BITSIGHT

REPORT

Bitsight identifies nearly 100,000 exposed industrial control systems

Written by Noah Stone, Senior Manager, Thought Leadership

Research by Pedro Umbelino, Principal Security Researcher

Bitsight has identified nearly 100,000 exposed industrial control systems (ICS) owned by organizations around the world, potentially allowing an attacker to access and control physical infrastructure such as power grids, traffic light systems, security and water systems, and more. ICSs — a subset of operational technology (OT) — are used to manage industrial processes like water flow in municipal water systems, electricity transmission via power grids, and other critical processes. Critical infrastructure sectors heavily rely on ICSs to control cyber-physical systems, compounding concerns that the exposed systems identified in this research could present significant risks to organizations and communities around the world.

Fortune 1000 organizations are among the exposed, including organizations from 96 countries and a variety of sectors.

To measure device exposure, Bitsight identified exposed ICSs and mapped them to our inventory of global organizations. Our analysis reveals that — contrary to industry norms — thousands of organizations are using ICSs directly reachable from the public internet, presenting a series of potential consequences of which private and public sector leaders should be aware.

Exposed Systems and Potential Consequences

In recent years, both opportunistic and advanced cyber threat actors have shown increased willingness to target industrial and operational sites. In response to these threats, Schneider Electric — a global leader in the digital transformation of energy management and automation — recently partnered with Bitsight to help strengthen industrial security by providing more visibility into industrial infrastructure and ICS devices that may be at risk of a cyber breach.

Notwithstanding progress, ICS — and more broadly, OT — security remains a complicated and global concern.

What are industrial control systems?

Industrial control systems allow organizations to control industrial machinery, equipment, and other physical infrastructure.

Examples of industrial control systems include:

- Sensors that report field data to controllers.
- Actuators, switches, valves, and relays that control the movement of machinery.
- Building management systems (BMS) that control the operation of elevators and escalators, fire and safety systems, and security systems.
- Automatic tank gauges (ATG) that monitor fuel levels in commercial fuel tanks like those at consumer gasoline stations.

These ICS devices are used to control much of the physical infrastructure in our society, from traffic lights to vaccine production. An attacker's control and manipulation of these systems is a serious matter.

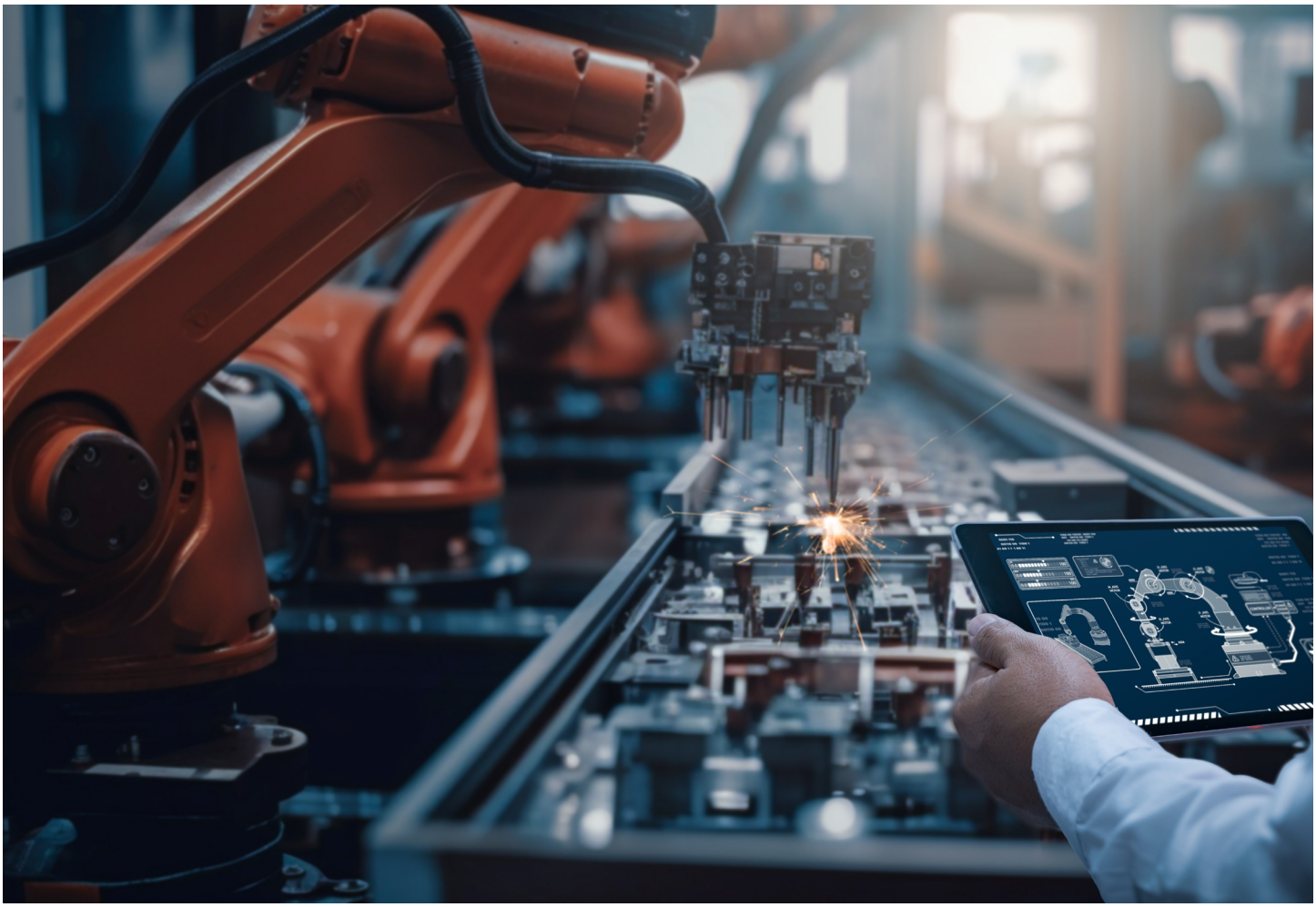
Potential consequences of exposed industrial control systems

