ISASecure Web Conference

Industrial Control System Cybersecurity - Equipment Supplier Perspective

Dan DesRuisseaux – Cybersecurity Program Director

10/12/2020

ISASecure®

About the Speaker

- **Dan DesRuisseaux**
- **Industrial Automation Cybersecurity Program Director**
- **Dan DesRuisseaux** possesses over 25 years of diverse experience in engineering, sales, and marketing roles in high tech companies. Mr. DesRuisseaux presently serves as the Cybersecurity Program Director for Schneider Electric's Industrial Division where he works to ensure the proper and consistent implementation of security features across SE's diverse product portfolio. Mr. DesRuisseaux is also the marketing Chairman of the ISA Security Compliance Institute - a non-profit organization seeking to improve ICS security through standards compliance.

ISA Security Compliance Institute

About the Speaker

- **Kevin Staggs**
- **Senior Fellow**
- **Kevin Staggs** possesses over 43 years of experience in hardware, software and systems engineering at Honeywell with 39 years focused on control systems. Mr. Staggs has been driving product cybersecurity development since 1996. Mr. Staggs is currently a Senior Fellow in Honeywell's Advanced Connected Technology Solutions organization and serves as a cybersecurity consultant to Honeywell's product development organizations. Mr. Staggs currently serves as co-chairperson of ISA99 working group 4 and is also the technical Chairman of the ISA Security Compliance Institute - a non-profit organization seeking to improve ICS security through standards compliance.

ISA Security Compliance Institute

How Does a Vendor Prioritize Cybersecurity Features - Cybersecurity Drivers

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Americas: Examples of Laws/Frameworks

Law	Description	Area
SB327 – California Connected Device Law	Reasonable security required for connectable devices	California
House B 2395 – Oregon Connected Device Security Law	Similar to SB327, adds Bluetooth. Focuses on consumer products.	Oregon
National Defense Authorization Act	Implications for supply chain, acquisition reform, cybersecurity, 5G, and artificial intelligence	US
NIST Privacy Framework	NIST development of a federal privacy framework.	US
Executive Order 13873 / Executive Order on Bulk Power Systems	Executive order on bulk power distribution supply chain impacting products and services doing business with "foreign adversary“	US
Secure and Trusted Communications Networks Act of 2019 (HR 4998)	Promotes secure 5G deployment by excluding Chinese providers and establishing a Supply Chain Security Trust Fund	US
DoD Cyber Maturity Model Certification (CMMC)	Procurement standard that will require all Defense Industrial Base companies to be certified.	US

There are 30 pending actions underway that could impact cybersecurity features and policies.

ISA Security Compliance Institute

EMEA: Laws & Frameworks in Effect

Law	Description	Area
BSI	IT Security Act to prevent breakdowns of critical infrastructure. Targets facilities. health, finance and insurance, transport and traffic sectors.	Germany
ANSII CSPN	Product security validation and certification is critical	France
Cybersecurity Act: EN 303 645 - IOT	This standard is the new IOT regulation in EU. Based on ETSI TS 101 645.	EU
Low Voltage Directive Revision	Targets electrical equipment within certain voltage limits to ensure protection for European citizens. Applicable since 20 April 2016.	EU
Cybersecurity Act	Provides resources and responsibilities for the European Union and provides a framework for the development of cybersecurity certification schemes.	EU
FSTec	Compulsory requirement that certify the conformity of components to Russian Industrial Cyber Security standards.	Russia
Yemen Cybersecurity Law	Strategic Vision for Telecommunication and Information Technology in Support of Integrated Development Plans in Yemen	Yemen
Cyber Resilience Upgrade	Standards driving government agencies to upgrade security, including cloud computing and industrial control systems	Saudi Arabia

There are a variety of pending actions underway that could impact cybersecurity features and policies.

ISA Security Compliance Institute

APAC Summary: Laws and Frameworks in Effect

Law	Description	Area
SCA 38, SCA 39 NN	China cryptography law. Import and export licensing system for commercial cryptography.	China
Cybersecurity review measures	Government organizations may require security reviews for critical infrastructure.	China
Cybersecurity Protection Scheme for Critical Information Infrastructure	Product requirements for MLPS system (similar to IEC 62443-4-2) for critical information.	China
GB/T 35273-2020 - Data Privacy	Data privacy requirements – personal inform.	China
Indian Ministry of Power Order	Mandates all imported products used in a power supply network to be tested and certified in India for any kind of malwares or cyber threats.	India
Cybersecurity Law No. 24/2018/QH14	Cybersecurity requirements.	Vietnam

Variety of pending actions underway in Japan, Australia, India, Thailand, and Singapore that could impact cybersecurity features and policies. Actions cover a wide range of topics, including supply chain, IoT, data privacy, and security policy.

ISA Security Compliance Institute

Regulatory Summary

Impact of the regulatory driver is likely to be a major influencer of cybersecurity features/policies in the near term. Regulatory demand leads to customer demand.

