CYBERSECURITY IN CONSTRUCTION & REAL ESTATE

HOW TO MITIGATE RISKS FROM RANSOMWARE, SOCIAL ENGINEERING, AND BEYOND.

WEBINAR: November 12, 2024

PBMares SM
CPAs and Consultants

Today's Presenters

Jennifer French,
CPA

Partner, Construction & Real Estate Team Leader

Antonina K. McAvoy,
CISA, CISM, QSA, PCIP

Partner, Cybersecurity & Risk Advisory Services

2024 Cyber Threat Landscape: Navigating Risks

Construction and real estate companies face diverse cyber threats in 2024, necessitating proactive defense measures.

- **Ransomware:** Increasing attacks disrupt services and extort data.
- **Phishing and Social Engineering:** Target employees for data theft.
- **Supply Chain Vulnerabilities:** Increased risks from interconnected networks.
- **Emerging Technologies Threats:** AI and quantum computing vulnerabilities emerge.

Spotlight – Latest Cyber Attacks Capturing Headlines:

Construction Dive
Skender hit by ransomware attack
The Chicago-based builder disclosed the breach, which affected 1,067 people, in a filing with the Maine Attorney General's office on April 5...
Apr 10, 2024

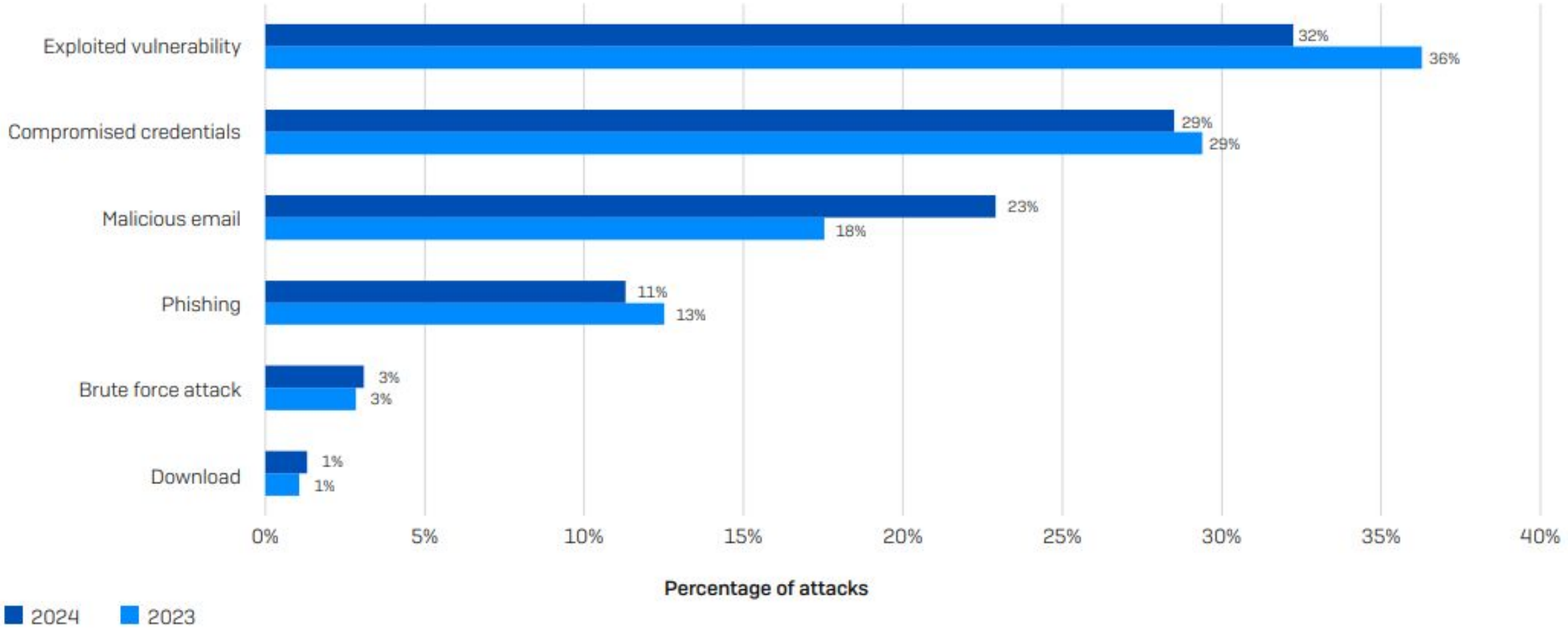
futuredigital360.com
https://futuredigital360.com › real-estate-giant-marcus-...
Real estate giant Marcus & Millichap has suffered a ...
Real estate giant Marcus & **Millichap** has **suffered** a ransomware **attack**. Suspected to be the work of the BlackMatter ransomware gang, the firm disclosed in an SEC ...

