

White Paper

# Ransomware Attacks By Industry

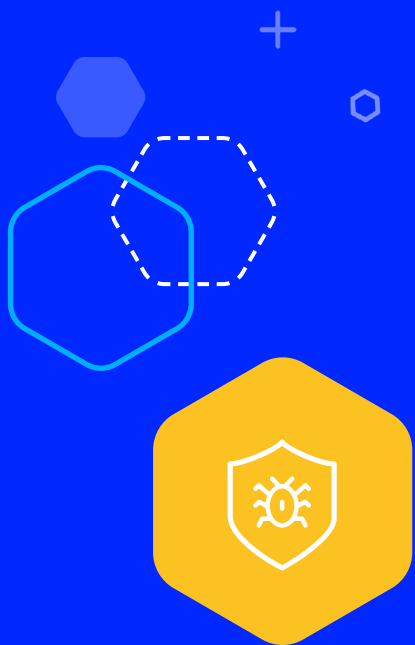
Recent Attacks and How to Defend Your Company



**IRONSCALES**  
SAFER TOGETHER



**SRC CYBER  
SOLUTIONS LLP**  
CYBER RISK SOLUTIONS



## Introduction

Ransomware is a plague on companies of all shapes and sizes around the globe, with no signs of slowing down. While progress has been made by various government agencies to identify, prosecute, and jail key members of various ransomware gangs, new gangs continue to pop up and former gangs reconstitute themselves with a new name but the same nefarious purpose.

In this guide, we will provide examples of ransomware attacks across a wide swath of industries as well as suggestions for your organization to consider implementing in order to better protect yourself.

00:00:00:38  
00:00:08:33  
00:00:14:19  
00:00:20:17  
00:00:25:53  
00:00:26:56



# Contents

---

Retail.....	4
Higher Education .....	7
Healthcare .....	11
Transportation.....	15
Hospitality.....	18
Mining.....	22
Media & Entertainment.....	24
Energy .....	28
Telecommunications .....	32
Agriculture .....	35
IT Services .....	37
Finance.....	41
Pharmaceutical.....	45

# Retail

## Notable Ransomware Attacks That Hit Retailers

Here is a brief run-through of five notable ransomware attacks on retailers within the last couple of years.

### The Works: April 2022

UK-based retailer The Works was the victim of a successful [ransomware attack](#). Reports indicate that the company had to shut down all 526 of its stores initially while its IT team investigated the impact of the attack but fortunately was able to open all but five stores within days of the attack. To date, there has been no ransom demanded of the company, but the software used in the attack is known to be a weapon of ransomware gangs. The company reported that no credit card data was stolen, as these payments are processed by an external third-party vendor.

### Moncler: January 2022

Italian luxury fashion designer brand Moncler reported that it had been the victim of a successful [ransomware attack](#). Reports after the attack said that it was the ransomware group [Black Cat](#) who attacked the company. The attackers demanded payment of \$3 million and threatened that they would post sensitive company details on the dark web if not paid. Montcler refused to pay the ransom, so Black Cat posted a series of documents related to the company's finances and customer base.

### Coop Grocery Store: June 2021

Coop is a Swedish chain of supermarkets that became one of the worst impacted companies from the Kaseya [ransomware attack](#) in July 2021. Affecting over 1,500 organizations around the world, the Kaseya attack exploited vulnerabilities in Kaseya VSA, which is an endpoint management application used by managed service providers.

The threat actors involved in this attack was the [REvil](#) ransomware group, which claims to make annual revenue of \$100 million through its malicious cyber activities. Coop had to close over 800 of its stores because the Kaseya attack directly impacted its cash registers. The ransomware propagated to Coop's payment systems Visma, which is a Swedish MSP that manages payment systems for the supermarket chain.



### **Dairy Farm Group: January 2021**

In January 2021, [ransomware struck](#) one of Asia's largest retailers, the Dairy Farm Group. Once again, REvil instigated the attack and demanded a whopping \$30 million ransom payment. It appears this was a double extortion attack in which the attackers demanded a higher ransom payment for the victim to decrypt compromised IT assets and avoid having exfiltrated data posted on the dark web.

The severity of this incident was such that the threat actors managed to take full control of the company's email system. Losing access to email is a nightmare scenario because it's much harder to communicate with employees about an in-progress cyber incident and instruct them on which actions to take that will help deal with the incident.

### **Whirlpool: December 2020**

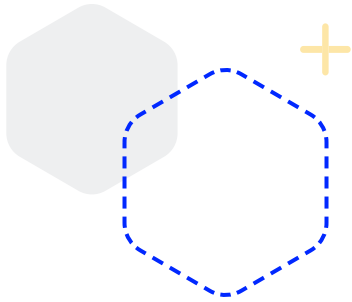
Whirlpool is a multinational home appliances provider that became the victim of a [ransomware attack](#) on the first weekend of December 2020. The Nefilim ransomware gang typically focuses its attacks on large companies using double extortion methods.

A ransom note left on Whirlpool's computers said, "we have encrypted your files with military-grade algorithms. If you don't have extensive backups, the only way to retrieve your files is with our software." Whirlpool managed to detect and contain the incident swiftly, which meant no noticeable operational impact. Nefilim published some data on the dark web obtained from Whirlpool's network, including inventory spreadsheets, work charts, and plant audit details.

### **E-Land: November 2020**

In November 2020, the South Korean retail giant E-Land had to close 23 of its retail outlets in response to a [ransomware incident](#). The Clop gang carried out the attack on E-Land whose CEO claimed at the time that sensitive customer data was safe. The network was disrupted, which impacted the ability to carry out in-store operations at some retail outlets.

However, a media interview with the [Clop gang](#) revealed that this ransomware attack was more damaging than first disclosed. According to Clop operators, they had breached the E-Land network well over 12 months prior. The result was to install POS malware and obtain the credit card details of over 2 million customers. After exfiltrating this potentially valuable data, the gang then installed ransomware that locked important files and systems.



## Travelex: December 2019

In December 2019, the foreign exchange services retailer Travelex fell victim to a serious [ransomware attack](#) that ultimately led to the company's bankruptcy and the loss of 1,300 jobs. The attack, instigated by REvil, forced the shutdown of the company's website and disrupted operations at brick-and-mortar outlets for over two weeks.

The incident occurred when threat actors breached the network by exploiting unpatched vulnerabilities in VPN servers used by Travelex. Some customers were left stranded in foreign locations without local currency as a result of the disruptions. Ultimately, the level of desperation to get their systems back resulted in the decision to pay a \$2.3 million ransom.

## Suggestions for retail companies

Based on the above ransomware incidents, there are several takeaways for retailers that help to understand the risks they face and put in place defenses to mitigate those risks.



**Software Supply Chain Risks:** The Kaseya incident highlighted the often-underplayed risks that can stem from a retailer's software supply chain. Retailers run complex operations, relying on many different software vendors to provide customer-facing and back-store functionalities. It's important to have visibility into all aspects of the software supply chain and react quickly after a compromise.



**Business Continuity Strategies:** While the Whirlpool incident resulted in some data theft, an efficient incident response (IR) strategy meant no operational disruptions. Retailers should have business continuity strategies in place, which include disaster recovery, the ability to restore email, and effective incident response teams who can contain an attack before it locks down the entire network.



**Advanced Endpoint Security:** The E-land attack showed that legacy signature-based endpoint security solutions aren't enough to detect cyber attacks. The Clop gang breached E-Land's network and probed it undetected for up to 12 months. Advanced endpoint security solutions use AI-driven features to detect suspicious endpoint behavior that can indicate an attack.



**Unpatched Vulnerabilities:** The Travelex attack was particularly surprising due to the basic cybersecurity flaws exposed. A security patch for the VPN vulnerability was available months before the incident occurred, but Travelex failed to apply the patch on time. Automated patch management is one of the quickest wins for any company—not just retailers—in avoiding data breaches.

# Higher Education



Higher education institutions are prime targets for ransomware attacks. Universities and colleges handle large amounts of sensitive personal data, facilitate a campus-wide intranet, and manage research data. These factors combine to make targeting the higher education sector a potentially lucrative operation for threat actors. The more sensitive the data, the more valuable it becomes in the wrong hands.

This article looks at the state of ransomware in higher education. You'll get the lowdown on relevant statistics, notable recent ransomware attacks, and some guidance for managing this threat.

## Ransomware in Higher Education: Overview

The tenets of higher education, encompassing openness, trust, and information exchange, add to the ransomware risks in this sector. These tenets contrast with the necessary rules, controls, and best practices for securing networks and data.

Ransomware is malicious software that blocks access to networks, systems, and/or files in an attempt to extort a ransom payment from its victims. Typically, access to valuable resources is blocked through encryption methods with a message indicating a return of those resources upon payment of the ransom.

Security experts have confirmed that at least seven US-based universities have been hit by ransomware attacks already in 2022, including Ohlone College, Savannah State University, University of Detroit Mercy, Centralia College, Phillips Community College of the University of Arkansas, National University College and North Carolina A&T.

## Recent Ransomware Attacks on Higher Education Institutions

### Kellogg Community College: May 2022

Kellogg Community College, a regional school system with five campuses in Michigan, was forced to cancel classes at the beginning of the final full week of the spring semester after being hit by a successful [ransomware attack](#) in early May 2022. The school system's IT systems, including online classes, campus emails, and other online resources, were adversely impacted for two days while their team investigated and remediated the attack. The IT team also initiated a forced password reset for all staff and students as a precautionary measure. No details have been provided as to who was responsible for the attack or if a ransom was ever demanded or paid.



### **Florida International University: April 2022**

Florida International University reported that they were the victims of a ransomware attack in April 2022. The ransomware group known as [ALPHV/Black Cat](#) claimed responsibility for the attack and said they stole 1.2 TB of data, including social security numbers of both staff and students, email databases, and accounting/contract details. Administration officials claim that no sensitive student or staff personal data was stolen. As of June 2022, no details have been provided to the public about what exactly was stolen or if a ransom was ever demanded or paid.

### **North Carolina A&T: March 2022**

North Carolina A&T reported that they were attacked during the week of Mar 7-11, 2022, while students were on spring break. The attack affected a number of security and educational tools, including single sign-on, VPN, and their document management system.

The ransomware group known as [ALPHV/Black Cat](#) claimed responsibility for the attack and said they stole personal information about students and staff as well as contracts and other financial data. School officials acknowledge that the attack happened but dispute the statement that any data was stolen. As of April 2022, recovery efforts continue but not all impacted systems have been restored yet.

