MID-CONTINENT LDC FORUM

CYBERSECURITY MEASURES FOR NATURAL GAS INFRASTRUCTURE

9/15/2021

Daniel McGrath- Advanced System Director

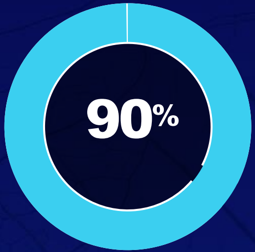
Who is FIS?

LEADING MARKET SOLUTIONS

Enabling How the World Pays, Banks and Moves Energy

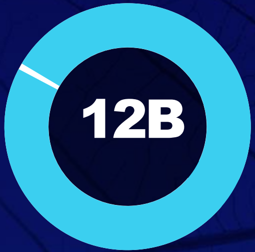
$40 TRILLION Financial Transactions Managed over FIS' Technology

Over 55,000
Employees
Largest
FinTech



90% Market Share
of Global Banks

$40 TRILLION



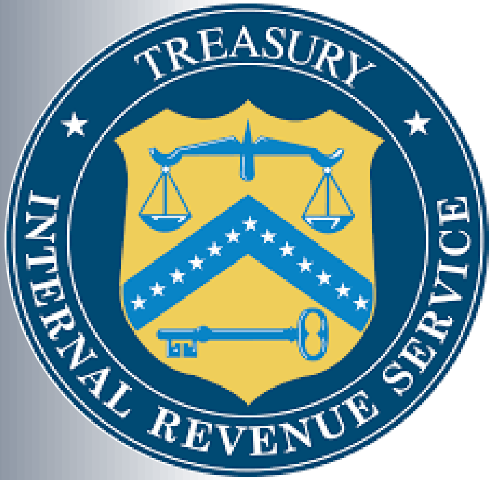
Over
$12B
Fortune 300
Company

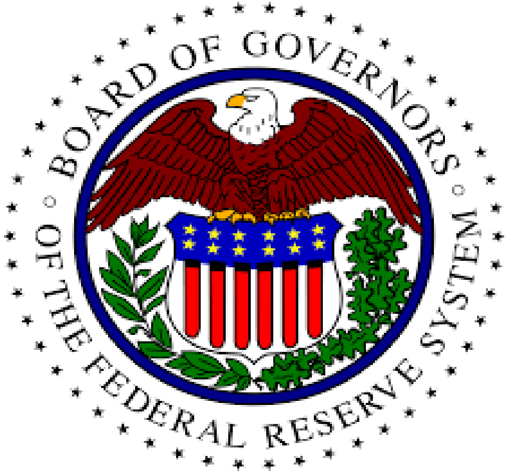
Over 200
Energy
Customers

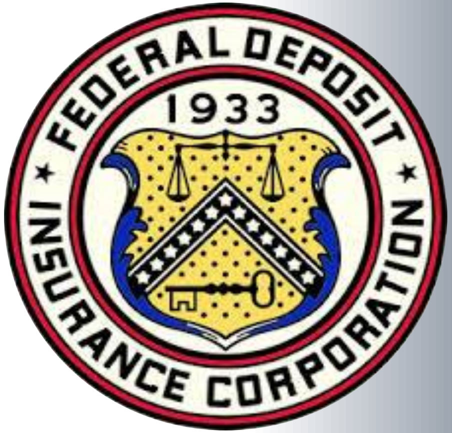
SOME OF OUR NORTH AMERICAN ENERGY PARTNERS-

AMERICAN ELECTRIC POWER
ENGIE
ENSTAR Natural Gas Company
AVANGRID
PSEG
GAS SOUTH
HOWARD ENERGY PARTNERS
Consumers Energy
conEdison
ATMOS energy
dcp Midstream
ATCO Energy Solutions
TALEN ENERGY
IEnova INFRAESTRUCTURA ENERGÉTICA Una empresa de Sempra
nrg
Gasoductos de Chihuahua S. de R. L. de C. V.
PHILLIPS 66
MONTANA-DAKOTA UTILITIES CO.
A Division of MDU Resources Group, Inc.
In the Community to Serve®

