Kaspersky ICS CERT

kaspersky

Q2 2024 – a brief overview of the main incidents in industrial cybersecurity

08.11.2024

Version 1.1

Executive summary 3
Quick stats for the quarter 4
Manufacturing 6
HOYA hit by cyberattack 6
Targus hit by ransomware 6
Swisspro hit by ransomware 7
Le Slip Français hit by cyberattack 7
Lemken hit by cyberattack 7
Crown Equipment hit by cyberattack 8
LivaNova hit by cyberattack 8
Taiwan United Renewable Energy hit by cyberattack 9
Electronics 9
Dell data breach 9
BECOM hit by cyberattack 10
Key Tronic Corporation hit by ransomware 10
Nexperia hit by ransomware 11
GlobalWafers hit by ransomware 11
Automotive 11
Sandhar Technologies hit by cyberattack 11
Meiller Kipper hit by cyberattack 12
CDK Global hit by ransomware 12
Food and beverage 13
Lewis Brothers Bakeries hit by ransomware 13
Agropur hit by cyberattack 13
Construction 14
Eucatex hit by cyberattack 14
Wehrle-Werk hit by cyberattack 14
Max Wild hit by ransomware 14
Pharmaceutical 15
Octapharma Plasma hit by ransomware 15
Rekah hit by cyberattack 15
Pharmascience hit by cyberattack 16

Mining and Metallurgy 16
Westfälische Stahlgesellschaf hit by ransomware 16
Schuette hit by ransomware 16
Northern Minerals hit by ransomware 17
Iluka Resources hit by cyberattack 17
Logistics and transportation 18
Barnett's Couriers hit by cyberattack 18
Skanlog hit by ransomware 18
Porto de São Francisco do Sul hit by ransomware 18
Ocasa hit by ransomware 19
Utility 19
Tipton Municipal Utilities hit by cyberattack 19
Emcali hit by ransomware 20
Sawnee EMC hit by cyberattack 20

Executive summary

In the second quarter of 2024, 35 incidents were publicly confirmed by victims. Half of the attacks reportedly resulted in the denial of operations or product shipments. The majority of victims are various types of manufacturing enterprises that produce goods for sectors such as electronics, automotive, agriculture, medical and construction. In addition to manufacturing, other types of industrial companies also fell victim, including utilities, transportation and logistics, pharmaceuticals, and food and beverage.

The most severe damage occurred as a result of a ransomware attack on CDK Global, the software-as-a-service provider for US auto dealers, which disrupted operations at nearly 15,000 dealerships, resulting in a combined direct loss of $1 billion.

This is neither the first, nor the last case of its kind. Certainly, the cybersecurity of niche market product vendors and service providers, on which many businesses nevertheless depend, is something that is seriously neglected at the moment.

Another alarming case worth highlighting is the attack on UK-based medical device manufacturer LivaNova. In the course of the attack, intruders not only stole the personal medical data of the company's customers but also their medical device serial numbers. As our multiple vulnerability researches show,

some IoT device manufacturers are still engaging in the unfortunate practice of using device serial numbers to generate encryption keys and authentication data, thereby facilitating the development of attacks on their products.

Unfortunately, we see that even the world's leading vendors can have disappointing security flaws either in their products or in their public-facing infrastructure, putting their customers' and partners' data at risk, as in the case of the Dell data breach. Of course, there is no such thing as free cybersecurity, and additional investment in vendor security would definitely represent an additional cost to the customer. Hopefully, organizations around the world will soon start to recognize the lack of cybersecurity maturity of their core technology providers as a major risk that needs to be addressed.

Quick stats for the quarter

- The number of incidents publicly confirmed by victims **increased by 16%** compared to the first quarter of 2024 (30 incidents).
- Almost half of all victims reported **denial of IT systems** (49%) and **denial of operations** (46%) as a result of an incident. In the previous quarter, these figures were 43% and 30%, respectively.
- More than half (51%) of all victims reported being **affected by a ransomware attack**. This compares to 47% in the previous quarter.
- Two-thirds of all victims (66%) are in the manufacturing sector. 57% of them reported **data leakage** and **personal data leakage** as a result of an incident.
- One company **was unable to recover from the impact of a cyberattack** and decided to cease operations.
- **The most affected countries are:**
  - USA – 26% (9 incidents)
  - Germany – 14% (5)
  - Australia – 9% (3)
- Among the other most affected countries are **Columbia, Argentina** and **Israel**.

