IMSA Webinar Series

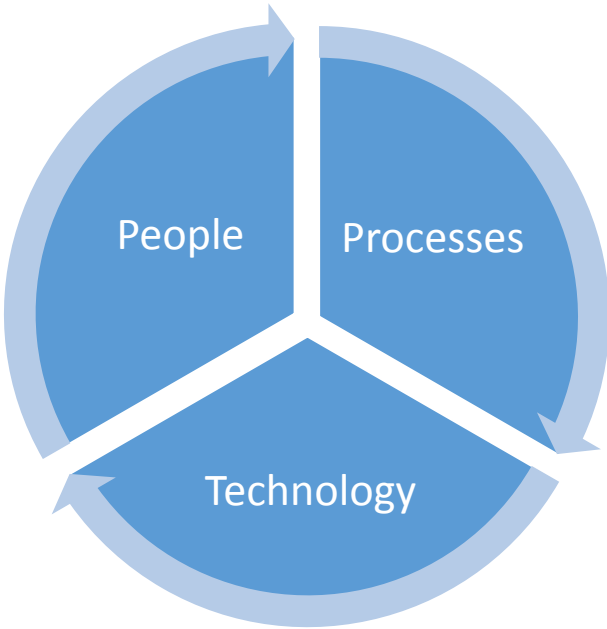
Cybersecurity and Smart Cities

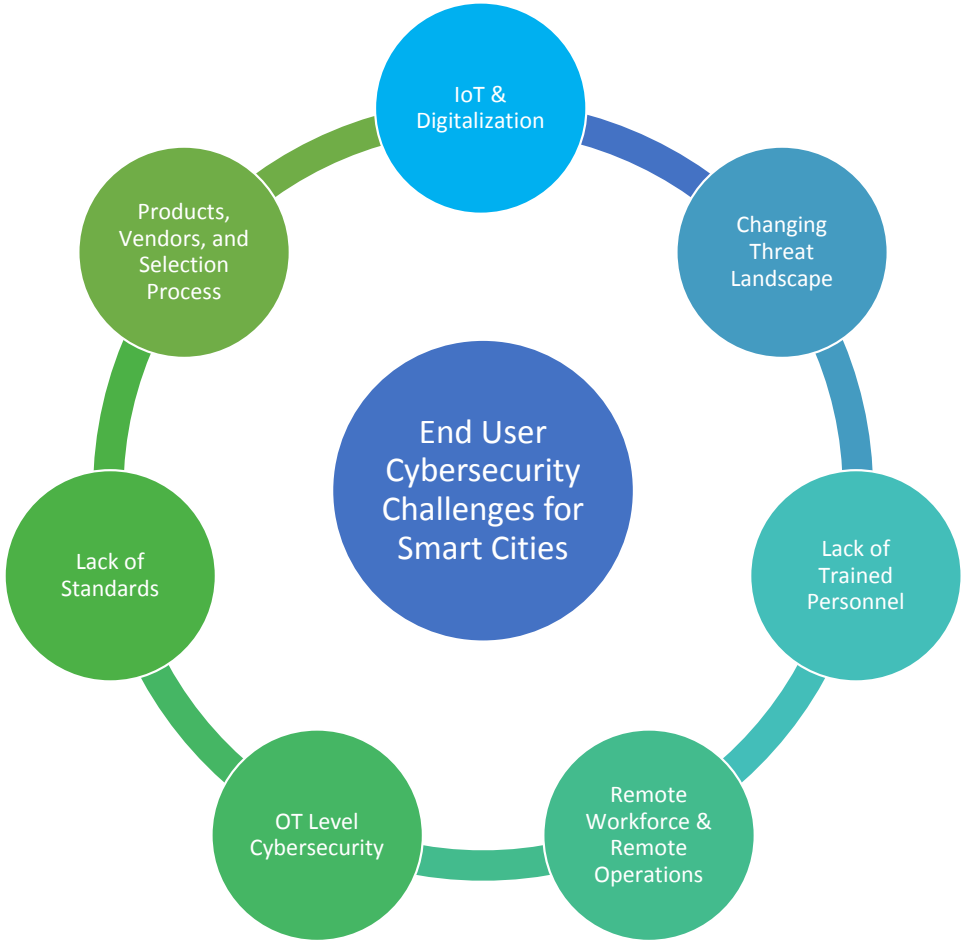
Speaker

- Background in Process Control, Process Safety, Instrumentation and Networks.
- Over 25 Years of Experience in Industrial Markets
- Member of the ARC Smart Cities Team and Cybersecurity Team

© ARC Advisory Group

Primary End User Challenges in Cybersecurity for Smart Cities

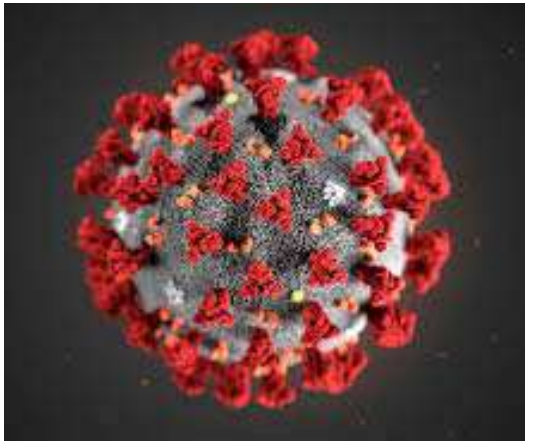




© ARC Advisory Group

Pandemic Specific Cybersecurity Challenges: Today

- Anyone that can work from home is working from home, this creates security challenges on a massive scale
- Shift to remote monitoring and operations at the OT level AND the IT level requires access to sensitive and critical data from remote locations
- City budgets are decimated due to decreased tax revenue
- Workforce reductions in cities and local governments
- Opportunistic cyber attacks related to the pandemic (mostly ransomware)
- Cities need access to wider range of data, and they need to be able to run that data into useful information to fight the pandemic



© ARC Advisory Group

From Pandemic Response to Long Term Resiliency

- People will return to office spaces, but more people will be permanently working remotely.
- Remote monitoring and operations of OT level assets will continue to increase.
- Smaller number of personnel will need access to data and information from a wider range of systems and assets. Less people, more responsibility.
- Attacks specifically aimed at OT assets will increase, particularly from advanced persistent threats.
- Cities will increasingly implement smart city platforms that will integrate formerly separate islands of functionality within the city infrastructure.
- Volume of data will increase exponentially and lots of additional computing power will be used, including cloud computing, edge computing, containers, and more.

© ARC Advisory Group

Smart Cities are Critical Infrastructure

This Photo by Unknown Author is licensed under CC BY-NC

- Smart city systems have an impact on human health, life and safety
  - Power Distribution
  - Water Treatment and Distribution
  - Emergency Management, EMS
  - Stormwater Management
  - Transportation Management
  - Rail
  - Building Management

A Few Words About Ransomware

- Opportunistic attackers have ramped up ransomware attacks, taking advantage of increased remote workforce, lack of cybersecurity training and awareness.
- Ransomware attackers have ranges of capabilities and sophistication, from coordinated campaigns that affect multiple sites at once funded by nation-state backed threat groups to smaller criminal or activist groups.
- Most ransomware attacks are the result of phishing campaigns, targeted fraudulent emails that trick the user into clicking a link, downloading an attachment, etc.
- Not just a big city problem, smaller and rural communities are particularly vulnerable.
- A ransomware attack may put a major dent in a city's budget, but it can completely paralyze and bankrupt a small town.
- Better funding is needed for municipalities and better coordination at a state level for resources, including training.

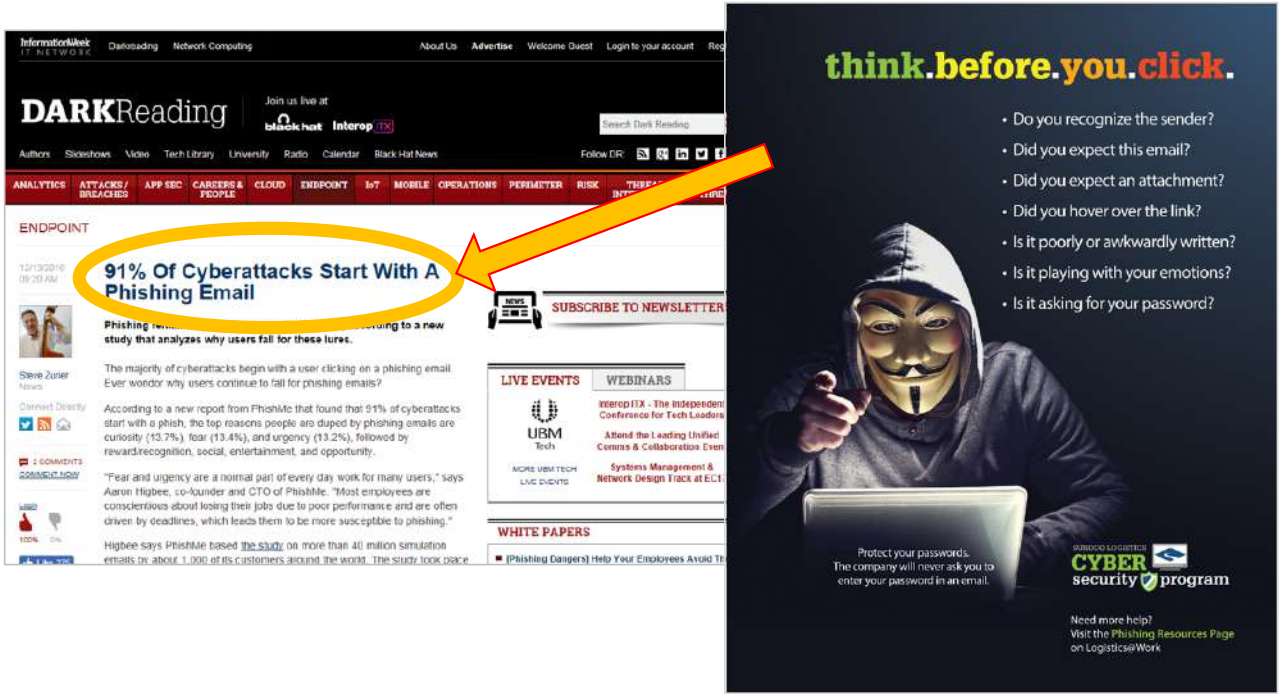
© ARC Advisory Group • 7

Recent Examples of Ransomware Attacks

- Knoxville, TN, June 15, employee falls victim to phishing attack, cost yet to be determined. Ransomware affects police department, courts, total loss of connectivity, cost TBD.
- New Orleans, LA: Cost will be at least $7 million, despite the city having a $3 million cyber insurance policy
- Lakeland City, FLA: small town of 12,000 residents, $460K ransom
- Atlanta, GA: More than $17 million?
- Texas: 22 Mostly rural communities: cost undisclosed

