Google Cloud
Security

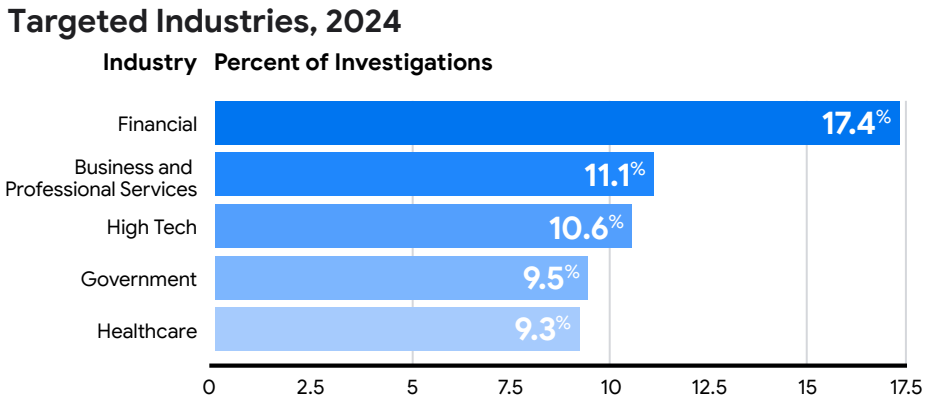
White paper

Securing Nations in the Digital Age

Table of Contents

Introduction: The Vulnerable Public Sector

Governments have been prime targets for cyber attacks since the dawn of the digital age. According to the Mandiant M-Trends 2025 report, healthcare and government / public sector entities remain a top five industry targeted by threat actors today. As such, IT security decision makers at the national level, and at the public sector level, can expect the onslaught of data breach incursions and ransomware events of recent years to sustain well into the future. They will need to prepare and execute national cybersecurity strategies that take into account increasing and diversifying cyber threats, while also navigating a steadily more complex threat landscape shaped by Artificial Intelligence and hybrid multi-cloud environments.



Understanding, detecting, investigating and responding to threats across national infrastructure is notoriously difficult. The majority of governments simply lack adequate cybersecurity investment and maturity, all while facing increased threats from the most advanced and persistent threat actors who constantly evolve their tactics. It's a common perception that the main IT security challenge governments face are attacks by rival nation states and intelligence groups. Yet in recent years financially motivated activity has been on the rise and become more frequent. In 2024, 55% of all attackers observed by Mandiant were financially motivated.

Still, state-sponsored cyber espionage groups continue to target governments and are the most prolific attackers to exploit zero-days, which have grown by 56% from 2022 to 2023. It should also be noted that state-sponsored cybercriminals can be just as financially motivated as non-state actors. In a report published by Trend Micro in early 2025, researchers documented that hacking groups affiliated with at least six nation-states (including groups from North Korea, Iran, Russia and China) are actively exploiting a zero-day vulnerability in Microsoft Windows to conduct espionage, steal data and pilfer cryptocurrency. This vulnerability, designated as ZDI-CAN-25373 by Trend Micro, enables attackers to execute concealed malicious commands due to the way Windows handles the display of shortcut (.lnk) files, also known as shell link files. State-sponsored threat actors have been leveraging this zero-day since 2017, primarily targeting government entities but also think tanks and organizations in sectors such as finance, cryptocurrency, telecommunications, military and energy.

Exacerbating the direct challenges to government is the fact that threat actors are also increasingly targeting public and private sector industries that provide infrastructure critical to the smooth functioning society: healthcare, transportation, public works and utilities. Of course, every nation is distinct in how it organizes public services and maintains critical infrastructure. Many European nations notably opt for a more nationalized approach to health and

welfare services, while countries such as the United States, Japan and Australia rely more on decentralized, public / private approaches that mix nationalized and for-profit entities. The same holds true for national rail, air transport, electric and water utilities and more.

