Understanding and Building IRM Maturity

Presenters:

Kyle Martin, Senior Director, Customer Success & Professional Services | NAVEX Global

Matt Crome, Manager, Customer Success & Partner Services | NAVEX Global

Agenda

- What is Integrated Risk Management?
- How mature are our customers?
- Evaluating the maturity of your program
- Getting started with an IRM program
- How technology can help (and where it doesn’t)
- Questions and discussion

What is Integrated Risk Management?

Gartner's Definition

Integrated Risk Management (IRM) is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

What is Integrated Risk Management?

Attributes

1. **Strategy**: Enabling and implementation of a framework, including performance improvement through effective governance and risk ownership
2. **Assessment**: Identification, evaluation, and prioritization of risks
3. **Response**: Identification and implementation of mechanisms to mitigate risk
4. **Communication and reporting:** Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response
5. **Monitoring**: Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives and the effectiveness of risk mitigation and controls
6. **Technology**: Design and implementation of an IRM solution architecture

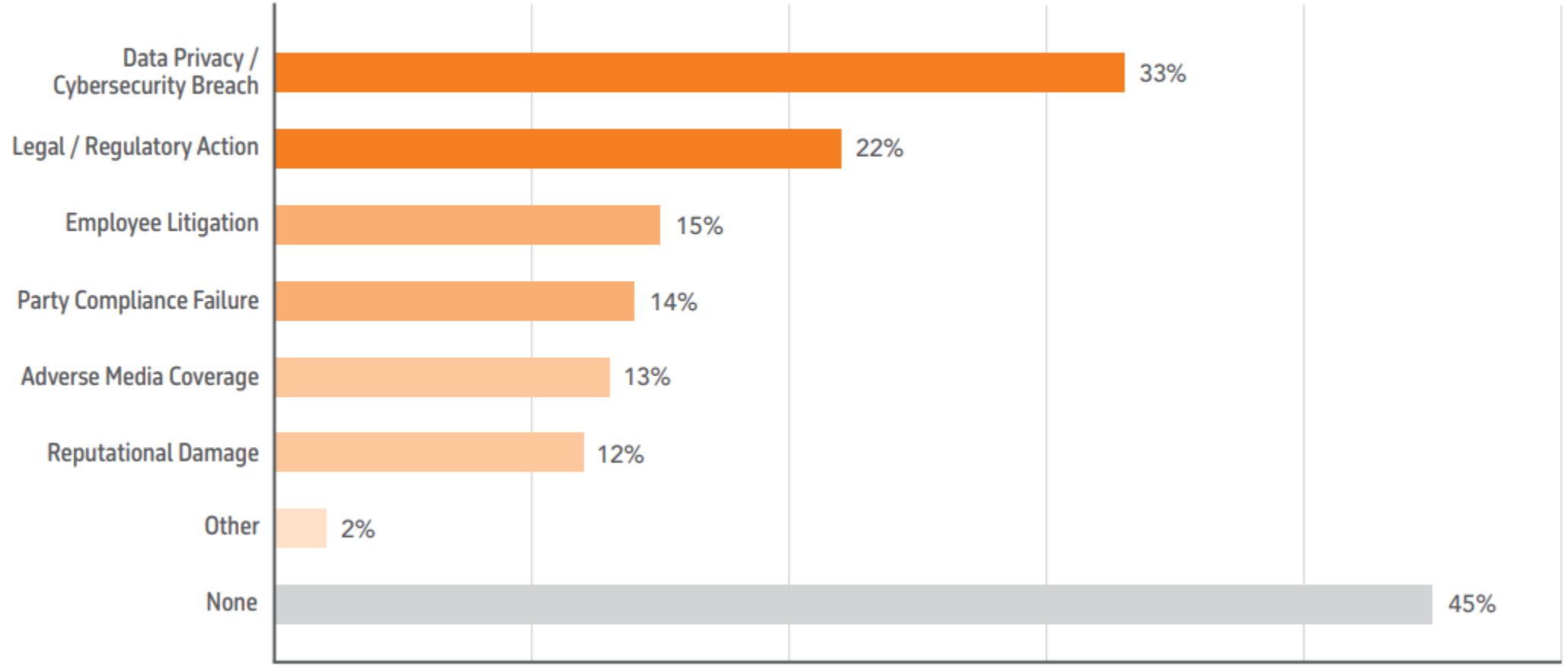
The Definitive Risk & Compliance Benchmark Report

