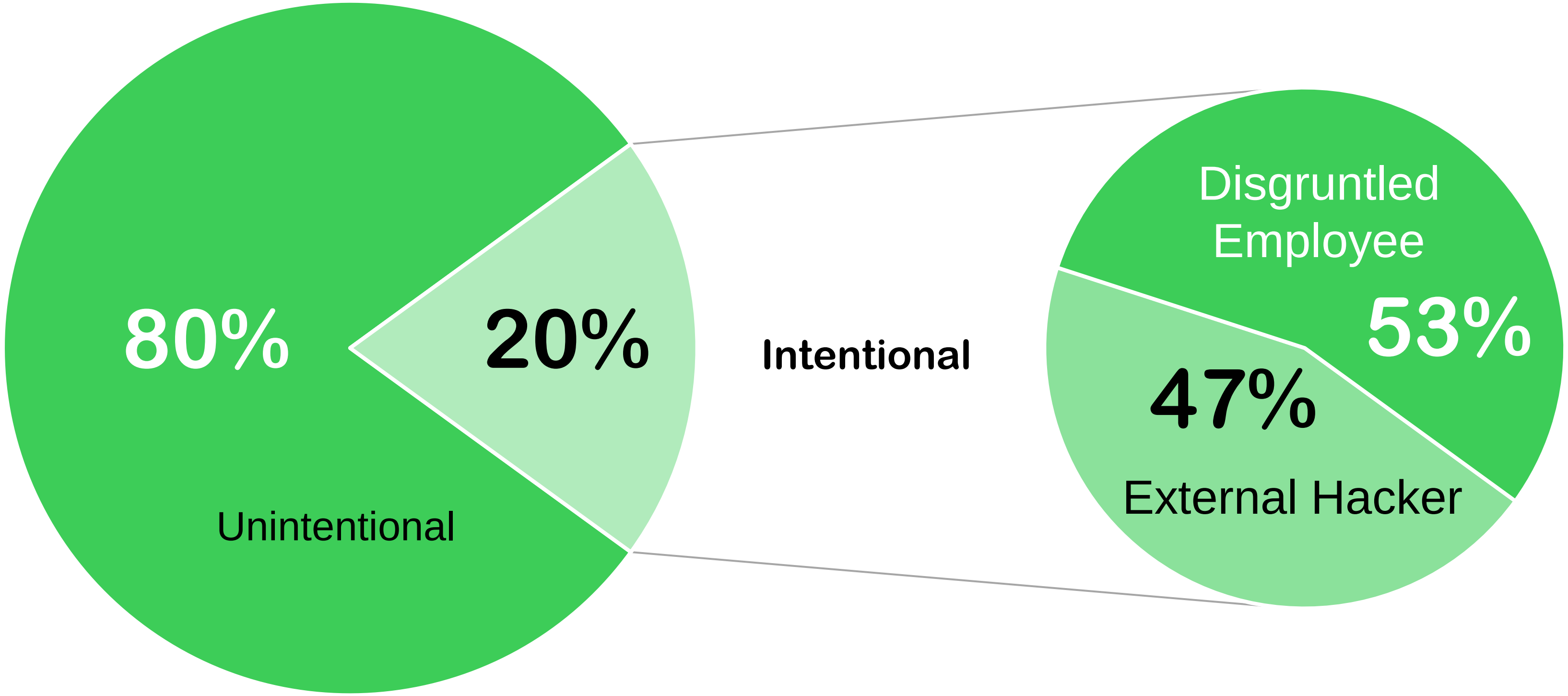
Threat actors targeted NPD servers

Outcome

- 1.3 billion individuals affected
- The data sold on the Dark Web could be used for attacks with stolen credentials

NordLayer Trends & Statistics “Biggest data breaches of 2024” Dec. 16, 2024
https://nordlayer.com/blog/data-breaches-in-2024/

Cybersecurity Incident Types



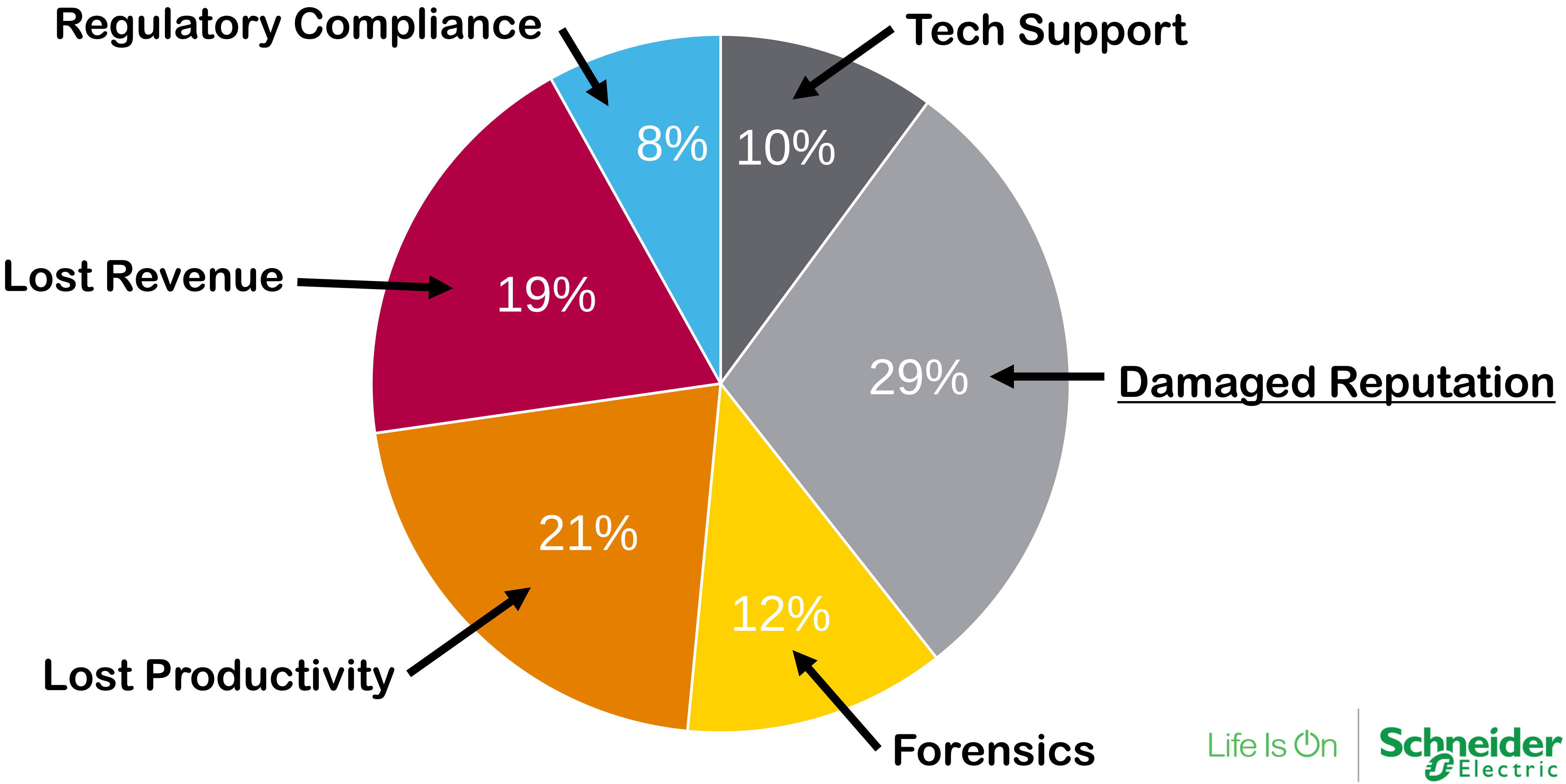
There is a hacker attack every 39 seconds