The point being: the diverse nature of how IT resources are deployed to support these types of national and public sector operations globally give threat actors almost limitless choices in vulnerabilities to attack. The alarming spate of ransomware attacks that hit the U.S. hospital sector in 2023 and 2024 was just part of a growing international wave that has seen thousands of attack world wide, notably France's Hospital Centre Sud Francilien Attack in 2022, Canada's Newfoundland and Labrador Healthcare Attack and the attack on Brazil's – Ministry of Health, both in 2021. That each of these attacks was carried out by a different ransomware group exploiting different points of weakness in the target organization shows the enormous challenges public sector entities and nation states face.

The Need for a Comprehensive Cybersecurity Approach

Very few nation states are able to effectively manage security operations (SecOps) across their entire geographies and national IT grids because most government entities lack adequate cybersecurity investment. This weak footing is compounded by the fact that public sector agencies face increased threats from the most advanced and persistent bad actors who constantly evolve their tactics. Primary threat detection, investigation and response challenges for governments include:

- **Siloed security tools and data sources** that hinder a unified security posture and limit attacker insight. This lack of insight precludes a deep understanding of who is attacking your environment, why they are attacking it, and the tactics and techniques that these threat actors use. The result is that many governments are confronted with multiple needle-in-haystack scenarios.
- **Not enough real-time information sharing** amongst federated SOCs when it comes to relevant threat intelligence, detection rules and playbooks. This lack of sharing and visibility across security operations makes it difficult to detect and understand the criticality of threat actor activity at the national level. It also complicates effective investigation of and response to incursions, increasing the likelihood of a widespread attack.
- **The manual nature of SecOps** processes today, coupled with the ongoing talent shortage, leaves SecOps teams understaffed, overworked and overwhelmed. Most governments—like many private sector organizations—cannot hire enough skilled security experts to get the job done.
- **The cybersecurity talent shortfall**. According to a 2024 ISC2 study, the worldwide workforce of cybersecurity professionals has stalled at 5.5 million people, leaving a gap of 4.8 million workers short of the 10.2 million needed globally to satisfy current demand. In fact, the World Economic Forum (WEF) estimates the global talent shortage, which spans nations, states and industries, could reach 85 million workers by 2030, causing approximately $8.5 trillion in unrealized annual revenue.

The numbers from the ISC2 and the WEF are stark: the worldwide shortage of cybersecurity talent is unlikely to be resolved anytime soon. The fact that universities and industry simply can't train the number of cyber professionals needed to meet demand in the years ahead means the cavalry will not be arriving to save the day for nation state cybersecurity. What's needed is an approach that can both neutralize the lack of professional talent while also overcoming the technological shortcomings of siloed security tools and lack of real-time information sharing at the nation-state level.

Real World Turmoil – Notable Attacks on Public Sector Infrastructure and Services

Cyberattacks on critical public sector infrastructure, including the energy sector, telecommunications and core government functions, have been a worldwide phenomenon for many years.

United Kingdom – NHS WannaCry Attack (2017)
In 2017, the WannaCry ransomware attack severely impacted the UK's National Health Service (NHS), disrupting patient care by forcing the cancellation of over 19,000 appointments, resulting in an estimated £92 million in financial losses, and affecting over 600 NHS organizations.

Israel – Water System Attack (2020)
In April 2020, suspected Iranian hackers attempted a coordinated cyberattack on multiple Israeli water and sewage facilities. This was one of the first known cyberattacks targeting water infrastructure as part of geopolitical conflict. The attack targeted programmable logic controllers used to control the flow and chemical treatment of water in an attempt to manipulate chlorine levels in the water supply, potentially harming citizens.

Ireland – Health Service Executive (HSE) Attack (2021)
In 2021, a cyberattack on Ireland's Health Service Executive (HSE) caused significant disruption, leading to the delay or cancellation of over 100,000 outpatient appointments, disrupting critical services like cancer treatment, and incurring an estimated cost of €100 million.