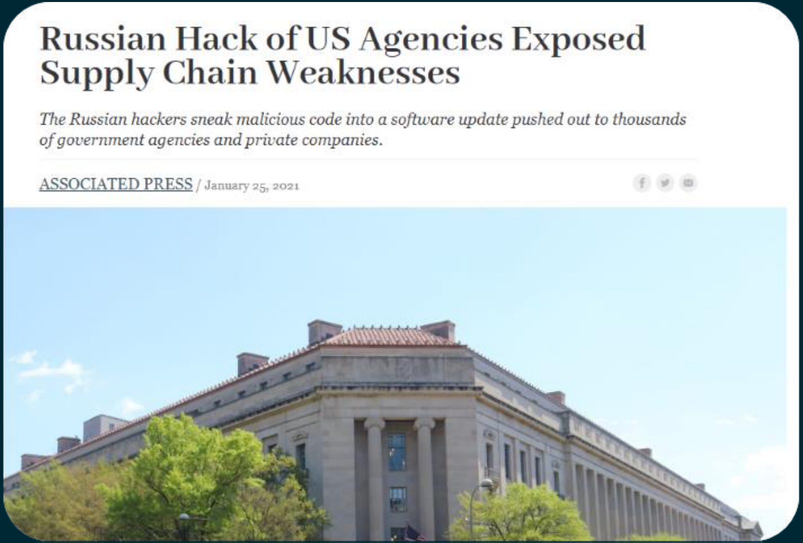
SOME OF OUR GOVERNMENT CLIENTS







SOLARWINDS



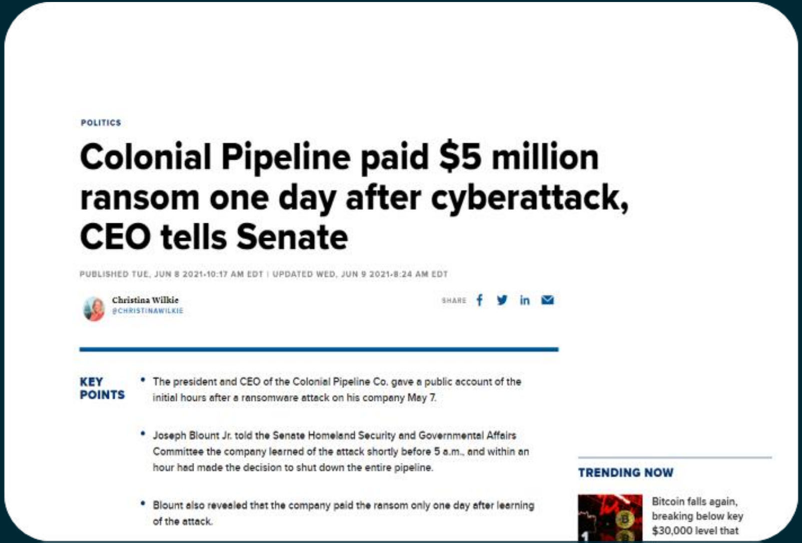
Russian Hack of US Agencies Exposed Supply Chain Weaknesses

The Russian hackers sneak malicious code into a software update pushed out to thousands of government agencies and private companies.

ASSOCIATED PRESS / January 25, 2021

SUPPLY CHAIN ATTACK

COLONIAL PIPELINES



POLITICS

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021-10:17 AM EDT | UPDATED WED, JUN 9 2021-8:24 AM EDT

Christina Wilkie
@CHRISTINAWILKIE

SHARE

KEY POINTS

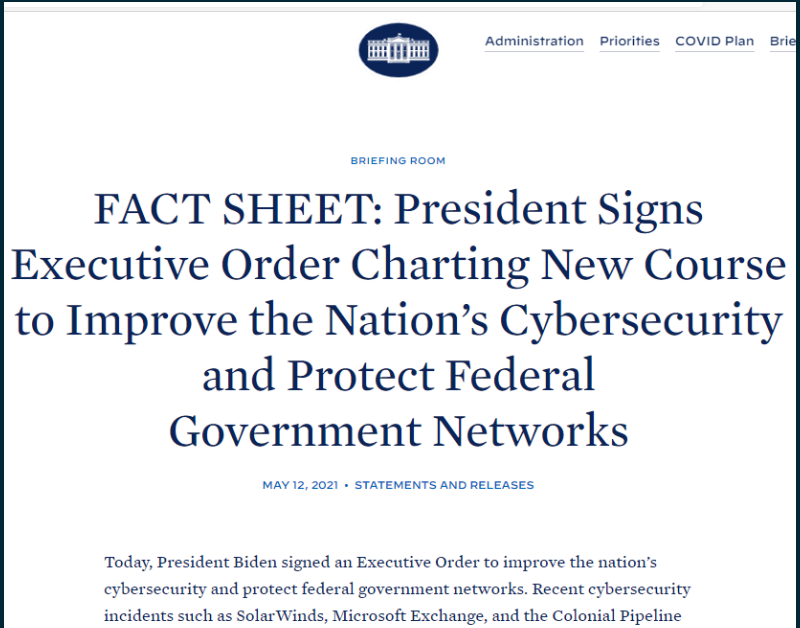
- The president and CEO of the Colonial Pipeline Co. gave a public account of the initial hours after a ransomware attack on his company May 7.
- Joseph Blount Jr. told the Senate Homeland Security and Governmental Affairs Committee the company learned of the attack shortly before 5 a.m., and within an hour had made the decision to shut down the entire pipeline.
- Blount also revealed that the company paid the ransom only one day after learning of the attack.

