UHY Technical Webinar

The Merger of Cybersecurity and Compliance

October 24, 2023

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Agenda

1. Introduction
2. Learning Objectives & CPE
3. The Evolution of Cybersecurity and Compliance
4. Benefits and Challenges Ahead
5. Cyber Health Check Opportunity

Learning Objectives

CPE Credits

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

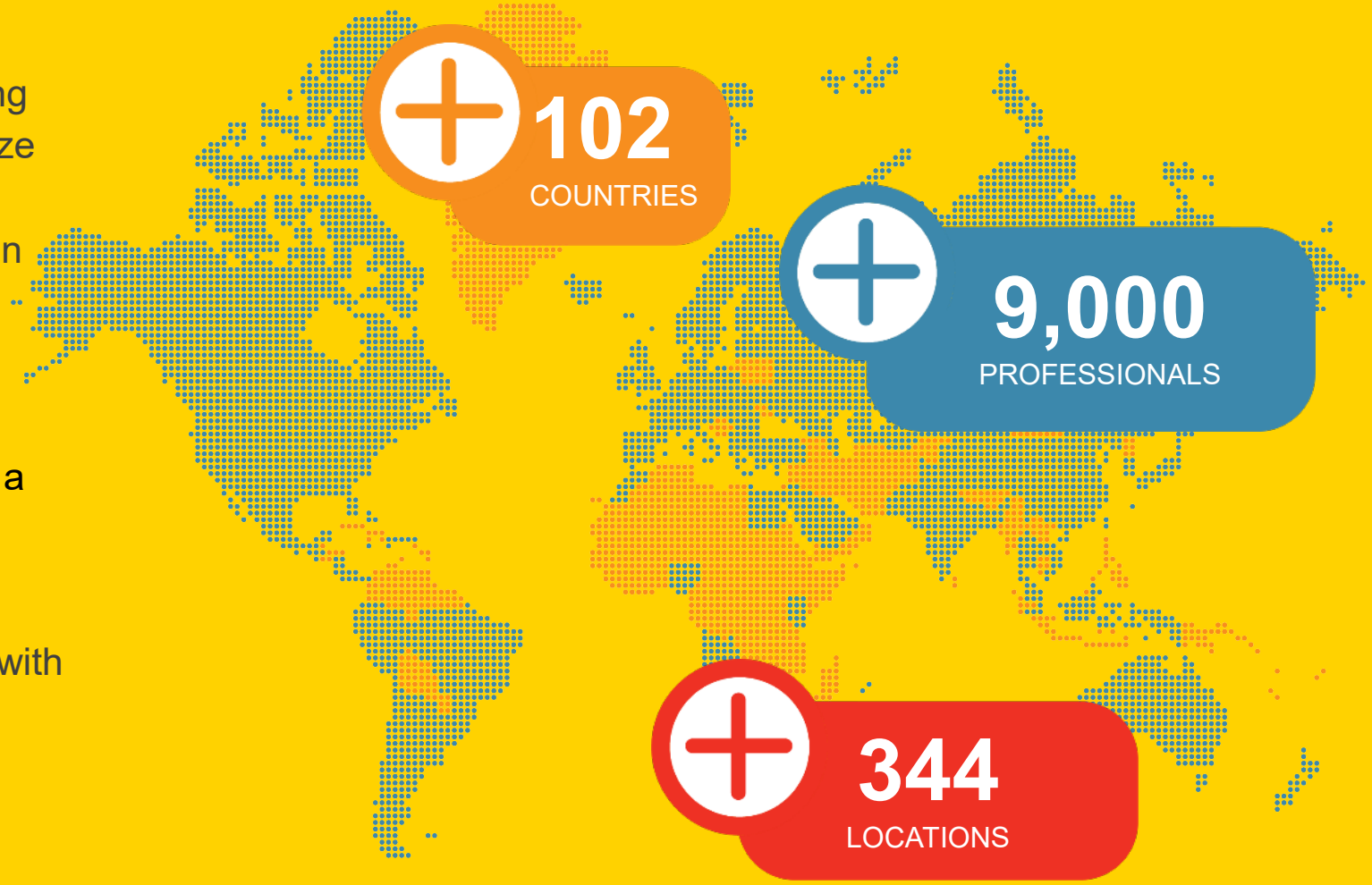
Our UHY Affiliation

UHY Consulting is a management consulting firm that inspires clients to imagine and realize a company with unlimited potential, leaving lasting results that strengthen an organization and its people.

Cybersecurity and Risk Consulting
Providing a comprehensive Cyber Readiness Program from assessments to a roadmap and remediation plan.

Affiliate of UHY LLP
A Top 30 national professional services firm with over 35 locations across the U.S.

Member of UHY International
Size and strength of a Top 20 Accounting and Consulting Network



An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Learning Objectives

KEY OBJECTIVES

- Understanding the Significance of Cybersecurity and Compliance
- Exploring the Regulatory Landscape
- Recognizing the Interplay Between Cybersecurity and Compliance
- Developing a Comprehensive Cybersecurity and Compliance Strategy

COMPLIANCE

Compliance is not your Blueprint

Avoid Checkbox Compliance

Compliance is an Ongoing Requirement

CYBERSECURITY

Security is not a Product but a Mindset

Security is an Ongoing Program

Security is not just an IT Responsibility

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

CPE

The questions below will be covered during this webinar. Please remember to respond throughout the presentation!

