Cyber Intelligence 4U

Cybercrime Course
2022-2023 Syllabus

Cybercrime Course

Course Overview

Cybercrime like ransomware and other attacks related to Covid-19 have grown enormously. This includes phishing, malicious websites, and malware targeting remote users. Cybercriminals are being despicably opportunistic taking advantage of vulnerable companies as we have seen notable spikes in attacks that can be correlated to key days in the COVID-19 news cycle.

Ransomware is a type of malware that is typically delivered via phishing emails. The ransomware malware uses encryption to make your digital assets unavailable and causes significant business interruption losses. Some ransomware events are reportable to regulatory agencies and many companies are unprepared for a ransomware event.

Other cybercrime is data exfiltration where attackers deliver malware like in a ransomware attack, but the payload steals data instead of encrypting your digital assets. Data breaches may incur heavy regulatory fines in addition to the costs of the data breach.

This two and one-half hour program is an introduction to cybercrime, cyber criminals and how to give yourself a fighting chance. Companies will be empowered by:

- The ability to understand ransomware holistically from a business perspective across regulation, insurance, cybersecurity and risk. Firms will be able to strategize how to lower their ransomware exposures and work with stakeholders to increase cyber resilience.
- The program provides an in-depth understanding of cybercrime and the financial exposures that can result and the typical attack vectors.
- Understanding where others have failed using case studies of cybercrime and its implications with an in-depth view into the how, what, where and impacts.
- A premier certificate from Pace Seidenberg's School of Computer Science and Information Systems, as validation of newfound cybersecurity knowledge, as well as access to a global network of likeminded cybersecurity professionals that make up Pace's Cybersecurity Advisory Board, cybersecurity panel discussions and insight interviews that are recorded for sharing with colleagues and peers.

Our programs are based on three years of research with the Fortune 1000 and cyber insurance industry to understand how to get businesses cyber resilient.

Suggested Text for Enhanced Cyber Risk Understanding

Managing Cyber Risk - Strategies for Surviving and Thriving in the age of Interconnectivity and Innovation, Evans; 1st Edition, ISBN-13: 978-0367177737.

Session 1: Introduction to Cybercrime (45 minutes)

Session Description
This session provides an introduction to cybercrime and the dark web from a real-world perspective. Cybercrime will remain a large-scale concern for years to come. From 2019–2023, approximately $5.2 trillion in global value will be at risk from cyberattacks, creating an ongoing challenge for corporations and investors alike according to Accenture.

This course will explore how cybercriminals work, how you and your firm are at risk and what you can do about it. A deep dive into the dark web and the world of the cybercriminal followed by solid advice to not become a victim.

We will study real life case studies that explore what has happened and how the cybercrime could have been avoided.

Session 2: Cyber Criminal Marketplace (45 minutes)

Session Description
This session outlines the methods cyber criminals use and the level of sophisticated organization that they will employ to cause harm. The ways and means that are utilized, how they are deployed and what the damages can be are explored.

We will explore the cybercrime marketplace and the tactics that are used by cyber criminals, their costs and their impacts.

Session 3: Defeating Cyber Criminals (60 minutes)

Session Description
This session provides the ability to understand where the financial exposure is and how to defeat it. We will explore cyber threat intelligence and how it is used to identify threats and remediate them before the cybercriminal attacks.

A focus on ransomware and effective strategies including cyber insurance, ransomware recovery time objectives and a cost-benefit analysis will be provided.

In this session, the focus includes:

- Financial exposure quantification
- Strategies to reduce risk
- Ransomware strategies
- Cyber threat intelligence

Exam for certification: 75 questions