Deloitte.

How resilient is your critical infrastructure against cyberattacks?

The recent DarkSide ransomware attack serves as another reminder of the impact cyberattacks can have on critical infrastructure. Ransomware attacks are on the rise with increasing persistence and sophistication by threat actors adept in evasion techniques. According to publicly-available reports, multiple affiliates of DarkSide targeted organizations across the United States prior to this attack. DarkSide's targets span multiple sectors, including energy, financial services, legal, manufacturing, professional services, retail, and technology.

Although this specific ransomware threat group and their associated tactics are well established, this attack is considered unprecedented as a result of the impact to the oil industry — 45% of pipeline operators have been affected; more than 17 states have declared a state of emergency; and consumers are already suffering from oil supply shortages felt directly at the gas pump in certain parts of the country.[1]

According to the Department of Homeland Security, pipelines were shut down out of precaution so that the IT infection (where the alleged ransomware attack occurred) did not disrupt operational technology (OT) operations.[2] This attack highlights the growing blur between the digital and physical world and how organizations need to take a serious look not just at their cyber defense posture, but also the resiliency of their business in the event of a cyberattack.

A new precedent in ransomware attacks

What we know about the attack

- A ransomware attack was executed against Colonial Pipeline Company by a sophisticated cybercriminal using DarkSide ransomware.[2]
- The DarkSide ransomware group is based out of the Eastern European region and are known to advertise their Ransomware-as-a-Service in cybercriminal forums. The group has stated that their objectives are monetary, not political, and tend to target companies that have the financial means to meet their large ransom demands.
- The threat actors were able to exfiltrate more than 100 gigabytes of critical data from Colonial Pipeline's network to add leverage to their ransomware demand.[3]

What makes the attack noteworthy

- Colonial Pipeline temporarily halted all 5,500 miles of pipeline operations in an abundance of caution to contain the threat, impacting businesses and millions of people on the east coast of the United States.[1]
- Colonial Pipeline is the largest supplier of gasoline, diesel, and jet fuel on the east coast. They transport 2.5 million barrels of fuel per day—nearly half of the east coast's total fuel supply—through their network of pipelines on the Gulf Coast and distribution centers across the eastern and southern United States.[3]
- Shortly after this attack, a new executive order intended to improve national cybersecurity was announced, highlighting the need for the federal government "*to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.*"[4]

Common security challenges that make organizations susceptible to ransomware

Lack of confidence in segmentation of OT and IT networks to confine an attack from propagating over to critical networks and control systems	Limited awareness of attack surface vulnerabilities and paths to critical systems and assets
Lack of redundant backups that have been tested for resiliency and business recovery effectiveness	Lack of modern tools to provide remote and administrative access to OT systems, such as multi-factor authentication
Inadequate vulnerability management and lack of broad and efficient patching cycles and testing	Lack of a ransomware incident response plans to bring critical systems back online and enable business continuity
Limited ability to monitor for anomalous uploads through user and entity behavioral analysis (UEBA) and data loss prevention (DLP) tools	Limited coordination between OT and IT, leading to siloed views of cyber threats and segregated incident response and resiliency plans

[1] *Washington Post;* "Panic buying strikes Southeastern United States as shuttered pipeline resumes operations"; https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/; *May 12, 2021*

[2] *Cybersecurity & Infrastructure Security Agency; "Alert (AA21-131A) - DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks"; https://us-cert.cisa.gov/ncas/alerts/aa21-131a ; May 11, 2021*

[3] *Bloomberg;* "Colonial Hackers Stole Data Thursday Ahead of Shutdown"; https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown; *May 8, 2021*

[4] *White House;* "Executive Order on Improving the Nation's Cybersecurity"; https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ ; May 12, 2021

Neutralize ransomware and improve future resilience with layered response tactics

NOW: *Are you confident in your ability to respond to a ransomware attack?*

- ✓ **Are you identifying all your IT and OT assets and their associated risks, vulnerabilities, and patching?**
  - Build strong, integrated capabilities for software and hardware asset management across IT and OT, combined with the processes and workflows of vulnerability and cyber threat management
- ✓ **Do you have appropriate visibility into potential threats targeting your environment and adequate telemetry & analytics to identify suspicious and potentially malicious activity across the enterprise?**
  - Increased telemetry across systems, data, networks, and users (including OT) will enhance awareness of baseline activity in order to streamline the identification of outlier activity and inform monitoring use cases
- ✓ **How prepared is your organization to recover from a ransomware incident and follow your crisis plan?**
  - Review Business Continuity (BC) and Disaster Recovery (DR) processes for single points of failure (technical and human) in order to support rapid response to an attack. Procure an incident response retainer
  - Hire skilled cybersecurity leaders and staff with the appropriate level of risk and technical experience to effectively respond. Augment existing skillsets with emphasis on training and education to promote retention

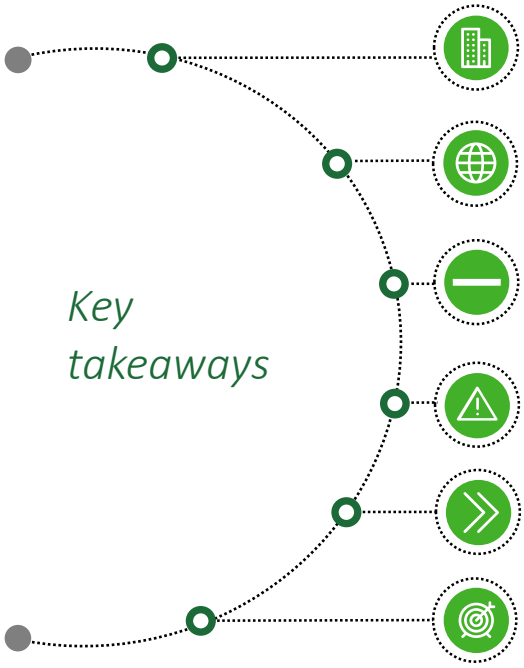
NEXT: *Are you taking proactive steps to enhance your cybersecurity controls?*