Download Benchmark Report

Risk and Compliance Challenges Faced

1,000 Risk and Compliance Professionals assessed

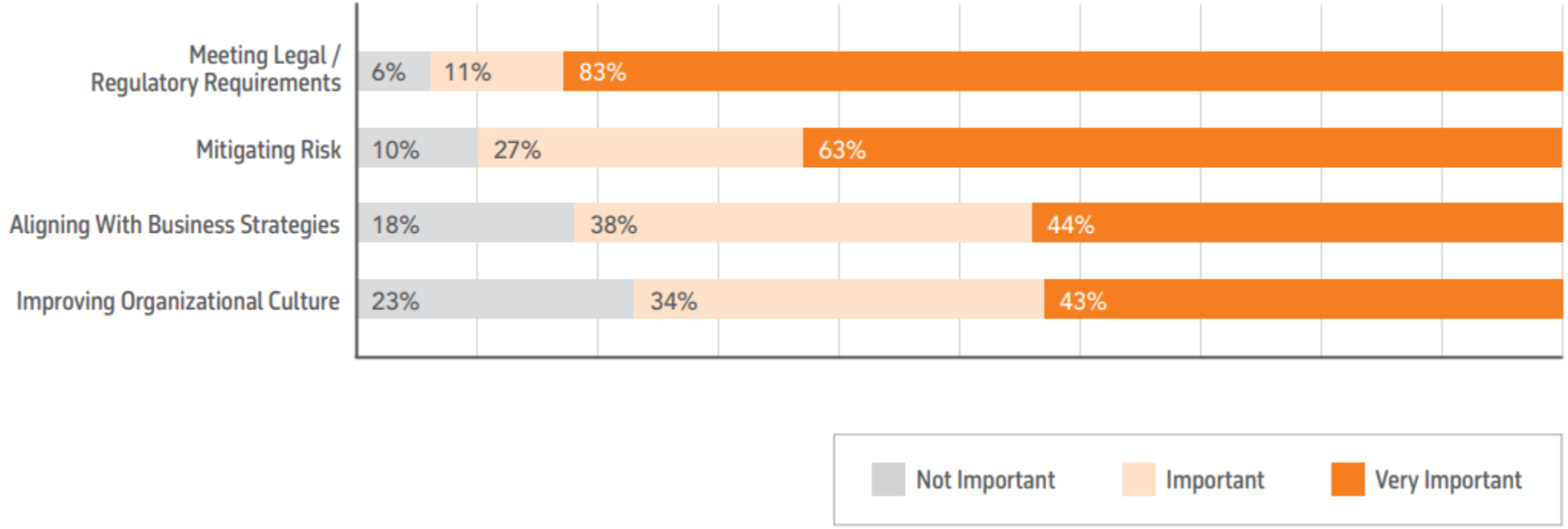
Shown: Percent of respondents who answered "yes" when asked if they had experienced any of the following in the past 3 years



Decision-Making Considerations

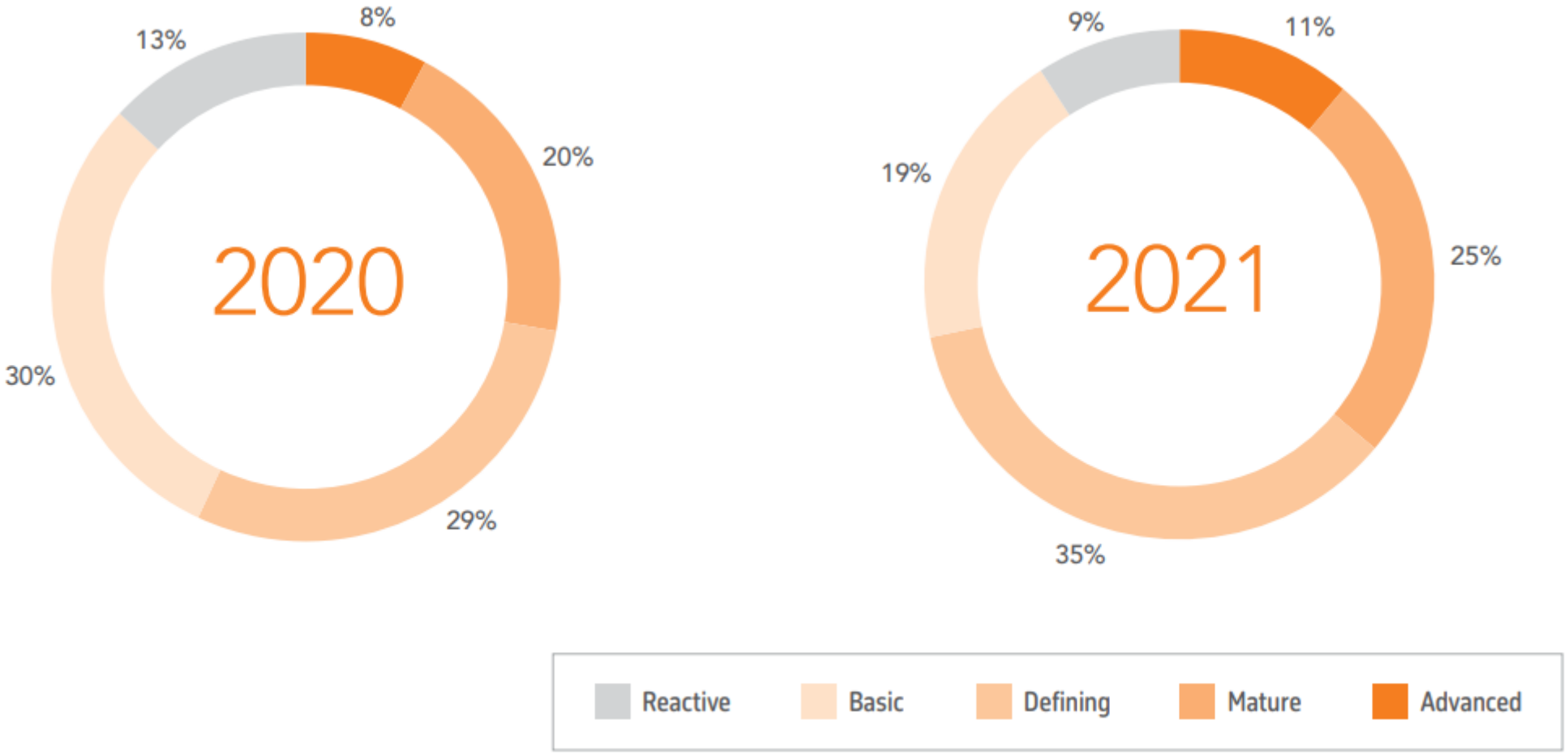
1,000 Risk and Compliance Professionals assessed

Shown: Responses to "How important are the following considerations in your R&C program's decision-making process?"



Where are we at today?

Risk & Compliance Program Maturity



Evaluating Maturity

Processes as part of TPRM Framework

Vendor Assessments

Contract Management

Control Testing

Policy Management

Risk Assessments

Business Continuity

Reactive

Tier 1

Ad hoc

Decentralized

Non-defined

Lacking process

Informal

Subjective

Basic

Tier 2

Consolidated

Centralized

Organized

Consistent

Objective

Still reactive

Defining

Tier 3

Process

Lifecycle

Quantitative

Qualitative

Clear Ownership

Mature

Tier 4

Managed

Integrated

Proactive

Cross-functional

Scheduled

Harmonized

Advanced

Tier 5

Optimized processes and use cases, by definition, are not isolated to that process or use case.

Programs and frameworks are optimized, and by achieving mature capabilities across those individual areas, organizations can support optimized end-to-end processes, satisfying all stakeholder groups.

Getting started

What authoritative sources of information do you seek to comply with?

- Start with what is mandated
- Validate against those controls
- Identify gaps
- Determine what can be resolved and what you must accept

Getting started

Do you have an organizational risk methodology?

- Establish a risk and compliance committee
- Build meaningful models for evaluation and scoring
- Create a culture from the top

Getting started

Pick one process to focus on.

- Do you want to improve your process for requesting and accepting new vendors?
- Do you need a better asset library?
- Do you have an upcoming audit where you can dig in on the control reviews?
- Focus on making things better, not making things perfect.

Evaluating key processes

Quick Wins

- Consolidating manual process (spreadsheets!)
- Organizational reporting
- Data relationships and repository

Goals

- Workflow and accountability
- Executive reporting
- Assessment and awareness

Tools can help

People

- Who will use it? When will they use it? Where will they use it?
- What value must the service deliver?

Process

- Fit for purpose
- Reevaluate processes, not people

Technology

- Finding business value
- Service enablement through technology

Tools can help

How does the process function OUTSIDE of technology?

- Committees
- Stakeholders
- Documentation

What are we trying to accomplish INSIDE of technology?

- Efficiency
- Accountability
- Visibility

Key Takeaways

Pick somewhere to start

Establish a risk and compliance committee

Aim for better, not perfect

Improve, Improve, Improve

NAVEX GLOBAL®

Protecting your people, reputation and bottom line

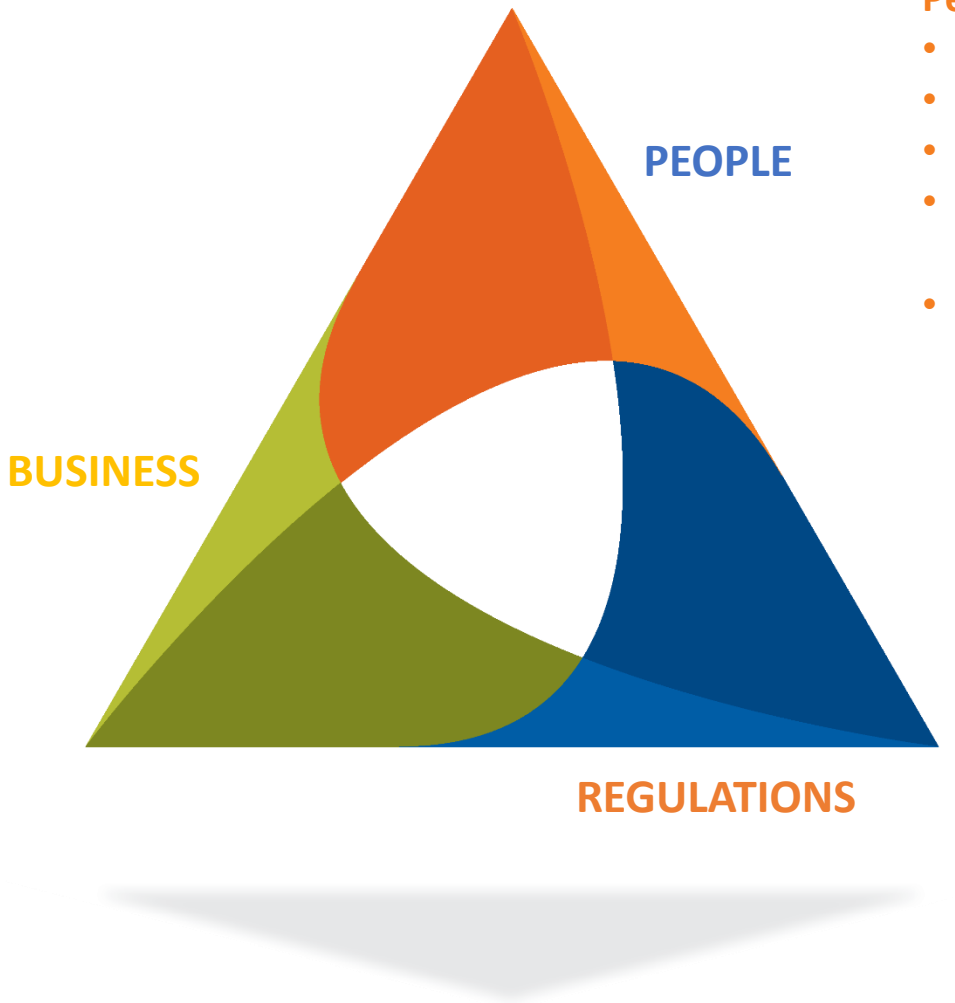
NAVEX Global's Integrated Risk & Compliance Solutions help our customers:

- Foster an ethical workplace culture
- Address complex regulatory compliance
- Manage business risk strategically

C-Suite and Board of Directors

Increasingly concerned about three broad areas of risk…

Business Risks:
- Data Security & Privacy
- Vendor Management
- Business Continuity
- Environmental Health & Safety
- Audit



People Risks:
- Ethical Lapses
- Employee Legal Actions
- Reputational Damage
- Negative Impact on Brand Image & Share Price
- Employee Recruitment, Retention & Loyalty

Regulations Risks:
- Bribery & Corruption
- Insider Trading
- Conflict of Interest
- Wage & Hour Issues
- Fraud

Building the World's Leading Risk & Compliance Solutions Company

Driving corporate performance by integrating all areas of ethics, risk & compliance

NAVEX GLOBAL®

#1 **Ethics & Compliance Suite**

- **PolicyTech** (PT) — Automated policy management
- **NAVEXEngage** (NE) — Online employee training
- **EthicsPoint** (EP) — Anonymous whistleblower solutions
- **RiskRate** (RR) — Vendor risk management
- **GRC Insights** (GI) — Data-driven benchmarking and best practices

+

LP LOCKPATH® Integrated Risk Management

Leading Integrated Risk Management (IRM) Platform

- Rapid momentum and visibility in the high-growth multi-billion IRM market
- Recognized by Gartner as a leader in the IRM market
- Shared relentless focus on customer success and satisfaction
- Well-poised for growth on a global scale

The most comprehensive suite of Risk & Compliance workflow solutions for the increasingly-complex global risk management marketplace

Ransomware Attacks in 2021: Compliance Lessons Learned

Tuesday, October 26th // 60 minutes // 12 PM CT

Register Now!

- Ransomware attacks on organizations are increasing at an alarming rate. Almost 2,400 organizations in the United States were victimized last year alone.
- Ransomware attacks, in which hackers lock up a computer system and demand a ransom to free up the system are a global problem. Paying a ransom comes with compliance risks. As the Office of Foreign Assets Control (OFAC) warned in an October 2020 advisory, paying ransoms potentially results in compliance violations if the cyber-criminal demanding the payment has a sanctions nexus.
- Mitigating cybersecurity risks, like ransomware attacks require a collective effort. You need coordination with compliance and information security leaders across your business.
- Join us for a fireside chat with Matt Kelly with Radical Compliance and Kyle Martin our Senior Director of Customer Success & Professional Services as we discuss best practices for your risk-based compliance program to be better prepared for the escalating cybersecurity threats.

Questions

Thank You!