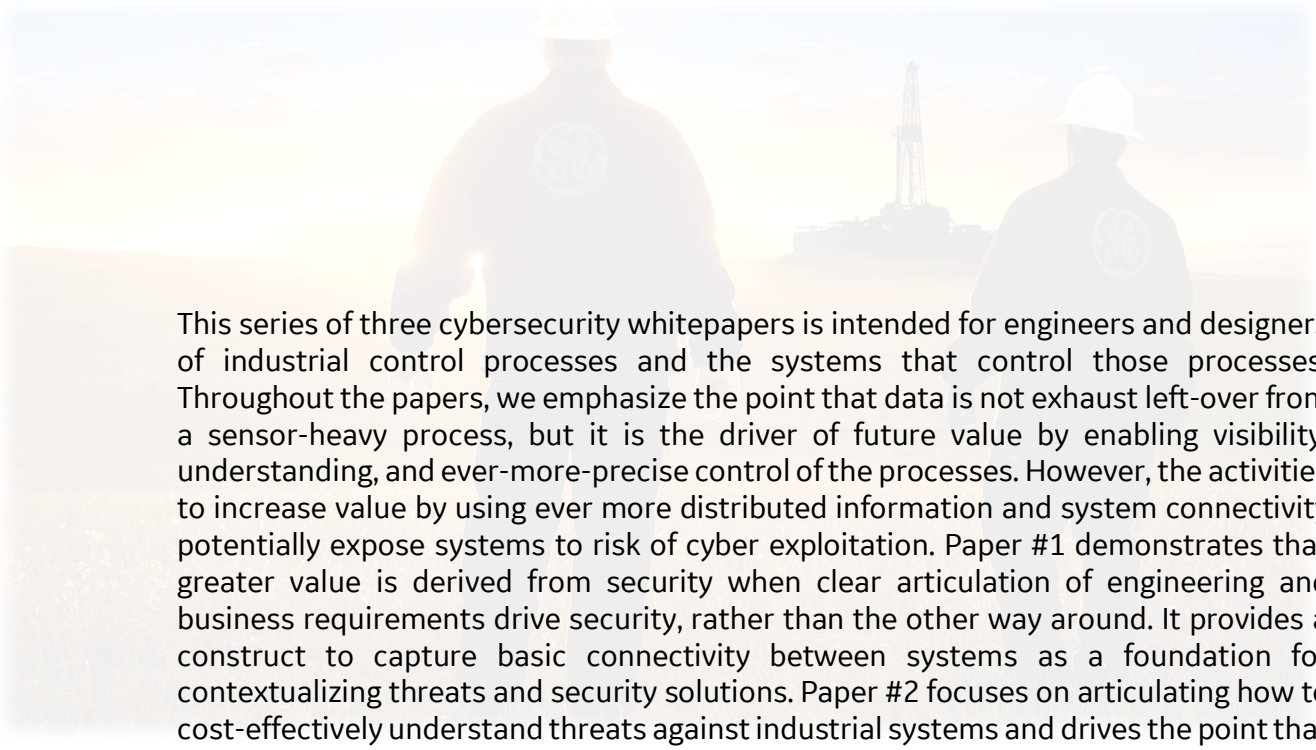
2018

Blending Resilience and Protection to Achieve Greatest Security for Business-Viable Industrial Systems

DESIGN AND BUILD PRODUCTIVE AND SECURE INDUSTRIAL SYSTEMS, WHITEPAPER #3

KENNETH G. CROWTHER (KENNETH.CROWTHER@GE.COM), ROBERT M. LEE (RLEE@DRAGOS.COM), K. REID WIGHTMAN (RWIGHTMAN@DRAGOS.COM)

A COLLABORATION BETWEEN GENERAL ELECTRIC AND DRAGOS.



