Cyber Risk in **Critical Infrastructure**

Gallagher

Insurance | Risk Management | Consulting

The cyberthreat landscape continues to evolve, and the attack surface grows alongside new and emerging technology. This provides new opportunities for threat actors to carry out their crimes against just about every industry sector imaginable.

Of particular concern are 16 specific targets—the US categories of critical infrastructure that provide essential services to society across a wide swath of industries.[1] If any one of these are attacked, essential services could be disrupted significantly for citizens and organizations around the globe. This could lead to material impacts to bottom lines and threaten physical security. As a result, the highest levels of the US government have taken deliberate steps to address these systemic cyber risks. These include:

Chemical

Commercial Facilities

Communications

Critical Manufacturing

Dams

Defense Industrial Base

Emergency Services

Energy

Financial Services

Food and Agriculture

Government Facilities

Public Health

Information Technology

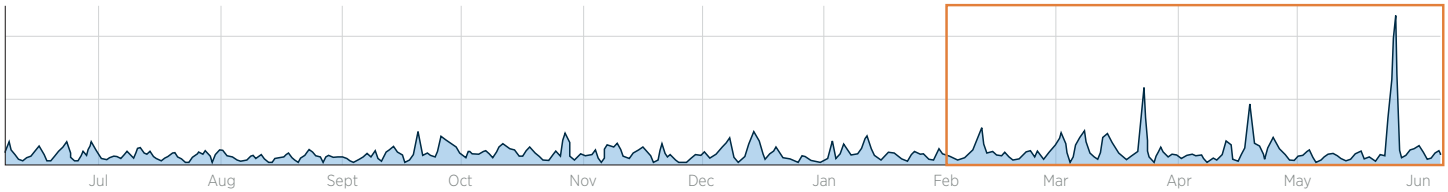
Nuclear Reactors, Materials and Wastewater

Transportation Systems

Water and Wastewater Systems

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors — *Cybersecurity and Infrastructure Security Agency*

Cyberthreat Intelligence:
The Latest Data on Critical Infrastructure



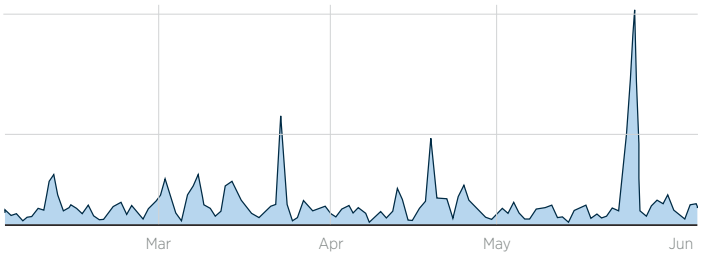


Figure 1: Total social media activity relating to critical infrastructure data breaches and attacks from June 2022 to May 2023, demonstrating some very significant recent spikes of activity.

Gallagher's Cyber team continuously tracks threats to critical infrastructure targets. According to a wide range of industry data sources, the incidence of attacks on critical infrastructure by nation-state groups doubled between 2021 and 2022. This surge in cyberthreat activity underscores the pressing need for enhanced security measures, particularly within critical infrastructure industries. Specifically, IT, financial services, healthcare, transportation and communications have been focal points for cybercriminals, accounting for about 40% of the total activity.

40%

of recent breach activity targeted core critical infrastructure sectors.