Infosecurity Magazine
Research Shows IT and Construction Sectors Hardest Hit By Ransomware
New research has shed light on the profound impact of ransomware attacks on the IT and construction sectors, revealing that these industries bore the brunt of...
Mar 19, 2024

Planning, BIM & Construction Today
Construction industry faces growing cybersecurity risks amid digital transformation
There's an urgent call for construction businesses to implement robust measures that will prevent and protect them against cybersecurity risks.
Jun 18, 2024

Ransomware Rampage

Root Causes of Ransomware Attacks (2023 – 2024)



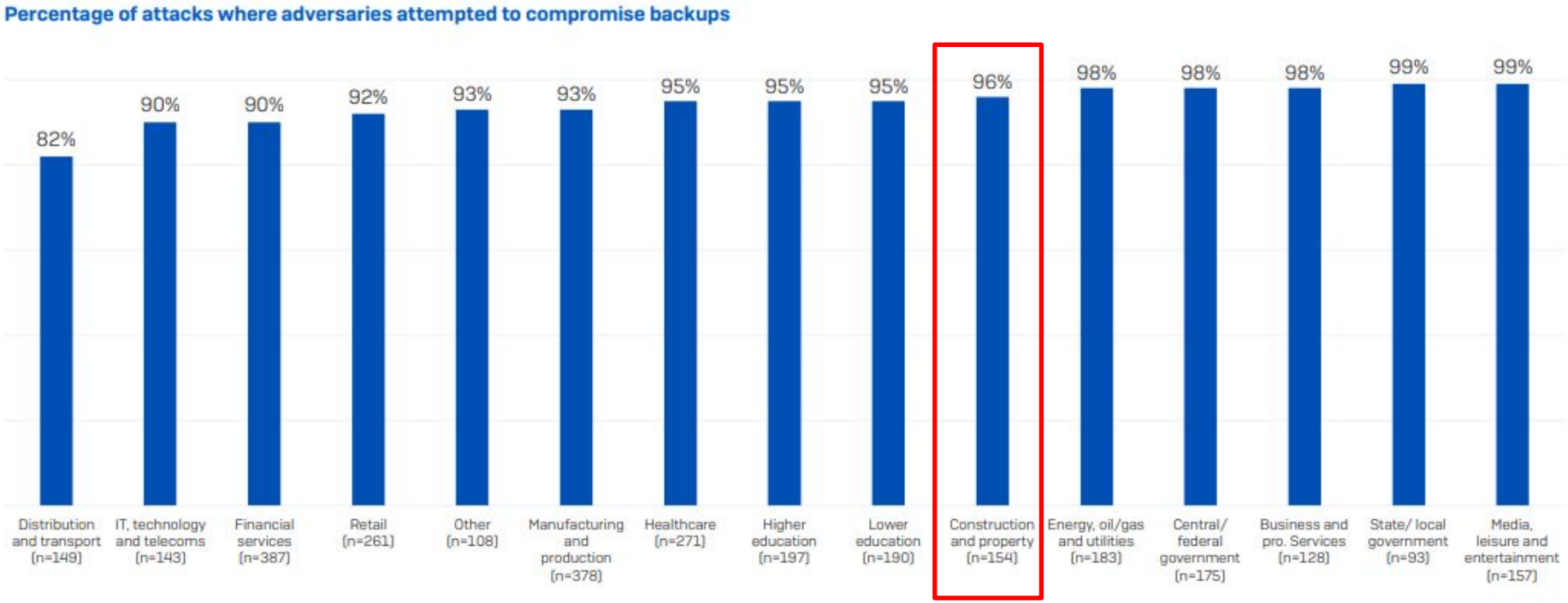
Source: The State of Ransomware 2024 by Sophos, April 2024.

Data Recovery and Propensity to Pay the Ransom

In ransomware attacks, organizations have two main options for recovering encrypted data: restoring from backups or paying the ransom. Compromised backups limit recovery options, increasing pressure to pay.

- 34% paid ransom, 75% relied on backups.
- Backup usage rose from 63% in 2022 to 75% in 2023.

