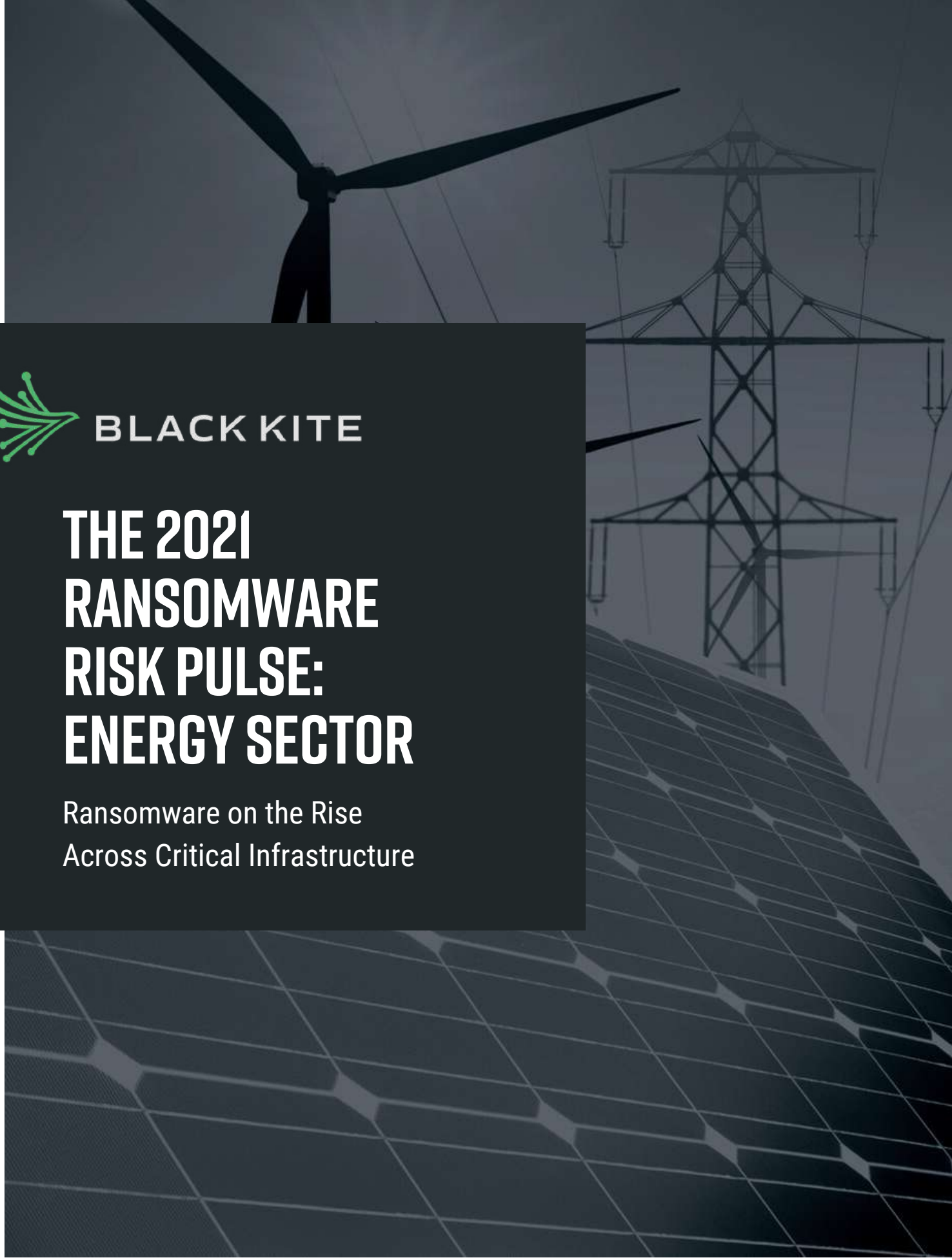


BLACK KITE

THE 2021 RANSOMWARE RISK PULSE: ENERGY SECTOR

Ransomware on the Rise Across Critical Infrastructure

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The U.S. energy infrastructure is integral to growth and production across the nation. Presidential Policy Directive 21 identifies the energy sector as “uniquely critical”, as it provides an “enabling function” across all critical infrastructure sectors. Commonly divided into three interrelated segments (electricity, oil, and natural gas), energy organizations have a heavy responsibility to fuel just about everything we do on a daily basis such as transportation, electricity in our homes, utilities and more.

