GLOBAL CYBERSECURITY ALLIANCE

THE TIME IS NOW

www.isa.org/GCA

Industrial cybersecurity is a global imperative.

Threats are increasing

47% of industrial control systems computers were attacked in 2018. 38,500 malware modifications were detected on industrial automation systems.[1]

Vulnerabilities are expanding

415 vulnerabilities were detected on industrial control systems computers in 2018; 342 of those vulnerabilities could be accessed remotely without any expertise or special skills. 68% of the identified vulnerabilities were classified as critical or high risk.[1]

Industry's response is inconsistent

Only 23% of companies are complying with mandatory minimum industry or government guidance.[1] ISA/IEC 62443 is a series of automation cybersecurity standards that address these issues, but most people don't know how to apply the standards or aren't sure how to adjust them for their industries. 58% of companies in the industrial space say that hiring employees that are cyber aware or skilled in cybersecurity is a critical challenge, but only 30% plan to invest in cybersecurity workforce development.[2]

Cybersecurity is critical to digital transformation. It's critical not only for the protection of information and intellectual property, but also for the protection of physical assets, the environment, and worker safety. We make it a priority to collaborate with partners and research institutions to develop secure products. We have earned our ISA/IEC 62443-4-1 Security Development Lifecycle certification, and recently introduced the first programmable automation controller to obtain ISA/IEC 62443-4-2 certification, showcasing our standards-focused approach to cybersecurity. Our engagement with the Global Cybersecurity Alliance will be another important step in our efforts to help customers identify and mitigate risks.

—Blake Moret, CEO, Rockwell Automation

These challenges will only grow as we continue to advance our technologies

The factors that are triggering increases in threats and vulnerabilities are the same factors that we depend on make our industries safer, more reliable, and more efficient.

- **IIoT and Digital Transformation**
  Accelerated connectivity, leveraging remote access and cloud resources, translates into a larger attack surface and more opportunities for exploited vulnerabilities. A group of autonomous hackers within IBM Security estimates that the number of vulnerabilities exposing control systems has increased 83% since 2011.
- **OT/IT Convergence**
  IT components, like servers and cloud computing, are driving improved uptime, performance, quality, and productivity in manufacturing environments. Increased connectivity means increased vulnerabilities, and IT and OT must work together to build a more secure enterprise.
- **Legacy Systems**
  Many legacy systems are used in plants and facilities around the world, but these systems were designed for a different time. While IT systems are designed around confidentiality, integrity, and availability, operational technology environments are mission-critical and therefore prioritize availability and integrity above confidentiality. Instructions being sent between devices are trusted and often executed without verification or validation.

[1] Kapersky Labs, *The State of Industrial Cybersecurity 2018*

[2] SANS, *2019 State of OT/ICS Cybersecurity Report*

- **Multi-Vendor Environments**
  Most environments are increasingly complex—distributed control systems, SCADA systems, and components of each are built, integrated, and managed by different entities. If cybersecurity isn't built into products by design or verified when products and systems are connected, vulnerabilities are heightened. To make matters worse, companies are slow to patch vulnerabilities because they don't want to impact the system function or increase downtime. Cisco estimates that nearly half of the security risk that organizations face stems from having multiple security vendors and products.
- **Skill Gaps and Contract Workforces**
  Nearly every industry sector is relying heavily on contracted labor resources to run their enterprises, and this trend isn't likely to change with the pending Baby Boomer generation moving into retirement. Many companies say that finding skilled employees is a critical challenge—and people can make an even bigger difference than technology or devices. 62% of respondents in the SANS 2019 State of OT/ICS Cybersecurity Report identified people, internal and external, as the greatest risk for system compromise. Kapersky Labs research agrees—they found that the number of incidents caused by the unintentional activities of current service providers, consultants, and contractors more than doubled in 2018.

Over the last few years, global industry has recognized that taking on increasingly dangerous cyber risks can't be limited to a single company, segment, or region. However, until now, there has been limited ability to respond as a unified whole to these worldwide threats. But by establishing an open, collaborative, and transparent body, with a focus on strengthening people, processes, and technology, we can drive true cultural change. Together we will bring to bear the standards-based technology, expertise, and special skills required to better secure and protect the world's most critical operations and the people and communities we serve."

