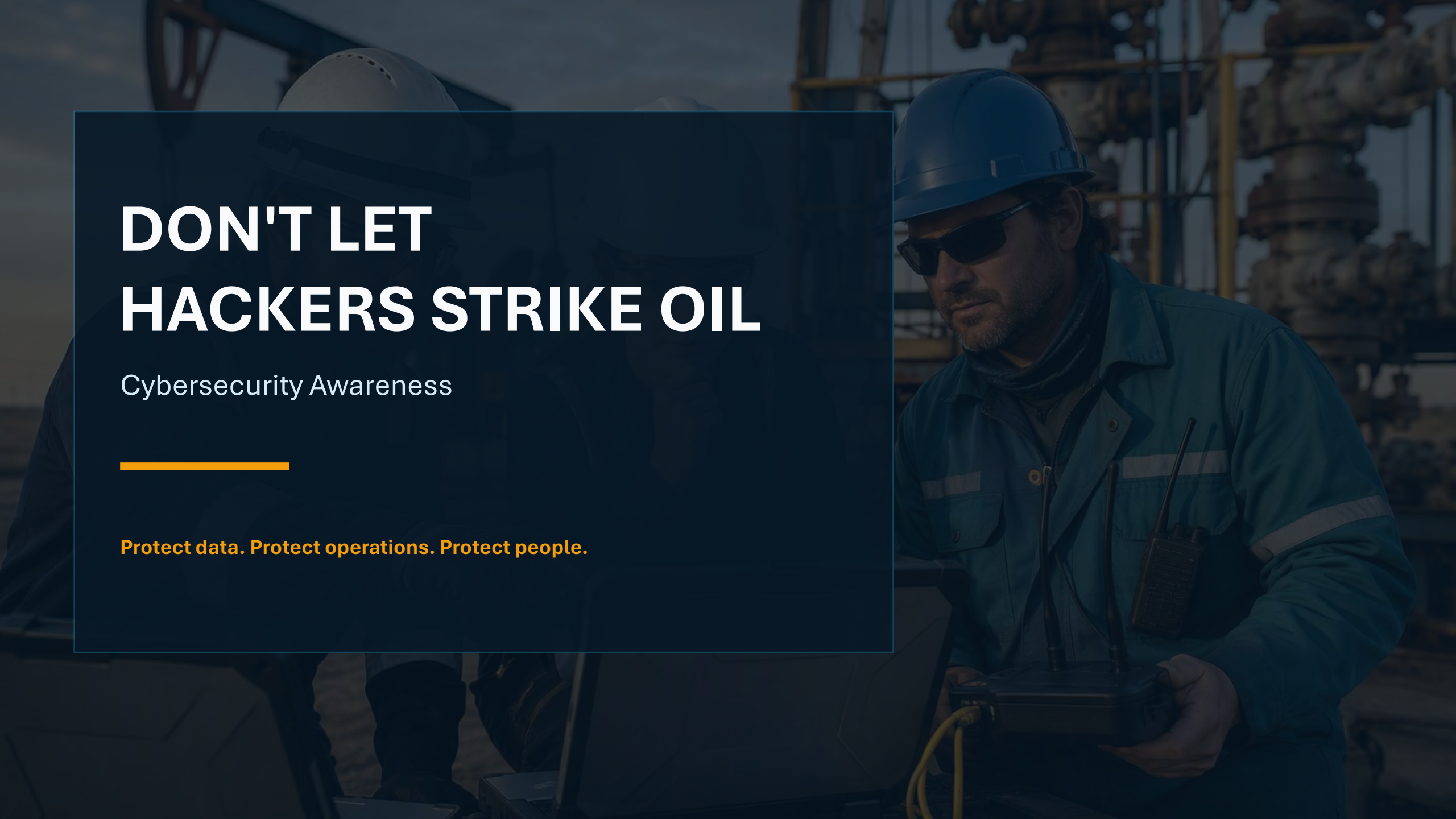


DON'T LET HACKERS STRIKE OIL

Cybersecurity Awareness

Protect data. Protect operations. Protect people.

