



# OFFICE OF INFORMATION SECURITY AND CYBER DEFENSE

EXPLORING EVOLVING CYBER  
THREATS, TRENDS, AND DEFENSE  
STRATEGIES

DEPUTY DIRECTOR ADAM MILLER

# AGENDA OVERVIEW



- Key Findings of 2024-2025
- Notable Cyber Incidents of 2024-2025
- Trends in Cybersecurity Defenses
- Future Outlook and Predictions



# GLOBAL THREAT REPORTS: WHAT THEY DO



## **Understanding Threat Landscape**

These reports help organizations grasp the current threat landscape, enabling better strategic planning and risk management.

## **Informed Decision-Making**

It aims to inform decision-makers about evolving threats, ensuring they are equipped to address potential risks effectively.

## **Guidance on Security Measures**

Reports provide guidance on enhancing security measures to protect organizations against identified threats.



# KEY FINDINGS OF 2024-2025

# THREAT LANDSCAPE OVERVIEW



China-nexus activity surged **150%** across all sectors, with a staggering **200-300%** increase in key targeted industries



Vishing attacks skyrocketed **442%** between the first and second half of 2024



Average eCrime breakout time dropped to **48 minutes**, with the fastest breakout observed at just **51 seconds**



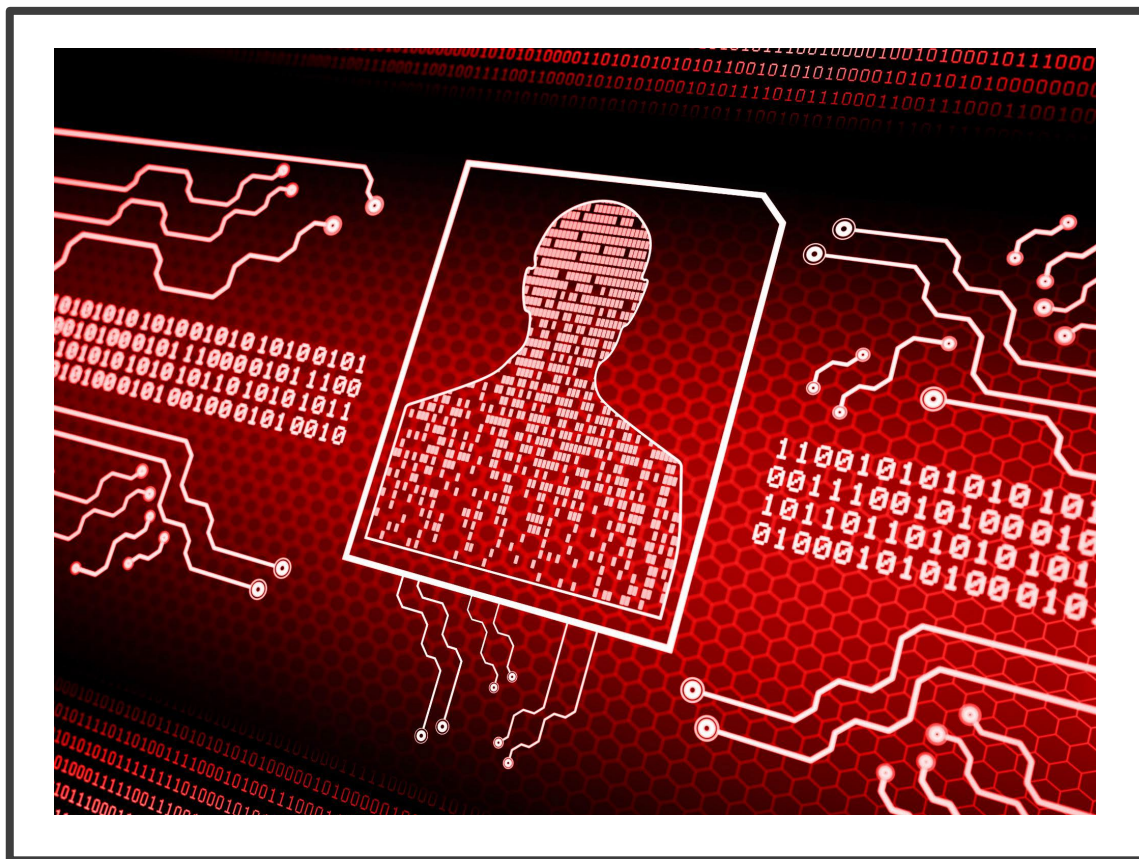
**79%** of detections in 2024 were malware-free, up from **40%** in 2019