April

- LivaNova
- Nexperia
- HOYA
- Swisspro
- Targus
- Taiwan United Renewable Energy
- Le Slip Français
- Octapharma Plasma
- Schuette
- Skanlog
- Tipton Municipal Utilities
- BECOM
- Max Wild
- Dell
- Barnett's Couriers

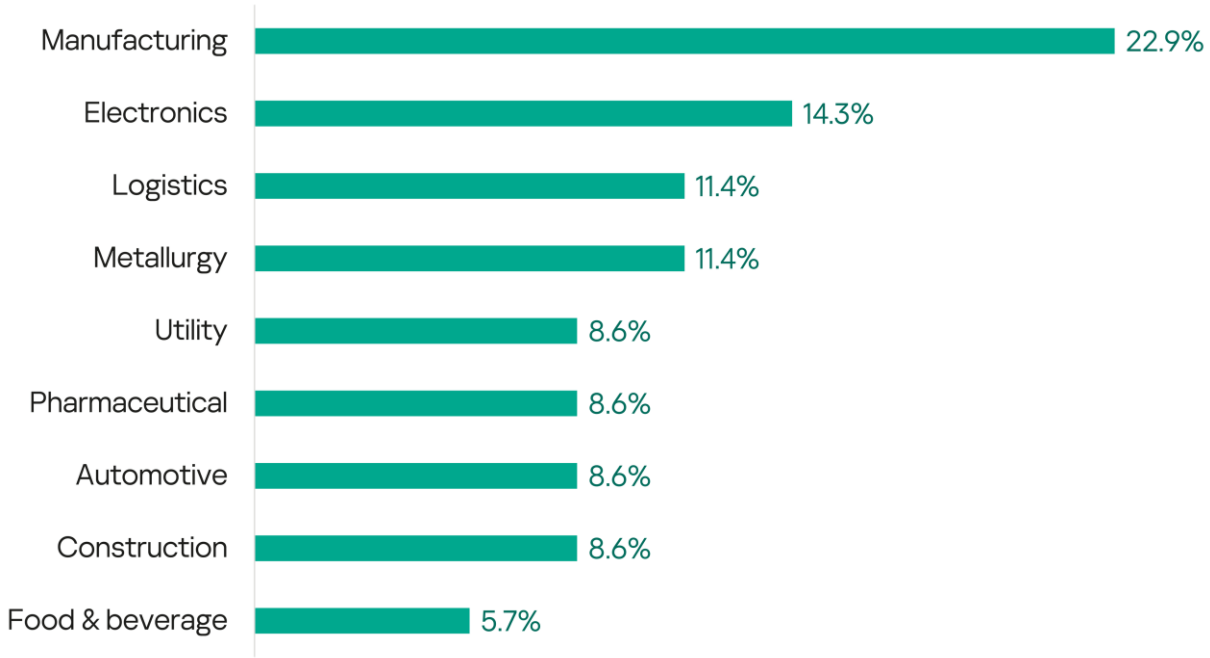
May

- Eucatex
- Key Tronic Corporation
- Porto de São Francisco do Sul
- Sawnee EMC
- Lewis Brothers Bakeries
- Lemken
- Wehrle-Werk

June

- Agropur
- Northern Minerals
- Pharmascience
- Iluka Resources
- Westfälische Stahlgesellschaf
- Emcali
- Crown Equipment
- GlobalWafers
- Rekah
- CDK Global
- Sandhar Technologies
- Ocasa
- Meiller Kipper

2024



Manufacturing

HOYA hit by cyberattack

Manufacturing
Data leakage, denial of IT systems, denial of product shipment, denial of operations
Ransomware

Japanese lens maker Hoya learned on March 30 that its corporate headquarters and several of its business divisions had experienced an IT system incident, according to a company statement. The company confirmed a disruption despite its efforts to isolate the affected servers. The company investigated whether any of its confidential or personal data had been compromised and cooperated with authorities to resume production as soon as possible. Hoya's consumer eyeglass lens division, Hoya Vision Care, said on its website that there were delays in delivering orders. As part of the ongoing investigation, the company confirmed that an unauthorized third party gained access to certain servers and exfiltrated a limited number of files. A Hoya spokesperson declined to say whether any of the company's other optical products, including components for chipmaking equipment and hard drives, were affected by the disruption.