Sheryl Ryan, CISSP, CBSM

Senior Information Security Consultant

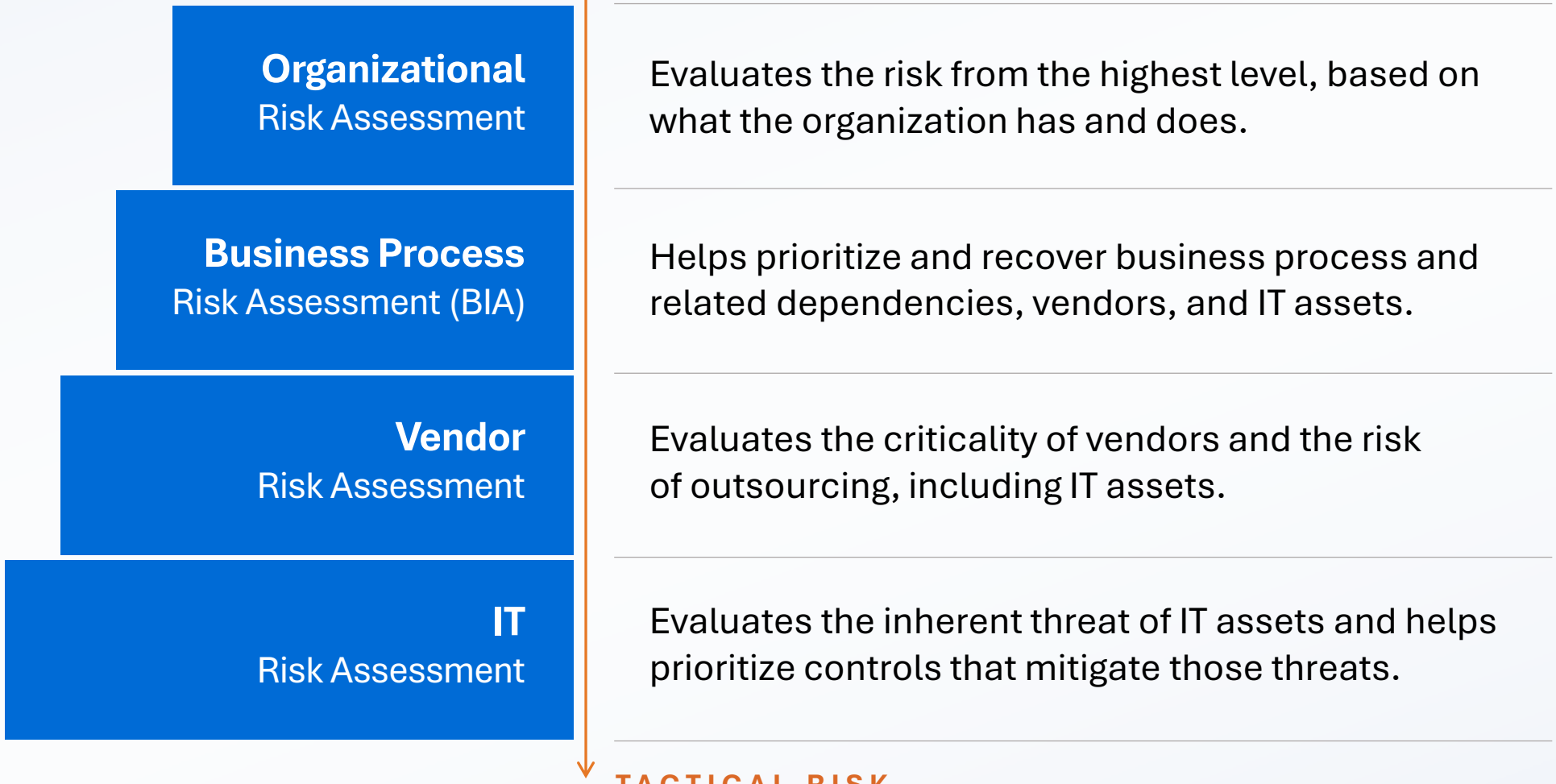
sheryl.ryan@sbscyber.com

432.413.1811

sbscyber.com

- Over 2 ½ years as a Senior Information Security Consultant for SBS Cybersecurity
- CISSP and CBSM Certifications
- GSB Bank Technology Security School
- Over 29 years of information technology and security experience in the banking, education, and oil and gas industries
- Spent over ten years as a bank Vice President and Information Security Officer

Risk Management Hierarchy



ROAD MAP

From subsurface data to surface operations

Five practical stops, built for technical professionals.

01 Why energy is targeted

02 What we must protect

03 How people are targeted

04 How incidents spread

05 What to do next

WHY ENERGY IS TARGETED

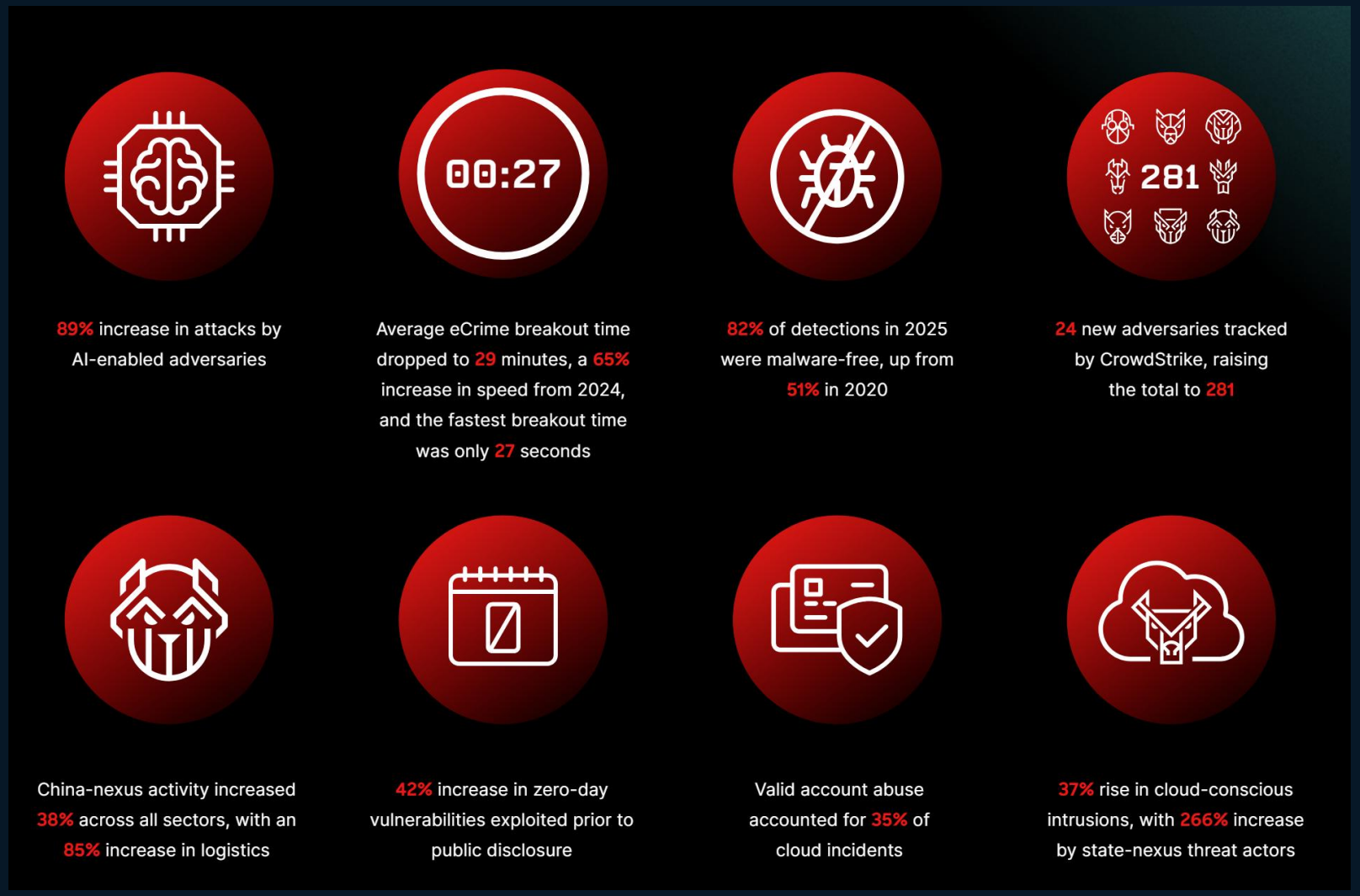
THREAT LANDSCAPE

Why attackers care about energy operations

High-value information, distributed assets, and operational pressure create leverage.