# THREAT LANDSCAPE OVERVIEW

## Top 10 Industries Targeted by Interactive Intrusions



# MAJOR CYBER THREATS IDENTIFIED



## Ransomware Incidents

Ransomware incidents are characterized by harmful software that encrypts data, requiring a ransom for its decryption, and represent a major risk to businesses.

## Phishing and Vishing Attacks

Phishing attacks employ misleading emails or messages to deceive individuals into disclosing confidential information, marking them as a common cyber threat.

## Government-backed Espionage

Government-backed espionage refers to cyber operations executed by nations aimed at acquiring sensitive data from other countries or entities.



# EMERGING THREAT ACTORS AND TACTICS



## **Emerging Threat Actors**

New threat actors are continuously emerging in the cybersecurity landscape, utilizing innovative and sophisticated tactics.

## **Innovative Tactics**

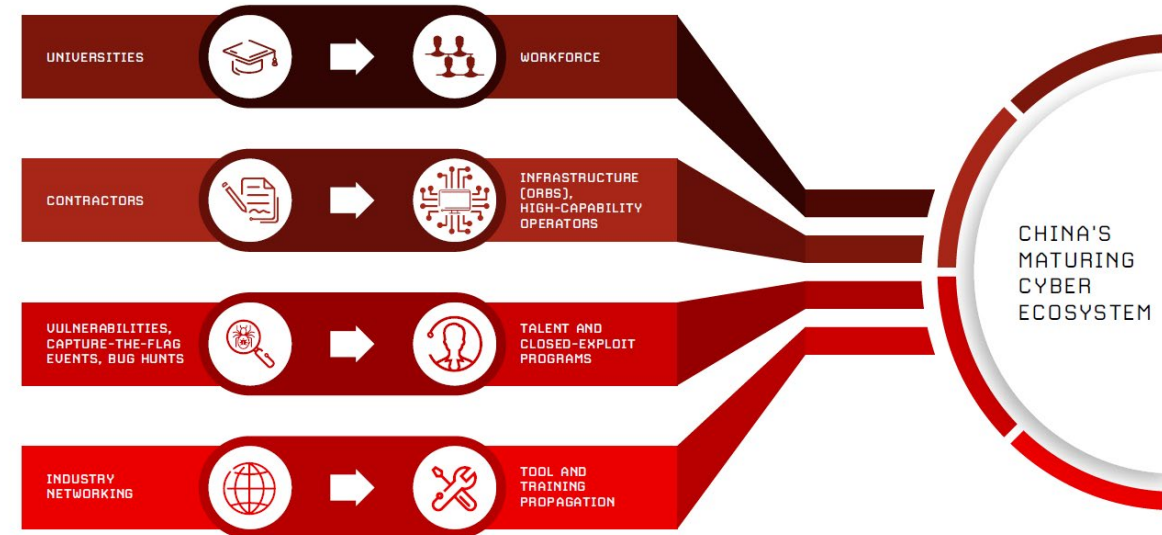
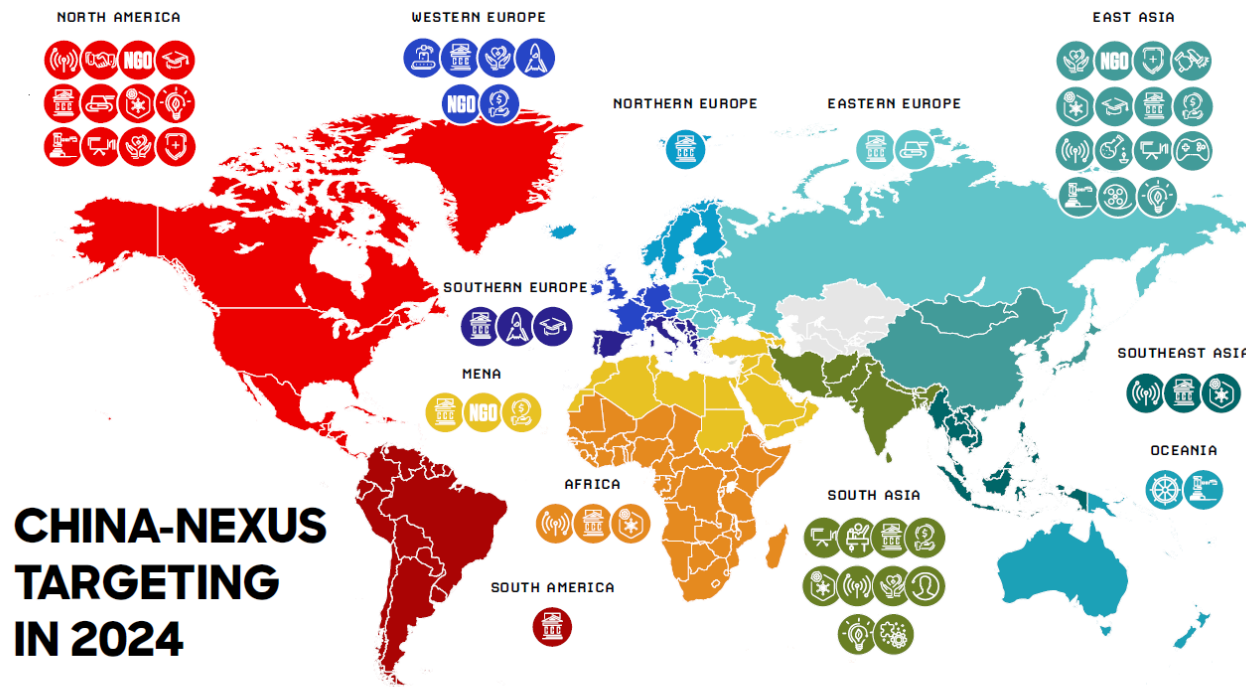
Threat actors are employing advanced tactics to breach security systems, highlighting the evolving nature of cyber threats.