Regulatory disharmony in place today – no foreseeable change in near term

- 11 different state in the US with varied definitions and requirements
- Multiple standards being created in China, relationship between standards unclear

Cyber-nationalism likely to drive independent country/regional standards over acceptance of international standard. Focus in on secure supply chain.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Customers Demanding Secure Offers

Customers expect a secure offer, they are beginning to demand compliance to cybersecurity standards.

Customers demand for cybersecurity is dependent on the offer.

- DCS, safety system, PLC customers require cybersecurity functionality, some require compliance certification.
- Drives, HMI, relays, protocol converters, etc. might require cybersecurity functionality. Currently these offers are not required to obtain compliance certification.

Customers are including cybersecurity in specifications

- Large customers have dedicated specifications which may be derived from in house standards.
- Small customers typically provide abbreviated cybersecurity specifications.
- Many reference industry standards such as IEC-62443.

ISA Security Compliance Institute

Example of ICS Customer Requirements

Project	IEC 62443 Requirement	Other Security Requirements	Additional Points
DCS System	Compliance to IEC 62443-1-1, 2-1, 2-3, 2-4, 3-1, 3-2, and 3-3. Target SL2.	• IEC 17799 risk assessment guidelines • GS EP INS 135 • IEC 61511 Functional safety • Country regulations and standards	• Support OPC UA MDIS specification. • Standard SIEM offering. • Integration of IEC 61850 with ICSS network.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Offer Managers Monitor Competitive Offers

Most offers have some level of cybersecurity functionality.

- Certification to an IEC 62443 security level represent a major step to differentiate an offer from competitors.
- Approximately 25 IEC 62443 certified offers: majority 4-2 certified, 2 certified systems per 3-3.
- Majority of certified offers are SL-C 1, newer products obtaining SL-C 2.

Historically, competitive positioning has been the key driver propelling offer certifications. That is starting to change with increased customer demand and looming regulatory requirements.

As a result the rate of certified offers have steadily increased over time, we expect continued acceleration.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Equipment Suppliers Typically have Internal Cybersecurity Requirements

Companies institute internal cybersecurity requirements and policies.

Equipment suppliers have internal requirements as they recognize the potential implementation risk.

- Specified in Marketing Requirements documents and Technical Specifications.
- Internal documents ensure that features are available across a platform, that they are interoperable, and they provide a similar user experience to customers.

Companies can also leverage external requirements – OWASP web and IEC-62443 are examples.

ISA Security Compliance Institute

Equipment Suppliers Have Also Implemented Cybersecurity Policies to Drive Secure Processes

Examples of cybersecurity processes

- Secure development lifecycle utilization
- Vulnerability management
- Security testing policies
- Data privacy
- Vendor security assessment

Defined in IEC-62443-4-2 and suppliers are being certified to be compliant.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Threat Intelligence Can Drive Offer Requirements

Advanced Persistent Threat (APT) - A stealthy threat actor that gains unauthorized access to a computer network and remains undetected for an extended period of time. Motives include intelligence gathering and potential sabotage.

Vendors typically subscribe to threat intelligence platforms which provide APT details that can be used to harden offers.

Analyzing APTs can highlight features that can be implemented to mitigate attacks. Threat intelligence can lead to internal policy development, leading to new internal requirements.

Major APTs impacting industrial control systems include:

- Allanite, Palmetto, Fusion
- APT33, Elfin, Magnallium
- Dragonfly, Energetic Bear
- Dragonfly 2.0, Beserk Bear, Dymalloy
- Hexane, Lyceum

ISA Security Compliance Institute

APT Example - Dragonfly 2.0, Beserk Bear, Dymalloy

A threat group targeting the energy sector located in the United States, Switzerland, and Turkey.

Techniques Used

- Spear Phishing Attachment – Used the Phishery tool kit to conduct attacks to gather credentials.
- Supply Chain Compromise - Trojanized software to deliver malware disguised as standard windows applications.
- Drive-by Compromise - Utilized watering hole attacks to gather credentials by compromising websites that energy sector organizations might access.
- Valid Accounts - Used credentials collected through spear phishing and watering hole attacks.

Features to Counter APT

- Supply Chain Compromise - Firmware signing, code signing, device genuiness, and secure boot.
- Valid Accounts - IDS system secure syslog, centralized RBAC, secure configuration.
- Drive-by Compromise - Internal IT policies.
- Spear Phishing - Internal policies and training.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Cybersecurity Insurance Coverages

Risk can be addressed via Tolerate, Terminate, Treat, or Transfer strategies. Transfer involves transferring risk to an external entity - which can be insurance.

