Kaspersky ICS CERT

kaspersky

Q3 2024 – a brief overview of the main incidents in industrial cybersecurity

19.02.2025

Version 1.0

Executive summary

The diversity of industries affected by cyberattacks this quarter is extremely wide. Industrial enterprises manufacturing textiles, electronics, composite and construction materials, machinery, automotive and other types of goods were hit by cyber-incidents, most often caused by the activities of ransomware gangs. Many large companies, including some well-known brands, were on the list. Although the estimated damages from the incidents confirmed by victim organizations in the quarter were not extremely high (the highest was $21.4 million reported by the US chipmaker Microchip Technology), for Schumag AG, a German manufacturer of precision steel parts, a cyber-incident may have been the last straw that led to the company's bankruptcy. Other sectors such as food and beverage, construction, engineering, mining and logistics were not exempt. An unusually high number of victims were in critical sectors such as utilities and power and energy. Fortunately, none of the attacks resulted in the denial of core operations such as water or electricity supply, but the provision of digital services suffered for many of the victims.

Quick stats for the quarter

- Total of 58 incidents publicly confirmed by victims.
- Most victims (71%) reported being **affected by a ransomware attack**.
- Two-thirds of all victims (66%) are in the manufacturing sector; 68% of them (64% of all victims) reported **personal data leakage** as a result of an incident.
- 31% of all victims reported a **denial of operations** and 29% reported a **denial of IT systems** as a result of an incident.

- **Countries with the highest number of confirmed incidents:**
  - USA – 60% (35 incidents)
  - Germany – 7% (4)
  - Japan – 5% (3)
- This quarter we saw incidents in some countries from which we rarely see public confirmation of incidents: **British Virgin Islands, South Africa, Singapore.**

July

- AKG
- Metalfrio
- Bassett Furniture
- Cadre Holdings Inc.
- K-FLEX USA
- TotalEnergies Clientes SAU
- BMW Hong Kong
- Hiap Seng Industries Ltd.
- Basement Systems
- Kulicke and Soffa Industries, Inc.
- Peco Foods
- Industrias Peñoles

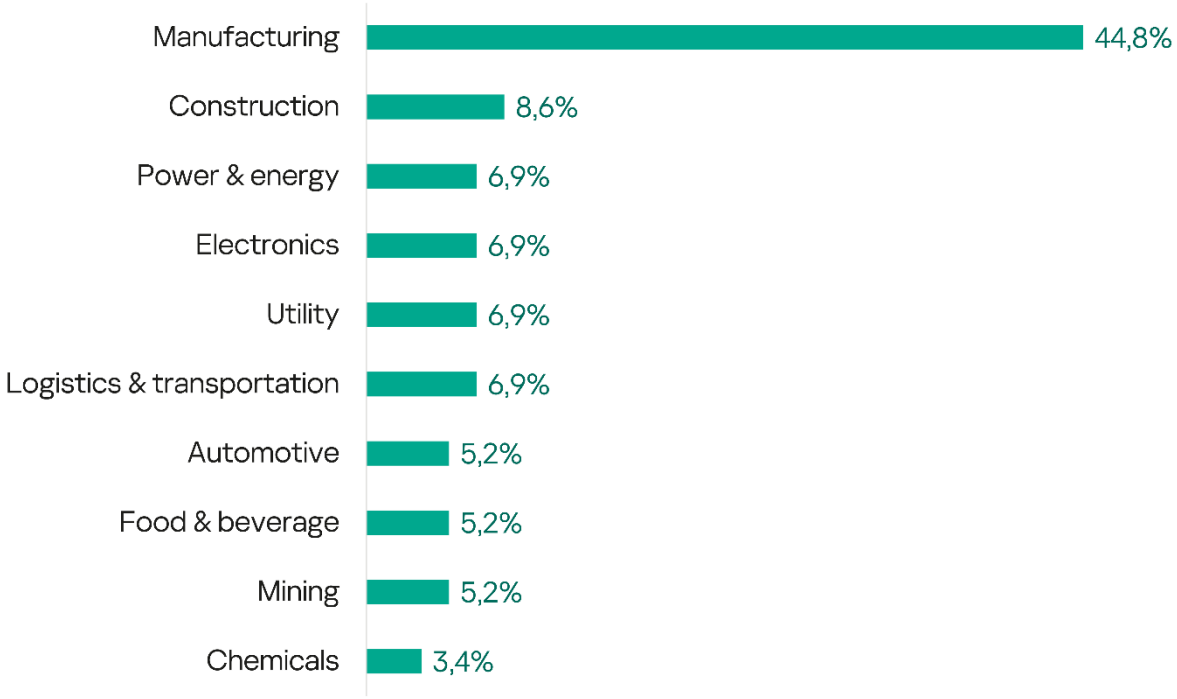
August

- Schlatter Industries
- Arntz Optibelt
- Direct Signalétique
- Nilörngruppen
- Lavelle Industries
- Noritsu America Corporation
- Congoleum Acquisition
- Hanwha Qcells
- Clark Material Handling Company
- M&R Printing Equipment
- Anderson Feazel
- Toyota Motor North America
- CRB Engineering
- Siegfried's Basement
- S&F Concrete Contractors Corp.
- Microchip Technology Incorporated
- Kernex Microsystems
- British Virgin Islands Electricity Corporation
- Blue Ridge Rural Water Company Inc.
- JAS Worldwide
- Port of Seattle
- Banham Poultry
- Innophos Holdings Inc.
- Evolution Mining

September

- Zacros
- Smeg
- Kawasaki Motors Europe
- Schumag AG
- Oldenburg Group
- Noble Biomaterials
- Granit Design
- V H Blackinton & Company
- The Gill Corporation
- Elyria Foundry
- New England Wooden Ware
- Halliburton
- Netherland Sewell & Associates, Inc.
- Hanon Systems USA
- MEMC LLC
- Air-e
- Arkansas City Water Treatment Facility
- Kantsu
- Brown Integrated Logistics Inc.
- McIlhenny Company
- Ortec
- Sibanye Stillwater

2024



Manufacturing

AKG hit by cyberattack

Manufacturing

Denial of IT systems and operations, personal data leakage

AKG, a German manufacturer of coolers and heat exchangers with more than 10 business units worldwide, suffered a cyberattack that disrupted production and communications at several of its sites around the world. Although IT systems were temporarily stopped to contain the spread of malware, production was resumed and critical data was not affected, according to an interview with the German press. An investigation was launched with the involvement of the Hessian State Office of Criminal Investigation and data protection authorities. AKG also called in an IT forensic expert.

AKG North America, Inc. later notified the attorney general of the Commonwealth of Massachusetts that it had experienced a data breach in which sensitive personal identifiable information in its systems may have been accessed. In the breach notice, AKG North America, Inc. stated that the information affected varies depending on the individual; the type of information potentially exposed includes name and Social Security number.

On August 15, 2024, AKG North America, Inc. began mailing data breach notification letters to impacted individuals. Based on the breach notice sent to Massachusetts residents, AKG is providing those individuals with a list of the specific type of sensitive information affected and 24 months of free credit monitoring services.