## **Cyber Threat Landscape**

The current cyber threat landscape comprises various key players and their methods of operation, which are crucial for analysis.



# THREAT ACTOR HIGHLIGHT: CHINA



# SECTOR-SPECIFIC THREAT ANALYSIS



## **Vulnerabilities in the Finance Sector**

The finance sector encounters distinct threats, including cyber attacks, fraud, and regulatory obstacles that necessitate focused attention.

## **Challenges in the Healthcare Sector**

The healthcare industry is at risk of data breaches, compliance difficulties, and disruptions in the supply chain, requiring customized strategies to address these issues.

## **Risks in Manufacturing**

Manufacturing sectors confront risks associated with equipment malfunctions, workforce shortages, and vulnerabilities in the supply chain that can affect production efficiency.

## **Threats to Critical Infrastructure**


Critical infrastructure is particularly susceptible to cyber attacks due to the ongoing exploitation of known software vulnerabilities, targeted efforts by state-sponsored groups like Volt Typhoon, and systemic weaknesses in areas such as patch management, penetration testing, and credential security across essential sectors like water, energy, and transportation.

## HIGHLIGHT: RISKS OF CYBERATTACKS ON CRITICAL INFRASTRUCTURE



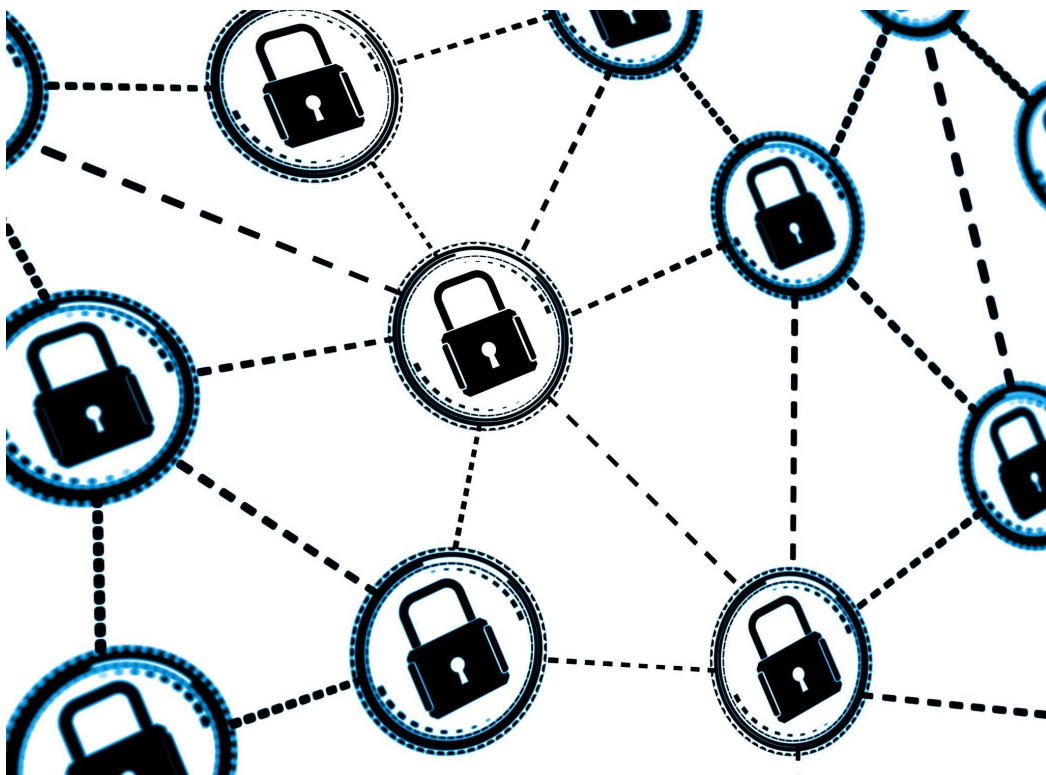
- Growing reliance on digital infrastructures amplifies exposure to risks.
- Cyber intrusions can interfere with vital services such as electricity and water supply.
- State-sponsored groups frequently aim at key infrastructure targets.
- Ransomware incidents can severely hinder operations and create disorder.
- Strong cybersecurity protocols are crucial for reducing potential threats.





# NOTABLE CYBER INCIDENTS OF 2024-2025

# HIGH-PROFILE ATTACKS AND BREACHES



## **Evolving Cyber Threats**

High-profile attacks in 2025 highlight the constantly evolving nature of cyber threats impacting various sectors.

## **Critical Infrastructure Targeted**

Attackers have increasingly targeted critical infrastructure, demonstrating the significance of cybersecurity in these areas.

## **Persistence of Attackers**

The report emphasizes the persistence of cyber attackers in their quest to exploit vulnerabilities in essential systems.

# IMPACT ANALYSIS OF THESE INCIDENTS



## **Economic Consequences**

Cyber incidents can lead to significant financial losses for organizations due to direct costs and lost revenue.

## **Operational Disruption**

Notable breaches can cause operational disruptions, affecting productivity and efficiency across affected organizations.

## **Reputational Damage**

Cyber incidents can severely damage an organization's reputation, leading to loss of customer trust and confidence.



# NOTABLE CYBER INCIDENTS IN 2024:



- **SolarWinds Redux:** A complex assault echoing the 2020 SolarWinds incident targeted various government entities and private firms. The attackers exploited a vulnerability in the supply chain to penetrate systems and extract sensitive information.
- **Healthcare Ransomware Attack:** A widespread ransomware incident affected numerous hospitals throughout Europe, leading to service interruptions and the compromise of patient data. The attackers demanded a significant ransom in cryptocurrency.
- **AI-Enhanced Phishing:** Cybercriminals have started leveraging AI technology to generate highly persuasive phishing emails, increasing the difficulty for individuals and organizations to identify and thwart these attacks.