### **Des Moines Area Community College (DMACC): June 2021**

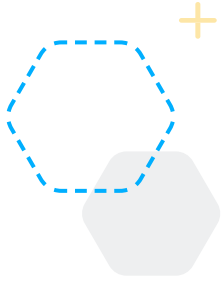
The most recent [ransomware incident](#) focuses on a community college in central Iowa. In early June 2021, an attack wreaked havoc on the DMACC IT network and led to the cancellation of all online courses followed by in-person classes the next day. The ramifications were such that online classes remained canceled for a full two weeks while the college attempted to restore its IT network.

It was interesting to see that the college's decision-makers opted not to pay the ransom demanded by the group behind this attack. It is not exactly clear what ransomware group was behind the attack or what the demanded ransom was. Federal organizations don't recommend paying ransoms because doing so can incentivize more attacks. Furthermore, paying up doesn't necessarily result in getting full access back to compromised systems, files, or other resources.

### **Sierra College: May 2021**

The scourge of [ransomware struck](#) a Northern Californian college at one of the worst times possible—during finals week. Like the previous incident, details on the type of ransomware or the perpetrators behind this attack also weren't revealed. What is known is that valuable learning resources for students were taken offline and required workarounds to get access to them.





According to a statement in the immediate aftermath of the attack, the college was “working with law enforcement and third-party cybersecurity experts to investigate this incident, assess its impact, and bring our systems back online”. The college’s registration service wasn’t available as a consequence of the attack, which potentially affected prospective students. An update two weeks after the initial incident disclosure revealed the restoration of most IT services at Sierra College.

### Multiple Universities: March 2021

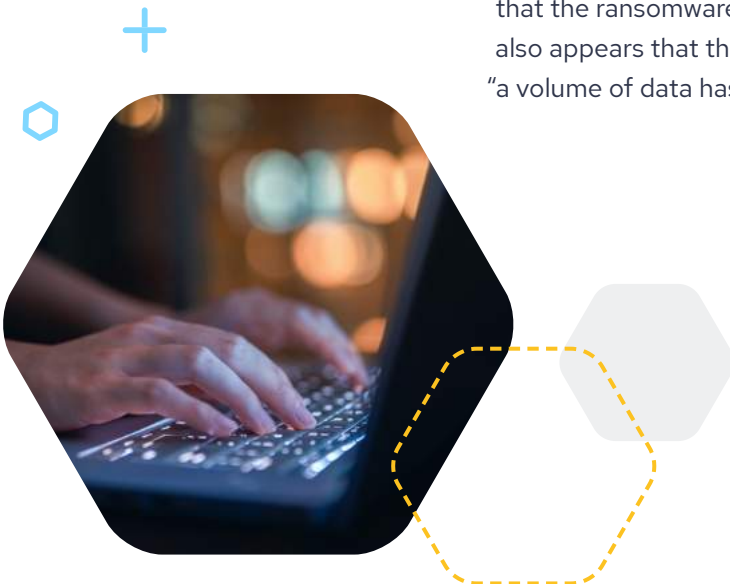
Multiple high-profile universities became victims of a [ransomware attack](#) conducted by the Eastern European Clop gang in March 2021. [Clop ransomware](#) uses phishing emails with malicious attachments to get into networks, lateral movement to spread quickly, and evasive techniques to avoid detection by security solutions. Data exfiltration is also a feature of Clop; the ransom demand comes with a threat to disclose stolen data to the dark web if the payment isn’t made.

In this incident, universities such as the University of Colorado, the University of Miami, and the University of California had sensitive data stolen when Clop ransomware compromised the [Accellion file transfer service](#). The stolen data included grades and other personal information. This incident highlighted the cyber risks that can come from third-party software vendors.

### South and City College Birmingham (UK): March 2021

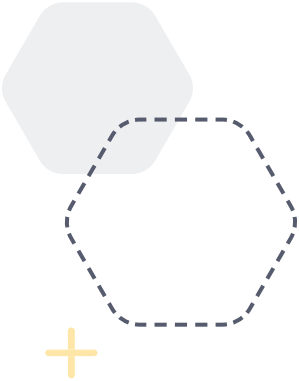
Across the Atlantic in England’s second city, Birmingham, a local college with eight campuses distributed throughout the city had to close all campuses following a major [ransomware attack](#).

On-campus servers and workstations were impacted, which resulted in students having to return to online learning only a week after they resumed in-person classes after a national lockdown to curb Covid-19. An official college [Tweet](#) stated that the ransomware attack disabled many of the core IT systems at the college. It also appears that this was a double extortion attack because, according to quotes, “a volume of data has been extracted from our servers”.



## Suggestions for Higher Education organizations

Thankfully, many educational institutions recognize the pervasive threat of this ever-increasing form of cyber attack. Most colleges and universities have IT teams with cybersecurity knowledge. Here are some tips to manage the threat of ransomware:



**Use Backups:** Having backups of important data and systems is always a useful strategy for minimizing the impact of ransomware attacks. A properly executed backup strategy provides the most comprehensive and effective way of getting compromised files and/or systems back. It's worth noting that organizations across all sectors that pay ransoms to perpetrators rarely get all of their affected data or systems back.



**Segment the Campus Network:** Ransomware and other forms of malware often proliferate through a network to inflict maximum damage. Good network segmentation splits a campus network into logical segments, which can isolate the harm from ransomware to one particular segment rather than across the whole network.



**Have an Incident Response Plan:** Organizations that contain and minimize the damage from in-progress ransomware attacks are invariably those with a solid incident response plan in place. This plan establishes instructions for responding to and recovering from detected cybersecurity incidents. A solid incident response plan needs to clearly and logically identify key roles, actions, and responsibilities during a cybersecurity incident.



**Implement a Cybersecurity Framework:** A cybersecurity framework provides a set of standards and guidelines for protecting against modern cybersecurity threats. Implementing these frameworks can prove to be an invaluable way to increase protection against ransomware and a whole host of other attack vectors. Cybersecurity frameworks are created by groups of cybersecurity experts. Example frameworks include the NIST Cybersecurity Framework and the CIS Controls.



**Combat Phishing Threats:** In an information-sharing space like a college or university intranet, trust and openness are encouraged. Unfortunately, this trust is exploitable by hackers who commonly use phishing techniques to gain an initial foothold into a network. By spoofing emails, the perpetrators can get victims to click malicious links or download email attachments that install malware. Email security tools can filter out or flag phishing emails before they get the chance to deceive people. A modern solution equipped for sophisticated threats should ideally be a self-learning AI-driven solution that continuously improves its effectiveness over time as it scans, filters, and flags deceptive emails.



# Healthcare



The sensitive nature of information gathered about patients makes healthcare organizations particularly vulnerable to ransomware attacks. Seeking a large payday, opportunistic hacking groups target the healthcare sector believing that disrupting critical patient services or stealing valuable data is more likely to result in payouts. This article looks at ransomware in healthcare by focusing on some recent incidents, statistics, and mitigation strategies.

## Ransomware in Healthcare: The Numbers

Think of all the types of data collected by a typical healthcare provider about their patients: names, addresses, social security numbers, symptoms, dates of admission/discharge, passport photos, and cardholder data. All this information is extremely valuable in the wrong hands. Furthermore, due to the critical nature of healthcare services, taking an organization's IT systems down and holding them to ransom may well result in getting paid.

The result of these factors is that ransomware is rampant in healthcare. Attackers attempt to gain entry routes into IT systems and lock down computers and servers with malware. Here are some of the most telling statistics.

- A [2021 report](#) found that 34 percent of surveyed healthcare organizations were hit by ransomware in the last year.
- The same report found that 34 percent of victims paid the ransom to get their data and/or systems back.
- The total cost of ransomware attacks on healthcare organizations was [\\$20.8 billion](#) in 2020.
- Recent Ransomware Attacks on Healthcare Organizations.

There have been innumerable high-profile ransomware attacks on healthcare organizations globally over the last 18 months. Hacking groups don't distinguish between public or private service providers—every organization is a target. Here are some recent examples that serve as important reminders of how ransomware can impact the provision of critical health services or expose sensitive patient information.



### **Partnership HealthPlan of California: March 2022**

The Partnership Healthplan of California (PHC) is a non-profit community-based healthcare organization that provides services across 14 counties in Northern California. In March 2022, the ransomware group as Hive made claims on their website that they had stolen 400 GB of data that included over 850,000 records that included social security numbers and home addresses of PHC's patients. The claim was later removed from Hive's website. To date there has been no confirmation of Hive demanding payment or if such a payment was ever made.

### **University Medical Center, Nevada: June 2021**

The [REvil](#) ransomware group (of JBS and Kaseya infamy) [breached the systems](#) of University Medical Center in Las Vegas and posted personally identifiable information (PII) online in June 2021. Luckily, the ability to continue caring for patients was not impacted by this attack, and no clinical systems were compromised. The attackers published information about numerous patients that included social security numbers and passport photos.


REvil is a ransomware-as-a-service (RaaS) operation that leases out pre-made ransomware variants to any customer willing to pay. Because subscribers to a RaaS service can access ransomware without much technical knowledge, this type of operation increases risks for healthcare organizations who are obvious targets to turn to. It's unknown at the time of writing how the hackers gained access to sensitive patient information at the hospital.

### **Scripps Health, San Diego: May 2021**


Scripps Health became the [victim of a severe ransomware attack](#) in May 2021 that resulted in over 147,000 patients having their personal information breached. The breached data included names, addresses, medical record numbers, and more. Scripps Health had to send breach notifications to all affected individuals and offer credit monitoring and identity protection support services.

An opinion piece written in the [San Diego Union-Tribune](#) by the CEO of Scripps Health highlighted the attack's impact. "Our IT team detected unusual network activity on our systems...we took down our systems; access to electronic medical records was restricted. This created operational disruption at our hospitals and facilities."

It appears this attack used the double-extortion technique increasingly favored by threat actors. Not content with just locking down systems, the intruders first acquired files with sensitive information before attempting to lock down important IT systems. It took almost a month to get the organization's patient portal back running again.



Hacking groups don't distinguish between public or private service providers—every organization is a target.



### HSE, Ireland: May 2021

Ireland's entire public health system, the Health Service Executive (HSE), made global headlines in May 2021 when it became the victim of a [vicious ransomware attack](#). Officials working for the HSE said the attack impacted every single aspect of patient care. The ramifications of this cyber attack were such that Ireland was the only country in the EU not ready to adopt the EU travel certificate system well over a month after the attack happened.

Reports emerged in the media that sensitive patient information was also leaked online as a result of the attack. In one instance, the medical file of a patient in palliative care surfaced on the dark web. Often, the perpetrators of ransomware attacks trickle stolen information online to encourage victims to pay up before the full data is released.

### University of Vermont Medical Center: October 2020

The University of Vermont Medical Center suffered a [ransomware attack](#) in October 2020. The initial detection of the attack coincided with the IT department finding a note instructing the hospital to contact the perpetrators. Often, the first message a victim receives about an attack is payment instructions to unlock their systems.