© ARC Advisory Group

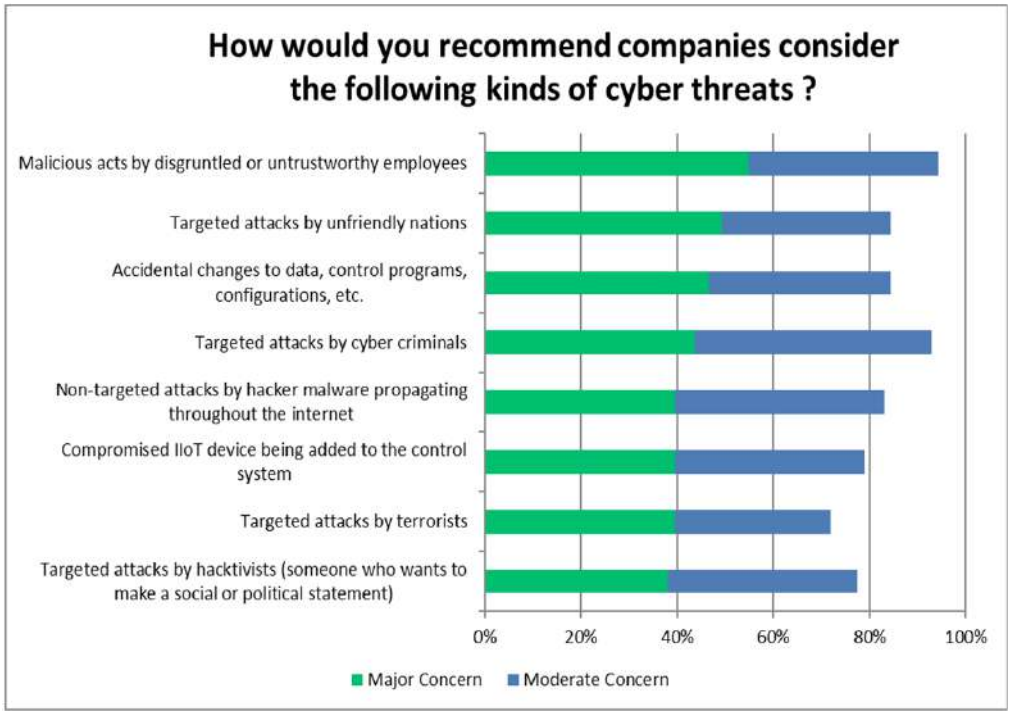
Ransomware, Phishing, and Starting a Cybersecurity Program



© ARC Advisory Group

Threats have Evolved Significantly from Simple Ransomware

- Ransomware gets headlines and can cripple communities
- New age of threats focuses specifically on operations and aims to impact equipment in the physical world

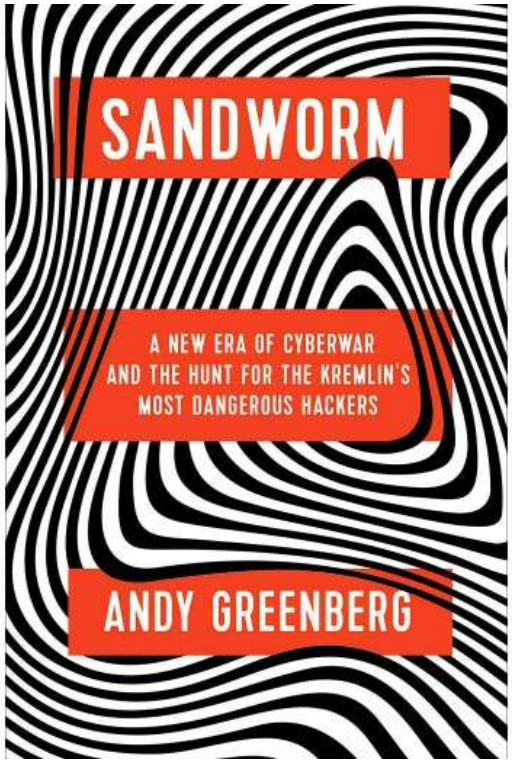


Recent ARC Survey Showing End User Concern with Different Kinds of Attacks

© ARC Advisory Group • 10

Advanced Persistent Threats

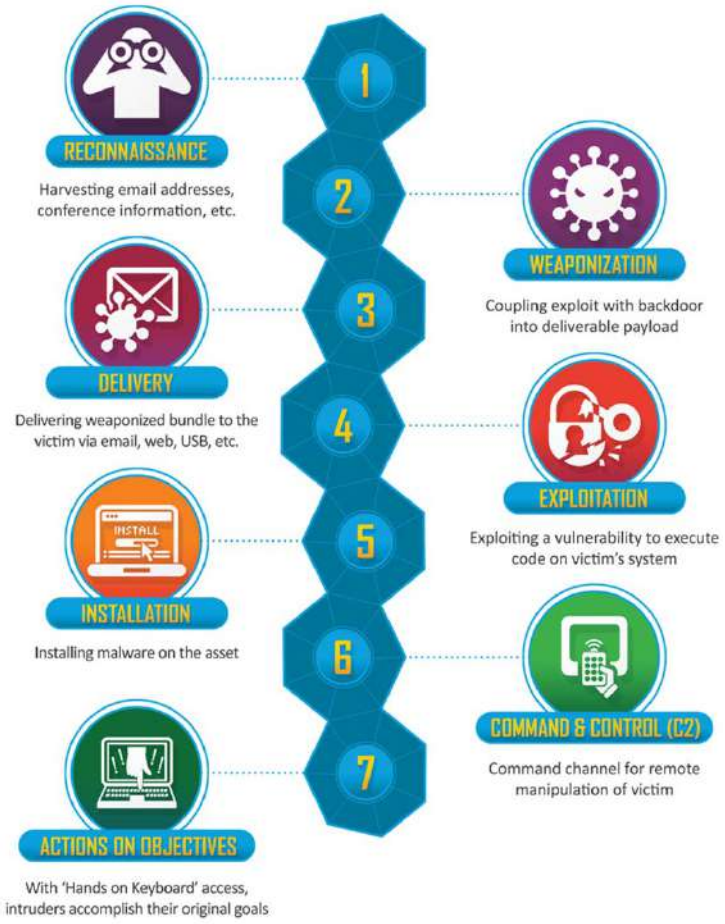
- Have the financial and resource backing of nation states (China, Russia, North Korea, Iran)
- Will mount long term attacks in phases (cyber kill chain)
- Will exist in an organization's network for months or years, doing reconnaissance, gathering sensitive data, monitoring processes and behaviors
- Are increasingly looking to cause damage in OT systems, creating action in the physical world (causing power outages, damaging equipment, etc.)



© ARC Advisory Group

Lockheed Martin Cyber Kill Chain Framework Documents the Stages of a Cyber Attack (Source: Lockheed Martin)

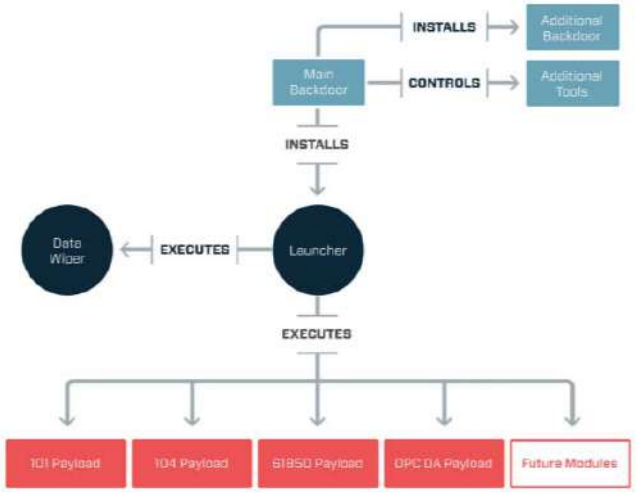
- Ransomware is like throwing rocks.
- Coordinated OT level attacks are like an organized military operation.



© ARC Advisory Group • 12

Ukraine Power Grid Attack of 2015

- Prior compromise of corporate networks using spear-phishing emails with BlackEnergy malware
- Seizing SCADA under control, remotely switching substations off
- Disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators)
- Destruction of files stored on servers and workstations with the KillDisk malware
- Denial-of-service attack on call-center to deny consumers up-to-date information on the blackout



Modular Structure of CRASHOVERRIDE Malware Reveals New Level of Sophistication in Targeted Infrastructure Malware (Source: Dragos)

© ARC Advisory Group • 13

Xenotime Threat Group TRITON Malware Attack

- Hydrocarbon Processing Plant in the Middle East
- Multi-phased, and prolonged cyber-attack that resulted in a safe plant shutdown in August of 2017
- Breach was enabled through multiple security lapses
- Deny the ability of the plant or process to shut down safely

"XENOTIME is easily the most dangerous threat activity publicly known. It is the only activity group intentionally compromising and disrupting industrial safety instrumented systems, which can lead to scenarios involving loss of life and environmental damage." -- Dragos