Many of the physical systems ICSs control can be critical to a region's or organization's functioning. Therefore, disruption of these systems could lead to significant business disruption, threats to human safety, data and intellectual property (IP) compromise, national security threats, and more.

Cyber attacks leveraging physical infrastructure are not new:

- Last month, reports claimed **attackers breached a national power grid** in Asia;
- A ransomware event targeting the Colonial Pipeline **disrupted oil and gas delivery on the eastern coast of the United States, causing shortages and panic;** and
- Industroyer malware in 2016 targeted **Kyiv, Ukraine's electrical supply,** shutting down power in targeted regions.

Many industrial systems — whether critical infrastructure or not — use old, hard-to-patch software but still play critical roles in societies and organizations, so patching downtime is costly or inflicts inconvenience or suffering on the population. Shutting down a power grid or otherwise critical industrial environment to fix issues has far reaching consequences typically greater in magnitude than those experienced from shutting down an information technology (IT) environment. OT systems are therefore more complicated to secure and present unorthodox bottlenecks unlike those experienced on the IT front.

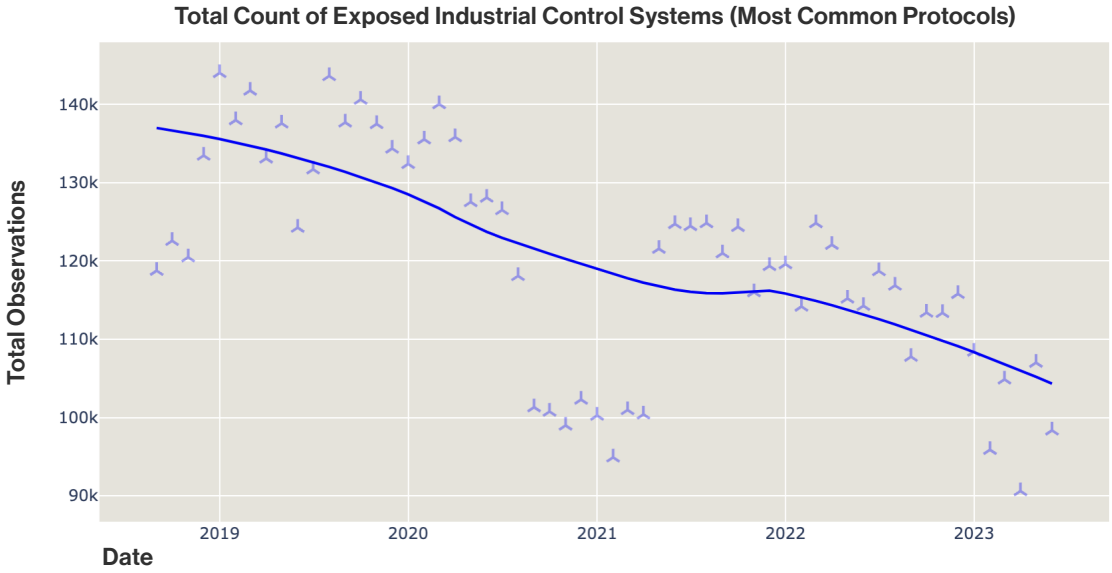


Global State of Exposure

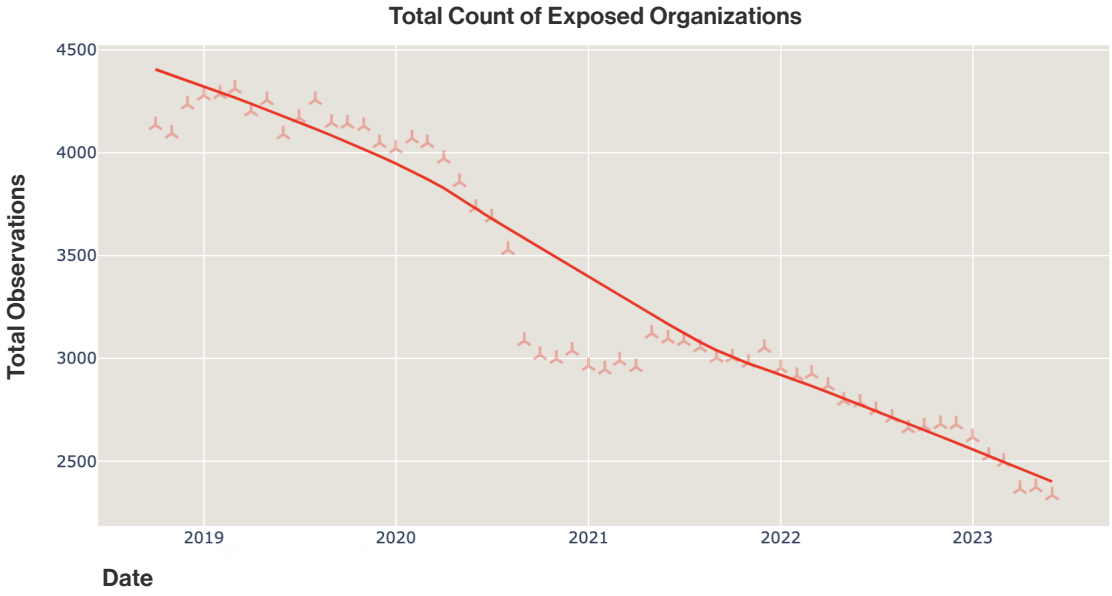
Bitsight identified exposed industrial control systems around the world, revealing both concerning and promising trends. We studied systems communicating via the most commonly used ICS protocols, including Modbus, KNX, BACnet, Niagara Fox and others.

ICS exposure remains high albeit trending downward

The number of exposed — or internet-facing — industrial control systems remains high at nearly 100,000 as of June 2023, but our research revealed a promising trend. From 2019 to June 2023, we observed a decline in the number of ICSs exposed to the public internet. This is a positive development, suggesting that organizations may be properly configuring, switching to other technologies, or removing previously exposed ICSs from the public internet.

