GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

Webinar on

Creating A Cyber Incident Response Program That Works

Learning Objectives

- *Adopting a systematic approach to risk tracking to enhance the effectiveness of the Cyber Incident Program*
- *Cyber Incident Response: Getting started, research, training, testing and maintaining*
- *Standards and Best Practice: ISO 27001, ISO 27035, ISO 27005, ISO 22316 NIST, FFIEC, HIPPA, AND HITRUST*
- *Outlining the critical actions to take if an event affects the company or its partners*
- *Understanding an organizations' susceptibility to a Cyber Attack*

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

This webinar includes how to develop a CSIRT Policies, Program, Plan, Playbook, Training, and Exercises.

PRESENTED BY:

Dr. Michael C. Redmond, PhD is Consultant, Speaker, and Author. Her certifications Include MBCP, FBCI, PMP, CEM ISO 27001 Lead Implementer and Lead Auditor, as well as many other ISO certifications. She has recently been named on the list of "Women of Distinction for 2015" by Women of Distinction Magazine for her work in Cyber Security.

GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

On-Demand Webinar

Duration : 60 Minutes

Price: $200

Webinar Description

The best way forward is an efficient Incident Response Program that allows an organization to respond with speed and agility while empowering businesses to maintain continuous operations. Such a solution also reduces revenue loss, reduces fines and lawsuits and protects brand reputation.

Information Security, Governance & Risk, are all critical aspects of the planning and execution of the Information Security Plan. Who in your organization has a key responsibility to develop an information security governance program; review existing Information Security policies and standards to ascertain their adequacy in coverage scope against industry best practices, and update them as appropriate, taking into account compliance recommendations?

Establish Key Performance Indicators (KPI) to determine if your Information Systems Incident Response program meets business objectives and operational metrics for ongoing process improvement.

Learn how to develop a CSIRT Policies, Program, Plan, Playbook, Training, and Exercises.

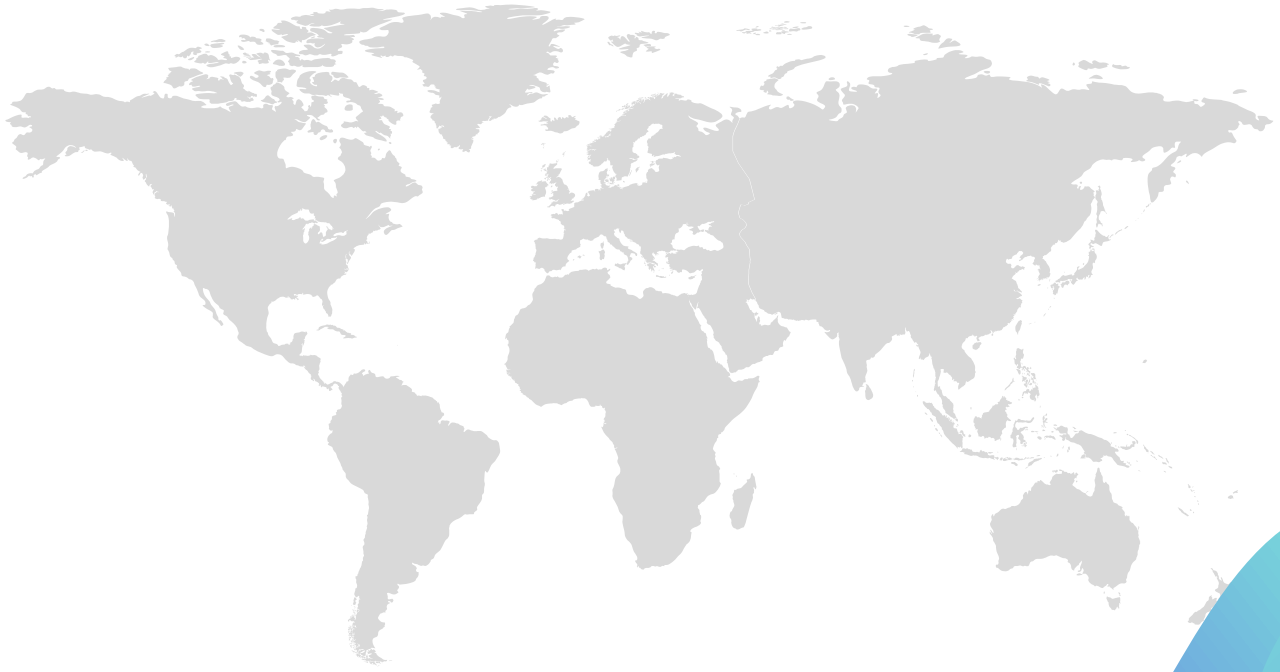
Who Should Attend ?