# NOTABLE CYBER INCIDENTS IN 2025:



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

- **Threat of Quantum Computing:** As quantum computing continues to evolve, a new form of attack has surfaced that has the potential to undermine traditional encryption techniques. This represents a major risk to data security across multiple industries.
- **Hacking of IoT Devices:** A large-scale botnet assault that involved compromised Internet of Things (IoT) devices resulted in widespread interruptions to internet services. This incident exposed the weaknesses inherent in many consumer-focused IoT products.
- **Deepfake Fraud Schemes:** The rise of deepfake technology has led to an increase in fraudulent activities, with perpetrators producing realistic videos of corporate executives to authorize fake transactions. This has resulted in substantial financial losses for various organizations.
- **Breach of Microsoft SharePoint:** Cybercriminals took advantage of a zero-day vulnerability in Microsoft SharePoint, allowing them unauthorized access to sensitive information stored on the platform. This breach impacted numerous entities, including state and local governments, leading to significant data leaks and operational challenges.

## HIGHLIGHT: KEY ADVERSARY THEME -VISHING



- In 2024, a significant number of eCrime perpetrators incorporated vishing into their tactics, resulting in a monthly growth rate of 40% in recorded vishing activities over the year. The latter half of 2024 saw a marked increase in the use of this approach.
- Vishing is effective as it takes advantage of human errors or vulnerabilities instead of focusing on flaws within software or operating systems.
- In addition to vishing, many eCrime threat actors are increasingly employing help desk social engineering techniques. In these scenarios, attackers reach out to an organization's IT help desk, impersonating legitimate employees, and attempt to persuade a help desk representative to reset passwords or multifactor authentication (MFA) for the compromised account.



# HIGHLIGHT: KEY ADVERSARY THEME - VISHING

## STEP 1



### CURLY SPIDER

CURLY SPIDER spam bombs the victim



### CHATTY SPIDER

CHATTY SPIDER sends phishing email to the victim



### PLUMP SPIDER

## STEP 2

CURLY SPIDER calls the victim posing as IT support (vishing)

Victim calls in response to CHATTY SPIDER's email

PLUMP SPIDER calls the victim posing as IT support (vishing)

Victim downloads RMM tool, providing these adversaries with access



Quick Access, TeamViewer



Zoho Assist, Atera, SuperOps, Syncro



SoftEther UPN, Ammyy Admin, DWAgent, HopToDesk, RustDesk, Supremo, TeamViewer

## STEP 3

PLUMP SPIDER obtains valid credentials from the victim

## STEP 4

CURLY SPIDER deploys tools for persistence, including a custom backdoor

CHATTY SPIDER downloads WinSCP and/or Rclone to the victim system

PLUMP SPIDER introduces reconnaissance tooling

## STEP 5

CURLY SPIDER performs reconnaissance, including for security software

CHATTY SPIDER exfiltrates sensitive data to C2 infrastructure

PLUMP SPIDER performs a fraudulent transaction from victim payment system

## STEP 6

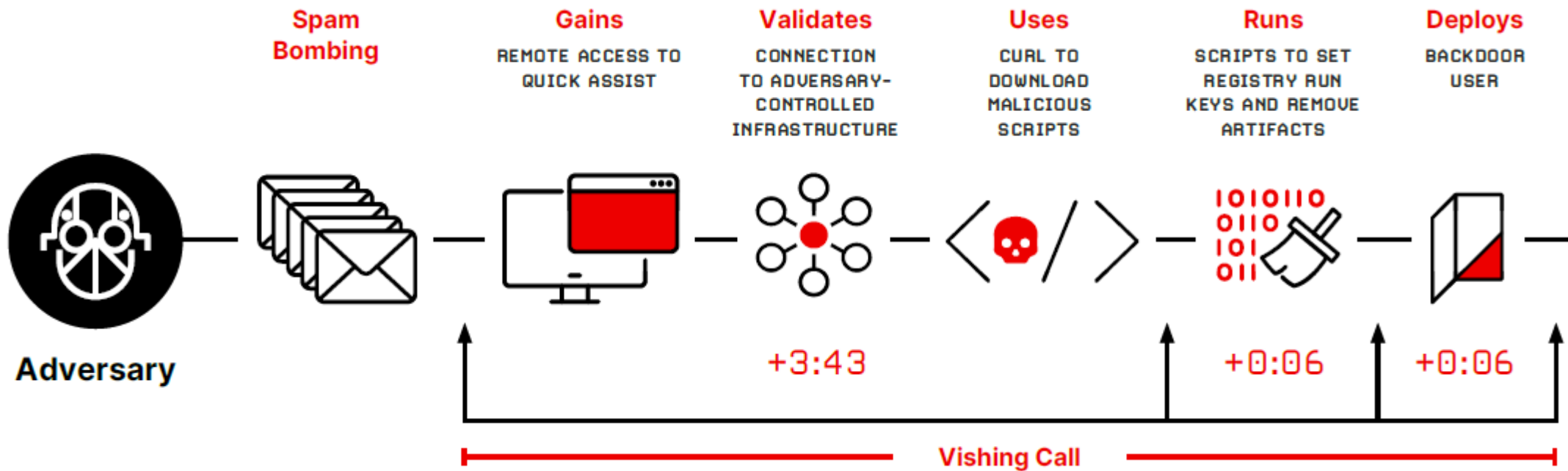
CURLY SPIDER exfiltrates data to C2 infrastructure