On April 10, the Hunters International ransomware gang demanded a $10 million ransom for a file decryptor and for not releasing files stolen during the attack. Later, Hoya released the update, confirming there had been disruptions to operations and product delivery, and that some data had been exfiltrated from its systems. By the time of the update (April 24), most of the affected labs had already opened.

Targus hit by ransomware

Manufacturing
Denial of operations
Ransomware

Targus, a US-based manufacturer of mobile computing accessories, revealed in a regulatory filing that it was the victim of a cyberattack that disrupted its operations after a malicious actor accessed its file servers. The incident, detected on April 5, 2024, was contained with the help of cybersecurity consultants, and resulted in a temporary interruption of Targus' business operations. Although the company notified regulators and law enforcement, it did not confirm whether any corporate data was stolen in the attack. The Red Ransomware group claimed responsibility for the attack on April 19 and released a sample of the data stolen in the breach.

Swisspro hit by ransomware

Manufacturing
Data leakage, denial of IT systems
Ransomware

Swiss electrical installation, ICT and automation company Swisspro, part of BKW Building Solutions (Swiss building technology group), was hit by a ransomware attack affecting its legacy IT environment, as confirmed to local media. A task force was set up to assess the impact and possible consequences of the attack, while taking immediate measures such as isolating affected systems and changing passwords. There was no indications of outbound attacks affecting customers or other companies within BKW, and Swisspro was able to continue providing its services. The extent of the data leak was part of the ongoing analysis.

The Black Basta ransomware gang claimed responsibility and published 700GB of information allegedly stolen from Swisspro.

Le Slip Français hit by cyberattack

Manufacturing
Personal data leakage

French underwear and loungewear manufacturer and retailer Le Slip Français announced on its website that it had been the subject of a cyberattack on April 15 that compromised the personal data of its customers. A complaint was filed for fraudulent access to an automated data processing system and a report was made to the French Data Protection Authority CNIL and other judicial authorities. The company said that the incident concerns names, first names, telephone numbers, postal addresses, emails and sometimes order numbers. The company informed RTL of a partial list of customer account data stolen and disclosed on the dark web. The alleged perpetrator, who goes by the name ShopifyGUY, claimed responsibility for the data leak.

Lemken hit by cyberattack

Manufacturing
Denial of IT systems, services and operations

German agricultural machinery manufacturer Lemken was hit by cyberattack on May 11. The attack infiltrated the company's networks on a global scale, resulting in disruptions to production and remote working of employees. Among other things, the attack affected the processing of spare parts orders. Upon discovering the breach, the company immediately shut down all IT systems worldwide and assembled an investigation team with external experts in cooperation with the State Criminal Police Office. According to initial detailed analysis, customer data was not affected, as the company's security systems were very effective. According to the company's CEO at the time, some systems were down, while some were expected to be back online within days. The company resumed machine production at its Alpena factory in June. The email system is managed externally and has never been affected by any attacks.

Crown Equipment hit by cyberattack

Manufacturing
Personal data leakage, denial of services and operations

US-based forklift manufacturer Crown Equipment acknowledged that it suffered a cyberattack that disrupted its manufacturing operations. For a period of time from June 10, production at the manufacturer's sites in Roding, Germany, and in New Bremen, USA, was at a standstill. The manufacturer couldn't be reached by phone and the company's website was down. According to the letter received by the employees (and published by Bleeping Computer) on June 18, the investigation discovered that hackers of an international cybercriminal organization managed to break into their system because an employee allowed unauthorized access to their device. Employees were warned not to accept MFA approval requests and to be vigilant about phishing attempts.

In a later update, Crown Equipment confirmed that an unauthorized third party gained access to certain Crown records, such as accident and injury reports, and employee participation in the company's benefit and retirement programs. These records contained sensitive personal information about the company's employees and, in limited cases, their family members.

LivaNova hit by cyberattack

Manufacturing, medical
Personal data leakage, denial of IT systems

UK-based medical device manufacturer LivaNova notified nearly 130,000 individuals that their personally identifiable information was compromised in a cyberattack in late October 2023. According to the notification letter to affected individuals, LivaNova became aware of the incident in mid-November 2023, and a subsequent investigation determined that the intruders stole names, addresses, social security numbers, medical information such as diagnosis, condition, treatment information, prescription, physician, medical record number and device serial number, and health insurance information, among other data. The incident resulted in disruption to portions of LivaNova's IT systems. Immediately after detecting the issue, the company began an investigation with the assistance of external cybersecurity experts, coordinated with law enforcement, and took certain systems offline. LivaNova disclosed the incident in late April, shortly after the extent of the breach was determined.

