Securing Critical Infrastructure

Its safety depends on phishing-resistant MFA

Across the globe there is an increasing number of malicious actors trying to cause mass disruption to public life and safety by targeting critical infrastructure with cyberattacks. Such attacks were responsible for impacting Ukraine's power grid, striking a Brazil-based meat processing company, holding a Los Angeles hospital's medical records for ransom, and infiltration of email and fare-collecting systems for San Francisco public transit.

Vital sectors and their impact

Although definitions of critical infrastructure vary across countries, these sectors are vital because their 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

Sources

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

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)

Sources

Microsoft, Government Technology, IBM, Trend Micro, FS-ISAC

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

40%

Cyberattacks targeting critical infrastructure around the world—a 20% increase since June 2020

80%

Critical infrastructure organizations that don't adopt zero-trust strategies

89%

Electricity, oil & gas, and manufacturing firms experienced cyberattacks that impacted production and energy supply

22%

Increase in DDoS attacks on financial firms globally compared to the previous year

$9.3 million

Average cost for a healthcare data breach—the highest average of any sector

yubico

Phishing-resistant MFA's role in securing critical infrastructure

A core part of a successful cybersecurity strategy depends on multi-factor authentication (MFA), 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.

See real stories of how these sectors across the globe are implementing modern phishing-resistant MFA within their organizations and supply chain

To learn more about how to implement a zero trust approach go to yubi.co/ZeroTrust →



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

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

yubico

© 2023 Yubico