Ransomware	Extortion through downtime and data loss
Espionage	Theft of exploration, reservoir, or engineering data
Supply chain	A vendor connection becomes the path in
OT intrusion	Changes to configurations or operational visibility

The Statistics



2026 Crowdstrike Global Threat Report

More Statistics

USD 6.29M

Average cost of a breach in the financial services industry

Critical sectors face the brunt of AI-driven attacks, accounting for 62% of all AI-driven breaches studied. The two most targeted sectors were financial services and energy, where breach costs averaged USD 6.29 million and USD 5.2 million respectively. This targeting is a concerning trend. The concentration of AI-driven attacks across these two interdependent sectors creates a systemic risk. Disruptions in one organization can cascade into broader impacts across consumer finances, economic systems and power grids. On the plus side, both sectors are experienced at identifying and containing breaches, with approximately four weeks shorter average breach times than the global average.

IBM Cost of a Data Breach Report

Software and Hardware Vulnerability

Of 48,000+ CVEs Published in 2025, Only 58 Posed a Genuine Threat to Enterprise Supply Chains

Vendors Are Compromised 7 Days Before a CVE Exists

AI-Related CVEs Rose 34.6% in 2025

Ransomware, APTs, and AI-Enabled Attackers Targeting Supply Chains in 2025

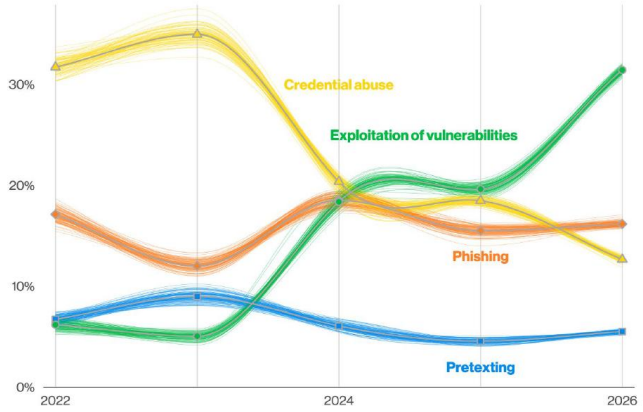


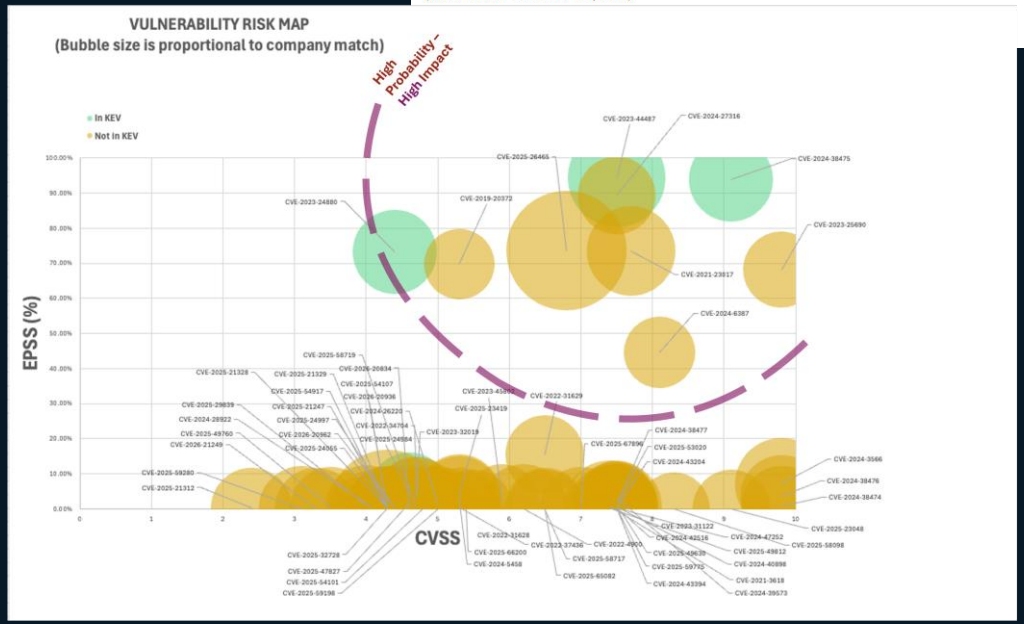
Figure 5. Known initial access vectors in non-Error, non-Misuse breaches over time (n for 2026 dataset=19,905)

Rise of vulnerability exploitation

Exploitation of vulnerabilities is now the most common initial access vector for breaches. It has risen to 31% in this year's reporting dataset, while credential abuse – the previous leader – is down to 13%.

Only 26% of critical vulnerabilities – defined as being in the Cybersecurity Infrastructure and Security Agency Known Exploited Vulnerabilities (CISA KEV) catalog – were fully remediated by organizations in 2025, a drop from the previous year's 38%.

The median time for full resolution went up to 43 days, almost two weeks more than the previous year's 32 days. In the median case, organizations had 50% more critical vulnerabilities to patch in this year's reporting dataset compared to the previous year.

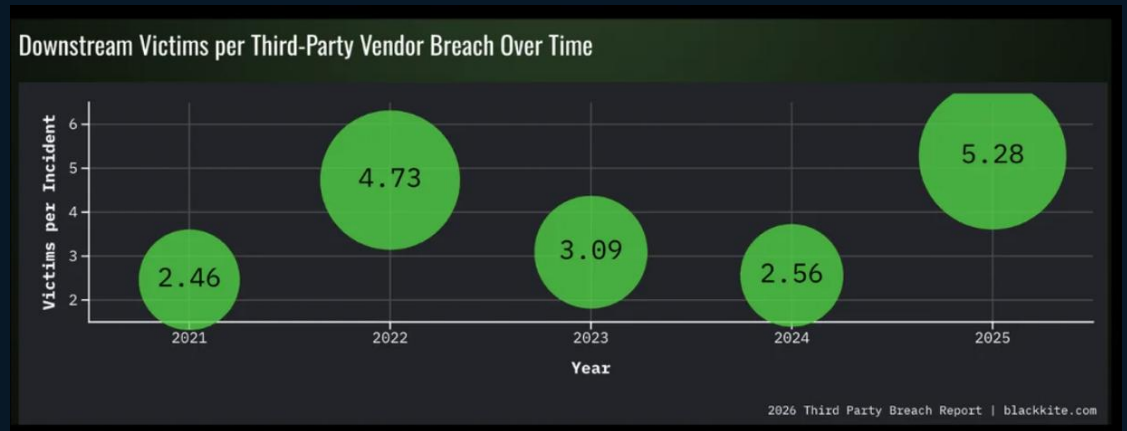


[Key Findings From the 2026 Supply Chain Vulnerability Report]

Third-Party Breach - The Rule of Three

The third-party metric combines three different kinds of business relationship archetypes, where the initial access happens, and where the data that was breached was stored.