The risk landscape of the energy sector is not only expansive, but key stakeholders have just recently shifted their focus to cybersecurity with global expansion and trade agreements. Black Kite Research identified three specific areas in which the energy sector is especially vulnerable to modern cyber threats:

1. Increasing nation-state attacks: Cybercriminals with an understanding of the economic opportunity within this sector have increased targeted focus in order to cause widespread disruption.
2. Increasing ransomware attacks: Ransomware poses multiple high-value impacts including operational, financial, legal, reputational and more. Even worse, those hit by a ransomware attack have been more inclined to pay the ransom than not.
3. Increasing attack surface: The digital supply chains of the energy sector have tripled in complexity, requiring more resources and oversight in cybersecurity departments in which hasn’t been available

KEY FINDINGS

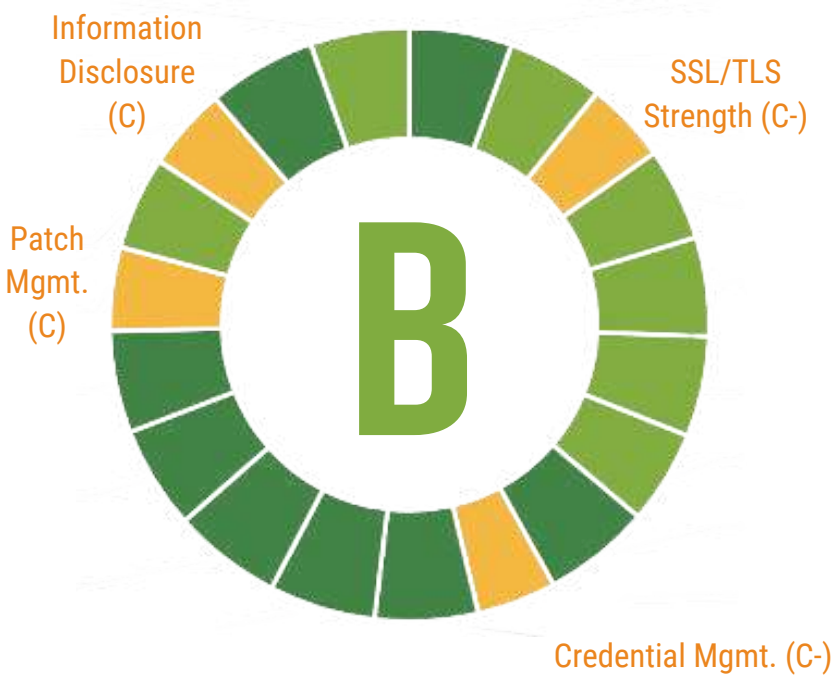
- 25% of the energy sector is highly susceptible to a ransomware attack
- 77% of the energy sector has at least one leaked credential within the last 90 days
- 28% of the energy sub-sector, oil, is highly susceptible to a ransomware attack
- 49% of the energy sector has a critical vulnerability due to out-of-date systems
- 74% of energy companies have not deployed the necessary configurations (DMARC record) to prevent email spoofing attacks

CYBER RISK POSTURE
U.S. ENERGY COMPANIES

In this report, Black Kite Research examined 150 of the top energy companies based on market capitalization [1]. Here you will find a detailed study around common vulnerabilities indicating susceptibility to a ransomware attack, breach highlights corresponding to our data analysis, and data trends over the last year in the energy sector.

THERE'S MORE TO A RATING

On the surface, the energy sector has a decent cyber posture reflecting a "Good" or "B" rating. However, Black Kite Research has identified and analyzed emerging threats causing the industry to remain a prime target for cybercriminals.