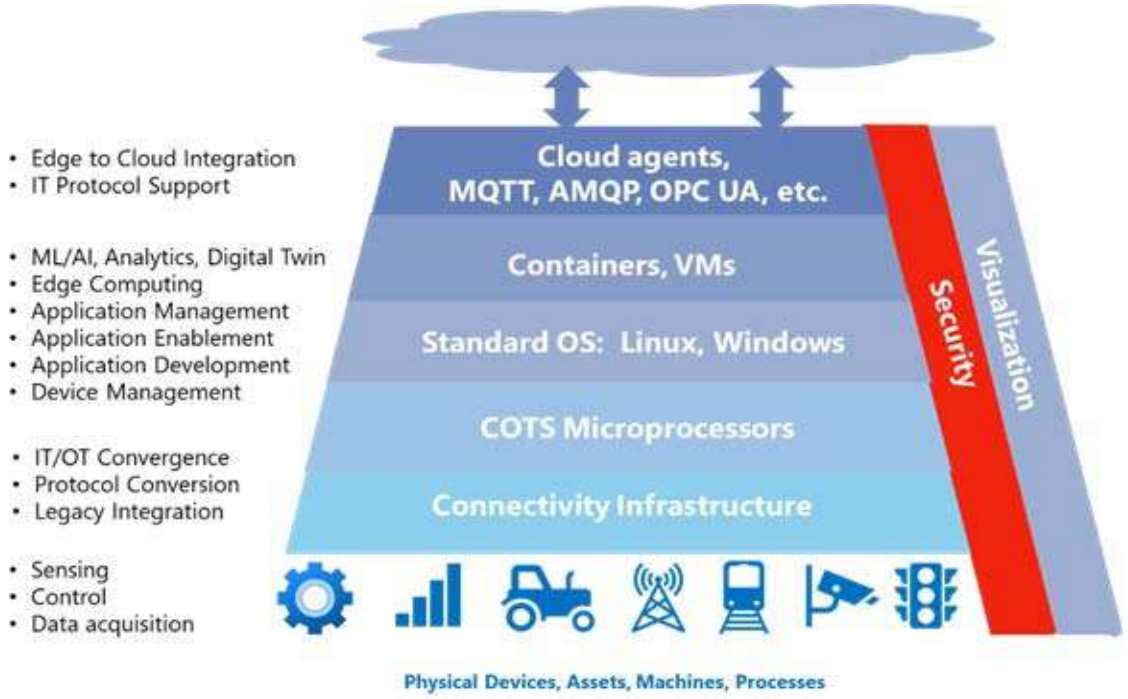
© ARC Advisory Group • 14

IoT Impact on Cybersecurity

- IoT is really a catch all term that encompasses a suite of new technologies being adopted by today's smart cities and buildings.
- Cloud computing (which includes multiple definitions), edge and fog computing, analytics, machine learning, AI, networking technologies (MQTT), wireless infrastructure, 5G – all are part of IoT suite of technologies.
- These technologies are being driven into many new products at a rapid rate.
- Not everyone understands or considers the cybersecurity implications of these technologies and how they find their way into products and applications.
- IoT also means connected. Millions of sensors, controllers, and computing devices.
- Many large end users and owner/operators are struggling with how to balance the innovation of IoT and the business value that it brings with the associated (and sometimes significant) risk to secure and dependable operations.
- Cybersecurity should be part of your selection criteria for products, systems, and applications.

© ARC Advisory Group • 15

For IoT, the Edge is Where the Rubber Meets the Road



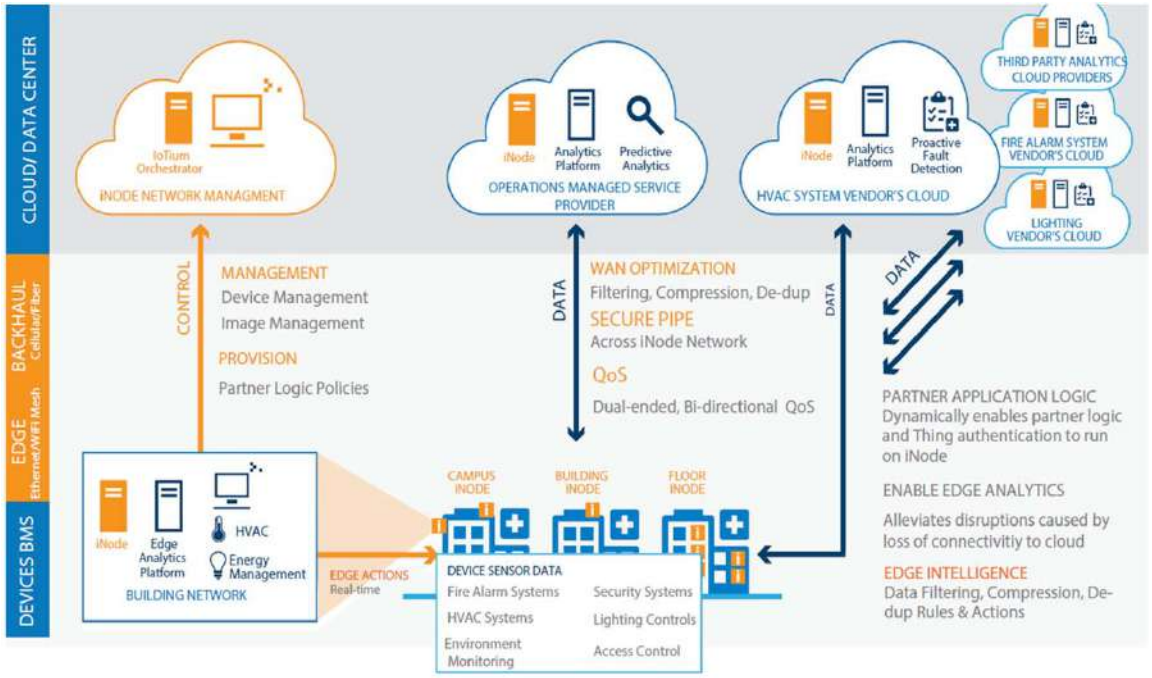
© ARC Advisory Group • 16

The Business Value of IoT: Building Automation Use Case

- Rapid adoption of IoT-based systems with the promise of significantly reduced operational costs is driving rapid growth in the building and facility automation marketplace.
- The major objectives of these systems are to improve occupant comfort, reduce energy consumption and total cost of ownership, operate building systems efficiently, and increase the lifecycle of utilities.
- Digitizing these systems presents a huge opportunity to reduce energy and operational costs for building or facility owner-operators.
- Commercial buildings consume over 70 percent of the electricity produced in the US.
- Many buildings are older and incorporate dated legacy technology and could significantly benefit from retrofitting the building control infrastructure to help reduce total cost of ownership and enhance security and safety.

© ARC Advisory Group • 17

Example of an IoT-Based Architecture for Managing Smart Buildings that Enables Edge Analytics



(Source: Kilroy Realty and Iotium)

© ARC Advisory Group • 18

Zero Trust Cybersecurity Schemes and IoT

- Security remains one of the leading inhibitors to widespread adoption of Industrial IoT applications.
- Zero trust security, where the hardware doesn't trust the software and vice versa, is emerging as the baseline for edge implementations.
- End-to-end secure encrypted network designs are necessary.
- The migration toward using Linux and other standard operating systems coincides with a migration away from secure by configuration, which relies on implementation, to a secure by design emphasis that enables more standardized approaches.
- Scalable device access and authorization strategies are paramount, as are data encryption and intrusion protection. Make sure device authentication occurs be-fore connection is enabled, an improvement over legacy procedure.

© ARC Advisory Group • 19

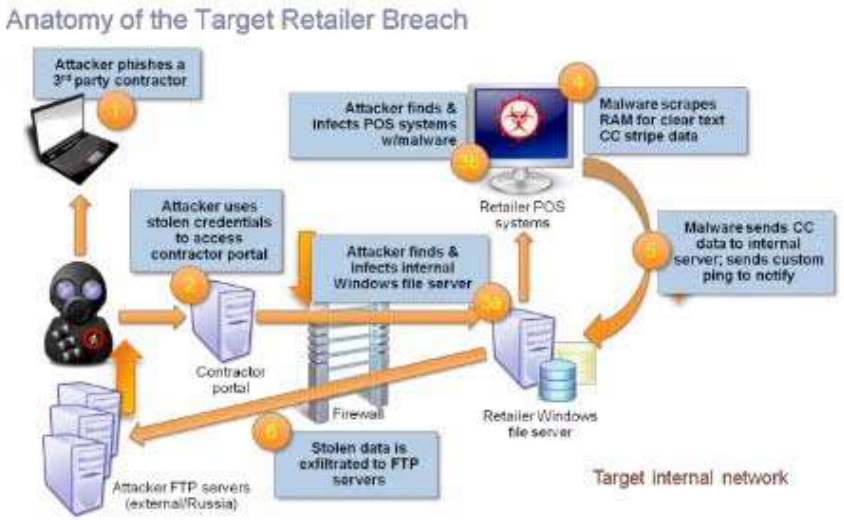
IoT, Connectivity, and Managed Services

- IoT has created a new wave of remote monitoring, managed service providers, and millions of new remote connections for things like performance monitoring, predictive maintenance, etc.
- Exploiting security flaws at trusted third parties is often used as a tactic to gain entry into end user owner/operator sites.
- Target hack is an example of this. Remote monitoring of HVAC systems.
- TRITON also used this technique, harvesting credentials for control system access from a third party.

© ARC Advisory Group • 20

Vetting Third Party Service Providers for Cybersecurity

- The Target Hack (Cost $220 Million Plus)



http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/

© ARC Advisory Group • 21

IT and OT: Domains with Different Goals and Requirements

This Photo by Unknown Author is licensed under CC BY-NC-ND

This Photo by Unknown Author is licensed under CC BY-SA

This Photo by Unknown Author is licensed under CC BY-SA

IT: Primarily concerned with the flow of data and information (and the flow of cash)

OT: Concerned with operating assets in the physical world safely and reliably

What do we Mean by IT/OT Convergence?

IT has always received more attention as far as budget, planning, etc.