- Vendor in an organization’s software supply chain
- Vendor hosting an organization’s data in its environment
- Vendor with a connection to an organization’s environment



719

named victim companies

Verified incidents reached **136** events, with **719 named victim companies**, and a much larger hidden layer behind aggregate disclosures.

~26,000

additional affected companies

Publicly disclosed impact reached 433M people, while vendors reported ~26,000 additional affected companies without naming them.

Ransomware: More Than a Computer Problem

What Is Ransomware?

In a nutshell, it’s extortion.

Ransomware is a type of cyberattack where criminals lock, encrypt, or steal information and then demand payment to restore access or prevent the release of stolen data.

Ransomware attacks can have significant downstream impacts on operations and critical services.

Ransomware: More Than a Computer Problem

How Does It Usually Start?

- A phishing email
- A compromised vendor
- A weak password
- An exposed remote access connection
- Unpatched systems

Email phishing, ransomware, and third-party risks continue to be among the most common cyber threats facing organizations.

WHAT WE MUST PROTECT

CROWN JEWELS

What petroleum professionals uniquely protect

Information has operational, competitive, and safety value.

- Seismic interpretation
- Reservoir models
- Well logs and drilling plans
- Production forecasts
- Field configurations
- Research and intellectual property

If it would be expensive, dangerous, or difficult to recreate, treat it as a crown jewel.

CONNECTED OPERATIONS

IT + OT + field technology

The boundary is no longer a wall. It is a managed set of connections.

Every connection creates value…

…and must be understood, authorized, monitored, and recoverable.

Know what is connected and why.

WHY ARE PEOPLE TARGETED

HUMAN ELEMENT

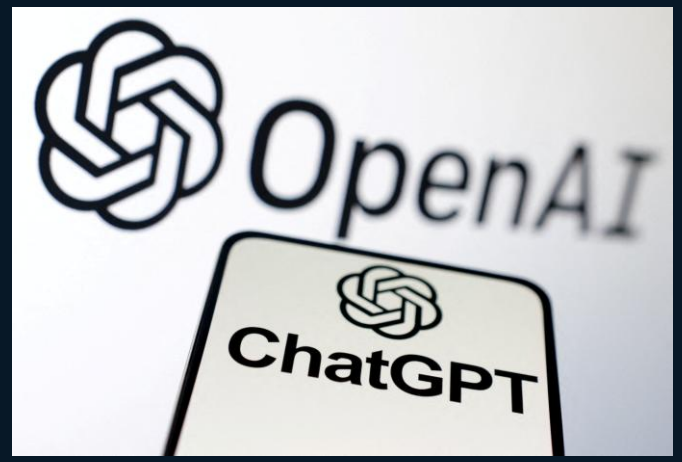
Phishing wears a hard hat

The best lures look like routine work.

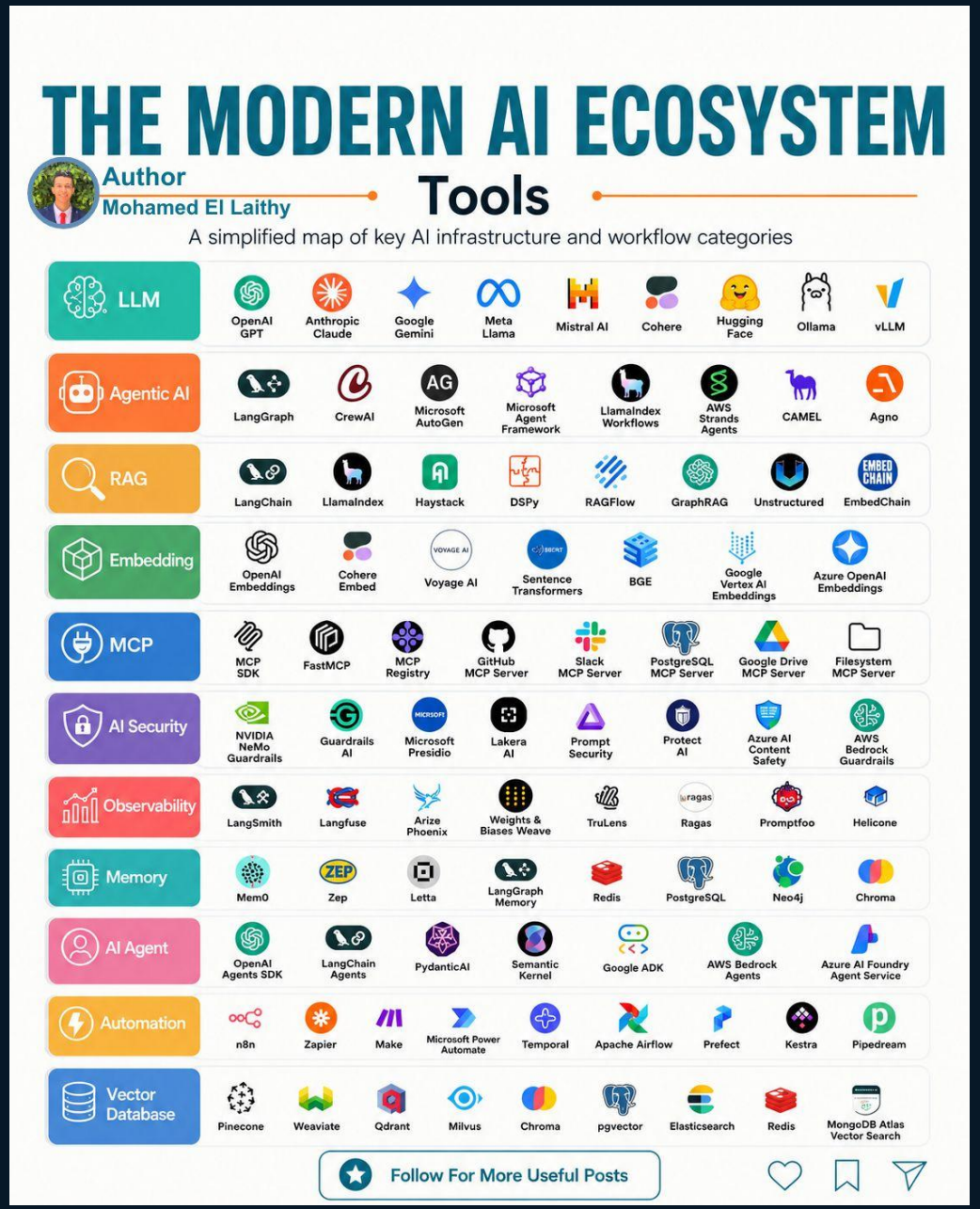
“Updated drilling program attached”	Unexpected attachment
“Vendor needs remote access now”	Urgency + access
“Shared seismic file expires today”	Cloud-sharing lure
“Executive approved this payment”	Authority pressure