Information Security Managers

CEO, CIO, CFO, CSO

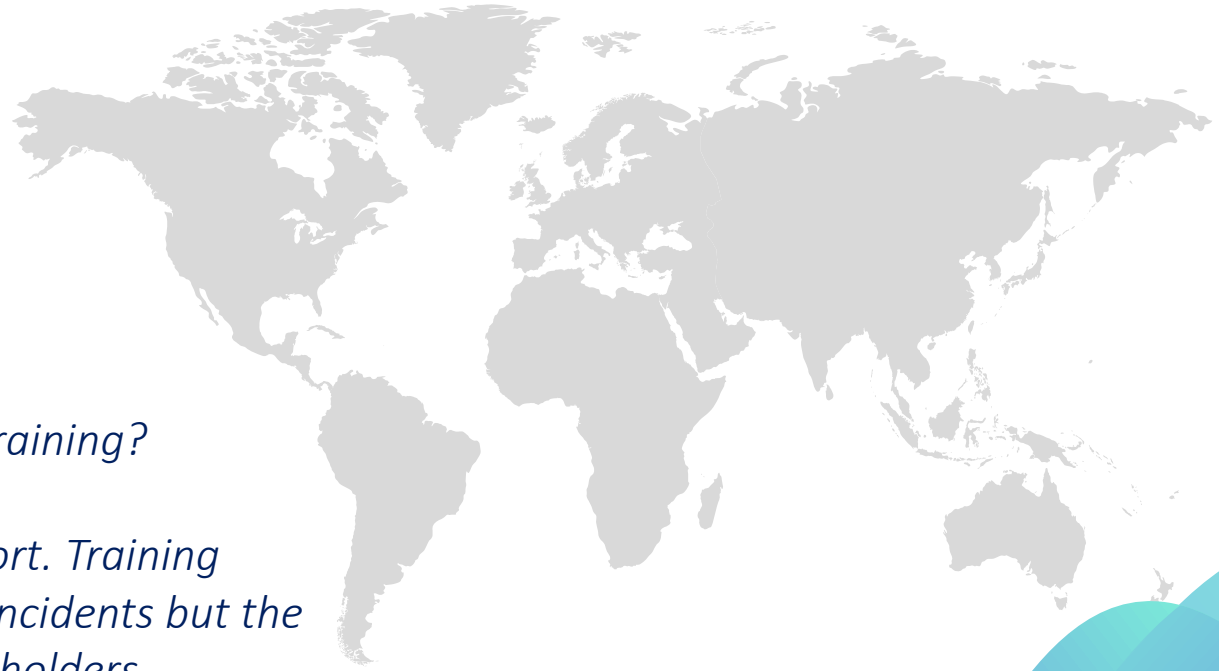
Technology Managers

Auditors



GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

Why Should Attend ?



Is your Cyber security Incident Response team trained to respond to an Incident? Many organizations thought they were and then the results proved otherwise.

Are you willing to risk your Business Reputation on their training?

Coordination of incident handling stops duplication of effort. Training should concentrate not only on the capability to react to incidents but the ability to utilize the resources to alert and inform its stakeholders.

We will cover tabletop tests, tabletop exercises, full Red Team Blue team training. Playing the role of an attacker can make your team better at defense.

Many companies exercises do not use formal blue teams. This is an effective way to have a more realistic idea of their true defensive capabilities. Exercises do not have to be expensive. There are so many types of tests.

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

To register please visit:

www.grceducators.com
support@grceducators.com
740 870 0321