Traditional Cybersecurity Insurance Coverage

Third Party

- Privacy injury liability
- Network security liability
- Regulatory fines/penalties
- Media liability

First Party

- Incident response expenses
- Network loss or damage
- Bricking
- Network business interruption
- System failure
- Cyber extortion

OT-Relevant Cybersecurity Insurance Coverage

- Property damage
- Cyber bodily injury
- Failure to supply
- Spot market coverage
- Regulatory shutdown
- Voluntary shutdown
- Reputational loss

What is Not Usually Covered

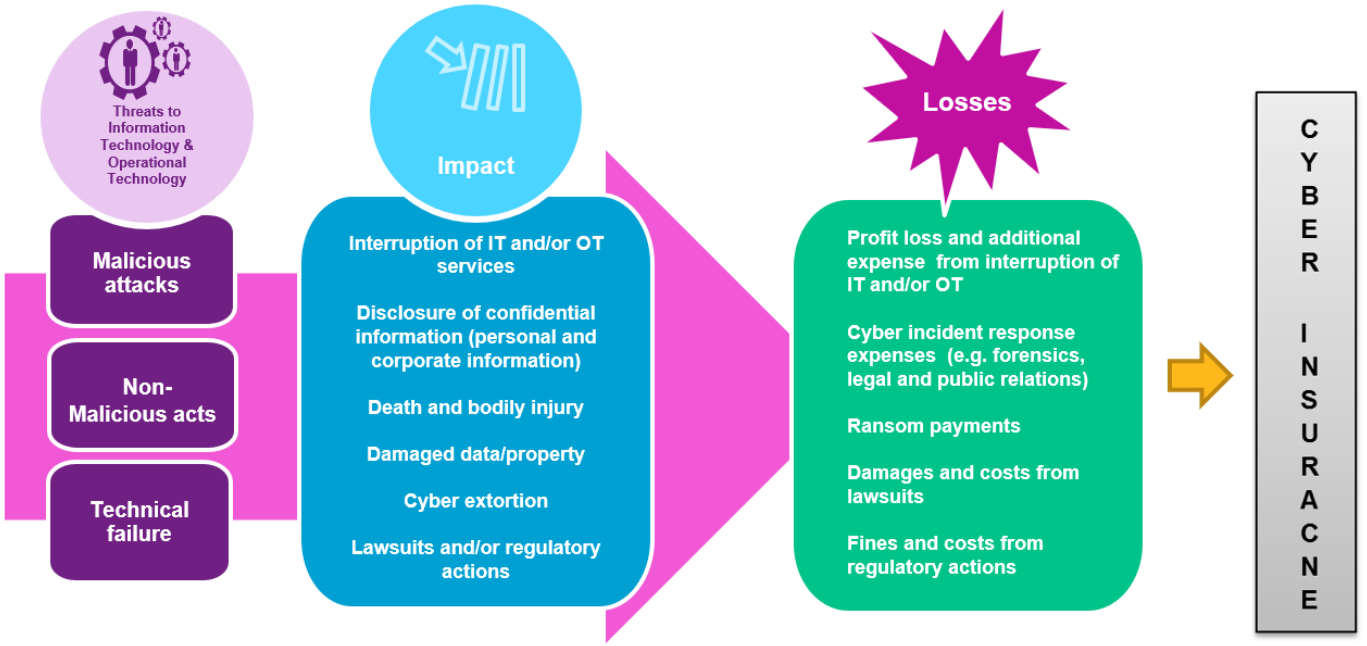
- Potential future lost profits
- Loss of value due to theft of intellectual property
- Cost to improve technology, including software or security upgrades after a cyber event
- Ransomware attacks (considered an act of war)

ISA Security Compliance Institute

OT Cyber Risk as Business Risk

The application, underwriting, and renewal process can improve security by driving discussions between the insurance company, the insured party, and associated vendors about how to best prevent or reduce cyber loss impacts. Cybersecurity insurance covers a percentage of losses that businesses incur after an attack.

There are no standard cybersecurity insurance policies – policies are sold à la carte.



Cybersecurity Insurance Can Lower Cyber Risk

Coverage assessments help companies discover cyber risks. Conditional coverage drives clients to address gaps to obtain coverage on desirable terms. The more OT companies undergo the underwriting process, the sooner relevant OT cybersecurity baselines will emerge to define effective practices.

Policy renewal is "reward time" for clients who effectively manage cyber risk.

- Companies that have not experienced significant cyber incidents or have minimized losses by responding and recovering quickly.
- Access to meaningful cybersecurity insurance at affordable rates becomes a motivator to continuously improve cybersecurity performance.
- Assessing progress against key cyber risks over the prior coverage year becomes an opportunity to update cybersecurity strategy on a regular basis.

Cybersecurity Insurance Summary

The cyber insurance market is growing – it is targeted to achieve 26.3% CAGR between 2020 and 2030 (PMS Market Research).

Insurance cybersecurity baselines are in the process of being defined. Asset owners are likely to overpay until insurers gather more data and define baselines.

The cyber insurance will be a major driver in the intermediate term. Mature baselines will drive asset owner security feature and policy requirements in RFPs.

ISA Security Compliance Institute

AGENDA

1	Regulatory
2	Customer Demand
3	Competition
4	Internal Policy
5	Threat Intelligence
6	Cybersecurity Insurance
7	Conclusions

Conclusions

Equipment vendors have been driving cybersecurity requirements and certifications.

Customer demand and regulatory drivers are beginning to impact cybersecurity requirements.
Requirements are focused primarily on controllers and control systems.

- Cyber-nationalism likely to drive independent country/regional standards over acceptance of international standard.

Cyber insurance will be a major driver in the intermediate term, insurance baselines are coming.

ISA Security Compliance Institute