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.

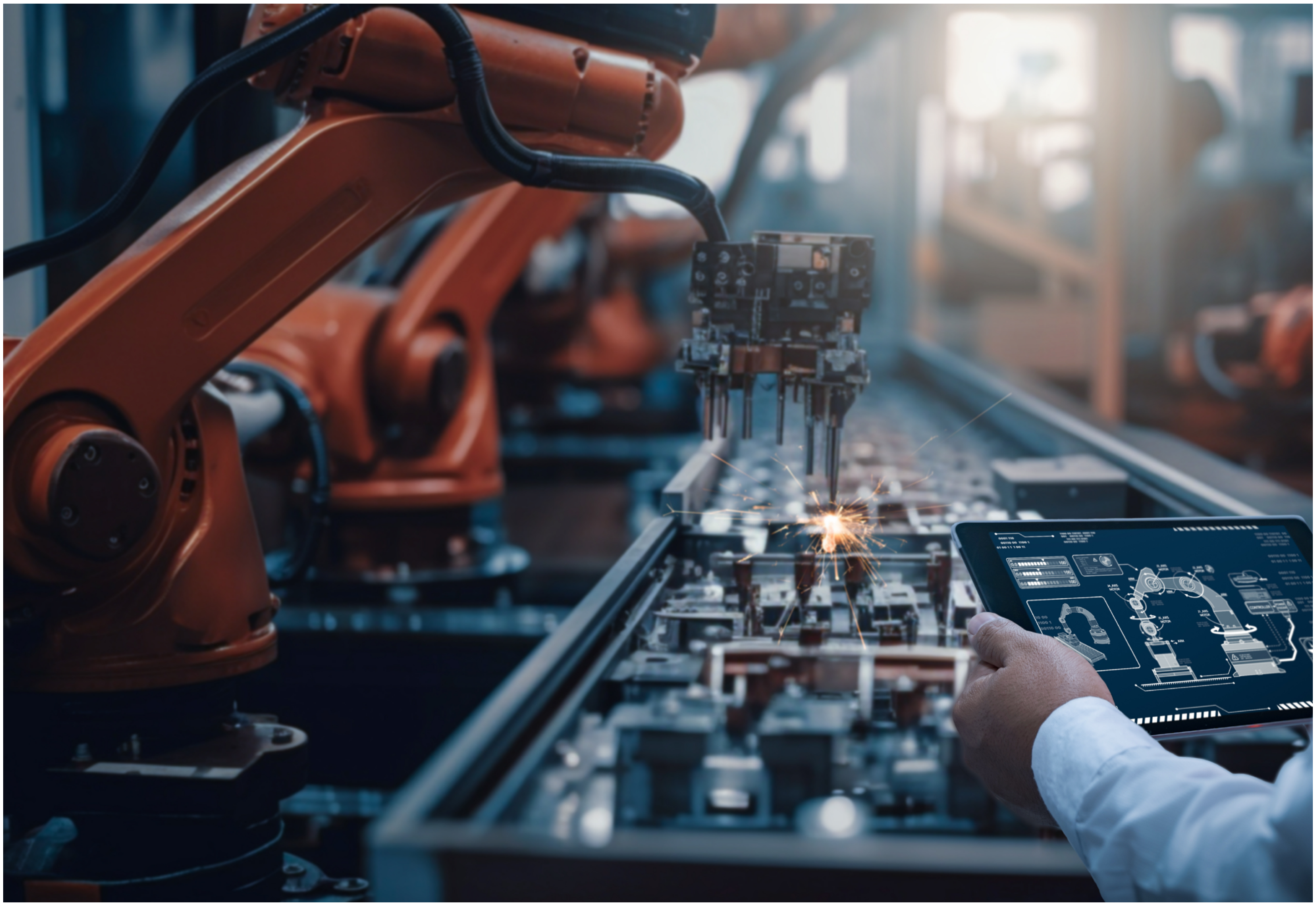
Potential consequences of exposed industrial control systems

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.

