Cyber Intelligence 4U

Executive Cybersecurity Ransomware Program 2022-2023 Syllabus

CYBER
INTELLIGENCE 4U

Executive Cybersecurity Ransomware Program and Workshop

Program Overview

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.

This program is a three hour hands-on session that will be focused on your company's ransomware strategy and provide a working plan for ransomware which includes ransomware preparation, restoration readiness, calculations of ransomware trigger amounts, cyber extortion cyber insurance sublimits, ransomware recovery time objectives and a ransomware cost-benefit analysis.

Company's participating will have access to the VRisk platform. VRisk is a hands-on cybersecurity platform that is used in Pace training. It provides the only defensible cyber risk quantification metrics according to Gartner. This program is ideal for the following roles: CEO, CRO, CISO, General Counsel, Board Members on the Audit and/or cybersecurity committees and anyone who participate in the ransomware strategy.

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 ransomware financial exposures that influence whether to pay the ransom or restore the systems, determination of cyber insurance ransomware sublimits, and a written corporate strategy to address ransomware.
- Hands on risk financial quantification with the VRisk product that allows the company to use live or dummy data to model ransomware financial exposures, perform a cost-benefit scenario analysis of paying a ransom vs. restoring the systems and delivers information on cyber insurance needs for ransomware.
- 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.

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.

Prerequisites – Cyber insurance policy in place, corporate revenue, a list of on-premise and cloud revenue generating assets, key decision makers should be present.

Session 1: Introduction to Ransomware (60 minutes)

Session Description
This session provides an introduction to ransomware from a real-world business perspective. A series of ransomware case studies are introduced that define what happened, how it happened, how it could be avoided, and its financial impacts in business language.

A deep dive into how ransomware works, the teams involved and the strategic options available to mitigate, transfer or accept risk. The session introduces the concept of digital asset cyber risk quantification that is based on three years of research with the Fortune 1000 and cyber insurance industry to understand risk exposures and their use cases. In 2001, 10% of a business was digital, today 85% of an organization's value is digital. The session focuses on understanding IT assets from a business perspective, cloud strategies, disaster recovery and business continuity programs, and the relationship between digital assets and ransomware.

Time will be spent tailoring information to the company's digital asset and cyber risk posture through a series of questions aimed to tailor the experience for the company. This will start to define strategic options for ransomware such as restoration readiness, the scope of a ransomware event and other key data points.

Session 2: Ransomware Financial Exposures (60 minutes)

Session Description
This session outlines the method to quantify ransomware exposures and uses the VRisk product to identify digital assets that may be interrupted, create cyber exposure algorithms and quantify the exposures to use in the use cases that ware part of the strategy.

Attributes related to the ransomware strategy will be utilized in the quantification analysis. Each attribute will be review in context with the company to produce several metrics and KPIs that are used in the strategy.

Session 3: Ransomware Strategic Plan (60 minutes)

Session Description
This session provides a final report that outlines the strategy that the company has helped to define using the calculation in the VRisk product.

In this session, the report provides includes:

- Formal strategy
- Ransomware readiness evaluation
- Ransomware cost-benefit analysis
- Ransomware recovery time objective
- Ransomware cyber insurance sublimit