# Information security risks at industrial companies

ptsecurity.com

# Attacks on industry

Industrial companies attract criminals by their size, the importance of business processes, and their impact on the world and people's lives. For example, a man-made accident at a hydroelectric power plant can leave an entire country without electricity, as happened in Venezuela, where the nationwide blackouts lasted for a full five days. Downtime at an automobile plant can lead to major losses, as was the case of the Honda plant hit by a ransomware attack. Fortunately, cyberattacks on industrial companies with such serious consequences are just isolated cases, as they require a higher level of attacker qualification. The mission of information security experts is to make sure that industrial accidents do not become a regular occurrence. To do this, it is necessary to identify unacceptable events and achieve a level of information security that will prevent such events from happening as a result of a cyberattack.

In 2020, the industrial sector was the second most popular target for hackers after the government sector: according to our analysis, 12 percent of attacks were aimed at industrial companies.

The main threats for industrial companies are espionage and financial losses. Thus, in 2020, hackers were mostly motivated by data theft (84% of cases), while financial gain was the aim of 36 percent of criminals.



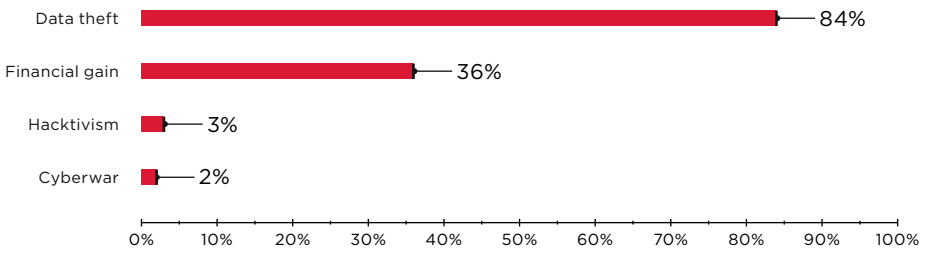


Figure 1. Motives of cyberattacks on industrial companies in 2020

The consequences of cyberattacks can be:

### Interruption of operations

After a ransomware attack on the corporate network of automaker Honda, the company had to halt production at several plants for a full day. After such an attack, it takes a lot of effort for the company to return to normal operations, restore full functionality of technological and business systems, and prevent a recurrence of such incidents in future.

### Disruption of technological processes

In May 2021, Colonial Pipeline, the largest U.S. fuel supplier, suffered a ransomware attack. The week-long downtime of the company's computer systems led to a shutdown of half of the company's gas stations in several southeastern states, an increase in wholesale gasoline prices, and roaring demand for fuel. In 2020, attackers tried to attack water-supply and purification systems in Israel. Finally, in February 2021, a hacker managed to obtain access to the water treatment systems in a small U.S. city and change the chemical composition of the water.

### Disruption of business processes

In February 2020, as a result of a hacker attack, Croatian oil company INA was unable to issue invoices, register loyalty card use, issue new mobile vouchers, and allow customers to pay gas utility bills. The culprit was the Clop ransomware, which encrypted data on the company's internal servers, disrupting business processes.

Today, the main objective of information security specialists is to assess the feasibility of various security risks in companies and identify the possible consequences of cyberattacks; and then build an efficient security system based on this knowledge. The problem is that a company's management will never agree to any action in the infrastructure that could negatively affect the technological process.

## Risk feasibility assessment at the cyber-range

Cyberexercises are controlled attacks that assess and improve the detection and response skills of information security experts. In The Standoff cyberexercises, attacks are emulated by attacker teams consisting of information security experts.

In May 2021, at The Standoff cyber-range, attacker teams were tasked with triggering information security risks at a gas distribution station. The conditions matched reality as closely as possible. Even network interaction was via standard ICS protocols, such as OPC DA, Modbus TCP, UMAS, IEC 60870-5-101, Siemens Simatic S7, Siemens DIGSI, Vnet/IP, CIP (Ethernet/IP), IEC 61850, and BACnet/IP.

It took the attackers two days to disrupt the gas flow at the station. They gained access to the gas station management system, stopped the gas flow, and caused an explosion. Each day, the defenders registered an average of 32 incidents at the company's office.