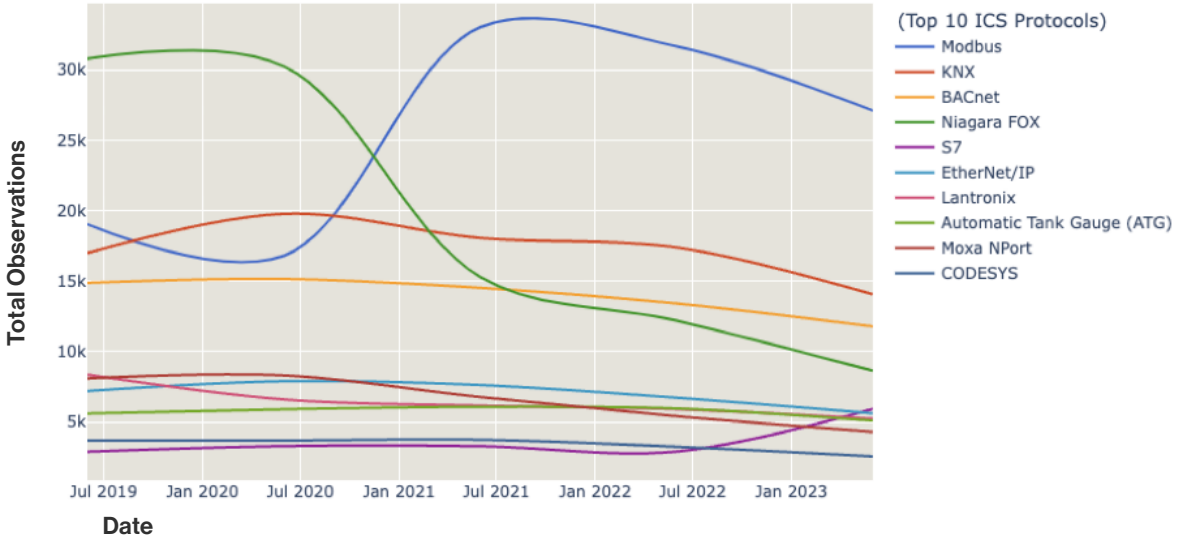


The decline in exposed organizations — those organizations using at least one exposed industrial control system — follows a similar trajectory:



While the aggregate number of exposed ICSs has been trending downward, we detected unique behavior on a protocol-by-protocol basis. Exposed systems and devices communicating via the Modbus and S7 protocols are more common in June 2023 than before, with the former increasing in prevalence from 2020 and the latter more recently from mid-2022. However, exposed industrial control systems communicating via Niagara Fox have been trending downward since roughly 2021. Organizations should be aware of these changes in prevalence to inform their OT/ICS security strategies. One of the first steps in mitigating OT risk is knowing where the risk is likely to lie.

Count of Exposed Industrial Control Systems



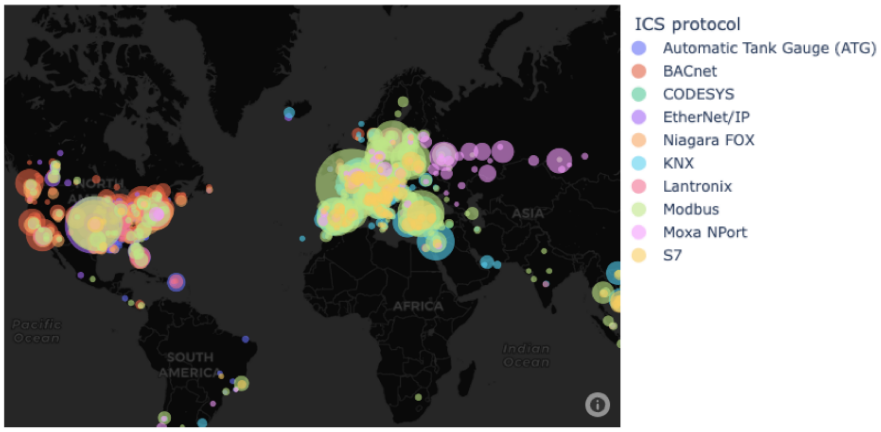
Geographic distribution of exposed industrial control systems

Exposed industrial control systems are spread across the globe, with notable concentrations of systems relying on specific protocols. The geographic distribution of these exposed systems is important – private and public sector leaders should leverage this information to identify which protocols are most prevalent in geographies relevant to their operations, business or otherwise.

For example, organizations with operations in the United States and Europe may approach their strategy differently. Exposed industrial control systems using CODESYS, KNX, Moxa Nport, and S7 are largely concentrated in the European Union (EU). Therefore, EU-based organizations — including government agencies and businesses — may opt to focus on these protocols first. Meanwhile, exposed systems using ATG and BACnet largely reside in the United States, likely warranting more acute attention from organizations based in or operating in the U.S.

Bridging the gap are protocols with significant global relevance, such as Modbus, Niagara Fox and others. Explore global prevalence using the map below, a fully interactive version of which can be found at the Bitsight blog.

Exposed Industrial Control Systems



Bitsight found the top 10 countries by number of organizations having at least one exposed ICS ("exposed organizations") are the following:

1. United States
2. Canada
3. Italy
4. United Kingdom
5. France
6. Netherlands
7. Germany
8. Spain
9. Poland
10. Sweden

Country callout: U.K.

U.K. organizations — and organizations with operations in the U.K. — should be alerted to recently identified industrial control systems (ICS) exposed to the public internet. These exposures could potentially allow an attacker to access and control physical infrastructure such as power grids, traffic light systems, security and water systems, and more. The U.K. ranks as having the second-largest number of exposed organizations in Europe, with heavy concentrations of exposed systems in the London metropolitan area, Cambridge, and Brighton.