This series of three cybersecurity whitepapers is intended for engineers and designers of industrial control processes and the systems that control those processes. Throughout the papers, we emphasize the point that data is not exhaust left-over from a sensor-heavy process, but it is the driver of future value by enabling visibility, understanding, and ever-more-precise control of the processes. However, the activities to increase value by using ever more distributed information and system connectivity potentially expose systems to risk of cyber exploitation. Paper #1 demonstrates that greater value is derived from security when clear articulation of engineering and business requirements drive security, rather than the other way around. It provides a construct to capture basic connectivity between systems as a foundation for contextualizing threats and security solutions. Paper #2 focuses on articulating how to cost-effectively understand threats against industrial systems and drives the point that security should be adapted based on connectivity requirements from the business and the threats to the processes, rather than published vulnerabilities and exposures. Paper #3 ties the two pieces together and further explores details of how engineers can guide the implementation of good industrial control system (ICS) security into the future as next generation control systems and connectivity requirements emerge (e.g., Industrial Internet of Things (IIOT) or Industry 4.0). It assumes some knowledge of the basics, and focuses on what engineers should learn to design next-generation security around the business and engineering requirements of ICS.

In Whitepaper #1 (titled, *Building security to achieve engineering and business requirements*) we described trends in industrial control systems (ICS) toward cross-enterprise machine-to-machine connectivity, data integration to derive value from process efficiencies, and new roles for collaboration and analytics from integrated data. We described general trends driven by the value of connectivity and coordinated control that are consistent with a movement toward Industrial Internet of Things (IIOT) or Industry 4.0. We described how highly connected and remotely controlled processes benefit from a next generation Purdue Model that might include a "zero-trust" Automation Control Bus (ACB) that flattens Purdue Levels 1 through 3 and introduced Edge Services that provide highly-monitored and controlled bi-directional connections between the ACB and the partner entities without going through the Enterprise IT network. That paper recognized that multiple architectures exist, and introduced a sliding scale of connectivity that helped to compress the complexity of dozens of architecture features into a single dimension related to connectivity and remote control.

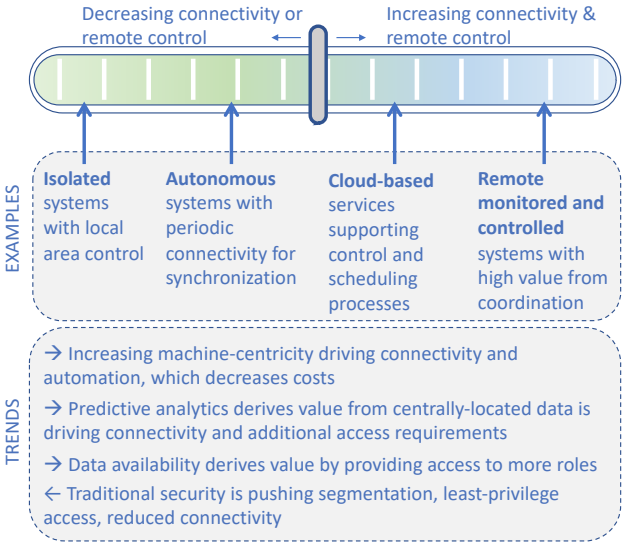


FIGURE 1. ICS ARE TRENDING TOWARD GREATER CONNENTIVITY AND REMOTE CONTROL DUE TO HIGH VALUE OF CONNECTIVITY.

