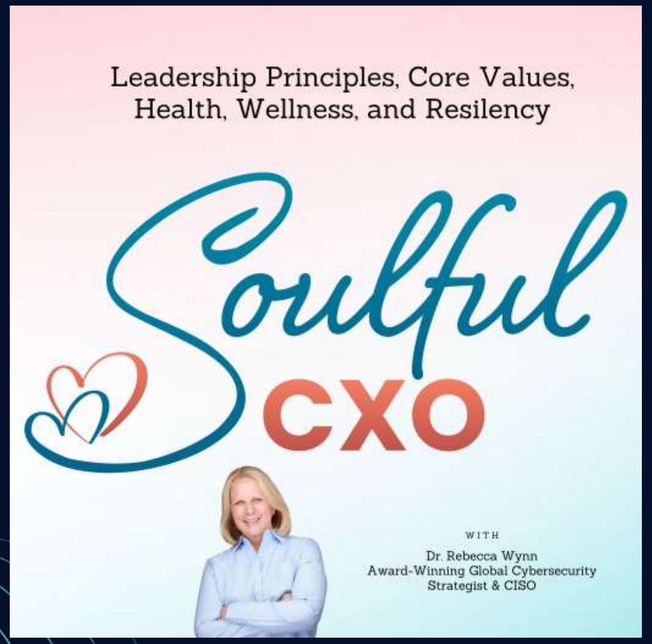
Why Leading the Way in Data Privacy and Security is Critical for Enterprise Risk Management

By Dr. Rebecca Wynn
April 6, 2023

DAMA Phoenix Chapter



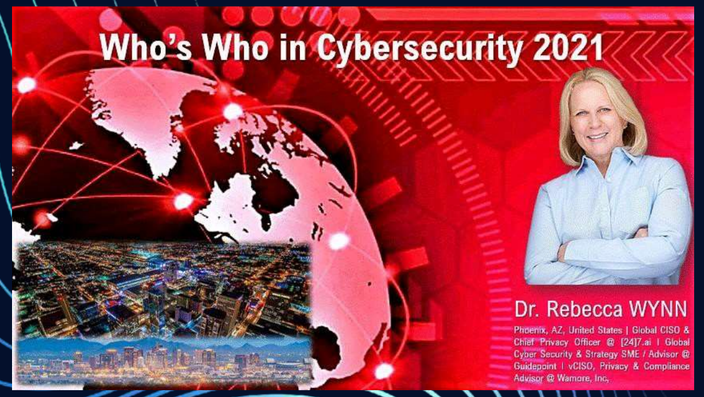
Dr. Rebecca Wynn
CISSP, CRISC, CASP, CICA, CCISO
www.DrRebeccaWynn.com

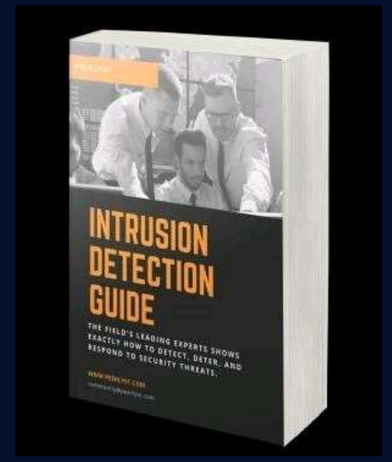
Chief Cybersecurity Strategist & CISO
Click Solutions Group

Global Award-Winning Cybersecurity & Privacy Executive Advisory Board Member, Author, Speaker