Taiwan United Renewable Energy hit by cyberattack

Manufacturing, renewable energy
Denial of IT systems and operations

Taiwan United Renewable Energy Co., Ltd., a of manufacturer of renewable energy products, announced on April 11 that due to a cyberattack on some information systems, its factory was in a state of shutdown and the impact on the company's finances was being assessed. The company's information department initiated all relevant defense mechanisms and restoration operations, while working with technical experts from external financial security companies. At the time of the announcement, all domains and related files were thoroughly scanned and tested. Once information security was ensured at a high level, the daily backup data could be restored and put into operation.

Electronics

Dell data breach

Manufacturing
Personal data leakage

US computer manufacturer and retailer Dell notified customers on May 8 that it had experienced a data breach involving customer data. In the email, the company wrote that it was investigating an incident involving a Dell portal that contains a database with limited types of customer information related to purchases from Dell, such as: customer names, physical addresses, Dell hardware and order information, including service tag, item description, order date and related warranty information. Dell did not say whether the incident was caused by malicious outsiders or an inadvertent error. On April 29, the website Daily Dark Web reported that a threat actor was advertising customer and other information for systems purchased from Dell between 2017 and 2024 on a hacking forum. The person claimed that the dataset had information on 49 million people and included details such as full name, full address, system service tag, customer number, and more.

A threat actor calling himself Menelik told TechCrunch that to hack Dell's portal he applied to register two fake companies as Dell "partners" (product resellers). After the application was approved, he logged in to the portal and brute-forced customer service tags that appeared to be seven characters long and consisted of only numbers and consonants. While interacting with the customer portal, he made 5,000 requests per minute for nearly three weeks without Dell noticing.

BECOM hit by cyberattack

Manufacturing, electronics, engineering
Denial of services and operations

Austrian electronics engineering, manufacturing and service company BECOM was hit by a cyberattack on April 23. Company management announced that they had intervened in time and disconnected the network, thereby preventing encryption. The top priority was to restart production areas. The company said it worked intensively to get production areas up and running at the sites and worked with external specialists to do this. These experts worked with BECOM's internal IT team to determine the extent of the compromise, remove any malicious elements from the company's systems, and ensure that there were no lingering threats that could be exploited in the future. The company informed its business partners that its usual methods of communication were limited.

Key Tronic Corporation hit by ransomware

Manufacturing, electronics
Data leakage, personal data leakage, denial of services and operations
Ransomware

US-based electronics manufacturing services company Key Tronic Corporation (also known as KeyTronic) disclosed a cybersecurity incident in an SEC 8-K filing on May 6. The company activated its cyber-incident procedures to investigate and contain the attack, working with external cybersecurity experts and notifying authorities. The incident resulted in disruptions and access limitations to some business applications that support aspects of the company's operations and corporate functions, including financial and operational reporting systems. The company believed the unauthorized activity had been contained and was working to restore the affected systems. At the time of the initial announcement, the company didn't believe the incident would have a material impact on its operations or financial results. On June 14, the company amended the form to state that the attack also caused it to suspend domestic and Mexican operations for two weeks, but that other international operations continued without disruption while it responded to the attack. Normal operations were later resumed. The new filing also stated that the company's investigation confirmed the threat actors stole personal information during the attack. As required by SEC guidelines, the company also confirmed that the attack and loss of production would have a material impact on the company's financial condition during the fourth quarter ending June 29, 2024. The Black Basta ransomware group claimed responsibility for the attack in late May, leaking 530GB of stolen data, including financial and corporate data, technical documents, and consumer and employee PII.

In the later filing, the company estimated the total losses caused by the incident at $17 million ("...the company incurred approximately $2.3 million in additional expenses and believes it lost approximately $15 million in revenue during the fourth quarter...").

Nexperia hit by ransomware

Manufacturing, electronics
Data leakage
Ransomware

Chinese-owned Dutch semiconductor manufacturer Nexperia acknowledged that its IT systems were breached in March 2024. Nexperia disconnected the affected equipment to contain the breach, launched an investigation with the assistance of third-party experts to determine the nature and scope of the incident, and took strong measures to stop the unauthorized access. The incident was reported to the relevant authorities. Nexperia's disclosure followed the release of data by the Dunghill Leak ransomware group on a darknet site on April 10. The hackers claimed to have hundreds of gigabytes of sensitive material, including trade secrets, chip designs and many hundreds of folders with customer data from SpaceX, Apple and Huawei, among others. The list of stolen files on the darknet site includes a number of confidential documents as proof of the hack, including an employee's passport photo, as well as legal and technical documents.

GlobalWafers hit by ransomware

Manufacturing, electronics
Denial of IT systems, services and operations
Ransomware

GlobalWafers, a Taiwanese manufacturer of silicon wafers for semiconductors, reported a cyberattack that impacted some production lines on June 13. The company used existing inventory to fulfill orders, but said delivery delays could occur into the third quarter. Investigations and recovery efforts were initiated, and measures were taken to strengthen cybersecurity. A thorough investigation confirmed that no critical information was accessed. GlobalWafers partially shut down its operating systems during the initial phase of the attack, which impacted production and shipments at certain plants. GlobalWafers stated that it will continue to improve the security management of its network and information infrastructure in the future to ensure data security. Shipments were partially restored and largely returned to normal on June 18. The company was listed as a victim by the Black Basta ransomware group.

Automotive

Sandhar Technologies hit by cyberattack

Manufacturing, automotive
Denial of IT systems

Sandhar Technologies, an Indian automotive component manufacturer, announced on June 19 that it had detected a cyber-incident affecting some of its systems. The company responded immediately by mobilizing its technical and cybersecurity teams to address the threat. It assured that no confidential data had been compromised and that the incident did not have a material impact on its operations. On June 21, the company issued an update stating that it had

successfully resolved the issue. All financial, human resources and confidential data was backed up and secured by the company's cloud partner. The affected systems were successfully formatted and restored. There was no breach of confidential data or information as a result of this incident, and the cloud providers were not affected by this incident.

Meiller Kipper hit by cyberattack

Manufacturing, automotive
Denial of IT services

German vehicle manufacturer Meiller Kipper was hit by a cyberattack that resulted in limited availability of employees and some services. Authorities alerted the company to specific indicators of the attack, prompting Meiller Kipper to engage security and forensic experts to assess the situation. As a precautionary measure to protect its business partners, Meiller Kipper opted to deactivate all established internet-based communication channels, including fixed-line telephony, until the investigation yields concrete results. On its website, the company asked its suppliers to resend outstanding invoices by July 10 as a result of technical limitations.

CDK Global hit by ransomware

Automotive
Denial of IT systems and operations
Ransomware

US automotive software-as-a-service (SaaS) provider CDK Global suffered a cybersecurity incident that disrupted operations at North American car dealerships and automotive equipment manufacturers. CDK was first attacked on June 18, shut down its systems as a precaution and restored some services on June 19, but was attacked again later that evening and shut down its systems again. The company launched an investigation with third-party experts and notified customers and law enforcement about the incident. CDK Global set up interactive voice-response lines for customers to obtain information about the attack. According to an unnamed Bloomberg source, CDK Global suffered a ransomware attack and negotiated the ransom payment with the BlackSuit cybercrime group. CDK warned customers about phishing attempts by crooks posing as CDK employees in order to obtain system access. CBS News reported that the company sent a memo to customers on June 22 saying the restoration process would take several days and referred to the incident as a "cyber ransom event" for the first time.

The attack halted operations at approximately 15,000 dealerships in the United States and Canada, as the company provides essential software that helps auto dealers manage day-to-day operations, including vehicle sales, financing, insurance, and repairs. The attack caused significant disruptions to the operations of nearly every car dealership that relies on the company's services.

The Anderson Economic Group estimates that the total direct losses to franchised dealers as a result of this cyberattack may have reached 56,200 new vehicle sales, lost earnings on parts and service, additional labor and IT costs, and additional floor plan interest costs on inventory over three calendar weeks that equate to $1.02 billion.

Food and beverage

Lewis Brothers Bakeries hit by ransomware

Manufacturing, food and beverage
Data leakage, personal data leakage, denial of IT systems
Ransomware

US food manufacturer Lewis Brothers Bakeries Inc. (LBBI) stated in a May 9 data breach notification letter that it discovered attackers encrypted certain files on its servers on April 1. LBBI immediately launched an investigation into the nature and scope of this activity with the assistance of third-party forensic specialists. The investigation determined that unauthorized access to LBBI's network occurred between March 25 and April 1, during which time certain files were copied and removed from the network. LBBI conducted a comprehensive review of all data that may have been accessed to determine the type of information impacted and to whom the information related. According to a complaint filed on May 17 in the US District Court for the Southern District of Indiana, the information exposed in the breach included names, social security numbers, and possibly other types of data. LBBI notified federal law enforcement authorities of the incident. LBBI also worked to implement additional safeguards and training for its employees. The Medusa ransomware group claimed responsibility for the attack on April 30.

Agropur hit by cyberattack

Manufacturing, food and beverage
Data leakage

Canadian dairy producer Agropur was the victim of a cyberattack that affected part of its online directory. The company said its operations were not disrupted and that measures were taken to mitigate the impact of the incident and strengthen data protection. Agropur said the breach didn't extend to its transactional systems. The company noted in the notification letter that there was no evidence that the exposed data had been misused, but warned customers out of an abundance of caution and to raise awareness of the potential risks until the investigation concludes and more details are available. The company launched an investigation to determine the scope and impact to customers, and was working with external cybersecurity experts and law enforcement.

Construction

Eucatex hit by cyberattack

Manufacturing, construction
Denial of IT services
Ransomware

Brazilian building materials and home furnishings manufacturer Eucatex reported on May 2 that it suffered a cyberattack that resulted in the shutdown of its ERP and electronic mail systems. According to the company, its databases remained intact and there was no evidence of any loss or leakage of information. The problem was subsequently resolved, and the systems were restored. Eucatex stressed that it will keep the financial market and the relevant authorities informed should any new relevant information emerge.

The RansomHub ransomware group added Eucatex to its list of victims. They claimed to have stolen 150GB of sensitive information, including information on customers, contractors, financial documents, NDA agreements, and application source codes.

Wehrle-Werk hit by cyberattack

Construction, engineering
Denial of service and operations

German mechanical engineering and construction company Wehrle-Werk was the victim of a cyberattack. According to SentiGuard, the attack took place on May 11. Since then, the company's production and communications have been severely restricted. On May 22, the company announced that it was working intensively to restore the affected systems and resume full operations. The company's internal information technology department was being supported by an IT service provider.

Max Wild hit by ransomware

Construction, logistics
Data leakage, denial of IT systems, denial of IT services
Ransomware

German logistics and construction company Max Wild GmbH was the victim of a cyberattack that was discovered on April 25 and immediately stopped. According to an announcement on its website, cybercriminals apparently managed to break through IT security barriers and existing protection systems and penetrate the IT systems during the attack. As a result, many of the company's IT systems were switched off, and there were restrictions on accessibility, digital communication and scheduling, especially email communication. The company asked that all urgent questions be directed by phone. The company worked with external and internal specialists to secure traces of the cyberattack and examine the effects on IT systems in detail. The ransomware group Metaencryptor claimed responsibility for the attack. It claimed to have stolen 85GB of data.

Pharmaceutical

Octapharma Plasma hit by ransomware

Manufacturing, pharmaceutical
Data leakage, personal data leakage, denial of IT systems, denial of operations
Ransomware

Swiss medical and pharmaceutical company Octapharma discovered unauthorized network activity on April 17 that resulted in the temporary closure of more than 150 plasma donation centers in the United States. According to statements on its website, plasma donation centers in Germany were not affected and continued to operate as normal, and European production sites continued normal production operations. The company activated its incident response procedures to investigate the attack and also took systems offline to limit the potential scope of the incident. The BlackSuit ransomware gang took credit for the attack, claiming to have exfiltrated business, laboratory and personal data. A source told the Register that the ransomware gang gained access to the company through VMware systems, and that the downtime in the United States could affect the supply of plasma to Octapharma's European operations.

The breach investigation, supported by third-party cybersecurity experts and the FBI, concluded on August 2, 2024. Octapharma disclosed that data from its file sharing systems had been compromised, potentially impacting the personal information of customers. The exposed data included sensitive information such as: full names, social security numbers, driver's license numbers, financial account numbers, health insurance information. Approximately 1,423 individuals have been identified as potentially affected. They were notified and offered a complimentary 24-month credit monitoring service. The service guards against identity theft and credit card fraud, and also tracks changes in borrower behavior to alert consumers of potential fraud.

Rekah hit by cyberattack

Manufacturing, pharmaceutical
Denial of IT services, denial of product delivery

Rekah, a major Israeli pharmaceutical company producing medicines, cosmetics, vitamins and nutritional supplements, was hit by a cyberattack and shut down its distribution system, it was confirmed to Calcalistech. The company worked to contain the incident, locate and counter the attack, and restore the compromised systems. According to an announcement to the stock exchange published by Rekah on June 17, the company identified a potential cybersecurity incident involving an intrusion by an unauthorized party into the computer systems of its subsidiary Ophir & Shalpharm Medicines and Cosmetics, which operates the central distribution and sales system for the company. According to Rekah's chief executive, the company prepared to restore the distribution system as quickly as possible, while testing manual

alternatives to operate the computerized system in case the investigation into the attack was prolonged. A special team was set up that included external specialists. The CEO estimated that a short shutdown of the distribution system would not cause a shortage of the company's drugs. Rakah's production system was not damaged and continued to function normally.

Pharmascience hit by cyberattack

Manufacturing, pharmaceutical
Denial of operations

Canadian pharmaceuticals manufacturer Pharmascience was the target of a cyberattack, according to local media. The company confirmed that it had discovered an intrusion into its computer system on June 1, but refused to provide details on the scope and duration of the attack. The company declined to confirm whether a ransom was demanded or paid, or whether any data was stolen. The company said it responded quickly by bringing in cybersecurity experts, who helped secure its computer systems. Pharmascience has since resumed operations safely and effectively, according to the company.

Mining and Metallurgy

Westfälische Stahlgesellschaf hit by ransomware

Manufacturing, metallurgy
Data leakage, personal data leakage, denial of IT systems
Ransomware

German steel company Westfälische Stahlgesellschaf was the victim of a ransomware attack, according to a news item on its website. On June 9, the attackers downloaded certain data from the systems and encrypted the systems. Production was not disrupted by the incident, and the company was confident that it could meet all delivery deadlines. The incident involved personal data of the company's employees. Westfälische Stahlgesellschaf immediately shut down any internet access to its IT systems, restored systems and data from backups and notified the relevant data protection authorities. The Lockbit 3.0 ransomware group claimed responsibility for the attack.

Schuette hit by ransomware

Manufacturing, metallurgy
Data leakage, personal data leakage
Ransomware

US-based metal manufacturer Schuette Inc. announced that it had fallen victim to a ransomware attack. According to a filing, on or around April 18, Schuette became aware of certain unauthorized activity within its computer systems. Upon discovery, the company immediately secured its network and quickly engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. On May 14, following a thorough investigation, Schuette determined that a limited amount of personal information

may have been accessed by an unauthorized third party in connection with this incident. The company added there was no evidence that any information was misused. It added that the information accessed by the threat actor may have included first and last names, in combination with social security numbers. On May 28, 2024, Schuette began notifying individuals whose information may have been affected.

Upon learning of the incident, approximately one month after the breach, the company took steps to secure its systems and enhance the security of its network to prevent similar incidents from occurring in the future. The Cactus ransomware group added Schuette Metals to its list of victims on May 20.

Northern Minerals hit by ransomware

Mining
Data leakage, personal data leakage
Ransomware

Australian rare earths mining company Northern Minerals announced on June 4 that some of the company's data was compromised and released on the dark web following a cyberattack in late March 2024. The breach did not have a material impact on its operations or broader systems, according to the company's statement. The company has reviewed its processes, implemented measures to strengthen its systems, notified the appropriate authorities and engaged legal, technical and cybersecurity specialists. The announcement came shortly after the BianLian ransomware group published several archives on its Tor-based leak site that allegedly contained operational, human resources, management, project and email data stolen from Northern Minerals. "The exfiltrated data included corporate, operational and financial information and some details relating to current and former personnel and some shareholder information," Northern Minerals said in a company filing.

The Department of Foreign Affairs and Trade published a notification confirming the personal data of some of Northern Minerals' current and former employers, and said the compromised Australian passports were still safe to use for international travel.

Iluka Resources hit by cyberattack

Mining
Denial of service

Australian mining and rare earths company Iluka Resources announced that threat actors attempted to disrupt its external website through a denial-of-service (DoS) attack, but did not gain access to the company's systems or exfiltrate any data. Following queries from the local media, the company's spokesman confirmed that the company had experienced a cyber-incident and reported it to the authorities.

Logistics and transportation

Barnett's Couriers hit by cyberattack

Logistics
Denial of services and operations

Australian logistics company Barnett's Couriers was hit by a cyberattack sometime in 2024, which led to the company's closure according to a recorded message on an emergency mobile number. The message said that the company's business could not operate productively as a result. The company worked tirelessly with leading IT consultants to restore its systems and unfortunately was unable to overcome the challenges and made the difficult decision to cease operations of Barnett's Couriers. The automated email response, similar to the voicemail, added that the company had a small team that would finalize all outstanding accounts. NSW Police initially said the company had not reported the cyberattack, which the company blamed for its sudden closure. Employees and owner-drivers were given a few hours' notice that they would no longer be employed by the company from May 1. In June a NSW Police spokesperson confirmed that police had started investigations into a cyberattack on Barnett's Couriers.