Pause • Verify • Report

When I say “AI” you probably think of this?



What it really is:



EMERGING DECEPTION

AI makes social engineering faster and more convincing

Trust the process, not the voice, face, or writing style.

VOICE

A familiar leader requests an urgent action

VIDEO

A convincing caller joins a virtual meeting

TEXT

Highly tailored messages reference real projects

Verification rule: unusual + urgent + sensitive = use a second channel

Deepfakes: How Do We Know Who's Who?

How do we know who’s who?

🎤 Voice Deepfakes

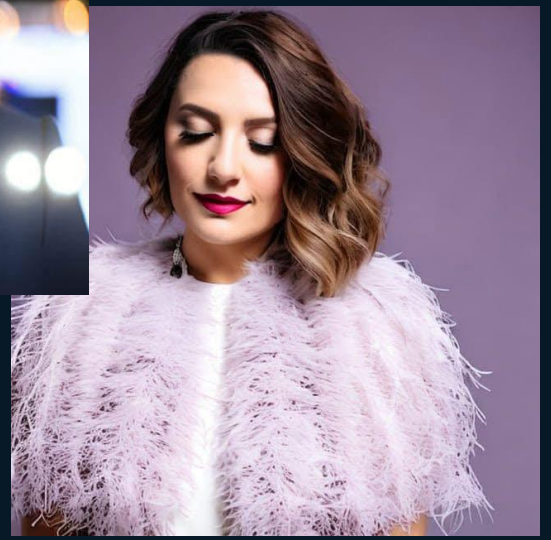
- Unusual urgency or pressure
- Requests that bypass normal procedures
- Slightly unnatural pauses or speech patterns
- Asking for sensitive information, money, or access

🎥 Video Deepfakes

- Poor lip synchronization
- Unnatural facial movements
- Blurred edges around the face
- Unusual lighting or visual distortions

📧 AI-Generated Messages

- Unexpected requests from executives
- Changes to established processes
- Requests for credentials, payments, or confidential data
- Communication outside normal channels
- Trust the Process, Not the Person



Deepfakes: How Do We Know Who's Who?

Verify unusual requests through a second communication channel

- Call a known phone number
- Confirm verbally with a supervisor
- Follow approval workflows

Never bypass procedures because a request appears to come from a trusted person

The Three-Question Test
Before taking action ask:

- Is this unusual?
- Is this urgent?
- Is this asking for something sensitive?

If the answer is yes to all three, STOP and verify.

[Deepfakes in 2026: We Are Not Ready]
Perry Carpenter from KnowBe4

HOW INCIDENTS SPREAD

What happens if your systems go offline tomorrow?

A cyber event can become an operational event in minutes.

1 **SAFETY**

Could operators trust alarms, setpoints, and field data?

2 **PRODUCTION**

Could teams monitor, control, or restore output?

3 **DECISIONS**

Could engineers rely on models and current operating data?

Cybersecurity is part of operational risk management, not just an IT concern.

SCENARIO

03:00: production monitoring becomes unavailable

Ransomware is suspected. Equipment status is uncertain.

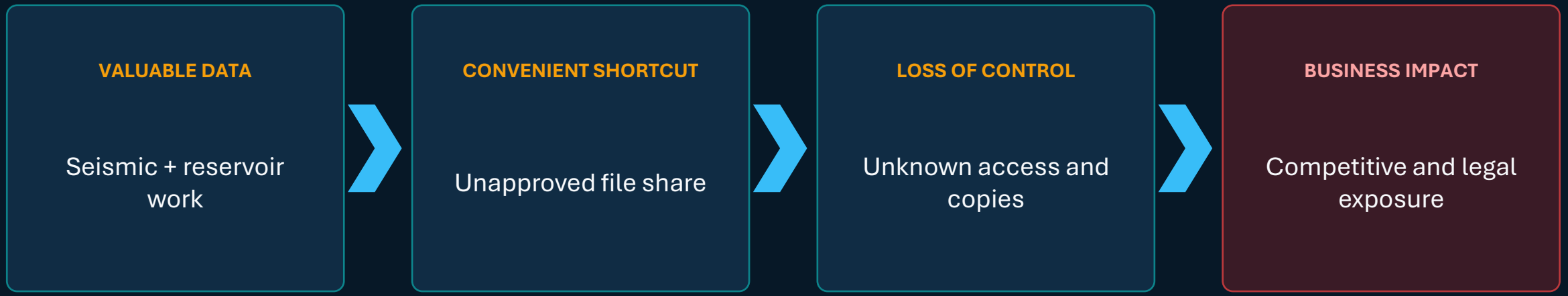
1. What must remain safe?
2. What can operate manually?
3. Who has the authority to make decisions?
4. How do we communicate if normal tools fail?

First priority: protect people and the physical process.

SCENARIO

A competitor has your subsurface advantage

A geoscience project folder was shared outside the approved platform.