Spotlight (construction): 96% retrieved encrypted data

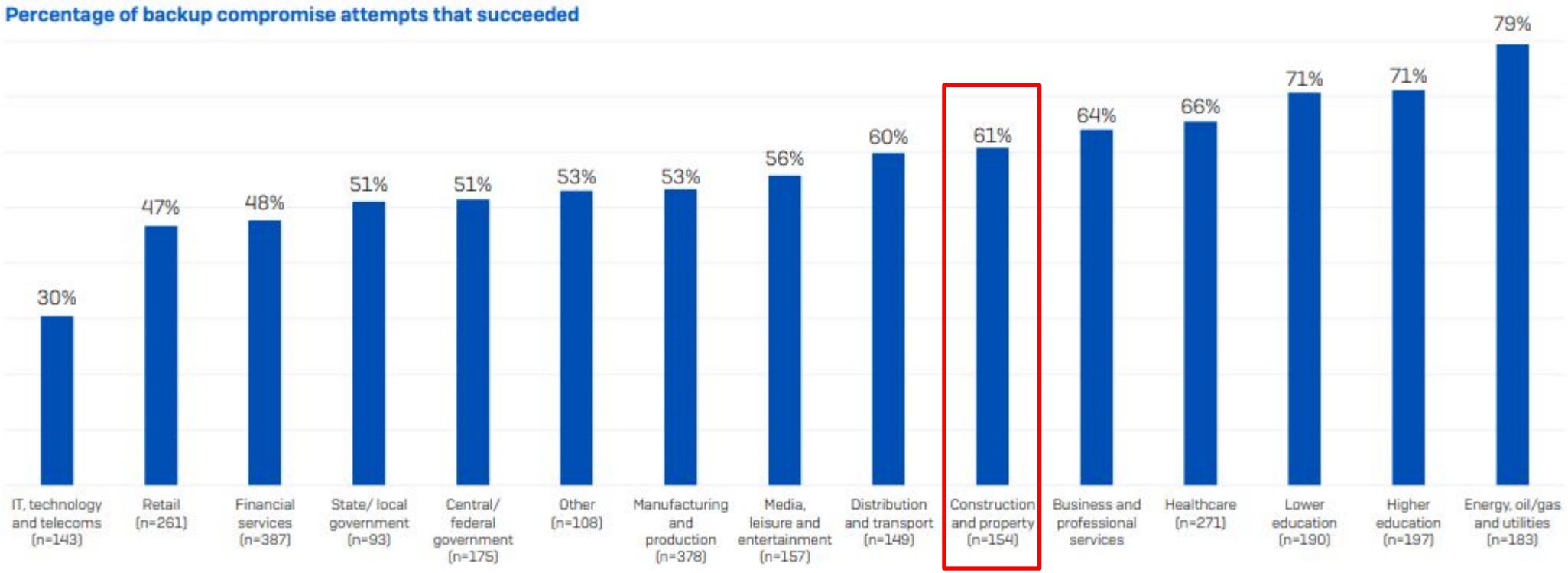


Source: The State of Ransomware 2024 by Sophos, April 2024.

Success Rate of Backup Compromise Attempts

Across all sectors, an average of 57% of backup compromise attempts were successful and adversaries were able to impact the ransomware recovery operations of over half their victims.

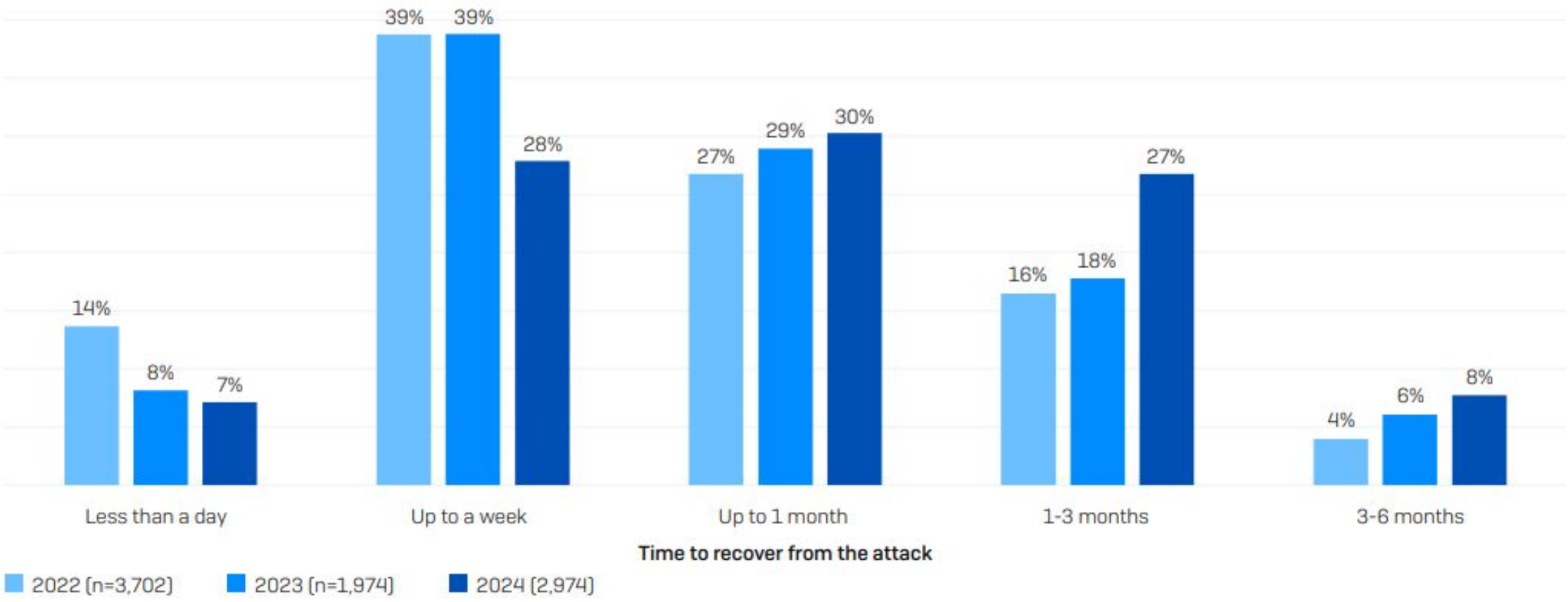
Spotlight: Ensure strong backup protection in place and sufficient technology to detect and stop an attempted compromise before the attackers succeed.