United States – Colonial Pipeline Ransomware Attack (2021)
A ransomware attack by the DarkSide hacking group targeted Colonial Pipeline, a major fuel supplier in the U.S. The company shut down operations for several days, leading to fuel shortages and panic buying. Colonial Pipeline paid a $4.4 million ransom, but the broader economic disruption was estimated to be as high as $10 billion.

Australia – Medibank Attack (2022)
In 2022, the Medibank attack in Australia compromised the sensitive health records of 9.7 million customers, highlighting the severe consequences of data breaches, including the risk of blackmail and reputational damage, and resulting in over AU$46 million in costs.

Costa Rica – Government Ransomware Attack (2022)
In April 2022 the Conti ransomware group, later joined by Hive ransomware group,compromised nearly 30 government institutions in Costa Rica, including the Ministry of Finance. The attacks severely disrupted tax collection and customs operations. The situation led to a national state of emergency, with the country's import/export logistics collapsing and government employees facing payment delays.

Viasat Cyber Attack – Europe-Wide (2022)
In February 2022 a cyberattack targeted the commercial communications company Viasat, affecting internet services for tens of thousands of households across Europe, particularly in Ukraine. The attack disrupted critical infrastructure and communications, highlighting vulnerabilities in satellite-based networks.

The United Nations Grapples With the Worldwide Hospital Ransomware Crisis

How dire has the worldwide cyber assault on the healthcare sector become? The United Nations recently convened a meeting of global healthcare and cybersecurity experts to explore solutions. In front of the United Nations Security Council in November 2024, Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO), emphasized that the digital transformation of healthcare, coupled with the high value of health data, has made the sector a prime target for cybercriminals. He cited the 2020 ransomware attack on Brno University Hospital in Czechia and the May 2021 breach of the Irish Health Service Executive (HSE) as examples. Beyond hospitals, cyberattacks also disrupted the broader biomedical supply chain. Taken together, cyberattacks on the healthcare sector have truly become a global phenomenon.

Taking a step back from the fact that ransomware attacks have risen to the level of a serious concern at the highest reaches of international governance, one has to consider just how shocking to the conscience these crimes are. That these cyber attackers can demonstrate such depraved indifference to human life on a global scale is disheartening, at the very least. Yet it also puts into stark relief the urgency of putting into place a security solution that will bring an end to such moral outrages.

> "At best, these attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend, and even cause patient harm and death."
>
> **Tedros Adhanom Ghebreyesus**
> **Director-General, UN World Health Organization (WHO)**

The Way Forward: The Core Components of a Comprehensive, Effective National Cybersecurity Solution

Having established the parameters of the challenging IT security environment many nations and public sector entities are confronting, let's consider what steps should be taken toward a coordinated national cybersecurity effort. The first is developing a nationwide SOC that will enable your national cybersecurity leadership and frontline administrators to better understand and analyze threat actors and their behaviors.

Centralized National Security Operations Center

A centralized SOC connected to key players and network resources across the country makes it far more workable to stay ahead of emerging threats. A comprehensive national SOC capability enhances threat detection, making it possible for your security team to investigate and resolve threats with the context and scale your nation requires. It does so by making knowledge sharing across government agencies and beyond to public and private administrators of critical infrastructure far easier. Specifically, it improves the flow of threat intelligence, relevant detections, and incident response plans and playbooks that enable fast, effective mitigation efforts. A centralized national SOC also enables all stakeholders to better understand and analyze threat actors and their behaviors. It also automates

incident response and management, helping to protect against and prevent the spread of major threats. With a modern, nationwide SOC, governments gain the capabilities to:

- Centralize security management and monitoring.
- Access actionable threat intelligence for informed decision-making.
- Enact proactive threat detection and response capabilities.
- Automate security operations for enhanced efficiency.
- Protect against major threats.