Metalfrio hit by cyberattack

Manufacturing

Denial of IT systems and operations

Ransomware

Metalfrio, a Brazilian manufacturer of commercial refrigerators, announced on July 15 that it had fallen victim to a cyberattack that rendered parts of its systems unavailable in Brazil and Mexico. The company quickly activated its security protocols to minimize the impact and isolated its systems to prevent further damage. The company also reported that it was receiving assistance from a specialized external consulting firm. Metalfrio said it had not identified any leakage of customer or supplier data or personal data processed by the company. The company took all necessary measures to restore normal operations in the days following the incident. On July 16, the RansomHub group claimed responsibility for the attack on its leak site.

Bassett Furniture hit by cyberattack

Manufacturing

Denial of IT systems, services and operations

US furniture manufacturer and retailer Bassett Furniture detected unauthorized activity on a portion of its information technology systems on July 10 according to an 8-K filing with the Securities and Exchange Commission. The threat actor disrupted the company's operations by encrypting some data files. Upon detecting the unauthorized activity, the company immediately began taking steps to contain, assess and remediate the incident, including launching an investigation, activating its incident response plan, and shutting down some systems. The company's retail stores and e-commerce platform remained open, and customers were able to place orders and purchase available merchandise; however, the company's ability to fulfill orders was impacted. Bassett's CEO told an industry media outlet that the company's factories were at a standstill for four and a half days. Bassett Furniture acknowledged that the attack had a material impact on the company's business operations and would likely continue to do so until recovery efforts were complete.

Bassett's CEO later reported a loss in the third quarter of 2024, in part because its performance was impacted by the cyberattack. While the full effects of the incident were unclear, the company stated that it included $600,000 in

manufacturing wages paid during the one-week production shutdown caused by the attack.

Schlatter Industries hit by ransomware

Manufacturing

Denial of IT systems

Ransomware

Swiss manufacturer of resistance welding and weaving machines Schlatter Industries was the victim of a cyberattack on August 9. According to an official statement, the attack involved the deployment of malware, after which the hackers attempted to extort the company. The company immediately initiated the necessary security measures and involved the relevant authorities. Security experts worked to limit the damage and restore systems as quickly as possible. The company investigated whether any data had been stolen and experts worked to get all systems back up and running. Schlatter Industries told Reuters on August 20 that its computer network had been back up since August 19 following a cyberattack. The company's latest statement did not provide details on the impact of the cyberattack or whether any data was stolen.

Arntz Optibelt hit by cyberattack

Manufacturing

Denial of IT services

German belt drive manufacturer Arntz Optibelt was the victim of a cyberattack. The company detected a disruption on the morning of August 25 and took appropriate measures, including setting up a task force to investigate the incident. Arntz Optibelt worked closely with security authorities to determine the origin and extent of the attack. According to German media, emails sent to the company couldn't be delivered. A company spokeswoman said the cyberattack had resulted in restrictions, but with the support of specialists, the company was working hard to maintain the business capabilities of all its locations worldwide.

Direct Signalétique hit by cyberattack

Manufacturing

Denial of IT services

French sign maker Direct Signalétique was the victim of a cyberattack on August 16, according to local media, which cited the fact that "nothing worked anymore." On August 27, the company posted a message on LinkedIn explaining that its IT service provider had been subjected to a cyberattack, resulting in the disruption of the company's website and data processing software. The company could still be contacted by phone and email.

Nilörngruppen hit by ransomware

Manufacturing

Denial of IT systems, denial of services, operations and product delivery

Ransomware

Swedish clothing and fabric manufacturer Nilörngruppen discovered on August 6 that its IT systems had been compromised by a cyberattack. This resulted in operational disruptions and temporary interruptions to services. The company's systems were down as a result of the attack, and the company worked to restore functionality as quickly as possible. Nilörngruppen activated its IT security protocols and worked with cybersecurity experts to determine the extent of the breach and take the necessary steps to secure its systems. On August 13, Nilörngruppen issued an update announcing that the company had successfully resumed deliveries from all sites and was gradually restoring operations. The company first restored the most business-critical systems and was able to resume deliveries to customers. On August 9, the Play ransomware group added Nilörngruppen to its list of victims on a dark web site.

On October 25, the company stated in its Q3 2024 report that the cyberattack impacted the group's results by 4.4 MSEK (approximately $400,000).

Lavelle Industries hit by ransomware

Manufacturing

Personal data leakage

Ransomware

US rubber and plastics manufacturer Lavelle Industries issued a data breach notification in August following a cyberattack in March 2024. Lavelle said it became suspicious of unauthorized activity in its systems on March 17. In response, the company quickly took steps to secure its systems and launched an investigation to determine the nature and scope of the incident. The investigation determined that between March 10, 2024 and March 17, 2024, an unknown actor gained access to certain systems and may have accessed or taken certain information stored on those systems. The information in question included names, Social Security numbers, driver's license numbers, and financial account information. Lavelle issued an initial notification to potentially affected individuals on April 4. The company indicated that it would also be notifying state regulators, as required, as well as federal law enforcement. Lavelle said it is working to implement additional safeguards and training for its employees. The company added that it had no evidence of misuse or fraud related to the incident. The LockBit ransomware group claimed responsibility for the attack on Lavelle in March.

Zacros hit by ransomware

Manufacturing

Denial of IT services, denial of operations and product delivery

Ransomware

Japanese flexible packaging manufacturer Zacros suffered a ransomware cyberattack that encrypted some of its servers, according to a brief statement posted on its website on September 15. On September 27, the company released a statement with more details. Some of the company's production management system and core system servers were found to have been hit by ransomware on September 14, encrypting some of the information stored on them. Some products experienced production and shipping delays, resulting in delayed delivery dates. The company disconnected the affected systems from the network and suspended their use, and initiated a forensic investigation by an outside specialist firm to determine the extent of the damage and identify the information that was lost or leaked. Steps were also taken to prevent a recurrence, such as strengthening security in order to restart the system.

From the time of the statement, the company used a backup system and worked to fully resume operations such as production and shipping. Zacros reported the incident to the police and the Personal Information Protection Commission. The company planned to promptly notify those whose personal information may have been compromised by the attack as soon as it was detected.

The Argonauts hacking group claimed to have breached Zacros and exfiltrated 140 GB of data. The company received a ransom demand, but chose not to pay.

Smeg hit by cyberattack

Manufacturing

Denial of IT systems, denial of operations

Smeg, the Italian manufacturer of home appliances, was the victim of a cyberattack discovered on September 27. The attack halted production and led to the shutdown of IT systems, including production management, logistics, human resources and accounting processes. For security reasons, the system was locked down to prevent the loss of sensitive data. As a precautionary measure, activities were temporarily suspended until full system functionality was restored. According to local media, hundreds of the company's employees were unable to continue working and sent home. The Interlock hacking group claimed responsibility for the incident. They allegedly exfiltrated 820 GB of data.

Kawasaki Motors Europe hit by cyberattack

Manufacturing

Denial of operations

Ransomware

Kawasaki Motors Europe, the European division of the Japanese vehicle manufacturer, suffered a cyberattack that targeted the company's EU headquarters, resulting in operational downtime due to temporary server isolation to prevent further damage. As a precaution, it was decided to isolate each server and implement a cleanup process to review all data and identify and address any suspicious material. The company also responded by launching an investigation involving external cybersecurity experts. Normal business was resumed with dealers, business administration, and third-party suppliers such as logistics companies.