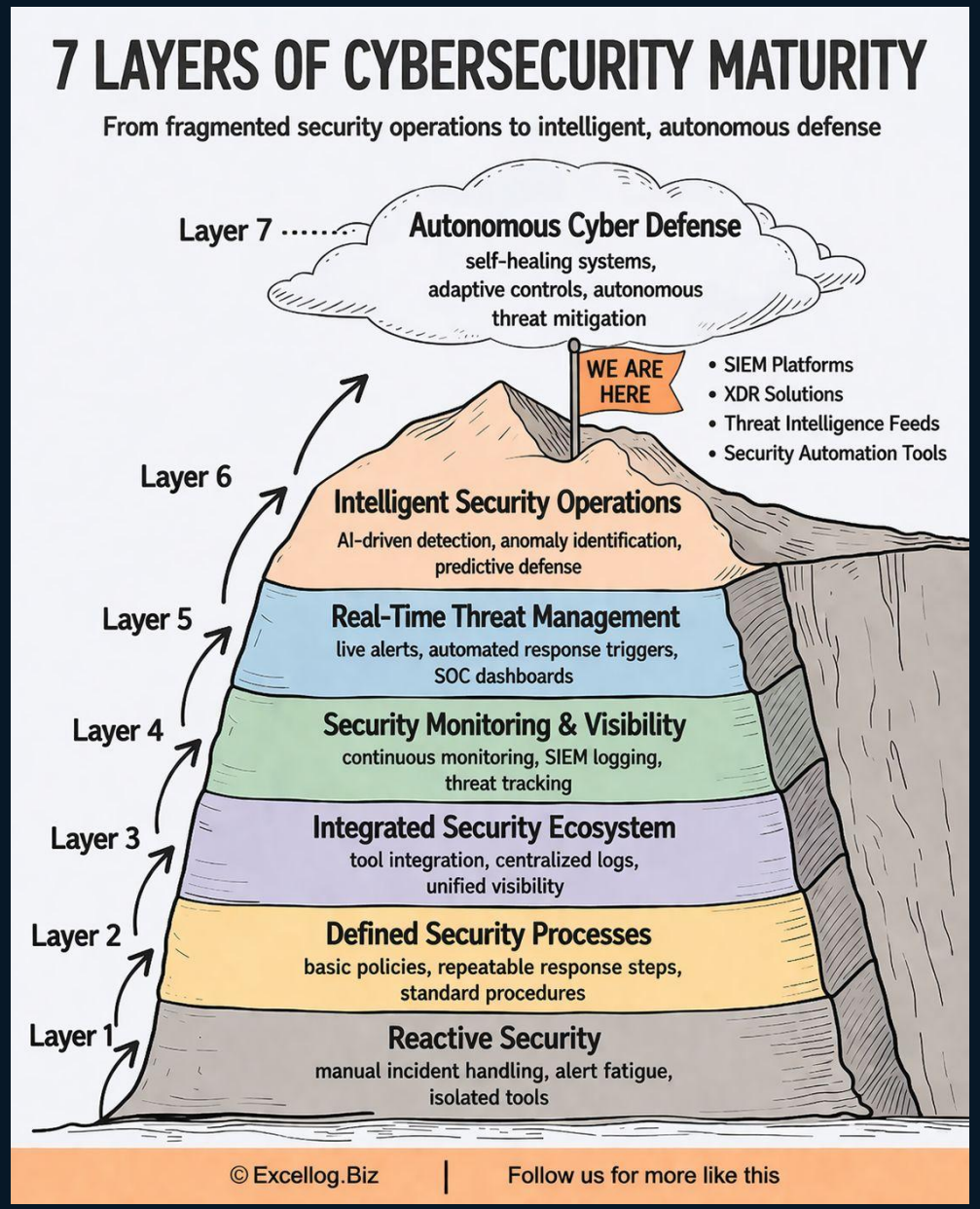


Before sharing: confirm data classification • recipient • platform • retention

WHAT TO DO NEXT

“We are trying to govern machine-speed systems with human-speed controls.”

“We’re no longer operating on human time. We’re operating on machine time.”



Cybersecurity Controls Your Organization Should Have

Identity & Access Controls

- Multi-Factor Authentication (MFA)
- Strong password management
- Periodic access reviews
- Privileged account controls for administrators
- Vendor and contractor access management

Data Protection Controls

- Encryption of sensitive data
- Secure file sharing and collaboration tools
- Data classification programs
- Backup and recovery capabilities
- Protection of geological and engineering intellectual property

Cybersecurity Controls Your Organization Should Have

Human Controls

- Annual security awareness training
- Phishing testing and education
- Incident reporting procedures
- Data handling and classification training
- Clear acceptable-use policies

Governance & Risk Controls

- Cybersecurity risk assessments
- Vendor risk management program
- Incident response plan
- Business continuity and disaster recovery planning
- Executive and/or Board oversight
- Establish AI governance policies covering acceptable use, security, privacy, and data handling.

Cybersecurity Controls Your Organization Should Have

Monitoring & Detection Controls

- Security monitoring (SOC)
- Security Information and Event Management (SIEM)
- Endpoint Detection & Response (EDR/XDR)
- Intrusion Detection / Prevention Systems (IDS/IPS)
- ***Continuous vulnerability management***

Operational Technology (OT) Controls

- Asset inventories
- Network segmentation between IT and OT
- Monitoring of remote access connections
- Change management for control systems
- Incident response procedures for operational disruptions

6 Questions Everyone Should Ask Their IT Team or Managed Service Provider

- If ransomware hit us today, how quickly could we recover?
- How are our seismic, reservoir, and drilling data protected?
- Who has remote access to our systems and field operations?
- How would I know if something suspicious was happening?
- What should I do if I receive a suspicious email, phone call, or request?
- Are we using a public AI service, or an enterprise instance governed by our organization?