TRENDING NOW

1 Bitcoin falls again, breaking below key $30,000 level that

RANSOMWARE ATTACK

What are the new Executive Orders?



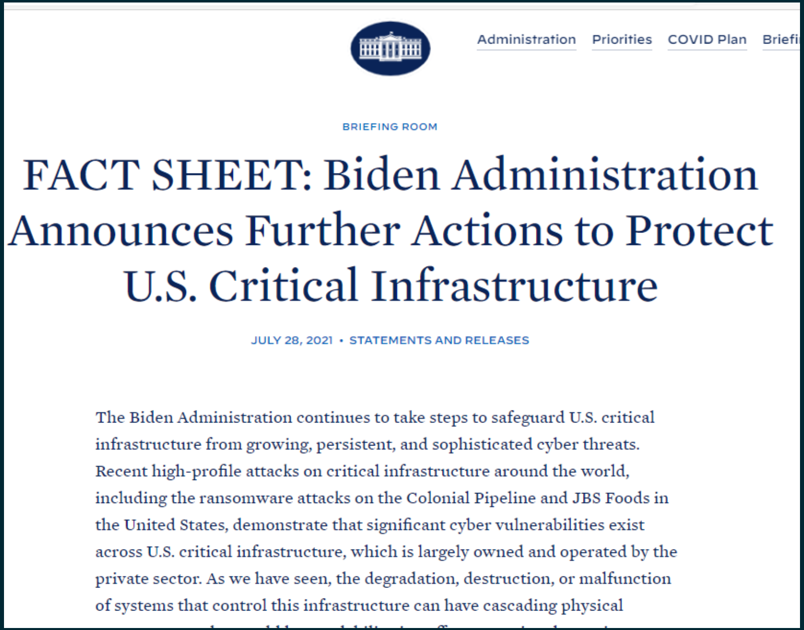
BRIEFING ROOM

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks

MAY 12, 2021 • STATEMENTS AND RELEASES

Today, President Biden signed an Executive Order to improve the nation's cybersecurity and protect federal government networks. Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline

Government Networks



BRIEFING ROOM

FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure

JULY 28, 2021 • STATEMENTS AND RELEASES

The Biden Administration continues to take steps to safeguard U.S. critical infrastructure from growing, persistent, and sophisticated cyber threats. Recent high-profile attacks on critical infrastructure around the world, including the ransomware attacks on the Colonial Pipeline and JBS Foods in the United States, demonstrate that significant cyber vulnerabilities exist across U.S. critical infrastructure, which is largely owned and operated by the private sector. As we have seen, the degradation, destruction, or malfunction of systems that control this infrastructure can have cascading physical

Pipelines

What are the new Directives for Pipelines?

