# Start Planning Now

## Cyber Threats and Trends for 2023

Allen Eaves

Managing Director, Information Security and Technology

jack henry™

01/24/23

# contents

Where Are We?

Rear-view, side-view Mirror

What’s Ahead?

Through the windshield, traffic report

How do we Plan Forward?

We have found a better route

# Where Are We?

Rear and Side-view Mirrors

# Where Are We? -------- Predictions from 2022

- **Ransomware evolving – more automation – 2/3 of attacks by low-level threat actors using ransomware tools (RaaS)**

- **Beyond Double Extortion – Ransomware gets even more disruptive**
  - Data extorsion is predicted to surpass traditional encryption in 2023. Combination attacks increasingly common

- **Legitimate IT management tools used as malware**

  -SolarWinds, Kaseya (REvile's attack of legit software update processes - $70M ransom demand)

- **Supply Chain Attacks**
  - SolarWinds Orion, Log4j
  - Quanta – Apple's major business partner; $50M ransom demand.
    - Turned to target Apple and released product blueprints
- **List of "terrorist organizations" that can't be paid ransom will increase**

- Where Are We?

# 2022 Verizon Data Breach Investigation Report: Financial and Insurance Industry

- Organized crime responsible for 79% of breaches compared to 49% in 2018
- Discovery method of Actor disclosure is at 58% compared to 5% in 2016
- Denial of Service (DoS) attacks are twice as common in security incidents for the vertical
- Of 2,527 incidents, 690 with confirmed data disclosure:– 73% external, 27% internal Threat Actors

# IBM X-Force 2022 report

- 37% of ransomware attacks from the prior year were REvil ransomware actors
- REvil shut down after 31 months, average gangs persist for ~17 months – repeat actors, new organization
- For the first time:
  - Attacks against Manufacturing overtook Financial services
  - North America was the 3rd most attacked region behind Asia

# Verizon Data Breach Investigations Report – 2022

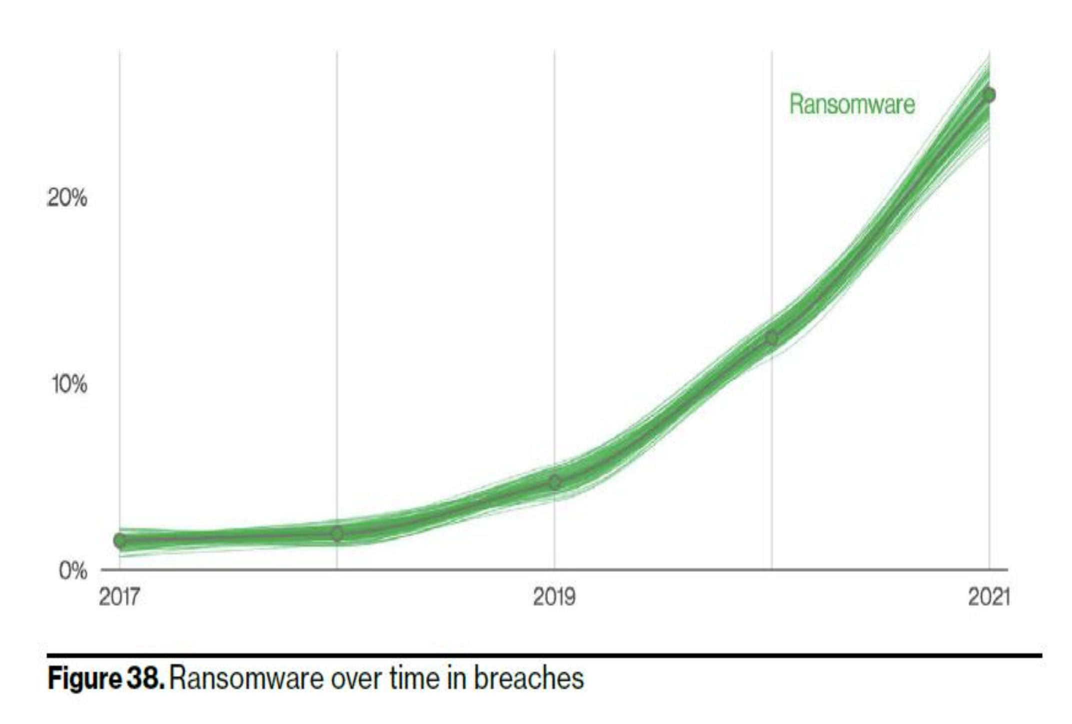


**Figure 38.** Ransomware over time in breaches

- Ransomware isn’t showing signs of slowing down – RaaS
- Third parties and supply chains will continue to be a major contributor to propagation of cyber incidents