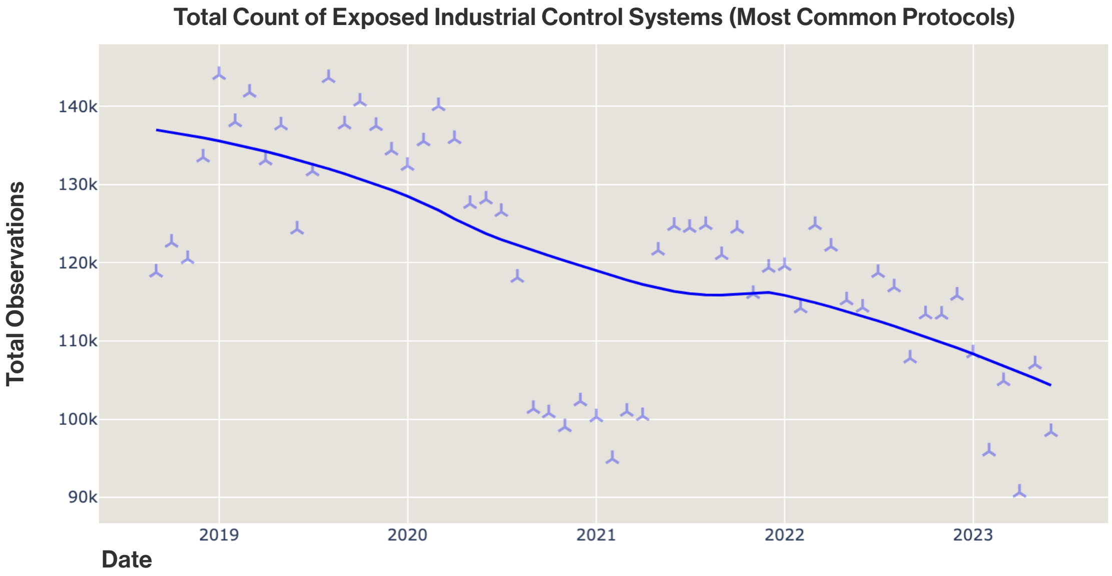


Global State of Exposure

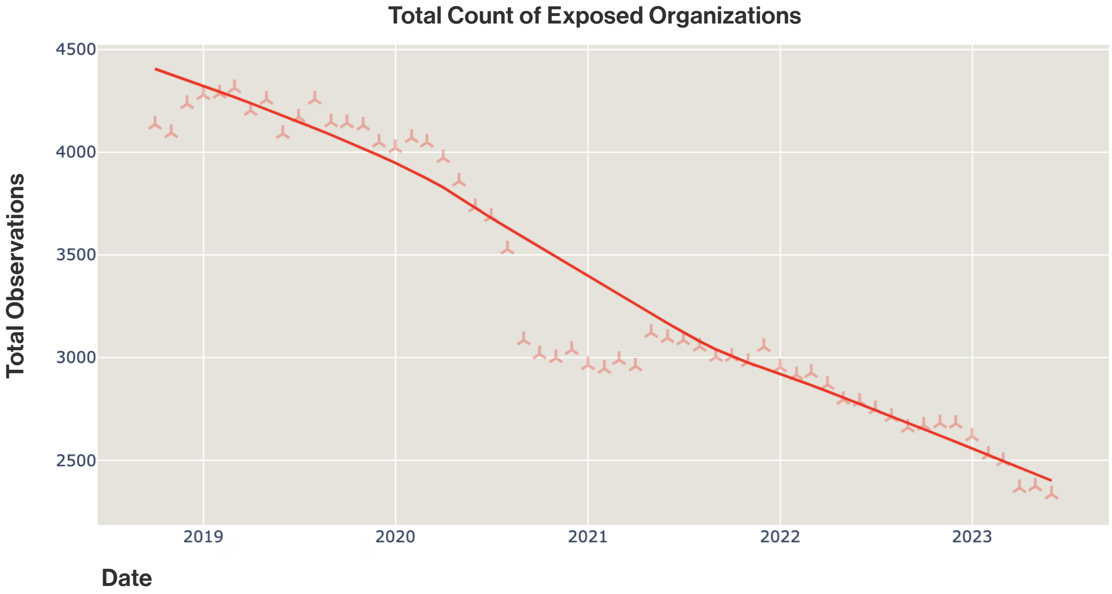
Bitsight identified exposed industrial control systems around the world, revealing both concerning and promising trends. We studied systems communicating via the most commonly used ICS protocols, including Modbus, KNX, BACnet, Niagara Fox and others.

ICS exposure remains high albeit trending downward

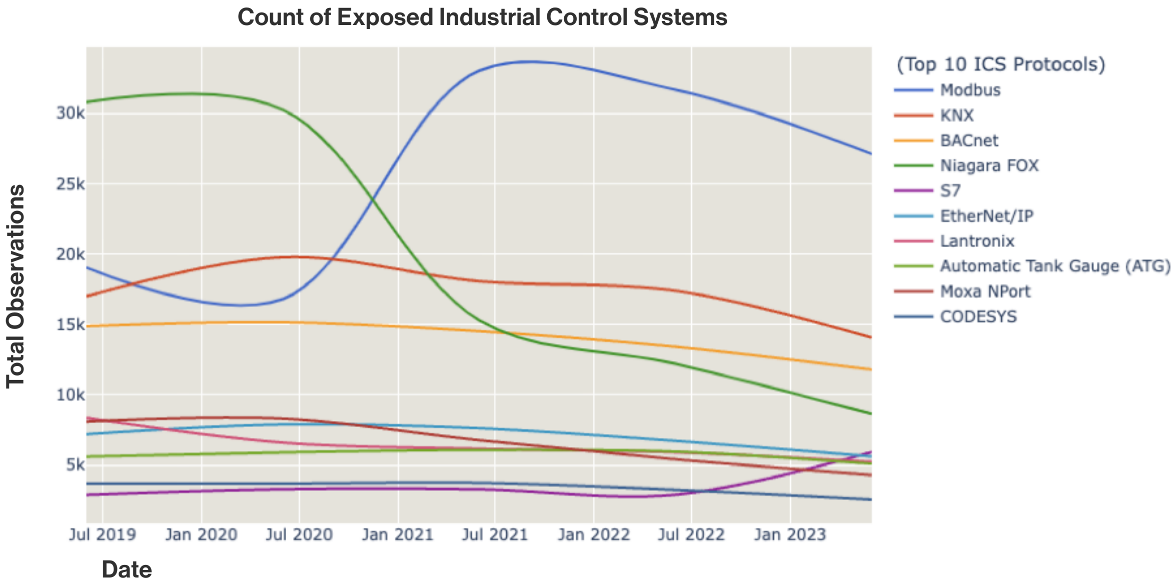
The number of exposed — or internet-facing — industrial control systems remains high at nearly 100,000 as of June 2023, but our research revealed a promising trend. From 2019 to June 2023, we observed a decline in the number of ICSs exposed to the public internet. This is a positive development, suggesting 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.



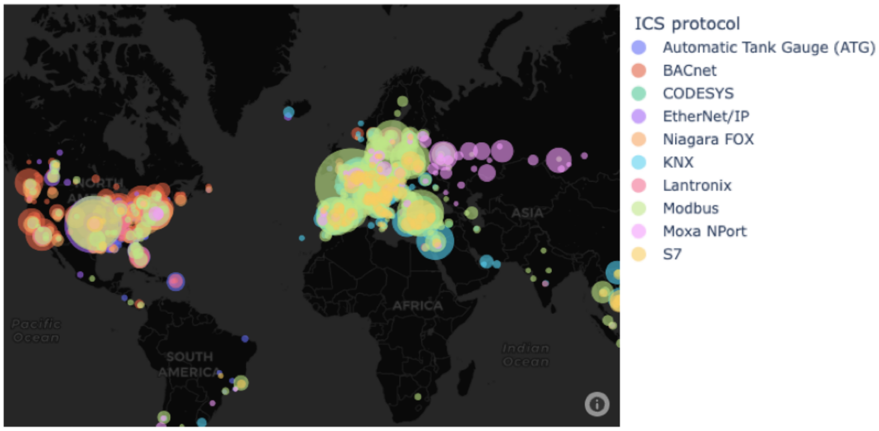
Geographic distribution of exposed industrial control systems