The RansomHub ransomware group listed the company on its dark web victim site on September 5, saying it had stolen 487 GB of data from Kawasaki Motors Europe. Later, on September 16, RansomHub posted data it said was stolen from KME. The breach affected business documents, financial data, banking records, dealership details and internal communications.

Schumag AG hit by cyberattack

Manufacturing

Denial of operations, bankruptcy

Ransomware

Schumag AG, a German producer of precision steel parts, announced on September 23 that it had fallen victim to a cyberattack. According to an official statement, Schumag AG decided to cancel its annual general meeting scheduled for September 25. Despite the attack, production was partially restored before the consequences and damage were assessed. The company planned to convene a new general meeting as soon as possible. The 8Base ransomware group added the company to its data leak site.

Later the company filed for bankruptcy (or "self-administration restructuring") with the Aachen District Court. In this special type of insolvency the board of directors retains control over the management, but is supervised by an (external) administrator. The company's operations continued and the wages of the company's 450 employees were secured through insolvency benefits. The CEO of Schumag AG stated: "We already had a clear turnaround plan, but we had to accept that the previous restructuring plans were no longer sufficient after the cyberattack. The additional burdens caused by the hacker attack have seriously disrupted our schedule."

Oldenburg Group hit by ransomware

Manufacturing

Personal data leakage

Ransomware

Oldenburg Group and its Visa Lighting division, a US-based supplier of heavy equipment and architectural lighting products, reported to the attorneys general of Maine and Vermont that it experienced a cyberattack between May 4 and May 5, in which an attacker believed to be associated with the Play ransomware group installed ransomware on the company's primary servers and may have accessed personal information stored on the servers. As a result, Oldenburg Group launched an investigation to determine the nature of the incident. Through its investigation, Oldenburg Group learned that sensitive personal information in its systems may have been compromised. The company began a review of the data to determine what information was impacted and to identify those affected. While the information involved varied depending on the individual, the type of information that may have been exposed includes: name, Social Security number, address, date of birth, email address, driver's license number, financial account information, as well as tax, medical, and health insurance information. The company hired third-party forensic and IT services, as well as outside consultants to assist in the investigation, and took steps to enhance its existing security protocols. In September, the Play ransomware group claimed responsibility for the attack on Oldenburg Group Inc./Visa Lighting.

Noble Biomaterials hit by cyberattack

Manufacturing

Personal data leakage

US biotechnology company Noble Biomaterials became aware of suspicious activity on its computer network, according to a breach notification document filed with the Maine attorney general in September. Noble Biomaterials launched an investigation and determined that its network had been infected with malware that prevented access to certain files on its systems. Through its investigation, Noble Biomaterials determined that between July 25 and August 3, an unauthorized actor may have had access to some systems that stored information related to certain current and former employees. Although Noble Biomaterials had no evidence of identity theft or fraud related to the incident, the company undertook efforts to notify individuals whose information was present in its systems. Information that may have been subject to unauthorized access included individuals' names and Social Security numbers. Upon discovery of the suspicious activity, Noble Biomaterials moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. In addition, Noble Biomaterials notified federal law enforcement authorities of the incident and cooperated with their

investigation. The company worked to implement additional safeguards and training for its employees.

Granit Design hit by ransomware

Manufacturing

Personal data leakage

Ransomware

Granit Design, a Canadian manufacturer of natural stone, quartz and ultra-compact surfaces, notified the attorneys general of Maine and Vermont in September that it had experienced a cybersecurity incident affecting the confidentiality of its employee data. Upon discovery, Granit Design immediately took steps to secure its network environment and launched an investigation with help from outside cybersecurity and forensic experts. The investigation subsequently determined that between July 20 and August 2, an unauthorized third party accessed the server and acquired a subset of its files. The company said that at the time of notification there was no indication that any identity theft had occurred as a result of the incident, but some personal information was on the affected systems. The following types of personal information were stored on the compromised systems: full name, date of birth, driver's license number, Social Security number, bank account number and routing number, and other personnel-related information, including medical questionnaires. The Play ransomware group claimed responsibility for the attack on Granit Design in August.

V.H. Blackinton & Company hit by cyberattack

Manufacturing

Personal data leakage

V.H. Blackinton & Company, Inc., a US manufacturer of public safety badges and uniform insignias, discovered unusual activity in its digital environment on August 30, according to a report submitted to the attorneys general of Maine and Vermont in September. Upon discovering the activity, the company immediately took steps to secure its network and launched an investigation, with the assistance of independent cybersecurity experts. As a result of the investigation, V.H. Blackinton & Company, Inc. learned that an unauthorized actor had acquired certain files and data stored in its systems. After completing a comprehensive review of all potentially affected information, V.H. Blackinton & Company, Inc. confirmed on September 4 that the personal information of certain individuals may have been affected by the incident. The data sets affected by the incident included individuals' names and Social Security numbers. Since that time, V.H. Blackinton & Company, Inc. has been working to gather contact information for individuals and preparing to notify all those

affected. V.H. Blackinton & Company, Inc. implemented additional security measures to prevent a similar incident from occurring in the future.

The Gill Corporation hit by ransomware

Manufacturing

Personal data leakage

Ransomware

US composite materials supplier The Gill Corporation (TGC) suffered a cyberattack in late June in which threat actors encrypted data, and the company filed a breach notification document with the attorneys general of Maine and Vermont in September. During the cyberattack an unauthorized third party compromised TGC's systems by encrypting many of the company's files and backup systems. Since the cyberattack, TGC investigated whether, among other things, the attack may have resulted in unauthorized access to and acquisition of personal information of former TGC employees. The investigation determined that the personal information involved in this incident may have included names and Social Security numbers, a limited number of driver's license numbers and/or bank account numbers and W-2 forms. The company identified the vulnerability exploited by the third party and has removed it from TGC's systems. TGC deployed additional protective measures to secure its systems and was examining additional steps the company could take to prevent such incidents in the future. The Hunters International ransomware group claimed responsibility for the attack on The Gill Corporation via its dark web leak site in July.

Noritsu America Corporation hit by ransomware

Manufacturing

Personal data leakage

Ransomware

Noritsu America Corporation, a US manufacturer of high-end professional digital imaging equipment and a subsidiary of the Japanese holding company Noritsu, was the victim of a cyberattack that exfiltrated personal information, according to a data breach notification submitted in August. Noritsu America Corporation discovered unusual activity in its network environment that originally began on April 29. On July 31, Noritsu learned that customers' personal information may have been affected by the incident. The company immediately took steps to contain the activity and engaged a cybersecurity firm to determine what happened and identify any information that may have been accessed or acquired without authorization. The potentially affected information may have included names along with Social Security numbers. The company implemented additional security features to reduce the risk of a similar incident occurring in the future, notified the Federal Bureau of Investigation, and said it planned to cooperate with any subsequent investigation. The Hunters International

ransomware group claimed responsibility for the attack on Noritsu America Corporation via its dark web leak site in May.

Congoleum Acquisition LLC hit by ransomware

Manufacturing

Personal data leakage

Ransomware

US flooring manufacturer Congoleum Acquisition LLC notified the attorney general of Maine that it had experienced a data breach in which attackers stole sensitive personal identifiable information. According to the breach notice, Congoleum Acquisition LLC discovered unauthorized activity within its digital environment on June 30. Upon discovering this activity, the company immediately took steps to secure the network and launched an investigation, with the assistance of independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, Congoleum Acquisition LLC learned that an unauthorized actor had acquired certain files and data stored on its systems. After completing a review of all potentially affected information, Congoleum Acquisition LLC confirmed on July 11 that the personal information of certain individuals may have been involved in the incident.