CHATTY SPIDER emails the victim with extortion demand

## STEP 7

CURLY SPIDER provides access to the victim to other actors, including BGH adversary WANDERING SPIDER

# HIGHLIGHT: KEY ADVERSARY THEME -VISHING





# TRENDS IN CYBERSECURITY DEFENSES



# ADVANCEMENTS IN CYBERSECURITY TECHNOLOGY

## **AI-Powered Threat Detection**

Tools powered by AI can now identify threats in real-time, enabling organizations to respond swiftly.

## **Response Solutions**

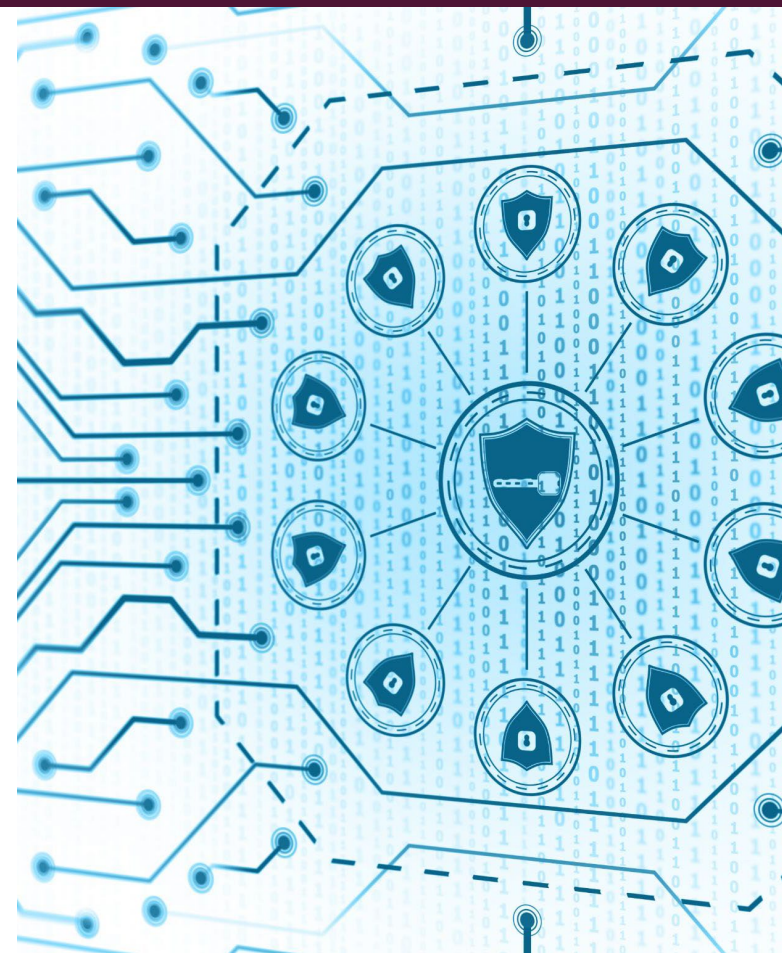
Advanced cybersecurity response solutions assist organizations in efficiently alleviating threats, thereby reducing potential harm.