More IT level technology is making its way down the OT level

Industrial IoT and edge/cloud computing is replacing many traditional industrial systems

Shift to remote monitoring and operations is facilitated by the IoT and its suite of technologies

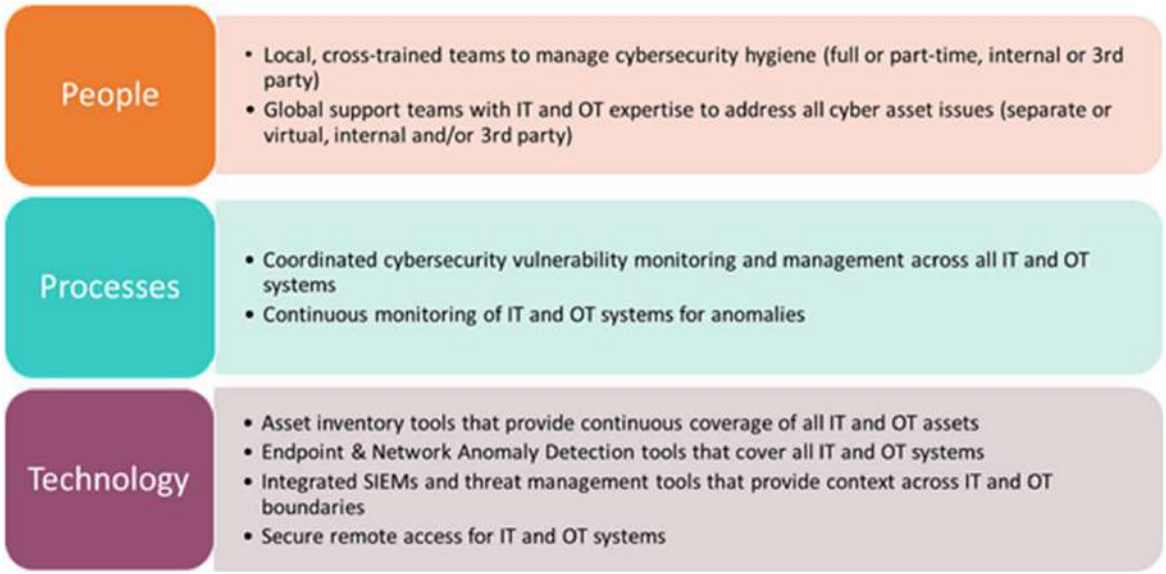
OT has unique requirements that the IT world may not understand (control loops, determinism, response times, message complexity, sensors, etc.)

The OT level lacks a comprehensive understanding of cybersecurity and the accompanying risks of adopting new IoT technology

Many technology departments at the OT level are being merged with IT, either whole or in part, which creates more challenges

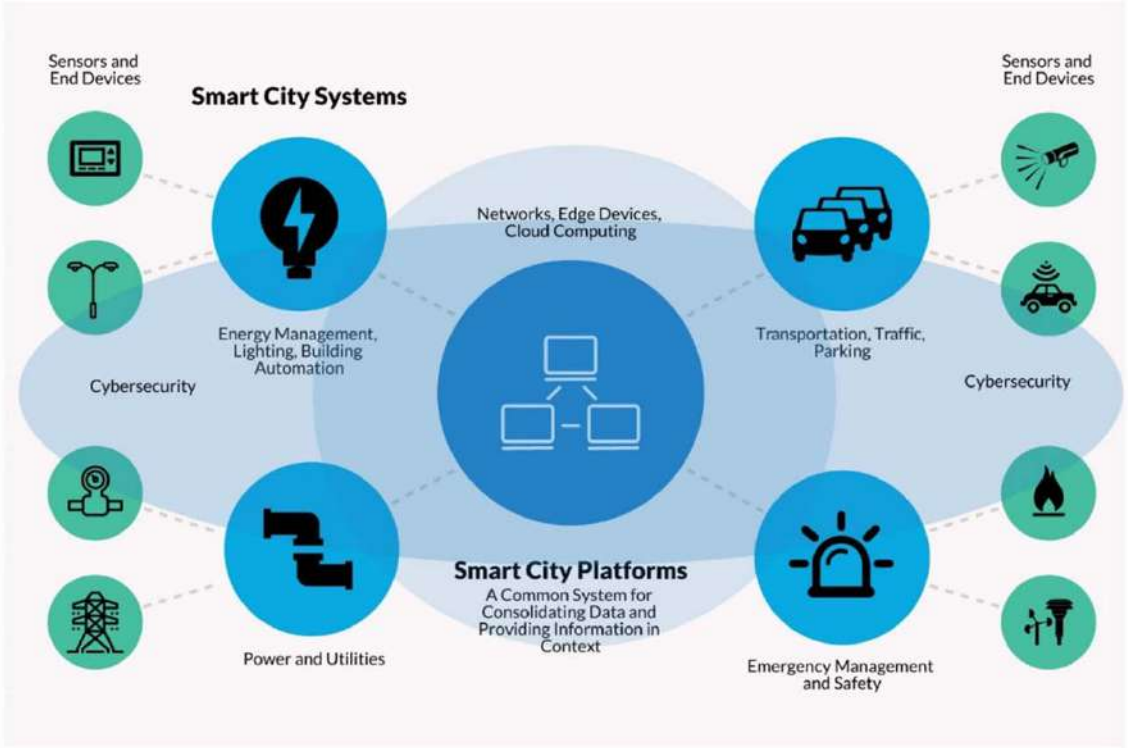
© ARC Advisory Group

IT/OT Convergence Requires Coordination of Cybersecurity Functions and Training



© ARC Advisory Group

Example of IT/OT Convergence: Smart City Platforms



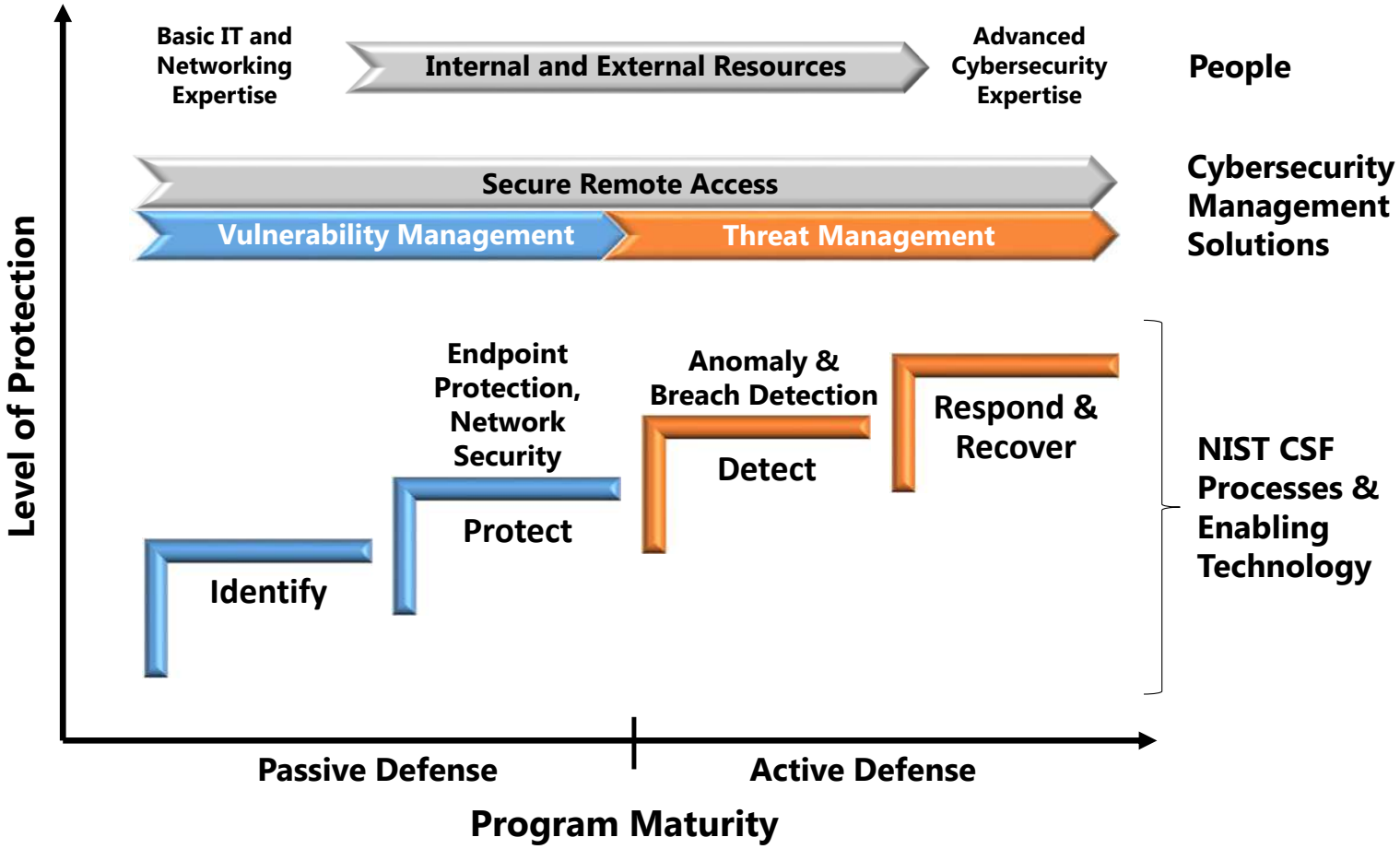
Smart City Platforms Can Seamlessly Combine Data from Multiple Smart City Systems

© ARC Advisory Group • 25

Threat Response and Mitigation

		Mitigation Focus		Mitigation Scope – Types of Attack Risks that May be Reduced					
				Insider Threats			External Threats		
	Mitigation Method	Reduce Likelihood	Reduce Impact	Misuse of Privileges	Insecure Protocol Exploit	Malware Intrusion	Misuse of Privileges	Insecure Protocol Exploit	Malware Intrusion
Secure	Physical Security	x		x	x	x	x		x
	Security Practices	x		x		x	x		x
	Access Control	x		x		x	x		x
	Asset Inventory	x				x			x
	Device Hardening	x				x			x
	Device Management	x				x			x
Defend	Perimeter Firewall(s)	x							x
	Unidir Gateway	x	x			x		x	x
	IDS/IPS	x				x			x
	Access Control	x		x			x		
	Anti-Malware SW	x				x			x
Contain	Zone Firewalls	x	x		x	x		x	x
	Device Firewalls	x	x		x	x		x	x
	App Whitelisting		x			x			x
Manage	Breach Detection		x	x		x	x		x
	Incident Management		x	x	x	x	x	x	x
	SIEM/Remediation		x	x		x	x		x
Anticipate	Threat Intelligence	x				x			x

ARC Industrial Cybersecurity Maturity Model



© ARC Advisory Group • 27

IoT Cybersecurity Standards and Efforts

- NIST Cybersecurity for IoT Program: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Cybersecurity-for-IoT-Program/images-media/NIST%20Cybersecurity%20for%20IoT%20Program.pdf
- ISO 27000 Series of Standards: ISO/IEC 27030 — Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT): https://www.iso.org/standard/44373.html
- IoT Security Foundation: www.iotsecurityfoundation.org
- US Federal Trade Commission (FTC): Building Security into the Internet of Things (FTC is working with NIST also): https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

IIoT Cybersecurity Standards Efforts

- **Industrial Internet Consortium:** The Industrial Internet Consortium's Security Working Group was created to develop a common security framework and a rigorous methodology to assess security in Industrial Internet Systems. This is a direct reflection of the high priority placed by Industrial Internet Consortium members on collaboratively building a safe, reliable and secure Industrial Internet.