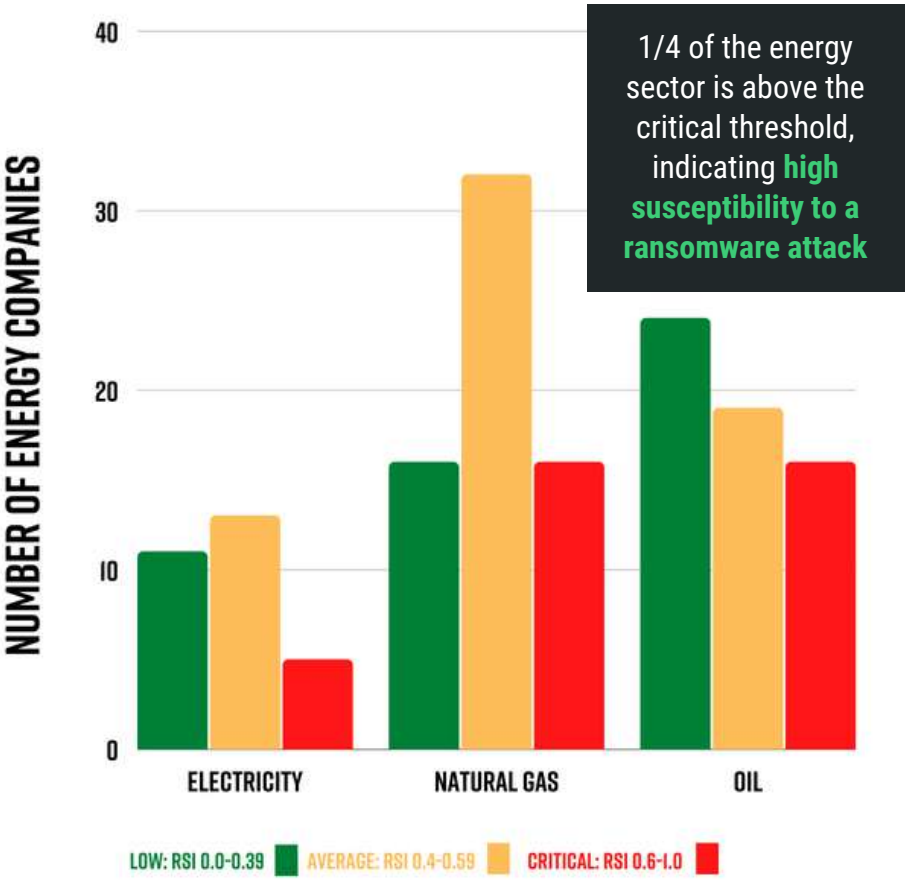


- A 'point-in-time' cyber assessment blinds security professionals to the shifting risk landscape of their supply chain. Black Kite's continuous monitoring provides 24/7 intelligence and alerts organizations to changes in their network.
- Risk categories, such as credential management (C) and patch management (C-), are key indicators of ransomware susceptibility. Attackers accessed the Colonial Pipeline network with the open password of a VPN account.
- Risk professionals must view risk from a hacker's perspective. The key to risk management is understanding what cybercriminals look for when crafting a ransomware attack.

RANSOMWARE SUSCEPTIBILITY
OIL, GAS, ELECTRICITY

RANSOMWARE SUSCEPTIBILITY INDEX™ (RSI™): 0.4

Black Kite's Ransomware Susceptibility Index™ determines how susceptible a company and its third parties are to a ransomware attack on a scale from 0.0 (least susceptible) to 1.0 (most susceptible). An average RSI™ rating is 0.42, with a critical threshold of 0.6. All three energy sub-sectors face susceptibility to ransomware, however some are more vulnerable than others.



1/4 of the energy sector is above the critical threshold, indicating **high susceptibility to a ransomware attack**

OIL - 'B' RATING

Ranking as the most susceptible energy sub-sector, 28% of oil companies are highly likely to incur a ransomware attack. On a daily basis, pipelines carry billions of gallons of gasoline-refined products coast to coast. Targeted attacks on the oil industry result in massive shortages nationwide, from the diversion of gas carrier trucks to consumers hoarding gas through various means.

NATURAL GAS - 'B' RATING

Today, 25% of the natural gas sub-sector is highly susceptible to a ransomware attack. Due to more automation in natural gas systems, outdated systems expose unattended remote devices along the entire length of a pipeline.