Expert Guidance to Support Your Team

Any comprehensive national cybersecurity solution must also be backed by cybersecurity expertise–ideally, a strike team that can be deployed on short notice to help public sector entities combat critical threats and incidents. Just as important is having a team of experts available to help you to define and roll out strategies and strategic priorities, as well as deploying SIEM, SOAR and other security technologies. This team should also be equipped to help uplevel the skills of your team and establish best practices, as well as deliver training and certifications.

Introducing Google Cloud Cybershield™

To address these critical challenges and build a strong foundation for national cyber defense, governments need a comprehensive and integrated solution like Google Cloud Cybershield™. Google Cloud Cybershield is trailblazing a new, AI and intelligence-driven approach to national SecOps. It's a powerful combination of cutting edge technology backed by deep human expertise and hands-on services. Designed to empower security transformation and increase threat awareness on the national level, the solution is based on three pillars:

Tailored and Applied Threat Intelligence

Google Threat Intelligence's unparalleled and real-time visibility of threat actors and their ever-changing tactics, techniques and procedures (TTPs) equips governments with actionable insights most relevant to their environment. Google Threat Intelligence is automatically applied to each government's unique infrastructure and IT framework to uncover threats without the requirement for intensive custom engineering. By defending billions of users, seeing millions of phishing attacks, and spending hundreds of thousands of hours investigating incidents, Google brings market-leading visibility across the threat landscape to keep the most important organizations protected: your core national infrastructure and those of your most critical sectors.

Streamlined Nationwide Security Operations

Google Security Operations' unique approach to speed, scale and intelligence enables simple onboarding and maintenance for a number of interconnected SOCs across public and/or private organizations. With Google SecOps, security teams across the nation can continuously feed virtually unlimited data to the nationwide SOC for analysis and hunting, and then push curated detection rules that are written and maintained by Google security experts to protect different sectors that make up your critical national infrastructure—or even the entire nation—from new and novel threats. But Google Security Operations doesn't stop there. The platform also provides an intuitive analyst

workbench that enables security teams to share information like threat intelligence in real-time to conduct context-driven investigations, as well as relevant playbooks to respond with speed and precision—all helping to prevent widespread attacks.

Capability Excellence

Mandiant's deep expertise empowers security teams with professional guidance and training coupled with Google's Gemini AI technologies to enhance their skills, knowledge and capabilities. Here is where Google Cloud Cybershield meets the moment: applying human expertise exactly where and when it is needed, and also exploiting the potent powers of AI to bolster the skills of national cybersecurity teams, which so often are stretched thin by staffing shortages.

It's a comprehensive solution that can help governments identify and research threats, enhance knowledge sharing and collaboration, and build the skills required to action Google's frontline threat intelligence and a nation's own threat intelligence to quickly and easily identify and respond to threats. And to take skill building even further, Gemini in Security Operations and Threat Intelligence reduce the toil of repetitive tasks, and pair novices and security experts with AI expertise to make it easier to "do" security.

Cybersecurity Transformation

There are various ways that Mandiant experts are contributing to Google Cloud Cybershield. The industry is probably most familiar with Mandiant Consulting Services, but the Mandiant team's deep expertise and domain knowledge also inform Mandiant Threat Defense for Google SecOps and the Mandiant Incident Response solution. The goal is to pair the world's elite threat hunters with advanced AI-powered tools and the latest threat intelligence to create turnkey solutions for resource-strapped public entities. The Mandiant team will lead your cybersecurity transformation, with dedicated security experts helping you to develop and mature security capabilities, and put in place a nationwide CISO function. Your cybersecurity transformation will take place across three primary functions:

1. Incident Management

Capability excellence means you'll not only be able to resolve incidents faster, but you'll learn from them and steadily improve your security posture. How? Because you'll always know the answers to critical security questions including:

- Have I been breached?
- Am I prepared to handle a breach, including addressing legal and regulatory obligations?
- Can I attribute malicious activity and whether it is part of a wider campaign?

2. Skills Pipeline

The Mandiant team will deliver instructor-led and web-based training to your security team, so you'll always have the insights needed to answer questions including:

- How can I optimize my security processes?
- How can I up-level and retain my staff?
- Can I quantify and plan for long-term skills requirements?