March 16, 2018 / Cybinet New

- Software or Device Flaw
- Human Error
- Malware

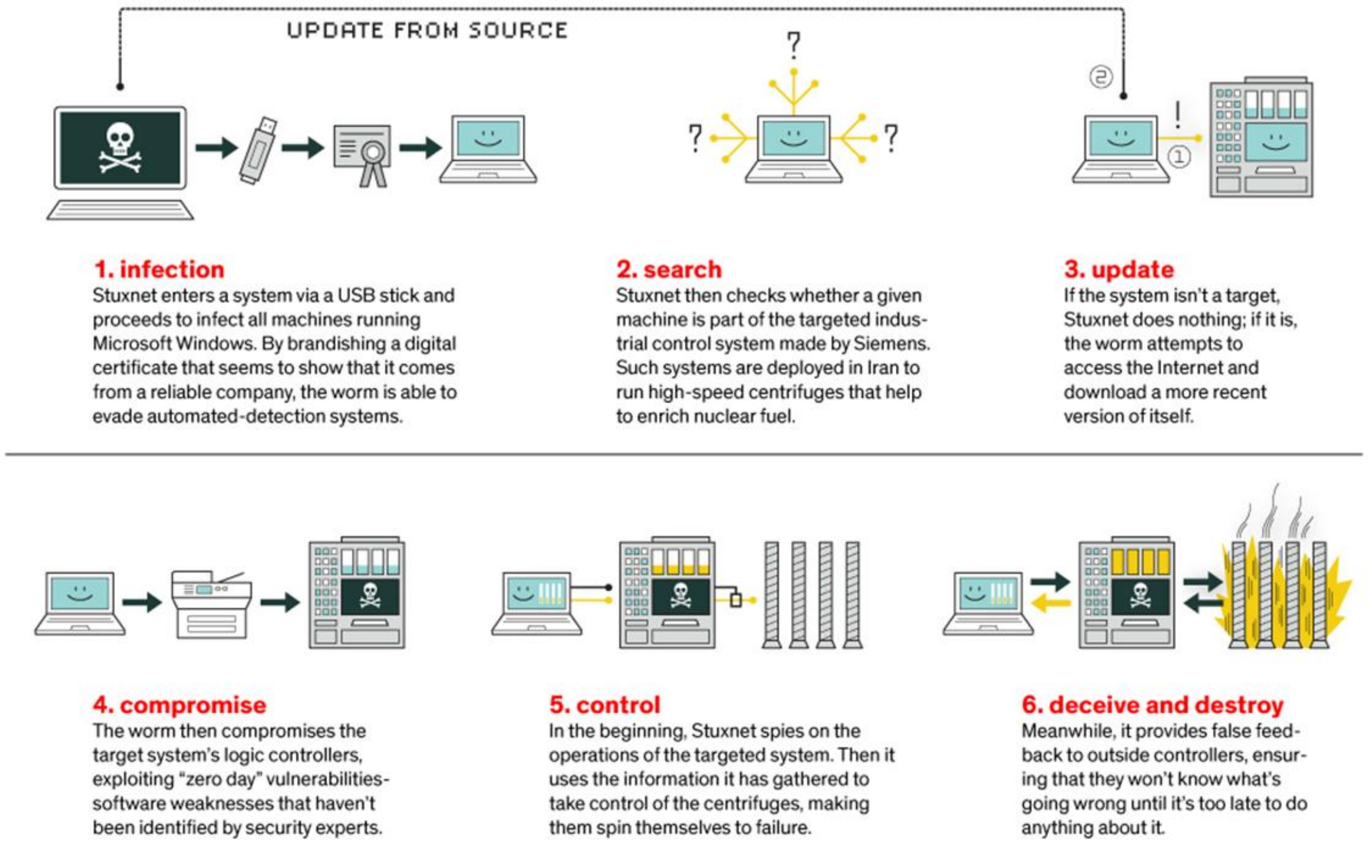
Life Is On | Schneider Electric

Cost Breakdown of a Cyberattack



Where the story begins…Industrial PLCs 2010

June 2010: Discovery of **Stuxnet**,1st worm developed to target automation system (Win PC & PLC). 1/3 of the centrifuges were destroyed. The Iranian nuclear program delayed by >2 years.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

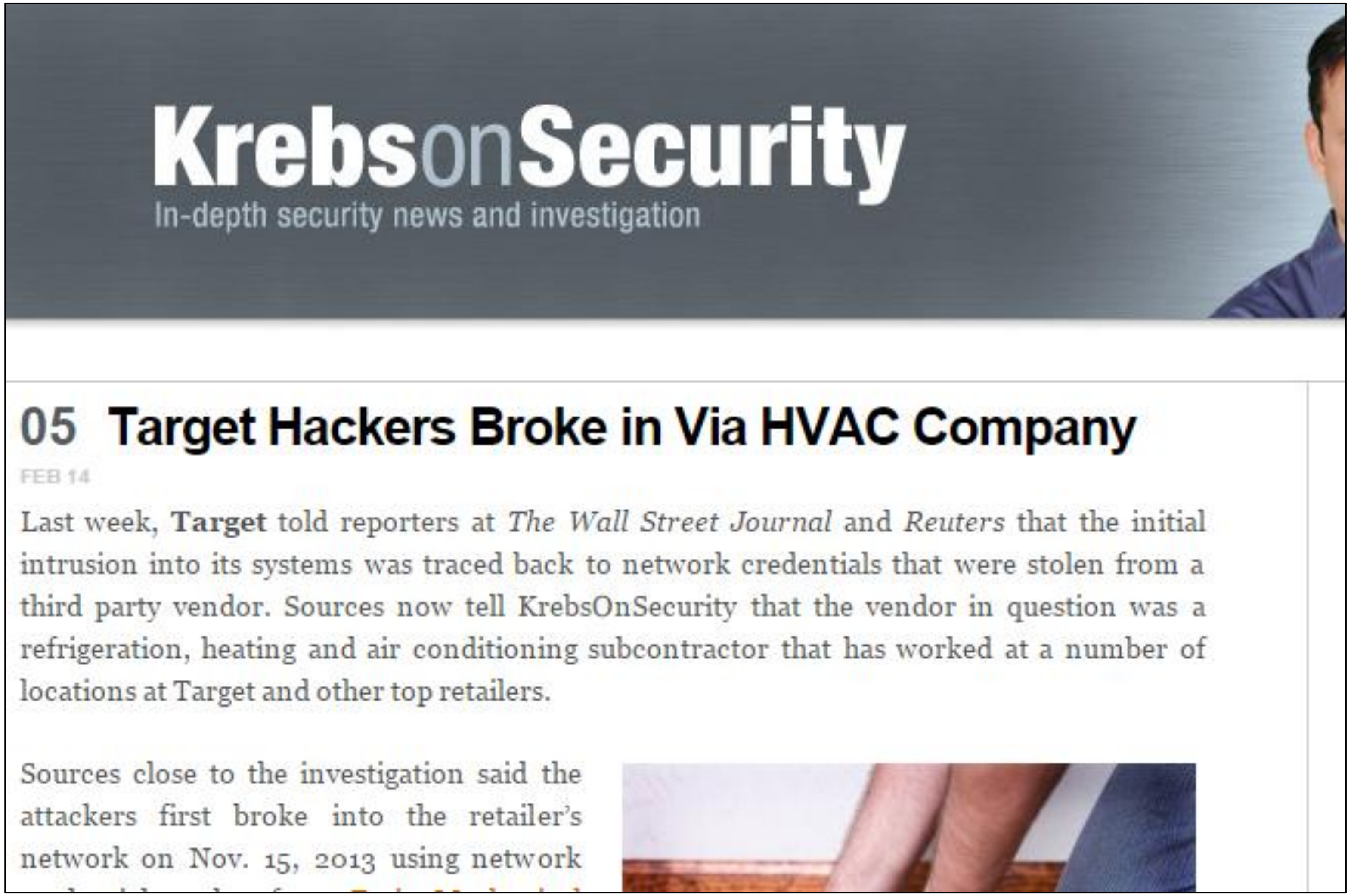
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

.ieee.org

Where the story begins….Commercial Controls 2013

December 2013 Target Pays $18.5M to 47 states!

May 2014 Profit Fall 46% or $520M



KrebsonSecurity

In-depth security news and investigation

05 Target Hackers Broke in Via HVAC Company

FEB 14

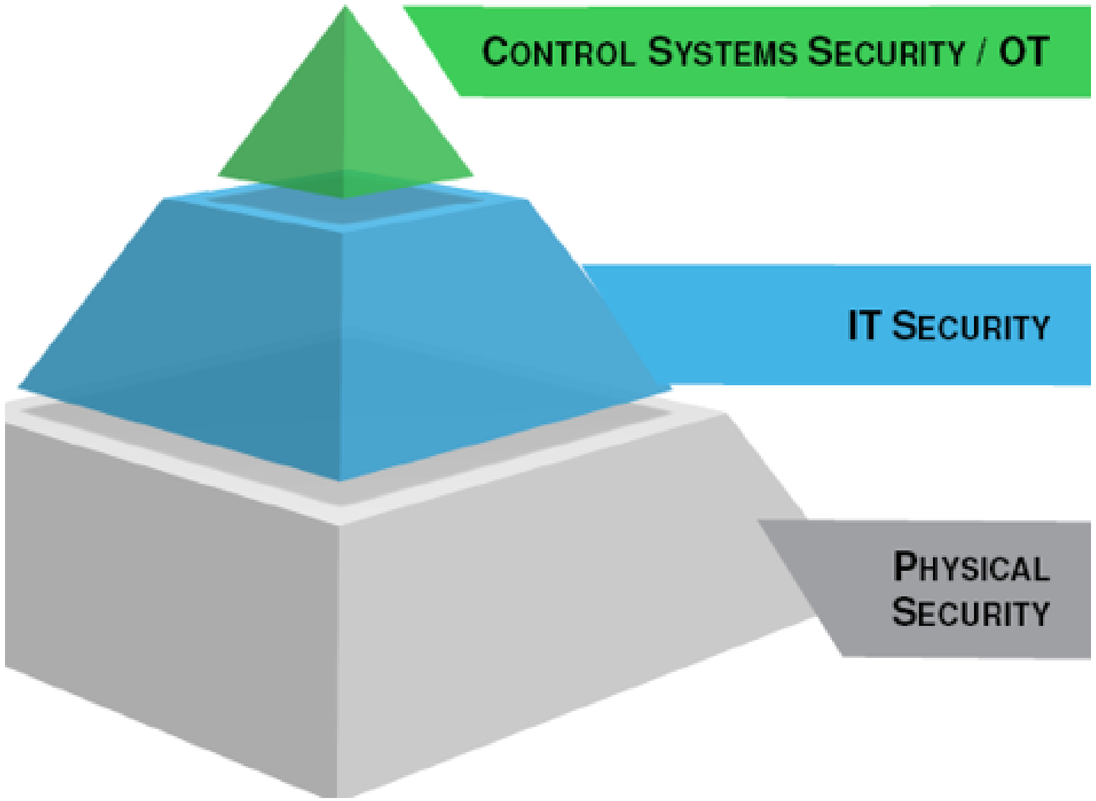
Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network

Reducing Cybersecurity Attaches - A Risk-Based Approach

- Asset Identification
- Threat Identification
- Vulnerability Identification
- Existing Security Controls Identification
- Consequence Analysis
- Risk Ranking
- Security Controls Recommendations