- AiteNovarica *Top 10 Trends in Cybersecurity, 2023*
- Forbes’ *The Top Five Cybersecurity Trends In 2023*
- Splunk’s *Predictions 2023: Strategies for Turbulent Times*
- Forrester *APAC Predictions 2023: Cybersecurity And Risk*
- Forrester *Predictions 2023: Security Pros Face Greater Internal Risks*
- *Sophos 2022 Threat Report*
- *Cybersecurity Trends: IBM’s Predictions for 2023*
- *DCMS cyber security newsletter - January 2023*
- Open Access Government: *What cybersecurity trends can we expect to see in 2023*
- Secureworks *Emerging Cybersecurity Trends to Watch in 2023*
- *Presidio’s 2023 Cybersecurity Predictions*
- *F5 Labs: 5 Cybersecurity Predictions for 2023*
- *WatchGuard’s 2023 Cybersecurity Predictions*
- *Spiceworks 12 Cybersecurity Trends Every CISO Must Prepare for in 2023*
- *2023 Cybersecurity Predictions From CrowdStrike*
- *Verizon’s 2022 Data Breach Investigations Report and IBM X-Force 2022 Report*
- *KrebsOnSecurity*
- *NIST and National Cybersecurity Center*

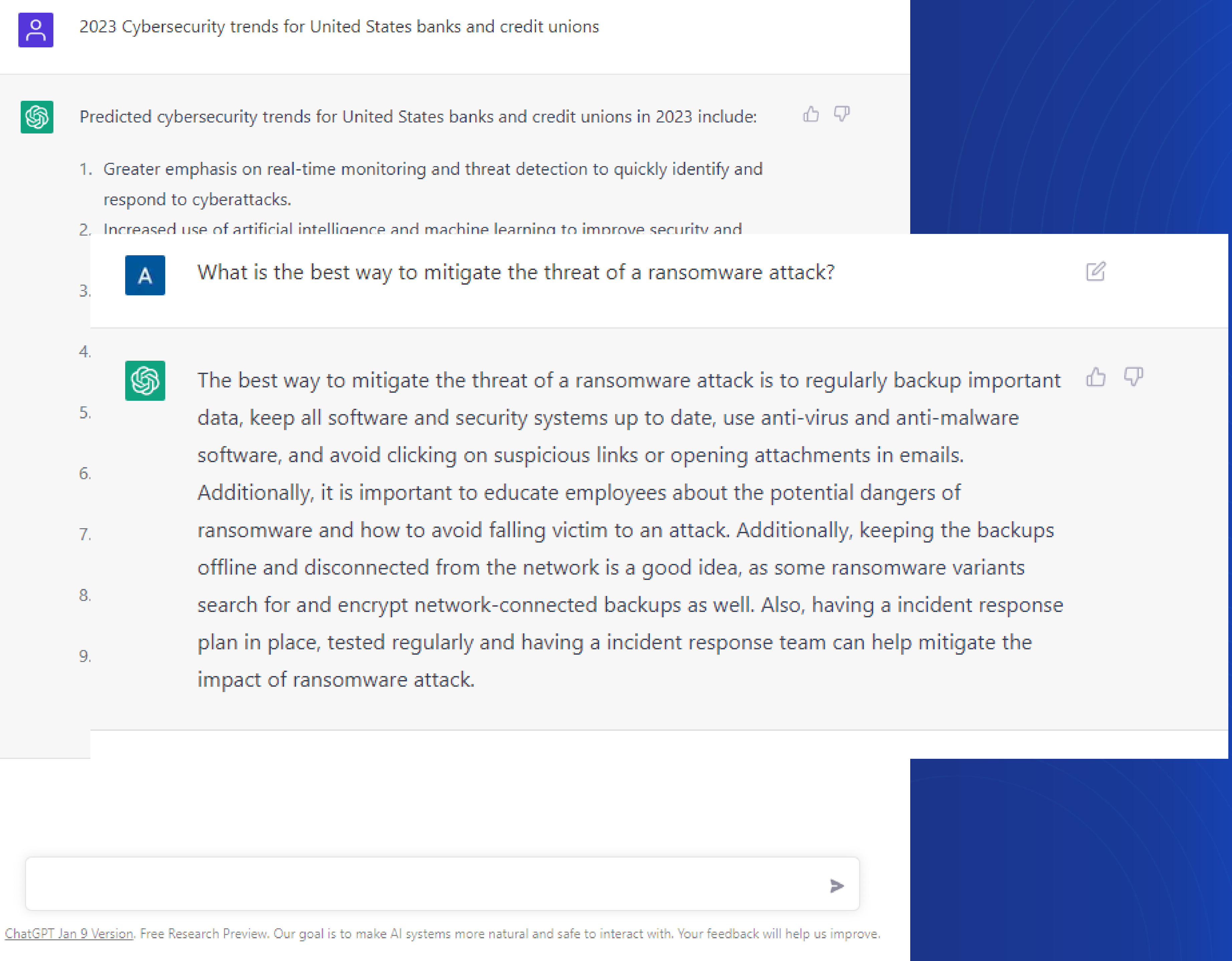
# What’s Ahead

Through the windshield and traffic report

## What’s Ahead?

- **Surge of Endpoint Detection and Response (EDR/ETDR | XDR) evasion tools for sale on the dark web**
- **Fraud, cybersecurity, IT Operations consider convergence - Fusion Centers**
- **Artificial Intelligence (AI) used widely in attacks**
  - Personalized and convincing Phishing
  - Evasion of automated email defense systems
  - Clone voices of senior executives for transaction authorizations
  - ChatGPT (launched November 30, 2022)

# ChatGPT



2023 Cybersecurity trends for United States banks and credit unions

Predicted cybersecurity trends for United States banks and credit unions in 2023 include:

1. Greater emphasis on real-time monitoring and threat detection to quickly identify and respond to cyberattacks.
2. Increased use of artificial intelligence and machine learning to improve security and
3.
4.
5.
6.
7.
8.
9.

A

What is the best way to mitigate the threat of a ransomware attack?

