WISHIN HIE SUMMIT 2024

CONNECTED

WISHIN’s Cybersecurity Posture & WISHIN as a Business Continuity Solution

PRESENTED BY

Greg Stadter | *Director of Operations, WISHIN*

Kerry Wardius | *Public Health Nurse, Oak Creek Health Department*

Caitlyn Stockhausen | *Disease Intervention Specialist, City of Milwaukee Health Department*

Katie Lepak | *Outreach Specialist, Wisconsin Cancer Collaborative*

SPONSORED BY

cloudticity

Speakers

Kevin Scharnhorst
CISO
Health Catalyst

Steve Rottmann
CEO
WISHIN

Mark Ziesemer
Information Security Architect
Heartland Business Systems

Brian Meyer
Director of HIPAA Security & IT
WISHIN

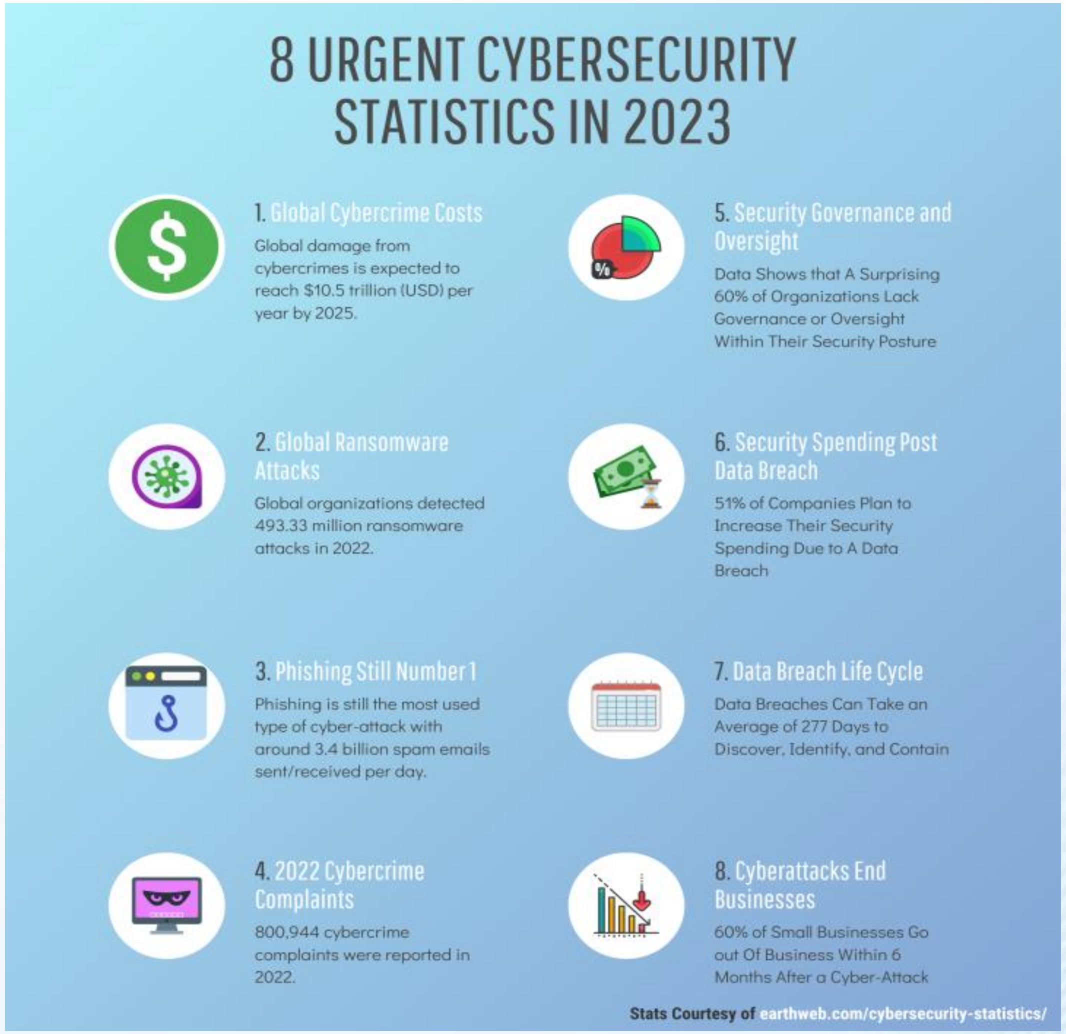
Cybersecurity - Threats & Protections

Cybersecurity Statistics & Facts

- Average time to detect a breach is 118 days
- Over 75% of attacks begin with an email
- 95% of data breaches are due to human error
- Cybersecurity budgets have increased 51%
- Inversely, 30% of executives stated their IT & Security budgets are not sufficient
- 62% of users have shared a password over email or text
- 91% of industries have Ransomware as 1 of the top 3 priorities

ONC announced a reorg with focus to emphasize cybersecurity, data and AI – ASTP

(Assistant Secretary for Technology Policy and Office of the National Coordinator for HIT)



8 URGENT CYBERSECURITY STATISTICS IN 2023

1. Global Cybercrime Costs

Global damage from cybercrimes is expected to reach $10.5 trillion (USD) per year by 2025.

2. Global Ransomware Attacks

Global organizations detected 493.33 million ransomware attacks in 2022.

3. Phishing Still Number 1

Phishing is still the most used type of cyber-attack with around 3.4 billion spam emails sent/received per day.

4. 2022 Cybercrime Complaints

800,944 cybercrime complaints were reported in 2022.

5. Security Governance and Oversight

Data Shows that A Surprising 60% of Organizations Lack Governance or Oversight Within Their Security Posture

6. Security Spending Post Data Breach

51% of Companies Plan to Increase Their Security Spending Due to A Data Breach

7. Data Breach Life Cycle

Data Breaches Can Take an Average of 277 Days to Discover, Identify, and Contain

8. Cyberattacks End Businesses

60% of Small Businesses Go out Of Business Within 6 Months After a Cyber-Attack

Stats Courtesy of earthweb.com/cybersecurity-statistics/

https://www.terranovasecurity.com/blog/cyber-security-statistics
https://www.hhs.gov/about/news/2024/07/25/hhs-reorganizes-technology-cybersecurity-data-artificial-intelligence-strategy-policy-functions.html

Cybersecurity Incident Causes & Impact

- 94% of breaches fall under System Intrusion
- 90% of reported incidents to the FBI’s Internet Crime Complaint Center (IC3) had no financial loss
- Remaining 10% of IC3 reported incidents lost $11,500… range of $70 - $1.2M
- Second highest breach contributor = “Misc. Errors”
  - Human errors
  - Lack of training
- 68% of all breaches have affected healthcare

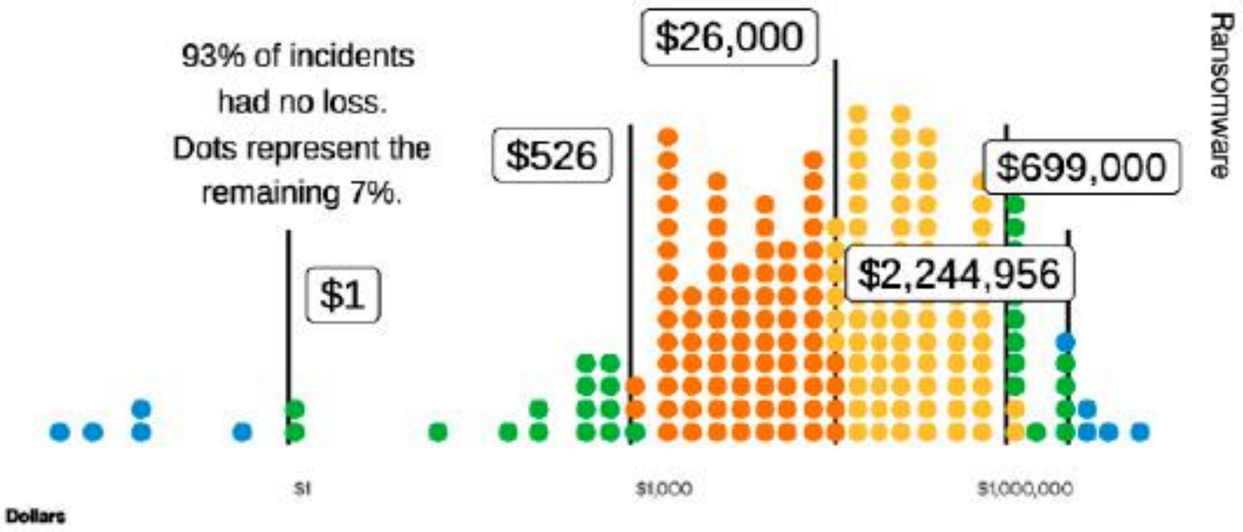


Figure 33. 95% and 80% confidence intervals of Ransomware incident cost per complaint (n=2,575)

Verizon – 2023 Data Breach Investigations Report (DBIR)

WISHIN Protections & Preventative Measures

- WISHIN's partnership with Health Catalyst – HITRUST CSF certified
- Partnership with Heartland Business Systems
  - Enforcement of Multifactor Authentication (MFA)
  - Microsoft InTune
  - XDR - 24x7x365 security solution
  - Always on endpoint protection
  - Data loss prevention policies
- WISHIN's independent audit of HIPAA Privacy & Security policies and controls

Business Continuity

WISHIN as your Business Continuity solution

WHEN:

- Faulty EHR upgrade
- Cybersecurity attack
- Disaster or interruption to business operations

HOW:

- Organization disruption mitigate by using WISHIN Pulse
- WISHIN Pulse – a reliable and secure source of clinical data
- Access to your own (historical) and other participant data
- WISHIN can enable users quickly… do this now as a preventative measure
- Write WISHIN into BC/DR plans!

Thank you for participating!

Check out the full video of this session on
our YouTube Channel

@WISHINPulse