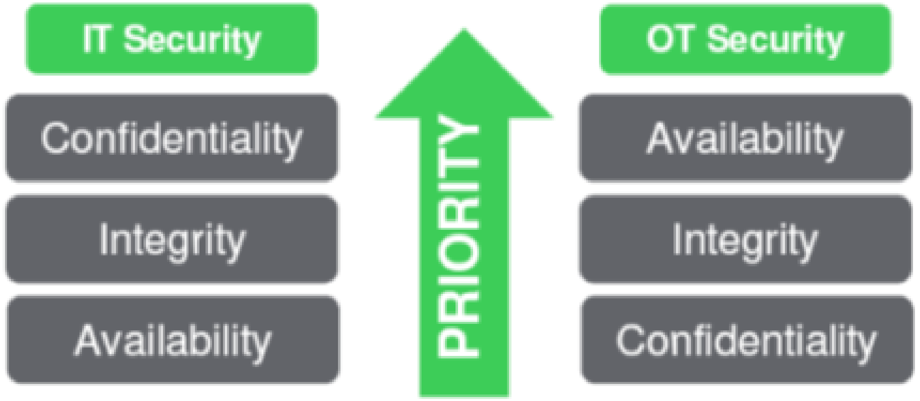
Commercial Cybersecurity Is MORE Than Just IT Security



CONTROL SYSTEMS SECURITY / OT

IT SECURITY

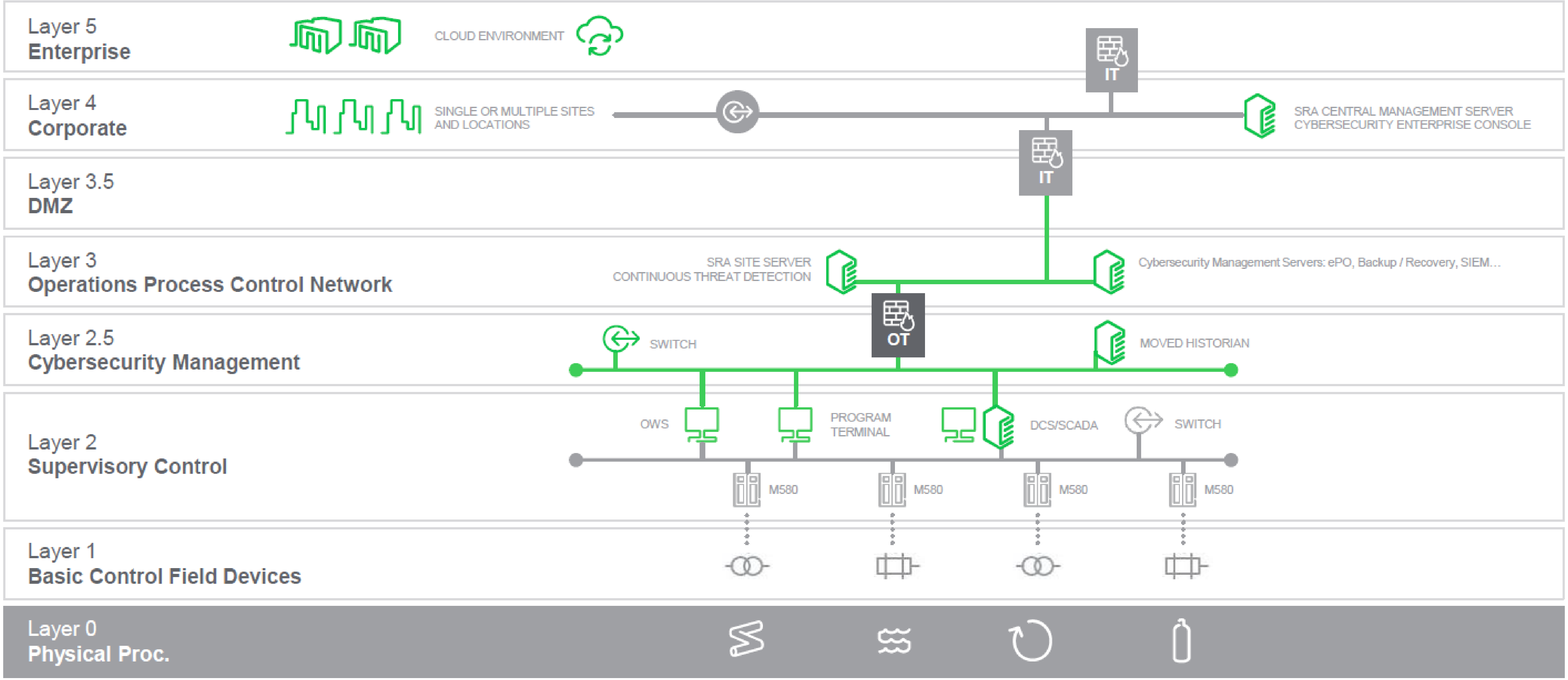
PHYSICAL SECURITY



IT Security	PRIORITY	OT Security
Confidentiality		Availability
Integrity		Integrity
Availability		Confidentiality

Do you think Re-Shuffling IT priorities will allow OT needs to be met?

OT Cybersecurity Reference Architecture (Purdue Model)



Layer 5
Enterprise

CLOUD ENVIRONMENT

Layer 4
Corporate

SINGLE OR MULTIPLE SITES AND LOCATIONS

SRA CENTRAL MANAGEMENT SERVER
CYBERSECURITY ENTERPRISE CONSOLE

Layer 3.5
DMZ

Layer 3
Operations Process Control Network

SRA SITE SERVER
CONTINUOUS THREAT DETECTION

Cybersecurity Management Servers: ePO, Backup / Recovery, SIEM…

Layer 2.5
Cybersecurity Management

SWITCH

MOVED HISTORIAN

Layer 2
Supervisory Control

OWS

PROGRAM TERMINAL

DCS/SCADA

SWITCH

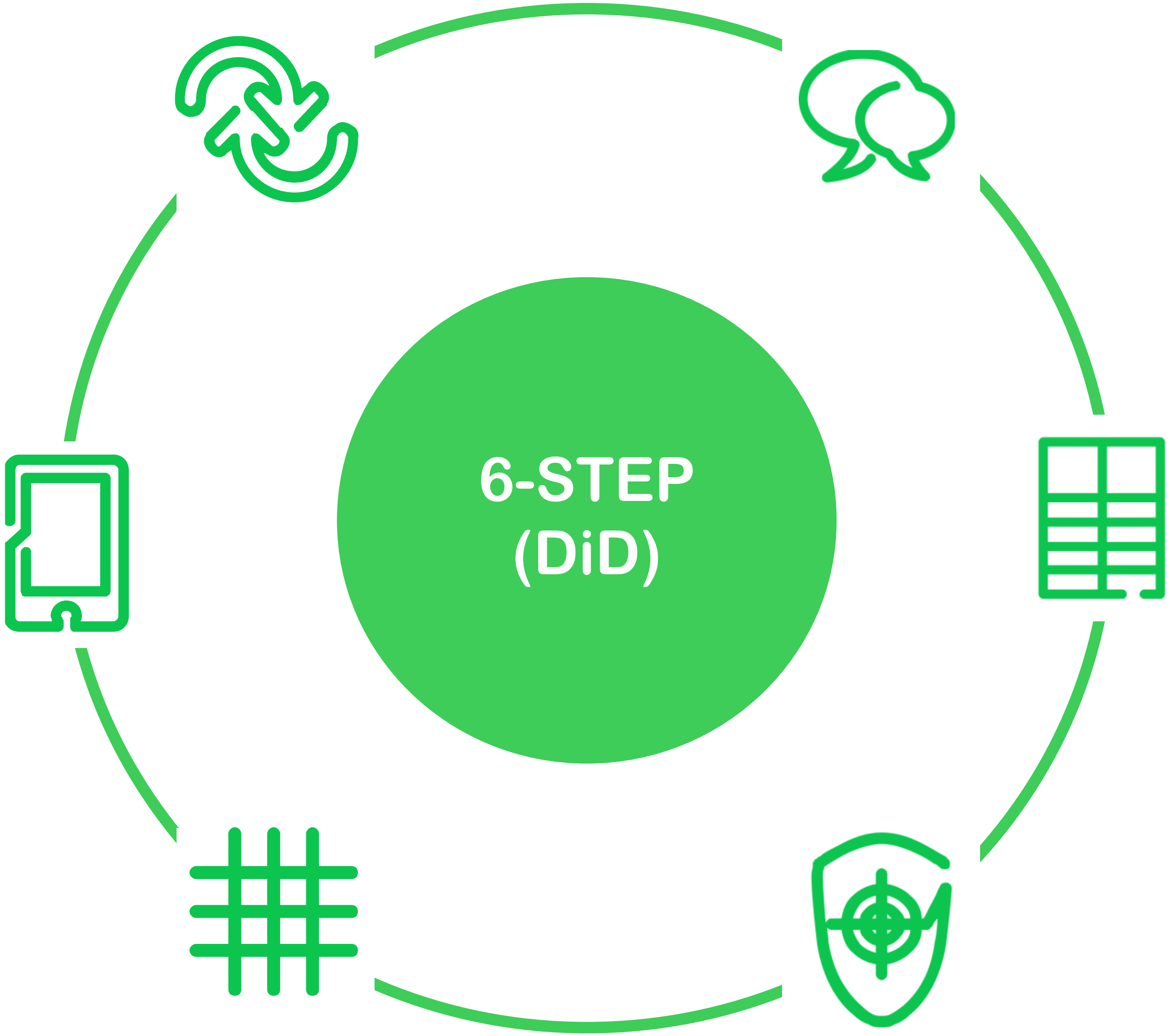
Layer 1
Basic Control Field Devices

Layer 0
Physical Proc.

