txOne networks

ANNUAL REPORT

Insights Into ICS/OT Cybersecurity 2022

The threat landscape of cyberattacks evolves at the same fast pace as technology, if not faster. As a result, insufficient cybersecurity has even become a matter of national security. Industry 4.0 is a double-edged sword, and the benefits of automation and connectivity come with significant risks. As more industries embrace automation, the threat of supply chain attacks is becoming a real and present danger. Organizations must prioritize OT network protection as the cornerstone of their cybersecurity strategy. However, a strategy cannot be formulated without a clear understanding of the threat it is countering. With this article, TXOne offers these crucial insights.

In 2022, vital industries such as manufacturing, energy, food and agriculture, healthcare, and public health suffered from a sharp increase in cyberattacks carried out by ruthless RaaS, which used multiple extortion strategies to disrupt operations, steal sensitive information, and weaken customer trust and brand value. Car-related product manufacturers were particularly affected, with 24% of victims falling within this classification.

A global survey conducted by Frost and Sullivan on behalf of TXOne Networks showed that the increased complexity of OT and the lack of visibility into third-party security capabilities are becoming serious security challenges for organizations. The survey also revealed that 94% of IT security incidents have also impacted the OT environment as IT and OT become more integrated.

Despite the rising threat, only 6% of organizations have 100% of their Windows devices protected by endpoint security solutions. Additionally, despite increased investment in OT security, 70% of organizations are still considering adopting IT security solutions for the OT environment. This is not a time for complacency or half-measures. Organizations that do not prioritize comprehensive, integrated, and performant cybersecurity solutions are putting themselves and their stakeholders at risk.

In addition, the energy industry is a prime target for cyberattacks on critical infrastructure, and geopolitical conflicts are escalating critical infrastructure security risks. Governments must confront this fact, as a successful compromise could seriously impact a country. State-supported or politically motivated attackers continually target critical infrastructure, and cyberattacks can be wielded as weapons against entire nations and governments. The interdependence in utilities industries and the threat of APT and ransomware attacks on suppliers is also a severe concern. Critical infrastructure industries are often interconnected, and in the event of a cyberattack on a supplier, the corresponding industry may be unable to provide stable public infrastructure services. This highlights the potential impact on national economies.

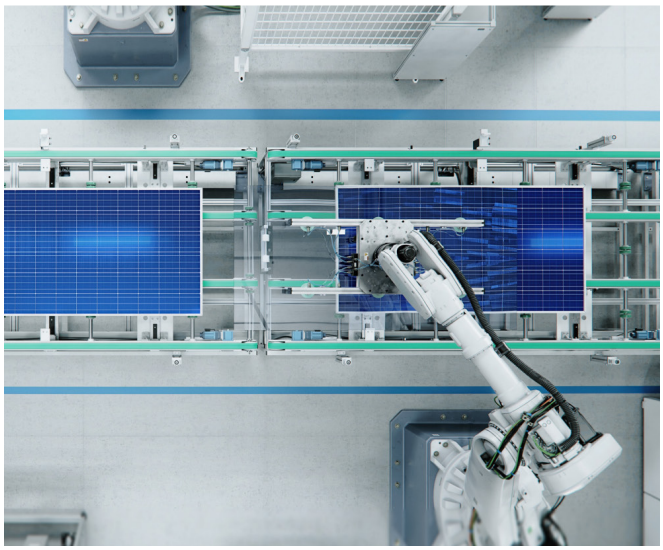
One of the challenges in securing critical infrastructure is the vast and complex network of interconnected systems that make up the infrastructure. This complexity creates a multitude of entry points for attackers, making it difficult to protect all of the components of the system adequately. Additionally, many of the systems that make up critical infrastructure were designed without security in mind, leaving them vulnerable to attack.

Moreover, the threat of cyberattacks is not limited to traditional forms of critical infrastructure, such as power grids and water treatment plants. The proliferation of connected devices and the Internet of Things (IoT) has expanded the attack surface and created new vulnerabilities that can be exploited by attackers. These include devices that control home security systems, medical devices that monitor patient health, and even cars that are connected to the internet.

To address these risks, governments and organizations must take a proactive approach to cybersecurity. This includes investing in the development of secure systems and technologies, as well as implementing robust cybersecurity policies and protocols. Organizations must also conduct regular risk assessments to identify vulnerabilities in their systems and take steps to address them.

In order to formulate a robust cybersecurity strategy, a crucial component is effective incident response planning. In the event of a cyberattack, organizations must be prepared to respond quickly and decisively to minimize the damage and restore services as quickly as possible. This requires a coordinated effort between various departments and stakeholders.

Employees and contractors with access to critical infrastructure systems must be trained to recognize and report potential security threats. This includes basic security practices, such as strong password management, as well as more advanced techniques, such as social engineering and phishing. This publication goes into deep detail on how organizations from major countries worldwide have approached their cybersecurity strategy thus far in the hopes of providing guidance on how to better navigate the increasingly perilous threat landscape in the immediate future.



Clearly, it is important to recognize that cybersecurity is an ongoing process that requires continuous monitoring and improvement. Organizations must regularly assess their systems and processes to identify areas for improvement and take steps to implement the necessary changes. This includes staying up to date with the latest threats and vulnerabilities and adapting security measures accordingly.

The consequences of cyberattacks can be severe and far-reaching. The future of OT security requires a different set of security solutions, skills, processes, and methods than IT. Building specific cyber defenses to manage OT/ICS security risks is not an option; it is a necessity. Don't wait until it's too late - act urgently to protect yourself and your organization from cyberattacks that can cause irreparable damage. To understand the gravity of the situation and learn how to protect yourself and your organization from the ever-evolving threat. Download our full report at https://www.txone.com/security-reports/insight-into-ics-ot-cybersecurity2022/.

Download TXOne Cybersecurity Report 2022