While the information stolen varied by individual, the type of information exposed includes names and Social Security numbers. The Play ransomware group claimed responsibility for the attack on Congoleum Acquisition LLC in July.

Cadre Holdings Inc. hit by cyberattack

Manufacturing

Denial of operations

US safety and survivability products provider Cadre Holdings Inc. determined on July 15 that it had experienced a cybersecurity incident in which an unauthorized third party gained access to some of the company's technology systems, according to an SEC 8-K report. In response to the incident, some systems were shut down, which impacted some of the company's operations. After detecting the incident with its security tools, the company immediately initiated its standard response protocols to contain, assess and remediate the incident, including beginning an investigation with outside experts, activating its incident response plan, notifying federal law enforcement authorities, and taking certain systems offline out of an abundance of caution. Although some of the company's operations were affected, the company was unable to determine at the time of the report whether the incident had, or was reasonably likely to have, a material impact on the company's financial condition or operating results.

Later, the impact of the attack on Q3 2024 earnings was estimated to be approximately five points of gross margin pressure.

Hanwha Qcells hit by ransomware

Manufacturing

Personal data leakage

Ransomware

The German site of photovoltaic cell manufacturer Hanwha Qcells was subject to a cyberattack. According to a customer letter obtained by heise online, the attack on the company's IT systems occurred on July 14. Hanwha QCells later confirmed the incident to the media outlet. According to the letter, unknown third parties apparently managed to gain access to parts of the customer and business partner database, and personal data of customers and business partners was leaked. The company worked to restore the systems. The State Office of Criminal Investigation and the State Commissioner for Data Protection of Saxony-Anhalt were involved.
In August the Abyss ransomware group claimed responsibility for the attack on Hanwha Qcells and told to have obtained over 5.4 TB of the company's data.

Elyria Foundry Holdings LLC hit by ransomware

Manufacturing

Personal data leakage

Ransomware

Elyria Foundry Holdings LLC, a US manufacturer of iron castings for various industries, including automotive, engineering, and other commercial uses, detected suspicious activity on its computer network on June 25 and filed a breach notification document with the attorney general of Maine in September. The company immediately took steps to secure its systems and launched an investigation into the nature and scope of the incident with the assistance of third-party forensic specialists. The investigation revealed that for a period of several hours between June 24 and June 25, 2024, an unknown actor gained access to certain systems on its network and may have viewed or copied specific files from those systems. In response, Elyria Foundry Holdings LLC conducted an extensive, time-consuming review of the affected files to determine what information they contained and to whom that information relates. On August 1, 2024, the company completed its review and began notifying potentially affected individuals. The type of information affected by this event includes name and Social Security number. Elyria Foundry Holdings LLC has since worked to implement additional technical safeguards in its information technology environment. The Play ransomware group claimed responsibility for the attack on Elyria Foundry Holdings LLC in July.

New England Wooden Ware Corporation hit by ransomware

Manufacturing

Personal data leakage

Ransomware

US packaging manufacturer New England Wooden Ware Corporation (NEWW) reported to the attorney general of Maine in September that on or around April 5, NEWW 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 August 2, following a thorough investigation, NEWW determined that a limited amount of personal information may have been accessed by an unauthorized third party as a result of the incident. The information potentially accessed by the unauthorized individual(s) may have included first and last names, as well as data that wasn't specified in a public document. NEWW took steps to address the incident and is committed to protecting personal information in its care. Upon learning of the incident, the company immediately took steps to secure its systems and enhance network security to prevent similar incidents from occurring in the future. The Play ransomware group claimed responsibility for the attack on New England Wooden Ware Corporation in April.

Clark Material Handling Company hit by ransomware

Manufacturing

Denial of IT systems, personal data leakage

Ransomware

US forklift manufacturer Clark Material Handling Company became aware of a security incident impacting its internal systems on March 3. It was reported to the Maine attorney general in August. The company took immediate steps to investigate, contain and remediate the incident with the assistance of external cybersecurity experts. The investigation determined that between approximately February 14, 2024 and March 3, 2024, an unauthorized third party accessed and copied files contained within certain segments of the company's network. The investigation confirmed that this incident occurred as a result of a compromise of the company's outside web developer, which resulted in the unauthorized third party gaining access to the company's environment through the web developer's account. As part of the investigation, Clark Material Handling Company initiated a detailed review of these files. The review concluded on July 9, by which time it was determined that some of the affected files contained personal information, including full name, Social Security number, and possibly one or more of the following: passport number, driver's license number, tax ID, financial account number, payment card number, medical information, and/or insurance information. Upon learning of the incident, the company moved quickly to initiate a response that included working closely with forensic consultants to investigate, contain and eradicate the incident, as well as to confirm the security of the network environment. The company also notified

federal law enforcement authorities of the incident, reset all passwords, and implemented additional security measures to help protect the privacy of the information stored in its systems. The Hunters International ransomware group claimed responsibility for the attack on Clark Material Handling Company in March.

M&R Printing Equipment Inc. hit by ransomware

Manufacturing

Denial of IT systems, personal data leakage

Ransomware

US digital and screen printing equipment manufacturer M&R Printing Equipment Inc. discovered on June 6 that it had been the victim of a sophisticated ransomware attack, according to a data breach notification filed in August. Upon discovery, the company immediately began working with its IT team and third-party forensic specialists to secure its network, restore its systems to full operability, and investigate the full nature and scope of the incident. The company also reported the incident to federal law enforcement authorities. The investigation determined that data of current and former employees may have been impacted. The comprehensive review was completed on July 8. M&R Printing Equipment Inc. has not publicly disclosed the exact nature of the personal information that may have been exposed.

K-FLEX USA LLC hit by cyberattack

Manufacturing

Personal data leakage

US insulation manufacturer K-FLEX USA LLC notified the attorney general of Maine in July that it had experienced a data breach in which the sensitive personal identifiable information in its systems may have been accessed and acquired. According to the breach notice, on or about November 14, 2023, K-FLEX USA LLC discovered that it was the victim of a cybersecurity attack. As a result, the company launched an investigation to determine the nature of the incident. Through its investigation, it learned that sensitive personal information may have been viewed or taken from its systems. As a result, K-FLEX USA LLC began a review of the data to determine what information was affected and to identify the specific individuals impacted. On July 12, the company completed this review. While the affected information varied depending on the individual, the type of information potentially exposed includes name, Social Security number, and/or driver's license or state identification card number. K-FLEX USA LLC implemented additional security measures to minimize the risk of a similar incident occurring in the future.

Power and energy

TotalEnergies Clientes SAU hit by cyberattack

Energy

Personal data leakage

TotalEnergies Clientes SAU, a global energy company headquartered in France, reported a significant cyberattack that compromised the personal data of 210,715 customers. The company detected unauthorized access to one of its sales management computer systems, which exposed sensitive customer information. The company worked with the police and the Spanish Data Protection Agency to take all appropriate legal action against those responsible.

Halliburton hit by ransomware

Energy

Denial of operations, data leakage

Ransomware

US oilfield services company Halliburton confirmed that it suffered a cyberattack. In a filing with the US Securities and Exchange Commission, Halliburton wrote that the company became aware of the incident on August 21 and took certain systems offline to mitigate the situation and prevent it from spreading. Upon learning of the issue, Halliburton activated its cybersecurity response plan and launched an internal investigation with the assistance of external advisors to assess and remediate the unauthorized activity. The attack appeared to impact business operations at the company's north Houston campus, as well as some global connectivity networks, according to Reuters. The company asked some staff not to connect to internal networks. On August 30, Halliburton released another filing confirming the data theft. The filing stated that the incident caused disruptions and limited access to portions of the company's business applications that support aspects of the company's operations and corporate functions. The company incurred, and may continue to incur, expenses related to its response to this incident.

BleepingComputer learned that the RansomHub ransomware group was behind the attack after receiving an email from Halliburton containing a list of IOCs with file names and IP addresses associated with the attack. One of the IOCs was for a Windows executable called maintenance.exe, which BleepingComputer has confirmed to be a RansomHub ransomware encryptor. TechCrunch has seen a copy of a ransom note purportedly related to the Halliburton incident that claims to have encrypted and stolen the company's files. The note says the RansomHub ransomware group had taken credit for the cyberattack.

The company later reported $35 million in charges directly related to the attack.

Anderson Feazel Management, Inc. hit by cyberattack

Energy

Personal data leakage

US energy company Anderson Feazel Management, Inc., which specializes in oil and gas production, suffered an attack on its computer system on or around July 31. In September the company began sending data breach notification letters to victims and notified the attorneys general of Maine and New Hampshire. The malicious actor behind the attack accessed and exfiltrated unencrypted financial documents that contained individual and employee records, business records, mineral leases, payroll records, and other private or personal information. Upon discovering the intrusion on August 1, Anderson Feazel Management, Inc. immediately notified the FBI and state law enforcement authorities. The company said the personal information stolen by the attackers varied depending on the victim's relationship with the company and may have included: name, date of birth, Social Security number, address, salary information, W-2s, and tax return documents. Upon discovery, Anderson Feazel Management, Inc. contacted federal and local law enforcement agencies and took steps to safely restore its systems and operations, including forced password changes and increased security monitoring. Anderson Feazel Management, Inc. also enlisted the services of an independent forensic expert to conduct a full forensic investigation to determine the vector of attack, the nature and scope of the incident, and to assist in remediation efforts.

Netherland, Sewell & Associates, Inc. hit by ransomware

Energy

Denial of IT systems, personal data leakage

Ransomware

Netherland, Sewell & Associates, Inc., a US upstream engineering provider specializing in the oil and gas industry, suffered a ransomware attack that disrupted the company's network in July and filed a breach notification document with the attorney general of Maine in September. Netherland, Sewell & Associates, Inc. began investigating immediately, enlisting the help of an outside law firm and forensic experts. The investigation consisted of a thorough review of the information systems affected by the attack. On or around August 16, it was determined that customers' personal information, including Social Security numbers, may have been affected by the incident.

Automotive

BMW Hong Kong data breach

Manufacturing, automotive

Personal data leakage

BMW Hong Kong suffered a data breach affecting approximately 14,000 customers. The leak was disclosed on July 15 following a post on a dark web forum by a threat actor known as 888. The leaked data includes sensitive personal information such as titles, surnames, first names, mobile phone numbers, and SMS opt-out preferences. On July 25, BMW Concessionaires (HK), the exclusive distributor of BMW vehicles in Hong Kong, confirmed that confidential information had been leaked. The company said the compromised data was managed by a third-party contractor, Sanuker, which had alerted both the police and the privacy watchdog about the BMW data leak. The Office of the Privacy Commissioner for Personal Data investigated the incident.

Toyota Motor North America data breach

Manufacturing, automotive

Data leakage, personal data leakage

Toyota's US subsidiary confirmed to BleepingComputer that it suffered a data breach after threat actor ZeroSevenGroup posted an archive of 240 GB of data stolen from its systems on a cybercrime forum. The company initially claimed that the security breach was limited in scope and not a system-wide problem. Toyota Motor North America added that it was working with those affected and would provide assistance if needed. A day later, in a new statement shared with BleepingComputer, a spokesperson clarified that Toyota Motor North America's systems were not breached or compromised, and that the data was stolen from what appears to be a third-party entity that is misrepresented as Toyota, but declined to identify the breached third party. The data leaked on the forum allegedly includes personal and professional contact details, financial records, customer profiles, business plans, employee information, and more. The hackers claim to have accessed Toyota's internal systems, and the data also reportedly contains photos, databases, network infrastructure details and emails. The hackers also released a tool called AD-Recon, which provides a detailed survey of the target network, including passwords and other sensitive network information.

Hanon Systems USA, LLC hit by ransomware

Manufacturing, automotive

Personal data leakage

Ransomware

US thermal management solutions manufacturer Hanon Systems USA, LLC was the victim of a ransomware event on July 21 that saw certain information accessed by a third-party actor and held under the threat of ransom, according to a breach notification document filed with the Maine attorney general in September. The company confirmed that some personal information was affected by the incident. Information potentially affected by the incident may have included names, contact information and Social Security numbers. Upon discovering the incident, the company immediately took steps to prevent such an event from occurring in the future, including enhanced security measures. The Hunters International ransomware group claimed to have breached Hanon Systems USA, LLC in August. The hackers allegedly exfiltrated 2.3 TB (1,632,581 files) of data.

Construction

Hiap Seng Industries Ltd. hit by ransomware

Construction, engineering

Personal data leakage

Ransomware

In July, Singapore-based construction engineering company Hiap Seng Industries Ltd. announced that it was the subject of a ransomware incident in which an unknown party gained unauthorized access to the company's servers. Upon discovering the incident, the company immediately took containment measures by isolating its servers from the network and activating restoration and recovery steps to ensure business and operational continuity. As of July 2, the incident had had no material impact on the company's operations, and Hiap Seng Industries Ltd. had appointed third-party experts to conduct a forensic investigation into the incident and provide advice on how to strengthen its overall cybersecurity. The company also reported the cybersecurity incident to the relevant authorities.

In October, the Personal Data Protection Commission of Singapore shared details of the attack on Hiap Seng Engineering. Investigations revealed that on June 11, a threat actor gained access to the company's network via a firewall VPN device using a local administrator account credential obtained by exploiting vulnerabilities in the VPN device. Passwords were found stored in the VPN device's configuration file and were encrypted using old encryption methods that the threat actor was likely able to decrypt. The incident affected the personal data of 10,000 individuals, including employees, former employees, and contractors, most of which were stored and encrypted by the company in on-premises payroll software. The types of personal data affected included a

combination of name, address, NRIC/FIN number, date of birth, photograph, work permit number, bank account details, telephone number and passport number.

CRB Engineering hit by ransomware

Construction, engineering

Denial of IT systems, personal data leakage

Ransomware

US engineering, construction and consulting firm CRB Engineering notified the New Hampshire attorney general that it had experienced a data breach that may have compromised the sensitive personal identifiable information in its systems. According to the breach notice, on January 3, 2024, CRB Engineering experienced a network disruption that impacted some computer systems. The company launched an investigation to determine the nature of the incident. Through its investigation, CRB Engineering learned that sensitive personal information in its systems may have been viewed and taken by an unauthorized actor between December 25, 2023 and January 3, 2024. As a result, the company began a review of the data to determine what information was affected and to identify the specific individuals affected. On August 21, CRB Engineering mailed data breach notification letters to impacted individuals. The LockBit ransomware group claimed responsibility for the Lavelle attack in February.