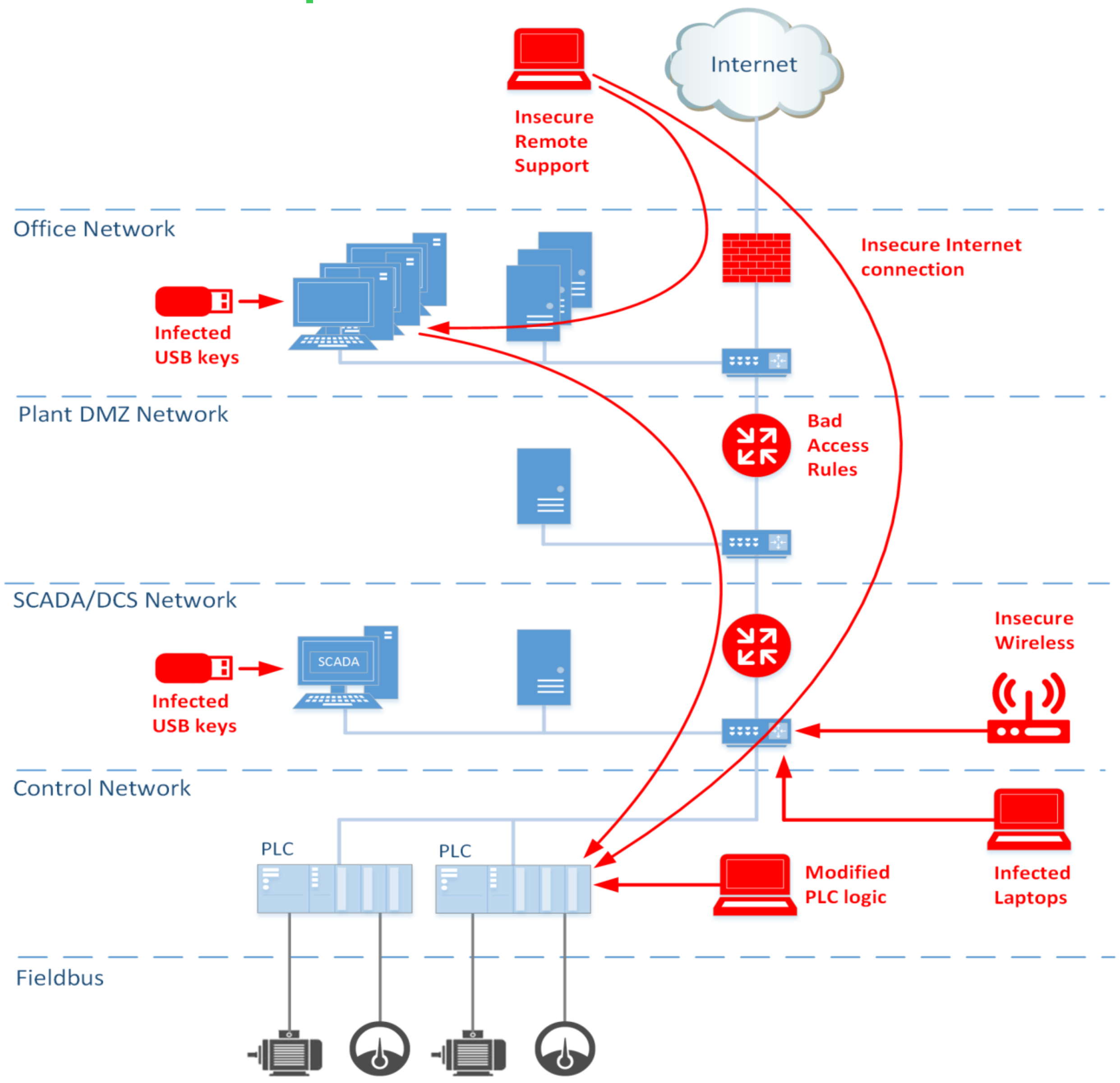
Life Is On Schneider Electric

“Defense in Depth”

1. Security Plan
2. Network Separation
3. Perimeter Protection
4. Network Segmentation
5. Device Hardening
6. Monitoring & Update



Potential Avenues of Compromise



Life Is On Schneider Electric

Defense in Depth - Step 1: Security Plan (Customer)

Define

- Roles and responsibilities
- Allowed activities, actions and processes
- Consequences of non-compliance

Full network assessment

- Communication paths
- Audit of all device
- Security settings
- Network drawings

Vulnerability assessment

- Potential threats
- Consequences, risk assessment and mitigation

Assessment and Design Service

Product Alerts

Password Policy

Patch Updates

Example Policy: Password Management

- **Change all default passwords**
- **Grant passwords** only to people who need access; Prohibit sharing
- **Do not display passwords** during password entry
- Passwords should be **strong**
- Require users/applications to **change passwords** on a scheduled interval
- **Remove employee access** account when employment has terminated
- Require use of different passwords for different accounts, systems, and applications (i.e**. roles**)
- Passwords should **not be transmitted electronically** over the insecure Internet, such as via e-mail

Policies and procedures on password management are often lacking or missing entirely

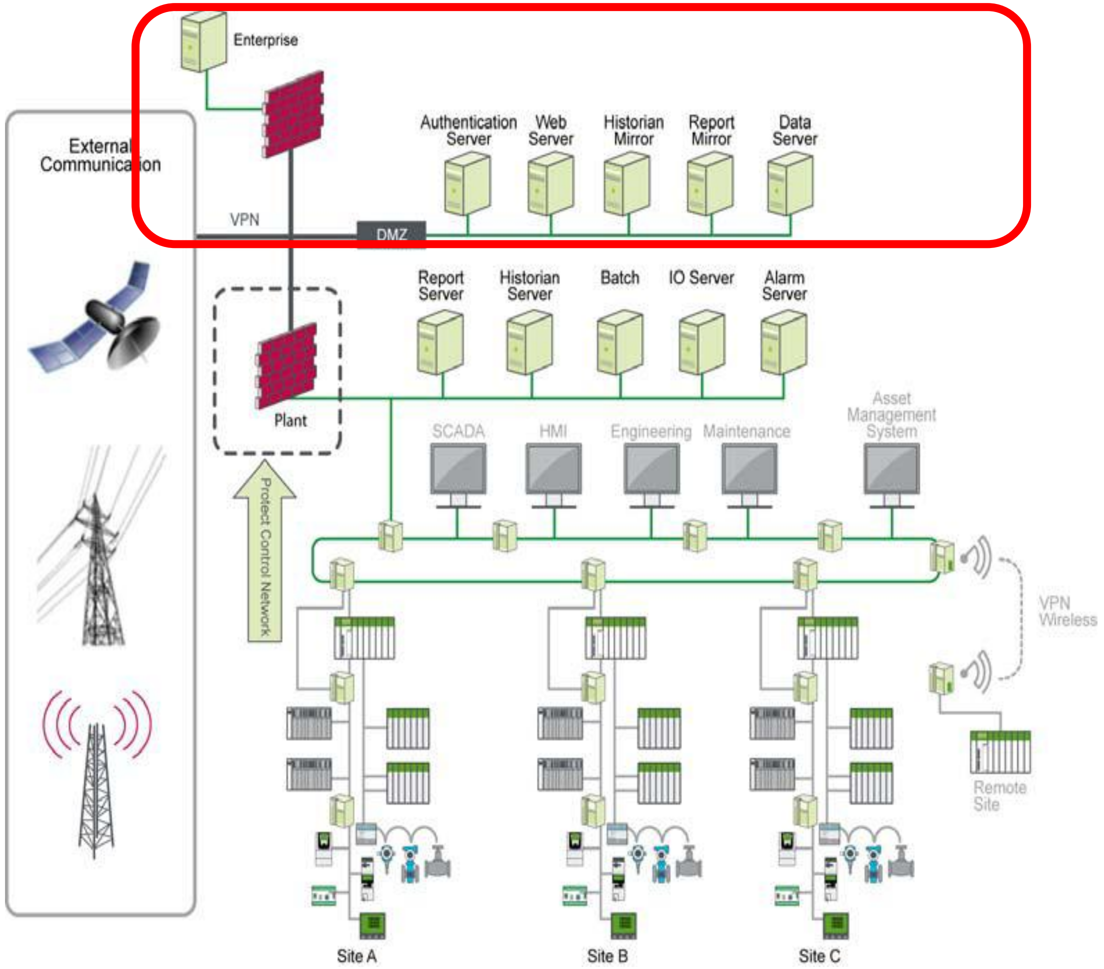
Defense in Depth - Step 2: Network Separation (from Public)

Separate the Systems from the outside world

- Create a ‘buffer’ network (**DMZ or demilitarized zone**) between the BAS network and the rest of the world, using routers and firewalls
- **Block inbound traffic** to the BAS except through the DMZ firewall
- **Limit outbound traffic** to essential and authorized traffic only