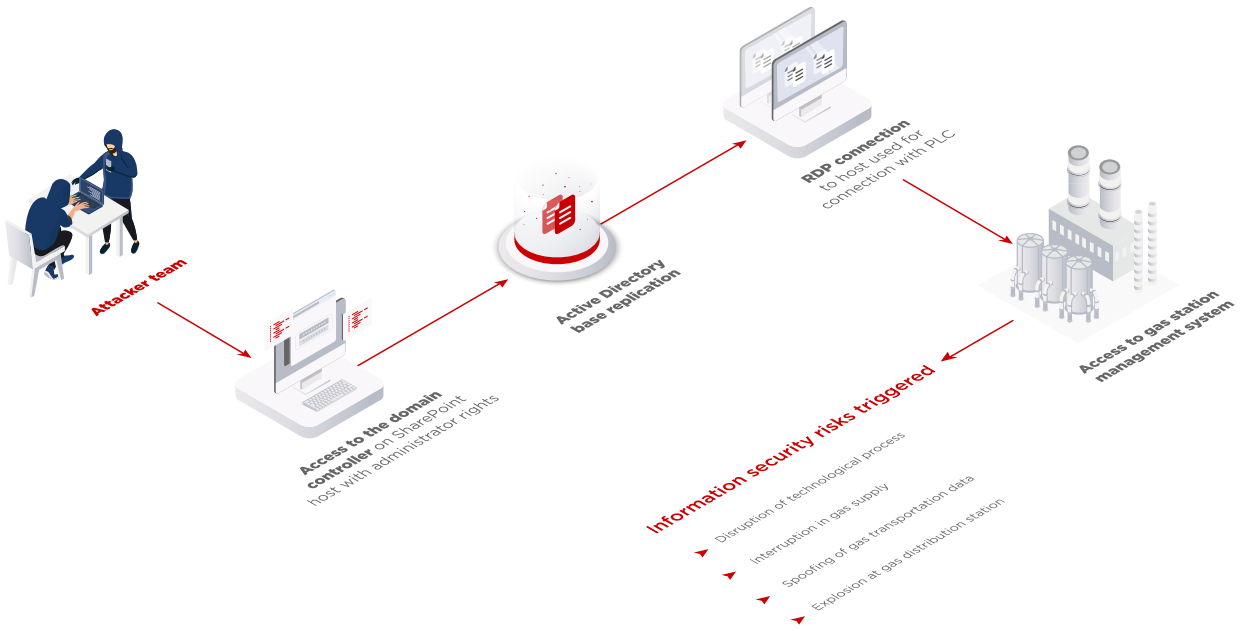


Figure 2. Simplified scheme of triggering information security risks at a gas distribution station during The Standoff 2021