Basement Systems hit by ransomware

Construction, engineering

Denial of IT systems, personal data leakage

Ransomware

US construction company Basement Systems notified the attorneys general of Maine and Vermont that it had experienced a data breach that may have compromised the sensitive personal identifiable information in its systems. According to the breach notice, on May 13, Basement Systems discovered that it had experienced an incident that temporarily disrupted its computer network. As a result, Basement Systems launched an investigation to determine the nature of the incident. Through its investigation, Basement Systems learned that sensitive personal information may have been viewed by an unauthorized third party between April 12 and May 14. As a result, Basement Systems began a review of the data to determine what information was impacted and to identify the specific individuals affected. While the information impacted varied depending on the individual, the type of information potentially exposed includes name and Social Security number. The company implemented aggressive measures to enhance network security and minimize the risk of a similar incident occurring in the future. The company notified the Federal Bureau of Investigation and said it would provide whatever cooperation was necessary to bring the perpetrators to justice. The Cicada3301 ransomware group claimed

responsibility for the attack on the company in June, allegedly stealing 739 GB of data.

Siegfried's Basement hit by ransomware

Construction, engineering

Personal data leakage

Ransomware

US construction company Siegfried's Basement notified the attorney general of Vermont it had experienced a data breach that may have compromised sensitive personal data. The exposed information potentially included names, contact details, Social Security numbers, dates of birth, and financial and banking information, including credit card numbers. Siegfried's Basement started mailing data breach notifications and offering credit monitoring services to affected individuals. The ransomware group BlackSuit claimed responsibility for the cyberattack on Siegfried's Basement.

S&F Concrete Contractors, Corp. hit by ransomware

Construction, engineering

Personal data leakage

Ransomware

US construction company S&F Concrete Contractors, Corp. notified the attorneys general of Vermont and Maine it had experienced a data breach that may have compromised the sensitive personal identifiable information and protected health information in its systems. According to the breach notice, S&F Concrete Contractors, Corp. discovered suspicious activity in its computer systems earlier this year. As a result, the company launched an investigation to determine the nature of the incident. Through its investigation, S&F Concrete Contractors, Corp. learned that sensitive personal information in its systems may have been compromised between May 5 and May 20, 2024. As a result, the company began a review of the data to determine what information was impacted and to identify the specific individuals affected. While the affected information varies depending on the individual, the type of information potentially exposed includes: name, Social Security number, driver's license number, state or federal identification number, financial account information, and health insurance information. The company reported this incident to law enforcement authorities, and took steps to implement additional safeguards and review policies and procedures relating to data privacy and security. The Danon ransomware group claimed responsibility for the attack on S&F Concrete Contractors, Corp. in May, allegedly stealing 1 TB of data.

Electronics

Microchip Technology hit by ransomware

Manufacturing, electronics

Denial of IT systems, denial of operations and services, data leakage, personal data leakage

Ransomware

US chip manufacturer Microchip Technology Incorporated detected suspicious activity in its information systems on August 17, according to an SEC 8-K filing. The attack disrupted some of the company's business operations and the work of some of its factories, and impacted the company's ability to fulfill orders. The company investigated the incident and worked to restore its systems and normal operations. Upon detecting the issue, the company began taking steps to assess, contain and remediate the potentially unauthorized activity, isolated the affected systems, shut down certain systems and launched an investigation with the assistance of external cybersecurity advisors. The financial impact of the incident was yet to be determined. The Play ransomware group added Microchip Technology to its data leak site on August 29. They claimed to have stolen a wide range of information from Microchip Technology's compromised systems, including private and personal confidential data, customer documents, as well as budget, payroll, accounting, contract, tax, ID and financial information.

In a September 4 filing with the US Securities and Exchange Commission, Microchip Technology announced that its mission-critical IT systems were back online, operations were substantially restored and the company had been processing customer orders and shipping products for more than a week. The company continued to work diligently to bring the remaining affected portions of its IT systems back online while continuing to follow cybersecurity protocols. Microchip Technology believes an unauthorized party obtained information stored in certain IT systems, including employee contact information and some encrypted and hashed passwords. The company has not identified any customer or supplier data obtained by the unauthorized party. The company reported expenses of $21.4 million as a result of the attack in its quarterly report.

Kernex Microsystems hit by ransomware

Manufacturing, electronics

Ransomware

Kernex Microsystems, an Indian provider of electronic systems and software solutions for railways, reported in accordance with Regulation 30 of the Securities and Exchange Board of India that a cybersecurity incident targeting its IT infrastructure with a ransomware attack occurred on August 28. The company's technical team, assisted by external cybersecurity experts, actively analyzed the incident. No significant impact on the company's operations was reported.

MEMC LLC hit by ransomware

Manufacturing, electronics

Personal data leakage

Ransomware

MEMC LLC, a US producer of advanced semiconductor materials for the electronics industry, experienced an unauthorized intrusion into its network in June and filed a breach notification document with the attorney general of Maine in September. Upon learning of the issue, MEMC LLC immediately began a prompt and thorough investigation, contained and secured the network, eradicated the threat, and notified law enforcement. Following an extensive forensic investigation and manual document review, MEMC LLC determined on September 18 that an unauthorized individual(s) may have removed certain files containing personal information from its network. The company said the files taken by the threat actor contained the customer's name and other information it did not disclose.

The BlackBasta ransomware group claimed responsibility for the attack on MEMC LLC via its dark web leak site in July. The group claimed to have access to 1 TB of organizational data, including corporate data, financial data, NDAs, confidential data, HR data, hiring data, R&D data, engineering data, personal employee documents and information, and customer data.

Kulicke and Soffa Industries, Inc. hit by ransomware

Manufacturing, electronics

Denial of operations, personal data leakage

Ransomware

Kulicke and Soffa Industries, Inc. (K&S), a US manufacturer of semiconductors and electronic assembly solutions, reported to the attorney general of Maine and submitted an 8-K filing that it experienced a data breach in which the sensitive personal information in its systems may have been accessed and acquired. According to the breach notice, K&S first became aware of a ransomware attack on May 12 when it was contacted by an organization that claimed to have accessed and encrypted specific K&S files and that provided screenshots to support its claims. Disruption to the company's business operations was limited due to robust isolation, backup and recovery efforts. The company's continuity planning strategy allowed it to continue operations and customer services with minimal disruption. Through its investigation, K&S confirmed on July 12 that sensitive personal information in its systems may have been viewed and obtained by an unauthorized third party. As a result, K&S began a review of the data to determine what information was affected as well as identify the specific individuals affected. On September 16, K&S completed this review and discovered that the potentially exposed records included the names, identification numbers, bank account numbers, and/or bank routing numbers of current and/or former employees as well as their dependents and other individuals associated with K&S. Upon discovering the incident, K&S reset

passwords for all employee accounts, suspended mobile email access for employees, identified and removed malicious files, and significantly enhanced its monitoring, logging, and detection capabilities. The company brought in global security professionals to conduct an independent investigation and assist with recovery efforts.