The best way to mitigate the threat of a ransomware attack is to regularly backup important data, keep all software and security systems up to date, use anti-virus and anti-malware software, and avoid clicking on suspicious links or opening attachments in emails. Additionally, it is important to educate employees about the potential dangers of ransomware and how to avoid falling victim to an attack. Additionally, keeping the backups offline and disconnected from the network is a good idea, as some ransomware variants search for and encrypt network-connected backups as well. Also, having a incident response plan in place, tested regularly and having a incident response team can help mitigate the impact of ransomware attack.

ChatGPT Jan 9 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

# What’s Ahead?

- **Geopolitical tensions driving nation-state cyber attacks**
- **Triple Extortion or more – Ransomware tentacles expand**
  - From Encryption of Data/Systems to extortion of business partners, combined DDoS attacks, business partners
- **Economic constraints driving more targeted and effective security**
  - Vulnerability management playing an increasingly important role
- **Shadow APIs**
- **Multi-Factor Authentication defeated**
- **Cyber insurance passing more cost to insured and increased security requirements**

# How do we Plan Forward?

We have found a better route

## How do we Plan Forward

- **Leverage Indicators of Compromise (IOCs) with live analytics**

- **Specialists –> Generalists Fundamentals as important as ever**
  - Decrypt for Security Inspection
  - Identity and Access Management (IAM)

- **Zero Trust and Reduced Trust –a foundation for digital transformations**

## How do we Plan Forward

- **Fundamentally Important:**

Fast track critical security fixes. Test and patch promptly

- **Prioritize detection and response strategies**

When not if

- **Concentrate protections**

Utilize Risk Assessments to most effectively build and refine security strategy

# Start Planning Now

## Cyber Threats and Trends for 2023

Allen Eaves

Managing Director, Information Security and Technology

jack henry™

01/24/23