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: France

French organizations — and organizations with operations in France — should be alerted to the exposed industrial control systems identified in this research. **France ranks as having the third-largest number of exposed organizations in Europe,** with heavy concentrations of exposed systems in the Paris metropolitan area.

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

- Energy/Resources (Modbus)
- Business Services (Modbus)
- Telecommunications (Excluding Service Providers)(Modbus)

French and European officials, business leaders, and society at large should be aware that most of the exposed organizations identified in this research are from the Energy/Resources sector. The exposed industrial control systems used in this sector could potentially control critical infrastructure systems that, if attacked, could lead to a catastrophic event. Therefore, it is critical that organizations promptly assess exposure and engage in remediation efforts.

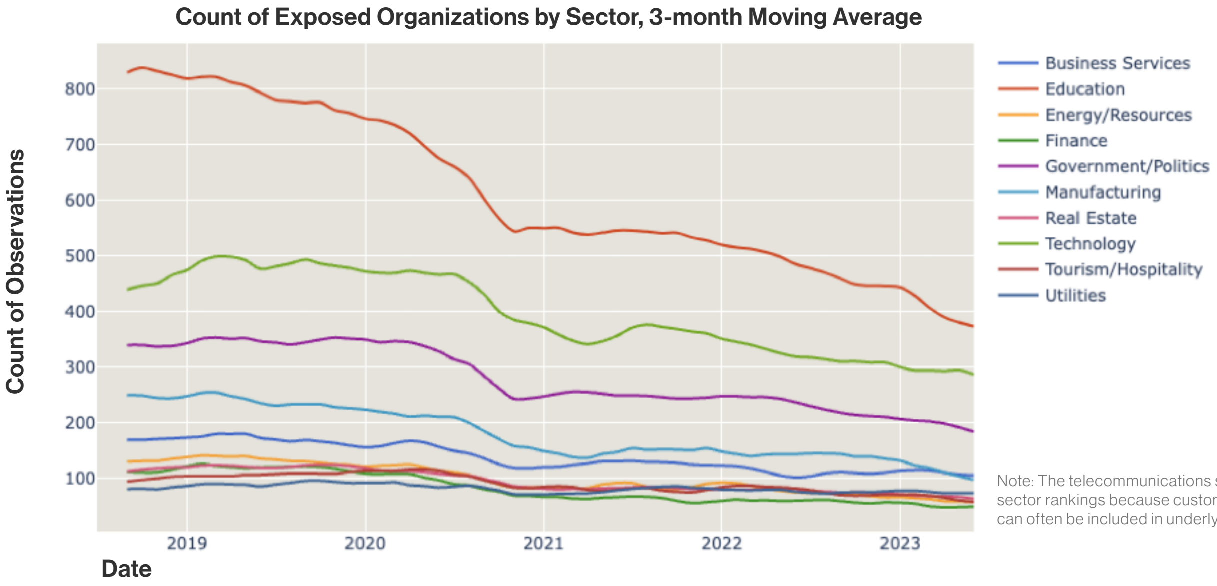
Sectors with the greatest degree of exposure

