CEOs: Secure critical infrastructure starts with you —and depends on phishing-resistant MFA

A growing number of cyber criminals are trying to cause mass disruption to public life and safety by targeting critical infrastructure. As the leader of a critical infrastructure organization, a culture of cyber security starts with you.

Is your organization considered critical?

Critical infrastructure definitions vary across countries, but their essence is the same: sectors in which incapacitation or destruction would have a debilitating effect on a nation's security, economic security, public health, and/or safety which can pose a physical threat to human lives. This includes, but is not limited to, the following sectors:

- Chemical
- Banking and Financial Services
- Food and Agriculture
- Information Technology
- Healthcare and Public Health
- Government Facilities
  National, federal, state, local, tribunal
- Commercial Facilities
- Communications
- Emergency Services
- Dams
  Critical water retention and control services
- Critical Manufacturing
  Primary metals, machinery, electrical equipment, transportation
- Defense Industrial Base
  Companies and subtractors supply materials, services, and facilities to national militaries
- Energy
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Waste Systems

Deloitte, The U.S. Cybersecurity & Infrastructure Security Agency (CISA,)
Organization for Economic Co-operation and Development (OECD)

yubico

Only 51% of CEOs demand cyber risk management plans for major business or operational changes. So ask yourself:

- Do your senior leaders know how to respond to a cyber incident?
- What plans do you have to maintain business continuity?
- What are you doing to empower your CISO?
- What are your thresholds for reporting potential cyber incidents to senior management and the federal government?
- How will you respond to the worst-case scenario?

The undeniable proof that the cyber threats targeting critical infrastructure are all too real:

40%

Cyberattacks targeting critical infrastructure around the world **jumped from 20%** of all nation-state attacks **to 40%** (Source)

40%

40% of 500 US critical infrastructure suppliers surveyed said cyber criminals have attempted to shut down their control systems (Source)

80%

Almost 80% of critical infrastructure organizations studied in a 2022 IBM report didn't adopt zero-trust strategies, seeing average breach costs rise to $5.4 million—a $1.17 million increase compared to those that did (Source)

$9.23 million

Healthcare has the highest average total cost for a data breach at **$9.23 million** (Source)

89%

89% of electricity, oil & gas, and manufacturing firms experienced cyberattacks that impacted production and energy supply between mid-2021 and mid-2022 (Source)

yubico

Every CEO's business continuity strategy should start with phishing-resistant MFA

A core part of a successful cybersecurity strategy depends on multi-factor authentication (MFA) and device-bound passkeys, **but not all forms of MFA are created equal.** Modern phishing-resistant authentication and hardware-backed security are the best way to safeguard the most critical information, processes, and IT and OT systems that our society depends on—which is why it has become the standard for government agencies and a growing number of regulatory bodies.

To see real stories of how critical infrastructure sectors are implementing this within their organizations, supply chain and across the globe check out:

A U.S. state uses the YubiKey to protect voter registration databases from hackers

READ CASE STUDY

yubi.co/USGovernment

Schneider Electric enhances global supply chain security with YubiKeys and YubiHSM

READ CASE STUDY

yubi.co/SchneiderElectric

YubiKeys are defending Ukraine's national oil and gas company against cyberattacks

READ CASE STUDY

yubi.co/Naftogaz

yubico

In an interconnected world, everyone is responsible for strengthening the cybersecurity ecosystem

> “One of the greatest cybersecurity threats is the human factor, through phishing attacks when cybercriminals obtain passwords or credentials.”

Oleksandr Tarasov

Head of Security Controls at Security Operation Center, Naftogaz-Bezreka (Ukraine’s national oil and gas company)

Yubi.co/Naftogaz

10%

10% of all breaches are financial services (Source)

11 states

11 states in the U.S. suffered temporary gas outages during the Colonial Pipeline ransomware attack in 2021 (Source)

Cyber security incidents impacting Australian critical infrastructure increased by almost one-third in the 22-23 financial year (Source)

Cybercriminals knocked the Polish stock exchange offline (Source)

Japan’s critical infrastructure, industries, and government agencies have all seen an increase in cyberattacks (Source)

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: www.yubico.com.

Contact us
yubi.co/contact-us

yubico