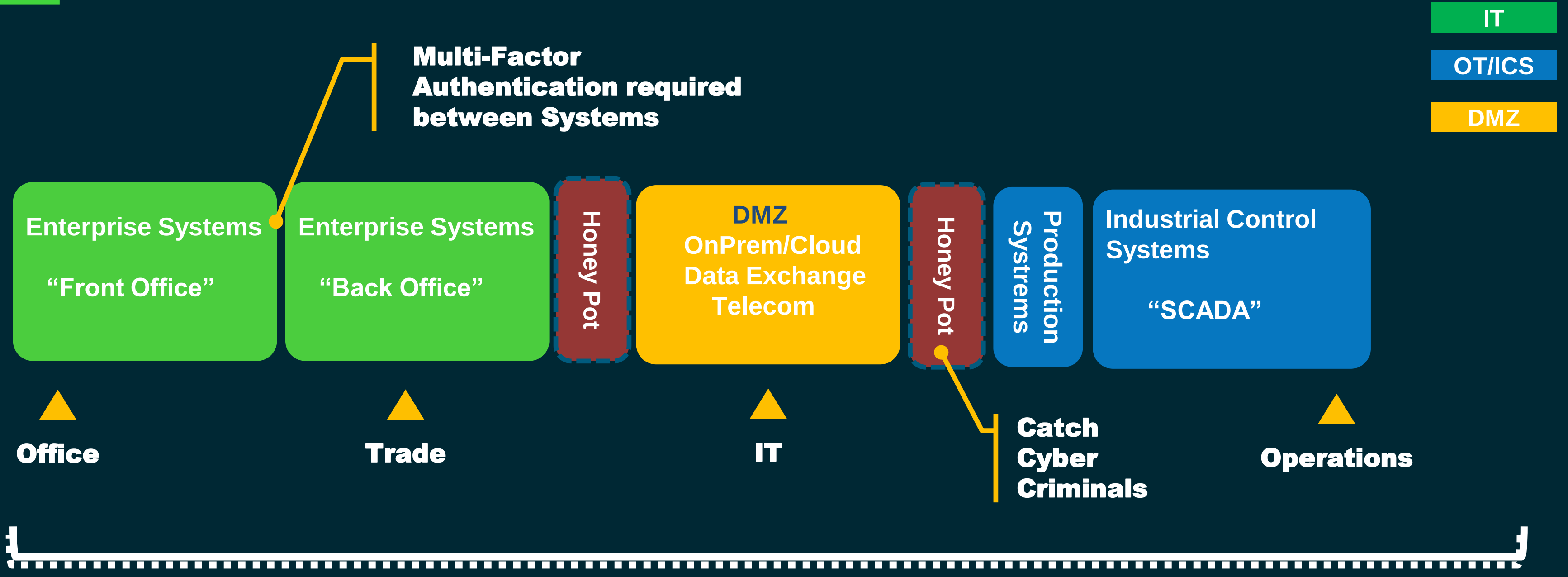
“1st Directive”

1. Report all cybersecurity incidents to CISA within 12 hours
2. Primary and alternative Cybersecurity Coordinator accessible 24/7 to TSA and CISA
3. Conduct cyber vulnerability assessment and report to TSA and CISA within 30 day

“2nd Directive”

1. Implement immediate mitigation measures to protect against cyberattacks
2. Develop a cybersecurity contingency and recovery plan, and
3. Conduct a cybersecurity architecture design review

ZERO TRUST ACCESS ACROSS THE PIPELINE NETWORK



🟩 IT

🟦 OT/ICS

🟨 DMZ

Multi-Factor Authentication required between Systems

Enterprise Systems “Front Office”

Enterprise Systems “Back Office”

Honey Pot

DMZ
OnPrem/Cloud
Data Exchange
Telecom

Honey Pot

Production Systems

Industrial Control Systems

“SCADA”

Office

Trade

IT

Catch Cyber Criminals

Operations

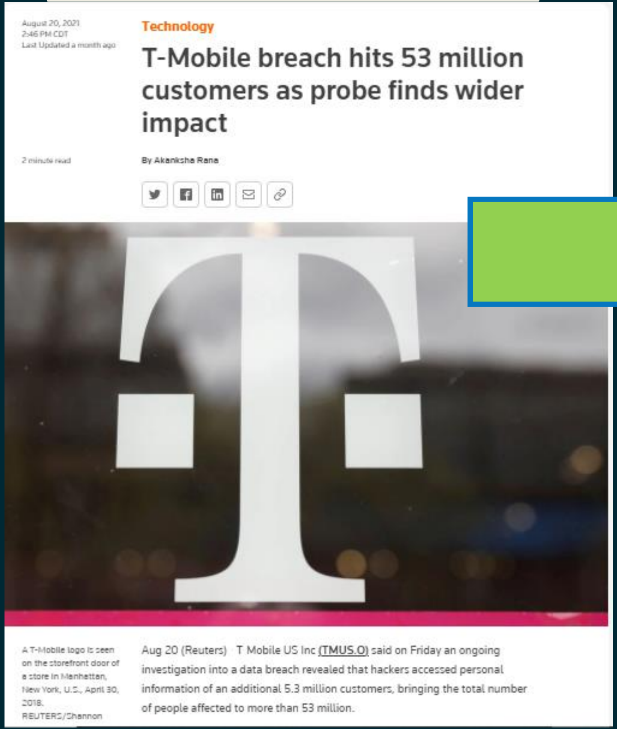
Multi-factor Authentication required to move laterally across the Network
DMZ separates the Enterprise IT Applications from the ICS/OT Systems
Honey Pot Servers set up to catch cyber criminals attempting to change files or remove data