—Klaus Jaeckle,
Chief Product Security Officer, Schneider Electric

Digital transformation in the building sector continues to accelerate, which heightens the urgency for cybersecurity across the industry and beyond. As a leader in the industrial automation controls business, Johnson Controls is already a strategic member of the ISA Secure program and is consistently taking proactive actions to protect customers against cyber-threats and risks. Joining ISA Global Cybersecurity Alliance is a necessary and meaningful step as it supports our company values, customer adoption of the ISA/IEC 62443 standard and efforts to educate global government and regulatory bodies. We are proud to solidify our commitment to this important effort.

—Jason Christman, Vice President,
Chief Product Security Officer, Global Products, Johnson Controls

$$\left(\frac{\text{threats x vulnerabilities}}{\text{industry response}}\right)$$ **Digital Transformation**

The ISA Global Cybersecurity Alliance

The bottom line

The impact is significant, and it's only a matter of time until it becomes life threatening. We've seen cyber-attacks in every industry – critical manufacturing, energy and utilities, oil and gas, healthcare and life sciences, facilities and buildings – no sector is exempt.

Threats will reach your networks, vulnerabilities will be present, and the resulting attacks will impact your operations.

That means you'll experience disruption and damage to your physical assets and processes.The safety and reliability of your operations will be compromised, affecting the quality of your products, and more importantly, the safety of your employees and your community.

So, the question is: what are we going to do about it?

We could continue to work in our separate corners on pieces of the problem. We could continue to work with our own customers and supply chains to make improvements. That's good, but is it enough?

We don't think so.

We must work together openly and collaboratively to drive a unified response to these challenges.

The purpose of the GCA is to help companies and communities stay ahead of the threat curve. We are committed to fostering a sustainable, secure, resilient environment for all industry segments to thrive and grow.

To see the list of companies in the Alliance, visit: **www.isa.org/GCA**

One of the most effective ways to drive consistency in an industry is by putting standards in place. We're looking forward to collaborating with all of these founding members, as well as future Alliance members, to help drive global best practices forward in this historically standard-less environment. Claroty is committed to the mission of protecting all IoT and OT networks from cyber risks. Through our work with the Global Cybersecurity Alliance, we will be able to help shape the future of cybersecurity in these high-risk industries.

—Dave Weinstein, Chief Security Officer, Claroty

The ISA Global Cybersecurity Alliance welcomes members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Objectives of the Alliance

Companies and organizations that join the ISA Global Cybersecurity Alliance will work together to progress important objectives focused on the three aspects of cybersecurity: people, processes, and technology.

- We'll facilitate open dialogue and engagement to drive consistency and prioritization across all industry segments and types of facilities
- We'll educate and inform global governments and agencies ensuring they understand industry's challenges and the benefits of standardization
- We'll help insurance companies and other stakeholder groups identify recommended practices and objective ways to reduce risk

We will leverage our collective intelligence and experience for the benefit of all.

- We'll share knowledge, information, and threat intelligence in an open environment
- We'll develop safe, secure, and customized ways to identify best practices and vulnerability remediation guidance across industry segments

We will accelerate expansion and adoption of the ISA/IEC 62443 cybersecurity standards.

- We'll create high-quality, standards-based procedural security guidelines for industry segments and stakeholder groups
- We'll work closely with worldwide standards organizations to facilitate the use of ISA/IEC 62443 as a reference standard

We will optimize compliance and prevention initiatives.

- We'll expand compliance programs, ensuring all vendors develop inherently secure products
- We'll develop and publish a baseline of common cybersecurity requirements for suppliers within the supply chain to follow
- We'll harmonize certification specifications globally for products, systems, and processes

At Honeywell, we see cybersecurity as a core part of the future we are making, and we see the Global Cybersecurity Alliance as an important way to work together to make that happen. Cybersecurity is critical to the connected world we live in and the cornerstone of trust that the world needs to be able to operate. Whether protecting critical infrastructure or managing a building's operations, users need to do this with the confidence that the employed systems are robust and secure. We are committed to and proud to work together with ISA and the GCA members to continue to drive the adoption of the ISA/IEC 62443 series of standards and identify further ways to secure and protect the connected world. Honeywell has a robust history with ISA and is also founding member of the ISA Security Compliance Institute.