Source: The State of Ransomware 2024 by Sophos, April 2024.

Recovery Time

The time taken to recover from a ransomware attack is getting steadily longer. The slowdown may indicate more complex attacks, requiring extensive recovery, and a lack of preparation.

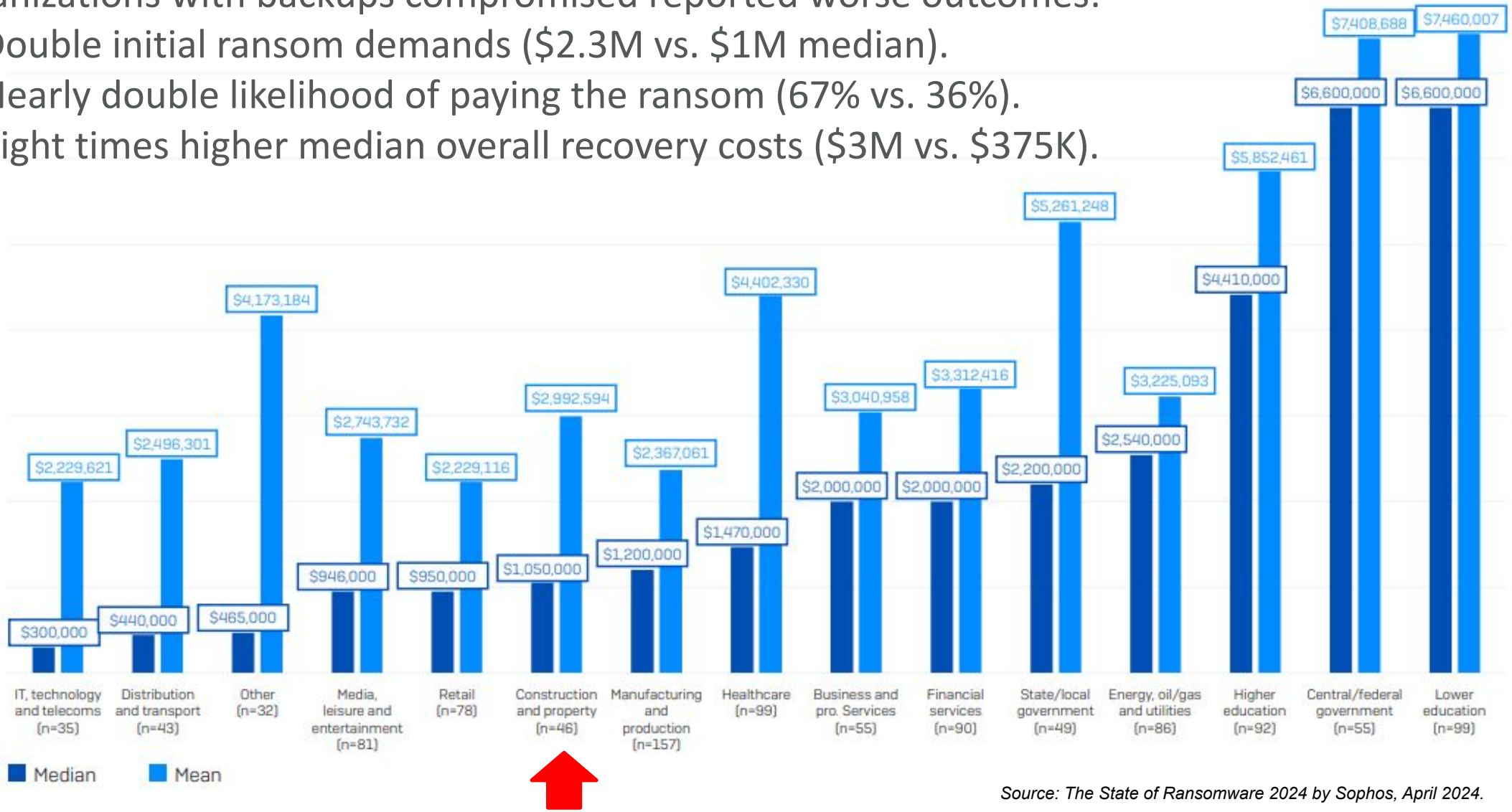


Source: The State of Ransomware 2024 by Sophos, April 2024.

Ransom Payment by Industry

Organizations with backups compromised reported worse outcomes:

- Double initial ransom demands ($2.3M vs. $1M median).
- Nearly double likelihood of paying the ransom (67% vs. 36%).
- Eight times higher median overall recovery costs ($3M vs. $375K).



Source: The State of Ransomware 2024 by Sophos, April 2024.

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, organizations reported a mean cost to recover from a ransomware attack of $2.73M, an increase of almost $1M from the $1.82M reported in 2023 (downtime, people time, device cost, network cost, lost opportunity, etc.).

2021	2022	2023	2024
$1.85M	$1.4M	$1.82M	$2.73M

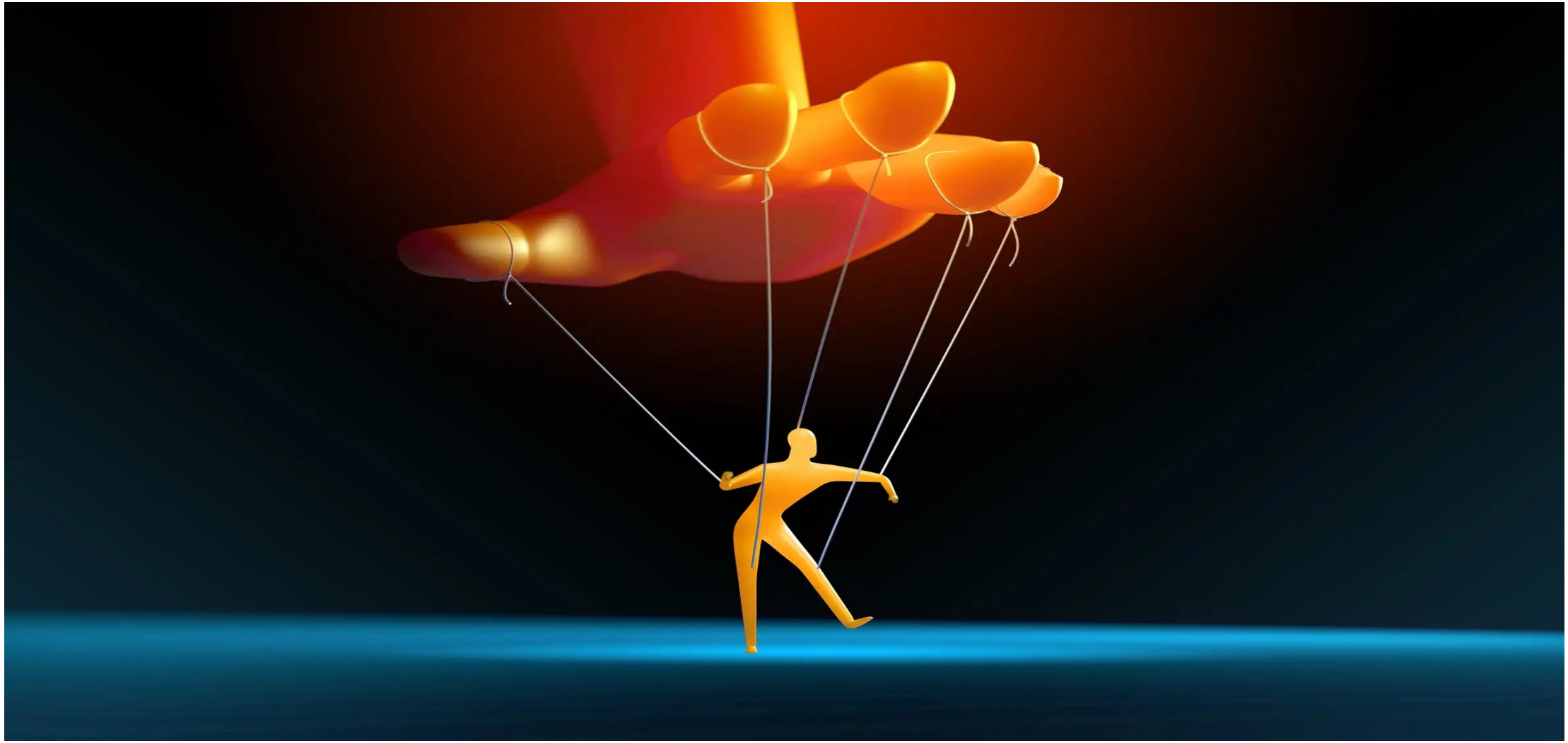
Source of ransom payment funding

Source: The State of Ransomware 2024 by Sophos, April 2024.

