ICS SECURITY MANAGER AS A SERVICE

by
Isiah Jones, MPS, CISSP, GICSP, C|CISO
Director, ICS Cyber Security Engineering
LEO Cyber Security

ICS SECURITY MANAGER AS A SERVICE

OVERVIEW

As ICS assets and operations increasingly become the targets of opportunity it is important that new strategies and ideas for focused and tailored security approaches are introduced to the community. ICS security manager as a service can enable the community to contract skilled resources for a new role dedicated solely to securing ICS within resource constrained operations staff for ICS asset owners and operations of some of the world's most critical infrastructures operated, monitored and controlled by automation and control systems. The ICS Security Manager as a Service is like CISO as a Service on the IT side of the house with respect to building a security program. However, unlike the CISO as a Service, the ICS Security Manager as a Service is intended to be a more technical, hands-on role as well. Examples of duties and tasks the ICS Security Manager would perform as a service are: leading, coordinating and implementing day to day security tasks such as building ICS system security plans, inventory lists and testing products and services for ICS operators' operations and assets. Such a service would most benefit ICS owners and operators who cannot afford a full-time resource within their staff. Some example asset owners and operators would be electric cooperatives, municipalities, and small businesses that own and operate pipelines, water and wastewater plants and hydro dams.

ICS SECURITY MANAGER AS A SERVICE

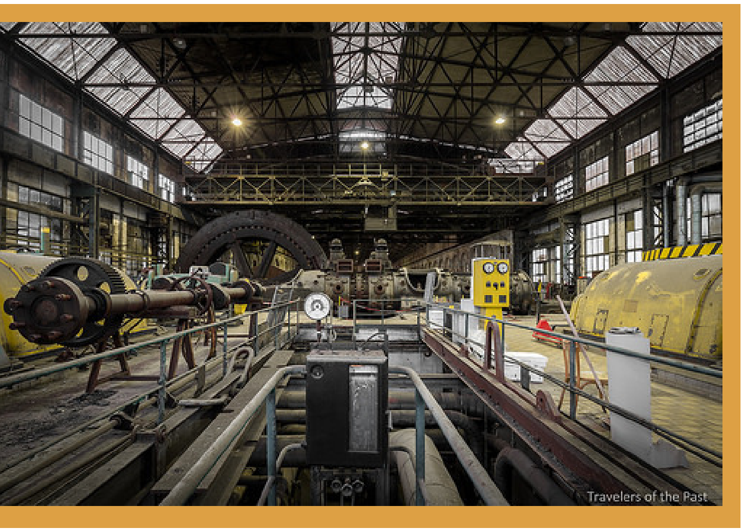
In my travels over the last four years, I've consistently encountered the same old tragedy over and over again regardless of what type of critical infrastructure asset type or sector vertical it was and regardless of what state, nation, continent, company and or military base it was. That tragedy was constantly connecting with and trying to support engineers and other personnel building security into active in-flight projects for both existing and new infrastructure monitored and controlled by some type of industrial automation and or control system device, network, protocol, system and or application.

I usually found many issues within contracts, cultures and understanding of system design, integration, system configurations, validation, testing, requirements specifications and contract language or systems security engineering principles in general. I also consistently found very small teams, mostly a team of one on the ICS side and a team of totally ill-informed bull in the china shop folks on the IT teams. In other cases, I found teams of impossible to work with engineers and desperately anxious IT staff. One day on a project it hit me: why do I continue to create templates, steps and solutions and share them with folks who either don't have the time to implement and maintain them, aren't interested in the first place or honestly have no idea what it is that I just provided them? Why don't I just complete the task for them, show them how I did it, show them how to maintain it then periodically return to make sure it is maintained? Thus, the idea for ICS Security Manager as a Service was born in my head at the time.

ICS SECURITY MANAGER AS A SERVICE

WHAT IS IT?

The easiest way for both the ICS and cybersecurity communities to wrap their heads around what the heck ICS Security Manager as a Service is would be to initially think of the ICS focused version of CISO as a Service only with additional duties that include hands-on technical engineering and architecture work. Some folks may see it as just another name for staff augmentation. However, staff augmentation implies a permanently contracted individual who essentially belongs to your organization as a contracted employee. Basically, they are simply just another extension to your pool of contractor employees. In some respects, ICS Security Manager as a Service is like a combination of CISO as a Service business models and traditional staff augmentations.