## **Proactive Threat Management**

Organizations must consistently evolve and utilize emerging technologies to remain ahead of changing cyber threats.

## **Training Programs**

Organizations should adhere to their State-approved KnowBe4 training, while also incorporating additional training programs as necessary to align with agency mission goals and systems.



# EFFECTIVE DEFENSE STRATEGIES



## **Layered Security Strategies**

Layered security strategies provide multiple levels of defense against complex cyber threats, enhancing overall security posture.

## **Employee Training**

Regular employee training is vital for raising awareness about cyber threats and ensuring proactive defense against potential breaches.

## **Incident Response Planning**

Effective incident response planning minimizes damage during a cyber incident and ensures quick recovery and continuity of operations.



# RECOMMENDATIONS FOR ORGANIZATIONS

## **Regular Security Assessments**

Organizations should conduct regular security assessments to identify and mitigate potential vulnerabilities in their systems.

## **Threat Intelligence Sharing**

Sharing threat intelligence among organizations enhances collective cybersecurity efforts and improves response to threats.

## **Continuous Monitoring**

Organizations should implement continuous monitoring to detect vulnerabilities and respond to threats in real-time.

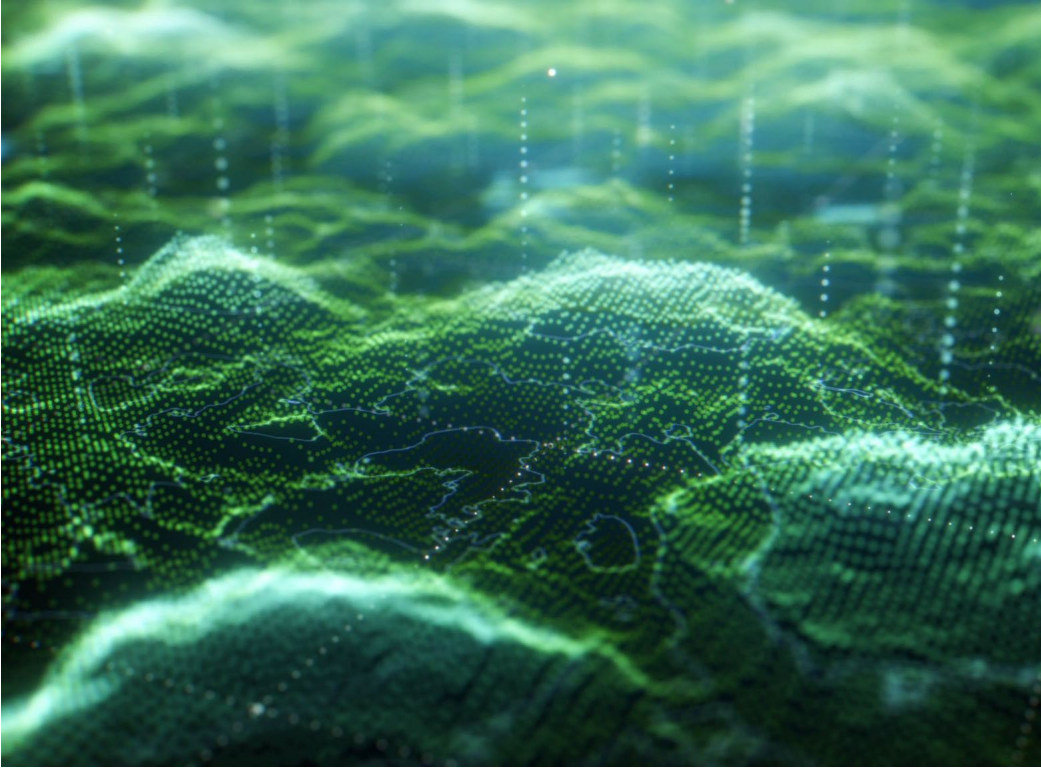






# FUTURE OUTLOOK AND PREDICTIONS

# PREDICTED CYBER THREATS FOR 2025-2026



## **Emerging Technologies**

The rise of emerging technologies will introduce new vulnerabilities, making organizations more susceptible to cyber threats.