WHAT DO THE ATTACKS HAVE IN COMMON:

Passwords

PASSWORD ENGINEERING:

Consumer Data Breach



August 20, 2021
2:46 PM CDT
Last Updated a month ago

Technology

T-Mobile breach hits 53 million customers as probe finds wider impact

2 minute read

By Akanksha Rana

A T-Mobile logo is seen on the storefront door of a store in Manhattan, New York, U.S., April 30, 2018. REUTERS/Shannon

Aug 20 (Reuters) T Mobile US Inc (TMUS.O) said on Friday an ongoing investigation into a data breach revealed that hackers accessed personal information of an additional 5.3 million customers, bringing the total number of people affected to more than 53 million.

Sold in Mass

Crack Your Password

"INSERT YOUR COMPANY NAME Here"

Industry and Government Partnerships

FIS Partners With Leading Organizations To Defend Against Cyberattacks

National Cybersecurity and Communications Integration Center (NCCIC)

FIS and DHS have partnered to share threat intelligence regarding cyber threats to the global financial industry

Financial Services Information Sharing & Analysis Center

FIS is a platinum member and actively participates in FS-ISAC activities

FIS has created an FS-ISAC TSP Risk Best Practices Group within FS-ISAC

Financial Services Sector Coordinating Council (FSSCC)

FIS is an active leader in the FSSCC, the primary public-private partnership in the financial sector to address operational risk and resiliency efforts

Flashpoint
FireEye
CrowdStrike
Anomali

FIS partners with several respected intelligence providers to obtain and act on analysis of current threats.

Financial Services Roundtable BITS

FIS is a member of BITS, the technology policy division of the Financial Services Roundtable

What is a Fusion Center?

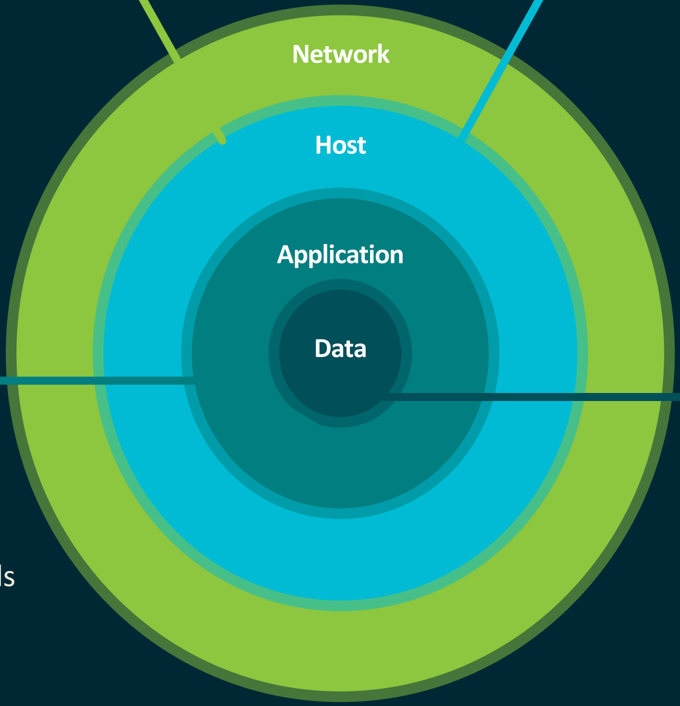
FIS Command Center to Defend Against Cyberattacks

- Brings FIS’s key information security teams together
- Embed with Dept Homeland Security and Microsoft Cyber Security
- Teams consist of Cyber Analysts, SIEM Experts, Forensics Analysts, Vulnerability Assessors, Tools Experts and Penetration Testers

Defense in Depth Strategy

- Vulnerability scanning
- Bastions
- Reverse proxy
- Centralized logging
- VPN
- Network pen testing
- IoC (Threat Detection)
- Wireless detection
- Firewalls
- IDS / IPS
- NAC
- Web App Firewall