—Matthew Bohne, Vice President and Chief of Product Security, Honeywell Building Technologies

We will enhance cybersecurity training and development programs.

- We'll drive awareness in three levels within owner/operator companies: executive leadership, operations, and maintenance
- We'll help end-user companies identify and mitigate risks
- We'll facilitate and encourage initiatives that bridge the gap between information technology and operations technology
- We'll develop and maintain training modules and certification options based on ISA/IEC 62443
- We'll provide user-friendly, accessible best practice tools to help companies and facilities consistently navigate the entire lifecycle of cybersecurity protection
- We'll recruit new talent into the OT cybersecurity workforce with a focus on mentorship and diversity

Your Financial Support and Expertise are Needed: Join the Movement

There are four ways to get involved in the ISA Global Cybersecurity Alliance:

- **Join the Alliance as a founding member company**
  - — three-year financial commitment based on annual revenues
  - — eligible to be selected by ISA to serve on the advisory board for the first year of the Alliance (after the first year, the general membership votes to select advisory board members)
  - — if selected to advisory board, vote to prioritize activities and allocate resources (each advisory board member company will have one vote)

- **Join the Alliance as a supporting member company**
  - — yearly financial commitment
  - — propose initiatives and deliverables for advisory board consideration
  - — vote on committee and workgroup decisions and approvals with a goal of establishing consensus
  - — opportunity to be elected to the advisory board after the first year of the Alliance, based on a distribution of seats to represent the different stakeholder groups such as end-user companies, and multiple tiers of supplier companies

- **Join the Alliance as an industry organization, government agency, insurance company, or other stakeholder**
  - — yearly financial commitment
  - — propose initiatives and deliverables for advisory board consideration
  - — collaborate with a large, diverse, all-inclusive, proactive alliance of cybersecurity stakeholders in the industry
  - — work with recognized experts to establish objective measures for underwriting and benchmarking
  - — identify recommended practices for reducing risk in OT cybersecurity

- **Employees of member companies can volunteer to help the Alliance as individual contributors**
  - — All member companies may designate volunteers to participate in committees and working groups
  - — Subject matter experts can volunteer as contributors to white papers, guides, e-books, or other media; and representatives of the ISA GCA at industry events

Nozomi Networks believes real community collaboration, actionable standards and effective education are key ensuring a secure future for industrial organizations around the world. That's why we are helping develop secure-by-design standards as a working member of IEC, why we've designed our industrial cyber security solutions for easy integration across the broadest possible set of industrial and IT technologies; and why we are thrilled to help establish the Global Cybersecurity Alliance. Together we will build a secure future for the industrial infrastructure that runs the world.

—Andrea Carcano, Co-founder and Chief Product Officer, Nozomi Networks

We can change the industrial cybersecurity conversation. We can create a culture that works openly and collaboratively to find solutions. We can drive a consistent, resilient approach to the expanding threat landscape, while protecting our ability to harness tomorrow's technologies. We can do all of this, and so much more.

But we can't do it alone.

Join us.

Let's talk about how your company or organization can engage with us.

For more information about joining the ISA Global Cybersecurity Alliance, contact:

Andre Ristaino
Director
ISA Global Cybersecurity Alliance
aristaino@isa.org
+1 919–990–9222

Rick Zabel
ISA Sponsorship Director
rzabel@isa.org
+1 919–990–9233

Elena Pitt
Strategic Business Development
epitt@isa.org
+1-919-323-4023

Media and analysts should contact:
Jennifer Halsey
ISA Marketing and Communications Director
jhalsey@isa.org
+1 919–990–9287

www.isa.org/GCA

International Society of Automation
Setting the Standard for Automation™

67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE +1 919-549-8411
FAX +1 919-549-8288
EMAIL info@isa.org
www.isa.org