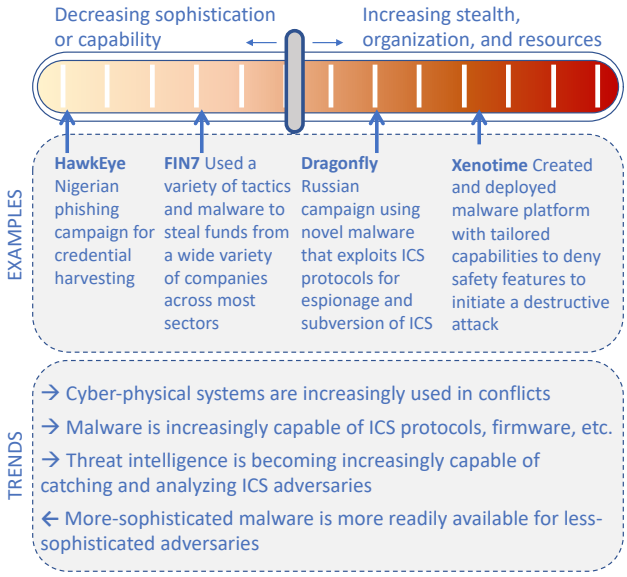
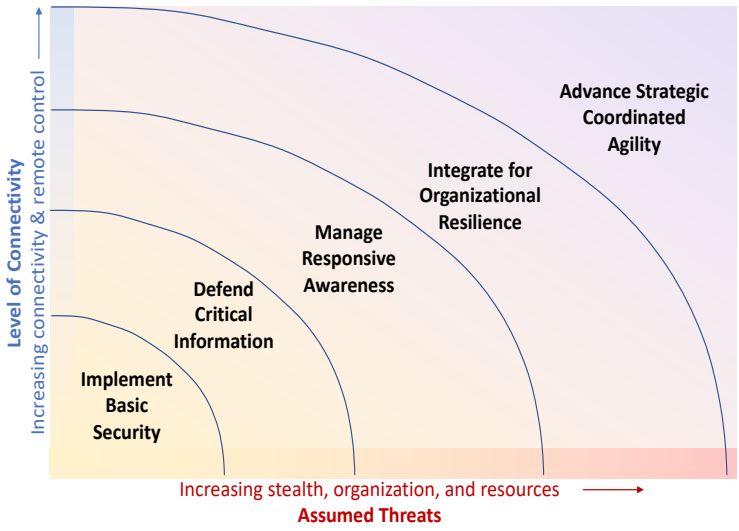


FIGURE 2. ICS ARE INCREASINGLY TARGETED IN CONFLICTS AND ADVERSARIES ARE GAINING CAPABILITIES IN THIS SPACE.

In Whitepaper #2 (titled, *Understanding threats will promote the "right amount" of security in industrial systems*) we discussed emerging threats against industrial networks and the value of threat intelligence that describes adversaries, adversarial capabilities (e.g., their malware, techniques), infrastructure leveraged by adversaries to deliver capabilities, and victims. We described how this information can be leveraged to prioritize your security controls, countermeasures, and mitigations by evaluating the capabilities used against victim with similar persona (e.g., similar industry, asset types, or vulnerabilities/exposures). We also introduced a sliding scale of threats that helped to compress the complexity of diverse threat activity groups into a single dimension of threat assumptions related to the level of stealth and sophistication of the adversarial techniques. We further described how those threat features can be captured in a diamond model that can help provide a framework for how an organization leverages threat information in order to prioritize what protection capabilities are best suited for their system, given the similarity between the specific system and the victimology of known adversaries.

This whitepaper provides a broad perspective to improve engineers' awareness of emerging security capabilities to help improve conversation with cybersecurity professionals for securely implementing business and engineering requirements that add value. These suggestions are not meant to represent the only approach, but instead present concepts as examples of practical prioritization based on an understanding of your threat landscape as it relates to your connectivity and remote-control requirements. The examples intend to reinforce the idea that ICS should be treated as systems in which security is part of the design and evolution, rather than a patch after the system is in operation.

The sliding scales described above are useful for building intuition of the level of protection generally desired based on your degree of connectivity and remote control in combination with the level of threat that you assume based on the similarity between your operations (e.g., industry) and those of victims being targeted. For example, an electric utility is concerned with known adversaries using malware platforms to transition through the ICS with capabilities to manipulate standard communication protocols thereby altering electric distribution processes; a petrochemical facility is concerned with known adversaries using malware platforms to manipulate Safety Instrumented Systems (SIS) to amplify the ability to create physical harm to the process or people. Figure 3 shows the integration of the two sliding scales to communicate the evolution of security needed as the connectivity of systems and sophistication of threats increase. There are short descriptions of each security level to the right of Figure 3. This paper describes each level in greater detail, and provides examples of emerging capabilities that could serve as a foundation for creative designs of security systems that aim to help accomplish modern engineering and business requirements.