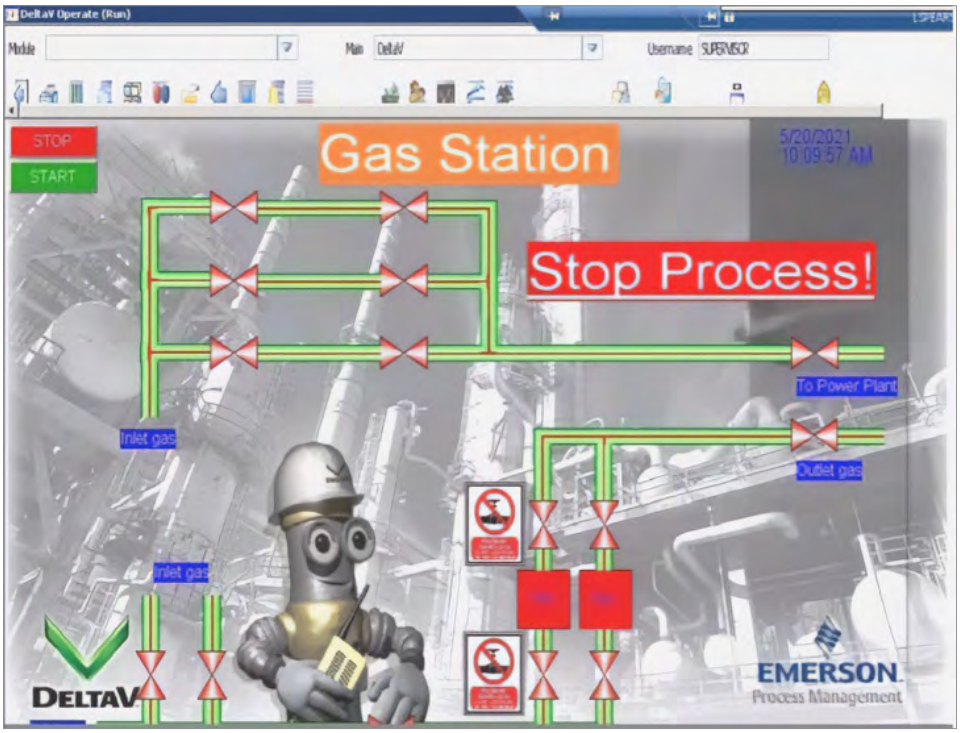


Figure 3. Gas distribution station: several seconds before the explosion

The real-life consequences of such risks triggered at a gas distribution station can include human losses, management resignation, lawsuits, erroneous actions or omissions by staff in case of an emergency, equipment failure, restoration costs, and loss of profits due to downtime.

When analyzing the security of an industrial company's real infrastructure, information security experts will most likely be able to demonstrate only the spoofing of gas transportation data in the monitoring system. They will certainly not be allowed to conduct attacks that can disrupt or stop technological or business processes, making it impossible to carry out a risk feasibility study.

# Information security risks at industrial companies

When analyzing the security of companies' infrastructure, Positive Technologies experts look for vulnerabilities and demonstrate the feasibility of attacks by simulating the actions of real hackers. In our experience, most industrial companies have a very low level of protection against attacks. Our studies revealed the following most common vulnerabilities:

- Low level of protection of the external network perimeter accessible from the Internet
- Low level of protection against hackers penetrating the industrial network
- Device misconfiguration
- Flaws in network segmentation and traffic filtering
- Dictionary passwords
- Use of outdated software

Security assessments conducted in 2020 revealed that in 91 percent of industrial organizations, an external attacker can penetrate the corporate network. Once inside the internal network, attackers can obtain user credentials and full control over the infrastructure in 100 percent of cases, and in 69 percent of cases they can steal sensitive data, including information about partners and company employees, email correspondence, and internal documentation. But most importantly, at 75 percent of industrial companies[1] our experts managed to gain access to the technological segment of the network. This allowed criminals to obtain access to industrial control systems in 56 percent of cases.

Such statistics are alarming, and it is vital to understand their causes. PT NAD pilot projects conducted by our experts reveal numerous suspicious events in the internal network of each industrial company.

PT NAD is a deep network traffic analysis system used to detect attacks on the perimeter and in the network. PT NAD knows everything that is going on in the network, detects malicious activity even in encrypted traffic, and facilitates incident investigation.

Some of these network anomalies may indicate a possible hacker attack:



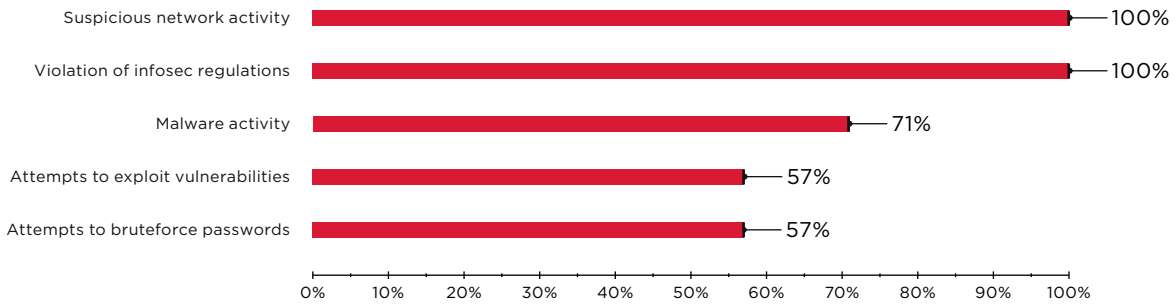


Figure 4. Information security threats actuated during the PT NAD pilot projects at industrial companies in 2020

For example, at one industrial organization, PT NAD registered an RDP connection to an external cloud storage. A total of 23 GB of data was transferred to the address of this storage via RDP and HTTPS.

