# **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**

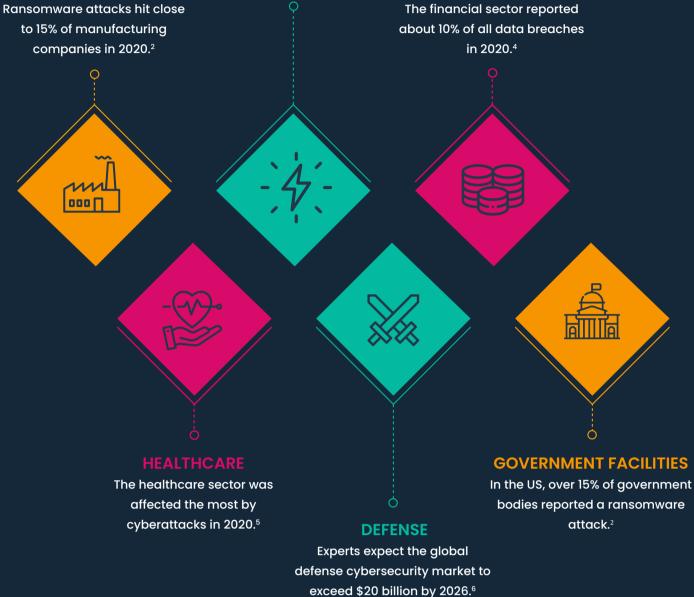
What falls under critical infrastructure may vary from one country to the next. Below is a list of a few of the sectors that, if incapacitated, could severely affect national security, the economy, public health or safety, etc.

### ENERGY

About 70% of energy companies have cyber liability insurance, indicating the impact cyberattacks have on the energy sector.<sup>3</sup>

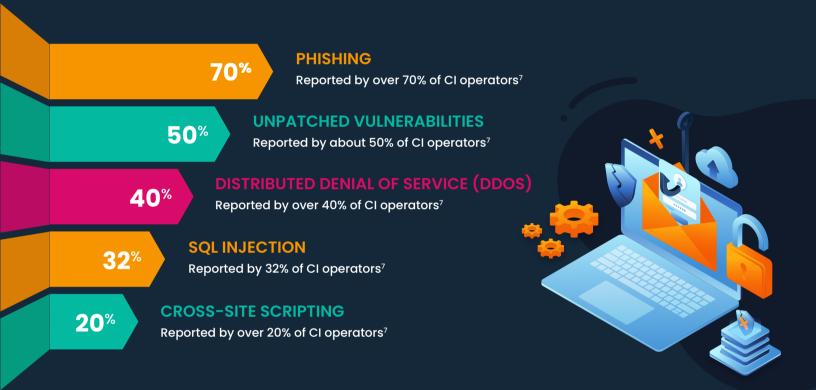
### MANUFACTURING

to 15% of manufacturing



### **FINANCE**

## **MAJOR THREATS TO CRITICAL INFRASTRUCTURE**

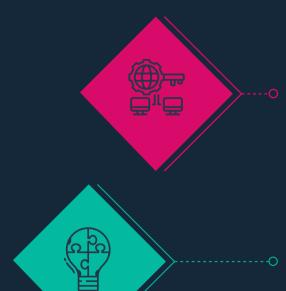


## **RECENT ATTACKS ON CRITICAL INFRASTRUCTURE**

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



### **WAYS TO PROTECT CRITICAL INFRASTRUCTURE**



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,

- 0 C

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.

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.