Implement Basic Security – Policies, physical security, access control, configuration control, control removable media

Defend Critical Information – ICS network monitoring, zoning, information backup, device & application hardening and maintenance, leadership & staff for cyber threat intelligence consumption and incident response

Manage Responsive Awareness – Rehearse incident plans, point of contact for decisions, cyber-security integrated into disciplines (engineering, ops, supply chain), use threat intelligence to drive priorities and security controls

Integrate for Organizational Resilience – Integration of engineering/business/cyber teams, coordination between cyber security and other key operational staff (supply chain, customer relationship), dedicated monitoring of industrial networks with ICS skilled personnel, integrated cyber team (defenders, malware analysts, tool developers)

Advance Strategic Coordinated Agility – Strategic planning engages cyber security, teams for active investigation of next-generation threats, plans exercised jointly with cyber security personnel, new forensic methods for continuous monitoring, collaboration across peer businesses

FIGURE 3. LEVELS OF CYBER SECURITY SHOULD EVOLVE WITH GREATER CONNECTIVITY OR THREAT SOPHISTICATION.

Whenever there is a system requirement that increases connectivity or an increase in the threat, there must be a corresponding evolution in security. Connectivity can come in various forms - such as, putting VoIP phones in operating centers, wireless sensors to save on infrastructure costs, or adding new control processing capabilities on the edge. Each would require an evolution in security to compensate for the new level of connectivity. Moreover, announcements of new adversarial campaigns with victimology consistent with a certain industry or asset type, should similarly trigger discussions for improved security through a collaboration between the process engineers or architects and the IT and OT security professionals. Good ICS security will demand collaboration between these groups to make adjustments that result in the greatest value to the organization.

Implement Basic Security

"The basics" are the most essential features of security necessary to notice malfeasance, or in others words that would enable you to "silhouette an adversary." This security level must include a set of policies that define industrial network standards and behaviors, a practice for tracking cyber assets and their configurations, procedures for controlling and monitoring (physical and virtual) access to cyber parts of the industrial process, control and management of configuration changes to cyber parts, and specific control of and mitigations for removable media across the site. The ways these are implemented are tailored to business process and operational culture so they are sustainable. But, if you cannot inventory assets and control access and configuration, then all additional layers of security will be crippled.

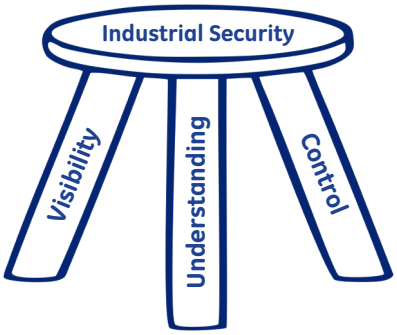


FIGURE 4. BASIC SECURITY REQUIRES VISIBILITY INTO THE SYSTEM, UNDERSTANDING OF HOW THE SYSTEM OPERATES, AND CONTROL OF ICS NETWORKS AND ASSOCIATED PROCESSES.

Examples of emerging security capabilities in this space:

Integration of Product Lifecycle Management (PLM) and other Enterprise Resource Systems (ERP, such as supply chain management, customer relationship management, systems engineering and design tools, product portfolio systems) enables the use of up-to-date information about assets and systems. In some cases, integration functions and advanced queries are needed to execute new policies and procedures to track assets. In other cases, the requirements for these systems could be augmented to track additional details about suppliers, original part manufacturers, configurations, etc. By so doing, one can decrease the work required for asset tracking and the system requirements for configuration management by taking advantage of existing systems and processes already in place for engineering changes.