Electricity - 'B-' RATING

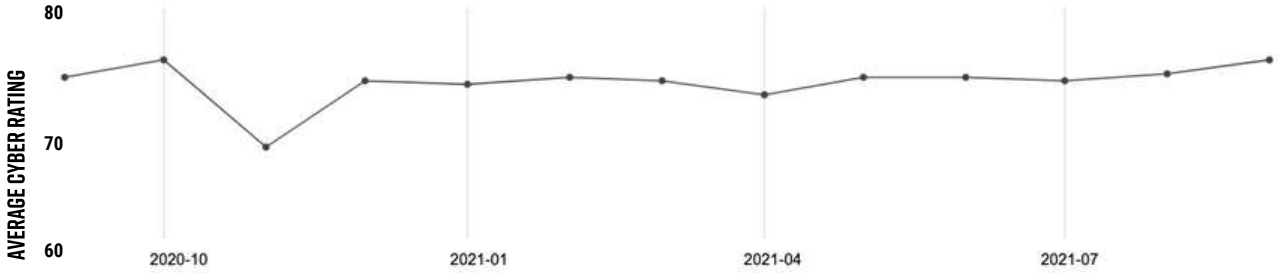
While electricity companies have a slightly lower grade than oil and natural gas, only 17% are highly susceptible to a ransomware attack. This illustrates a point we make often - accurately analyzing risk goes beyond taking a technical grade at face value and requires the full picture of security issues at hand.

BENEATH THE SURFACE OF CYBER RATINGS

A technical rating alone does not provide a comprehensive analysis into the overall risk of an organization. In addition to the technical cyber rating that all security ratings services (SRS) calculate, Black Kite provides the full picture of an organization's cyber risk from additional critical dimensions: technical, financial, compliance and ransomware.

AVERAGE TECHNICAL SCORE: ENERGY

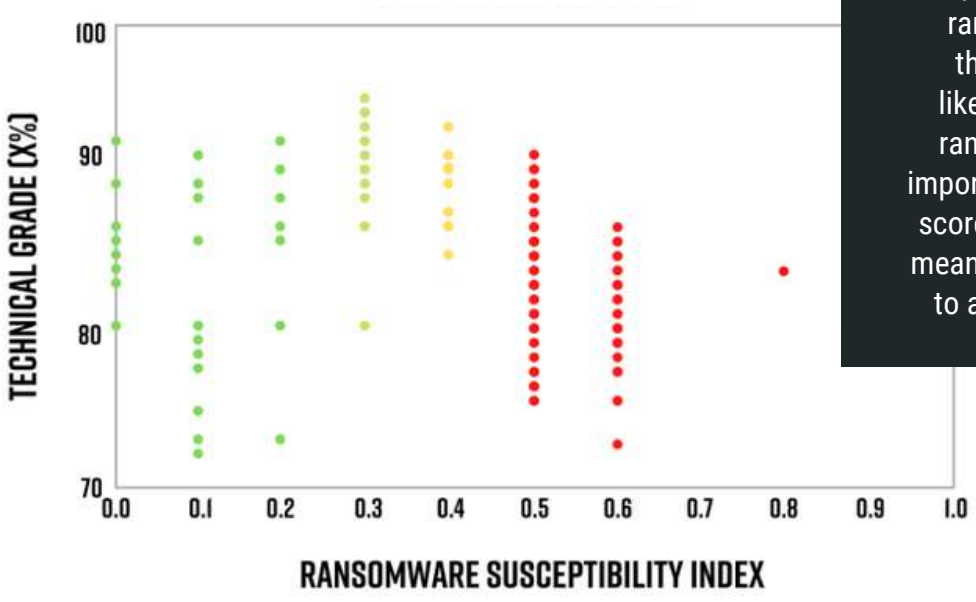
September 2020 - September 2021



While the relatively decent cyber posture of the industry appears to be consistent, Black Kite Research compared the recent average technical ratings with the recent ransomware susceptibility ratings of the sector.

RANSOMWARE RISK VS. TECHNICAL RATINGS

U.S. Energy



Companies with an "A" rating rank above the critical threshold with a high likelihood of incurring a ransomware attack. It's important to note a low RSI™ score does not necessarily mean a company is immune to a ransomware attack.