- To what extent do you believe cybersecurity and compliance should be integrated within modern enterprises?
- In your organization, how well are cybersecurity and compliance currently integrated and managed?
- Which benefits can result from a successful merger of cybersecurity and compliance?
- Which of the following best describes your organization's approach to managing cybersecurity and compliance integration?

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

The Evolution of Cybersecurity and Compliance

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Introduction

As the digital era continues to evolve, so does the complexity and volume of the data we generate. Today, the data landscape has transformed exponentially. We're not just talking about megabytes or gigabytes anymore. We're dealing with zettabytes and, soon, yottabytes of data.

Factors Driving the Data Explosion:

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

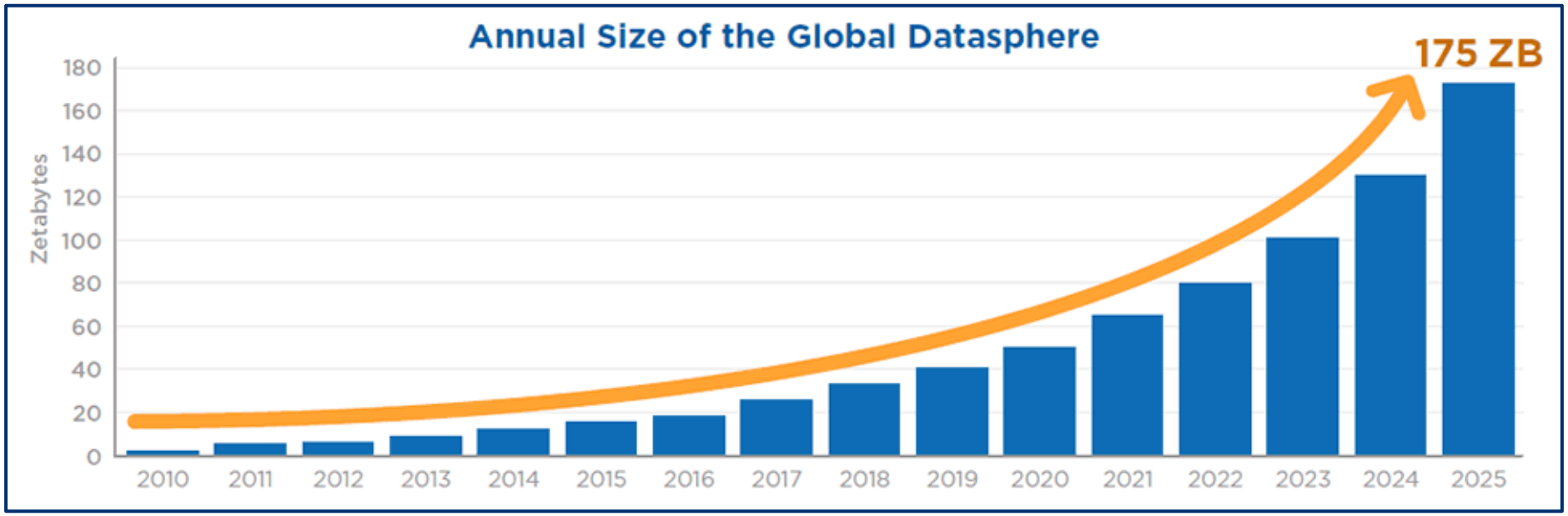
Data Landscape Transformation

30%

In 2025 nearly 30% of the world's data will need real-time processing as the role of the edge continues to grow.

49%

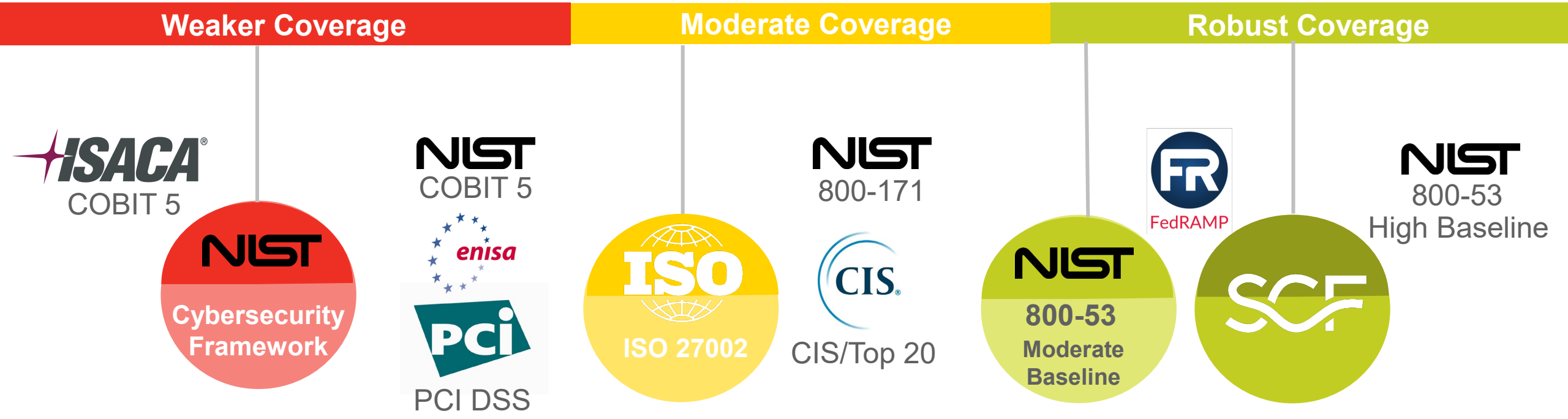
By 2025, 49% of all data in the world will reside in public cloud environments as the cloud becomes the new core.