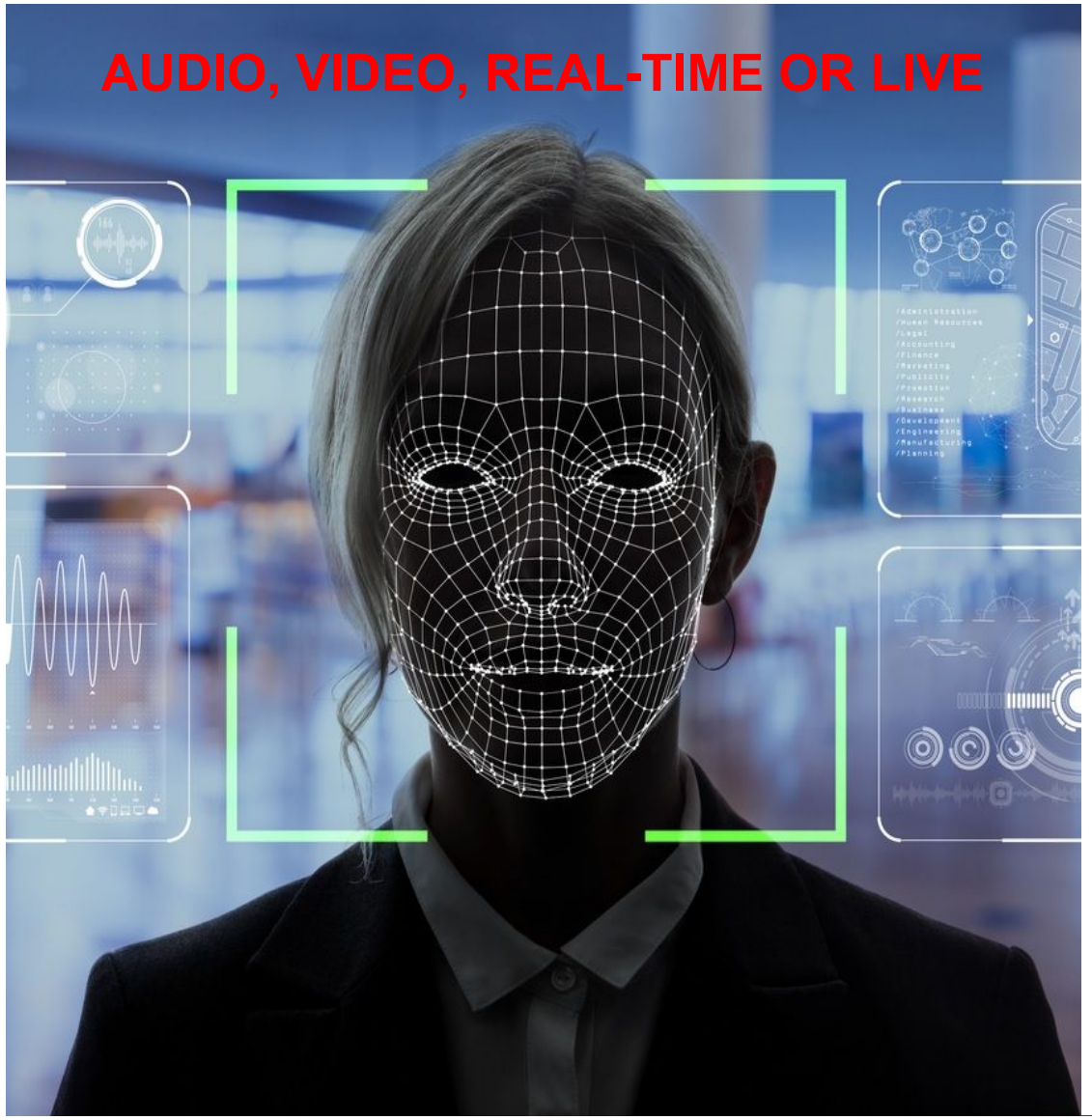
Spotlight: A look back at four cyber attacks.

City	Demand	Method	Paid	Estimated Costs
Atlanta, GA	$51,000	Bitcoin	No	$12 - $17 million
Baltimore, MD	$75,000	Bitcoin	No	$10 - $18 million
Lake City, FL	$490,421	Bitcoin	Yes	$10,000
Denver, CO	$51,000	Bitcoin	No	$1.5 million

Phishing & Social Engineering



Evolution of Threats: Deepfake Phishing



Risks Posed by Deepfake:

- Deepfakes can mimic the voices and appearances of trusted individuals, making it challenging to discern authentic communication from fraudulent ones.
- Increased risk of identity theft, financial fraud, and reputational damage due to the proliferation of deepfake content.

Detecting Deepfakes

- Implementing robust detection mechanisms is crucial to identify and mitigate the threat posed by deep-fakes.
- Utilize AI-powered tools specifically designed to analyze audio and video content for signs of manipulation or inconsistency.

Beware of Smishing

Protect yourself from smishing attacks by staying alert and cautious when receiving unexpected text messages. Your vigilance is your best defense against cyber threats.

- **Deceptive Tactics:** Attackers impersonate trusted entities, such as banks or government agencies, to deceive recipients.
- **Urgency:** Messages create a sense of urgency, urging recipients to take immediate action.
- **Risk:** Clicking on links or providing personal information can lead to identity theft, financial loss, or malware infections.

Supply Chain Vulnerabilities

Third Party Software Vulnerabilities

Third party software developed and maintained by external vendors.