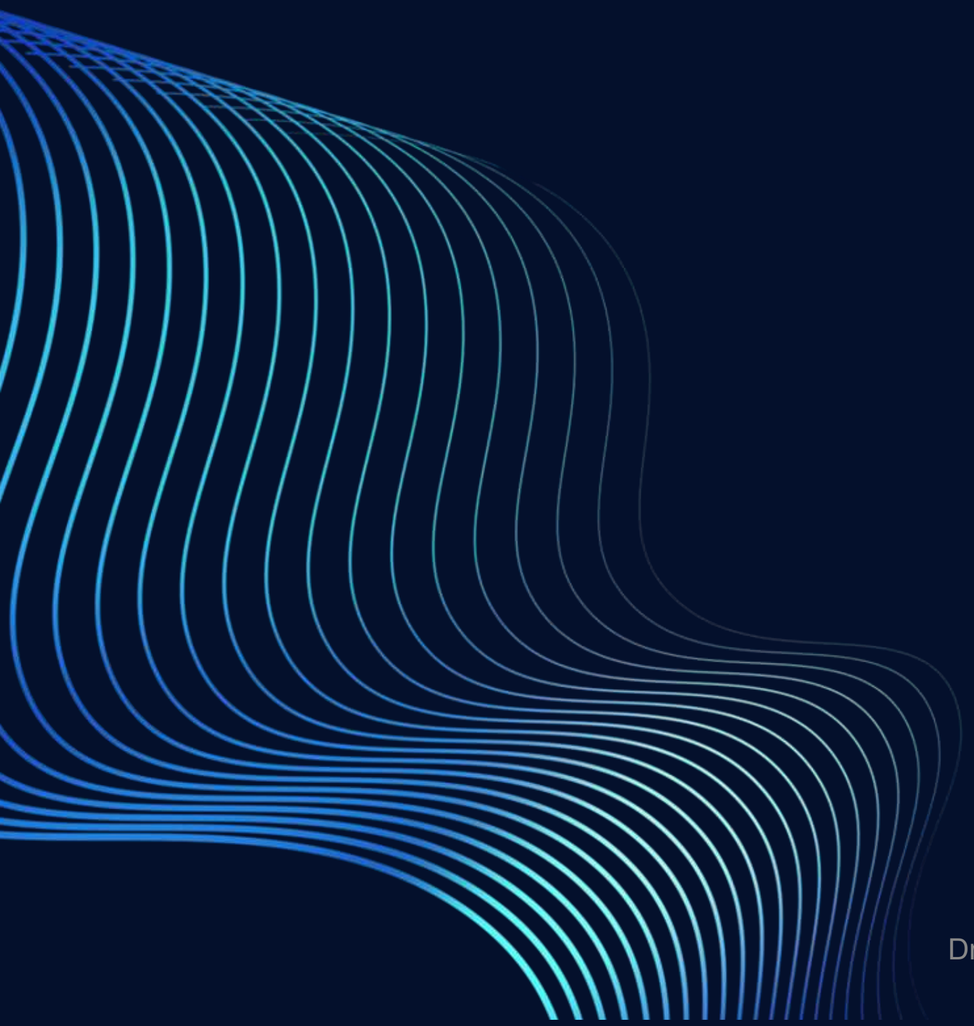
Soulful CXO Podcast Host

Threat Watch Show Host





Agenda



01 Data Privacy & Security in ERM

02 Risks & Consequences of Ignoring

03 Regulations

04 Best Practices

05 Role of Employees

06 AI & ML

Agenda

07 AI the Positives for Cyber Security

08 AI Design Issues

09 A Few Frameworks

10 And…

* Quick Transition Break

** Panel

Data Privacy & Security in Enterprise Risk Management

- 33 newly named adversaries in 2022
- 200+ adversaries targeting organizations across the globe
- 71% of attacks in 2022 were malware-free
- 95% increase in cloud exploitation
- 112% increase in access broker advertisements on the dark web
- 84-minute average eCrime breakout time

Reference: CrowdStrike 2023 Global Threat Report

Risks & Consequences of Ignoring Data Privacy & Security

- 32% average year-over-year increase in the estimated monthly number of insider-driven data exposure, loss, leak, and theft events
- $16 million per incident (on average) could cost companies
- 72% companies have dedicated Insider Risks/threats program but 71% expect data loss from insider in next 12 months
- 82% CISOs admit data loss from insiders is a problem for the company
- #1 Insider Risk, #2 Cloud data exposure, #3 Malware/Ransomware

