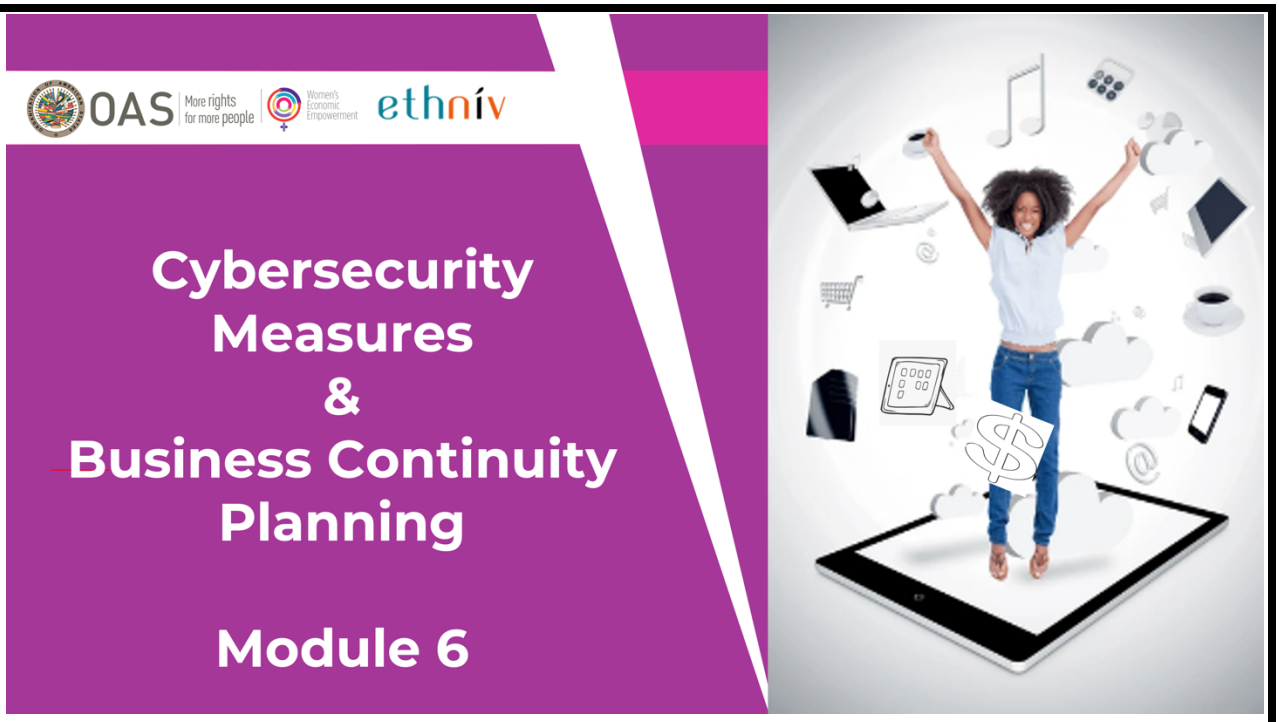

OAS WEE Project: Capacity Building in Digital Transformation for Success in the International Digital Marketplace

for Women MSMEs in the Eastern Caribbean

Cybersecurity Measures & Business Continuity Planning

Module 6

Foreword

The Secretariat for Integral Development (SEDI) of the General Secretariat of the Organization of the American States (GS/OAS) supports, facilitates, and fosters integral development in the member states in coordination with measures to strengthen democracy, multidimensional security, and the promotion of human rights.

The Executive Office (SEDI/EO) endeavors to mobilize resources for the formulation, promotion, and implementation of technical cooperation policies, programs, and projects in the area of integral development; Programs, projects and activities are geared towards strengthening human and institutional capacity of member states.

A key initiative of the Secretariat is the 'Economically Empowered Women for Equitable and Resilient Societies' (WEE) Project to empower women-led and women-owned MSMEs to actively participate in and benefit from the digital economy and build sustainable livelihoods. This project is being implemented in six countries of the Eastern Caribbean: Antigua and Barbuda, Dominica, Grenada, Saint Lucia, St. Kitts and Nevis, and St. Vincent and the Grenadines, and as such, this consultancy opportunity is established in support of this project.

The OAS-SEDI implements the WEE Project with funding from the U.S. Permanent Mission to the OAS and Meta.

The project SID2103: USDEP22/01

Disclaimer

The views expressed in this document are solely those of the author, Ethniv and do not necessarily reflect the views of the OAS.

Cybersecurity Measures and Business Continuity Planning

Learning Objectives

At the end of this session, you will be able to:

1. Understand the importance of business continuity management to an organization.
2. Understand the impact that business disruption can have on an organization.
3. The business continuity implementation process and implementation planning.
4. Identify the key security threats in the e-commerce environment.
5. Define how technology helps secure Internet communications channels, and protect networks, servers, and clients.
6. Appreciate the importance of cybersecurity as a part of an organization's BCP.