CRITICAL RANSOMWARE SIGNALS IN 2021 ATTACKS

With a 32% increase in ransomware attacks against utilities organizations in 2020 [3], Black Kite Research analyzed additional indicators increasing ransomware event susceptibility for the energy sector.

CREDENTIAL MANAGEMENT
COLONIAL PIPELINE

Compromised credentials are the No. 1 initial attack vector for data breaches. U.S. energy companies received a "C-" in credential management.

On May 7, 2021, the Colonial Pipeline company, which manages the largest pipeline in the USA, was hacked by threat actors called DarkSide, causing the fuel transfer to be disabled. It is one of the most devastating ransomware attacks ever against U.S. critical infrastructure. There were major problems with fuel shipments due to the cyber-attack, as almost half of the oil-related fuels on the East Coast of America were distributed by this company.

The attackers accessed the Colonial Pipeline network with the open password of a VPN account. It is stated that Colonial does not use multi-factor authentication on its VPN account, which allowed hackers to access Colonial's network with a compromised username and password.

CREDENTIAL MANAGEMENT

77%

of the energy sector has at least one leaked credential within the last 90 days.

FRAUDULENT DOMAINS
VOLUE ASA

The majority (65%) of ransomware attacks leverage phishing as a primary attack vector [4]. Educating employees on how to spot the increasingly sophisticated attacks is an integral to cybersecurity.

Norway-based green energy solutions provider Volue became a victim of ransomware a few days before Colonial Pipeline on May 5, 2021. As a result of the attack, applications that provide infrastructure to water and wastewater utilities that supply 85% of Norway's population were shut down. To prevent the ransomware from spreading to other computer systems, all other company-hosted applications were shut down and nearly 200 employee devices were quarantined.

While the exact source of the attack is still unknown, Volue asked customers to log off from its servers to “avoid any further spreading of the ransomware,” and also asked them to change their passwords for Volue services.

EMAIL SECURITY
COPEL

Despite email being the most common channel leveraged during ransomware deployment, the majority of energy companies have not deployed the necessary configurations to prevent related attacks.

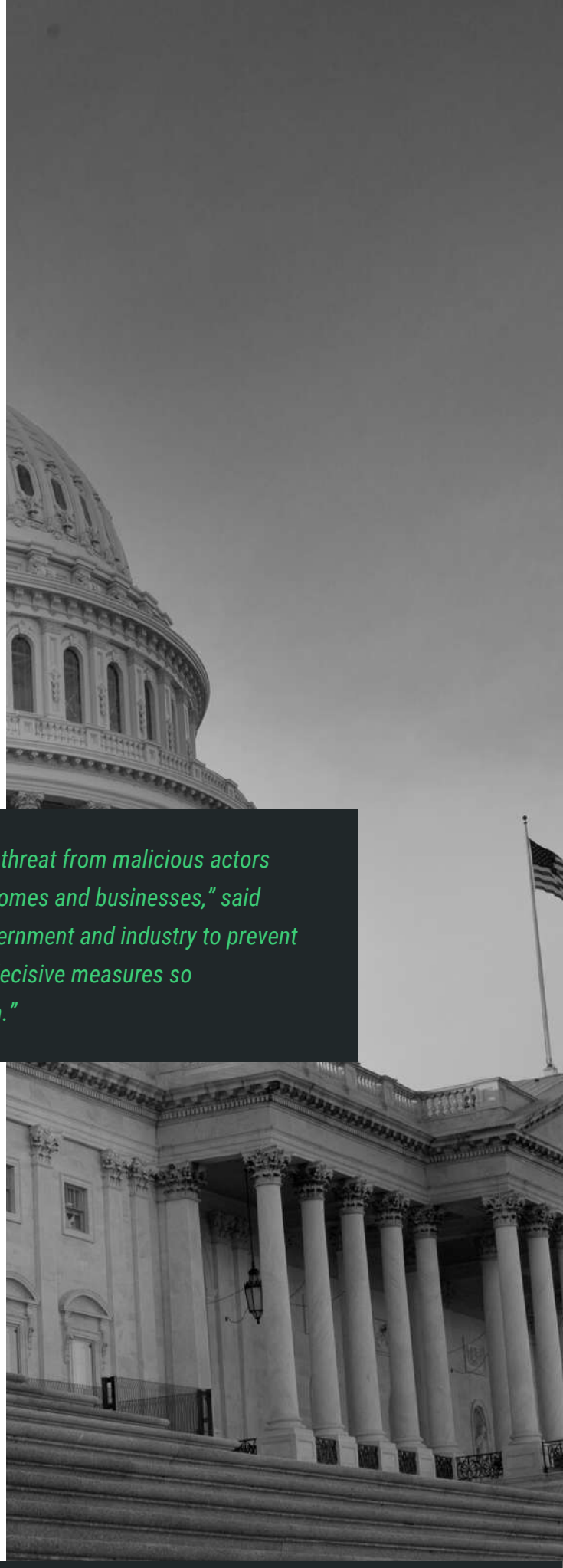
State-owned Brazilian energy utility organization Copel was hit by a ransomware attack in February 2021. Attackers said they gained access to the company’s CyberArk cloud-security solution for privileged access management and exfiltrated plaintext passwords across Copel’s local and internet infrastructure, according to the report.