Skanlog hit by ransomware

Logistics
Denial of IT systems and operations
Ransomware

Danish logistics company Skanlog was hit by a ransomware attack, the company's manager told a Swedish newspaper. The attack resulted in the company's entire system being down until it could be repaired and put back into operation. The attack could have potentially affected the supply of goods to a local chain of stores, for which Skanlog is the main supplier.

Porto de São Francisco do Sul hit by ransomware

Transportation, logistics, port
Data leakage, denial of IT systems and operations
Ransomware

The port of São Francisco do Sul in Brazil released an official notice informing that it suffered a cyberattack on its server on May 6, which resulted in the encryption of some data. To prevent the attack from spreading, the systems were temporarily deactivated, and the port's IT team, with the support of service providers, managed to partially resume functionality on May 7. The partial recovery of the system made it possible to fully resume port operations in less than 24 hours. The port reported that it investigated the extent of the data affected. Access control and security systems, such as automatic license plate readers, biometrics and CCTV, were gradually being restored. The attack was reported to the Federal Revenue, which authorized the resumption of operations, the National Waterway Transport Agency (Antaq) and the National Data Protection Authority.

The RansomHub ransomware group claimed responsibility for the attack on Porto de São Francisco do Sul, claiming to have stolen 548.72GB of data, including accounting, human resources, financial reports and employee details.

Ocasa hit by ransomware

Logistics
Denial of IT systems and operations
Ransomware

Argentine logistics company Ocasa experienced a ransomware attack that took down its website and disrupted operations, according to local media. The company took measures to contain the breach, restore services and secure its systems while investigating the extent of the damage. At the time of the official confirmation, the company's website was still down and, according to the company's statement, no data was leaked. The attack impacted other companies in the group that manages Ocasa such as Direxa, a company that offers custom and exclusive solutions in comprehensive logistics services, import, export and goods transit. The Akira ransomware group added Ocasa to their dark web portal on June 26.

Utility

Tipton Municipal Utilities hit by cyberattack

Water supply, energy, utility
Denial of operations

US-based Tipton Municipal Utilities (TMU), which provides electricity, water and wastewater treatment for Tipton, suffered a cyberattack. On April 20, the People's Cyber Army of Russia posted a video on Telegram claiming credit for a cyberattack on a TMU wastewater treatment plant. The video posted by the hackers purported to show them manipulating software that controls equipment that aerates and move fluids at the Tipton wastewater treatment plant. TMU's general manager told CNN that they were targeted and "have not been compromised". According to comments, TMU experienced minimal disruption and remained operational at all times. Federal authorities investigated the incident. According to comments made to StateScoop by TMU's general manager, the cyberattack on Tipton began disrupting operations on the evening of April 19. Plant managers sent employees to correct the activity, which again disrupted operations on the morning of April 21. He described the disruption to the plant's operations as minor and said the town's drinking water was never at risk. TMU maintained the plant's operational capability throughout the incident, and was able to continue to accept and release wastewater flows despite the disruptions.

Emcali hit by ransomware

Water supply, energy, utility
Denial of IT systems
Ransomware

Colombian utility Emcali experienced a major cyberattack aimed at disrupting its business and billing systems. The attack, which began on June 9, was contained in less than two hours due to the rapid response of the company's security team. The attack first affected Emcali's website. An Emcali manager told local media that the attack appeared to target the information systems associated with the commercial function. The company isolated its systems and had to reconnect and turn on those systems. Investigations were initiated to determine the motives and perpetrators of the attack, which the official said appeared to be aimed at extortion or sabotage.

Sawnee EMC hit by cyberattack

Energy, utility
Denial of IT services

US energy supply company Sawnee Electric Membership Corporation informed customers in an email on May 6 that it had discovered a cybersecurity incident affecting their website. They advised all customers to avoid the official "sawnee[.]com" website for any purpose, and to use the new site "www.sawnee[.]coop" instead. Sawnee EMC told customers not to attempt to log in to the old site or click on any links there. The company said a full investigation into the cybersecurity incident was ongoing.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com