Source: IDC Datasphere Whitepaper

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Security Frameworks



An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Frameworks & Regulations

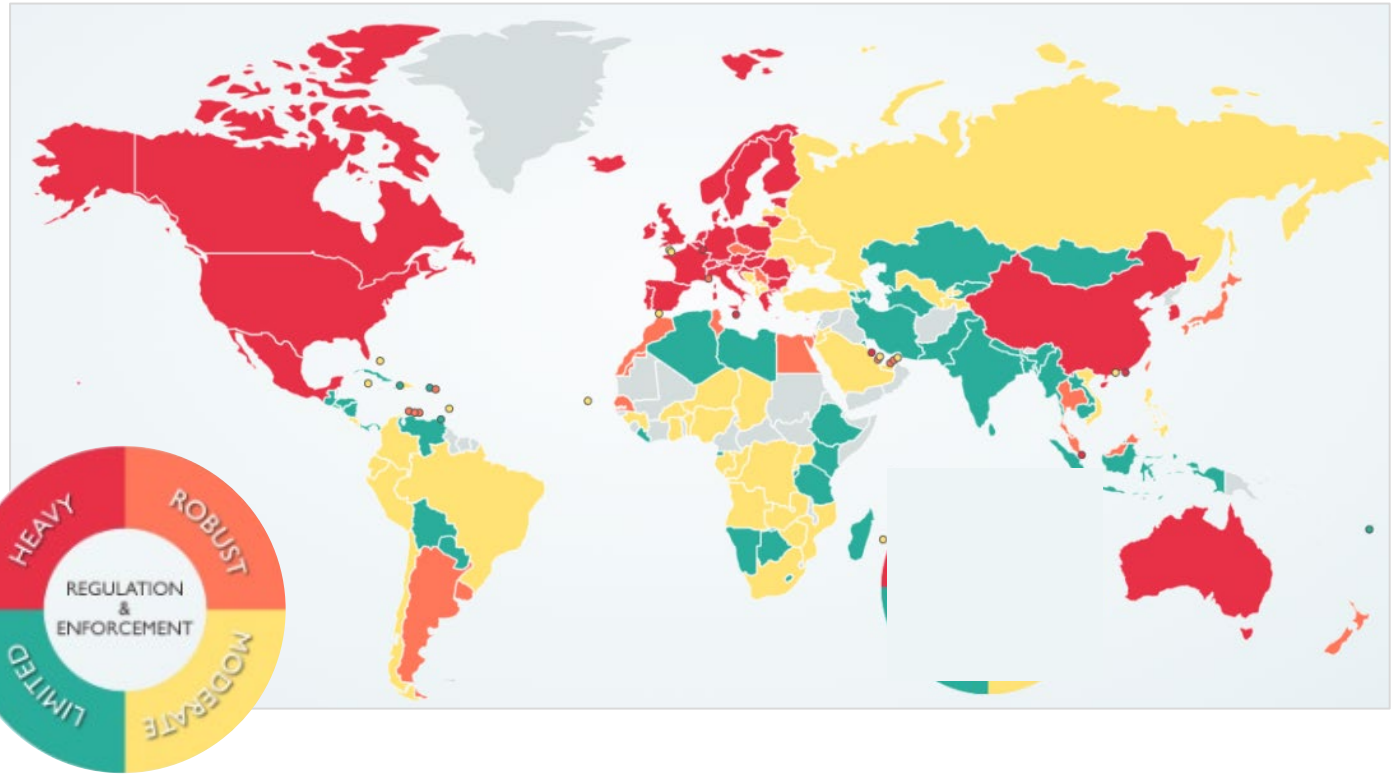
	BENCHMARK Designed for Specific Environments: Specific Prescriptive Controls	STANDARDS Provides Detailed Technology Implementation Guidance from Standards Body	FRAMEWORK Outlines Security Program Requirements and May Include Prescriptions, Methods	REGULATION Typically an Enforced Guideline with Prescribed Repercussions (Penalties)
CIS Benchmarks	✓			
DISA Checklists	✓			
Vendor Security Guidance	✓			
ISA/IEC-62443		✓		
ISO 15408 / Common Criteria		✓		
ISO 27001 and 27002		✓	✓	
NIST 800-53		✓	✓	
CIS Controls		✓	✓	
COBIT v.5			✓	
HIPAA			✓	✓
PCI			✓	✓
NERC CIP			✓	✓
SOX				✓
GLBA				✓
GDPR				✓

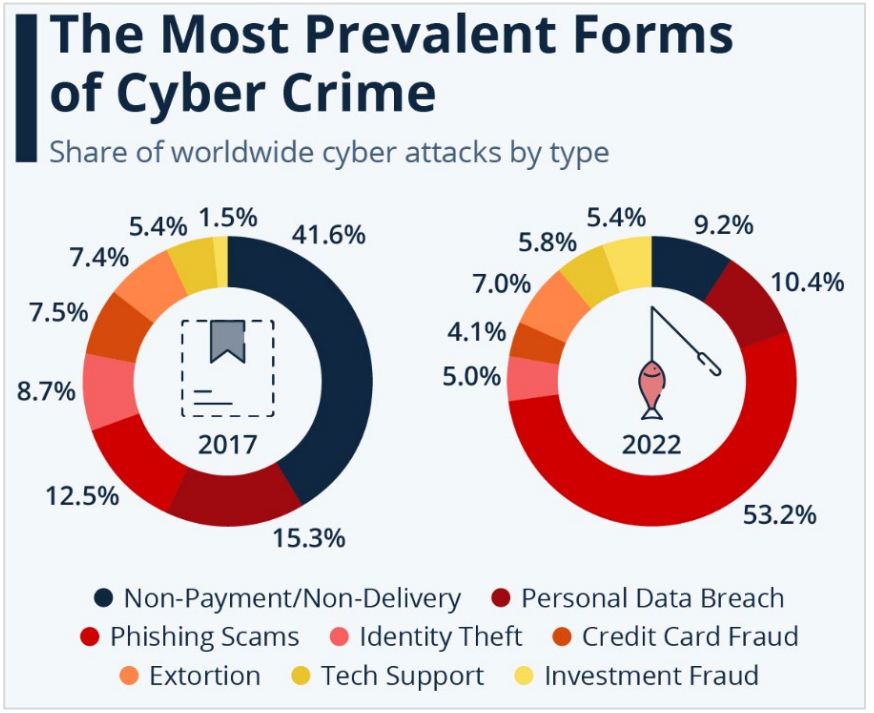
Source: Tripwire.com

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Privacy Laws Around the World

With the increasing reliance on digital platforms, data breaches and cyber-attacks have become commonplace. In parallel, global regulatory bodies are increasing efforts to impose stringent data protection and privacy requirements.





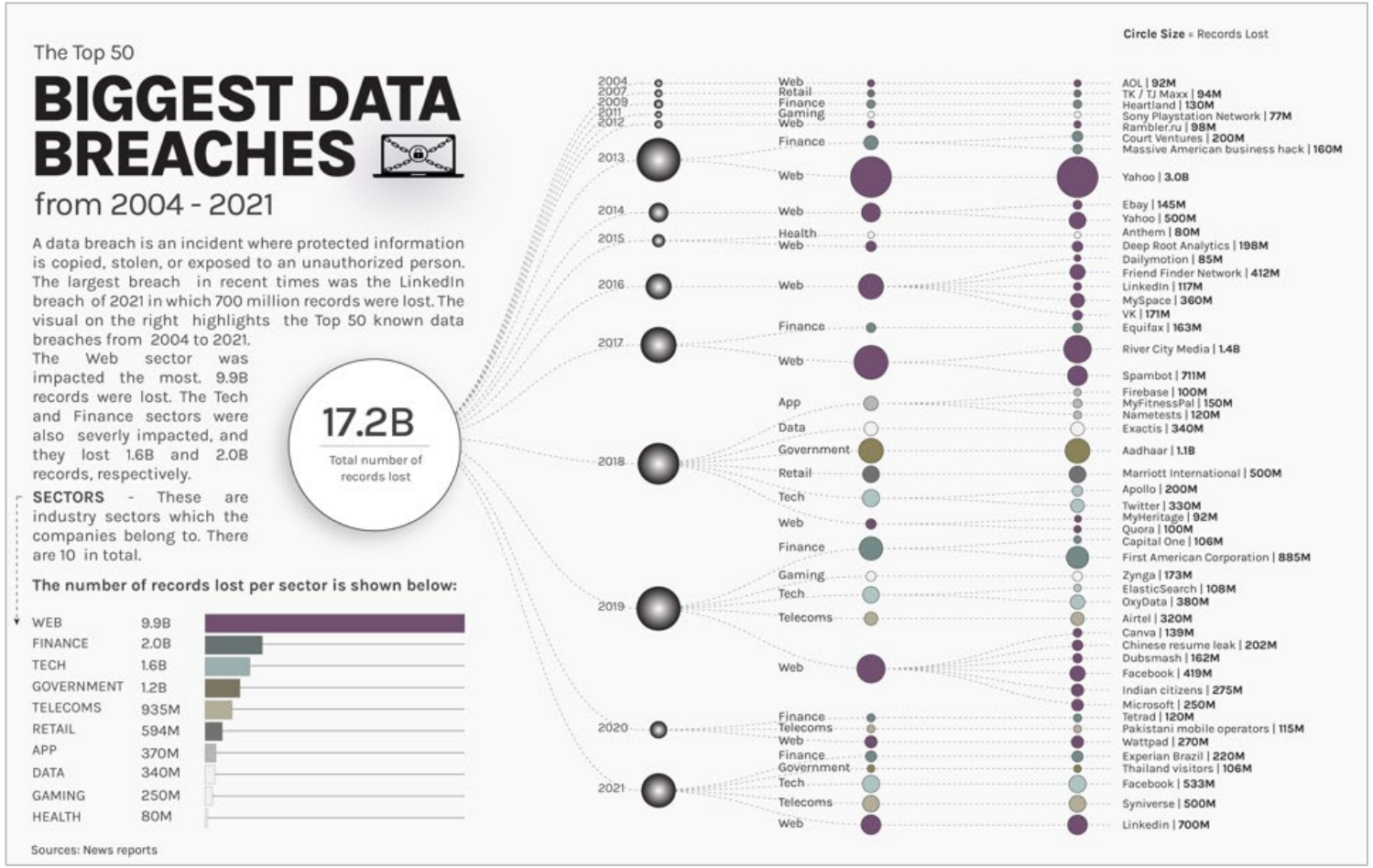
Source: Statista Market Insights, National Cyber Security Organizations

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Data Breaches and Hacks Through the Years

Let’s take a look at this in real time!

Events in Real Time



An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

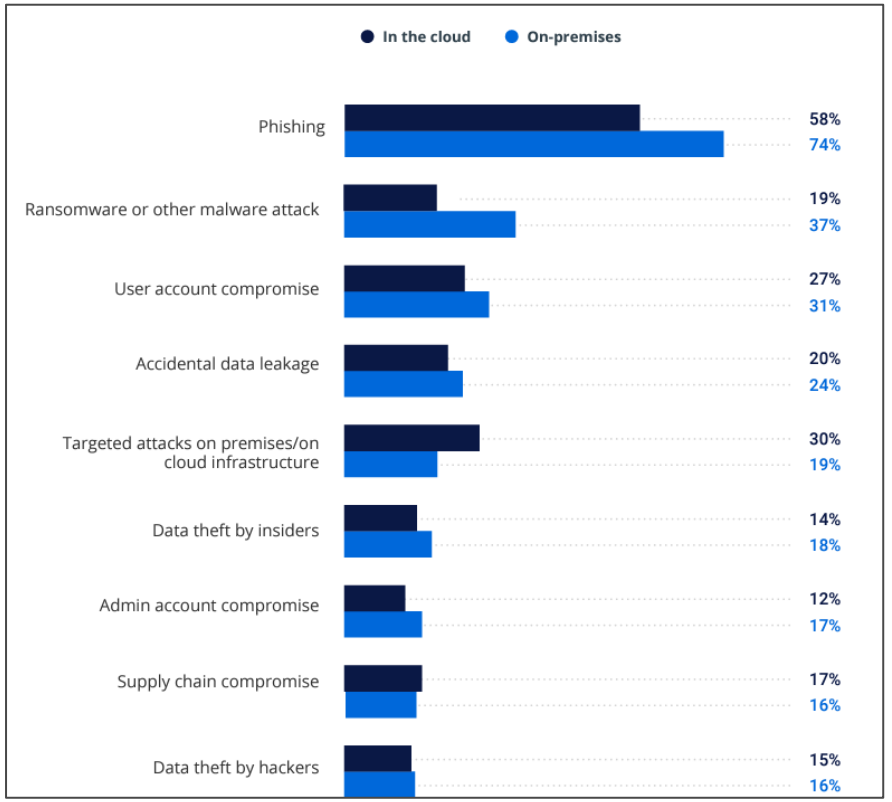
Organizations Experiencing Cyberattacks: Cloud vs On-Premises

68% of Organizations Have Experienced a Cyberattack in the Past Year

Security professionals know it's impossible to achieve full cybersecurity, which means that the remaining 32% had a very lucky year — or just haven't discovered the incident yet.

The results show that **on-premises infrastructure suffers more** cyberattacks than the cloud.

2023 Most Common Security Incidents
Cloud vs on-Prem



Source: Netwrix Hybrid Security Trends Report 2023

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Cost of a Data Breach 2023

USD 4.45M

Average total cost of a breach
The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million since 2020.

51%

Percentage of organizations planning to increase security investments as a result of a breach
While data breach costs continued to rise, IBM report participants were almost equally split on whether they plan to increase security investments because of a data breach. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies.

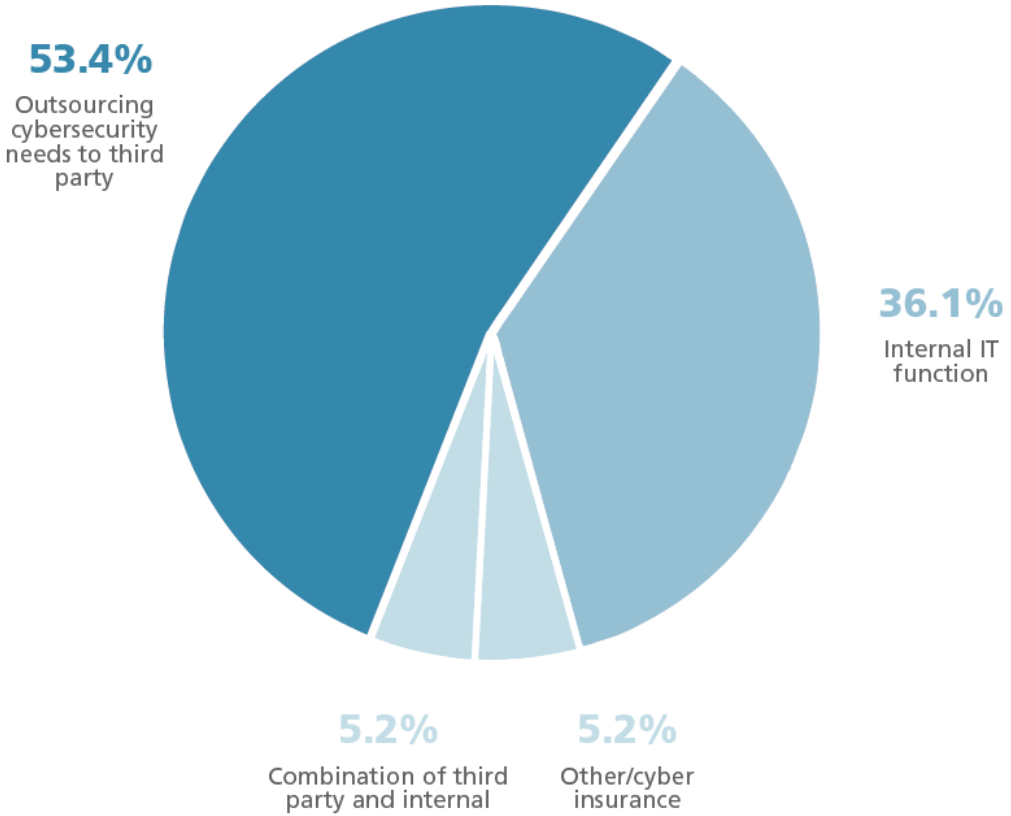
USD 1.76M

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.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

UHY 2023 Middle Market Survey

With increased connectivity and more devices in circulation than ever, seeking a **third-party provider** that specializes in Cybersecurity offers businesses an additional level of protection.



Limiting Vulnerability To Cyber Attacks

The internet has helped expand the amount of information exchanged and stored in the cloud rather than on hard drives, leading to increased opportunities for those databases to be hacked. According to respondents, middle market business owners are addressing their cybersecurity needs in a variety of ways.

Turning to Third-Party Vendors for Cybersecurity Needs

Businesses are dealing with balancing operations, staffing shortages, supply chain issues, economic uncertainty, and a litany of other external factors that make keeping up with the evolving cyber attacks increasingly difficult. With that context, 54% of respondents stated that they are hiring out their cybersecurity needs to third-party vendors.

With increased connectivity and more devices in circulation than ever, seeking a third-party provider that specializes in cybersecurity offers businesses an additional level of protection.

Thirty six percent shared that they have an internal IT function. Another 5% stated that they either had a combination of third-party resources and internal, some sort of cyber insurance, or stated that they rely on a third party to store important data and information making cyber protection a lower priority.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Cybersecurity and Compliance

Cybersecurity

- Primarily tech-driven, focusing on defending networks and systems from external threats.
- Over time, the scope broadened to address internal threats, continuous monitoring, and response strategies.

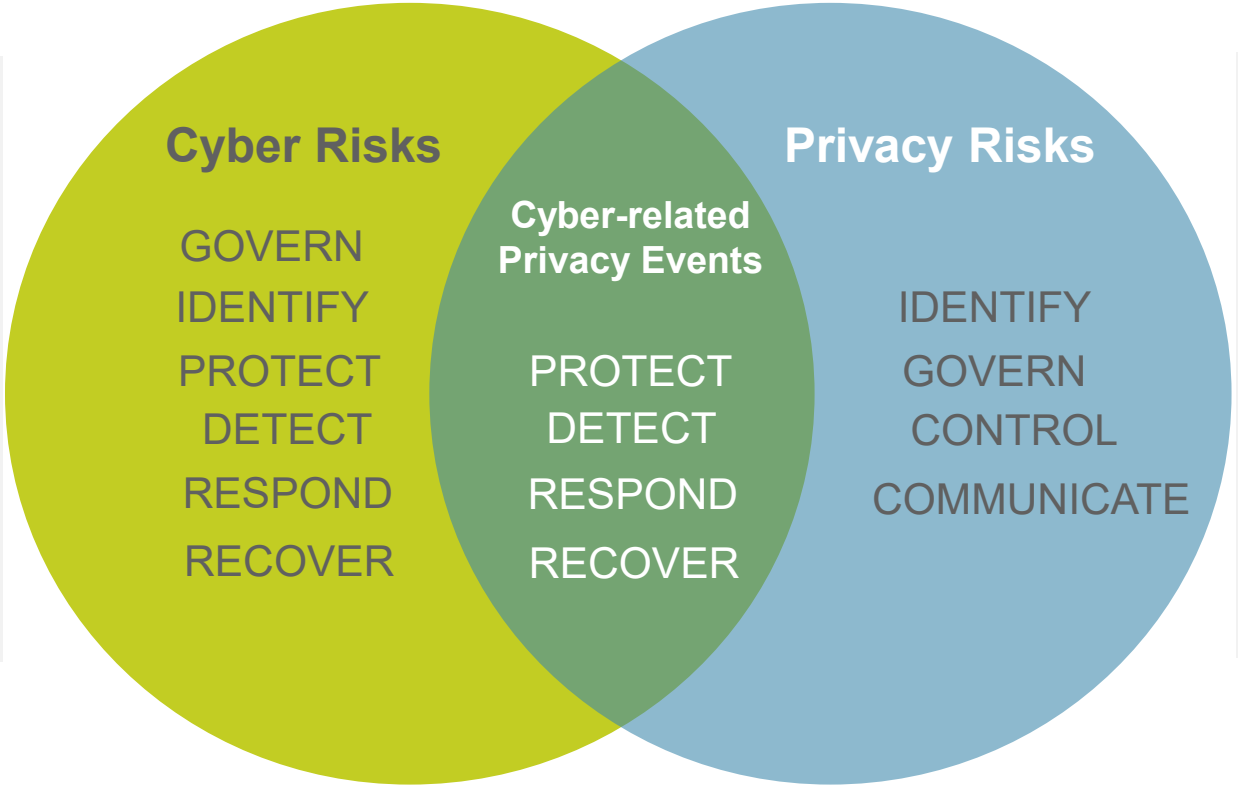
Compliance

- On the other hand, traditionally focuses on adhering to legal, regulatory, and policy requirements.
- With data becoming a greater asset, a necessity emerged to intertwine compliance with cybersecurity to protect this asset.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

The Confluence

Integrating cybersecurity and compliance for many companies **provides a holistic view** of organizational risks, facilitating better decision-making.