3. Operationalization

The Mandiant team will help you design and implement your solution, and then provide technical training for your security team so you will have the knowhow understand:

- Is the solution optimized?
- Is my team prepared to run the solution?

Finally, with Google Cloud Cybershield deployed and backed by Mandiant, you will gain the capabilities to:

- Regularly hunt for threats that may have evaded your security controls.
- Tap into Google SecOps' 12-months of hot retention, applied threat intelligence, powerful search, AI and additional capabilities.
- Surface findings and map them to the MITRE ATT&CK framework so that you can take action and understand which of your controls were subverted.
- Get back to business if you do encounter an incident.

Google Cloud Cybershield™ Key Benefits and Capabilities

Google Cloud Cybershield™ equips governments with a comprehensive solution to understand, detect, investigate and respond to cyberthreats. The solution is built on Google's hyperscale infrastructure, and leverages applied threat intelligence and AI. It's a combination of deep cybersecurity know-how backed by up-to-the minute cloud security technology that enables unmatched threat detection, insight into indicators of compromise (IOCs) and coordinated incident response capabilities at nationwide scale.

Enhance Situational Awareness

Provides a comprehensive view of the threat landscape and potential vulnerabilities. Google has a very diverse set of Intel sources that provide unmatched breadth and depth:

- **Threat Insights** – Google sees attacks on, and protects, more than 5 billion devices and 1.4 billion mailboxes in addition to the world's largest crowdsourced threat intelligence database providing massive scale to the breadth of our visibility.
- **Open Source Intelligence** – Provides a wide array of information on malware, vulnerabilities and hacking trends.
- **Crowdsourced Intelligence** – Provides real-time visibility into identifying emerging trends and IOCs to help hunt for breaches. This feature set is powered by Google subsidiary VirusTotal (now part of Google Threat Intelligence), which in the early 2000s pioneered the multiscanning technique where multiple anti-malware or antivirus engines run concurrently, vastly improving the ability to uncover emerging threats.
- **Frontline Intelligence** – A critical aspect is the depth of our visibility leveraging frontline threat intelligence from Mandiant responding to over 1,100 incidents per year and human curated intelligence delivered by over 500 global threat experts.
- **Human-Curated Intelligence** – Provides high quality contextualized intelligence including threat actor motivations, tactics, techniques, and procedures and likely targets.

Drive More Effective Security Operations

Automates and streamlines threat detection, investigation, and response workflows. Google Cloud Cybershield provides a rich and growing set of curated detections out of the box via Google Security Operations. These detections are developed and continuously maintained by our team of threat researchers, so you can detect more threats across the nation with less effort. You'll be able to mount a truly effective national SecOps program backed with capabilities unique to Google:

- **Threat Research** – Google and Mandiant researchers detect novel threats, often before you're aware of them.
- **Detection Maintenance** – Continuous maintenance and updates, from discovery to outcome.
- **Detection Engineering** – High fidelity detections are developed and published regularly in the Google SecOps console.

Reduce the Impact and Severity of Cyberattacks

Proactively identifies and mitigates threats to critical national infrastructure. Google Security Operations includes full-fledged security orchestration, automation and response (SOAR) capabilities. With a simple yet powerful drag and drop interface, you can easily build playbooks that automate common response actions, including advanced features such as parallel actions, version control and nested playbooks. You can also track and measure the effectiveness of response efforts such as analyst productivity and mean time to repair (MTTR), and communicate them with stakeholders. If you suspect an incident has occurred, these features make it possible to:

- Confirm a past or ongoing compromise.
- Contain and eradicate a breach, with in-depth attack analysis.
- Resolve incidents quickly with unmatched expertise from Mandiant when necessary.
- Guide incident management and crisis communications throughout the response.
- Recover business operations, learn lessons and build resiliency after a breach.