TASK GROUPS

The **Automotive Security Task Group** seeks to engage with automotive and transportation verticals, focusing initially on the Connected Vehicles Task Group to provide guidance on topics related to trustworthiness, including safety, security, reliability, privacy, resilience and others. **Chair:** Sven Schrecker, LHP Engineering Solutions; Riaz Zolfonoon, RSA

The **Security Applicability Task Group** is focused on applying Industrial Internet Consortium Security and Trustworthiness to real world situations. **Co-chair**: Ron Zahavi, Microsoft; James Clardy, NetFoundry

The **Testbed Security Task Group** is responsible for applying the security best practices and processes defined within the Security Working Group documents to IIC testbeds. **Co-Chairs:** Jesus Molina, Waterfall Security; Vyacheslav Zolotnikov, Kaspersky Lab; Suresh Damodaran, The MITRE Corporation

The **Trustworthiness Task Group** explores aspects of trustworthiness relevant to the IIoT and the IIC's vision of an IIoT ecosystem. Trustworthiness is the degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks. **Co-Chairs:** Marcellus Buchheit, Wibu-Systems; Frederick Hirsch, Fujitsu; Bob Martin, The MITRE Corporation

© ARC Advisory Group • 29

ISO 27000

Standard	Description	Activity
27037 [11]	Guidelines for identification, collection and/or acquisition and preservation of digital evidence	*Respond, Identify, Collect, Acquire, Preserve*
27038 [14]	Specification for digital redaction	*Report, Close*
27040 [15]	Storage security	*Collect, Preserve, Close*
27041 [12]	Guidance on assuring suitability and adequacy of investigation methods	*All activities*
27042 [16]	Guidelines for the analysis and interpretation of digital evidence	*Understand, Report, Close*
27043 [17]	Investigation principles and processes	*All activities*

© ARC Advisory Group • 30

OT Level Cybersecurity Efforts

- ISA 62443
- NIST Cybersecurity Framework
- UL 29000
- NERC CIP

© ARC Advisory Group

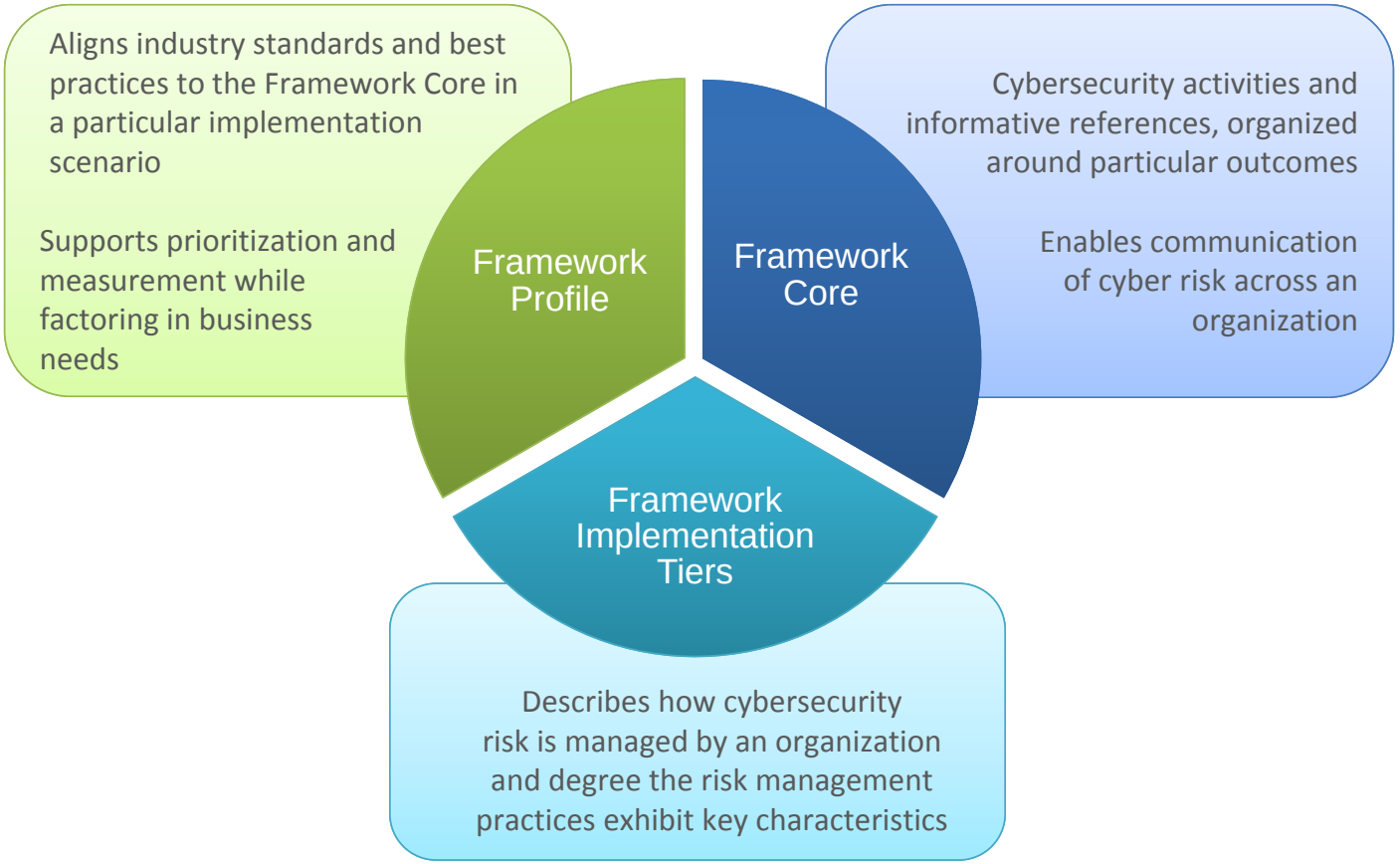
NIST Cybersecurity Framework (CSF)

NIST Cybersecurity Framework

- The US Commerce Department's National Institute of Standards and Technology (NIST) has received considerable recognition over the past few years for developing the Cybersecurity Framework (CSF), now widely used as the basis for establishing effective security management systems.