Module 6 Outline

Topic	Main Elements
1. Business Continuity Plan (BCP)	▪ Understand what a BCP is ▪ Know the main elements in a BCP
2. Cybersecurity?	▪ Understand what cybersecurity is ▪ Know the types of cyberattacks businesses can encounter ▪ Know how to protect your business against cyber attacks

6.1 Business Continuity Planning (BCP)

6.1.1 What is a BCP?

A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.

One of the main threats to the continuity of businesses is a cyberattack, making cybersecurity a critical aspect of a BCP.

6.1.2 Understanding Business Continuity Plans (BCPs)

BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include

natural disasters—fire, flood, or weather-related events. They may also be due to human error, application failure, power outage or service provider failure—and **cyber-attacks**.

Once the risks are identified, the plan should also include:

- Determining how those risks will affect operations
- Implementing safeguards and procedures to mitigate the risks
- Testing procedures to ensure they work
- Reviewing the process to make sure that it is up to date

6.1.3 How to Create a Business Continuity Plan

There are several steps many companies must follow to develop an effective BCP. They include:

- **Business Impact/Risk Analysis**: Here, the business will identify functions and related resources that are time sensitive.
    - Identify critical functions the organization must perform to continue to deliver services.
    - Identify risks to critical functions.
    - Rate risks according to the likelihood of them occurring and the level of impact.

- **Development of the Prevention/ Recovery Plan**: In this portion, the business must identify and implement steps to prevent damage/ recover critical business functions. A continuity team must be created. This team will devise a plan to manage the disruption.

  Consider these elements of the Plan:
    - Emergency Response Protocols
    - Data Backup and Recovery
    - Alternative Work Arrangements
    - Supply Chain Management
    - Financial Management
    - Communication Plan

- **Training/Testing of the Plan**: The continuity team must be trained, and the Plan must be tested. Members of the team should also complete exercises that go over the plan and strategies.

- Emergency Response Protocols
- Data Backup and Recovery
- Alternative Work Arrangements
- Supply Chain Management
- Financial Management
- Communication Plan

6.2 Cybersecurity

6.2.1 What is Cybersecurity

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats.

It is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

6.2.2 The cornerstone of Cybersecurity

A comprehensive cybersecurity program seeks to address these key concepts:

- **Confidentiality**: This refers to maintaining the privacy of sensitive data and preventing any unauthorized access.

- **Integrity**: This refers to preventing tampering, modifications, and alterations to sensitive business data by users with malicious intent.

- **Availability**: Providing authorized users timely and uninterrupted access to corporate data.

6.2.3 An effective Cybersecurity Approach

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks.

- **People**

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

- **Processes**

Organizations must have a framework for how they deal with both attempted and successful cyber-attacks. This framework should explain how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

- **Technology**

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber-attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

6.2.4 Types of cybersecurity threats

- **Phishing** is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber-attack. You can help protect yourself through education or a technology solution that filters malicious emails.

- **Social engineering** is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

- **Ransomware** is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered, or the system restored.

- **Malware** is a type of software designed to gain unauthorized access or to cause damage to a computer.

6.2.5 Best Practices in Cybersecurity

- **Data Protection Methods** - Data protection is a strategy set to secure privacy, availability, & integrity of data.

    - **Identify Sensitive Information** - The first step is to conduct a thorough inventory of all data assets and classify them based on their sensitivity.

    - **MFA/ 2FA (DUO)** - Duo multi-factor authentication protects your organization's data at every access attempt, from any device, and from any location.

    - **Backup, Backup, Backup** - Data backup means creating a copy of the data on your system that you use for recovery in case your original data is lost or corrupted.

    - **Encryption** - Data encryption is a security method that translates data into a code, or ciphertext, that can only be read by people with access to a secret key or password.

    - **Antivirus/Anti-Malware Protection** - Antivirus usually deals with the older, more established threats, such as Trojans, viruses, and worms. Anti-malware, by contrast, typically focuses on newer challenges, such as polymorphic malware (allowing subroutines to use variables of different types at different times), and malware delivered by zero-day exploits.

    - **Firewall** - A firewall is a security system designed to prevent unauthorized access into or out of a computer network.

    - **Limited Access to Authorized Personnel Only** - Data governance is the practice of ensuring that data is properly managed, secured, and used to

support business objectives and compliance requirements. One of the key aspects of data governance is to restrict data access to authorized personnel, based on their roles, responsibilities, and needs.

- **Perform regular updates** - Regular security updates fortify systems against potential breaches, ensuring that confidential information remains protected from unauthorized access.

- **Customer Protection Methods** - Companies can protect customer data through various technical tools and strategies, but also through the implementation of policies geared towards the protection of customer data.