DMZ host for servers

- Web Servers
- Cloud
- SQL Servers
- Mail Servers



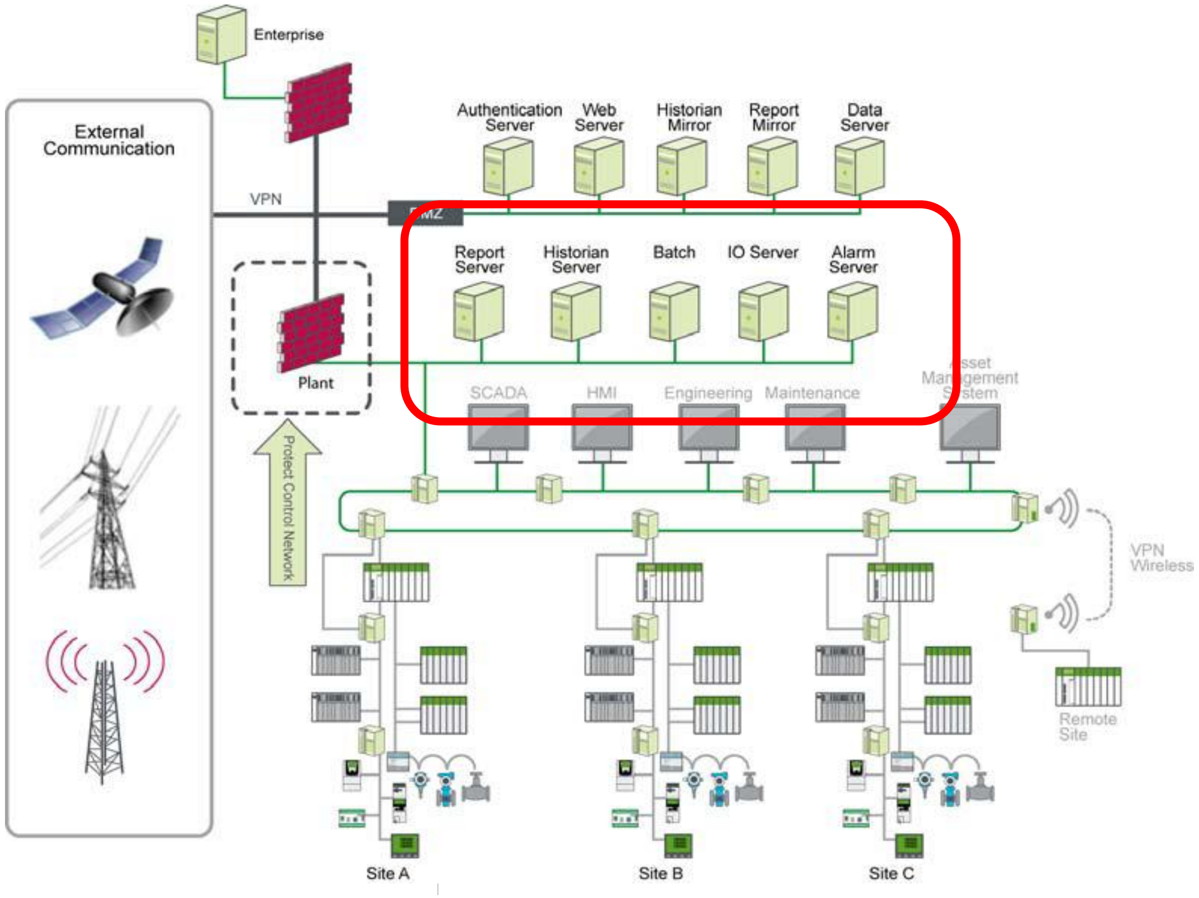
Defense in Depth - Step 3: Perimeter Protection (VLANs)

Protect the BAS perimeter using a firewall

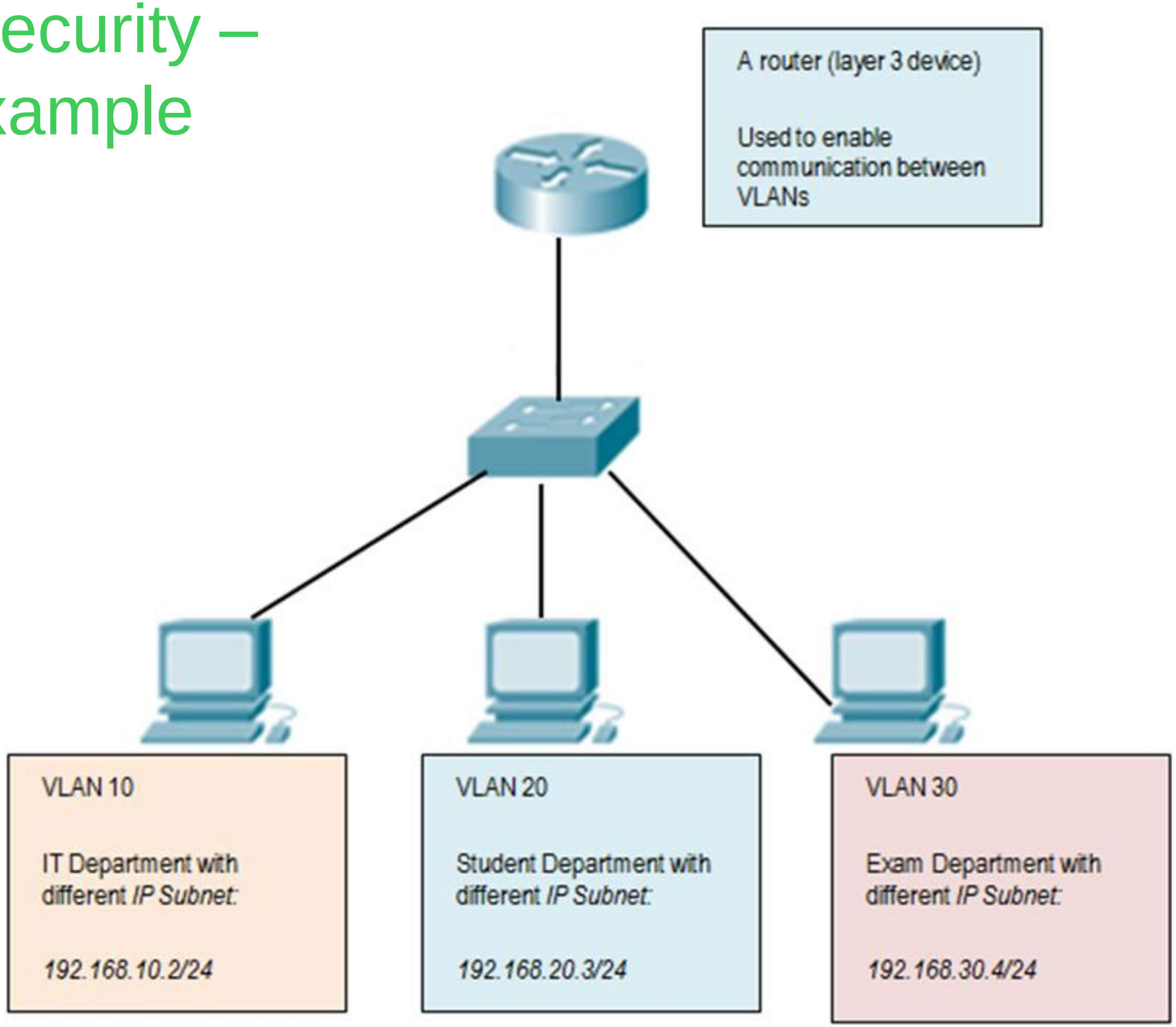
- Validate packets and protocols
- Manage authorization of certain data packets
- Restrict IP address or user access via authorization and authentication (Whitelist)

Secure remote accesses

- Use the VPN technology of routers and firewalls
- Use the latest authentication and authorization technologies; they're evolving fast



Network Security – VLANS Example



A router (layer 3 device)

Used to enable communication between VLANs

VLAN 10

IT Department with different *IP Subnet:*

192.168.10.2/24

VLAN 20

Student Department with different *IP Subnet:*

192.168.20.3/24

VLAN 30

Exam Department with different *IP Subnet:*

192.168.30.4/24

Defense in Depth - Step 3: Perimeter Protection

Firewall: A device for filtering packets based on source/destination IP address and protocol

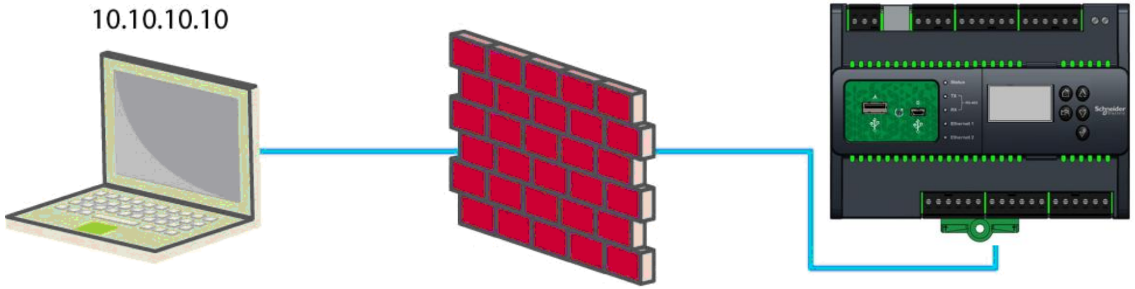
Ingress and Egress filtering

- Source IP addresses should be very few

Rule placement

- Rules that address the expected traffic
- Permit Rules should have specific IP addresses and TCP/UDP port numbers

Only Pre-defined traffic should be allowed from the IT network to control network