According to an official statement, the IT team had to scan and clean 5,000 computers and endpoints. The response to the attack also involved rebuilding critical computing infrastructure. The rebuilt infrastructure was then populated with backed-up files and data.

With IT systems voluntarily being shut down to contain the attack, patient services were directly impacted. Patients had appointments canceled and important treatments delayed. This attack was unique both for its lack of initial ransom demand and for the intensity with which IT systems were targeted.

## Suggestions for Healthcare Organizations



**Back Up Your Data:** Some may argue that backing up data does not help in a world where threat actors try to steal sensitive information before locking down systems. However, the UVM Medical Center attack shows that you can rebuild systems from backed-up data without needing to pay ransoms. Not every attack attempts to exfiltrate data, so backup remains a valid strategy.



**Use Advanced Email Security:** Threat actors favor phishing attacks as the initial attack vector for gaining entry to IT systems. These attacks use social engineering techniques to entice employees into downloading suspicious attachments or clicking suspicious links. An advanced email security solution can filter out emails before they even reach people's inboxes.



**Consider Data Loss Prevention Tools:** A data loss prevention (DLP) tool can provide an extra method of defending against the leakage of sensitive information outside a healthcare organization. These solutions monitor data flow to detect any violations of pre-defined security rules. The DLP solution can implement protective steps such as terminating login sessions, immediately encrypting the targeted data, or sending rapid alerts to IT security teams.



**Have A Robust Security Policy:** A good security policy addresses the human element that is often involved in ransomware attacks (and many other forms of cyber attacks). You can have all the latest solutions in place, but human error remains a primary way that hackers gain entry points into a network. Healthcare organizations need security policies that sets sensible rules and procedures for employees when using IT systems. All employees need to know their responsibilities to protect data. At a minimum, the policy should include the following:

- Requirements for setting strong passwords that outsiders can't easily break
- Rules for using email applications, such as not clicking on links or downloading attachments from external email addresses
- An internet usage policy that establishes how employees can use the internet and what types of sites they can/can't visit
- A physical security policy that sets rules and processes for ensuring outsiders can't access sensitive data



# Transportation

Transportation companies provide critical functions in shipping products and carrying people to their destinations. Encompassing both transport and logistics companies, the transportation sector is at a high risk of exposure to ransomware attacks that can disrupt services or even endanger peoples' welfare. This article examines the current state of ransomware in transportation.

## Why the Transportation Industry Is Susceptible to Ransomware

Transportation spans aviation, maritime, and ground services, and operators of all types of service are at risk of ransomware attacks. Three features of transportation make this sector attractive to threat actors:



The interconnected nature of transport services provides many different possible points of attack.



The knock-on effects of ransomware in transport can damage supply chains for many businesses, thereby increasing the likelihood of successful attackers getting a payday.



The critical societal function of transport gives state-sponsored actors the opportunity to wreak havoc in another country.

As far as the numbers go, data is not widely available about typical ransom demands resulting from successful attacks on transport service providers. The most recent general trends [showed a median ransom](#) of \$47,008.

## Recent Ransomware Attacks in Transportation

Transport operators tend to take cybersecurity seriously but attacks still occur with regularity. Threat actors operating ransom-as-a-service programs, lone wolf operators, or state-sponsored groups infiltrate networks and install malware that encrypts important files and systems. Here are some recent ransomware attacks in the transport sector.



### **Steamship Authority: June 2021**

The Steamship Authority of Massachusetts operates ferry services between destinations that include Cape Cod, Nantucket, and Martha's Vineyard. In June 2021, the company became the victim of a ransomware attack that impacted operations. Tweets from the [Steamship Authority's](#) official account mentioned that customers traveling by ferry could expect some delays to services.

The ransomware didn't impact important technology used to ensure the safety of ferry transport services, but the constant worry within the sector is that safety compromise could happen one day. A ransomware attack could feasibly impact radar technology for maritime services or air traffic control for aviation, posing significant safety threats to passengers.

### **Merseyrail: April 2021**

Merseyrail operates an urban rail network for customers in the Liverpool area of England. In April 2021, the disclosure of [this attack](#) was made public by the perpetrators, who emailed journalists and employees from a privileged Office 365 email account within the Merseyrail network.

According to the email's subject line, the ransomware strain in question was LockBit. This type of ransomware rapidly propagates through networks and infects multiple other host systems from an initial point of compromise. It appears the Merseyrail attack began with compromising a single privileged account credential either through phishing or brute force methods.

### **OmniTRAX: January 2021**

OmniTRAX operates short rail line services in Colorado. In January 2021, reports emerged in the media that the company was [successfully targeted](#) by the Conti ransomware gang. The attack used a double extortion tactic to first exfiltrate data and then lock systems down before demanding a ransom payment.

OmniTRAX decided to take the advice of federal bodies such as the CISA and not pay the ransom. The result was that approximately 70 gigabytes of internal OmniTRAX documents were leaked online. This incident did not result in any disruptions to OmniTRAX operations.

### **Forward Air: December 2020**

Forward Air is a trucking and freight logistics company that provides nationwide coverage for ground transportation in the United States. In December 2020, the company was hit by a [ransomware attack](#) by a new strain of ransomware dubbed Hades. The unknown group behind Hades ransomware has targeted several companies using common initial attack vectors such as malware delivered via Google Chrome updates and credential access via VPN connections.



Forward Air did not pay the undoubtedly hefty ransom demanded to return access to compromised systems. The company's response was to act swiftly and shut down all its IT systems to contain the attack. The knock-on effects on Forward Air's operations were so severe that responding to and recovering from the incident cost an estimated [\\$7.5 million](#). Truck drivers couldn't access important documents to get clearance for goods through US customs and backlogs ensued.

### STM Montreal: October 2020

An October [2020 ransomware attack](#) on Montreal's STM public transport system resulted in a ransom demand of \$2.8 million. Montreal STM decided not to pay the ransom and instead focused on rapid response to the attack. According to a [public statement](#) in the wake of a full cyber incident investigation, the organization was able to restore 600 critical servers that were affected by the ransomware attack.

The cost of restoring the servers was estimated at close to \$2 million. Bus and Metro services in Montreal weren't impacted by the attack, although the STM website stayed offline for several days. Personal information about 24 employees and 72 customers were apparently accessed in the attack, but the sensitivity of that information was limited to names and email addresses.

### Suggestions for Transportation Companies

The following are some best practices for dealing with the pervasive threat of ransomware:

- Understand that prevention is easier and cheaper than the cure. This means investing in resources and solutions that specifically help combat ransomware before it can cause devastating effects on your IT operations. Advanced email security solutions can protect against suspicious emails while investments in staff awareness and training can reinforce safer cybersecurity practices.
- Get the basics right. Investing in basic technical measures, such as network segmentation, endpoint defense solutions, and patch management software can go a long way towards stopping ransomware attacks in their tracks.
- Have a backup and recovery strategy. The critical nature of transport services calls for a dedicated strategy to rapidly restore encrypted data and systems. If ransomware locks down critical servers and data, it's vital to be able to restore these systems using saved images, cloud infrastructure, and data backup sources.
- Respond swiftly. The impact of several of the ransomware attacks was minimized due to a swift response strategy conducted by the victims. Specialized incident response teams can prove an invaluable investment during a time of crisis. Being able to contain an attack at speed and limit its damage on crucial transport services reduces the consequences of successful attacks.





# Hospitality



Ransomware attacks pose serious cybersecurity risks for companies in the hospitality industry, which is a broad sector that includes hotels, tourism agencies, restaurants, and bars. Common to these distinct businesses are direct interactions with paying customers who regularly use credit/debit cards for transactions.

The need to collect sensitive data and the proximity of these businesses to paying customers makes the hospitality sector a prime ransomware target. Whether by causing operational disruption or exfiltrating sensitive data, threat actors know that successful attacks can wreak havoc on victim organizations. This article explores the state of ransomware in hospitality.

## Ransomware Dangers in Hospitality

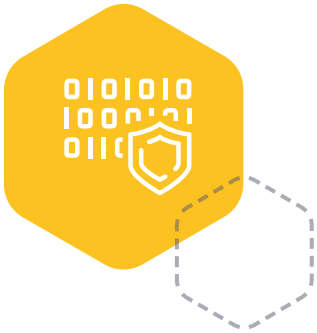
Hospitality companies depend heavily on digital technologies to handle business-critical operations, including processing payments, accounting, and reserving tables/rooms. In hotels, this use of technology even extends to providing key-card access to rooms using computer-controlled technology.

The computer systems used in hospitality, such as POS systems, and the networks they are connected to are vulnerable to ransomware attacks. Threat actors often regard hospitality companies as easy prey for locking down systems with malware that ultimately leads to large ransom payments.

The hospitality sector is still reeling from the after-effects of the pandemic; hotels, bars, and restaurants saw steep decreases in customers almost overnight lasting several months. A serious breach of customer data, costing an average of [\\$4.2 million per incident](#), could tip any hospitality company over the edge.

## Recent Ransomware Attacks on Hospitality Businesses

The potential damage of ransomware in hospitality was first noted in the mainstream news back in 2017 when luxury Austrian hotel Romantik Seehotel Jagwir became the victim of an [attack](#) that targeted its key card systems. Depending on the location of guests at the time, many were either locked out of or into their rooms for up to ten hours. Several ransomware incidents in recent times have targeted hospitality companies and made media headlines: here are four of them worth learning from.



### Techotel, June 2021

In June 2021, an interesting ransomware incident hit hotel management software provider Techotel. The Denmark-based company provides IT solutions for hotels, inns, conference centers, hotel chains, and restaurants. The ransomware attack impacted the ability to conduct normal check-in and check-out operations at hundreds of hotels.

The intrigue here stems from the fact that Techotel essentially [live-blogged](#) its response to the incident, including details of ransom negotiations with the perpetrators. With 250 servers and their data locked down, the company tried to pay the ransom via bank transfer, which was refused because the perpetrators wanted the anonymity provided by cryptocurrency.

According to Techotel CEO Klaus Ahrenkilde, the size of his company left no choice but to pay: "We cannot break the encryption. We are a small company, with hundreds of hotels affected." Shockingly, it still took up to a month for the restoration of data to be complete and for Techotel's software to become functional again.

### Epsilon Red, May 2021

Epsilon Red is not the name of a hospitality organization targeted by ransomware—it's a new ransomware strain uncovered by investigating a cyber attack on an unnamed hotel. According to the [investigation](#), this new ransomware strain resulted in a payment of 4.29 Bitcoin on May 15th, 2021, which at the time was worth over \$200,000.