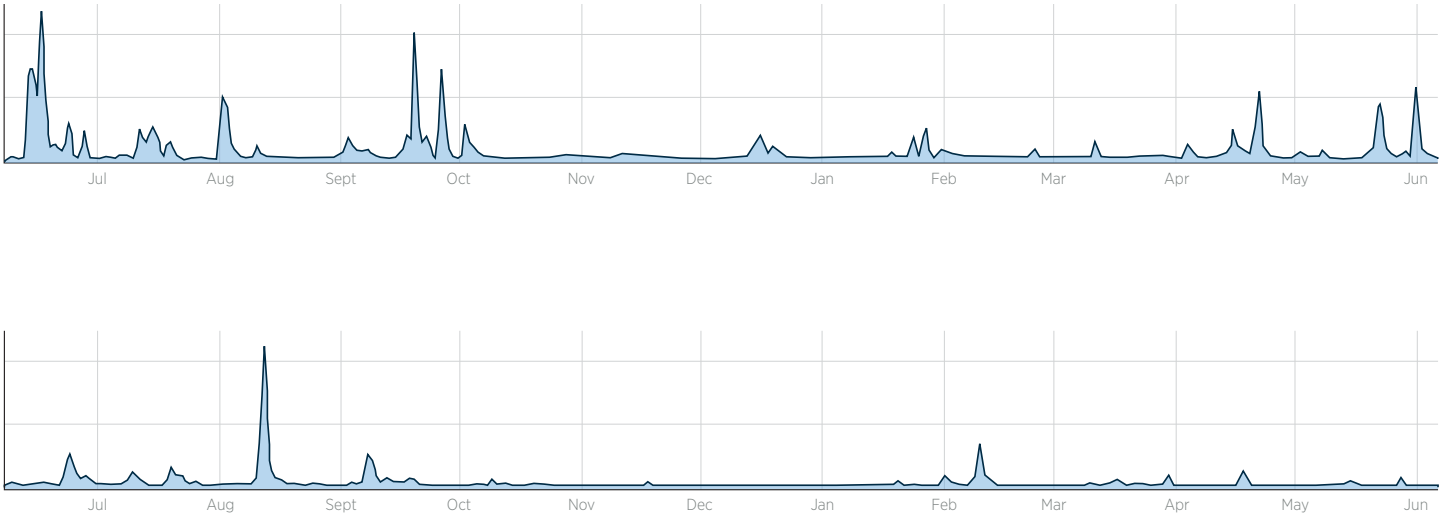


Figure 2: Blackcat ransomware (above) and Conti ransomware (below) activity signatures on social media over the past 12 months, showing significant spikes in the initial aftermath of the Russian invasion of Ukraine. Blackcat activity has recently increased once again, particularly in comparison to Conti.

The situation is particularly severe in Ukraine, where critical infrastructure has been heavily targeted. In fact, attacks in this region have tripled over the past year, with wiper malware becoming increasingly prevalent. While this trend is concerning, the geographic impact of these attacks isn't confined to one area. We are closely monitoring how this level and pace of activity could expand beyond the immediate theater of conflict if the geopolitical situation deteriorates, and drawing the line between cyber warfare and cyber criminality can be extremely difficult.

The financial implications of these security breaches are staggering. The average cost of a data breach, across all industries, currently stands at US$4.35 million according to IBM. Even when excluding the more heavily targeted sectors, the average cost is still a considerable $3.83 million. This economic impact is even more alarming when considering the root causes behind these breaches. Nearly half, about 47%, can be attributed to IT failure or human error, while 28% are caused by ransomware and other destructive attacks. Despite these threats, many organizations tasked with managing critical infrastructure have been slow to adapt and implement more secure architectures.[2]

US$4.35 million

average total cost of a data breach.

Compounding this issue is the challenge of translating operational technology (OT) and IT risks to board members and executives. This communication gap hinders informed decision-making at the highest levels of an organization, thus slowing down the implementation of crucial cybersecurity measures. In light of these findings, it is clear that a shift in mindset, strategies and communication is required to counter the evolving cyberthreat landscape effectively. This will also align extremely closely with how clients subsequently engage with the insurance industry for the purposes of risk transfer, as clients increasingly seek to focus their efforts on buying coverage for specific catastrophic-level risks.

[2] https://www.ibm.com/reports/data-breach — *IBM*

SUMMARY[2]

$4.72 million

average total cost of a data breach in the energy sector.

100GB

of data compromised from Colonial Pipeline in two hours.