Continuously Test Threat Detection Capabilities

Simulates real-world attacks to uncover security gaps and improve response readiness. You can battle-test your security program with red teaming from Mandiant experts:

- Launch active attacks against your environment and operational technology.
- Assess your entire attack surface from human faults to your digital estate.
- Harden controls against the latest and most-relevant APT campaigns.
- Protect critical assets by identifying and mitigating security gaps and vulnerabilities.
- Enable your SecOps blue team to learn with open book and purple team simulated attacks.

Improve Security Governance

Establishes clear policies, standards, and best practices for national cybersecurity. Mandiant experts will partner with you to build and operate your nationwide SOC.

- **Assessment** – The first step in this journey is working with our consultants to determine where your nations' cybersecurity maturity stands.
- **Design** – With assessment complete, we will work together to establish your organizations' Prioritized Roadmap for Cybersecurity to address national operational imperatives, and to help implement the solution.
- **Enhance** – We will also help define the governance, processes and best practices required to fully operationalize the solution.
- **Sustain** – Lastly, we will continue to provide guidance and drive continual improvement based on your unique environment, all aligned to the most relevant threats and trends.

Build Advanced Skills, Talent and Capabilities

Equips security teams with the knowledge and tools to effectively defend against modern threats. Google Cloud Cybershield offers security expertise in critical areas via Mandiant Cybersecurity Consulting. This includes:

- Cybersecurity transformation enabled by partnering with Google security experts to develop and mature security capabilities with a nationwide CISO function.
- Incident response services that will enable you to respond to active breaches more effectively and minimize the impact of an attack.
- Skill building via instructor-led and web-based training to enhance skills, processes and strategies across the security team.
- Operationalization of Google Cloud Cybershield with help from Mandiant security experts to design and implement the solution and also provide technical training for the security team.

What Google Cloud Cybershield™ Customers and the Analyst Community Are Saying

One of the earliest adopters of Google Cloud Cybershield™ for nation states was the Central Agency for Information Technology (CAIT) in Kuwait. CAIT develops plans and information technology policies at the national level, while also supervising the implementation of e-government plans and projects. Google Cloud Cybershield appealed to CAIT decision makers based on its ability to provide a platform for:

- Coordinating all information technology development and security plans between government agencies.
- Developing and managing IT security methodologies, standards, and patterns for information technology systems, devices and services across the nation.
- Improving the security posture of the official online portal for delivering e-government services.
- Training technical administrators working in the field of information technology and cybersecurity.

"Our vision for the future of national cyber defense is aligned with Google's. The focus on threat intelligence – combined with monitoring and incident management and continuous validation – will allow us to take our capabilities to the next level, and provide a federated national security operations center and more."

Dr. Ammar Alhusaini
Director General of the Central Agency for IT, Kuwait

Google: a Leader in External Threat Intelligence Services

Google: a Visionary in Security Information and Event Management

Google: a Leader in Incident Response Services

All three Google technology solutions underpinning Cybershield for Nation States have been validated by industry experts. Our threat intelligence and incident response services have been recognized as leaders for years. Google was also named a Leader in the IDC MarketScape: Worldwide SIEM for Enterprise 2024 Vendor Assessment. The report noted, "Google Security Operations is the foundation of Cybershield, Google Cloud's solution for securing nation states. Cybershield is resonating with customers that are developing national SOCs that are powered by Google Cloud Cybershield with information able to be federated to industries or other government entities through integration with the national SOC. There are now four nations using Google Security Operations as part of a Cybershield federated national and sectional SOCs."

Conclusion

Google Cloud Cybershield™ empowers governments to strengthen their nationwide cyber defense with an AI and intel-driven approach, streamlined security operations, all backed by expert guidance. By adopting Google Cloud Cybershield, governments can proactively protect their critical infrastructure, enhance their security posture, and build a more resilient nation in the face of evolving cyber threats.

To learn more about how Google Cloud Cybershield can help your government strengthen its cybersecurity posture, visit our website or contact us for a consultation.