More than 1000GB of company sensitive data was stolen from Copel. Among the stolen data including clear-text passwords from all local and internet infrastructure, network maps and diagrams, and personal data of employers and customers, including top management; and NDAs, finances and contract info; and detailed engineering schemes, plans, and network switches.

SHARED PROGRESS TOWARD PROTECTION

On May 12th, President Biden signed an Executive Order to improve the nation's cybersecurity and protect federal government networks. Recent incidents became a reminder that U.S. public and private sector entities increasingly face targeted attacks from old and emerging hacker groups. According to the administration, the Executive Order aims toward modernizing cybersecurity defenses by "protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur."

However, incidents such as Colonial Pipeline emphasized that federal action alone is not enough. A large portion of our domestic critical infrastructure is owned and operated by the private sector, which determines their own cybersecurity investments.



"The United States faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity Americans rely on to power our homes and businesses," said Secretary of Energy Jennifer M. Granholm. "It's up to both the government and industry to prevent possible harms—that's why we're working together to take these decisive measures so Americans can rely on a resilient, secure, and clean energy system."

79% of utility companies are educating employees about safe email use, how to spot phishing attempts, and similar skills.

39% of utilities are setting requirements for and/or testing the security measures of their third-parties.

38% of utilities are establishing procurement and supply chain cybersecurity protocols to enhance system and data security [5].

RECAP AND RECOMMENDATIONS

Ransomware indicators aren't new to cybersecurity professionals. In fact, CISA has encouraged companies to actively monitor and address these controls for over a decade. Today's ransomware crime playbook, however, is enough to threaten mature cybersecurity programs due to their inability to scale.

The uptick in ransomware has enabled the cybersecurity community to detect trends that paint a much more accurate picture of organizations' ransomware risk exposure. It's the correlation between vulnerabilities and how they are perceived by threat actors that will enable risk professionals to make better business decisions to prevent ransomware.

The "secret" to uncovering your ransomware susceptibility is understanding the interrelationship between controls—and being able to do so at scale.

Black Kite's Ransomware Susceptibility Index™ reduces that unscalable compliance checklist approach with a data-driven methodology that discovers the likelihood of experiencing a ransomware attack.

FREE RSI™ RATING

REFERENCES

[1] **List of Top Energy Companies in USA by Market Cap as on Jan 1st, 2020**
https://www.value.today/top-companies/top-energy-companies-usa
[2] **CISA Critical Infrastructure, Energy Sector**
https://www.cisa.gov/energy-sector
[3] **2021 Cyber Security Statistics, The Ultimate List Of Stats, Data & Trends**
https://purplesec.us/resources/cyber-security-statistics/#SmallBusiness
[4] **The Third Annual Study on the State of Endpoint Security Risk**
https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf
[5] **Utility Dive, State of the Electrical Utility 2021.**
https://resources.industrydive.com/state-of-the-electric-utility-2021-survey-report

ABOUT BLACK KITE

One in four organizations suffered from a cyber attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective.

With 250+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial and compliance.

CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston Street, Suite 2905
Boston, MA 02199