Impact:

- Suspension of power systems
- Changes to water quality
- Depleted petrol supplies
- Loss of historical data

THE INCREASING BUSINESS INTERRUPTION EXPOSURE OF THE ENERGY SECTOR

In 2022, the average cost of a data breach in the energy sector reached $4.72 million, further emphasizing the severe financial implications of cybersecurity incidents in this vital industry.[2] Several attacks serve as stark examples of this vulnerability:

- An attack occurred in January and February of 2021 against two major Brazilian energy companies. The DarkSide gang, a group of cybercriminals known for their ransomware attacks, was behind this incident. This led to a temporary suspension of their systems to control the spread of the ransomware.
- In February 2021, a Florida water supply facility was attacked by a cybercriminal who momentarily adjusted the levels of sodium hydroxide in the water supply. Although quickly thwarted in real time, the incident highlighted the potential for cyber attacks to pose direct threats to life.
- In May 2021, the Colonial Pipeline, the largest pipeline system for refined oil products in the US, fell victim to a significant cyber attack. This attack was the most substantial publicly disclosed attack against US critical infrastructure. In a two-hour window, cybercriminals stole 100GB of data, with the ransomware, known as DarkSide, leading to the pipeline being shut down to prevent the ransomware from spreading further.
- In November 2021, the Department of Military and Emergency Affairs (DEMA) suffered a ransomware attack that resulted in significant data loss. The attack was so severe that it shut down 90% of the organization's internal controls and wiped out 25 years of historical data.
- A widespread attack on oil facilities in February 2022 disrupted petrol supplies in northern Germany. Several northern European energy companies were impacted by ransomware attacks led by the BlackCat/Conti group. This incident underlined the potential for such attacks to significantly disrupt critical supply chains.

SUMMARY[2]

$10.10 million

average total cost of a data breach in the healthcare sector.

60%

of healthcare institutions were affected by a ransomware attack in 2022.

Impact:

- Delays in surgeries, patient care and appointments
- Exposed patient records
- Reputational harm

GLOBAL HEALTHCARE REMAINS MOST EXPOSED TO LIABILITY AND DATA EXFILTRATION RISKS

The healthcare sector continues to face a considerable data exfiltration threat, with the average cost of data breaches in 2022 escalating to $10.10 million. This industry's sensitivity, combined with the value of the data it holds, has made it an attractive target for cybercriminals. From 2010 to 2022, healthcare breaches in the US have exposed a staggering 385 million patient records. Moreover, in 2022 alone, ransomware attacks affected 60% of healthcare industries. Such attacks can bring operations to a halt, impacting patient care and causing significant reputational damage.[2]

An alarming series of ransomware attacks in 2022 targeted hospitals and healthcare providers. For instance, a large US non-profit healthcare system was subjected to a ransomware attack, causing delays in surgeries, patient care and appointments. Another attack occurred in Paris where the hackers demanded a $10 million ransom.

The UK's National Health Service (NHS) suffered a supply chain attack in 2022 when Advanced, a communications software provider, fell victim to a ransomware attack.

The incident led to the loss of significant services like NHS 111 and caused interruptions to clinical management, care home and mental health services. This attack followed the infamous WannaCry incident in 2017, which also significantly disrupted NHS operations.

One of the most notable data breaches in recent years occurred in Singapore in 2018. One of the largest healthcare groups in the country was subjected to the largest data breach in Singapore's history. This breach affected 1.5 million patients who had visited SingHealth's specialist outpatient clinics, including the prime minister. The stolen personal information encompassed names, national registration identity card numbers, addresses, gender and date of birth. Furthermore, detailed records related to outpatient dispensed medicines were stolen for 160,000 patients.

THE INCREASED COST OF REMEDIATION WILL CONTINUE TO LEAVE GOVERNMENTS VULNERABLE

In 2022, cyber attacks on government agencies and services witnessed a significant surge, with a reported increase of 95% as per CloudSEK.[3] Notably, cyber incidents within the United States, India, Indonesia and China comprised approximately 40% of these attacks, highlighting these nations as prime targets.

Illustrative of these attacks was an incident in March 2019 when the Australian Parliament became the target of a major breach. Multiple political party networks, including the Liberal, Labor and the Nationals, were infiltrated. The Australian Parliament House networks fell victim to a nation-state threat actor, with indicators linking the attack to China. Although the breach resulted in data loss, none of the compromised data was classified as sensitive, according to the head of the Australian Signals Directorate (ASD). The culprits used phishing methods to deceive employees into providing their credentials, which they then used to gain access to the government's network. Interestingly, this attack was precipitated by a few parliament staff visiting an infected external website.