In addition, industrial companies often use outdated software. According to statistics by cybersecurity company Claroty, the number of vulnerabilities in ICS components has grown steadily in recent years. In 2020, security experts detected 25 percent more vulnerabilities than in 2019, mostly affecting the energy sector, manufacturing, and water treatment plants. The problem is that in order to update industrial equipment, a special "maintenance window" is required, which is only allowed a few hours a week or even month.

1 Based on the results of 12 internal and external security assessments of corporate information systems conducted in 2017–2020, the goal of which was to gain access to industrial networks.

The attack vector on critical systems can be simple. For example, during a security assessment of one industrial company, Positive Technologies experts penetrated the corporate network and obtained maximum privileges in the domain. Next, they collected information about the industrial network hosts, obtained the ICS equipment connection schemes, and found out that one computer was connected to the ICS network. Using this node, the experts accessed the industrial network.

A common error in administering such computers is to save connection parameters (username and password) in a remote access authentication form (for example, via RDP). By obtaining control over such a computer, an attacker can connect to the resources of an isolated segment without credentials. In addition, connection parameters, addresses, schemes, and passwords for systems in industrial networks are often stored in cleartext (for example, in Excel spreadsheets) on the computers of engineers and other persons in charge.

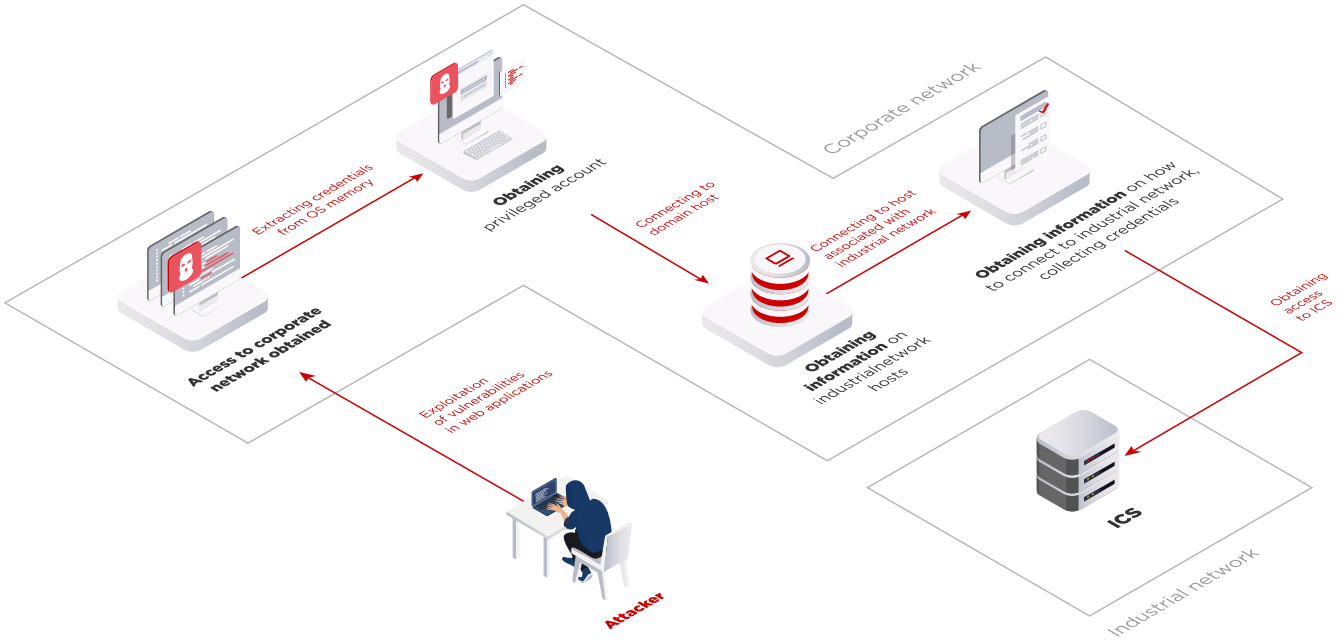


Figure 5. Vector of attack on an industrial network

Attackers with access to ICS can trigger the following risks:

- Interruption of operations
- Industrial equipment failure
- Damage to products
- Accidents

However, it is impossible to verify these risks in the real infrastructure precisely because of the negative impact it can have on technological processes.