  - **GDPR (General Data Protection Regulation)** - The GDPR sets out detailed requirements for companies and organizations on collecting, storing and managing personal data. It applies both to European organizations that process personal data of individuals in the EU, and to organizations outside the EU that target people living in the EU.

  - **Data Privacy (Policies)** - Most data protection policies have three key focuses: (1) Data security – protecting data from malicious or accidental damage; (2) Data availability – Quickly restoring data in the event of damage or loss; and (3) Access control – ensuring that data is accessible to those who actually need it, and not to anyone else.

  - **Data Protection (practice) cookies, limited Data collection -** Cookies are tools stored within browsers that track a user's experience online. Cookies can track which websites users visit and how frequently they visit them. They can also track a user's behavior on an individual website, such as the time spent on a page, clicks to another page, purchases, video views, and more. Marketers can use these kinds of cookies to determine how to serve a user different kind of content based on their browsing history.

  - **Penalties** – These are consequences for a breach of consumer date protection and can include: Issuing warnings and reprimands; Imposing a temporary or permanent ban on data processing; Ordering the rectification, restriction or erasure of data; and. Suspending data transfers to third countries.

- **Know Your Customer (KYC) Methods -** KYC standards are designed to protect against fraud, corruption, money laundering and terrorist financing. KYC involves several steps to: establish customer identity; understand the nature of customers' activities and qualify that the source of funds is legitimate; and assess money laundering risks associated with customers.

    - **ID Card Verification** - Documents such as a government-issued ID (driver's license or passport) and public utility bills can be used for KYC verification. Other methods of identity verification can include the use of biometrics and face verification.

    - **Business Registration & Business in Good-standing -** Asking customers to provide a range of basic information about their business operations and individuals is a typical KYC method and can include information on business registration, the names of the company's directors, business addresses, and information from banks indicating creditworthiness.

    - **Banking Verification/ Address Verification –** See information above on Business Registration & Business in Good-standing.

    - **Biometric verification -** These traits can include fingerprints, facial recognition, iris scans, and voice patterns. The biometric verification flow involves capturing these traits and comparing them with stored data to authenticate the user's identity.

    - **Policies and practices (ex repeat annually/ biannually)** – These involve all the necessary actions to ensure their customers are real and assess and monitor risks.

    - **Penalties** - In some industries, you need a KYC program to meet compliance requirements. If you don't comply with KYC/AML laws, you could be fined or even imprisoned.

- **Website Security Methods** - Website security refers to the measures taken to secure a website from cyberattacks. That may include protecting a website from

hackers, malware, scams or phishing, and errors. In this sense, website security is an ongoing process and an essential part of managing a website.

- **SSL Certification (Free, Paid)** - SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser. Companies and organizations need to add SSL certificates to their websites to secure online transactions and keep customer information private and secure.

- **Application Security -** Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

- **Firewall (Enterprise)** - Enterprise Firewalls are a network security system that sits between the internal network and the external network. It is a data security protection system that permits or restricts data transfer based on predefined rules, which can prevent unauthorized remote login, Distributed Denial-of-service, and viruses and worms spreading on the network.

- **Antivirus/ Ransomware Protection** –
  - Antivirus solutions help detect and remove trojans, rootkits and viruses that can steal, modify, or damage your sensitive data.
  - Ransomware protection includes technologies, strategies, and tools that can prevent cybercriminals from performing successful ransomware attacks. Ransomware attackers encrypt sensitive data and require organizations to pay a fee to regain access to their information assets.

- **Backup – 3-2-1 -** The 3-2-1 backup strategy simply states that you should have 3 copies of your data (your production data and 2 backup copies) on two different media (disk and tape) with one copy off-site for disaster recovery.

- **Regular Updates/ Automated Updates -** Software updates are pivotal in enhancing security, fixing vulnerabilities, and ensuring your systems run smoothly. Ignoring them can expose your devices to various risks, including cyber threats and reduced performance. Keeping your operating system,

applications, and antivirus software up to date is essential to maintaining a secure and efficient digital environment.

- **PCI DSS Compliance** - Payment Card Industry Data Security Standard is a mandated set of requirements agreed upon by the major credit card companies. The security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as a form of payment.

- **HIPPA Compliance -** The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance.

Activity

Identify key elements of your own BCP with a focus on cybersecurity. Please use the table below to develop your plan, identifying the risk, the response and the recovery process and procedures. Remember to allocate a budget!

Table: Basic Cybersecurity BCP

Risk/Potential Disaster	Probability Rating	Description of controls	Impact Rating	Potential consequences	Potential Solutions
Disclosure of sensitive information					
Loss of records					
Cyber crime					

Note: Rating: 1-5, with 5 being the highest.

Resource: https://coe.caribbeanchambers.net/resource-hub/business-resilience/