© ARC Advisory Group • 32

Cybersecurity Framework Components



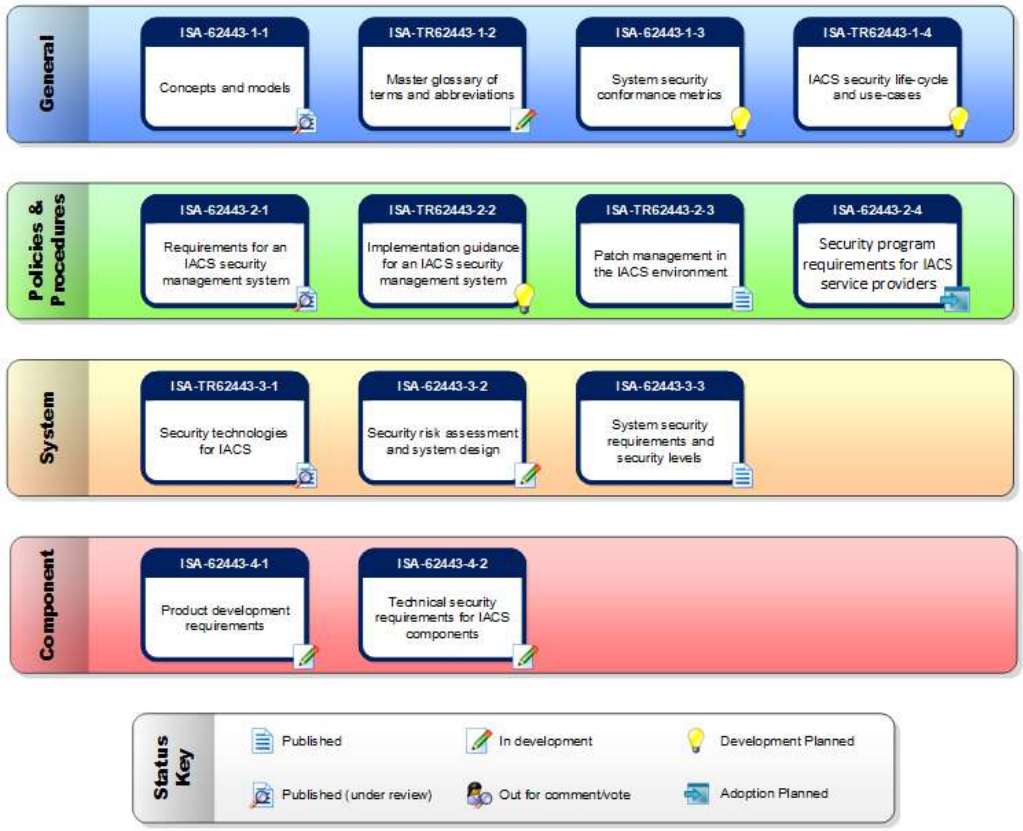
© ARC Advisory Group • 33

NERC CIP

NERC CIP Requirements – 23/49 Requirements Covered

CIP – 002	CIP – 003	CIP – 004	CIP – 005	CIP – 006	CIP – 007	CIP – 008	CIP – 009	CIP – 010	CIP – 011
BES CYBER SYSTEM CATEGORIZATION	SECURITY MANAGEMENT CONTROLS	PERSONNEL AND TRAINING	ELECTRONIC SECURITY PERIMETER	PHYSICAL SECURITY OF BES	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING AND RESPONSE PLANNING	RECOVERY PLANS FOR BES CYBER SYSTEMS	CONFIGURATION CHANGE MGMT AND VULNERABILITY	INFORMATION PROTECTION
1. Risk based assessment method (RBAM)	1. Cybersecurity policy	1. Awareness	1. Electronic Security Perimeter	1. Security Plan	**1. Ports and services**	**1. Cybersecurity incident response plan**	1. Recovery plans specifications	**1. Configuration change mgmt processes**	1. Information protection process
2. Apply RBAM	2. Leadership	2. Training	**2. Visitor Access Control**	2. Visitor access control plan	**2. Security patch management**	**2. Implement and test incident response plans**	**2. Recovery plan implementation testing**	**2. Configuration monitoring**	2. BES Cyber Asset Reuse and Disposal
3. Identify critical assets	3. Exceptions	3. Personnel Risk Assessment	**3. Monitoring Electronic Access**	3. Maintenance and testing program	**3. Malicious software prevention**	3. Incident response plan review and communication	3. Recovery plan review and communication	**3. Vulnerability assessment**	
4. Annual Approval	**4. Information Protection**	**4. Access**	**4. Information Protection**	4. Physical access controls	4. Security event monitoring		**4. Backup and restore**		
	5. Access Control		**5. Access Control**	5. Monitoring physical access	**5. System access controls**		5. Testing backup media		
	6. Change Control			6. Logging physical access	**6. Security status monitoring**				
				7. Access log retention	7. Disposal or redeployment				
					8. Cyber vulnerability assessment				
					9. Documentation				

ISA/IEC 62443 Cybersecurity Standard



http://isa99.isa.org/ISA99%20Wiki/Home.aspx

© ARC Advisory Group • 35

IEC 62443 IACS Lifecycle Overview

ASSESS

Key Standard: ANSI/ISA-62443-3-2

- High-Level Cyber Risk Assessment
- Allocation of IACS Assets to Security Zones or Conduits
- Detailed Cyber Risk Assessment

IMPLEMENT

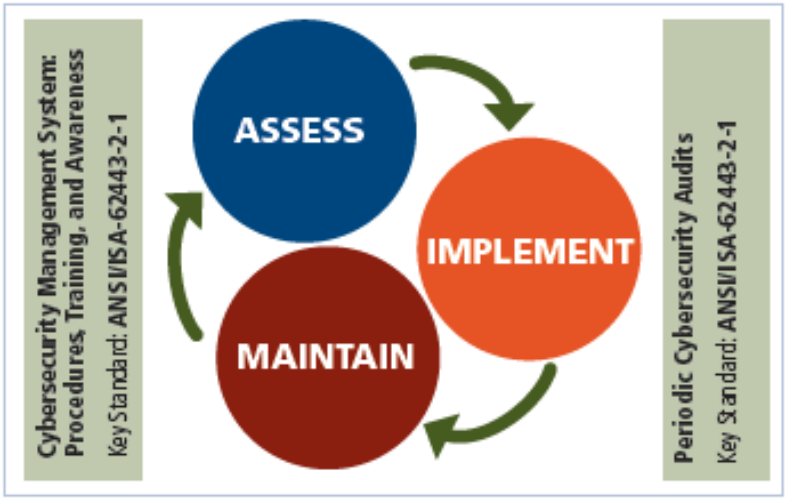
Key Standards: ANSI/ISA-62443-3-2 and ANSI/ISA-62443-3-3

- Cybersecurity Requirements Specification
- Design and Engineering of Cybersecurity Countermeasures
- Design and Development of Other Means of Risk Reduction
- Installation, Commissioning, and Validation of Cybersecurity Countermeasures

MAINTAIN

Key Standard: ANSI/ISA-62443-2-1 (last published as ISA-99.02.01-2009)

- Cybersecurity Maintenance, Monitoring, and Management of Change
- Cyber Incident Response and Recovery



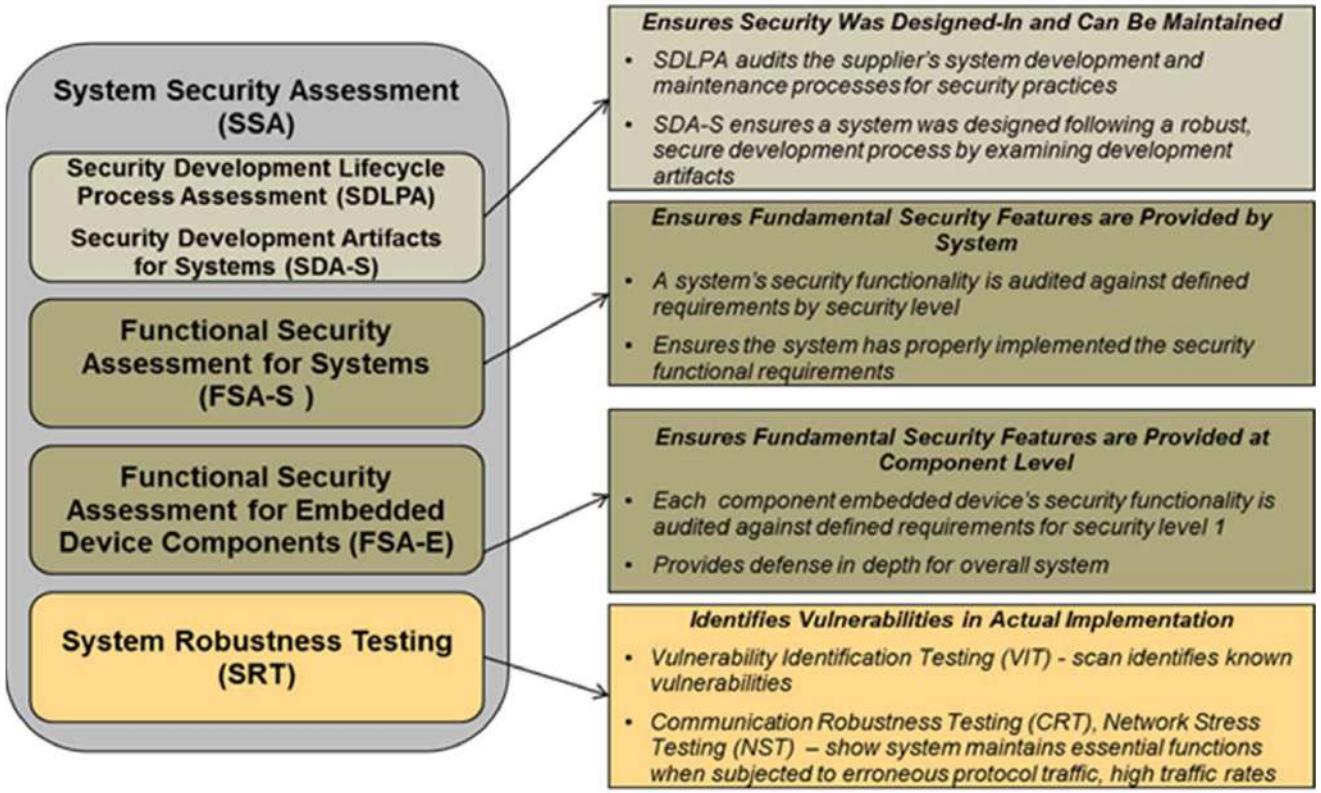
© ARC Advisory Group • 36

ISA Secure Certification

- The ISA Security Compliance Institute (ISCI), a neutral, not-for-profit consortium manages the ISASecure certification process.
- ISASecure certifications assess conformance to a subset of the IEC 62443 series.
- ISA-Secure certifies commercial-off-the-shelf (COTS) products and product supplier development lifecycle practices, for conformance with applicable parts of the IEC 62443 series.
- ISASecure has an initiative with CABA for certifying products for building control system (BCS) applications.

© ARC Advisory Group

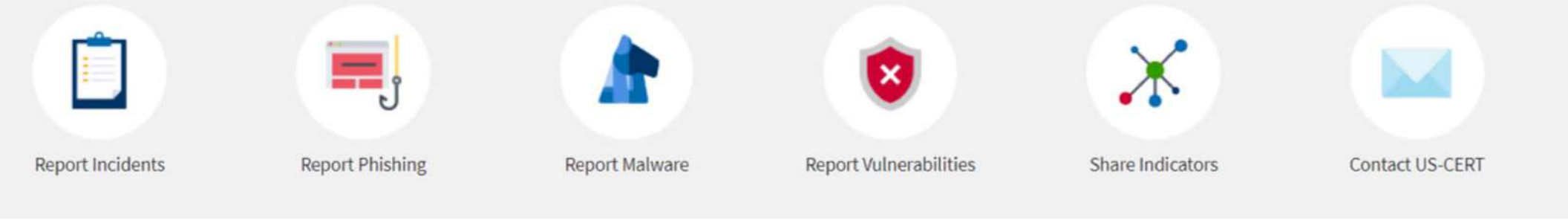
ISA SSA Security Assessment Process



© ARC Advisory Group • 38

DHS/ICSJWG

CISA
CYBER+INFRASTRUCTURE



© ARC Advisory Group

CSET Tool

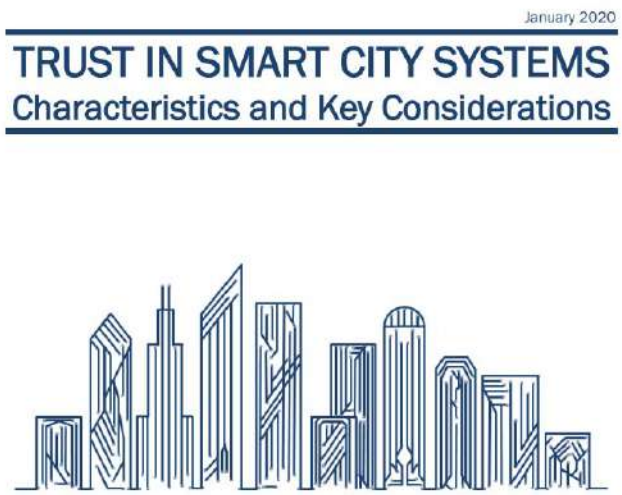
- The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.