Risks:

- Vulnerabilities in third-party software can be exploited by cybercriminals to gain unauthorized access to networks, systems, and sensitive data.
- Common vulnerabilities include unpatched software, insecure configurations, and inadequate authentication mechanisms.

Protective Measures:

- Vendor risk assessments
- Continuous monitoring
- Contractual agreements
- Patch management
- Secure integration practices

Contracts: Navigating IT Considerations for Success

Vendor contracts must meet security and privacy standards for third parties handling confidential data or critical services.

Management considerations for contract inclusion:

- Contracts ensure third-party responsibility for institution's data security;
- Third-party security controls validated by independent party;
- Recourse defined for security requirement breaches;
- Responsibilities outlined for incident response timing;
- Data return/destruction terms upon contract end;
- Formal device management responsibilities documented;
- Geographic limits on data storage/transmission specified.

Inadequate Security Practices Among Suppliers

Suppliers or key vendors may have varying security which can impact overall supply chain security.

Risks:

- Weak passwords, lack of encryption, insufficient backup frequency or backup restore testing, backup replication, and other security gaps can leave systems vulnerable to attacks.

Protective Measures:

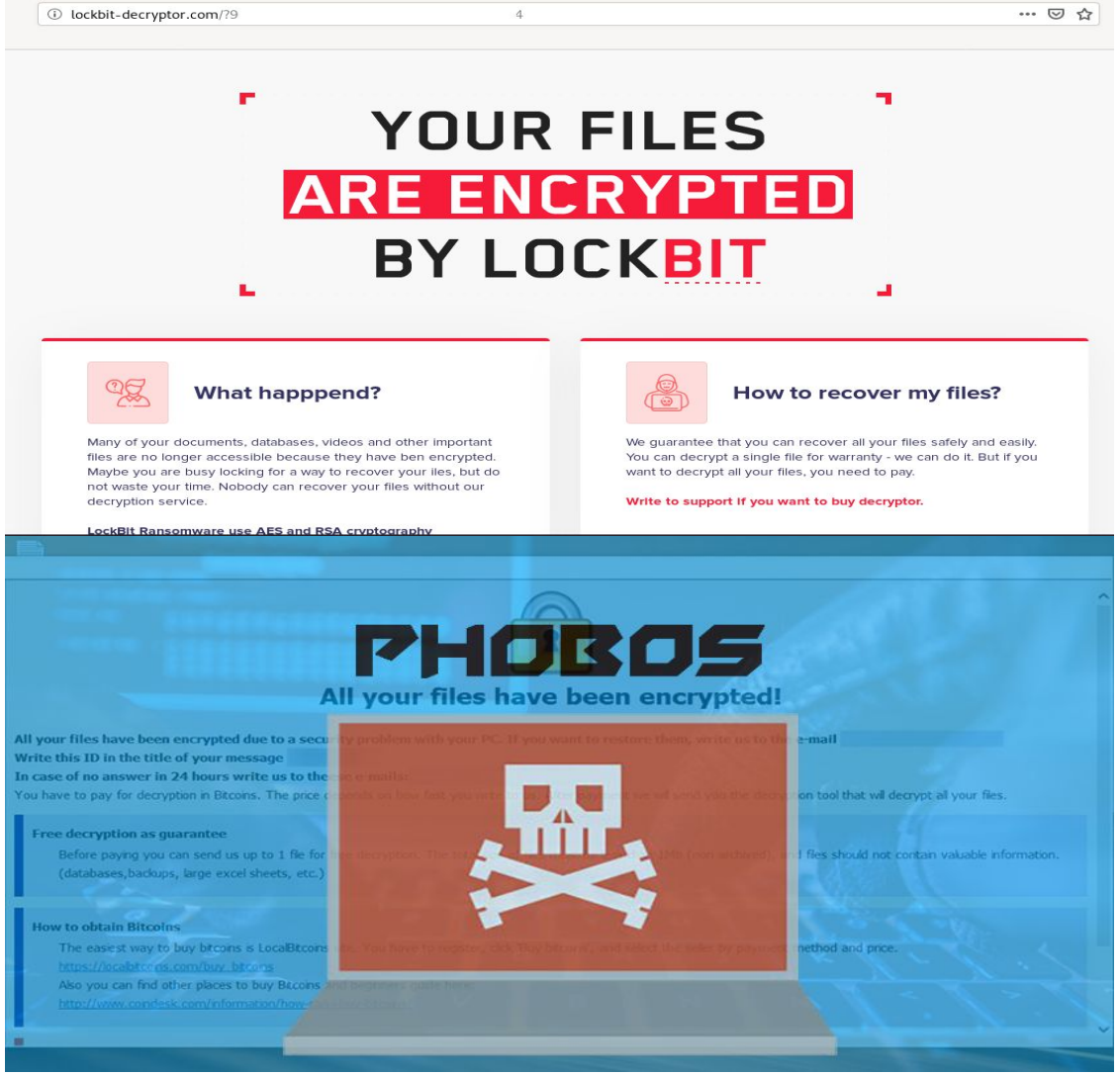
- Establish clear standards for suppliers
- Conduct assessments
- Implement appropriate controls

