LogRhythm®
The Security Intelligence Company

Cyber risk in critical national infrastructure

The approaching storm

Phones. Food. Electricity. Transportation. These items are not luxuries. These are the necessities of a modern society. Keeping these and other essential services running smoothly is, literally, a matter of life or death. Critical national infrastructure (CNI) is so fundamental to daily life that it is often taken for granted. But an interruption is highly visible, and it could affect millions of people.

CNI has long emphasised the physical security of plants and assets. Since the advent of modern terrorism, we have seen increasing physical security at power plants, airports, water treatment facilities, and many other locations. Securing the complex IT systems that run these facilities is equally vital. However, at the same time, CNI operators are expected to provide increased services across a wider area to more customers – and to do so in the context of tightening budgets or capped rates. Smarter, more flexible, and more accessible systems are a key part of CNI operators securely delivering on their mandate.

The days of staying secure by keeping systems isolated and unconnected from networks are rapidly ending. Research from the Centre for Economics and Business Research (CEBR) and Opinium shows 56 per cent of respondents in utilities think their IT system security may be compromised within the year – the most out of any sector[1]. Second was the Telecom sector, where 52 per cent said systems could be compromised. The attacks are coming. CNI operators need to be ready.

The forecast

The UK's Centre for the Protection of National Infrastructure (CPNI) identifies 13 sectors of national infrastructure as CNI, which is defined as:

> "Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks, and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery, or integrity of essential services, leading to severe economic or social consequences or to loss of life[2]."

The critical list

Thirteen sectors are identified as critical national infrastructure by the UK government. Some sectors also have defined sub-sectors. For example, emergency services can be split into Police, Ambulance, Fire Services and Coast Guard:

- Chemicals
- Civil nuclear
- Communications
- Defence
- Emergency services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

[1] Cybersecurity in the boardroom - UK Plc at risk https://www.cgi-group.co.uk/sites/default/files/files_uk/white-papers/cyber_security_launch_white_paper_-_15_march_2016.pdf
[2] Critical National Infrastructure https://www.cpni.gov.uk/critical-national-infrastructure-0

Due to the complexity and scale of CNI, disruptions can occur accidentally or be brought about by natural causes:

- Northeast Blackout of 2003: A software bug in a power company system in Ohio caused an alarm system to fail, without an alarm. What could have been a localised blackout spread to affect 50 million people in Canada and the United States, leaving some without power for more than a week.
- Tōhoku earthquake and tsunami of 2011: An earthquake and subsequent tsunami caused widespread damage and loss of life. Power, transportation, telecommunication, and emergency response systems, amongst others, were knocked out or severely compromised.

However, there are also more focused threats that CNI operators need to protect against, including criminals motivated by profit, ideology-driven hacktivism, terrorism, and military operations.

For example, the Stuxnet virus, used to attack and damage Iranian nuclear facilities, is widely suspected of being a cyber weapon developed to attack this research by targeting SCADA systems[3].

In addition, a 2017 cyberattack on EirGrid, operator of Ireland's electricity transmission grid is also believed to be the work of state-sponsored hackers. Routers were compromised, allowing the interception of communications[4].

Weathering the cybersecurity storm

Research from IDG reports that, in 2016, the average number of detected security incidents for enterprise organisations in the previous 12 months was 9,156, compared to 3,577 on average for small and medium organisations. These numbers represented huge increases over the previous year[5].

Addressing the threat of external attackers is the most obvious example of cybersecurity, and it's an essential first line of defence. However, it's not enough. You can build firewalls, install virus scanners for email, and require multiple passwords, but if attackers see the target as high value, they will still come. For example, the U.S Department of Defense's networks are probed millions of times per day for vulnerabilities[6]. In the case of the EirGrid compromise, the intrusion was not detected for about three months.

Point of entry, point of compromise

Supervisory control and data acquisition (SCADA) systems oversee and help coordinate systems used in running plants and machinery. These high-level systems connect with other controllers, such as programmable logic controllers (PLC) and proportional-integral-derivative controllers (PID), to monitor processes and issue commands. Each discrete instance of a system and every point of connection is a potential point of compromise.