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

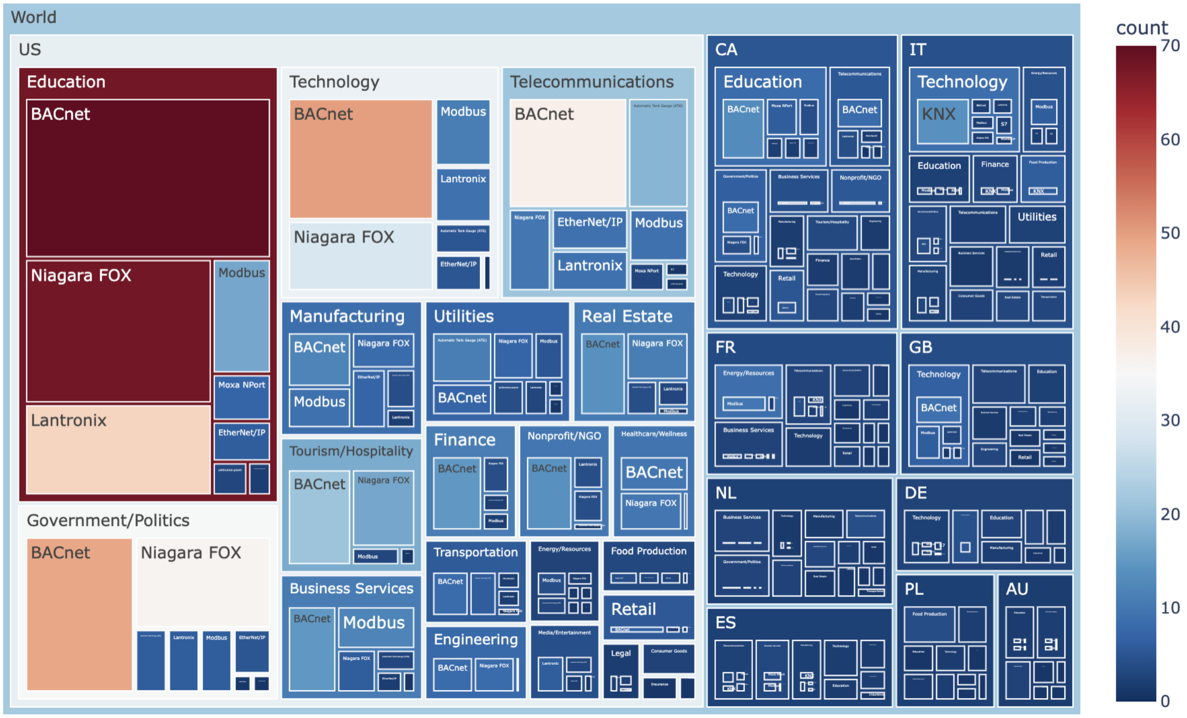
We observed broad declines in the number of exposed organizations across sectors:



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

BITSIGHT

DATA SHEET

Un leader mondial de la gestion des cyber risques

Bitsight est une entreprise internationale spécialisée en gestion des cyber risques, qui transforme la manière dont les responsables de la gestion des risques gèrent l'incertitude croissante liée à ces risques. Des entreprises du monde entier font confiance à nos solutions intégrées pour gérer les workflows critiques en matière d'exposition, de performance et de risque. Nous stabilisons l'incertitude liée aux cyber risques et nous permettons aux chefs d'entreprise, aux responsables de la gestion des risques et aux conseils d'administration de contrôler et de prendre en charge les risques, et ce en toute confiance.

Un leadership inégalé dans le secteur

La plus vaste communauté de responsables de la gestion des cyber risques à l'échelle mondiale se tourne vers notre héritage en matière d'innovation et de leadership en ce qui concerne la cybersécurité.

+ de 3 000 clients

20% des entreprises du classement Fortune 500

+ de 30 pays

+ de 50 000 utilisateurs

62 industries

Les **4** grands cabinets d'audit comptable et financier (« Big Four »)

7 des **10** premiers cyber-assureurs mondiaux

4 des **5** premières banques d'investissement

120 institutions gouvernementales

50% des primes en matière de cyber assurance à l'échelle mondiale sont souscrites par des clients de Bitsight

Il est temps de devenir le catalyseur de croissance et le stratège audacieux dont votre entreprise a besoin. Les principaux leaders mondiaux en matière de risques s'appuient sur Bitsight pour réduire la probabilité de pertes financières, hiérarchiser les investissements en matière de sécurité et instaurer la confiance dans l'ensemble de l'écosystème.