- The CSET Download has moved to GitHub: https://github.com/cisagov/cset/releases

- You can also find older legacy versions of the software on GitHub.

© ARC Advisory Group

CISA "Trust in Smart City Systems" Report



- https://www.cisa.gov/publication/trust-smart-city-systems-report

© ARC Advisory Group

NIST: Smart and Secure Cities and Communities Challenge

- https://pages.nist.gov/GCTC/uploads/blueprints/2019_GCTC-SC3_Cybersecurity_and_Privacy_Advisory_Committee_Guidebook_July_2019.pdf

SMART AND SECURE CITIES AND COMMUNITIES CHALLENGE (SC3)

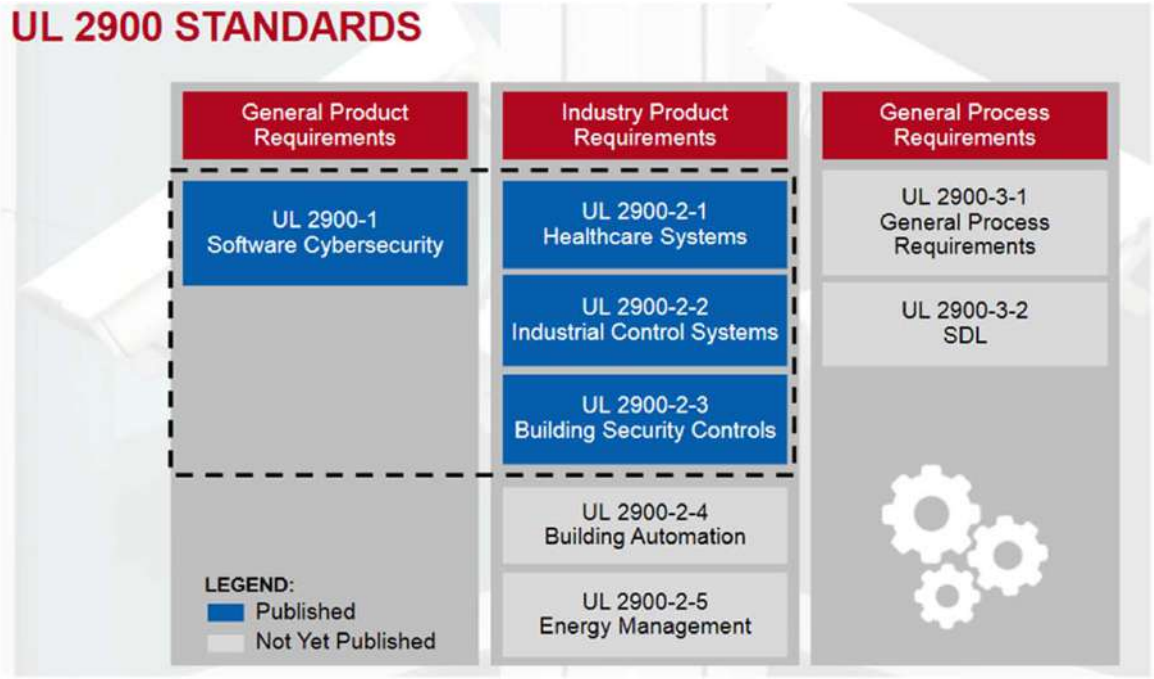
A Risk Management Approach to Smart City Cybersecurity and Privacy

A Guidebook from the
Cybersecurity and Privacy Advisory Committee
(CPAC) Public Working Group

July 2019

© ARC Advisory Group • 42

UL 2900 Series of Standards



UL 2900 Spans a Broad Range of Requirements and Products

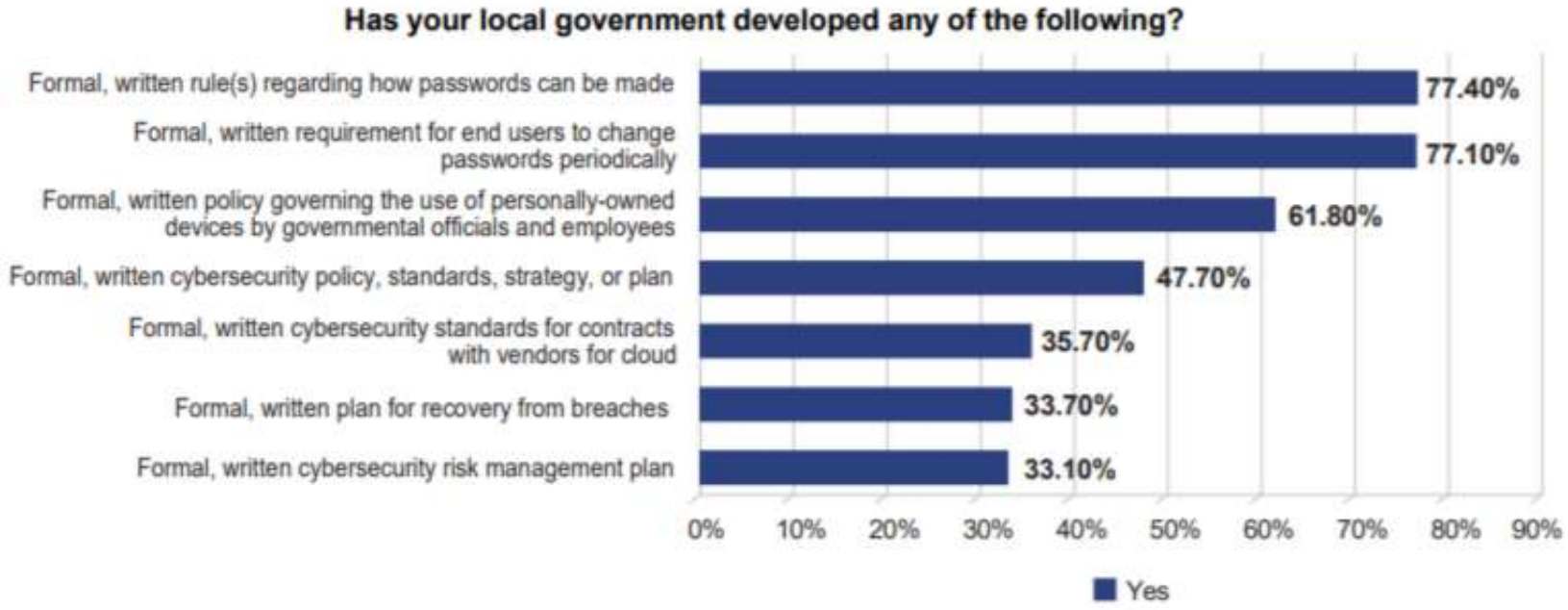
© ARC Advisory Group • 43

Developing Standard Cybersecurity Policy in Your Organization

- Cybersecurity does not equal buying and installing products.
- Having a good cybersecurity strategy does not have to involve huge investments in technology and training. A sound strategy and standard policies can provide significant benefits.

© ARC Advisory Group • 44

Most Smart City Owner/Operators Don't Have Formal, Written Cybersecurity Policies or Standards in Place



(Source: ICMA / UMBC 2016 Survey https://ebiquity.umbc.edu/_file_directory_/papers/881.pdf)

© ARC Advisory Group • 45

You Need A Good Response Plan

- Ransomware provides a good example of the benefit of having sound cyber-security policy and the need for a good response plan. Many owner-operators and city governments are completely caught off guard when they face a ransomware attack.