The discovery of any new ransomware strain is always a cause for concern. This attack used Microsoft Exchange servers as an initial entry point before executing a PowerShell script to set the foundation for the final payload that infected multiple systems. It's worth keeping a close eye on news headlines over the coming months for further incidents involving this dangerous new ransomware strain.





### Edward Don, June 2021

Edward Don is a leading distributor of food service equipment and supplies. This equipment includes kitchen supplies, bar supplies, and dinnerware that many hospitality companies depend on to service customers. The [ransomware attack](#) on Edward Don impacted phone and email systems, which resulted in employees having to use personal Gmail accounts to communicate with partners and vendors about urgent orders.

The Edward Don attack demonstrates another way that ransomware can severely impact hospitality businesses without directly hitting their IT systems. A new restaurant depending on an urgent delivery from Edward Don may not have even been able to open their doors if this attack delayed their order. As with many other sectors, the supply chain is also a point of vulnerability worth considering in your operational and IT security plans.

### CWT, July 2020

US-based travel management company Carlson Wagonlit Travel (CWT) became the victim of a devastating [ransomware attack](#) in July 2020 that rendered up to 30,000 computers unusable.

The ransom note indicated that the ransomware was Ragnar Locker, which affects devices running Windows, the world's most widely used operating system. Ragnar Locker uses a double extortion technique wherein attackers exfiltrate data and threaten to publish it on the dark web if the victim doesn't pay up. The Ragnar Locker file is only 55 kilobytes in size, yet its impact is vicious. News reports in the aftermath of this attack indicated that [CWT paid \\$4.5 million](#) to get encrypted systems back and avoid having stolen data published online.



## Suggestions for Hospitality Companies

Taking a reactive approach to ransomware is a risk that hospitality companies can't afford to take. Aside from the recovery costs, the direct reputational impact of a customer data breach serves to influence customers to seek competing firms that they may deem as less risky. Here are some ransomware prevention tips for hospitality companies to consider:

- **Adopt a security-first culture among all your staff** that educates them on basic cybersecurity best practices, spotting different types of attacks, and reporting incidents.
- **Make sure everyone is aware of the dangers of phishing emails**, which often provide an entry point for ransomware attacks by fooling recipients into clicking links or downloading files. Protect against these phishing emails using dedicated security solutions that can filter them out.
- **Update all software and operating systems in a timely manner**, including POS software. Many ransomware attacks start by exploiting unpatched software vulnerabilities, so proper patch management is a quick win in your defenses.
- **Implement prudent access controls** so that employees don't get too much access to different information systems. The principle of least privileges means giving access to only those assets strictly needed to perform job duties. To use an example, don't give your barman admin access to a POS system.
- **Be wary of IoT threats.** An increasing number of hospitality businesses use Internet-connected devices, such as smart televisions and coffee makers in hotels, and temperature sensors in commercial kitchens.
- **Secure these devices properly by not using default passwords** and by applying updates when they are available. A recent cybersecurity conference featured a presentation by a security researcher easily hacking a capsule hotel by exploiting IoT flaws.
- **A comprehensive data backup and business continuity strategy is as much a preventative defense as it is reactive.** If you can easily restore your data and swiftly resume critical business operations by temporarily using cloud infrastructure, you're already well-prepared for successful attacks when they occur. For smaller hospitality companies, engaging with a security services provider can provide the expertise needed to develop a robust business continuity plan.

# Mining



Whether by disrupting mining operations or interfering with a time-sensitive supply chains for producers of such items as industrial equipment, lithium batteries and more, threat actors believe ransomware can result in large payouts in the mining sector. This article looks at the state of ransomware in mining and highlights some recent attacks.

## Ransomware in Mining Overview

The global mining industry was valued at about \$1.64 Trillion in 2020 and is forecast to grow to \$2.43 Trillion by 2025. Asia accounts for most of the mining revenue, at about 71% of the global total. In recent years, companies in the mining industry have embraced new technologies that allow for automated extraction and movement of materials as well as Industrial Control Systems technologies to monitor mining sites and provide that data back to company headquarters in real-time. This explosion of technology, the high value of the minerals extracted, the need to communicate with remote locations and the significant negative impacts to the global economy should anything go wrong make this industry a focus of threat actors.

## Ransomware Incidents in Mining

### Gyrodata, January 2021

Gyrodata is a US-based company that supplies drilling tools to oil companies around the globe as part of their respective exploration and extraction activities. Media reports state that threat actors were able to access Gyrodata's IT systems in mid-January 2021 and remained in the environment until late February 2021. Gyrodata [reported the attack](#) in a public announcement in April 2021, stating that a large amount of their employees' personal data was compromised. This data included employee social security numbers, names, addresses passport details, W-2 tax forms and more. The company stated that their servers were hit by a file-encrypting malware from the ransomware group known as [REvil](#). It is not known whether or not Gyrodata paid a ransom to get access to their data.

### Rio Tinto Group, BHP Billiton Ltd and Fortescue Metal Groups, April 2010

Media reports stated that Chinese threat actors attacked these three firms with the intention of stealing intellectual property. It is believed the threat actors wanted to acquire the information in order to conduct corporate espionage operations.



### **BHP Billiton, February 2011**

A second large attack on the company took place less than a year after the first one and was again believed to be conducted by threat actors operating from China. The CEO of BHP Billiton stated that he believed the attack was conducted so that certain nation-states and competitors of the company could gain access to pricing details for a select number of commodities.

### **Australian Federal Parliament, April 2011**

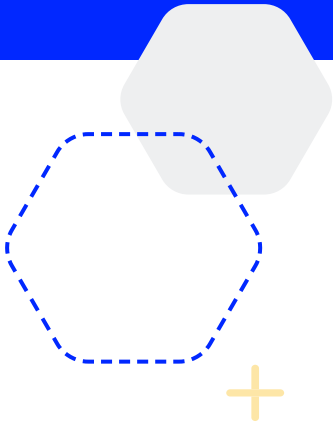
Chinese hackers gained access to a number of email accounts of the Australian Federal Parliament officials operating in China. These emails were believed to contain conversations between the federal officials and executives at several of Australia's leading mining companies with operations in China.

## **Suggestions For Mining Companies**

From operational disruptions to stealing sensitive data, ransomware attacks in the mining industry highlight the risks for all businesses in this industry. Stopping ransomware in its tracks helps to avoid costly recovery and containment measures. Here are some actions mining companies can take today to thwart ransomware attacks.

- **Use Anti-Phishing Defenses:** Phishing campaigns are a popular vector for threat actors to gain access to a company's IT infrastructure. By impersonating trusted individuals, hackers can target employees with phony emails or social media messages that get them to disclose passwords or to download malware. Anti-phishing defenses can include the use of advanced self-learning email filters that block, flag, or quarantine suspicious emails so that they don't reach target employees. Another anti-phishing defense is to conduct [simulated phishing tests](#) to help employees get better at recognizing phishing attacks. Simulated phishing may be particularly helpful for social media phishing.
- **Secure IoT devices:** There has been an explosion of IoT device usage in the mining industry in recent years, from using drones to survey extraction locations, deploying automated extraction and transportation equipment, and tracking material movement. IoT devices are notoriously insecure, as are the networks that connect them back to the company's core infrastructure. It is critical that mining organizations employing these new technologies are working with security firms to understand, implement and monitor for security issues within the IoT deployment.
- **Leverage Artificial Intelligence:** Artificial intelligence continues to evolve and play an increasingly important role in cybersecurity. AI can be used within several types of cybersecurity tools to detect and prevent ransomware. From email filters that leverage machine learning to intelligent user monitoring, AI can help to thwart ransomware before the dreaded encryption or data exfiltration events that cause the bulk of the damage from these attacks.

# Media & Entertainment



Whether by disrupting important customer-facing services or blocking access to important data, threat actors believe ransomware can result in large payouts in the media and entertainment sector. This belief is motivated by assuming that companies will pay up to avoid any reputational damage or a data leak. This article looks at the state of ransomware in media and entertainment and highlights some recent attacks.

## Ransomware in Media and Entertainment: Overview

In the United States, the media and entertainment industry is worth [\\$717 billion](#). A 2018 survey found that 51 percent of media and entertainment companies experienced three or more cyber attacks over a 12-month period. It is clear that companies in the sector are in the sights of prying hackers looking for the next big payday.

The current wave of double extortion attacks puts businesses within media and entertainment at risk. These attacks exfiltrate a company's prized data before encrypting systems. The perpetrators threaten to release the data on the dark web if the victim company doesn't pay the demanded ransom.

Consider the fact that the average cost to produce a major movie is [\\$65 million](#). Threat actors know that movie studios (and most other media and entertainment businesses) prize their content above all else.

Competent hackers can target the digital infrastructure of a movie studio and access files for an upcoming movie in a ransomware attack. Having a movie published on the dark web in advance of its release date would be a disaster, so most studios would be willing to engage with ransom demands in this scenario.

If content is the prized asset in media and entertainment, there are other ways to disrupt it aside from exfiltrating files. For example, a successful ransomware attack can cause an operational outage that prevents television stations from broadcasting or newspaper publishers from publishing. The risks are clear, and the volume of attacks continues to rise.





Having a movie published on the dark web in advance of its release date would be a disaster, so most studios would be willing to engage with ransom demands in this scenario.

## Ransomware Incidents in Media and Entertainment

### Cox Media, June 2021

Cox Media Group broadcasts to radio and television stations affiliated with major US networks, including CBS, NBC, and Fox. In June 2021, several Cox Media stations were disrupted from broadcasting due to a [ransomware attack](#). Details quickly emerged that this attack directly targeted Cox Media live streams and didn't impact any other aspect of the company's digital infrastructure.

The interconnected nature of media and entertainment meant that other companies broadcasting Cox Media stations were impacted by this attack. Hulu, the popular streaming provider, faced [complaints from disgruntled customers on Twitter](#) about unavailable television streams. Interestingly, Cox Media Group opted to remain quiet about any specific details of this attack, so it remains unknown who the perpetrators were and whether any ransom was paid.

### Nine Network, Australia March 2021

Nine Network is one of the five main free-to-air television networks in Australia. In March 2021, a [cyber attack](#) targeted the availability of [Channel Nine](#), which has the highest share of television ratings in Australia. The attack disrupted live broadcasts of Channel Nine and impacted its online news website.

Nine Network's parent company also owns The Sydney Morning Herald and The Age newspapers, but it appears neither of these business lines was impacted. Popular Australian breakfast television show Weekend Today could not air because of the attack. An official company statement said the disruption primarily affected the broadcasting and corporate units of the business.

As with the Fox Media Group incident, scant details have emerged of the ransomware variant, any ransom demand, or the group behind the attack.