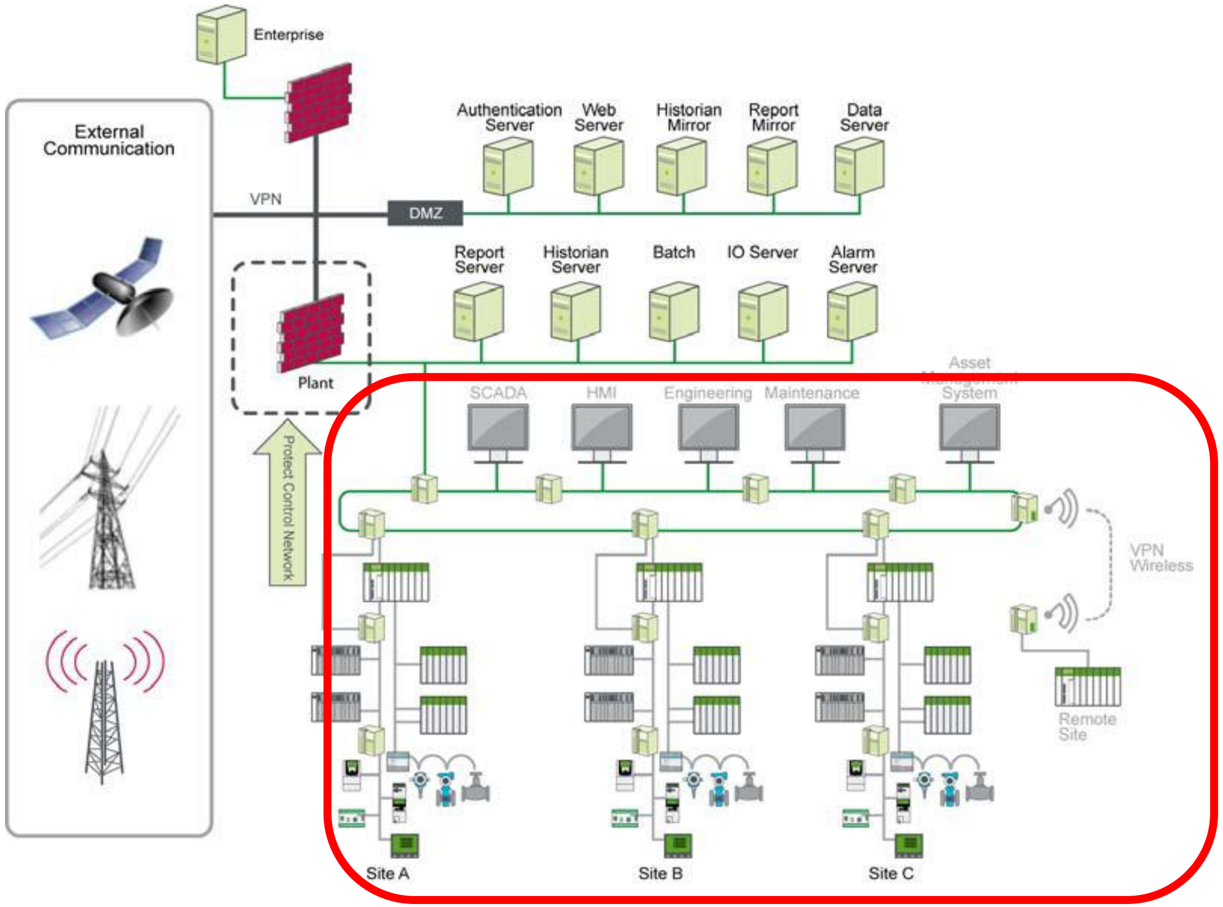


Access List

System Integrator	Port	NOE Address	Port	Allow
10.10.10.10	Port 80	192.168.10.10	80	OK
10.10.10.10	Port 69	192.168.10.10	69	Block

Defense in Depth - Step 4: Network Segmentation & Zones (BAS sub-LANs)

- **Apply normal firewall rules**
- Deep packet inspection
  - Filter data requests to read/write
  - Limit access to specific registers/ports
  - Allow or disallow programming
  - MAC address filtering
- Use special rules to mitigate vulnerabilities by blocking before they reach the device



Life Is On Schneider Electric

Defense in Depth - Step 5: Device Hardening (IP Devices)

On all devices

- Replace default passwords with ‘strong’ passwords
- Shut off unused ports, communication services and hardware interfaces
- Set up broadcast limiter functions
- Use multicast message filtering

On Computers

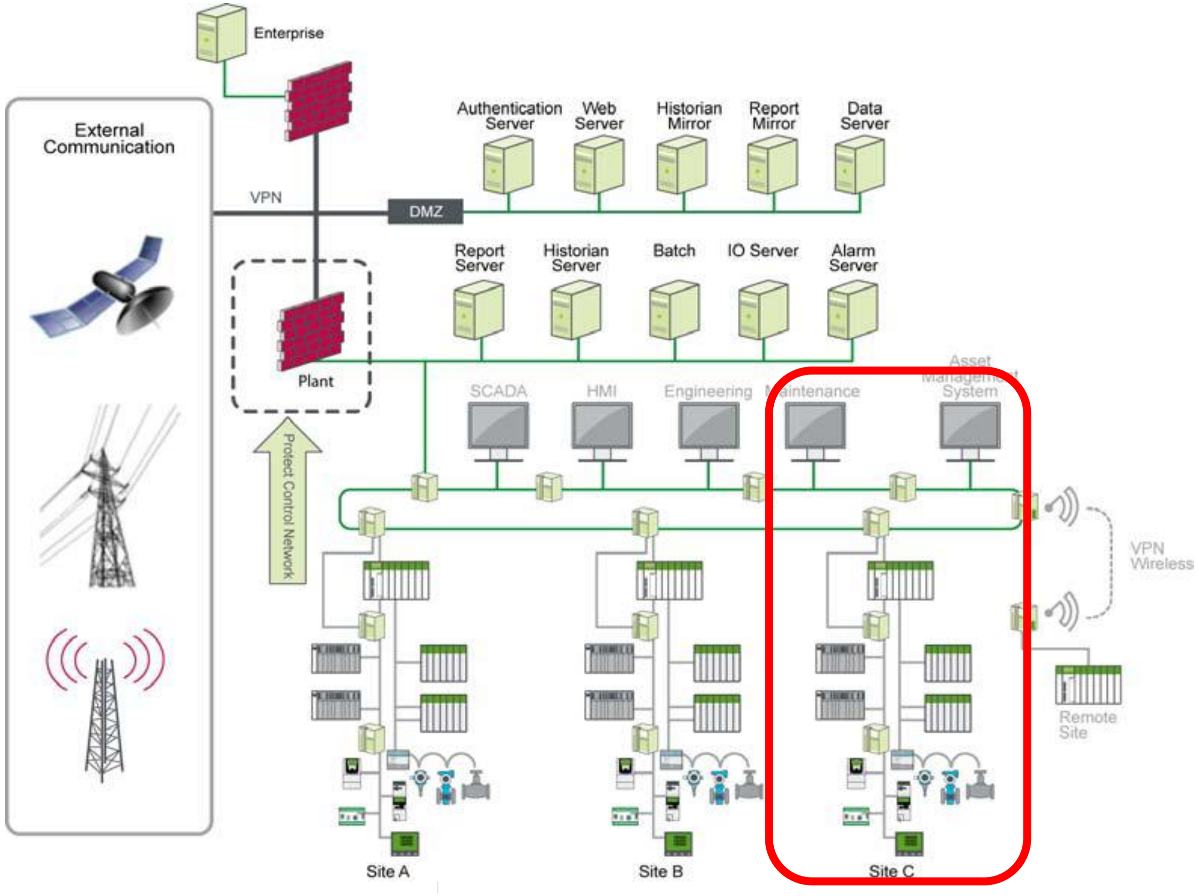
- Forbid or seriously control the use of any external memory

On Software

- Set up all security features: passwords, user profiles, operator action logging

On network switches

- Restrict access on ports to assigned addresses only



Life Is On Schneider Electric

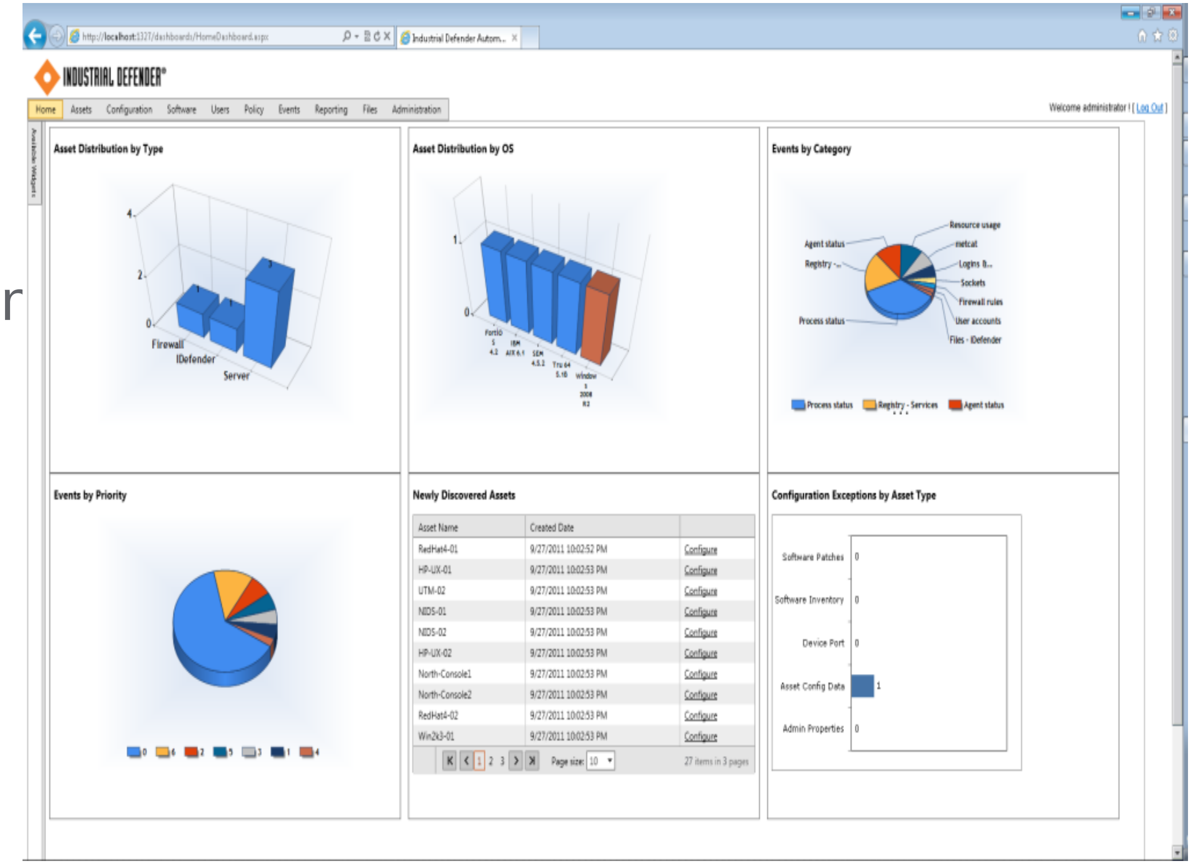
Defense in Depth - Step 6: Monitor & Update