Emerging Technologies & Threats

AI: Cybersecurity's Double-Edged Sword

- **Adversarial Attacks:** Threat actors exploit AI vulnerabilities, compromising system integrity.
- **Bias and Discrimination:** AI algorithms perpetuate biases, leading to unfair outcomes.
- **Privacy Concerns:** AI systems access vast data, raising privacy infringement risks.
- **Over-reliance on Automation:** Blind reliance on AI can lead to neglect of manual oversight.
- **Lack of Explainability:** AI's black-box nature hinders understanding and accountability.
- **Cybersecurity Arms Race:** Rapid AI advancement fuels a cycle of innovation between defenders and attackers.
- **Regulatory Compliance:** Compliance complexities arise, requiring alignment with **NIST AI framework** guidelines for ethical and responsible AI use.

LockBit vs. Phobos: Ransomware Showdown



AI is redefining ransomware phishing tactics.

Prevalence of Phishing

- Phishing, like that employed by LockBit and Phobos ransomware, is widespread due to exploiting human vulnerabilities.

Evolution of Phishing

- Phishing emails are becoming increasingly difficult to detect, aided by generative artificial intelligence (AI).

Generative AI's Role

- Generative AI contributes to creating highly convincing phishing emails.

What’s At Stake?

What’s at Stake: Common Data Types

Protecting sensitive data is crucial for the construction industry, especially as companies handle increasing amounts of digital information and client interactions.

- **PII (Personally Identifiable Information):** Protects sensitive data such as names, addresses, and SSNs of employees, clients, and subcontractors; requires stringent security measures.
- **PHI (Personal Health Information):** Safeguards health information of workers, ensuring confidentiality in health records and wellness programs.
- **FTI (Federal Tax Information):** Requires compliance to secure sensitive tax-related data from employees and subcontractors.
- **CJIS:** Ensures the security of criminal background checks and information for workers on government projects.
- **FERPA:** Relevant when working on educational construction projects, protecting student records.
- **PCI:** Establishes standards for securing payment card data when handling client payments for projects or services.
- **CMMC (Cybersecurity Maturity Model Certification):** Mandatory for contractors working with the Department of Defense, ensuring compliance with specific cybersecurity practices to protect Controlled Unclassified Information (CUI).
- **OSHA (Occupational Safety and Health Administration):** Although focused on worker safety, OSHA compliance increasingly involves protectin
- **GDPR (Ge** ts, requiring

Assets						Data Attributes							Data Classification Attributes		
						Does the system contain...? (Y/N)									
#	Functional Area	Business Process	Sub-Process	Application or System	System Owner	Personally Identifiable Information (PII) data elements?	Protected Health Information (PHI) data elements?	Federal Tax Information (FTI) data elements?	Criminal Justice Information System (CJIS) data elements?	Family Educational Rights and Privacy Act (FERPA) data elements?	Payment Card Industry (PCI) data elements?	Please list all sensitive data elements.	Data Protection	Backup Frequency	Data Retention
1															
2															
3															

Spotlight

Fortifying Your Digital Fortress

Unleashing Defense Strategies

Ransomware Defense Best Practices for Construction:

- ***Utilize Security Tools:*** Cover common attack vectors like phishing and malware.
- ***Endpoint Protection:*** Safeguard devices with anti-exploit capabilities.
- ***Zero Trust Access:*** Prevent unauthorized credential use.

Adapt with Technology:

- Deploy adaptive technologies to respond to attacks.
- Disrupt adversaries and buy time to protect critical systems

Ensure Continuous Detection:

- Establish 24/7 threat detection with Managed Detection and Response (MDR) services.

Prepare Against Attacks:

- Regularly backup data and practice recovery procedures.
- Maintain incident response and business continuity plans.
- Train staff on cybersecurity best practices and conduct risk assessments.

Maintain Hygiene:

- Regularly patch systems and review security configurations.

PBMares SM

CPAs and Consultants

www.pbmares.com

MARYLAND – Rockville NORTH CAROLINA – Morehead City • New Bern • Wilmington

VIRGINIA – Fairfax • Fredericksburg • Harrisonburg • Newport News • Norfolk • Richmond • Warrenton • Williamsburg

INSIDE public accounting TOP 100 FIRMS 2024

Forbes America's Best Tax & Accounting Firm 2023

Accounting Today Top 100 Firm & Regional Leader 2024

Accounting Today National Leader in Tax Specialty 2024

USA Today & Statista R America's Most Recommended TAX AND ACCOUNTING FIRMS

BEST of Accounting CLIENT SATISFACTION 2024 clearlyrated

THE TOP 50 CONSTRUCTION ACCOUNTING FIRMS 2024 CONSTRUCTION EXECUTIVE

Excellence in Achievement BOARDROOM Awards 2023