### CD Projekt Red, February 2021

CD Projekt Red is a Polish video game developer best known for creating The Witcher and Cyberpunk 2077 video games. A [Tweet posted by the company](#) in February 2021 confirmed that CD Projekt Red became the latest victim of a [ransomware attack](#) in the media and entertainment industry. Accompanying the tweet was a ransom note indicating that the threat actors had compromised the source code of the hugely popular Cyberpunk 2077 game and for an unreleased version of The Witcher 3.

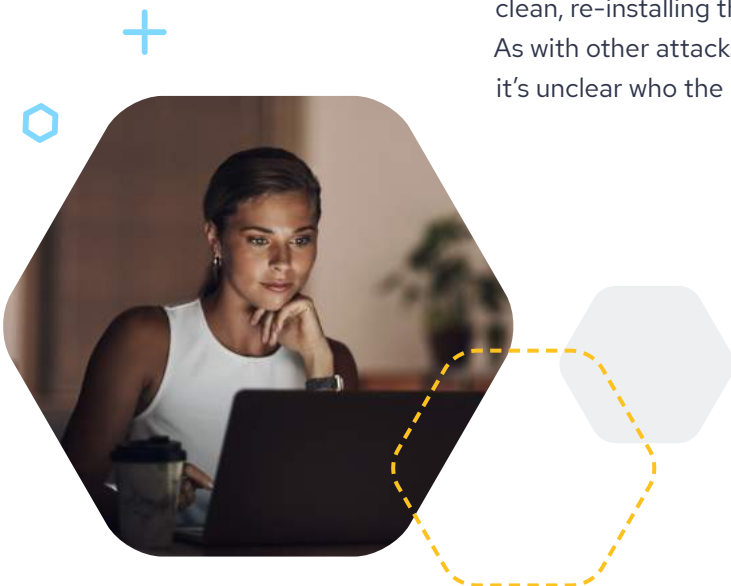
Aside from accessing sensitive source code, the hackers also managed to encrypt servers belonging to CD Projekt Red. In an official company statement attached to the original Tweet, CD Projekt Red said that its backups remained intact and that it was in the process of restoring its data while securing infrastructure.

CD Projekt Red specifically mentioned it was unwilling to engage with any ransom demands due to the likelihood of sensitive data being published regardless of whether they paid up. This prediction came through when it was revealed that hackers [began publishing](#) sensitive information about employees and contractors four months after the attack.

### Funke Media Group, December 2020

Funke Media Group is the third-largest newspaper and magazine publisher in Germany. In December 2020, a [ransomware attack](#) halted publishing at Funke's major printing houses resulting in an inability to publish print editions of several of its popular daily newspapers. Containing the incident required switching off the entire production systems and technologies for newspaper printing to prevent further damage.

This was a large-scale ransomware incident that encrypted up to 6,000 employee laptops and other endpoints. The recovery operation involved wiping the laptops clean, re-installing the operating system and apps, and returning them to employees. As with other attacks targeting media and entertainment companies in recent times, it's unclear who the perpetrators were.





## Suggestions For Media & Entertainment Companies

From operational disruptions to stealing sensitive data, the recent ransomware attacks in the media and entertainment industry highlight the risks for all businesses in this industry. Stopping ransomware in its tracks helps to avoid costly recovery and containment measures in addition to the types of severe operational disruptions that hit Channel Nine, Funke Group, and Cox Media. Here are some actions media and entertainment companies can take today to thwart ransomware attacks.



**Use Anti-Phishing Defenses:** Phishing campaigns are a popular vector for threat actors to gain access to a company's IT infrastructure. By impersonating trusted individuals, hackers can target employees with phony emails or social media messages that get them to disclose passwords or to download malware. Media and entertainment employees often interact heavily with social media, which is becoming a more widespread medium for phishing campaigns. Anti-phishing defenses can include the use of advanced self-learning email filters that block, flag, or quarantine suspicious emails so that they don't reach target employees. Another anti-phishing defense is to conduct simulated phishing tests to help employees get better at recognizing phishing attacks. Simulated phishing may be particularly helpful for social media phishing.



**Manage Access:** Large numbers of employees play a part in producing any movie or television show, running a live broadcast, developing video games, and printing newspapers. Since content is the most valuable asset in this industry, the intersection between large numbers of employees and sensitive content requires strong access management. Media and entertainment companies must implement identity and access management best practices, including privileged access management, least privilege access, multifactor authentication, and access lifecycle management.



**Leverage Artificial Intelligence:** Artificial intelligence continues to evolve and play an increasingly important role in cybersecurity. AI can be used within several types of cybersecurity tools to detect and prevent ransomware. From email filters that leverage machine learning to intelligent user monitoring, AI can help to thwart ransomware before the dreaded encryption or data exfiltration events that cause the bulk of the damage from these attacks.

# Energy



Businesses in the energy sector produce, extract, sell, and supply various sources of energy. These energy sources include oil and gas reserves, nuclear energy, and renewable energy for fuel and to generate electricity. The critical nature of the energy sector exposes both energy companies and wider society to severe risks resulting from cyber attacks. This article focuses on the specific threat of ransomware in the energy sector.

## High-Profile Ransomware Attacks on Energy Companies

Due to the far-reaching consequences of cyber attacks on the energy sector, the disruptions caused often make global media headlines. Here are examples of recent high-profile ransomware attacks targeting energy companies:

### Oiltanking GmbH Group and Mabanft Group

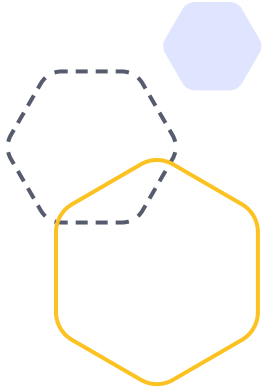
These two Germany-based companies confirmed on the same day that both had been hit by a successful ransomware attack. Both companies are involved in the storage and supplying of oil and other materials to downstream companies such as Shell. The attackers appear to have targeted the loading and unloading systems of the Oiltanking GmbH Group to reduce the company's ability to transfer oil products. Mabanft "declared force majeure for the majority of its inland supply activities in Germany" and immediately began executing on its contingency plans to help minimize the impact of the attack. Later reports indicated that only a small number of filling stations (~200) were adversely affected by limited gasoline availability issues resulting from the attack.

Security researchers believe that the attack was carried out by the ransomware group known as [Black Cat](#).

### Colonial Pipeline

It's impossible to start anywhere else but with one of the most disruptive [ransomware attacks](#) ever on US critical infrastructure. The Colonial Pipeline supplies gas and jet fuel from Texas to its terminus at the Port of New York and New Jersey. Stretching over 5,500 miles, this pipeline plays a prominent role in heating homes, refueling cars, and powering airplanes.

The ransomware attack on the Colonial Pipeline was conducted by the [DarkSide](#) ransomware gang. The gang targeted the billing system used by Colonial Pipeline. Upon seeing an on-screen ransom demand, an employee alerted his superiors who made the decision to shut the pipeline down completely.



The Colonial Pipeline supplies around 45 percent of the East Coast's fuel needs. The disruption caused by this ransomware attack resulted in a [\\$4.4 million ransom](#) payment made to the DarkSide of which the FBI helped recover a significant proportion. Aside from that direct cost, a large knock-on effect of shutting the pipeline down was the gasoline shortages resulting from panicked motorists queuing up to fill up their tanks in light of the news.

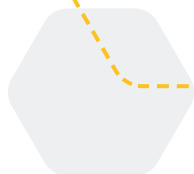
The Colonial Pipeline incident serves as a stark warning sign about the vulnerability of the energy sector to ransomware attacks. This incident did not even manage to breach any operational systems that directly control the pipeline, yet it still caused untold havoc and made global headlines. As threat actors become more sophisticated in their techniques and ambitious in their targets, other large-scale energy disruptions will happen to any company that neglects cybersecurity.

### **Volue ASA**

Shortly before the Colonial Pipeline incident, a [ransomware attack](#) also struck Volue ASA. The Norwegian company, which provides energy technology, was targeted by the Ryuk ransomware family.

The attack on Volue ASA impacted files, databases, and applications. Like other Ryuk attacks, this incident did not exfiltrate data and demanded a ransom to prevent the data from being published on the dark web. The method of attack was to encrypt files and make them unreadable.

A website statement made by Volue CEO Trond Straume outlined how "no ransom has been paid to the group behind the attack." It appears this was intended as a statement of defiance against caving into ransom demands. The worst consequences appear to have been disruptions to Volue's applications and employee workstations.



## COPEL

COPEL is a state-owned Brazilian energy utility organization. In a February 2021 attack, the same DarkSide gang responsible for the Colonial Pipeline incident claimed to have exfiltrated over 1,000 gigabytes of data from COPEL's systems as part of a [ransomware attack](#). According to DarkSide, this data included clear-text passwords, network maps, and employee personal data.

The COPEL incident struck at the same time as another major state-owned Brazilian electric utility company named Electrobras also disclosed a [ransomware attack](#). It remains unclear whether Darkside was involved in both incidents. A statement outlining the response to the COPEL attack mentioned that it was necessary to suspend the operation of COPEL's computerized environment, which presumably was a costly outcome for the company.

## Pemex

Pemex is a Mexican state oil company that was targeted in a [ransomware attack](#) by the Ryuk ransomware family back in November 2019. This incident came at a time when Pemex was already struggling to battle a declining credit rating, huge debts, and slowdowns in oil production.

Luckily for Pemex, it appears the cybersecurity defenses in place enabled a swift response to this attack. The critical operational functions of oil storage and production avoided any impact. Furthermore, the ransomware was contained to less than 5 percent of the organization's computers.

The Pemex incident may have caused more disruption than the company disclosed. An anonymous employee informed [Reuters](#) that the servers crashed and people weren't able to do their daily work.

## Norsk Hydro

Norsk Hydro is a Norwegian company focused on renewable energy. In March 2019, a [serious ransomware attack](#) rapidly propagated through the company's global network of 3,000 servers and thousands of workstations. The attack even stalled production in manufacturing facilities belonging to Norsk Hydro.

Upon seeing ransom demands to remove the encryption from affected devices, the company decided not to engage with these demands and rebuild everything from scratch. Recovering from an attack of this scale required relying on pen and paper to track many important business aspects, including orders, finances, and manufacturing processes.

The total cost of the attack on Norsk Hydro added up to \$70 million, however, the size of the company is such that it could absorb this type of cost. More pertinently, the aftermath of the attack resulted in a complete attitude shift that put cyber risk at the top of the company's [strategic agenda](#).

## Suggestions for Energy Companies

Given the devastating impact of successful ransomware attacks that result in even short outages and disruptions to energy supplies, it's critical to implement cybersecurity strategies that prevent such incidents.