Integrated Baseline Security Stacks are emerging from control and automation system vendors that provide a combination of capabilities from the IT security world with modifications specific to ICS technologies and practices (e.g., firewalls that can screen ICS protocols like Modbus and OPC). These stacks are typically selected and integrated with the controllers and workstations on the plant floor, and as such, they know their active scanning limits and can maintain visibility into the control network. These integrated platforms frequently come with services, such as labs for vetting patches/updates before deploying across the stack and helpdesks that understand capabilities across the stack for integrated support. For example, the GE Baseline Security Center has a stack that contains the following integrated services from across a set of vendors for ease of integration and implementation in an ICS environment:

- Network perimeter defense controller
- Central log collection/monitoring/management
- Backup and restore utility
- Local security policy enforcement
- Host intrusion detection and anti-malware
- Security event information management
- Central authentication/ID management
- Configuration persistence & version control
- Inventory awareness with patch and update deployment

DEFEND CRITICAL INFORMATION

Systems with any connectivity that might impact control must evolve beyond "the basics." This security evolution should be prioritized based on information or process components that are important to the system, and the threats against the system. Importance to the system can be assessed systemically and intuitively using something like the CARVER method, in which one evaluates components or their information according to the following questions:

- Critical? Is the information or component essential because of regulatory or safety reasons?
- Accessible? Is the information or component accessible due to connectivity required to produce value?
- Recognizable? Would a knowledgeable adversary recognize the value that the information or component plays in process production or disruption?
- Vulnerable? Does the information process or component have features or flaws that make it susceptible to be controlled or manipulated in a way that would cause disruption or lost value?
- Effects? Would the theft or disruption of the component create damage (e.g., injury, lost life, lost production)?
- Recoverable? If damaged, stolen, encrypted would the component need to be recreated, or could it simply be restored?

One's understanding of threats against the system can be based on the capabilities of the handful of adversaries whose victims are most similar in terms of persona (such as industry), susceptibilities (vulnerabilities and exposures), and operations. Focusing on the capabilities of known adversaries will provide the greatest return on a security investment when designing security features for your industrial system.[1] Remember not all security features are digital, for example electrical or mechanical safety interlocks would prevent life-safety disruptions in ways that no one can manipulate remotely.

At this security level, it becomes important to actively monitor the network, which might mean deployment of appliances or agents that can passively or actively interrogate various types of devices and protocols across the network. In IT networks, active monitoring can be done fairly aggressively, but on control systems it requires attention to the types of controllers and protocols used, so that the active monitoring considers older protocols, fragile coding on devices, unacceptable latency caused by scanning, vendor warranty requirements, insurance limitations, etc. For these reasons it is far more common, and safe, to leverage passive technology. Finally, basic processes and protocols for incident identification and management should help to cover the more general exposure.

The advancement of control system security requires increased collaboration between the process architects/engineers that "keep the plant running" and the OT/IT specialists that "keep the network running." Many examples of emerging security technologies will require knowledge of both process and networks. The evolution of security will furthermore demand greater involvement of leadership and staff to consume cyber threat information as it evolves, to improve device and application monitoring for better maintenance, and to improve the visibility, system understanding, and governance for incident response.

---

[1] Security is a process and there will always be unknowns such as threats and vulnerabilities that have not been identified. However, focusing on the known adversarial techniques gives a clear prioritization and way forward. Additionally, the ability to detect and respond to known threat tradecraft is additive as it is very common for attacks to overlap known tradecraft at some point in the attack. Attacks should not be viewed as singular events but as a chain of adversary actions.

Examples of emerging security capabilities in this space:

With log collection/monitoring and system event information management (SEIM) capability, one can begin to create baselines of network operations to hunt for threats. This helps to have earlier detection of cyber incidents and to hunt for threats based on threat reports. This is the foundation for **network baselining and threat detection**. Numerous ICS specific network asset identification and threat detection technologies exist on the market such as the Dragos Platform. Some of the technologies model system and protocol behaviors to identify anomalies and others leverage analytics to identify threat tradecraft and methods. There is no single best tool, but requirements should drive what technologies are chosen for where the security program is today and where it should go based on engineering and business requirements in the future.

The introduction of additional network abstractions, such as **software defined networking (SDN)**, enables additional flexible methods of segmentation to protect critical processes with fewer resources and can fit on top of a baseline security stack. Segmentation no longer needs to be once-and-done, nor does it need to be constructed around traditional Purdue Model zones. It can and should be both dynamic (adapts/changes to segment according to engineering temporal requirements and changing threat information) and flexible (segments according to critical groupings of operations instead of network-proximity to physical process). Finally, management of the SDN components should be limited to a dedicated management system. This will further limit an attacker's ability to move laterally by not allowing the attacker to reconfigure components.

The introduction of **edge services and infrastructure** provides capabilities for adding industrial-specific features to traditional network functionality to include control of network switches, protocol gateways, analytic load balancers, unidirectional gateways, and firewalls, in a way that is tailored to the industrial operation and its security. When engineers can participate in the design of cyber security, then their negotiations over ownership and operations of the DMZ that enables connection to the enterprise network can become less contentious. Most attacks on ICS are through the enterprise and site IT networks exploiting features or flaws and then laterally move into the control network. Instead of using enterprise historians to coordinate operations or boost processing capabilities, the control network should have sufficient processing power and controlled pushes of data so that control networks can accomplish full connectivity requirements while limiting visibility and access to outside networks.

Engineers will want to work with Process Hazard Analysis (PHA), Function, Modes, and Effects Analysis (FMEA), or other **safety/risk teams appropriate to their industry to ensure cyber parts of safety controls are considered carefully**. For example, cyber threats may result in selecting a mechanical or electrical interlock over a safety controller to hedge against lost or ineffective controls during a cyber-attack (it may also be cheaper). This can be done simply by reviewing the proposed controls from a safety assessment and evaluating reliance on cyber controls, then proposing alternatives around crown jewels processes. This can then be discussed with the safety teams so they understand the tradeoffs.

For critical devices, look for those with **device birth certificate and code signing technologies** that can establish a foundation of trust. These security products provide a publicly and third-party verifiable list of valid certificates for both code-signing of binaries and device identification. The code signing capability supports the public verification of cryptographic signing material for firmware, package managers, containers, operating system files, user-level applications, and other binaries. The device birth certificate capability supports the public verification of unique identification of any physical or virtual computing device where a trusted platform module (TPM) or trusted cryptoprocessor exists. This establishes a foundation for more sophisticated trust models (for both supply chain as well as for network operations) as the system evolves.

Manage Responsive Awareness

The next security level builds on the capabilities to defend critical information. The key to this step is to evolve not just your technology, but your organization, to appropriately track and consume information that will enable you to continuously manage emerging security threats. Good architecture and technologies help make an environment defensible; adding well trained human defenders and processes on top of this good architecture and technology move a defensible environment to a defended one. Security against advanced threats must evolve to integrate industrial specific cyber incident response, cyber security across multiple disciplines (e.g., engineering, operations, supply chain), consumption of appropriately contextualized threat intelligence, and combine it with increasingly better visibility and control over your industrial networks. Capital investment projects that shut down parts of a plant are a good opportunity to evaluate the adequacy of cyber security and make changes. This requires integration of operational, engineering, and cyber security teams. Plant leadership should contain at least one leader that is accountable and knowledgeable of industrial cyber security challenges and can build collaboration across teams.

Examples of emerging security capabilities in this space:

A set of negative tests should be incorporated into the system during the Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) which ensures minimum exposure between system components. This is done, to some extent, by those installing, configuring, and testing before start-up. With clear documentation of the tests and advanced networking features, many of **FAT and SAT tests can be automated and built into the network**. These can connect to external sources, such as the vulnerability advisories and collaborative research into threats (CRITs) portals, and can be re-tested using FAT/SAT methods.

Increased connectivity and data integration yields opportunities for building digital twins – digital models of your physical operations. Sometimes these models already exist for design or process improvement. These can also be used to improve process reliability, safety, and security by doing **process baselining and precursor detection**. GE's Digital Ghost is an example of a physics-based baselining system that computes a multi-variable representation of the normal operation and exploitation of weaknesses that cause outcome variance, unsafe operations, or process disruption. An analysis of the controller settings that lead to damage, results in a capability that can detect precursors of unsafe, unreliable, or unsecure operations – and in many cases can adjust process in real-time operations to avoid unreliable/unsafe operations. This improves security of the physical process without the necessity to understand all threats against the control networks.