Travelers of the Past

However, ICS Security Manager as a Service would not be a staff augmentation contractor employee position. Instead, it would be like having a firm of experienced lawyers on constant retainer whenever you needed them. They act on your behalf and look out for your interests, they know your organization and your secrets and not only advise you but can also take action up to and including representing you in court or taking legal actions on your behalf. In that spirit, ICS Security Manager as a Service would be a fractional, part-time, half-time or full-time scaled pricing-based retainer service that would provide asset owners with access to seasoned ICS Security professionals when they need them to perform various tasks on their behalf.

ICS Security Manager as a Service could be called upon to write security specifications and specific security controls and sub controls into ICS Master Plans, RFPs, RFIs, contract agreements, design guidelines, roadmaps throughout the lifecycle of your existing and new ICS assets and operations. The service could also include building out your inventory lists, architecture design, testing labs, systems security plans for each system, configuration plans and guides for each system and conducting evaluations of ICS vendor and integrator products and solutions on behalf of the asset owner and operator.

> In some respects, ICS Security Manager as a Service is like a combination of CISO as a Service business models and traditional staff augmentations.

ICS SECURITY MANAGER AS A SERVICE

Some of the duties and tasks this service could complete and maintain are as follows (this is not an exhaustive or complete list):

- Build, operate and maintain ICS Security Program (this includes policies, procedures, frameworks, regulations, standards and best practices)
- Act as ICS Security Manager on behalf of asset owner and operator (this includes authority to oversee and direct ICS vendors, integrators, staff and contractors)
- Serve as liaison between ICS business owners and IT staff and corporate leadership (e.g. CIO, CISO, COO)
- Coordinate, evaluate and execute annual ICS focused assessments
- Coordinate, evaluate and execute annual ICS focused penetration tests

  Lead, support and execute implementations to mitigate discovered risks and vulnerabilities for ICS assets and operations
- Integrate, create and enforce ICS security requirements, standards, best practices and functionality into all ICS projects, contracts, agreements, operations and assets on behalf of asset owners and operators
- Build, maintain and execute ICS system security plans, ICS configuration management plans, ICS inventory list, ICS incident response plans, ICS system, network and architecture diagrams, etc.
- Test, evaluate, authorize, certify and facilitate products and services used by and for ICS assets and operations on behalf of owners and operators
- Enable and deliver ICS focused security training and awareness for ICS operators and supporting stakeholders (physical security, HR, finance, procurement, IT, vendors, integrators, EPCs, etc.)

WHY DO WE NEED IT?

Many would say this sounds like an amalgamation of existing varied contracted services that different firms may or may not provide. It also sounds like some of the duties that an MSSP would perform in some cases as well. In some respects, yes, but holistically no. Many of these services today are performed by IT firms that have no real ICS security chops or ICS integrators and vendors who have no significant security chops especially no systems security engineering, assessment, validation, secure design, secure integration or security operations and maintenance experiences. Additionally, many existing firms would focus in on just policies, audits, assessments and penetration tests then move on and only return to check to see what mitigations have been implemented. None of these solutions would provide the full lifecycle continuous completion of tasks necessary for ICS Security on behalf of asset owners and operators.

Asset owners and operators often lack dedicated ICS security expertise and the funding to hire such resources. ICS integrators, ICS vendors and consulting firms that are mostly IT security, compliance, and audit based in their nature do not have the full lifecycle systems security engineering experiences or dedicated expertise to continuously close this gap for asset owners and operators. As a result, asset owners and operators end up spending the limited budget they have on expensive audits and assessments that leave them with gaps and findings they have no expertise on staff to help them mitigate. Owners and operators also end up depending heavily on integrators, vendors, and MSSPs to perform duties and tasks that only address portions of the gaps and mitigations or end up creating more gaps and risks than they mitigate. Simply put, the status quo means well and does serve a purpose of good but the gaps that remain are continuously putting asset owners, operators and the infrastructures they monitor and control at risk.

ICS SECURITY MANAGER AS A SERVICE

A list of some reasons why asset owners and operators need ICS Security Manager as a Service are as follows (this is not a complete or exhaustive list):

- Asset owners, operator and critical infrastructure needs ICS security focused and dedicated resources
- Organizations lack resources for full-time ICS security staff
- Collateral duty with IT biased approaches to ICS create more risk than solutions
- ICS operators cannot focus exclusively on security of their operations and assets and generally lack significant security experience and awareness
- Build, maintain and execute ICS system security plans, ICS configuration management plans, ICS inventory list, ICS incident response plans, ICS system, network and architecture diagrams, etc.
- Integrate, create and enforce ICS security requirements, standards, best practices and functionality into all ICS projects, contracts, agreements, operations and assets on behalf of asset owners and operators
- IT does not focus exclusively on ICS security and generally lacks the ICS focused education, training, certifications, understanding, and experiences needed
- Test, evaluate, authorize, certify and facilitate products and services used by and for ICS assets and operations on behalf of owners and operators
- Enable and deliver ICS focused security training and awareness for ICS operators and supporting stakeholders (physical security, HR, finance, procurement, IT, vendors, integrators, EPCs, etc.)

WHO CAN BENEFIT FROM IT MOST?

So, who would even benefit from this ICS Security Manager as a Service concept? The simple answer is every asset owner and operator with ICS assets that monitor and control any part of their operations. Any critical infrastructure sector that leverages automation and control systems to monitor and control critical infrastructure assets and operations can benefit from ICS Security Manager as a Service.

A more specific list of immediate winners are as follows (this list is not complete or exhaustive):

- Electric cooperatives, municipalities
- Hydro, water and wastewater
- Oil and gas pipelines
- Ships and ports, rail and urban public transit systems, airports
- Manufacturing
- Agriculture and food processing
- Hospitals, labs, and clinics
- Fire, Life safety and facilities management
- Small and mid-size businesses that own and operate critical infrastructure assets
- Large asset owners and operators with no single authoritative role for ICS security
- CISOs, CSOs, CIOs and or critical operations managers and business unit owners who have been tasked with the responsibility of ICS security for their assets
- ICS Vendors, Integrators, EPCs

ICS SECURITY MANAGER AS A SERVICE

CONCLUSION

Asset owners need skilled allies in their efforts to improve and secure some of our most vital infrastructures. They do not always need, nor can they always afford, the traditional consulting firm contractor staff augmentation and advisory service or MSSP SOC and incident response only services or product plug and play. Asset owners, especially the small to mid-market owners and operators, need a continued partner providing ICS Security Manager services on an as needed yet continued retainer style basis. This gives the asset owners the ability to have access to a cadre of experienced ICS Security Managers as a Service instead of being limited by staff augmentation assignment to a specific role for various tasks. Also, unlike just a CISO the ICS Security Manager as a Service brings in technical hands on abilities and creates an ICS focused buffer to help operations manage interactions with the CISO, IT and other stakeholders concerned with ICS security within an organization who don't have both detailed cyber and ICS experiences.

ABOUT THE AUTHOR

Isiah Jones has over 13 years of progressive experiences in information technology, information security, information assurance, cybersecurity, industrial control systems security and operational technology security. He has held roles such as systems analyst, security analyst, system security engineer, information assurance officer, Director of OT Security Solutions and Director, ICS Cyber Security Engineering, among others. Back in 2014 he decided to work exclusively on ICS security and has since traveled around the world doing it in places like the Middle East, East Africa, Europe, Hawaii and various states in the continental United States. He has performed ICS security work for the US Navy, US Marine Corps, Siemens, FERC, various asset owners and operators across several sectors and asset type verticals, collaboration with various ICS integrators and vendors. He has held national security clearances as high as TS/SCI and Q.

He carries a network of affiliations that reach into various parts of the US intelligence community, Defense community, Congress, FERC, Department of Energy, Depart of Homeland Security, Department of Commerce, various National Labs, ICS vendors, ICS integrators, asset owners and operators. He brings well rounded experiences, access, insights, connections and visibility into critical infrastructure security issues across many asset types (water, electric, oil, gas, building automation, airfields, maritime, hydro dams, manufacturing, logistics & warehouse, ERP etc) that is rarely found publicly and hard for asset owners and operators to encounter regularly.

ABOUT LEO CYBER SECURITY

LEO is a cyber security advisory and operations concern comprised of some of the world's most knowledgeable cyber experts. Its name is a derivation of the Renaissance visionary, Leonardo da Vinci, who refused to accept the status quo. LEO provides both advisory and operational assistance to our customers. With deep cyber skills, LEO is poised to help clients build effective and cost-efficient cyber programs.