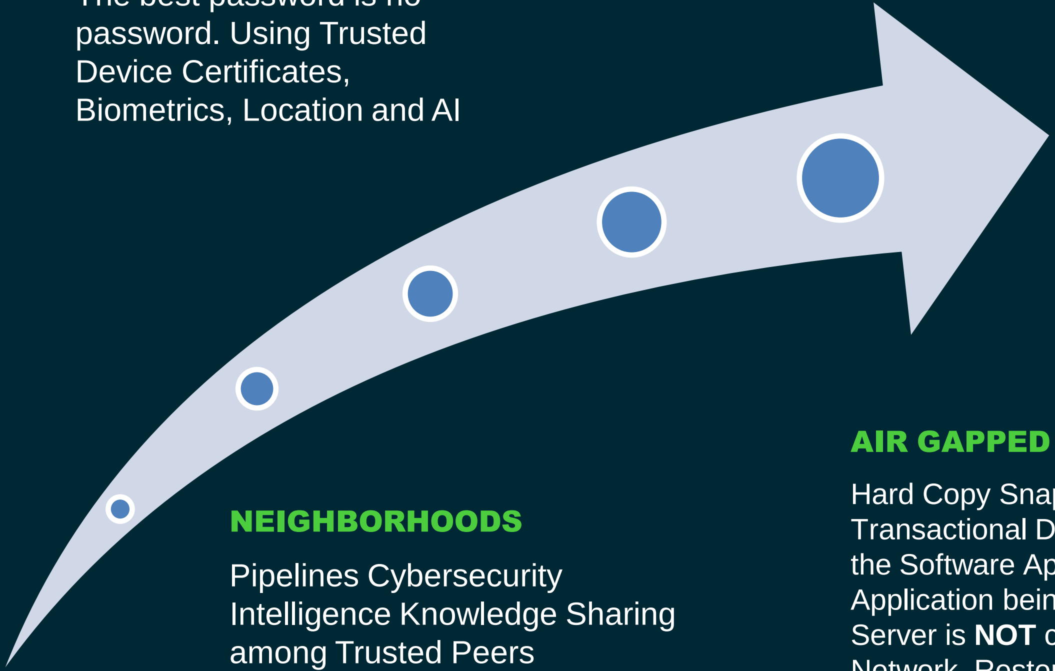
Centralized logical security management
Application Control
Disk Encryption
DLP
Standard builds
Vulnerability scanning
Network pen testing
Host IDS/IPS
AV / malware
Forensics Analysis



App pen testing
Encrypted backups
Vulnerability scanning
Authentication controls
Email encryption
SW development architecture standards

SMTP content filtering
Logical security management
Database Access Management logging
Vulnerability scanning
Network pen testing
Encryption at rest

NEXT Cyber Security Trends on the Horizon?



SBOMS

Software Bill of Material keeps a transparent inventory of what's in a vendor's software and the underlying dependencies on other software.

PASSWORDLESS

The best password is no password. Using Trusted Device Certificates, Biometrics, Location and AI

NEIGHBORHOODS

Pipelines Cybersecurity Intelligence Knowledge Sharing among Trusted Peers

XAAS

"Everything-as-a-Service" from Outsourced Cyber Command to Telco Data Management and Full Back Office Vendor Application Management including DevSecOps.

AIR GAPPED RESTORE SYSTEMS

Hard Copy Snapshots of the Meta Data, Transactional Data and Raw Data but without the Software Application or Database Application being Imaged.
Server is **NOT** connected to the internet or Corp Network. Restores to the last known **Uncompromised** Application Version in hours.

SUMMARY

Unrivaled financial strength

Government-grade cyber security

Comprehensive single-vendor solution

THANK YOU!

Equipped for remote deployment

Best-in-class gas management

Texas-based Energy team

CONFIDENTIALITY STATEMENT: This document contains information that is confidential or proprietary to FIS (or its direct and indirect subsidiaries).

BY ACCEPTING THIS DOCUMENT, YOU AGREE THAT:

(1) if there is any pre-existing contract containing disclosure and use restrictions between your company and FIS, you and your company will use this information in reliance on and subject to the terms of any such pre-existing contract; or

(2) if there is no contractual relationship between you or your company and FIS, you and your Company agree to protect this information and not reproduce, disclose or use the information in any way, except as may be required by law.

DISCLAIMER STATEMENT

When and if available, at its sole discretion, FIS will make available new developments and enhancements made to its currently available products and solutions to its customer base and/or specific customer.

FIS makes no commitment, implicit or explicit, as to the existence, availability, and/or delivery of any product beyond those commercially available as at the date of this presentation.

FIS could elect to make available as part of the standard maintenance services any new development or enhancement at FIS’s sole discretion. FIS reserves the right to modify the scope of functionality, product roadmap, and availability timeline for any development or product discussed, at its sole discretion.