Des partenariats performants

Nos partenariats de longue date ont renforcé notre solution de gestion des risques en matière de cybersécurité pour l'évaluation des risques liés aux investissements et l'amélioration de la visibilité des investisseurs sur les cyber risques.

- **Moody's Corporation :** l'analyse des données de Bitsight intégrée au processus de notation de crédit de Moody's
- **Glass Lewis :** les évaluations de Bitsight sont intégrées dans 14 000 rapports de votes par procuration
- **Marsh McLennan:** une étude indépendante révèle que les notations de Bitsight en matière de sécurité présentent la corrélation la plus forte du secteur avec la probabilité d'un cyber-incident

Une solution de gestion des cyber risques leader sur le marché

Grâce aux offres solides de Bitsight, les RSSI peuvent développer leurs écosystèmes sans s'inquiéter de la recrudescence des risques. Accélérez la transformation sans risquer les turbulences financières. Ajoutez des fournisseurs sans leurs vulnérabilités. Et faites en sorte que tout le monde parle un langage universel.

Notre solution s'appuie sur le moteur d'analyse des cyber risques (Cyber Risk Analytics Engine) de Bitsight qui fournit des données, des informations et des workflows leaders sur le marché pour la sécurité des entreprises, la supply chain numérique et la cyber assurance.

Données sur les cyber risques à la pointe du marché

Obtenez une vision complète des risques et des vulnérabilités potentiels grâce aux données sur les cyber risques les plus exhaustives sur le marché.

Objectif : une norme universelle

Mesurez et communiquez les cyber risques grâce à la norme universelle la plus fiable et la plus adoptée au monde.

Connaissances exploitables sur les risques

Construisez en toute confiance votre programme de lutte contre les cyber risques grâce à nos observations uniques et exploitables, alimentées par des données et des indicateurs exhaustifs.

+ de 40 millions
d'organisations activement surveillées

260
milliards de découvertes en matière de sécurité à ce jour

45
brevets accordés

1million
d'entités cartographiées

Gestion des performances en matière de sécurité pour la sécurité des entreprises

Une solution de gouvernance de la cybersécurité et de gestion de l'exposition qui fournit des informations analytiques uniques en matière de gouvernance des cyber risques et de gestion de la surface d'attaque externe. Elle permet aux RSSI de communiquer et de prouver en toute confiance les performances du programme auprès des parties prenantes.

Gestion des risques liés aux tiers pour la supply chain numérique

Une solution de bout en bout qui surveille en permanence les tierces et les quatrièmes parties, éliminant ainsi les « angles morts » tout au long de la supply chain. La gestion des risques liés aux tiers permet aux RSSI de réagir aux événements majeurs en matière de sécurité, d'intégrer efficacement les fournisseurs, de se concentrer sur les problèmes urgents et de déployer les programmes.

Cyber Assurance

Veille à la transparence des cyber risques tout au long du cycle de vie du processus de cyber assurance d'une organisation. Les assureurs exploitent nos données parce qu'elles sont corrélées aux violations, ce qui permet de prendre des décisions en matière de souscription, d'atténuer les pertes et d'améliorer l'efficacité opérationnelle.

Bitsight est un leader en matière de gestion des cyber risques qui transforme la façon dont les entreprises gèrent l'exposition, la performance et le risque pour elles-mêmes et leurs tiers. Les entreprises s'appuient sur Bitsight pour hiérarchiser leurs investissements en matière de cybersécurité, renforcer la confiance au sein de leur écosystème et réduire leurs risques de pertes financières. En s'appuyant sur plus d'une décennie d'innovation technologique, ses solutions intégrées apportent de la valeur dans les domaines de la performance relative à la sécurité de l'entreprise, des chaînes d'approvisionnement numériques, de la cyber assurance et de l'analyse des données.

BOSTON (SIÈGE SOCIAL) RALEIGH NEW YORK LISBONNE SINGAPOUR BUENOS AIRES

BITSIGHT