Exposed organizations are mostly from the following sectors, along with the most common exposed ICS protocol, respectively:

- Technology (BACnet)
- Telecommunications (Excluding Service Providers)(Modbus/Niagara FOX)
- Education (Modbus)

U.K. officials, business leaders, and society at large should be aware that most of the exposed organizations identified in this research are from the Technology sector. The exposed industrial control systems used in this sector could potentially control critical systems like building management systems (BMS) that, if attacked, could lead to a catastrophic event. Therefore, it is critical that organizations promptly assess exposure and engage in remediation efforts.

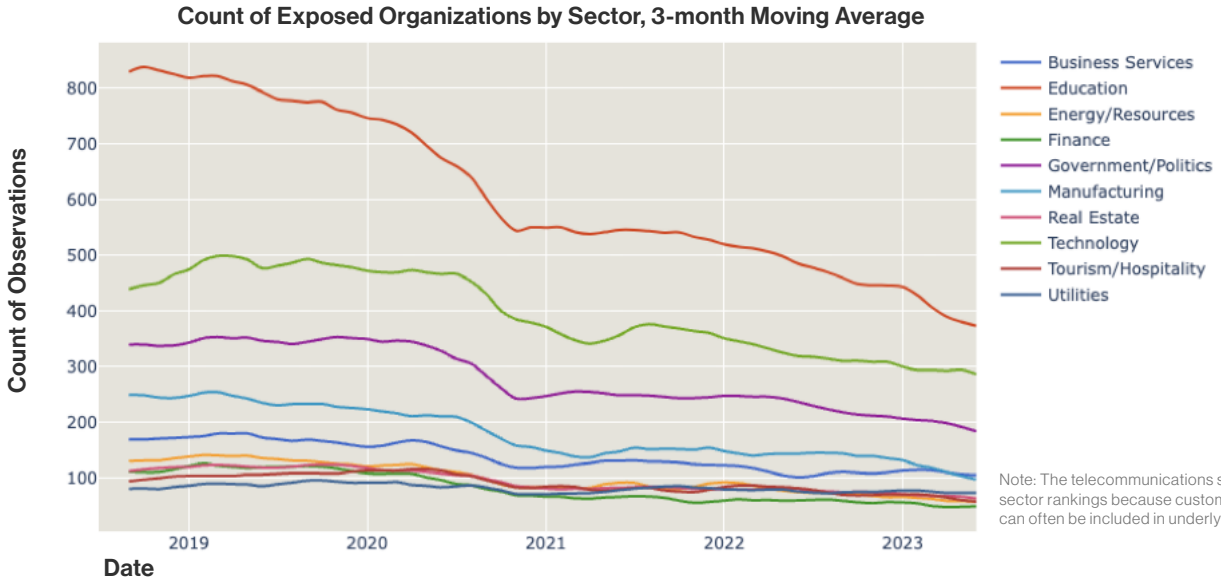
Sectors with the greatest degree of exposure

The number of organizations with exposed ICSs has been steadily declining since mid-2018. While these reductions in exposed entities are a positive development, the figures remain high. This indicates that exposed ICSs remain a significant risk to organizations, their partners, and their constituents.

As of June 2023, the top 10 sectors by exposed organizations are:

1. Education
2. Technology
3. Government/Politics
4. Business Services
5. Manufacturing
6. Utilities
7. Real Estate
8. Energy/Resources
9. Tourism/Hospitality
10. Finance

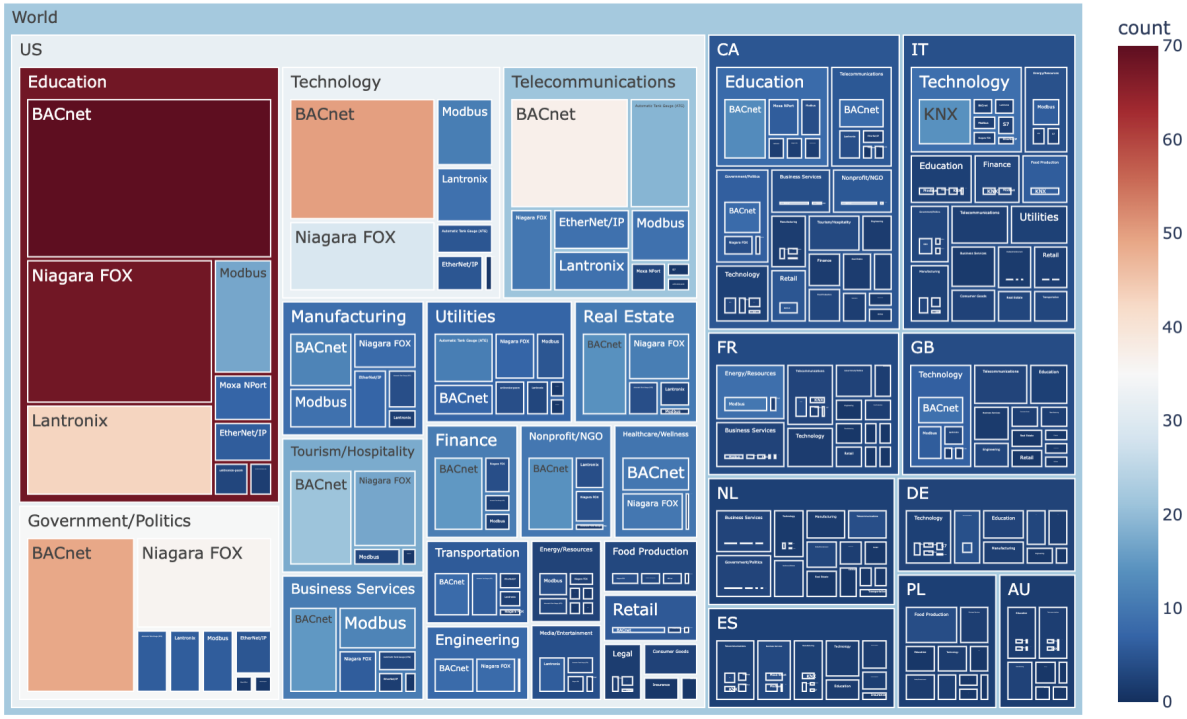
We observed broad declines in the number of exposed organizations across sectors:



Note: The telecommunications sector was excluded from sector rankings because customer-owned infrastructure can often be included in underlying reporting data.

To better understand ICS exposure, Bitsight revealed where exposed organizations are headquartered, to which sector they belong, and the protocol used by the exposed device(s). The tree map below — fully interactive on the Bitsight blog — is a great way for government officials, business leaders, and security professionals to explore global exposure in countries and sectors of interest, revealing targeted information potentially helpful in responding to these exposures.

Exposed Organizations by Country, Sector, Protocol



Note: Data related to the telecommunications sector may include underlying customer infrastructure.

Recommendations

For security leaders

Organizations should immediately engage in outreach and remediation efforts:

- Identify any industrial control systems deployed by your organization and/or your third-party business partners, and promptly assess the security of these systems.
- Remove any industrial control systems from the public internet.
- Employ safeguards like firewalls to protect against unauthorized access to your industrial control systems.

Security leaders must acknowledge the unique control needs that apply to OT including industrial control systems rather than just apply a traditional IT risk model to this infrastructure.

For ICS manufacturers

Manufacturers of industrial control systems and other operational technology must take action to increase the cybersecurity of their devices. This includes improving device security prior to deployment and working with clients to ensure the proper configuration and security of already deployed devices. Some manufacturers are leading with innovative initiatives to improve the security of their devices and their customers. For example, Schneider Electric has made device security and customer security a business priority. Through a joint effort with Bitsight, Schneider Electric is working to identify externally observable risks to the OT community and engage customers in remediation initiatives.

Manufacturers should follow Schneider Electric's lead and take steps to:

- Use secure-by-design principles to develop more secure technology.
- Improve the security posture of deployed equipment and machinery by leveraging data and insights.
- Build programs to accurately and swiftly detect misconfigured or otherwise exposed systems.

For government policymakers

The exposed systems identified in this research should alert policymakers to the current state of ICS — and more broadly, OT — security.

Due to the potentially serious consequences resulting from incidents involving industrial systems, policymakers should:

- Understand the risks of exposed industrial control systems, particularly those involving critical infrastructure.
- Inform national security strategies and programs to include adversarial threats targeting operational technology, and how an industrial cyber attack could impact national security and human safety.
- Quantify the impact — financial and otherwise — that a cyber attack targeting industrial infrastructure could inflict on national, regional, and local economies as well as diplomatic relationships.

If you believe you may have an issue, please contact Bitsight so we can help. →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT