PROJACS ACADEMY
by egis

Digital Security for Organizations in the Globalization Era

الأمن الالكتروني في عصر العولمة

16 – 20 October 2023

Dubai / UAE

Introduction

In the age of globalization, organizations face new challenges and opportunities in the digital realm. The rapid development of information and communication technologies (ICTs) has enabled unprecedented connectivity, collaboration, and innovation across borders and sectors. However, it has also increased the exposure and vulnerability of organizations to cyber threats, such as data breaches, ransomware, espionage, sabotage, and cyberattacks. These threats can compromise the confidentiality, integrity, and availability of organizational assets and operations, as well as the privacy and security of their stakeholders.

To address these challenges, organizations need to adopt a holistic and proactive approach to digital security, which encompasses not only technical measures, but also organizational policies, processes, and practices. Digital security is not a one-time project, but a continuous process that requires constant monitoring, evaluation, and improvement. It also requires the involvement and commitment of all levels of the organization, from senior management to frontline staff.

Who Should Attend?

This course is designed for managers, leaders, and professionals who are responsible for or involved in the planning, implementation, or oversight of digital security in their organization. The course is suitable for participants from various sectors and backgrounds, such as government, business, civil society, academia, media, or international organizations. No prior technical knowledge or experience in digital security is required.

Objectives

The main objective of this course is to provide participants with the knowledge and skills to design and implement a comprehensive digital security strategy for their organization. By the end of this course, participants will be able to:

- Identify the key concepts and principles of digital security and how they relate to organizational objectives and values
- Assess the current state of digital security in their organization and identify the main risks and gaps
- Develop a digital security policy that defines the roles, responsibilities, and rules for managing digital security in their organization
- Implement a digital security plan that outlines the actions, resources, and timelines for improving digital security in their organization
- Monitor and evaluate the effectiveness and impact of their digital security strategy and make adjustments as needed
- Promote a culture of digital security awareness and best practices among their staff and stakeholders

Course Outline

Day One

Introduction to Digital Security

- Welcome and introductions
- Course overview and expectations
- What is digital security and why does it matter?
- Key concepts and principles of digital security
- Digital security challenges and opportunities in the globalization era
- Group discussion: How does digital security affect your organization?

Day Two

Digital Security Assessment

- Digital security assessment framework and methodology
- Identifying your organization's assets and stakeholders
- Analyzing your organization's threats and vulnerabilities
- Evaluating your organization's existing digital security measures
- Group exercise: Conducting a digital security assessment for your organization

Day Three

Digital Security Policy

- Digital security policy framework and components
- Defining your organization's digital security vision, mission, and goals
- Establishing your organization's digital security roles and responsibilities
- Setting your organization's digital security rules and standards
- Group exercise: Developing a digital security policy for your organization

Day Four

Digital Security Plan

- Digital security plan framework and elements
- Prioritizing your organization's digital security needs and actions
- Allocating your organization's digital security resources and budget
- Scheduling your organization's digital security activities and milestones
- Group exercise: Creating a digital security plan for your organization

Day Five

Digital Security Monitoring and Evaluation

- Digital security monitoring and evaluation framework and tools
- Collecting and analyzing data on your organization's digital security performance
- Measuring and reporting on your organization's digital security outcomes and impact
- Reviewing and updating your organization's digital security strategy
- Group exercise: Conducting a digital security monitoring and evaluation for your organization

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a 7” Tablet containing a copy of the presentation, slides and handouts
- Post-assessment

Program Support

This program is supported by interactive discussions, role-play, case studies and highlight the techniques available to the participants.

Schedule

The course agenda will be as follows:

- Technical Session 08.30-10.00 am
- Coffee Break 10.00-10.15 am
- Technical Session 10.15-12.15 noon
- Coffee Break 12.15-12.45 pm
- Technical Session 12.45-02.30 pm
- Course Ends 02.30 pm

Course Fees*

- **3,200 USD**
  **VAT is Excluded If Applicable*

المقدمة

في عصـــر العولمة ، تواجه المنظمات تحديات وفرصًـــا جديدة في المجال الرقمي. أتاح التطور الســـريع لتكنولوجيا المعلومات والاتصـــالات (ICT) إمكانية اتصـــال وتعاون وابتكار غير مســـبوق عبر الحدود والقطاعات. ومع ذلك ، فقد زاد أيضًا من تعرض المؤسسات للتهديدات السيبرانية وضعفها ، مثل خروقات البيانات ، وبرامج الفدية ، والتجســس ، والتخريب ، والهجمات الإلكترونية. يمكن أن تضـــر هذه التهديدات بالسرية والنزاهة وتوافر الأصول والعمليات التنظيمية ، فضلاً عن خصوصية وأمن أصحاب المصلحة.

لمواجهة هذه التحديات ، تحتاج المنظمات إلى اعتماد نهج شـــامل واســـتباقي للأمن الالكتروني ، والذي لا يشمل فقط التدابير التقنية ، ولكن أيضًا السياسات والعمليات والممارسات التنظيمية. إن الأمن الالكتروني ليس مشروعًا لمرة واحدة ، ولكنه عملية مستمرة تتطلب مراقبة وتقييم وتحسين مستمر. كما يتطلب مشاركة والتزام جميع مستويات المنظمة ، من الإدارة العليا إلى موظفي الخطوط الأمامية.

الأهداف

الهدف الرئيسي من هذه الدورة هو تزويد المشاركين بالمعرفة والمهارات اللازمة لتصميم وتنفيذ استراتيجية أمنية الكترونية شاملة لمنظمتهم. في نهاية هذه الدورة، سيكون المشاركون قادرين على:

- التعرف على المفاهيم والمبادئ الأســـاســـية للأمن الالكتروني وكيفية ارتباطها بالأهداف والقيم التنظيمية
- تقييم الوضع الحالي للأمن الالكتروني في مؤسستهم وتحديد المخاطر والثغرات الرئيسية
- تطوير سياسة الأمن الالكتروني التي تحدد الأدوار والمسؤوليات والقواعد لإدارة الأمن الالكتروني في مؤسستهم
- تنفيذ خطة الأمن الالكتروني التي تحدد الإجراءات والموارد والجداول الزمنية لتحســـين الأمن الالكتروني في مؤسستهم
- رصد وتقييم فعالية وتأثير استراتيجية الأمن الرقمي الخاصة بهم وإجراء التعديلات حسب الحاجة
- تعزيز ثقافة الوعي بالأمن الرقمي وأفضل الممارسات بين الموظفين وأصحاب المصلحة

الحضور

تم تصميم هذه الدورة للمديرين والقادة والمهنيين المسؤولين عن التخطيط أو التنفيذ أو الإشراف على الأمن الالكتروني في مؤسستهم أو يشاركون فيه. الدورة مناسبة للمشاركين من مختلف القطاعات والخلفيات، مثل الحكومة أو الأعمال التجارية أو المجتمع المدني أو الأوساط الأكاديمية أو وسائل الإعلام أو المنظمات الدولية. لا يلزم معرفة أو خبرة فنية سابقة في مجال الأمن الالكتروني.