IRBIZ™

WLS

When a cyber incident occurs, the responsibility of complying with legislative requirements often falls on the entire executive management team. After a breach occurs is not the time to begin understanding your legal requirements. This course will guide business, IT, and non-technical leaders through the incident response methods and procedures that align with industry frameworks such as US-CERT's NICSP (National Incident Response Plan) and Presidential Policy (PPD) 41 on Cyber Incident Coordination Policy. Participants will also learn best practices, mitigation methods, and gain understanding of current incident response methods.

49% of organizations lack the expertise and tools for adequate incident response.

(VMware's "The State of Incident Response 2021")

The average total cost gap between organizations having incident response teams and testing vs. not having either was $2.46 million in 2021, representing a 54.9% difference up 26.4% from 2020.

(IBM Cost of a Data Breach Report 2021)

IRBIZ™ CERTNEXUS®

AUDIENCE

This course is designed for primarily business, IT, and non-technical leaders, plus any additional personnel who are responsible for creating, governing, or complying with incident response policies and regulations. Common job roles include the following:

- IT Leadership
- Non-Technical Leadership
- Compliance Officers
- Communications Leadership

READINESS ASSESSMENT

Measure your organization's level of preparedness to comply with incident response and handling process regulations with our complimentary IRBIZ Readiness Assessment.

AAAGZ6ORZA
https://certnexus.com/irbiz-readiness/