The LockBit ransomware group claimed responsibility for the attack in June, claiming to have exfiltrated 20 TB of sensitive information and data (over 12 million files) from over 2000 different devices.

Utility

British Virgin Islands Electricity Corporation hit by ransomware

Energy, utility

Denial of IT systems, denial of operations and services

Ransomware

The British Virgin Islands Electricity Corporation (BVIEC) announced on August 19 that it had fallen victim to a cyberattack that affected its internal and external operations. The energy company worked with experts and law enforcement agencies, both locally and in the United Kingdom, to resolve the issue and restore normal operations. Despite the incident, BVIEC continued its efforts to restore power to the British Virgin Islands after Tropical Storm Ernesto made landfall. The general manager of BVIEC told local media that the attack penetrated the company's defenses and the incident was identified as a ransomware attack. The incident severely hampered BVIEC's ability to digitally manage its operations. It was noted that the corporation had to disconnect all systems as a precautionary measure to prevent further damage. BVIEC's financial controller revealed that several of the utility's systems were affected, including the billing system and customer service database, the automated meter reading system, and the company's ability to calculate and print invoices and checks.

The customer payment system was not restored until November. Prior to that, customers were asked to make payments in person and provide receipts of past payments to help estimate billing.

Blue Ridge Rural Water Company Inc. hit by cyberattack

Water supply, energy, utility

Personal data leakage

US-based Blue Ridge Rural Water Company Inc. suffered a cyberattack on its corporate network, which was a separate system from its water management network. The rural water utility said it experienced the attack on July 23 and quickly moved into defense mode by implementing its security program. It immediately implemented its response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations was brought in. Blue Ridge Rural Water Company Inc. also notified law enforcement authorities and assisted with their investigation. The evidence indicated that on July 23, 2024, an unauthorized actor viewed and obtained files stored on certain servers in the company's network. Blue Ridge Rural Water Company Inc. conducted a careful review of the files and determined that one or more of the files contained the name and Social Security number of an individual residing in Maine.

Air-e hit by ransomware

Energy, utility

Denial of services

Ransomware

Air-e, an electricity service provider in Colombia, released a statement on September 5 stating it had been the victim of a ransomware attack. The statement followed complaints on social media about the unavailability of some services since September 2, and the receipt of anonymous screenshots of alleged messages left by attackers. According to the company's statement, the company detected a cyberattack on September 2 that compromised several of the company's internal systems. The attack succeeded in penetrating the security measures in place, including the Clara security monitoring service and an advanced protection tool. Air-e claimed that the ransomware used by the attackers had not been previously identified, suggesting a high level of sophistication. In response to the incident, Air-e reported the attack to the attorney general's office on September 2. The company's contingency plan for cyberattacks was activated, prioritizing the restoration of compromised systems from previously stored backups. Working with cybersecurity experts, the company conducted a thorough assessment to mitigate any further damage and strengthen security barriers. Air-e stressed that the provision of energy services was not affected at any time and continued to operate normally. The company informed its users that they would have to visit physical offices to pay for services. On September 13, Air-e reported that it had successfully reactivated the printing and distribution of invoices. The incident caused a delay of approximately four days in issuing some bills.

Arkansas City Water Treatment Facility hit by cyberattack

Water supply, energy, utility

Denial of operations

The Arkansas City Water Treatment Facility (USA) was the victim of a cyberattack on September 22. The incident was reported on September 24. As a precaution, the Water Treatment Facility went into manual mode while the situation was being resolved. The City manager assured the public the water supply remained completely safe and there was no interruption in service. Cybersecurity experts and government agencies worked to resolve the situation and return the facility to normal operations. Enhanced security measures were in place to protect the water supply, and no changes in water quality or service were expected for residents. City officials notified authorities about the incident, and Homeland Security and FBI agents investigated, according to local media.

The investigation confirmed that no sensitive data was accessed or exfiltrated. The attack required temporary adjustments to the facility and resulted in costs of $105,201 for server replacement, software, licenses, and technical assistance. The company had to pay an additional $58,550 for forensic analysis, legal guidance, and communication with the threat actors. The City said insurance would cover most of the costs, except for a $10,000 deductible.

Logistics and transportation

JAS Worldwide hit by ransomware

Transportation, logistics

Denial of IT services, denial of operations

Ransomware

JAS Worldwide, a global freight company headquartered in the USA, confirmed on August 27 that it had been the victim of a ransomware cyberattack that had disrupted its operations and customer services. The company quickly secured its systems and launched an investigation with the help of cybersecurity experts. It put in place measures to restore its services. On August 31, JAS Worldwide announced that it had managed to reactivate some of its operations, including its email system and website. A week after the attack JAS Worldwide confirmed that most of its systems were operational and that it was actively working through backlogged requests. The company conducted a global password reset and took additional measures to improve its cybersecurity posture. By that time JAS SmartHub was operational, so customers were able to track their shipments in real time. The vast majority of customers and vendors were served as usual, and any backlogged requests were worked on by a dedicated team.

Port of Seattle hit by ransomware

Transportation, logistics

Denial of IT systems, denial of services, data leakage

Ransomware

The Port of Seattle (USA), which operates the port and Seattle-Tacoma International Airport, announced via social media on August 24 that it had experienced certain system outages that indicated a possible cyberattack. The internet and web systems outage impacted some systems at the airport. Phone systems at the Port of Seattle Maritime Facilities were also down.
The port isolated critical systems and worked to restore full service. The Transportation Security Administration worked with its partners at the port. Its spokesperson told GeekWire that there was no impact on security operations. According to social media posts, some maritime operations were also in recovery mode.

The Port of Seattle released new details about the August cyberattack in a statement on September 13. The investigation determined that the unauthorized actor was able to gain access to certain parts of the computer systems and was able to encrypt access to some data. According to the statement, the ransomware attack was carried out by the Rhysida group. The Port of Seattle said Rhysida claimed to have stolen data and could post it on its dark web site as a result of the refusal to pay a ransom. The port took steps to block further activity, including disconnecting its systems from the internet, but the encryption and response measures affected some services, including baggage, check-in kiosks, ticketing, Wi-Fi, passenger display boards, the port's website, the flySEA app, and reserved parking. The team was able to bring most of the affected systems back online within the week, although work was still ongoing to restore some systems such as the external website and internal portals. On September 16, the Rhysida group posted a ransom demand of 100 bitcoins and images of alleged documents stolen from the organization.

Kantsu hit by ransomware

Transportation, logistics

Denial of services, denial of operations, personal data leakage

Ransomware

Japanese logistics and transportation company Kantsu was the victim of a ransomware attack on September 12, resulting in the detection of an infection on some of its servers and the shutdown of its networks to prevent further attacks. An emergency team was set up to investigate the incident and take measures to repair the damage and prevent further attacks. The company notified and consulted with relevant government agencies and police, and engaged external security experts to investigate the intrusion. On September 28, the company issued an update stating that the cyberattack, which was carried out via an external network connection, led to the encryption of several servers and caused disruptions to its goods storage and retrieval systems. The

attack affected both Kantsu and its business partners, delaying operations. Some of the affected servers contained personal information, prompting the company to file a report with the Personal Information Protection Commission. To restore operations, the company built a new environment separate from the affected one.