Threat intelligence and cyber incident response services are emerging, which can help industrial companies rapidly take advantage of capabilities without building their own internal teams. It is important to consider how these organizations can be integrated with engineering, operations, and other teams.

With a security services stack that includes SDN capabilities, device identification, and access control more sophisticated processes can be implemented to **reduce inherent network trust**. For example, integrated scores of devices and identities could provide a foundation for controlling lateral movement across the control network. This would be constructed to restrict changes from machines whose configuration or action deviates from baseline activity. This is a feature that should be reserved for advanced security needs. This can be integrated with additional baselining of device and identity operations behaviors for **insider threat detection**.

INTEGRATE FOR ORGANIZATIONAL RESILIENCE

The rest of the evolution of cyber security focuses primarily on improving the organizational capability to take advantage of the visibility, understanding, and control that the established security technologies can provide.[2] This security level builds on the responsive architecture established around a maturing and integrated organization and the technology that it uses. This stage makes a transition to an active creation of intelligence from data, stronger collaboration between operations, engineering, IT, and security groups. In addition to integrating cyber functions across the organization, you might start contracting differentiated expertise for tracking network changes, analyses of unusual or unexpected events, and translation of threat intelligence into internal security capabilities. Always consider the opportunity to leverage insights from threat reports as well as security best practices to design and engineer better security into the process and components to start with. The ICS community moves forward most effectively when best practices get moved into the architecture over time instead of just relying on bolt-on solutions after the fact.

Example emerging security capabilities in this space:

Establish a team that periodically or consistently evaluates control network adequacy and security. This might be done directly or through contractual assessment teams. This would be an **integrated cyber parts analysis team** that understands process operations, malware analysis, network operations, etc. They might consider setting up a lab that serves a dual purpose of evaluating maintenance and patching procedures, and also investigates controllers and appliances on the process network for vulnerabilities, attack paths, unreliability, etc. They would help recognize malware, update controls for newly discovered vulnerabilities, and work with the vendors to obtain updates and patches. Typically, these evaluation teams would stay connected with threat intelligence in order to prioritize what they evaluate.

Work to **take part in industry events** to occasionally provide best practices and insights learned in your organization with others while also learning from their insights. Industrial threats are pervasive and simply sharing technical insights is insufficient; share best practices on how threats were prepared for, dealt with, and countered across the organization from industrial specific security to business level continuity and preparedness. Defenders benefit by working with other defenders while also expanding an understanding of what is achievable in the industrial environments.

Continuous improvement requires additional evolutions of the organization that can integrate security more efficiently into the design, engineering, and operational process. Assure that there is a high-level center point that is accountable for "cyber decisions" in the operational/industrial environment of the company. Assure that the individual understands business and engineering requirements for operations and can lead the process of tailoring security. Move for integration between engineering, business, and cyber teams around key cyber challenges. Help create some common network architecture models and threat diamonds that provide a foundation for a common language to discuss cyber security needs.

[2] At no point in this paper do we recommend offensive cyber measures—there are unfortunately some references to this in the information security community, but it is widely seen as an extremely poor use of resources and better left to national governments. The best defense is doing that which enables resilient, profitable operations.

Maintain Strategic Coordinated Agility

This final stage continuously expands security operations to integrate at higher levels in the company and more tightly integrate with strategic planning and business direction setting. At this stage, strategic planning engages cyber security as part of key considerations, teams are established for active investigation of emerging threats, plans are maintained and exercised jointly with cyber security teams, new forensic methods are developed for continuous monitoring, and more consistent collaboration across peer businesses is established to share incident and threat information in a way that does not violate anti-trust laws or reveal proprietary information.

Examples of emerging security capabilities in this space:

An emerging capability in this space is the application of artificial intelligence, such as **computational creativity**, to project future adversarial targets and techniques. For example, ransomware integrates features from historical ransoms, malware, and confidence games. Most historic ransomware incidents use fairly simplistic encrypt-pay-to-decrypt techniques. Future attacks might involve much more sophisticated combinations of ransom and con tactics with a greater variety of physical and cyber features involved. A model output might include the use of malware to manipulate a food production process to produce or inject a toxin and ransom an antidote. A computational creativity algorithm would enable feature extraction from existing malware, ransoms, and confidence games to compose millions of possible scenarios. It would then prune those scenarios to identify the scenarios that are the most novel (i.e., different than current practice) and valuable (i.e., present best likelihood of gains to the adversary with the least risk). Those would help with **scenario-based strategic planning** and other strategic development.

Companies requiring high interconnectivity and remote control that are targeted by sophisticated adversaries will need **board-level attention** to cyber threats in a way to help shape business direction and business practices to incorporate cyber security in a way that provides assurances of business objectives. The highest-level of cybersecurity evolution will be integration of security across practices, not a separate department or division.

In the sliding scales, the highest level of cybersecurity is for organizations with high levels of remote control and connectivity that are a target of sophisticated adversaries. It is important to evolve the "right-level" of cybersecurity that is comparable to the value generated from connectivity and remote control and the observations of threat. The evolution need not happen all at once.

In paper #2, we summarized five attacks that successfully targeted ICS. To drive home some of the key features of each security level, briefly consider example outcomes had the owners/operators impacted by the malware evolved their cyber security:

Malware	**Protect Critical Info.**	**Manage Responsive Awareness**	**Integrate Org. Resilience**	**Maintain Agility**
STUXNET (cyber warfare)	Safety features may not have allowed destructive levels of centrifuge operations. Disaster recovery would have enabled rapid recovery.	Cyber incident response teams familiar with processes would have resulted in faster identification of malware and faster decisions on course of action.	Integrated teams accelerate ability to recognize and respond to situation outside of traditional business.	Integration of cyber security into operational planning would have enhanced security and preparedness across other categories.
HAVEX (cyber espionage)	SDN would have limited adversary visibility. Edge services would have limited access from the enterprise.	Rapid establishment of response team after realization across industry.	Collaboration across businesses would have limited the effectiveness of HAVEX across entire industries.	Integrated cyber espionage into strategic business planning would have resulted in improved controls.
BLACKENERGY 3 (cyber disruption)	Lateral movement would have been more complex from micro-segmentation.	Rapid establishment of response team after realization across industry.	Active defense would observe threat behaviors for rapid internal response.	Strategic planning would have built disaster recovery that could be executed quickly.
CRASHOVERRIDE (cyber disruption)	Backups would have accelerated recovery to wiper functions.	Knowing and monitoring proper use of protocols would have initiated some investigative response.	Cross-business collaboration might have projected these types of malware based on previous targeting.	Joint exercises would help to accelerate response across organizations.
TRISIS (cyber disruption)	Device signing would have made SIS overwrite more complex. SDN and micro-segmentation would have limited access.	Network control would not have restricted lateral move to SIS. Cyber response would have more-quickly identified as a cyber incident.	Active defense would have looked for tradecraft with SIS and designed response.	Strategy would balance cost savings from SIS with cyber-based attack vectors.

Further Reading:

R. Lee, 2015. The Sliding Scale of Cyber Security. (https://www.sans.org/security-resources/posters/sliding-scale-cyber-security/105/download and https://www.nti.org/media/documents/Mounting_an_Active_Cyber_Defense_in_the_Nuclear_World.pdf) This poster provides a visual overview of the sliding scale of ICS cyber security. It provides some breakouts of layers of ICS defense in depth, the active cyber defense cycle, and cyber intelligence collection.

MITRE, 2017. *Cyber Prep 2.0: Motivating Organization Cyber Strategies in Terms of Threat Preparedness.* (https://www.mitre.org/publications/technical-papers/cyber-prep-20-motivating-organizational-cyber-strategies-in-terms-of) While this paper is not focused on ICS, it does provide detailed information about threat types and assumptions and provides some initial details about protection strategies to correspond to threats.