The government of Costa Rica also suffered a significant ransomware incident which crippled the provision of essential services across the country. The attackers, believed to be the Conti/Hive group, demanded a $10 million ransom. As a consequence of this attack, key services were forced to shut down, causing a disruption that extended to nearly 30 governmental institutions and led to a state of paralysis. The economic impact was immense, with estimated losses amounting to approximately $30 million per day.

These instances underscore the urgent need for robust cybersecurity measures in the public sector. With cyberthreats becoming increasingly sophisticated, governments worldwide must prioritize the protection of their digital infrastructure to safeguard national security, public services and citizen trust.

SUMMARY[2]

95%

increase of cyber attacks on government agencies since 2022.

40%

of these attacks were targeted against the US, India, Indonesia and China.

Impact:

- Shutdown of essential public services
- Loss of historical data
- Compromised national security

[3] https://cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022 — *Cloudsek*

The Latest US Government Response

In March 2023, the White House launched their National Cybersecurity Strategy that outlines a new approach to cyberthreats along with a cohesive strategy that imposes responsibilities on both the public and private sectors. It focuses on five key areas:

- Improving cyber defenses for operators of critical infrastructure
- Disrupting threat actors
- Enhancing the security standards of technology sold to organizations
- Funding public investments to support cybersecurity improvements
- Internationally focused strategies to combat cybercrime

Specific details around these five initiatives have not been released as of this writing. However, the general theme indicates there will be an emphasis on increased responsibilities for cyber risk management on larger, more sophisticated and resource-rich companies. We also believe this may lead to increased liabilities for certain organizations that fail to implement a minimum level of security controls designed to prevent cyber attacks.[4] Ultimately, the Office of the National Cyber Director will work with the Office of Management and Budget will publish details of the plan and how it may be implemented. They intend to provide annual reports to the president and lawmakers on its progress. More details on the National Cybersecurity Strategy may be accessed here.[5]

Cyber Insurance Impacts

> The market remains laser focused on threats to critical infrastructure since the potential for an attack on one of these targets could lead to a dreaded systemic loss, having a cascading impact on multiple insureds around the globe.—John Farley

Cyber insurance products have evolved to cover the threats that underwriters believe can be quantified and effectively managed. Underwriting guidelines often follow generally accepted best practices, and we expect those that are ultimately communicated in the National Cybersecurity Strategy will be considered in future underwriting decisions. The market remains laser focused on threats to critical infrastructure since the potential for an attack on one of these targets could lead to a dreaded systemic loss, having a cascading impact on multiple insureds around the globe. As a result, the cyber marketplace has addressed these concerns by changing, and in some cases, restricting or excluding coverage.

[4] https://www.wsj.com/articles/biden-national-cyber-strategy-seeks-to-hold-software-firms-liable-for-insecurity-67c592d6—*The Wall Street Journal*

[5] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf—*The White House*

When reviewing cyber insurance and other policies that may provide a mechanism to transfer cyber risk for operators of critical infrastructure and those that rely on them, insureds should be mindful of several potential coverage pitfalls, including:

- Critical infrastructure exclusions that may eliminate coverage for all losses related to a specified critical infrastructure target.
- Cyber war exclusionary language that is generally being broadened and may contained ambiguous or undefined terms.
- Catastrophic or widespread loss sublimits and exclusions that may limit or exclude coverage for cyber losses that impact a large number of organizations.
- Regulatory risks that may limit or exclude coverage for regulatory investigations, lawsuits, fines and settlements.
- Contingent business interruption sublimits or exclusionary language that may apply to organizations that were not direct targets, but suffer consequences of a critical infrastructure cyber attack.
- Bodily injury and property damage that occur as a result of a cyber attack may not be covered.

Partnering With Gallagher

It is critical to work with a broker that understands the cyber landscape. At Gallagher, our knowledge extends beyond traditional cyber coverage, as we apply our unique expertise to your cyber concerns.

Our experience shows in our well-established models and practices, yet we continue to focus on innovation and agility in an industry that changes daily with the headlines. The wealth of data that follows showcases this combination of old and new—we have married our established benchmarking, analytics and reporting with new methods and new partners.

AUTHORS

John Farley, Managing Director
Cyber Practice, Gallagher

Jake Hernandez, Lead Consultant
Gallagher Specialty