Monitor, Manage and Protect Service

- 24/7 remote security monitoring
- Configuration monitoring
- Reporting for Audit Compliance
- Network and Host Intrusion Detectior systems

Monitor

- Authentication traps
- Windows Event Viewer
- Unauthorized login attempts
- Unusual activity
- Network load
- Device log files



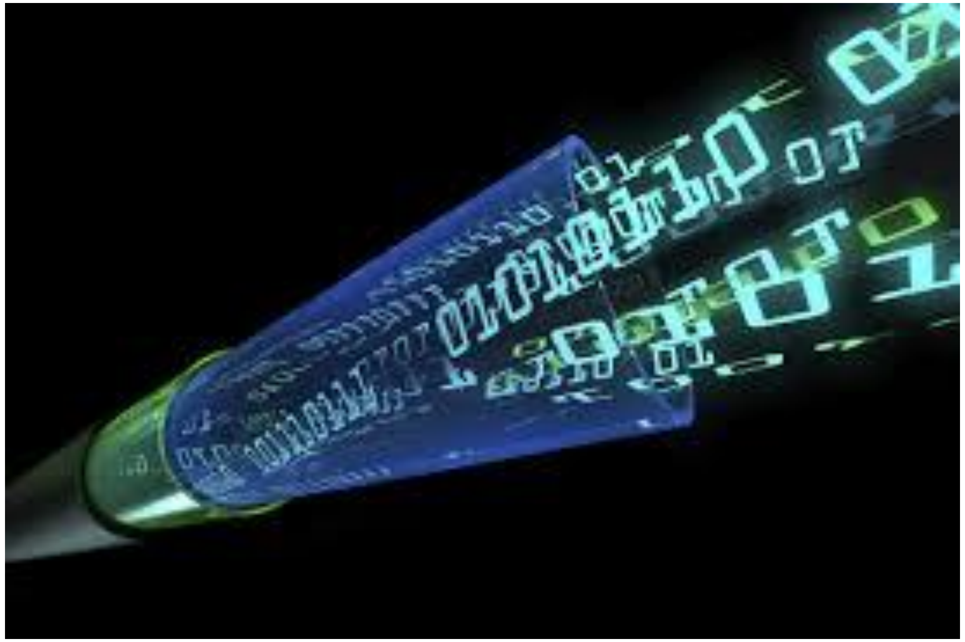
Newly Discovered Assets

Asset Name	Created Date	
RedHat4-01	9/27/2011 10:02:52 PM	Configure
HP-UX-01	9/27/2011 10:02:53 PM	Configure
UTM-02	9/27/2011 10:02:53 PM	Configure
NIDS-01	9/27/2011 10:02:53 PM	Configure
NIDS-02	9/27/2011 10:02:53 PM	Configure
HP-UX-02	9/27/2011 10:02:53 PM	Configure
North-Console1	9/27/2011 10:02:53 PM	Configure
North-Console2	9/27/2011 10:02:53 PM	Configure
RedHat4-02	9/27/2011 10:02:53 PM	Configure
Win2k3-01	9/27/2011 10:02:53 PM	Configure

1 2 3 Page size: 10 27 items in 3 pages

Network Security Best Practices

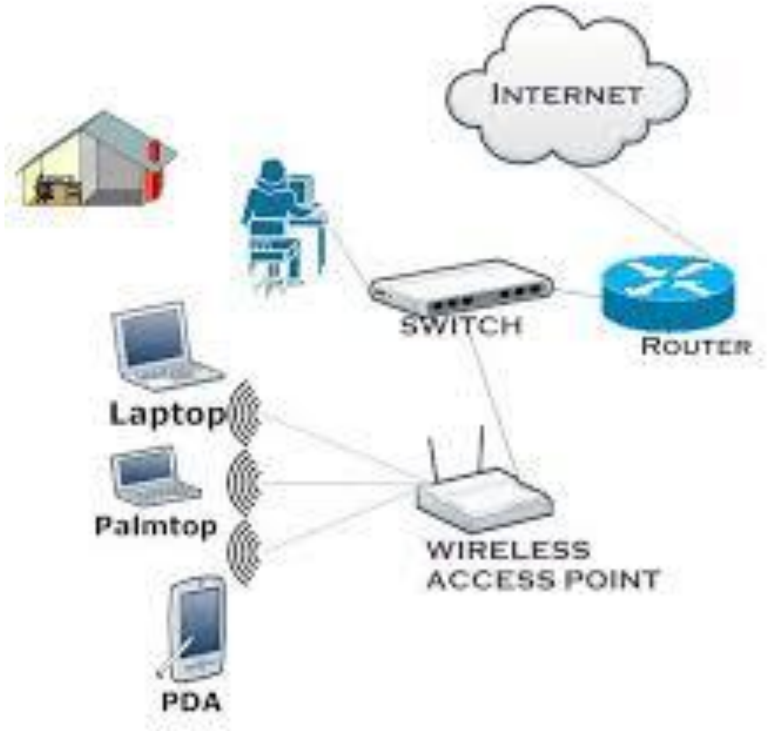
- Most BAS and Security System design do not cover network security in enough detail.
- Anti-virus is rarely included or defined
- No mention of Security aspects on Network Switches (Client/IT specified):
  - Port Security, Firewall
  - VLAN or VPN Separated entities, DMZ
- No 3rd party plugins (JAVA, Silverlight, etc.)
- DIARMF* compliant related projects



*Department of Defense Information Assurance Risk Management Framework

Designing for a Secure Solution

- Collaboration with the customer’s IT department during the early part of the design process
- Consult with manufacturers to understand the product/software security features
- Specify latest versions of all software
- Develop specifications in combination with the customer’s IT department
- Coordinate remote and local access as well as permanent or temporary network installation



Best-in-class cybersecurity

- **Advanced encryption & authentication**
- **IT system integration of password policies**
- **Full system backup, recovery & reconstitution**
- **Full Secure Development Lifecycle (SDL) practices (IEC & ISA)**
- **Cybersecurity for Sustainable Infrastructure**

Best Practices

- Supporting IEC62443-4-1 (ISA99)
- Federal NIST 800 Series Baseline Requirements (US Gov. & Military)
- Compliance with DoD Risk Management Framework (RMF)
- EC 27034 Cybersecurity Policies
- TLS 1.3 encryption support
- System information & event monitoring (SIEM) integration
- Active Directory integration & Audit Logs

Questions

Published Resources

[Five Best Practices to Improve BMS Cybersecurity]

[Cyber Security Portal - Schneider Electric]

Life Is On

Schneider Electric

Schneider Electric is Supporting IEC62443 (ISA99, ISASecure)

Certifications for product, processes, and people

International Industrial Cybersecurity Standards are emerging

- Local regulations and certifications pose a risk when working internationally.
- Some groups still applying IT security standards to OT offers, it can be done but needs to be done with experience and care …

https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

ASHB
Association for Smarter Homes & Buildings

THANK YOU!

Questions?

5. Smarter Homes & Buildings Podcast
Chris Larry (Exp US Services Inc.)

SMARTER HOMES & BUILDINGS PODCAST
ASHB
Association for Smarter Homes & Buildings

ashb.com/podcast

Join industry experts and leaders from around the globe as they discuss everything smart home and intelligent buildings.

Apple Podcasts

Spotify

ASHB is looking for guests and hosts for future pre-recorded episodes. Contact admin@ashb.com for more information.

Recent Recordings:

- The Road to Decarbonization: Strategies for Critical Environments
- Beyond Traditional Appraisals & Unseen Liabilities: Rethinking Commercial Real Estate
- ’Killer Apps’ and Actionable Data Migration: Make Yourself the Smart Building Hero!

