CYBER RISKS TO CRITICAL INFRASTRUCTURE (CI)

Critical infrastructure (CI) is the new favorite target of ransomware propagators looking for a quick payday. Foreign intelligence agencies also target CI, searching for strategic footholds for yet-to-be-determined purposes.

Regardless of intent, keeping threat actors out is essential to prevent critical infrastructure issues because experts listed cyberattacks on CI as a top concern in 2020.[1] This trend is expected to persist beyond 2021.

CRITICAL INFRASTRUCTURE SECTORS

What falls under critical infrastructure may vary from one country to the next. Below is a list of a few of the sectors that, if incapacitated, could severely affect national security, the economy, public health or safety, etc.

ENERGY

About 70% of energy companies have cyber liability insurance, indicating the impact cyberattacks have on the energy sector.[2]

MANUFACTURING

Ransomware attacks hit close to 15% of manufacturing companies in 2020.[3]

FINANCE

The financial sector reported about 10% of all data breaches in 2020.[4]

HEALTHCARE

The healthcare sector was affected the most by cyberattacks in 2020.[5]

DEFENSE

Experts expect the global defense cybersecurity market to exceed $20 billion by 2026.[6]

GOVERNMENT FACILITIES

In the US, over 15% of government bodies reported a ransomware attack.[7]

MAJOR THREATS TO CRITICAL INFRASTRUCTURE

70% — **PHISHING**
Reported by over 70% of CI operators[7]

50% — **UNPATCHED VULNERABILITIES**
Reported by about 50% of CI operators[7]

40% — **DISTRIBUTED DENIAL OF SERVICE (DDOS)**
Reported by over 40% of CI operators[7]

32% — **SQL INJECTION**
Reported by 32% of CI operators[7]

20% — **CROSS-SITE SCRIPTING**
Reported by over 20% of CI operators[7]

RECENT ATTACKS ON CRITICAL INFRASTRUCTURE

What is evident from the global threat landscape is that critical infrastructure is a growing focus area for cybercriminals.

Colonial Pipeline, one of the largest pipeline systems for refined oil in the US, was hit by a severe cyberattack that disrupted fuel distribution to the East Coast.[8]

Cyberattack on **JBS SA**, the largest meat producer globally, led to the shutting down of its US beef plants.[9]

A ransomware attack hit Australia's **NSW State Transit Authority** forcing them to take down their IT systems.[10]

The **Health Service Executive (HSE) from Ireland** had to temporarily shut down its IT systems because of a cyberattack.[11]

Data of over 4.5 million people got exposed after an IT system hack on India's national air carrier, **Air India.**[12]

WAYS TO PROTECT CRITICAL INFRASTRUCTURE

SECURE REMOTE ACCESS

Remote access, if not secured, could provide a freeway for cybercriminals. Therefore, it is vital to have network firewalls, endpoint protection, good password hygiene, etc.

CREATE ASSET INVENTORY

You cannot protect what you are not aware of. That is why it is essential to have an asset inventory. With an updated inventory of all your network assets, you can implement strategies to ramp up security.

IDENTIFY AND PATCH VULNERABILITIES

Many Operational Technology (OT) and IoT devices that operate within industrial networks are not secure enough to be part of a critical infrastructure environment. By deploying tools to identify system vulnerabilities, it is possible to find risky devices, sort them based on riskiness and recommend firmware updates.

DETECT ANOMALIES

Automated detection solutions backed by artificial intelligence can easily track anomalies and other minor suspicious changes within the network.

COMBINE OT AND IT NETWORKS

Security risks of connected industrial control systems fall when OT and IT networks are managed together as part of a unified operational platform.

Sources: 1- 2020 Global Risks Report, WEF | 2- TechJury | 3- Hiscox Insurance | 4- Verizon DBIR
5- IBM Cost of Data Breach Report | 6- Mordor Intelligence | 7- Cipsec.eu | 8- NBC News
9- Bloomberg News | 10- IT News | 11- BBC News | 12- SKY News

Ramping up your cybersecurity posture is easier with an expert like us by your side. Get in touch now to prevent your organization from falling into the quicksand of cyberthreats.