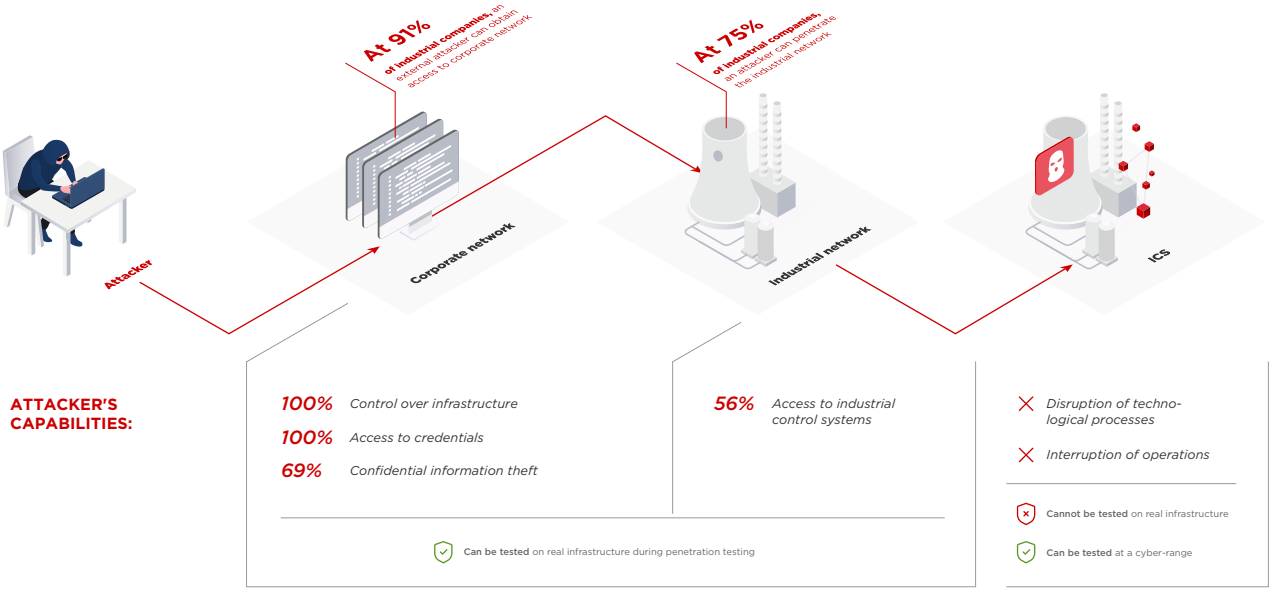


Figure 6. Results of the security assessment of industrial companies performed by Positive Technologies

# Conclusion to be drawn

The industrial sector has become increasingly attractive to hackers in recent years. Attacks are getting more successful and their scenarios more complex. On the other hand, companies often cannot detect a targeted cyberattack on their own. They may remain under the illusion of security for years on end, considering the likelihood of cyberrisk actuation to be minimal. The situation is exacerbated when such companies have blind faith in the reliability of security automation tools, and do not put infrastructure robustness to the test. Unfortunately, security assessments prove that attackers can easily gain access to such systems.

More than anywhere else, the protection of the industrial sector requires modeling of critical systems to test their parameters, verify the feasibility of business risks, and look for vulnerabilities.

A cyber-range is an advanced solution for assessing the security of production systems without disrupting real business processes, as well as for correctly verifying risks and their consequences, and evaluating potential damage. Cyber-range simulation of risks reveals the criteria of their actuation, that is, the preconditions and possible consequences of such attacks. This increases the efficiency of other security assessment tasks. In addition, a cyber-range is a place where information security specialists can test their skills in detecting and responding to incidents.

Risk simulation results guide a company in strengthening the protection of its infrastructure against cyberthreats.


## About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays


For 19 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.