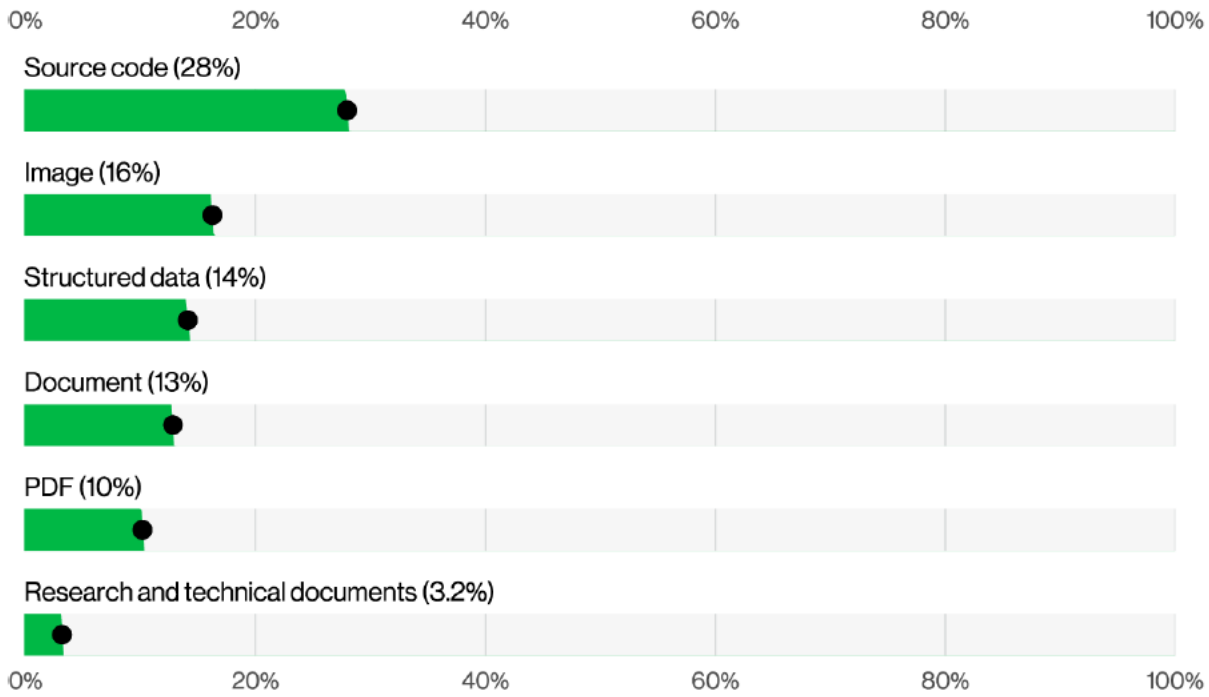


Figure 9. Select data types in untrusted DLP events targeting generative AI tools (n=858,440)

Shadow AI policy violations and malicious insiders

Regarding usage of unauthorized GenAI services ("Shadow AI"), 67% percent of users are using non-corporate accounts on their corporate devices to access AI services, a slight decrease from the previous year. However, 45% of employees are now considered regular users of AI (authorized or not) on their corporate devices, up from 15% in the previous year.

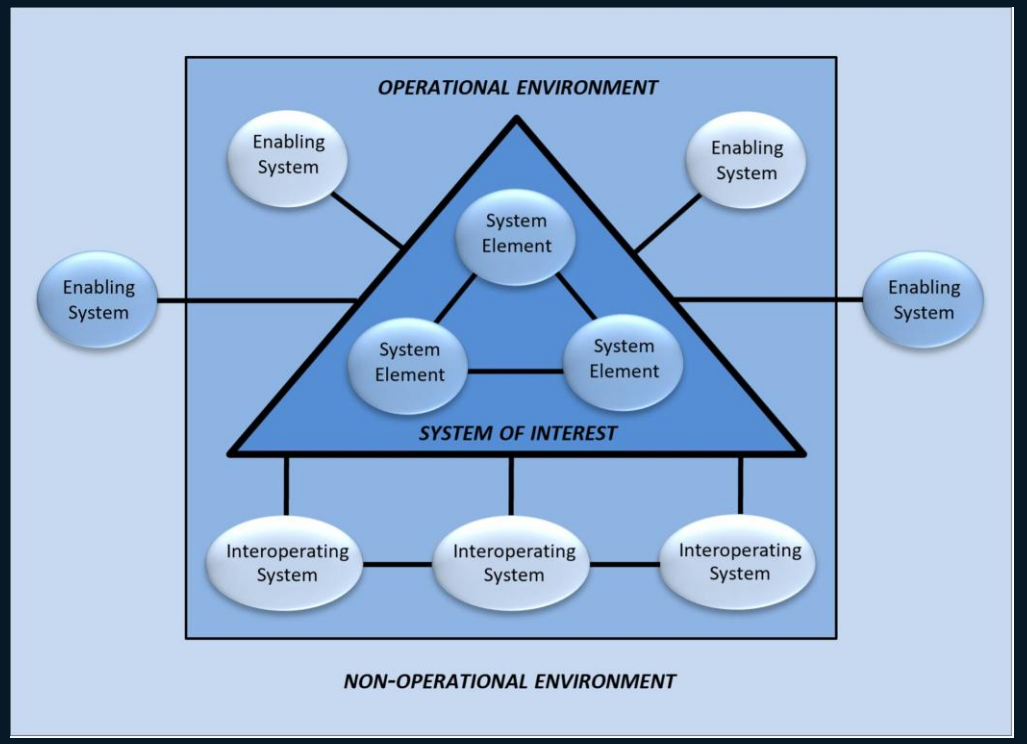
Shadow AI is now the third most common non-malicious insider action detected in our data loss prevention (DLP) dataset in 2025, a fourfold increase in percentage from the previous year.

The most common type submitted to external GenAI models was source code, followed by images and other types of structured data. In 3.2% of DLP policy violations, we even found research and technical documentation being uploaded to those unauthorized AI systems, which presents a risk of intellectual property exposure.

Third-Party Vendors - Why They Matter

Your Security Is Only as Strong as Your Connections

- Geophysical processing firms
- Reservoir modeling providers
- Cloud software providers
- Field service contractors
- Equipment manufacturers
- Managed IT and cybersecurity providers



Many cyber incidents begin through a trusted third party rather than a direct attack.

THIRD PARTIES

Trust is not a control

Contractors and vendors need the right access for the right time.

VERIFY	Confirm the person and purpose
LIMIT	Use minimum necessary access
TIME-BOX	Remove access when work ends
MONITOR	Report unusual requests or behavior

Questions Your Organization Should Ask Vendors

- How do you protect our data?
- Who can access our information?
- How do you detect and respond to cyber incidents?
- Can you demonstrate security?