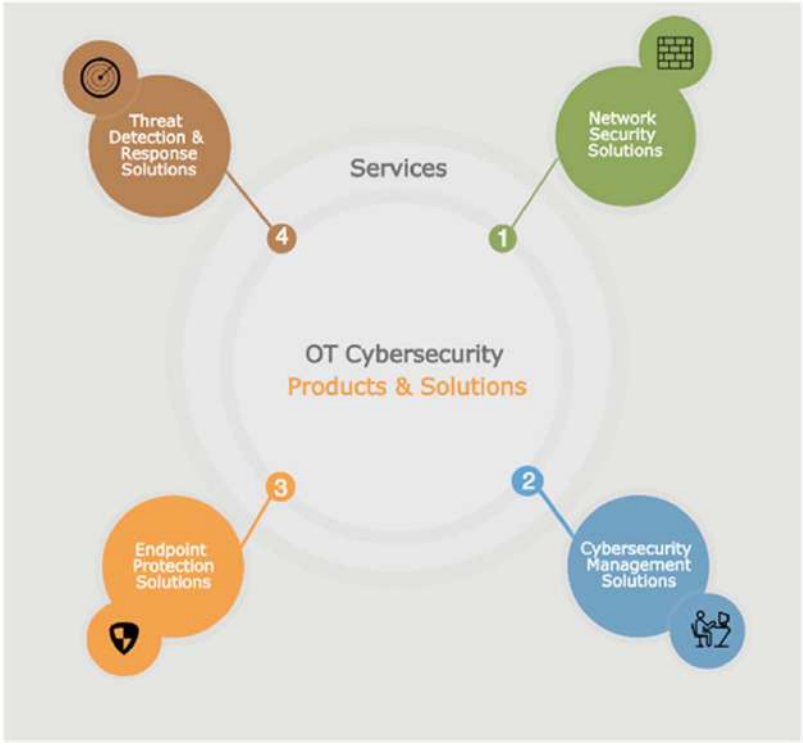
© ARC Advisory Group • 46

Invest in Training

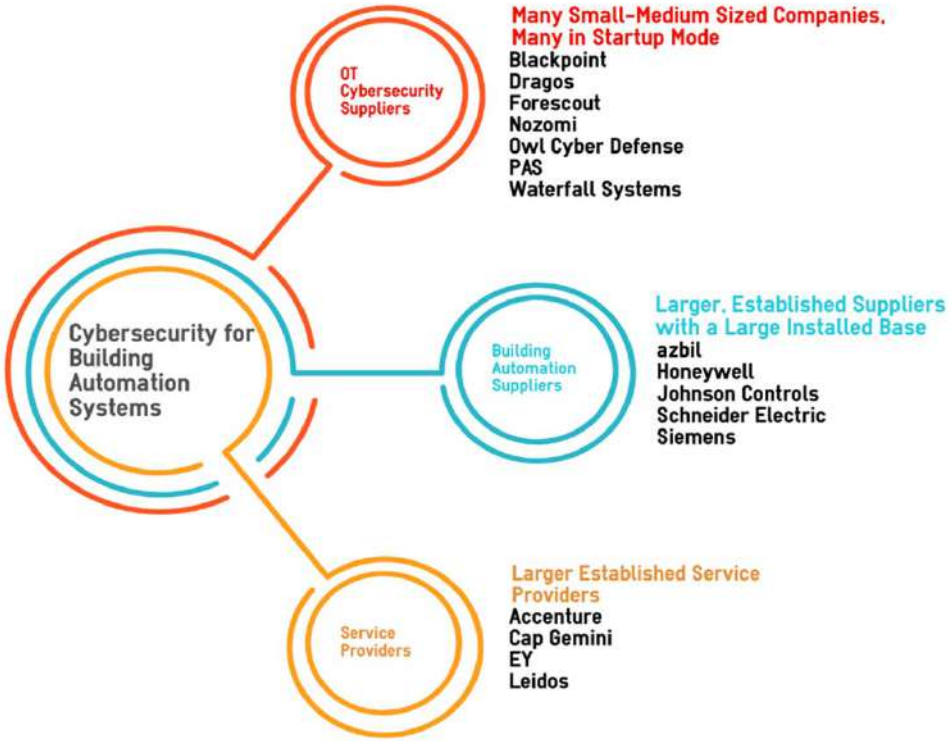
- Industrial cybersecurity solutions have become increasingly sophisticated and can require a high level of cybersecurity expertise to configure and maintain. This will increase the importance of additional vendor support and training programs for the end user.
- Look to SANS as an excellent source of training and certification for ICS and OT level specific cybersecurity certifications, CISSP, GCIA
- ISA, DHS

© ARC Advisory Group • 47

OT Level Cybersecurity Suppliers



© ARC Advisory Group • 48



© ARC Advisory Group • 49

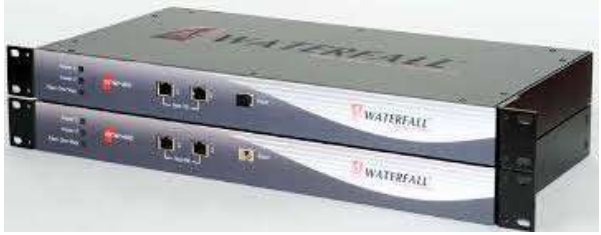
Threat Detection and Response Solutions

- Industrial/OT threat detection and response solutions include a range of products for monitoring OT networks and endpoint assets.
- A distinct segment of the overall threat detection and response solutions market, distinguished by features that address the unique network messages and controllers used in the automation systems that control critical industrial assets and infrastructure.
- **Endpoint Breach Detection Solutions** which continuously monitor endpoint devices
- **Anomalous Message Detection** solutions which monitor message flows within and across industrial networks
- **Threat Management Platforms** that help defenders investigate and manage detected anomalies

© ARC Advisory Group

Network Security Solutions

- **Next-Generation Firewalls (NGFW):** Most of the NGFW used in industrial facilities are hardened versions of those used in office environments. They are provided by the same suppliers that provide firewalls for corporate IT systems.
- **Industrial DPI Firewalls:** Firewalls that can analyze message content for industrial protocols like Modbus and DNP3 are becoming popular in many industrial settings. Plants use them as compensating controls for devices with vulnerabilities that cannot be patched.
- **Unidirectional Gateways and Data Diodes:** These products are generally used in place of NGFW for perimeter protection. They overcome weaknesses in DMZ, NGFW, and VPN approaches to security management commonly used to manage control system connections with enterprise IT systems, remote support offices, and service providers.



© ARC Advisory Group • 51

Endpoint Protection Solutions

- ARC defines industrial/OT endpoint protection solutions as products that actively block compromises to cyber assets within control systems. Technologies in this category include :
- **Anti-Malware Software**
- **Application Whitelisting**
- **Access Control**

© ARC Advisory Group

Cybersecurity Management Solutions

- **Security Management Dashboard** – Central platform for managing all security information about cyber assets, vulnerability alerts, patches, and firmware/software/hardware updates; launchpad and integration platform for a variety of security maintenance support modules.
- **Security Maintenance Support** – modules that enhance staff cybersecurity management capabilities and reduce the time required to perform security maintenance tasks like asset discovery and inventories, change and patch management, backup management and policy compliance.
- **Remote Security Management Support** - Secure remote access software/services that enable remote maintenance of cyber assets and incident response support.
- **Incident Management Support** - Security Information and Event Management (SIEM) and other solutions that manage security event information (alerts, configuration changes, etc.), help people analyze and deal with suspicious situations.
- **NERC Compliance Support** - NERC CIP Compliance Reporting Software

© ARC Advisory Group

Industrial Cybersecurity Services

Service Category	Focus	Suppliers
Assessments	Industrial/OT cybersecurity assessment services generally focus on securing existing facilities. Normal engagements include a review of control system architectures and equipment, processes and people, and identification of weaknesses. Generally high level, but can include detailed evaluations of networks, "hidden" access points, and penetration tests on endpoint devices. Final reports describe risks and mitigation recommendations. Assessment services may also include product and development process evaluations and certifications.	**System Assessments** - Automation system suppliers, Control system integrators, OT cybersecurity companies, IT/OT MSSPs **Product Assessments** – Testing & Certification Groups (TUV, UL, etc.), Niche security companies
Design & Implement	Design and implementation services include developing security strategies; procuring and configuring associated hardware and software; installing equipment and cabling; and configuring authorizations, firewalls, white-listing tools, etc. Developing procedures, incident response plans, business continuity plans, and training staff to use and maintain the new system are also services that may be included in these types of engagements	Automation system suppliers and Control system integrators.
Managed Security Services	Managed security services augment a company's internal capability to sustain defenses, deal with system alerts, and manage cyber incidents. Services in this category include: maintaining ICS system security patches and updates; system monitoring and incident management support; annual security and compliance audits; and training.	**Patches & Updates** - Automation system suppliers, control system integrators, IT/OT MSSPs **Monitoring & Incident Management** – Large MSSPs with OT knowledge, niche OT MSSPs

© ARC Advisory Group • 54

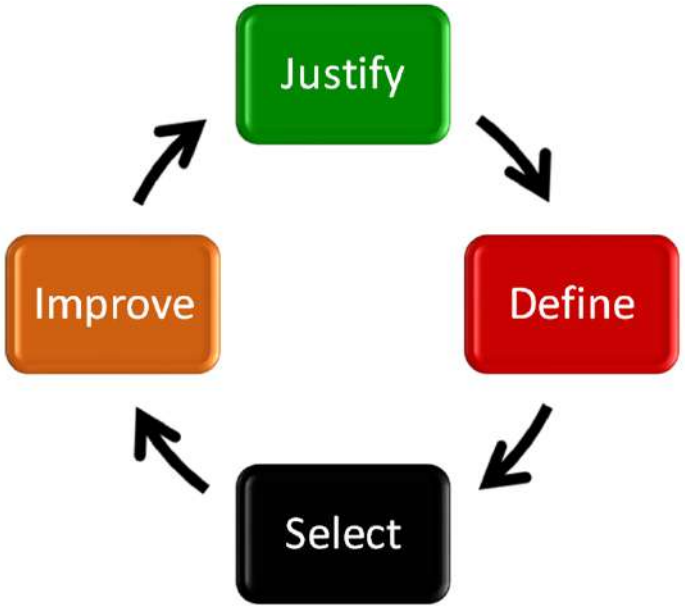
Cybersecurity Vendor Selection

- LOTS of suppliers. Many in the startup stages, with relatively small numbers of customers.
- Will they be around in five years?
- If they get acquired, will the still support you?
- Alliances with OT level suppliers.
- Do they understand the business?
- Product certifications and standards testing.
- Secure development processes

© ARC Advisory Group • 55

Cybersecurity in ICS/OT Vendor Selection

- Many end users don't have a good handle on the landscape of ICS cybersecurity solutions.
- Many end users don't have the right cybersecurity related criteria embedded into their ICS and OT asset selection process.
- "Undocumented" systems and devices currently receive the least amount of attention when it comes to cybersecurity. These obscure systems can include boiler controls, compressor controls, etc.
- Different stakeholders in the organization aren't always involved.



© ARC Advisory Group • 56

Elements of Success for Supplier Selection

- **Have a documentable, traceable, and fact-based selection process that proves how and why you made your decision**
- **Bring key stakeholders together to make a consensus-based decision**
- **Have a basic understanding of the market and the leading suppliers**
- **Make sure you have the right selection criteria**
- **Prioritize/weight criteria, remember that everything is not of equal importance to everything else**
- **The selection process doesn't end with the selection. It transitions into a supplier relationship management process.**

© ARC Advisory Group • 57

Summary and Conclusions

- If you don't already have a cybersecurity program or plan in place at your organization, you should take simple steps to start developing one. This presentation should give you information on the key steps needed to get started and resources.
- Attacks are only going to become more sophisticated and will increasingly target actions in the physical world through compromising complex control systems and OT infrastructure.
- Technology churn is driving a lot of todays cybersecurity challenges. IoT technologies used in an OT level environment need to be carefully vetted for cybersecurity risks, secure by design principles, etc.
- The smart city and smart building segment needs to adopt standards. ISA/IEC 62443 should seriously be considered as the standard of reference.
- Cybersecurity must be driven into the overall supplier selection process for all OT level systems and products.
- Consider development of standard cybersecurity policy and response plans in your organization.

© ARC Advisory Group • 58

Resources

- https://www.arcweb.com/consulting-services/cybersecurity-workshops
- https://www.arcweb.com/blog/cybersecurity-viewpoints
- https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/
- https://www.nist.gov/topics/cybersecurity
- https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center
- https://www.sans.org/netwars/cybercity

© ARC Advisory Group

Thank You

- Questions?

Larry O'Brien

lobrien@arcweb.com
@dcsanalyst
@smartcityvwpts

© ARC Advisory Group