Regulations like GDPR, CCPA, and HIPAA mandate certain security measures, **blurring the lines** between cybersecurity initiatives and compliance mandates.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Solutions

How UHY Can Help

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

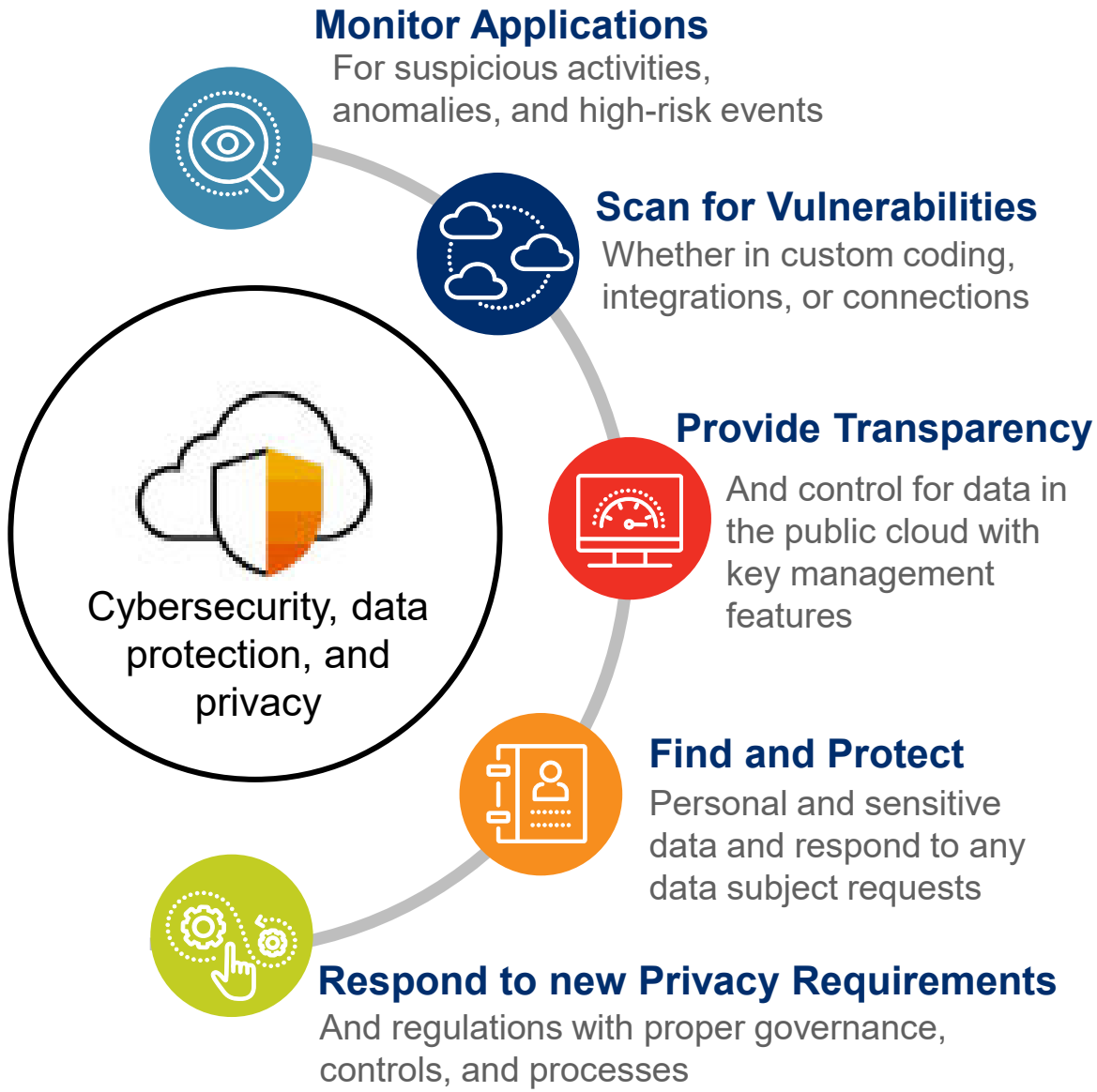
Is Integration Possible?

Developing a Comprehensive Cybersecurity and Compliance Strategy:

- Provide guidance on developing a holistic cybersecurity and compliance strategy.
- Outline best practices for creating policies, procedures, and controls aligning with cybersecurity and compliance objectives.

Implementing and Managing Integration:

- Describe practical steps for implementing and managing the fusion of cybersecurity and compliance within an organization.
- Address the role of technology, personnel, and training in successful integration.



Source: SAPInsider

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Roadmap

Developing a custom framework is an iterative process, that involves many steps.

Conduct Inventory

Identify where sensitive data resides, its flow within the organization, and the external entities

IT Structure & Stakeholders

Understand the current IT infrastructure and identify key stakeholders (RACI Matrix)

Regulatory

Identify all regulatory requirements.

Core Principles

Establish Data Minimization, Transparency, Confidentiality, Integrity, and Availability.

Map Frameworks

Create policies, protocols, and mechanisms tailored to identified needs

Threat Model

Develop a threat model of the environment.

Initial Risk Assessment

Promotions only work as well as the marketing.

Process for Collecting Evidence

Define a process for collecting evidence, automating where possible. Support audit and compliance efforts to demonstrate adherence.

Engage Stakeholders

Different departments need to understand data handling processes and technology interfaces.

Controls

Validate that controls are implemented and functioning and confirm that controls effectively mitigate or manage associated risks

Continuous Review

Regularly update the framework based on emerging threats

Benefits and Challenges Ahead

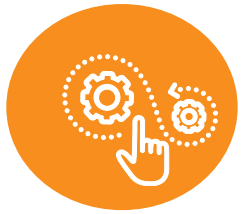
Cybersecurity Frameworks

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

UHY Consulting

Benefits of a Custom Cybersecurity/Privacy Framework

Considering two organizations, one using a generic cybersecurity framework and various compliance programs to address multiple regulatory obligations and another with a custom solution, the latter consistently outperforms in threat mitigation, stakeholder trust, and operational efficiency.



Tailored Risk Management

Each organization has distinct vulnerabilities based on its industry, operations, and technology stack.

Enhanced Data Protection

By focusing on unique threats and business-specific data handling processes, custom frameworks provide an additional layer of protection

Operational Efficiency

Custom solutions can be streamlined to the company's operations, and can integrate seamlessly with existing systems, making the operational workflow smooth.

Flexibility and Scalability

A tailored approach allows organizations to adapt their privacy and security protocols as they grow, shift markets, or incorporate new technologies.

Stakeholder Confidence

Custom frameworks signal to stakeholders—clients, partners, and shareholders—that the organization is committed to safeguarding its data assets.

Improved Compliance

Different industries and geographies have varying regulatory requirements.

Cost Efficiency

While there is an initial investment in developing a custom framework, it can lead to significant savings in the long term

Challenges Ahead – Custom Frameworks

Developing a custom framework demands an investment in time, manpower, and capital. This includes the costs associated with consultation, design, implementation, and testing of the new framework.

Custom frameworks also demand expertise that goes beyond generic cybersecurity knowledge. Finding and retaining professionals with the specialized skills needed can be challenging.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Wrap-Up

Interested in a customized Cyber Health Check?

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Wrap-Up and Blueprint for Success

The merger of Cybersecurity and Compliance by creating a **custom framework** is a logical response to the evolving digital landscape. Their fusion not only offers robust protection mechanisms but also reflects a proactive approach to risk management in the modern enterprise. Organizations that recognize and act upon this synergy stand to gain in terms of both security and operational efficiency.

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Interested in a customized Cyber Health Check?

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Exclusive Cyber Health Check Offering!

DON’T MISS OUT

Email cyber@uhy-us.com if your organization is interested in a cybersecurity health check.

As an exclusive offer for the attendees of this webinar --
The first 5 organizations who express interest today
will receive a complimentary Cyber Health Check!

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Questions?

Luke Nelson
lnelson@uhy-us.com
678-602-4370

Fred Charlot
fcharlot@uhy-us.com
832-647-3505

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Fred Charlot

Professional Expertise

- More than twenty years of experience managing, performing, and delivering information technology security solutions.
- Expert in IT security assessments, internal auditing, attack-and-penetration testing services, security analysis, digital forensics, and incident response.

Background

- Designing, assessing, and testing against multiple security standards, frameworks, and regulations; including ISO 27001/27002, Payment Card Industry Data Security Standard (PCI DSS), COBIT, and the National Institute of Standards and Technology (NIST).
- Communicating with and between executive leadership and technical teams to create an understanding of risk

Education

- Florida International University, Electrical Engineering
- Monmouth University, Computer Software Engineering

Fred Charlot
Director,
Cybersecurity Solutions

INDUSTRY EXPERTISE:
Oil & Gas
Energy
Finance & Insurance
Government & Municipalities
Medical Devices
Healthcare
Retail
Software

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Luke Nelson

Professional Expertise

- More than twenty years of experience identifying and assessing current state opportunities by working with them to improve their strategic, financial, operational, compliance, and IT processes and related technology
- Expert in utilizing risk-based methodologies and data analysis techniques to evaluate various business processes and their enabling application assets.

Background

- Supports Securities and Exchange Commission (SEC) compliant financial statements and Internal Control Over Financial Reporting (ICOFR) external audit opinions for publicly traded companies including interaction with the Public Company Accounting Oversight Board (PCAOB).
- Communicating with and between executive leadership and technical teams to create an understanding of risk

Education

- Bachelor of Business Administration, University of Georgia, Management Information Systems
- Bachelor of Business Administration, University of Georgia, Business Management

An independent member of UHY International. © 2023 UHY Consulting, Inc. All rights reserved.

Luke Nelson
Managing Director,
Cybersecurity Solutions and IT Risk

INDUSTRY EXPERTISE:
Automotive
Communications
Consumer Products
Finance & Insurance
Government & Municipalities
Healthcare
Manufacturing
Retail
Software