**Address Physical Security:** Physical security controls should cover both information technology (IT) and operational technology (OT), including industrial control systems and data centers. The interdependencies between the virtual and the physical in the energy sector require strong physical security controls. Physical security controls can include sensors and alarms that detect intrusions, guards posted in visible locations to deter people from trying to access a restricted location, and barriers such as high walls, tamper-resistant devices, and hard-to-pick locks.



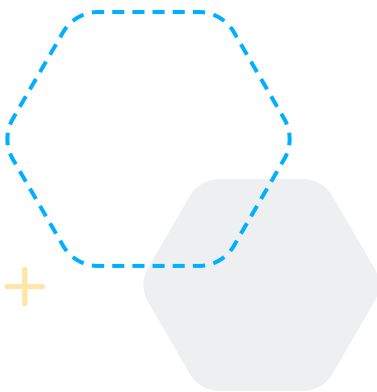
**Establish an OT Security Policy:** Operational technology (OT) uses hardware and software to monitor and control the physical devices and environment. OT technology is more interconnected than ever with the rest of the network thanks to the proliferation of the Internet of Things. It's critical that businesses address this increased interconnectivity with a dedicated OT security policy that covers fundamental security practices, including patching, changing default passwords, asset visibility, and incident response.



**Use Robust Threat Intelligence:** Companies in the energy sector should look to combine both tactical and strategic threat intelligence. Strategic intelligence is more proactive in nature; it focuses on industry-specific high-level overviews of the current threat landscape. Ransomware attack groups operate highly sophisticated operations, so it's critical to have skilled analysts who use robust threat intelligence to identify current trends and threats and help build mechanisms to defend against those threats.



**Combat Phishing:** Phishing emails remain a significant initial attack vector for ransomware. Cybercriminals target victims with well-crafted emails that dupe them into revealing login credentials to systems or downloading malicious files. From this initial attack vector, the perpetrators infiltrate the network and install malicious software on as many systems as possible. The fight against phishing begins with a dedicated email security platform. Ideally, energy companies should deploy a solution that has AI-driven, self-learning capabilities to help detect and flag suspicious emails. By stopping phishing campaigns with email security, you can prevent the account takeover or credential harvesting incidents from which ransomware often proliferates.



# Telecommunications



The fact that telecom companies facilitate communication on a global scale makes them a prime target for sophisticated ransomware attacks that take services offline. Both nation-sponsored and for-profit ransomware gangs have huge incentives to target companies providing these services. This article looks at the state of ransomware in telecommunications.

## The Perfect Storm for Ransomware in Telecommunications

The critical nature of services provided within the telecommunications sector is just one aspect of a perfect storm for ransomware attacks. Another feature that marks telecom providers and operators as attractive targets is the volume of customer data they store in their systems. Threat actors specializing in ransomware can encrypt multiple IT assets at target organizations and demand large payments for the keys to unlock those assets.

In 2021 alone, it's been predicted that businesses globally will fall victim to a [ransomware attack every 11 seconds](#). The total cost of ransomware is estimated at \$20 billion in 2021. These costs stem from breaches of sensitive data, ransomware recovery, and legal fees.

## Recent Ransomware Attacks on Telecommunications Companies


There has been a spate of ransomware attacks in the telecommunications sector within the last couple of years. Common to several of these attacks is a double extortion ransom demand with pre-encryption data exfiltration. It's clear that threat actors regard this sector as a lucrative target in which it's optimal to leave victims with little option but to pay.

### Corporacion Nacional de Telecomunicacione, July 2021


Corporacion Nacional de Telecomunicacione (CNT) is a state-run telecommunications corporation based in Ecuador. CNT's services span the full gamut of modern telecom services, including fixed-line phone service, mobile, satellite television, and internet. A notice in mid-July informed customers that payment portals and customer care were no longer accessible due to a cyber attack. It's believed the group behind the attack on CNT was RansomEXX. The ransom note that [BleepingComputer](#) gained access to mentioned 190 gigabytes of compromised data that RansomEXX threatened to publish if their ransom demand remained unmet. Screenshots of the stolen data indicated it was mostly contracts and support logs.







Threat actors specializing in ransomware can encrypt multiple IT assets at target organizations and demand large payments for the keys to unlock those assets.



RansomEXX has previously targeted several other large organizations in South America. Often, they'll use purchased stolen credentials and exploit poor password hygiene to gain access to a network, move laterally, and then encrypt multiple servers and workstations with malware. The gang even recently developed a Linux version of their ransomware to ensure they can maximally impact victim networks.

### **Schepisi Communications, May 2021**

Schepisi Communications is a telecom provider that provides services to high-level enterprise customers on behalf of the Australian telecommunications giant Telstra. In May 2021, a dark web disclosure identified Schepisi Communications as a [ransomware victim](#) with a threat to publish valuable company documents if the ransom wasn't paid.

The dark web leak site went into further detail with screenshots of compromised phone numbers, customer names, SIM codes, and IMEI numbers. A timer was set at 240 hours before the perpetrators threatened to start releasing stolen data. The group behind the Schepisi incident was Avaddon, and they target both Windows and Linux systems.

An interesting feature of Avaddon ransomware attacks is a concerted effort to delete backups and disable any recovery options for victims. It's clear Avaddon wants to maximize the chance of receiving payment by giving victims no option to restore data and infrastructure from backups.

### **Telecom Argentina, July 2020**

Telecom Argentina is one of the country's largest internet service providers. In July 2020, Telecom Argentina revealed details of a serious [ransomware attack](#) resulting in a ransom demand of \$7.5 million to decrypt infected over 18,000 systems. The attack focused on the company's call center and targeted workstations used by call center employees.

Stolen admin credentials provided the initial entry point and means by which the hackers could infect so many systems. It's heavily rumored that phishing emails were used to dupe privileged users into revealing their credentials. Ultimately, the Telecom Argentina attack didn't disrupt critical Internet services for customers, and the IT team was able to contain the damage.

## Orange, July 2020

Orange is a French telecommunications company and one of Europe's largest mobile phone operators. In July 2020, [Orange confirmed](#) a successful ransomware attack that compromised data belonging to the company's enterprise customers. Enterprise solutions offered by Orange include remote support, virtual workstations, and cloud backups.

The [Nefilim ransomware](#) family was behind this particular attack. Nefilim targets vulnerabilities and poor security practices in remote access technology. Once inside the network, the operators of these attacks almost always steal data before locking down systems with AES-128 encryption.

The exfiltrated data from twenty of Orange's enterprise clients in this incident included emails and intellectual property. According to a statement in the incident's immediate aftermath, "Affected customers have already been informed by Orange teams."

## Suggestions for Telecommunications Companies

Phishing emails remain a significant initial attack vector for ransomware incidents. By either targeting specific individuals within an organization or conducting generic phishing campaigns, hackers write emails that convince targets to disclose credentials, click suspicious links, or download malicious attachments.

The Telecom Argentina attack demonstrated that phishing is a problem that extends to the telecommunications sector. Phishing campaigns can deliver a quick return on investment for hackers because they are not technically challenging to conduct. Here are some ways to combat this problem and prevent future attacks whether you're in telecommunications or any other sector:

- Teach users how to spot the signs of a phishing attack and encourage them to report suspicious emails.
- Conduct simulated phishing attacks to gauge the current level of awareness around phishing emails among your workforce.
- Use advanced email security solutions that can leverage artificial intelligence to filter out, flag, or quarantine phishing emails.
- Clearly establish a corporate security policy specifying appropriate user actions around not opening email attachments from untrusted sources or not disclosing login credentials via email.



# Agriculture



Whether by disrupting food production or interfering with a time-sensitive distribution supply chain, threat actors believe ransomware can result in large payouts in the agriculture sector. This article looks at the state of ransomware in agriculture and highlights some recent attacks.

## Ransomware in Agriculture Overview

Agriculture, food and related industries contributed [\\$1.1 Trillion to the US GDP in 2019](#), a 5.2% share. The threat has become so significant that the [FBI just released a warning](#) to agriculture companies to be on the lookout for ransomware attacks and to take steps now to help prevent them.

## Ransomware Incidents in Agriculture

### HP Hood Dairy, March 2022

HP Hood Dairy is best known as the owner of the Lactaid brand of lactose-free milk. Reports suggest that a [ransomware attack](#) hit the company in March 2022. While details of the attack are scarce, the victim did state that they took all of their production facilities offline “out of an abundance of caution.” It isn’t known if any sensitive data was stolen, but the production shutdown resulted in a nationwide shortage of the Lactaid product for a number of weeks.

### JBS, June 2021

Based in Brazil, JBS is the world’s largest meat processor and has a large number of facilities in the US. The attack resulted in all [nine US-based facilities](#) being shut down, as their IT systems were incapable of operating due to the ransomware. The downstream effects of the shutdown were devastating to downstream customers like grocery stores and restaurants, who were themselves struggling to re-open after COVID shutdowns.

JBS leadership decided to pay an \$11M ransom in order to restore operations. Fortunately, the criminals at the [REvil](#) ransomware gang upheld their end of the bargain and provided the necessary decryption keys.

### Unidentified US farm, January 2021

An unidentified farm in the US was hit with a [ransomware attack](#) in early 2021 after threat actors were able to get into the farm’s internal network by using a set of stolen admin credentials. The FBI reported that the farm paid a \$9 million ransom in order to be able to restart their operations.

## Unidentified US-based international food & agriculture business, December 2020

A ransomware group known as the OnePercent Group was successful in deploying a ransomware attack against a US-based agricultural company. The group is notorious for deploying Cobalt Strike ransomware after compromising user credentials as part of a phishing attack. After exfiltrating the customer's data and encrypting the company's databases, the [OnePercent Group](#) demanded a \$40 million ransom be paid. Fortunately, the company had a solid backup and recovery plan in place and were able to restore the stolen data without having to pay the ransom.

### Suggestions for Agriculture Companies

From operational disruptions to stealing sensitive data, the recent ransomware attacks in the agriculture industry highlight the risks for all businesses in this industry. Stopping ransomware in its tracks helps to avoid costly recovery and containment measures. Here are some actions media and entertainment companies can take today to thwart ransomware attacks.

- **Use Anti-Phishing Defenses:** Phishing campaigns are a popular vector for threat actors to gain access to a company's IT infrastructure. By impersonating trusted individuals, hackers can target employees with phony emails or social media messages that get them to disclose passwords or download malware. Anti-phishing defenses can include the use of advanced self-learning email filters that block, flag, or quarantine suspicious emails so that they don't reach target employees. Another anti-phishing defense is to conduct [simulated phishing tests](#) to help employees get better at recognizing phishing attacks. Simulated phishing may be particularly helpful for social media phishing.
- **Secure IoT devices:** There has been an explosion of IoT device usage in the agriculture industry in recent years, from using drones to survey fields, using sensors to understand real-time soil conditions to putting devices on livestock to track their movements to better understand their health. IoT devices are notoriously insecure, as are the networks that connect them back to the company's core infrastructure. It is critical that agriculture organizations employing these new technologies are working with security firms to understand, implement and monitor for security issues within the IoT deployment.
- **Leverage Artificial Intelligence:** Artificial intelligence continues to evolve and play an increasingly important role in cybersecurity. AI can be used within several types of cybersecurity tools to detect and prevent ransomware. From email filters that leverage machine learning to intelligent user monitoring, AI can help to thwart ransomware before the dreaded encryption or data exfiltration events that cause the bulk of the damage from these attacks.



# IT Services



An IT service provider's operations are tightly intertwined with the networks of many businesses simultaneously. Ransomware attacks on IT service providers have the potential to disrupt operations not only for the direct target organization, but for all its downstream customers too. This article looks at the state of ransomware in IT services by focusing on recent attacks and suggested countermeasures to combat this pervasive threat.

## Ransomware: An Increasingly Expensive Problem

More threat actors continue to enter the fray and target organizations with malware that locks their systems and data down via encryption. Access to locked-down assets is not returned until a specified ransom payment is made with cryptocurrency.

The perception among cybercriminals is that ransomware attacks have a high probability of monetary gain. Recent statistics back up this perception—the average ransomware payment [increased by 82 percent to \\$570,000 in the first half of 2021](#).

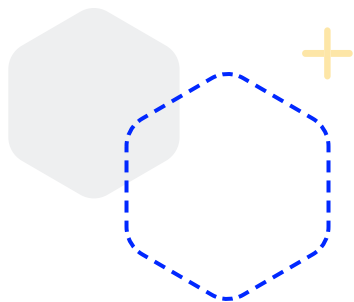
Ransomware attacks on IT services can be particularly harmful due to their downstream impact. Often, the customers of IT services are small and medium-sized businesses that lack in-house capabilities for business functions and technologies, such as disaster recovery or detection and response. IT services providers regularly have trusted access to customer networks, and hackers increasingly recognize just how lucrative it can be to conduct a successful ransomware attack on these companies.

## Recent Ransomware Attacks on IT Service Providers

### Accenture, August 2021

Accenture provides a range of IT consulting and services generating billions of dollars in revenue in over 120 countries. In August 2021, news of a [ransomware incident affecting Accenture](#) emerged. The company was hit by LockBit ransomware, which can encrypt thousands of files in seconds by exploiting protocols and tools like PowerShell.

A CNBC reporter originally disclosed the attack, which Accenture later confirmed. The multi-billion dollar company downplayed the impact of the ransomware incident, saying, "There was no impact on Accenture's operations, or on our clients' systems." These public statements seem to contradict the threat actors' claims that they stole six terabytes of data and compromised 2,500 computers.



### **Kaseya, July 2021**

One of 2021's biggest [ransomware incidents](#) struck the managed IT services sector in July. Kaseya is a vendor providing IT management software for managed services providers (MSPs). Threat actors from the [REvil](#) gang exploited security vulnerabilities in Kaseya's VSA remote monitoring software and released a malicious security patch that infected up to 40,000 computers at over 1,000 companies with ransomware.

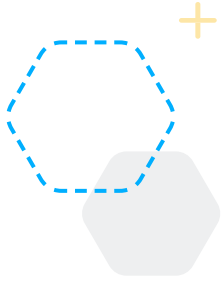
The Kaseya incident was a supply chain attack because it leveraged a vulnerability in the software supply chain to impact many downstream customers of managed service providers. The attack caused such chaos that it resulted in the temporary closure of the Swedish grocery chain Coop's 550 stores. Coop outsourced some IT services to an MSP, and that MSP was affected by the malicious patch in Kaseya's VSA software.

### **Swiss Cloud, April 2021**

In late April 2021, Swedish cloud hosting provider Swiss Cloud became the victim of a [ransomware attack](#) that took down its infrastructure. Up to 6,500 companies were directly impacted by the attack because they depended on Swiss Cloud to host their websites, run applications, or share files.

The response to the attack was to engage in a swift restoration of the company's server infrastructure. Statements released in the incident's aftermath mentioned engaging with HPE and Microsoft to help restore servers from backups. Swiss Cloud's employees worked around the clock to eventually restore the server infrastructure over the course of a few days.





### **Managed.com, November 2020**

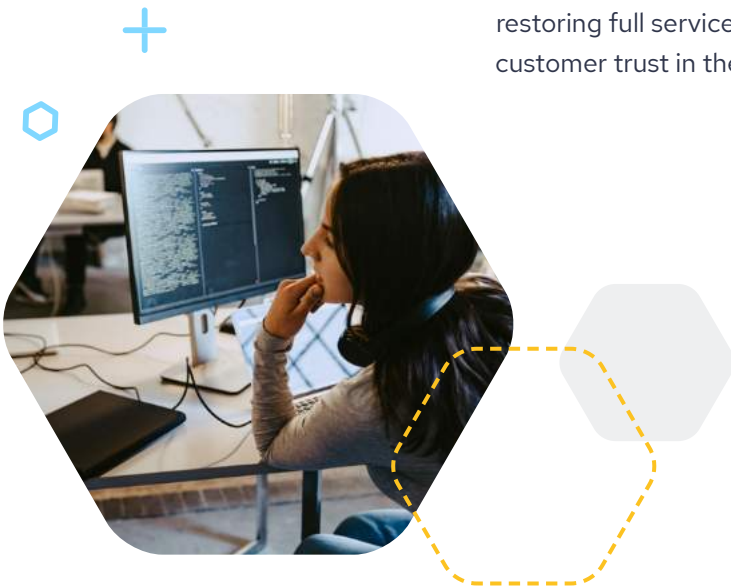
Managed.com provides managed web hosting solutions for website owners. In a world where eCommerce is a well-established business model, any website outage can directly result in lost revenue for affected businesses. The November 2020 incident was a [ransomware attack](#) targeting Managed.com's public-facing web hosting systems.

Several Managed.com customers had data on their sites locked down by encryption because of the attack. The affected websites were taken offline shortly followed by Managed.com's entire web hosting infrastructure. The company only disclosed the attack after angry customers contacted them about their websites not being available. REvil was behind this incident, and the group demanded a \$500,00 ransom payment.

### **Cognizant, April 2020**

Cognizant is another multi-billion-dollar IT services company that became the victim of a [ransomware attack](#) on its internal network in April 2020. The company's CEO said that the incident impacted internal services meant to facilitate remote work arrangements for Cognizant employees. The internal operational disruption meant that remote workers had to communicate using alternative methods.

However, Cognizant customers became fearful of the attack spreading to their own networks when Cognizant issued alerts urging clients to block traffic for a list of specific IP addresses. Aside from the costs of cleaning up infected systems and restoring full services, Cognizant faced the significant challenge of maintaining customer trust in the aftermath of the attack.





## Suggestions for IT Services Companies

Here are some of the main lessons learned from the attacks on IT services providers in terms of combatting the threat of ransomware.

- **Use Anti-Phishing Defenses:** Phishing campaigns are a popular vector for threat actors to gain access to a company's IT infrastructure. By impersonating trusted individuals, hackers can target employees with phony emails or social media messages that get them to disclose passwords or download malware. Anti-phishing defenses can include the use of advanced self-learning email filters that block, flag, or quarantine suspicious emails so that they don't reach target employees. Another anti-phishing defense is to conduct [simulated phishing tests](#) to help employees get better at recognizing phishing attacks. Simulated phishing may be particularly helpful for social media phishing.
- **Transparency is Important:** There was a disturbing lack of transparency in some of the ransomware incidents affecting IT services providers. One possible reason for this is that the nature of IT services is such that companies don't want to alarm customers and cause a run on their support teams. However, it's almost always better to be upfront and honest about cybersecurity incidents that directly affect your customers. An interesting thread on a [popular web hosting forum](#) about the Managed.com incident demonstrated the reputational impact of not showing sufficient transparency. One user wrote that "a certain amount of transparency and letting their customers know a basic game plan would have alleviated some of the anxiety". Several users in this thread mentioned switching to a different hosting provider due to this lack of transparency and uncertainty over when their websites would be back online.
- **Be Aware Of The Ripple Effect:** When ransomware strikes IT services companies, it has a ripple effect that can hit thousands of customers at once. The ripple effect is the reason that threat actors can demand huge ransoms, such as the \$70 million demanded after the Kaseya attack. This ripple effect is also the cause of huge financial losses, such as the [\\$50-70 million anticipated following the Cognizant incident](#). As the interface and point of connectivity with many customer networks, it's clear that threat actors see dollar signs when they consider IT services as potential ransomware targets.
- **Having A Functional Business Continuity Plan:** For the IT service companies that were able to restore operations quickly in the aftermath of a ransomware attack, it's clear a functional business continuity plan played a key role. This business continuity plan should include the use of data backup and the ability to replicate server infrastructure using images and cloud computing. It's particularly important for IT services that their infrastructure is not offline for extended periods because the downstream effects tend to hit multiple customers.





# Finance



Meeting the demands of modern digital-oriented customers has resulted in widespread digital transformation initiatives in the financial services industry. The new digital ecosystem harnesses microservices-based financial apps, mobile banking, cloud computing, and artificial intelligence. These activities alone increase cybersecurity risks, but those risks are amplified due to the nature of financial services.

Like healthcare, financial service providers collect and generate a lot of sensitive information about customers, markets, and new products. The threat of ransomware is so prevalent in this industry because hacking groups know that financial service providers have a huge incentive to pay the ransoms they demand. This article overviews the state of ransomware in finance by focusing on recent incidents, statistics, and mitigation strategies.

## Ransomware in Financial Services: The Numbers

When asked to name the greatest threat to their companies and the wider financial system, the chief executives of Wall Street's six largest banks gave "cybersecurity" as the most popular answer. An intriguing 2019 paper highlights the possibility of a "cyber run" where a serious and contagious bank run starts with a cyber attack on a large bank's deposits.

While a ransomware attack might never inflict that level of damage on the financial system, the numbers show how serious the threat is for individual companies.

**Double extortion ransomware attacks in the financial sector increased by up to 350 percent during Covid-19.**

**A 2019 report found that 90 percent of financial institutions responded that they'd been targeted by ransomware.**



## Recent Ransomware Attacks on Financial Service Providers

### Curo Fund Services, South Africa: January 2022

In early January 2022, Curo Fund Services, South Africa's largest investment administration provider, was impacted by a [ransomware attack](#). The company was unable to access its IT systems for almost a week. While no client data was reported to have been accessed, the attack did adversely impact the company's operations.