6. ASHB Whitepapers
Ken Wacks (Ken Wacks Associates)

ASHB
Research Program

Published IBC White Papers can be downloaded at:
ashb.com/whitepapers
Send proposals to admin@ashb.com

Recently Published

ASHB
Fire Alarm Systems in Smart Buildings
Primer on Fire and Life Safety Systems
AN ASHB WHITE PAPER

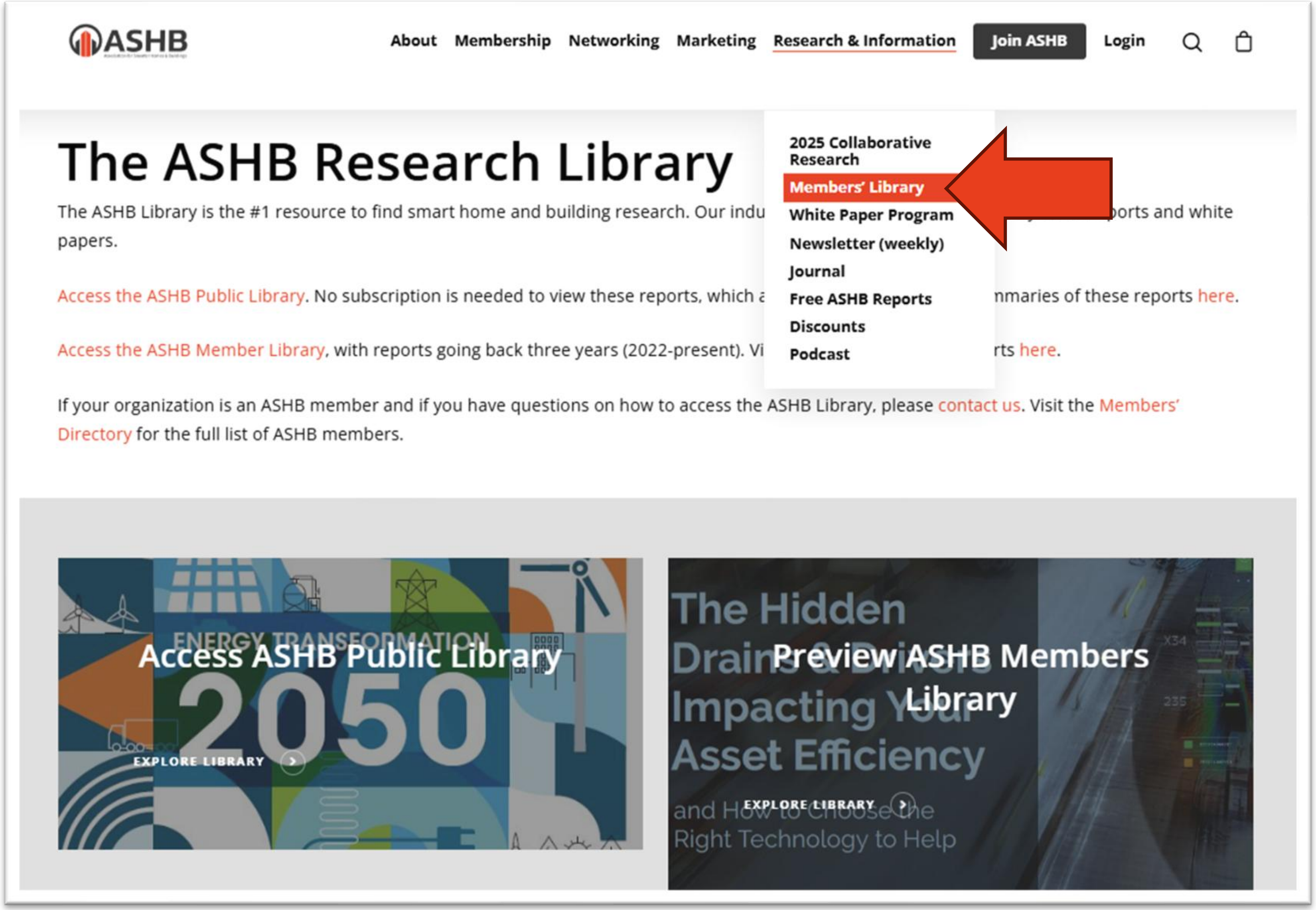
Mission Critical Global Alliance CABA
Cybersecurity for Building Automation Systems

CABA
Bipolar Ionization and Its Contribution to Smart and Safe Buildings

CABA
Benefits of Advanced Lighting Systems on the Human Experience

CABA
The Commercialization of LIFI

6. ASHB Research Library
Ken Wacks (Ken Wacks Associates)


ASHB
About
Membership
Networking
Marketing
Research & Information
Join ASHB
Login
2025 Collaborative Research
Members' Library
White Paper Program
Newsletter (weekly)
Journal
Free ASHB Reports
Discounts
Podcast
ENERGY TRANSFORMATION 2050
Access ASHB Public Library
EXPLORE LIBRARY
The Hidden Drains & Drivers Impacting Your Asset Efficiency and How to Choose the Right Technology to Help
Preview ASHB Members Library
EXPLORE LIBRARY

The ASHB Research Library

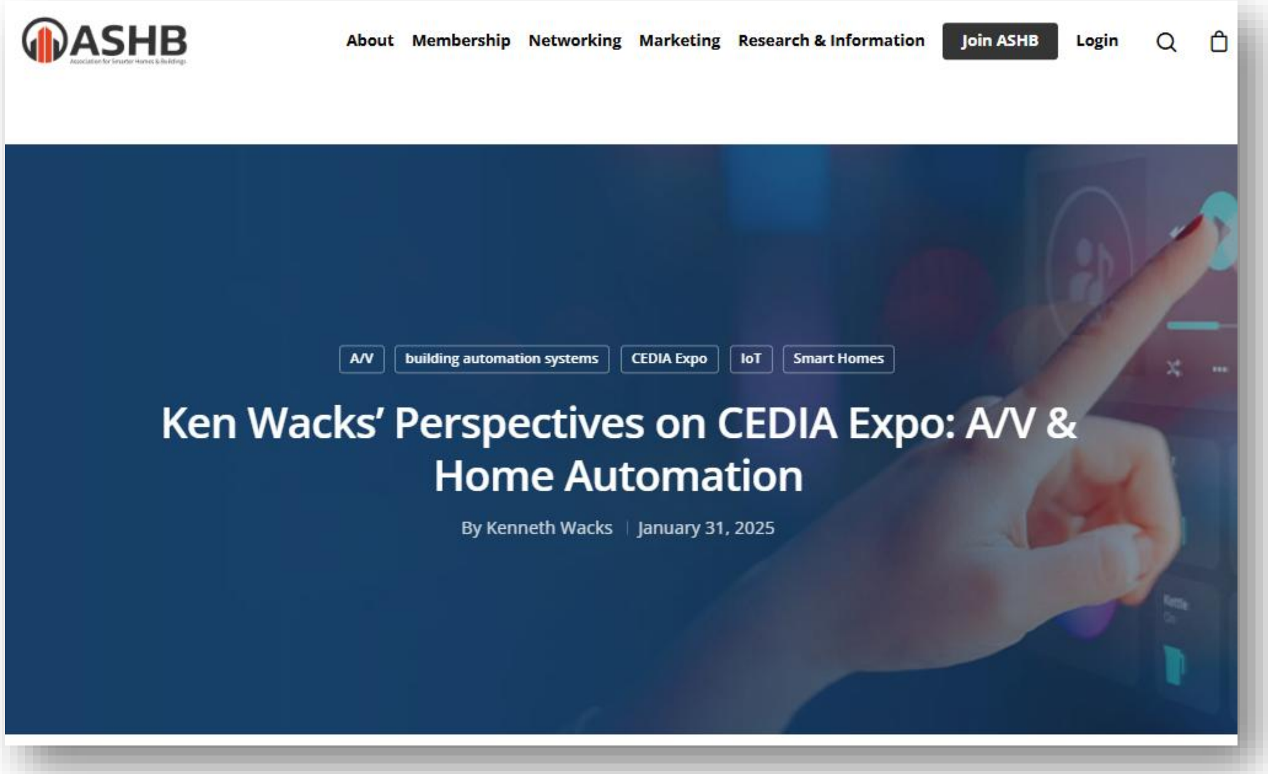
The ASHB Library is the #1 resource to find smart home and building research. Our indu ports and white papers.

Access the ASHB Public Library. No subscription is needed to view these reports, which a mmaries of these reports here.

Access the ASHB Member Library, with reports going back three years (2022-present). Vi rts here.

If your organization is an ASHB member and if you have questions on how to access the ASHB Library, please contact us. Visit the Members' Directory for the full list of ASHB members.

7. ASHB Journal
Ken Wacks (Ken Wacks Associates)



Ken Wacks' Perspectives on CEDIA Expo: A/V & Home Automation

By Kenneth Wacks | January 31, 2025

The ASHB Journal aims to educate and inform the ASHB membership and industry at large on emerging research, issues, challenges, and opportunities in the smart home and building sectors.

New articles are posted to the ASHB website, included in the weekly NewsBrief, and circulated on Twitter and LinkedIn.

Send proposals to admin@ashb.com

Recent posts:

- **Ken Wacks' Perspectives on CEDIA Expo: A/V & Home Automation**
- **Ken Wacks' Perspectives: Saving Lives with Standards**
- **Ken Wacks' Perspectives: CES 2024 Re-positioning the industry**

8. New Business

Bob Allan (NAVCO, Inc.)

New IBC Business?

9. Announcements
Harsha Chandrashekar (Honeywell International Inc.)

IFMA World Workplace
March 12-13 | Netherlands

DISTRIBUTECH
March 24-27 | Dallas, TX

ISC West
March 31-April 4 | Las Vegas, NV

LightFair
May 4-8 | Las Vegas, NV

Haystack Connect
May 6-8 | Washington, DC

Controls-Con
May 8-9 | Detroit, MI

Realcomm IBcon
June 3-4 | Savannah, GA

10. Adjournment

Bob Allan (NAVCO, Inc.)

Next IBC Meeting: May 2025

Association for Smarter Homes & Buildings (ASHB)

admin@ashb.com | www.ashb.com | www.ashb.com/ibc

Connect to what's next™

ASHB

Intelligent Buildings Council