[3] Here's What a Cyber Warfare Arsenal Might Look Like https://www.scientificamerican.com/article/here-s-what-a-cyber-warfare-arsenal-might-look-like

[4] EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack' https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html

[5] 2016 Global State Of Information Security Survey https://www.idgenterprise.com/resource/research/2016-global-state-of-information-security-survey/

[6] Here's What a Cyber Warfare Arsenal Might Look Like https://www.scientificamerican.com/article/here-s-what-a-cyber-warfare-arsenal-might-look-like/

Even air-gapping systems isn't a foolproof defence. The Stuxnet attack is believed to have entered air-gapped equipment via infected USB drives. The next step is scenario monitoring. CNI operators need to look for anomalies and respond to them, ideally automatically. If a pipeline, for example, shows an increased temperature in a section of the line, it needs to be identified, countermeasures need to be taken, and then the situation should to be investigated. It might be a real problem with the line or it could be an attacker spoofing the system to disrupt supply.

Getting a complete picture of an organisation is especially difficult in CNI sectors. There are numerous disparate systems, often legacy systems and embedded systems, all becoming increasingly connected and generating huge amounts of data that has often been isolated in information silos.

User and entity behaviour analytics (UEBA) can detect and respond automatically, not just to intrusion attempts, but also to unusual behaviour from staff or partners. For example, if an employee is accessing data for which she has clearance, but in much larger quantities than normal or for geographic regions she does not normally work in, she may be colluding with attackers (or maybe just with competitors). UEBA can identify this anomaly, flag it for investigation, and suspend access until the investigation is completed.

In addition to providing effective protection against intruders, malicious insiders, viruses, ransomware, malware and other threats, intelligent, system-wide automated monitoring can help meet regulatory and compliance requirements. While many operators of CNI are in the private sector, they often need to meet safety, regulatory and compliance requirements, and pass security audits. The U.S Department of Homeland Security and the UK's CPNI provide guidance to operators of CNI.

Lifting the fog

LogRhythm provides a complete, integrated solution to information security that fits the needs of CNI operators. Our technology allows organisations to see across silos, generating a complete picture across multiple systems. The LogRhythm NextGen SIEM Platform provides infrastructure monitoring to detect malicious activity – whether from outsider or insider threats – on networks.

How can LogRhythm help CNI operators

LogRhythm offers an integrated approach capable of addressing all common requirements and needs, including:

- Security automation and orchestration
- Real-time data management and network monitoring
- User authentication, verification and monitoring
- Regulatory and compliance demands
- Monitoring of privileged users with access to sensitive information
- UEBA
- Network traffic behaviour analytics (NTBA)
- Rapid detection, mitigation and auditing of threats
- Digital chain of custody

UEBA is among the capabilities of the LogRhythm NextGen SIEM Platform. It detects anomalous activity and responds with alerts and automated mitigation. Security automation and orchestration (SAO) frees up time so in-house IT teams can focus on other important tasks and improve operational efficiency. NTBA and network forensics enable complete visibility for more than 3,000 distinct applications as well as detection for cloud, bring your own device (BYOD), and the Internet of Things (IoT).

Advanced security analytics with artificial intelligence (AI) and machine learning also support automated, real-time alerts to verify activities and security, as well as reports for regulatory compliance and auditing requirements.

Collectively, LogRhythm's offerings provide CNI operators with industry-leading automation, compliance and auditing support, comprehensive reporting, and protection against advanced threats, ensuring CNI providers stand strong when the storm abates.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution.

LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

> “LogRhythm provides real-time actionable intelligence within a single pane of glass based on events across my entire infrastructure and allows me to quickly isolate unusual network behaviour by a user, machine or network device.”

Jason Riggins, Network Administrator, Kansas Medical Mutual Insurance Company

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | www.logrhythm.com

LogRhythm, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom.