



Cybersecurity
Your actions, your impact, your success.

Presenter



Jennifer Taylor

Senior Manager | IT Risk & Compliance

502.963.0820

jennifer.taylor@us.forvismazars.com



1. The Why
2. Trends & Statistics
3. Threats & Predictions
4. Final Thoughts & Resources
5. Questions

The Why



Cybersecurity

Why Should It Be A Priority For Nonprofits?



Action

“Action is the foundational key to all success.”

~ Pablo Picasso



Impact

“Everything you do has some effect, some impact.”

~ Dalai Lama XIV



Success

“Alone, we can do so little; together we can do so much.”

~ Helen Keller

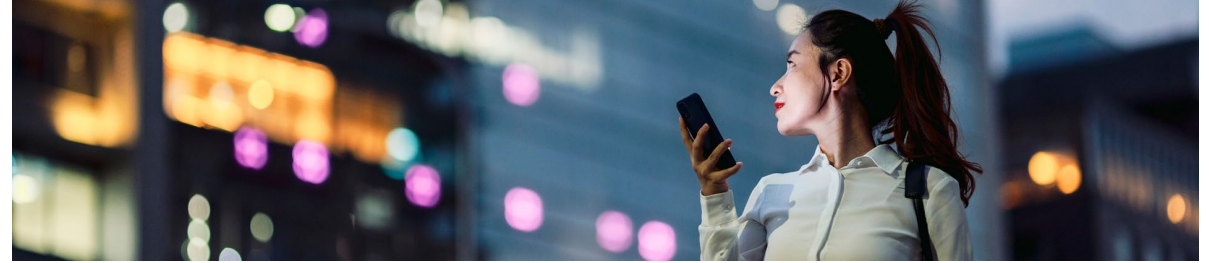
Cybersecurity

Why Should It Be A Priority For Nonprofits?



Ignorance Is Risk, Not Bliss.

Ignorance about cybersecurity can be dangerous and put individuals and organizations at risk. It can leave them vulnerable to attacks, legal issues, and significant financial losses.



If You Are Reachable, You Are Breachable.

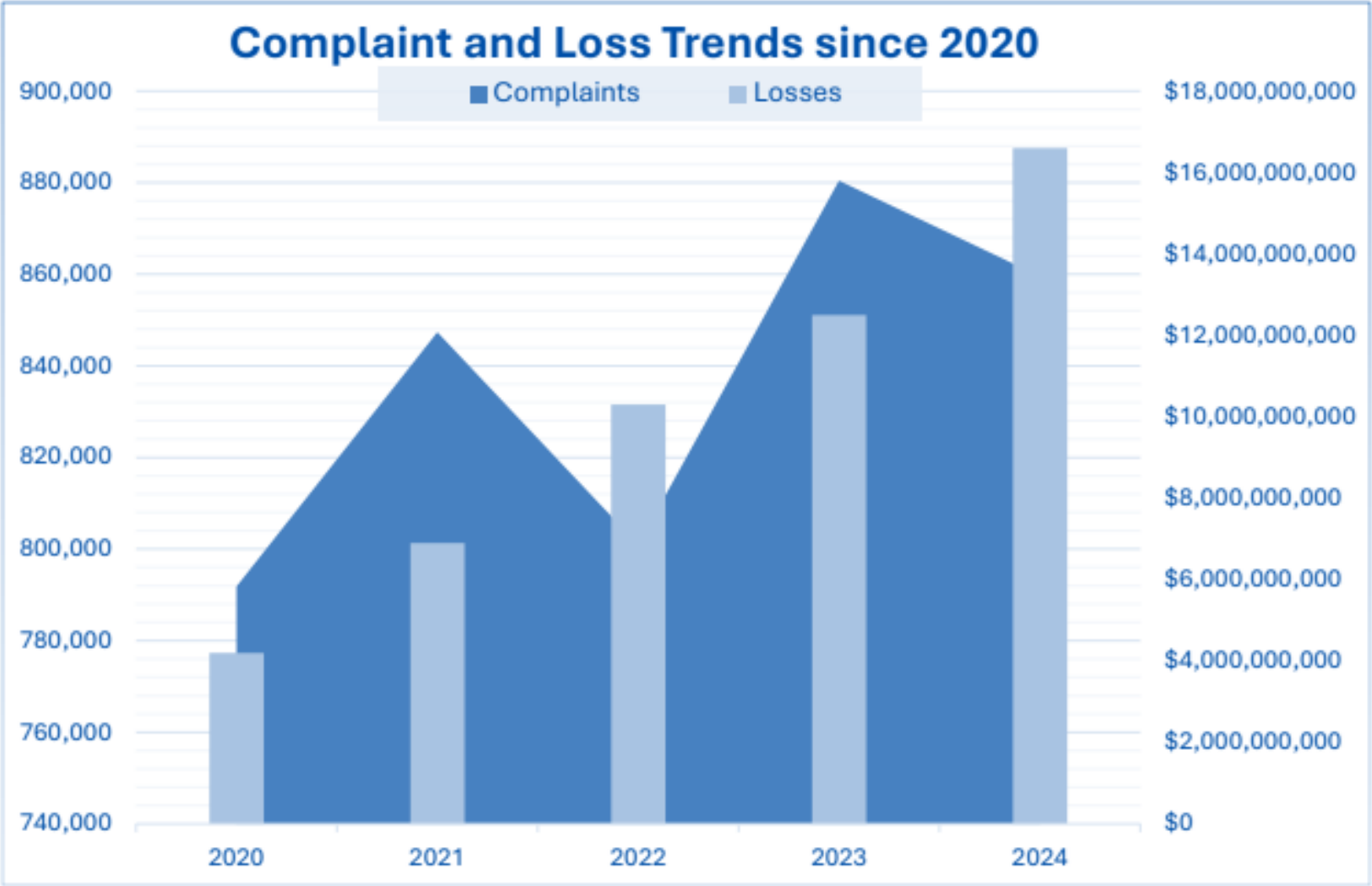
This means anyone on the internet is at risk, regardless of their size, location, or other factors

To protect digital lives and sensitive information, it's important to stay informed, vigilant, and take proactive measures.

Trends & Statistics



FBI's Internet Crime Complaint Center (IC3) Five-Year Statistics

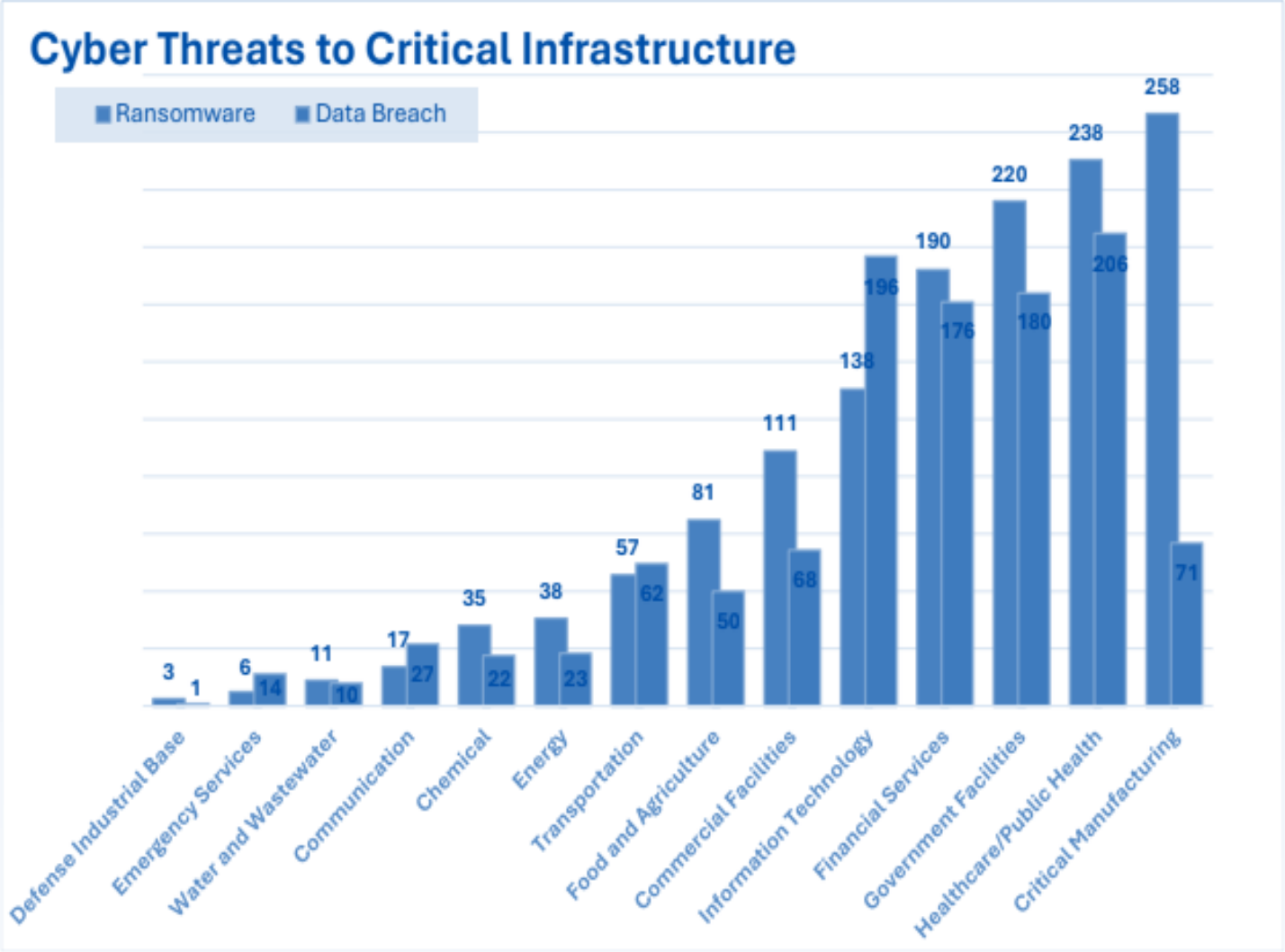


FBI's Internet Crime Complaint Center (IC3) Statistics

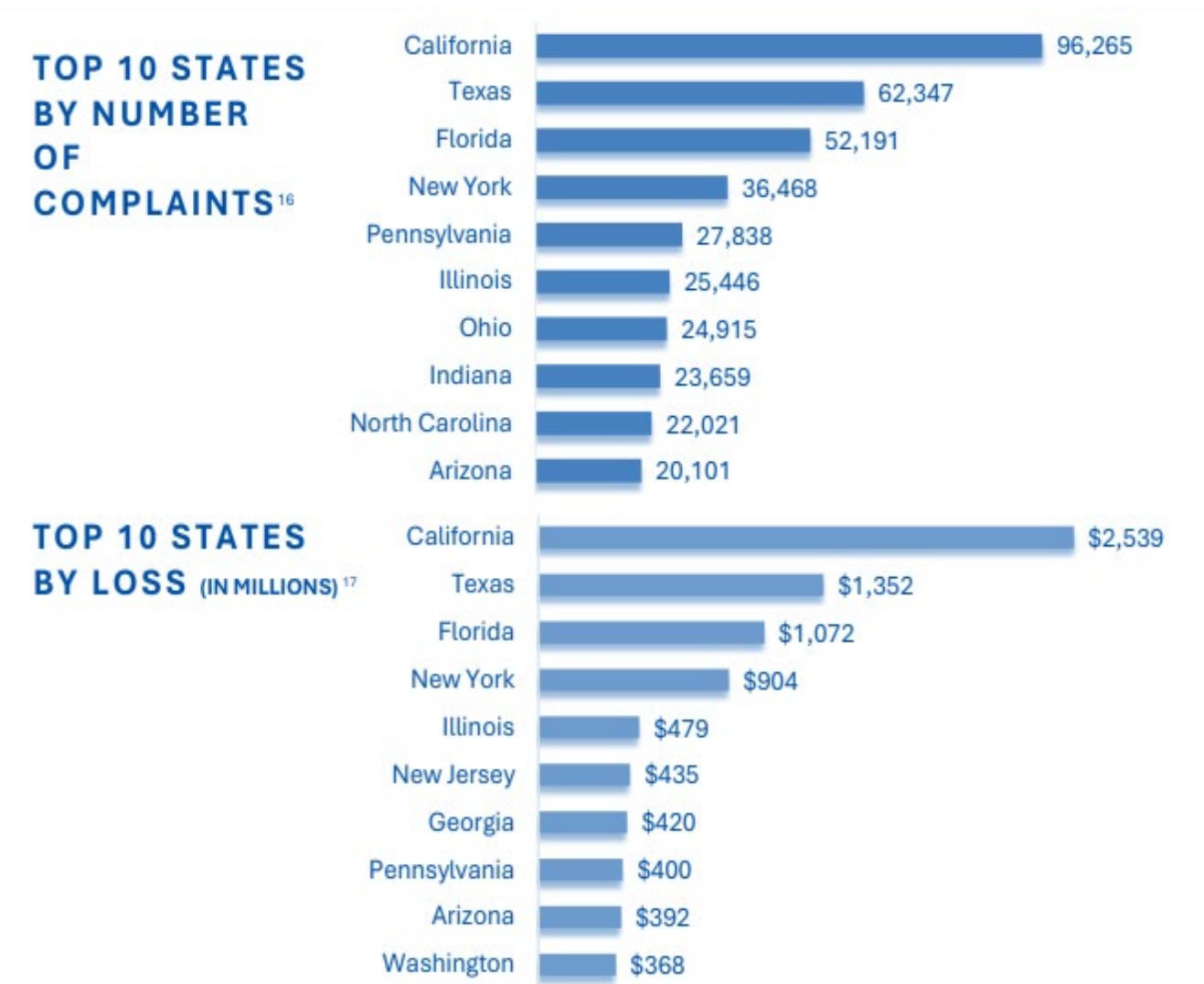
2024 BY THE NUMBERS¹



FBI's Internet Crime Complaint Center (IC3) Five-Year Statistics



FBI's Internet Crime Complaint Center (IC3) Statistics



Cybersecurity

Your Industry Statistics

Humans are still being exploited as the “weakest link” in a cybersecurity plan.

45%

of Americans have had their personal information compromised by a data breach in the last five years.

74%

Of all data breaches include the human element – either via error, privilege misuse, stolen credentials, or social engineering.

97

Nonprofits reported data breaches in 2023 compared to 48 in 2003.

26%

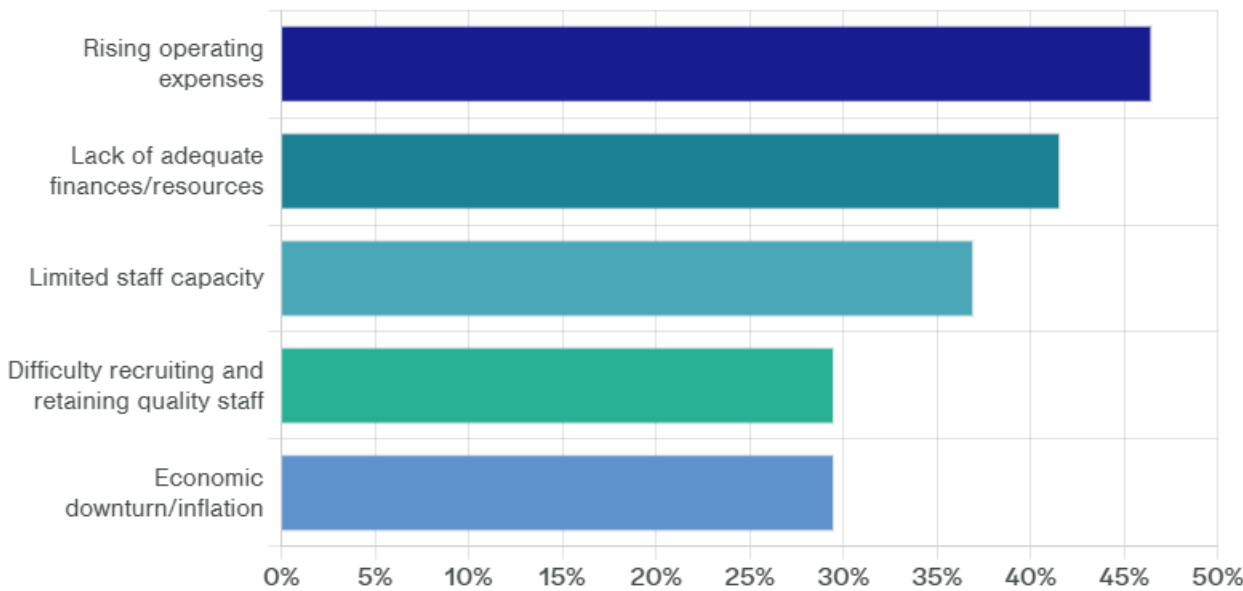
Of nonprofits actively monitor their environment.



Challenges Nonprofits Are Facing ...and how it impacts your cybersecurity.

Based on data from more than 325 nonprofit professionals across the U.S., our report found:

The top 5 challenges nonprofits face:



Stop saying:
“We can’t afford to.”

Start accepting:
“You can’t afford NOT too!”

Threats & Predictions



Why Is Your Industry a Target?

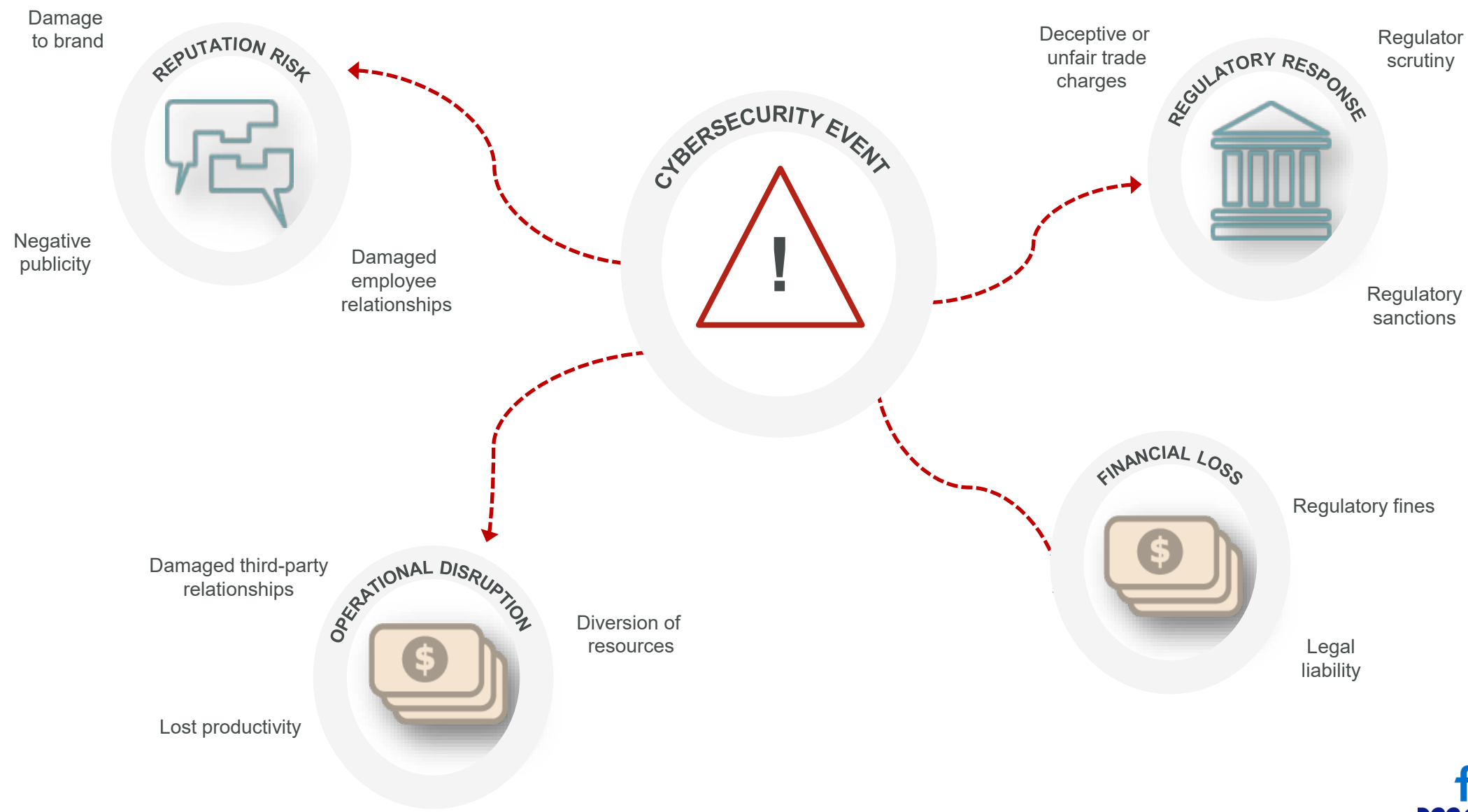
Cyber Poor & Target Rich



- Significant budgetary constraints
- Significant amount of sensitive data
- Aging infrastructure and resources
- You need more cyber-skilled employees
- Threat actors can remain undetected for long periods of time


Prioritizing cybersecurity is no longer an option but an imperative for nonprofits.

Breach Impacts

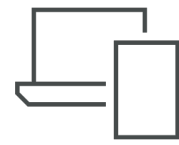


Threats

Most Common



Social Engineering Attacks




Business Email Compromise



Supply Chain Attacks



Malware/Ransomware

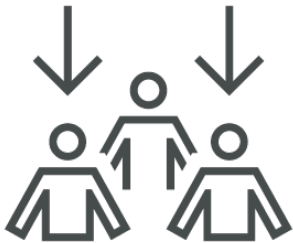


Cloud Applications



Artificial Intelligence

Threats
Root Cause



Inadequate Training



Weak Privileged Access Controls

Does this sound like
your organization?



Ineffective System Patching



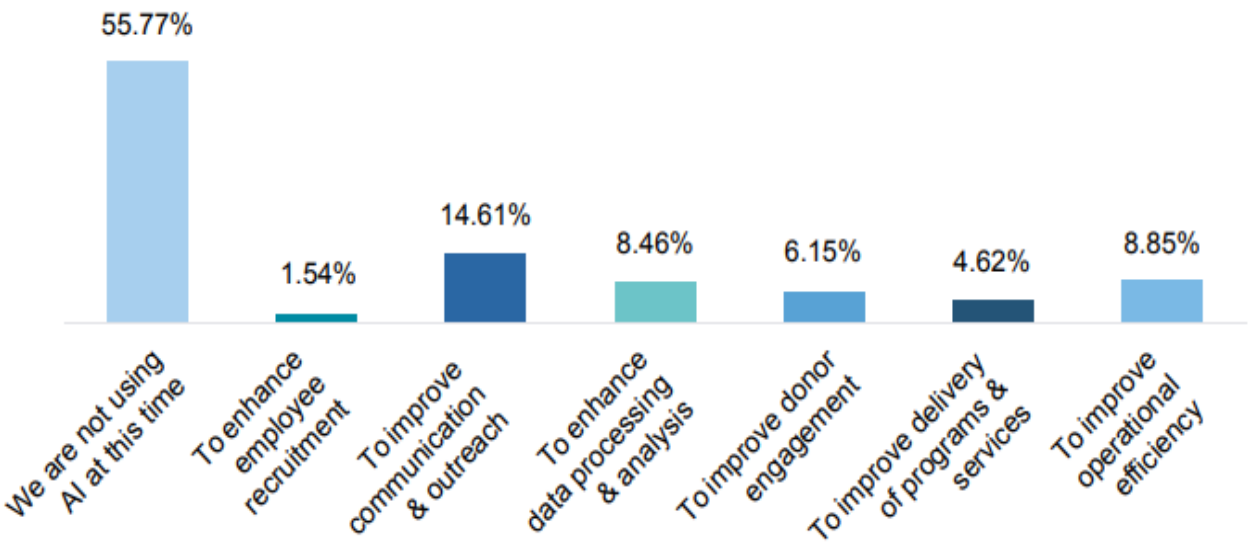
Unmonitored Detection Systems

Artificial Intelligence

Is it a Threat, Benefit, or Both?

AI is transforming the way we work. Are you trying to stay ahead or getting left behind?

How is your organization currently using AI?



Artificial Intelligence Positives and Negatives



The effect of extensive security AI and automation on the financial impact of a breach

Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches.

- Organizations that used these capabilities extensively within their approach experienced, on average, a **108-day shorter time** to identify and contain the breach.
- They also reported **USD 1.76 million lower data breach costs** compared to organizations that didn't use security AI and automation capabilities



Phishing / Deep Fakes

- AI can be used to automate and enrich phishing emails

Data Privacy / Breaches

- AI can be used to access and exploit personal data without permission or authorization

AI-assisted Fraud

- AI-assisted fraud can be used to bypass security measures and steal data.

Other Security Risks

- AI can be used to create security vulnerabilities or exploit weaknesses quickly

Top 10 Cybersecurity Predictions for 2024

- **RANSOMWARE BECOMES WEAPONIZED**

Ransomware attacks will develop to become a tool for cyberwarfare by nation states and cybercriminals.

- **SUPPLY CHAIN ATTACKS INCREASE**

Attacks on software supply chains will rise as hackers find it an efficient way to compromise multiple targets.

- **CLOUD SECURITY FAILURES**

Misconfigurations and vulnerabilities in cloud infrastructure will lead to major data breaches.

- **AI-POWERED HACKING**

AI will be used by hackers to automate attacks, evade detection and craft convincing phishing emails.

- **INTERNET OF THINGS BOTNETS SURGE**

Unsecured IoT devices will be increasingly hijacked into botnets to launch DDoS attacks.

- **QUANTUM COMPUTING THREATS EMERGE**

Quantum computers will be able to crack current encryption and undermine blockchain security.

- **CREDENTIAL STUFFING ATTACKS PROLIFERATE**

Automated credential stuffing attacks will grow as billions of stolen passwords are leveraged.

- **API VULNERABILITIES EXPLOITED**

API security failures will lead to data breaches as hackers target backend systems.

- **CRITICAL INFRASTRUCTURE HACKING**

State-sponsored hackers increasingly target critical national infrastructure like power grids.

- **DEEPPAKES FOR SOCIAL ENGINEERING**

Realistic deepfake videos will be used for more convincing phishing and social engineering.

Final Thoughts & Conclusions





*It's not a
matter of if, but
a matter of
when...*

Responsibility to our industry & future

Cyber security is how we can capitalize on opportunities to advance the state-of-the-art.

Cybercrime is predicted to **cost the world \$10.5 trillion** annually by 2025.

Source: Cybersecurity Ventures

The global cybersecurity **workforce must grow by 65%** in order to effectively defend critical assets and data.

Source: (ISC)²

A Quote to Motivate

“Act as if what you do makes a difference. IT DOES.”

- William James

Other Resources

- Infosec Institute – <https://resources.infosecinstitute.com/>
- Info Risk Today – <https://www.inforisktoday.com/>
- Security Week – <https://www.securityweek.com/>
- Dark Reading – <https://www.darkreading.com/>
- The Top Cyber Threat Intelligence Feeds – <https://thecyberthreat.com/cyber-threat-intelligence-feeds/>

Contact

Forvis Mazars

Jennifer Taylor

Senior Manager | IT Risk & Compliance

Lexington, KY

P: 502.963.0820

jennifer.taylor@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2025 Forvis Mazars, LLP. All rights reserved.