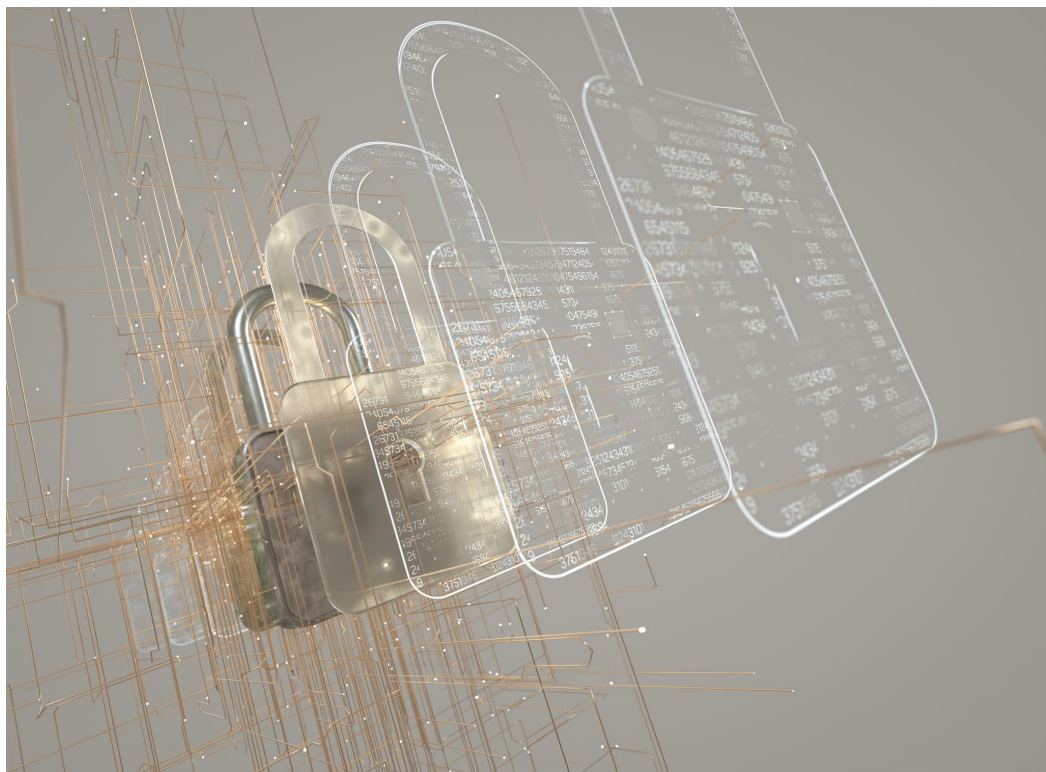
## **Geopolitical Tensions**

Geopolitical tensions are expected to escalate cyber threats, leading to increased state-sponsored cyber activities and attacks.

## **Organizational Vigilance**

Organizations must enhance their security measures and strategies to effectively adapt to the evolving cyber threat landscape in 2026.

# STRATEGIC RECOMMENDATIONS FOR THE FUTURE



## **Enhancing Cybersecurity Frameworks**

Organizations should strengthen their cybersecurity frameworks to protect against evolving threats and vulnerabilities.

## **Fostering Industry Collaboration**

Collaboration across industries can lead to sharing knowledge and strategies to better combat cyber threats.

## **Investing in Education and Training**

Investments in cybersecurity education and training will empower individuals to effectively respond to cyber challenges.



**ACT FAST, STAY  
SECURE, WHEN  
IN DOUBT  
SHOUT IT OUT!**



**Reach out to your Agency ISO** for immediate assistance.

**Submit a Help Desk Ticket through GTO:** [ServiceDesk@it.nv.gov]

**Get in touch with OISCD** for thorough threat sharing and support related to incident response:  
[IT-InfoSec@it.nv.gov]

(U) All screen shots in this presentation were copied from the CrowdStrike Global Threats Report