### Bank Indonesia: January 2022

In January 2022, the bank reported that it has been hit by a [ransomware attack](#) that infected over a dozen computers. Bank Indonesia claimed that there were no impacts on operations because of the attack and that only "non-critical data" was stolen. Shortly after the bank's public statement, the ransomware group [Conti](#) stated that they had approximately 14 GB of data that they would leak onto the dark web if the bank didn't pay the ransom being demanded.

### CNA Financial, Chicago: March 2021

In March 2020, CNA Financial was hit by a [sophisticated ransomware attack](#) that blocked access to key systems and exfiltrated data. The company is one of the largest commercial insurers in the United States. The response to the attack involved shutting down systems to avoid further compromise. The IT system shutdown affected CNA Financial's business operations for three days.

By first stealing data and then encrypting important systems, the perpetrators of the attack used the double-extortion technique to increase the likelihood of a payout. The group behind the attack, known as Phoenix, achieved its aim after [media reports](#) revealed CNA Financial stumped up an enormous \$40 million ransom payment.

### AXA, Multiple Locations: May 2021

The Asian division of insurance giant AXA became the victim of a [ransomware attack](#) that disrupted IT operations in Thailand, Malaysia, Hong Kong, and the Philippines. In the attack, the Avaddon ransomware group stole 3 terabytes worth of sensitive information, including passport copies, customer claims, illness reports, denied reimbursements, and records of payments to customers. This attack somewhat ironically occurred in the wake of an AXA announcement that it would no longer reimburse ransom payments on cyber insurance policies in France.

Avaddon ransomware typically gains an entry point to a network using phishing emails. The emails contain attachments with malicious code that executes on the opener's computer and spreads. Avaddon is a ransomware-as-a-service group that disbanded in June 2021 due to pressure from US and Australian authorities.

### Shirbit, Israel: December 2020

Shirbut is an Israeli insurance firm specializing in real estate, auto, and travel insurance. A group of threat actors known as Black Shadow managed to [hack into the company's network](#) in December 2020 and began leaking stolen information online. A series of Tweets publicized the leaks with an eventual ransom demand of roughly \$1 million to avoid further leaks.

According to a Shirbit statement at the time, the company had a full backup of its systems and data. The same statement conveyed confidence that the attack didn't succeed in obtaining sensitive policyholder data.

### Naz Sukhram, Canada: May 2021

In May 2020, local Canadian media reported that a small accounting firm named Naz Sukhram became the victim of a [serious ransomware attack](#). Hackers stole around 5 gigabytes of internal company documents, including personal and customer data. Such a small-scale incident usually wouldn't be worth covering except for two interesting aspects:

1. The emergence of a new ransomware group
2. The owner's quotes

The threat actors were from a recently discovered group known as Grief. According to a statement by an anonymous Grief member, the gang does not plan to enter into protracted negotiations with victims. Grief wants victims to pay up rapidly or else suffer the release of stolen data. New groups will continue to emerge as long as ransomware remains a lucrative form of cyber attack.

According to the firm's owner, "We thought we were a small company and would not get hit." This response shows that there's a perception among SMBs that only large companies get hit by ransomware because those incidents tend to make the headlines. The harsh truth is that companies of all sizes in every industry are targets. Basic security awareness can go a long way towards reducing risks for smaller companies.





The harsh truth is that companies of all sizes in every industry are targets.

## Suggestions for Finance Companies

The following four ransomware mitigation strategies can provide a good platform from which financial services organizations can reduce their individual risks. These strategies can also reduce the wider systemic risks associated with ransomware attacks on the financial sector.

- 1. Prevention:** Prevention is the first and most effective line of defense against ransomware attacks. Your prevention strategy should be multi-faceted with a focus on both tools and people. Building a security-first culture and providing ongoing training is important for ensuring employees remain vigilant and human error is reduced. However, with ransomware attacks becoming more sophisticated, phishing emails and other forms of social engineering are harder to detect. Advanced tools, such as email security solutions that can detect suspicious emails, can prove invaluable in preventing the initial entry into your network.
- 2. Swift Detection and Response:** Financial companies should have in place solutions that provide deep visibility into their networks so that they can swiftly detect malware propagating through the network. Behavioral-based solutions leveraging AI can come in useful. Rapid response is also critical. Security teams should be able to effectively investigate genuine threats and orchestrate incident response workflows to contain the damage. The aim is to limit or prevent operational disruption to key financial services and to limit any compromise of sensitive data.
- 3. Backup Strategy:** Whether a financial services company is targeted with encryption-only ransomware or double extortion ransomware, an effective backup strategy is always helpful. Even in the worst outcome where sensitive data is first exfiltrated before systems are encrypted, having backups in place can minimize downtime for important customer-facing services. A disaster recovery plan complements the backup plan by specifying how to restore compromised systems or assets to a functioning state as quickly as possible.
- 4. Build Operational Resilience:** Operational resilience means architecting and protecting your network in such a way that you can continue to provide mission-critical financial services to customers even after a disruptive ransomware attack. It's more difficult to achieve resilience than mere recovery from ransomware, however, given the nature of financial services, it's important to strive for resilience.

New rules are coming into effect in the UK requiring financial services providers to demonstrate a good level of operational resilience in the face of the cyber threat landscape. In October 2020, the [US Federal Reserve](#) released a paper on sound practices for strengthening operational resilience. The practices revolve around topics such as proper governance, risk management, scenario analysis, and business continuity management.

# Pharmaceutical



The pharmaceutical industry is comprised of public and private organizations focused on the research, development and manufacturing of drugs and medication. The global pharmaceutical industry was an estimated \$405B in size in 2020 and is forecast to grow at over 11% annually from 2021 – 2028. Of all industries affected by the COVID-19 pandemic, the pharmaceutical industry is by far the most visible. Governments around the globe have made significant investments into the research and manufacturing of vaccines and post-infection treatments. The pandemic has led to the unfortunate increase in cyber attacks against pharmaceutical companies from both pedestrian criminals to nation states looking to steal intellectual capital and obtain ransomware payments.

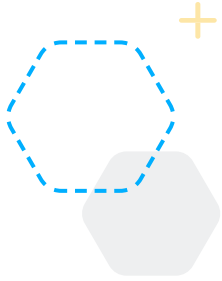
According to a recent [Forbes article](#): “Pharmaceutical and biotech companies suffer more breaches than those in any other industry, with 53% of them resulting from malicious activity, according to the 2020 Cost of a Data Breach Report from IBM and the Ponemon Institute. And the costs of those breaches are constantly growing.”

## Ransomware Incidents in the Pharmaceutical Industry

### Various pharmaceutical suppliers, 2014

A cyber attack known as “Dragonfly” or “Energetic Bear” that was originally thought to be targeting critical infrastructure companies turned out to actually be focused on disrupting suppliers of key ingredients of various drugs destined for pharmaceutical companies. Researchers eventually determined that the attackers were looking to steal intellectual property from the suppliers. The attack began with a spear phishing campaign that ultimately delivered malware to the victims. The attackers then attempted to steal the victims’ intellectual property, which investigators believed would then be used to create counterfeit materials.

The campaign was focused on very small suppliers and ultimately did little damage. Unfortunately, many of the larger pharmaceutical companies didn’t heed the warnings of attacks to come.



### **Merck, 2017**

In 2017, news agencies began reporting on what appeared to be a major ransomware attack named “Not Petya” against several companies located in Ukraine, including financial institutions, government agencies, media outlets and electricity producers (including the radiation monitoring system at the notorious Chernobyl nuclear power facility). The attack weaponized a tax software application named MeDoc that was used by companies around the globe, including Merck. Investigators later determined that the malware quickly spread throughout Merck’s technology infrastructure, taking down approximately 30,000 computers across their sales, research and manufacturing organizations. The company basically ground to a halt for a period of two weeks, which ultimately cost them nearly \$900 Million in damages and another \$400 Million in lost sales. To make things worse, Merck’s insurers refused to pay for the damages due to a clause in their agreement stating the insurance company did not cover what they considered “acts of war.”

The governments of Ukraine, the United States, and the United Kingdom all formally attributed the attack to the Russian government. Russia continues to deny this and claims they also had companies in their country that were adversely affected by the attack as well.

### **Bayer AG and Roche, 2018-2019**

In 2018, pharmaceutical company Bayer was attacked by a purported Chinese hacker group named Wicked Panda using a malware named Winnti. The company believed that the attack was intended to steal intellectual property from the company that would ultimately be used by Chinese pharmaceutical companies for production of knock-off medicines. Bayer stated that while the malware did manage to get into their network, no data was exfiltrated.

A year later, Roche identified a very similar attack. As with Bayer, Roche acknowledged that the malware did get into their network, but no data was ultimately stolen, and the company was able to rid itself of the malware.

### **Dr Reddy’s Laboratories, 2020**

As the pandemic grew in scale, cyber attackers turned their attention to companies involved with the development of COVID-19 vaccines. Dr Reddy’s Laboratories is an India-based drug company that was working on Russia’s COVID vaccine named Sputnik V. The attack crippled the company’s global infrastructure, forcing them to shut down their datacenters and production facilities around the globe. The criminals appeared to be trying to steal clinical trial data that the company had compiled as part of the final stages of their clinical trials. The company was eventually able to restore all systems and production facilities.

## Suggestions for Pharmaceutical Companies

- **Use Anti-Phishing Defenses:** Phishing campaigns are a popular vector for threat actors to gain access to a company's IT infrastructure. By impersonating trusted individuals, hackers can target employees with phony emails or social media messages that get them to disclose passwords or to download malware. Anti-phishing defenses can include the use of advanced self-learning email filters that block, flag, or quarantine suspicious emails so that they don't reach target employees. Another anti-phishing defense is to conduct simulated phishing tests to help employees get better at recognizing phishing attacks. Simulated phishing may be particularly helpful for social media phishing.
- **Leverage Artificial Intelligence:** Artificial intelligence continues to evolve and play an increasingly important role in cybersecurity. AI can be used within several types of cybersecurity tools to detect and prevent ransomware. From email filters that leverage machine learning to intelligent user monitoring, AI can help to thwart ransomware before the dreaded encryption or data exfiltration events that cause the bulk of the damage from these attacks.

## Closing Thoughts

Companies need to treat ransomware as a high-risk incident that they are exposed to at all times. Recovery can be incredibly painful, so it's best to get in place the right mindset, tools, and processes to prevent ransomware before it can cause damage.



To learn more about IRONSCALES' award-winning anti-phishing solution, please sign up for a [demo today](#)

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks are launched globally. Legacy technologies like secure email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit [www.ironcales.com](http://www.ironcales.com) today!



## ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.