- ✓ **How confident are you in your IT and OT network segmentation?**
  - Enforce least privilege and implement physical/logical separation of networks and data for different organizational units between IT and OT. Regularly test restriction of traffic flows between zones and plan for Zero Trust adoption to secure the modern enterprise environment
- ✓ **How confident are you in your organization's capabilities to respond to a potential ransomware incident?**
  - Develop and test emergency response playbooks to determine if they specifically account for a typical ransomware attack, including legal requirements and digital forensics support
  - Perform cyber simulation exercises to test incident response readiness and prepare for future disruptions, including crisis management scenarios emphasizing key business operations impacted by IT and OT
  - Shift from a defensive to offensive security posture. Engage in threat hunting, penetration testing, and breach attack simulation exercises to proactively test for known methods leveraged by ransomware
- ✓ **Are you leveraging modern and layered identity and access management controls?**
  - Protect administrator accounts, especially OT, by rotating passwords regularly, enforcing password vaulting, enabling multi-factor authentication, ensuring least privilege, and monitoring for behavior anomalies

LATER: *Are you pursuing strategic initiatives for future resiliency?*

- ✓ **Have you prioritized the adoption of Zero Trust as a capability across your organization?**
  - Zero Trust is a new security paradigm that commits to 'never trust, always verify' as it relates to access. Institute safeguards across systems by resisting trust for every transaction or action, even if they are recurrent or internal activities
- ✓ **How up to date are you regarding the specific threats facing your industry?**
  - Develop a risk-based threat intelligence program to provide actionable, timely feedback to your business stakeholders in nontechnical terms
- ✓ **How mature is your cyber security data analytics program?**
  - Identify opportunities for advanced cyber analytics within your organization (across IT, OT, cloud, and edge computing) to establish baselines and detect potential anomalous behavior before incidents occur
- ✓ **Have you identified extended enterprise risk across your business and technology supply chain?**
  - Determine systems or data that external parties have access to via direct or indirect business relationships
  - Incorporate supplier risk management into your broader strategic risk and crisis management planning
  - Consider cyber insurance to provide financial support in the event of a major cyber event

While these actions are valuable, even the strongest cyber defenses may not prevent future attacks – **incident response, recovery, and resilience efforts are critical to protect your business.**



Key takeaways

Proactively plan for a crisis: Prepare for technology disruption scenarios (including cyber incidents) with emphasis on security governance, strategic risk management, and supporting policies to effectively monitor and measure risk

Map out your most critical systems and assets: Identify assets critical to your operations which could appeal as targets for threat actors by mapping out your attack surface and maintaining a current inventory of assets continuously scanned for vulnerabilities

Prevent compromise of IT from spreading to OT: Segment your critical systems and OT network, deploy advanced monitoring for suspicious activity, and use jump-boxes to further control access

Accelerate your adoption of Zero Trust: Assume breach and remove implicit trust from users, workloads, networks, and devices. Protect administrative credentials with layered access controls and prioritize network segmentation as well as telemetry & analytics

Increase resiliency of your business: Place as much importance on response efforts as prevention and detection including business resiliency planning and simulation exercises

Go on offense: Modern security principles such as AI-enabled threat hunting, machine learning cyber analytics, and self-healing systems can help you take an offensive approach

Engage with Deloitte

How Deloitte can help

Deloitte can help clients design, build, and operate dynamic, business-aligned security programs wherever they may be in their cyber journey. Services best aligned to ransomware response efforts include, but are not limited to the following:

- Cyber Resiliency & Recovery Planning
- Crisis Management & Risk Management
- Threat Hunting & Intelligence
- Attack Surface Management
- OT Security Architecture
- Zero Trust Transformation
- Identity & Access Management (IAM)
- Threat Detection & Response
- Incident Response Retainers & Forensics
- User Behavior Analytics (UBA) Monitoring
- Red Teaming and Penetration Testing
- Breach & Attack Simulations

The Deloitte difference

We are cyber defense driven. Our Detect and Respond solutions and threat intelligence are continuously enriched, helping some of the largest enterprise and government clients respond to threats. We bring these experiences together with strong backgrounds in national security, intelligence, offensive and defensive cyber operations, and tactics and tool development. And we lead with an innovative IP product suite, including award-winning threat hunting and credential assessment solutions, bolstering our response capabilities via:

Advanced **Proactive Threat Hunting platform** that goes beyond passive detection and response, adversarial mindset required to detect, pursue, isolate, and mitigate threats

Innovative **Credential Risk Assessment analytics tool** that identifies weak credentials and combines broad data collection, advanced logic, and visualization to identify the links adversaries will likely exploit, allowing you to cut off the 'paths of least resistance' to your critical systems and data

Contact us

Deborah Golden
US Cyber & Strategic Risk leader
Deloitte & Touche LLP
Tel: + 1 571 882 5106
Email: debgolden@deloitte.com

Tiffany Kleemann
US Cyber & Strategic Risk Clients & Markets leader
Deloitte & Touche LLP
Tel: + 1 571 480 7196
Email: tkleemann@deloitte.com

Mike Kosonog
US Cyber Energy, Resources & Industrials leader
Deloitte & Touche LLP
Tel: +1 313 396 3622
Email: mkosonog@deloitte.com

Kevin Urbanowicz
US Cyber Energy, Resources & Industrials
Deloitte & Touche LLP
Tel: +1 713 982 2309
Email: kurbanowicz@deloitte.com