Third-Party Vendors – Red Flags

A vendor that:

- Refuses to share security information
- Has no incident response process
- Shares generic or outdated documentation
- Uses shared accounts
- Cannot identify who has access to your data
- Security responsibilities are undefined

ACTION PLAN

Five moves that reduce cyber risk today

Small professional habits reinforce operational resilience.

1. Pause before opening unexpected links or files
2. Verify urgent or unusual requests independently
3. Use approved tools for sensitive technical data
4. Protect credentials and require MFA where available
5. Report fast when something feels wrong

See it

↓

Stop it

↓

Report it

Cybersecurity is a Team Sport

- Your CTO or CIO and IT team manages technology.
- The CISO manages risk and sets the direction.
- Your Managed Service Providers (MSP/MSSP) manage outsourced services.
- And every employee has a role to play.

You help protect operations by asking questions, reporting concerns and following secure practices.

Our **Offerings**

Our goal is to arm you with the knowledge, strategies, and guidance needed to protect your organization effectively, without worrying about compliance issues. This means you can focus on what you do best — running and growing your business.

SBS offers a wide variety of services, including:

- vCISO
- Incident Response
- Business Continuity
- Vendor Management as a Service
- Security Awareness Training
- FTC Safeguards Rule
- IT Audit
- Cybersecurity Essentials Assessment
- NIST CSF Assessment
- ACH Audit
- HIPAA Security Audit
- Cloud Security Assessment
- Microsoft 365 Hardening Assessment
- Network Security Audit
- Penetration Testing
- Vulnerability Assessments
- Social Engineering
- Incident Readiness Assessments
- Red Team Services

SBS CyberSecurity

is a top-rated consulting and audit firm. With over 20 years in the cybersecurity industry, SBS has provided solutions to thousands of regulated organizations across the United States and abroad.

Clients Love Us

- Over 20 years in the cybersecurity industry
- 1,500+ organizations using TRAC in over 40 states
- Average 525+ monthly Hacker Hour webinar registrants
- 2,500+ certifications issued through the SBS Institute

Additional Resources

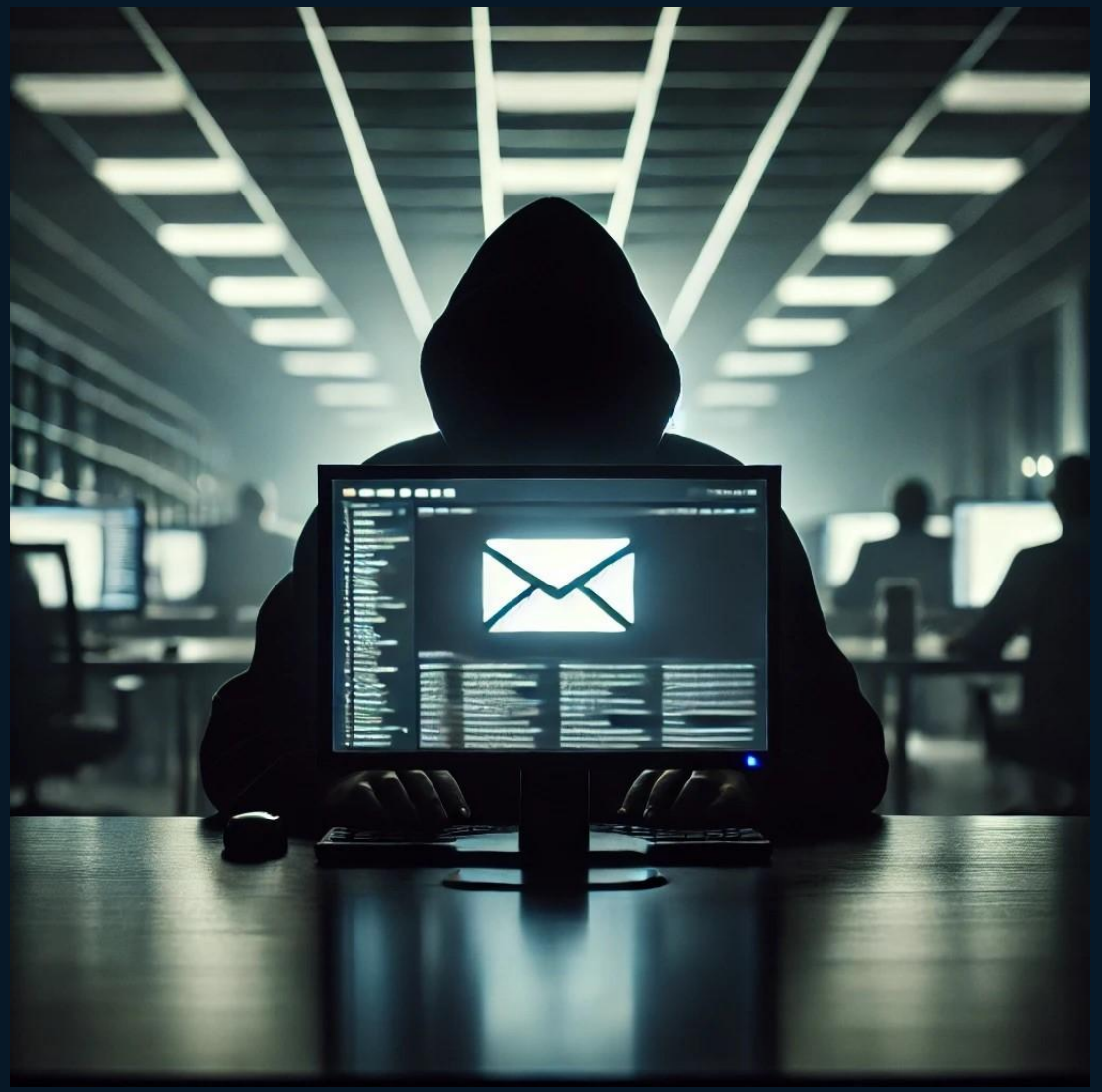
SBS Cybersecurity Blog: Cybersecurity News, Expert Tips, and Industry Trends

Cost of a Data Breach Report 2026 | IBM

2026 Data Breach Investigations Report (DBIR) | Verizon

CrowdStrike 2026 Global Threat Report

Cyber Guidance for Small Businesses | CISA



YOU ARE PART OF THE SAFETY SYSTEM

Cybersecurity protects:

People

Environment

Production

Technical advantage

Questions & discussion

sbscyber.com

Follow SBS