Brown Integrated Logistics Inc. hit by ransomware

Transportation, logistics

Personal data leakage

Ransomware

US company Brown Integrated Logistics Inc. (BIL) notified the attorney general of the Commonwealth of Massachusetts, and the attorneys general of Maine and Montana that it had experienced a data breach that may have compromised the sensitive personal identifiable information in its systems. On November 15, 2023, BIL became aware of suspicious activity in its computer network. The company immediately launched an investigation, with the assistance of third-party cybersecurity specialists. The investigation determined that, beginning on or about November 13, 2023, an unauthorized actor gained access to certain systems and that certain information in those systems was potentially accessible. BIL conducted a comprehensive, programmatic and manual review to determine what information was accessible and to whom the information relates. The company completed this process on August 27, 2024. The type of information potentially exposed included names and Social Security numbers. Around September 23, 2024, BIL began mailing data breach notification letters to affected individuals. The LockBit ransomware group claimed responsibility for the attack on Brown Integrated Logistics Inc. in November 2023.

Food and beverage

Banham Poultry hit by ransomware

Manufacturing, food and beverage

Personal data leakage

Ransomware

British producer of chicken products Banham Poultry said criminals had remotely accessed its system in the early hours of August 18. In an email to staff seen by the BBC, the company said information such as National Insurance numbers, copies of passports and bank details were accessed. The plant immediately shut down its systems and brought in external forensic specialists following the cyberattack. The email from the company's HR department said it was not aware of anyone's information having been used maliciously or that anyone had suffered any detriment as a result of the incident. The company said it had reported the incident to the Information Commissioner's Office and had

installed additional security. Banham Poultry was listed as a victim of the RansomHub ransomware group on August 21.

McIlhenny Company data breach

Manufacturing, food and beverage

Personal data leakage

Ransomware

US food manufacturer McIlhenny Company discovered a security breach around July 22 that stemmed from a vulnerability in third-party code, according to a breach notification document filed with the Maine attorney general in September. The issue was promptly addressed and a patch was issued and successfully applied to mitigate the risk. The company launched an investigation into the matter that revealed the vulnerability allowed an unauthorized party to access certain payment information. This information included customers' names, mailing addresses, email addresses, and credit card numbers, as well as credit card expiration dates and security codes. McIlhenny Company has not received any reports of related identity theft since the date of the incident.

Peco Foods hit by ransomware

Manufacturing, food and beverage

Personal data leakage

Ransomware

US producer of poultry products Peco Foods notified the attorney general of Maine in July that it had experienced a data breach that may have compromised the sensitive personal identifiable information in its systems. According to the breach notice, upon learning an unauthorized third party had accessed its systems, Peco Foods launched an investigation to determine the nature of the incident. As part of its investigation, the company learned that an unauthorized third party accessed this sensitive information on or around December 4, 2023. Peco Foods began a review of the data to determine what information was impacted and to identify the specific individuals affected. On May 23, 2024, the company completed the review. The exact type of personal information that may have been exposed was not publicly disclosed by Peco Foods. The BlackBasta ransomware group added Peco Foods to its dark web portal in December 2023.

Chemicals

Innophos Holdings Inc. hit by cyberattack

Manufacturing, chemicals

Denial of operations, personal data leakage

Innophos Holdings Inc., a US manufacturer of chemicals for the food, health, nutrition, and industrial markets, reported to the attorney general of Maine in August that it had experienced a data breach that may have compromised sensitive personal information in its systems. According to the breach notice, Innophos Holdings Inc. became aware of suspicious activity on its computer network on June 4. As a result, the company launched an investigation that revealed sensitive personal information in its systems may have been viewed by an unauthorized actor on or around June 4. The company then began a review of the data to determine what information was impacted as well as identify the specific individuals affected. The exact type of personal information potentially exposed was not publicly disclosed by Innophos Holdings Inc. The company took immediate action to lock down its systems, notify federal law enforcement authorities, bring in a leading cybersecurity forensic team to investigate the incident, and deploy enhanced monitoring technologies. As a result of these steps, the company was able to recover from the incident and bring its operations back online. Innophos Holdings Inc. continues to work with its teams of experts to address the incident and implement additional measures.

Ortec hit by cyberattack

Manufacturing, chemicals

Denial of IT systems, personal data leakage

US custom chemical manufacturer Ortec experienced a network disruption on May 28 and submitted a breach notification to the attorney general of Maine in September. The company immediately took steps to secure the network environment and engaged cybersecurity experts to conduct an investigation, which determined that certain files may have been taken without authorization on or about May 28. Ortec conducted a comprehensive review of the affected data to determine whether personal information may have been involved, and on September 5, Ortec determined that some personal information was present in the affected data set. This information may include customers' names and Social Security numbers. The company also implemented additional measures to reduce the risk of a similar incident occurring in the future. Ortec notified the Federal Bureau of Investigation, saying it would provide whatever cooperation may be necessary to hold the perpetrators accountable.

Mining

Sibanye-Stillwater hit by ransomware

Mining

Denial of IT systems, denial of operations

Ransomware

South African mining company Sibanye-Stillwater was the victim of a ransomware cyberattack that disrupted some operations. Computer systems were taken offline, before gradually being restored. The mining company said it took immediate steps to proactively isolate IT systems and safeguard data as soon as it became aware of the incident. In a July 11 press release the company said only payroll was impacted by the attack. However, officials from its Montana operations told local media that smelter operations in Columbus, Ohio, were affected after all the automated systems went down, but workers remained on site. The company did not know who was behind the attack, and there were no payment demands.

On September 9, Sibanye-Stillwater notified the attorney general of the Commonwealth of Massachusetts and the attorney general of Maine that it had experienced a data breach that may have compromised sensitive personal identifiable information and protected health information in its systems. In August 2024, Sibanye-Stillwater learned that sensitive personal information in its US systems may have been compromised. As a result, Sibanye-Stillwater began a review of the data to determine what information may have been impacted and to identify the specific individuals affected. While the affected information varied depending on the individual, the type of information potentially exposed includes: name, Social Security number, date of birth, contact details, government ID and/or passport number, financial information, and medical information. The total number of individuals affected was estimated to be 7258. Sibanye-Stillwater was listed as a victim by the RansomHouse ransomware group.

Industrias Peñoles hit by cyberattack

Mining

Ransomware

Mexican mining company Industrias Peñoles announced that it was the victim of a cyberattack in a filing with the London Stock Exchange on July 30. The attack also affected its Fresnillo subsidiary. The company said the attack resulted in unauthorized access to certain IT systems and data. Upon discovering the attack, Fresnillo initiated response measures to contain the breach and its IT experts, in coordination with external forensic specialists, investigated and assessed the impact of the incident. The company also stated that the cyberattack did not affect its operations and that it doesn't expect any

financial or material impact. The Akira ransomware group claimed responsibility for the attack.

Evolution Mining hit by ransomware

Mining

Denial of IT systems

Ransomware

On August 8, Australian mining company Evolution Mining became aware of a ransomware attack affecting its IT systems, according to an official statement on August 12. The company acted quickly by bringing in external cybersecurity forensic experts to investigate and contain the incident, which the company believed was successful. The incident was reported to the Australian Cyber Security Centre and was not expected to have a material impact on the company's operations. The Australian Cyber Security Centre told Reuters that Evolution Mining had not provided them with much information about the incident.

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