Reference: Code42 2023 Data Exposure Report

Regulations

- The Security and Exchange Commission (SEC) has proposed a new set of cybersecurity disclosure rules for public companies, which would require them to report “material cybersecurity incidents” to the SEC within 4 days. Reference: https://www.ftc.gov/legal-library/browse/federal-register-notices/non-compete-clause-rulemaking
- The Federal Trade Commission (FTC) has proposed a new rule to ban noncompete clauses, freeing up employees to leave for competitors. Reference: https://www.jdsupra.com/legalnews/sec-proposed-cybersecurity-rules-what-2345066/
- California Privacy Rights Act (CPRA) on January 1, 2023
- Virginia Consumer Data Protection (CPDA) on January 1, 2023
- Colorado Privacy Act (CPA) on July 1, 2023
- Connecticut’s Act Concerning Personal Data Privacy and Online Monitoring, also known as the Connecticut Data Privacy Act (CTDPA) on July 1, 2023
- Utah Consumer Privacy Act (UCPA) on December 31, 2023

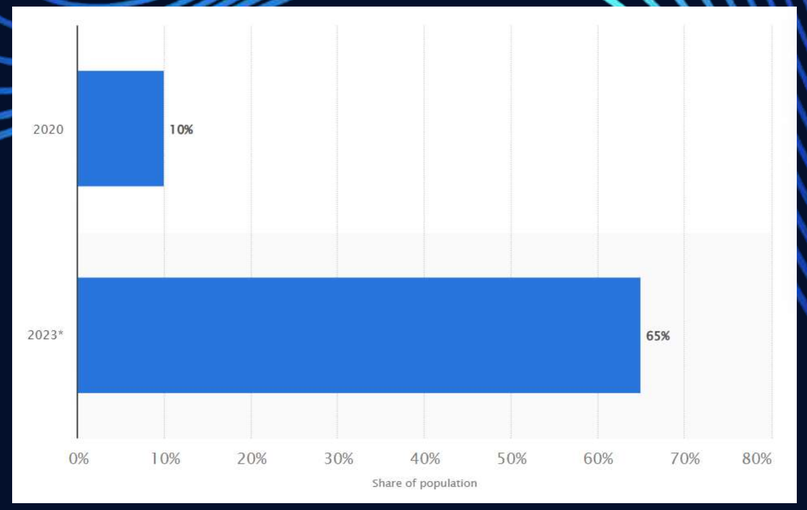
Best Practices

- Establish regulatory compliance
- Clean up unstructured data

According to Egnyte's 2021 Data Governance Trends, unchecked data growth, combined with a lack of visibility, is dramatically increasing the risk of breaches, ransomware, and compliance violations.

- Educate your employees

Share of the global population that have personal data covered under modern privacy regulations from 2020 to 2023



https://www.statista.com/statistics/1175672/population-personal-data-regulations-worldwide/

Role of Employees

- SCATTERED SPIDER has conducted targeted social engineering campaigns using phishing pages to capture authentication credentials for Okta, VPNs, or edge devices and socially engineers users to share one-time password multifactor authentication (MFA) codes or overwhelms them using MFA notification fatigue.
- According to Cybersecurity Ventures, the cost of cybercrime will hit $8 trillion in 2023 and grow to $10.5 trillion by 2025.
- Phishing Continues to be a preferred method of Hackers in 2023. According to the firm Lookout, the highest rate of mobile phishing in history was observed in 2022.
- Research company Trellix determined 78% of business email compromise (BEC) involved fake CEO emails using common CEO phrases, resulting in a 64% increase from Q3 to Q4 2022.

Artificial Intelligence & Machine Learning

- According to a Deloitte Center for Controllership poll. “During the past 12 months, 34.5% of polled executives report that cyber adversaries targeted their organizations' accounting and financial data.
- International Data Corporation (IDC) says AI in the cybersecurity market is growing at a CAGR of 23.6% and will reach a market value of $46.3 billion in 2027.
- According to Synopsys researchers, at least one open-source vulnerability was found in 84% of code bases.
- 92% of companies plan to use AI & ML to bolster their cybersecurity.
- 70% of IT professionals believe they cannot respond to or thwart advanced AI-driven cyber attacks

Reference: https://info.mimecast.com/cybergraph

Artificial Intelligence the Positives for Cyber Security

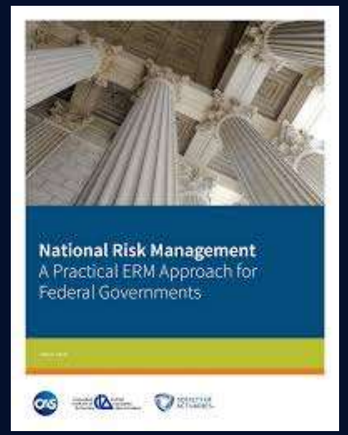
- Threat detection: extremely helpful when it comes to efficiently and accurately analyzing large volumes of data
- Automation: enables cyber security professionals to focus on investigating and mitigating complex threats, while AI takes care of tedious or monotonous basic tasks
- Machine learning: AI-powered cyber security systems consist of their ability to learn from past attacks and to improve on existing threat detection capabilities.
- Insider threats: AI-powered systems can analyze user behavior and identify patterns indicating an insider threat. Such patterns can then be flagged for further investigation.
- Endpoint security & threat intelligence: leverage machine learning algorithms to identify anomalous behavior and to detect previously unknown threats.

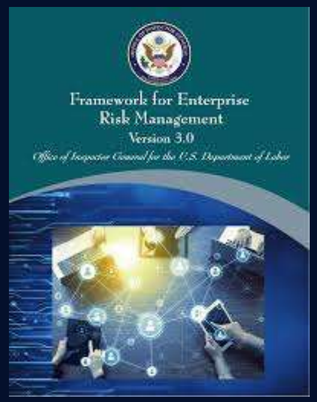
Artificial Intelligence Design Issues

- Artificial intelligence is integral to developments in healthcare, technology, and other sectors, but there are concerns about regulating data privacy.
- According to the European Consumer Organization, in 2020, a survey showed that 45-60% of Europeans agree that AI will lead to more abuse of personal data.
- Thanks to some companies' overreaching personal data use and mismanagement, privacy protection is becoming a public policy issue worldwide.
- As for the overall design of AI products and algorithms, de-coupling data from users via anonymization and aggregation is key for any business using user data to train their AI models.
- Privacy-respecting AI requires privacy-respecting companies.

Reference: https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/

A Few Frameworks





And…

- 69% of employees have bypassed their organization's cybersecurity guidance in 2022, according to a recent Gartner survey.
- 74% of employees in the same survey said they would be willing to bypass cybersecurity guidance if it helped them or their team achieve a business objective.
- Data privacy has significantly contributed to risk exposure for businesses today. With more focus on keeping the user data safe and the constantly changing global data regulations, organizations are keen on tracking how businesses interact with the user data.
- Proactive risk management implies focusing on preventive tactics that keep track of potential risks before they hit the organizational setup. This is possible through proper planning, effective communication, and rightful decision-making.
- Today, risk management has gone far beyond compliance. It is now a driver of value that protects businesses from risks and a strategic component that ensures long-term sustainable growth and innovation.

Remember we are in a cyber war. The bad actors – internal and external – only have to be lucky once. We as a TEAM have to be lucky ALWAYS.

Dr. Rebecca Wynn

Thank you.

Panelist

Debbie Christofferson, CISSP, CISM, CCSK
Moderator

Deb Bond

Joe Vadakkan

Kim Jones, CISSP, CISM, CRISC

Dr. Rebecca Wynn, CISSP, CRISC, CASP, CICA, CCISO

Thank you.

Thank you.

Thank you.

Thank you.

Thank you.