WIPO
ICT Leadership
Dialogue
(WILD)

Theme 5 : Cyber resiliency and best practices

The importance of cyber resilience in an intellectual property office

Presented by M. KENNE TIOTSOP Alain Aurelien

April 14, 2025 | Geneva

ORGANISATION AFRICAINE DE LA
PROPRIETE INTELLECTUELLE
OAPI

INTRODUCTION

In a context where cyberattacks continue to increase in frequency, intellectual property offices find themselves particularly exposed. They are becoming prime targets for cybercriminals.

With the rise of digital technology, our offices must remain operational despite incidents; investing in robust cyber resilience has become essential.

This cyber resilience, which combines preventive measures and rapid incident response capabilities, is now essential to ensure business continuity.

Our presentation will focus on the following points :

I- Assessing cybersecurity risks in an organization;

II- Implementing an architecture to strengthen the resilience of your IT infrastructure;

III- Some best practices for incident monitoring and detection;

IV- Implementing an incident response plan;

V- Business continuity and recovery plan (BCP/BRP)?;

VI- The importance of raising awareness about cybersecurity among our office staff;

I- Assessing cybersecurity risks in an organization

Risk assessment aims to identify, evaluate, and mitigate potential risks to a company's IT assets and sensitive data. How can risks be assessed to address threats (from natural disasters, power outages, hardware failures to cyberattacks, data breaches, and human error)?

1- Identify all IT assets;

2- Identify potential threats to these assets;

3- Assess the vulnerabilities of each asset;

Look for weaknesses that threats could exploit, such as outdated software, incorrect configurations, and weak passwords.

4- Calculate the risk level associated with each threat/vulnerability;

5- Document steps 1 to 4;

All reports generated at this level are useful for internal communication, decision-making, and risk management planning.

6- Periodically review the risk assessment to stay up-to-date and respond to changes.

II- Implementing an architecture to strengthen the resilience of your IT infrastructure

By designing your architecture to anticipate outages, attacks, and incidents, you can ensure business continuity and minimize unwanted disruptions.

1) System Redundancy
Use of redundant servers and networks;
Implementation of clusters and automatic failover systems;

2) Network Segmentation
Use of firewalls and VLANs;
Isolation of critical services;

3) Data Protection
Regular backups and restore tests;
Encryption of sensitive data;

4) **Identity and Access Management**
Implementation of strong authentication;
Management of access privileges.

III- Some best practices for incident monitoring and detection

Monitoring and incident detection play a crucial role in the resilience of your IT infrastructure.

By quickly identifying suspicious activity and detecting security incidents, you can take preventative measures to minimize potential damage.

1) Implement a log management system

Centralized log collection;

Event analysis and correlation;

2) Use of intrusion detection solutions

Implementation of probes and sensors;

Real-time monitoring of suspicious activity;

3) Implementation of alert systems

Configuration of automated alerts;

Establishment of an escalation procedure;

IV – Implementing an incident response plan

Implementing an incident response plan is an essential component in strengthening the resilience of your IT infrastructure.

1) Establishing a response team

Designating an incident response team;

Establishment of a clear hierarchy and defined roles;

2) Defining incident management procedures

Developing detailed procedures;

Classifying incidents and assessing their severity;

3) Communication and coordination

Establishment of secure communication channels;

Coordination with internal and external stakeholders;

4) Post-incident analysis and improvements

Evaluating actions taken and lessons learned;

Regularly updating the incident response plan.

V - Business continuity and recovery plan (BCP/BRP)?

Business Continuity Plans focus on tactics to maintain normal operations before, during, and immediately after a disaster.

In contrast, Business Recovery Plans are more reactive, describing ways to respond to an incident and restore the business to normal operation.

1)Business Continuity Plan (BCP)

- Conduct a business impact analysis
- Create potential responses
- Assign roles and responsibilities
- Rehearse and revise the plan

2) Disaster Recovery Plan (DRP)

- Conduct a business impact analysis
- Take inventory of your assets
- Assign roles and responsibilities
- Rehearse the plan

VI - The importance of raising awareness about cybersecurity among our office staff

1) Train and raise awareness about security for my users

- Learn to recognize a threat and understand how a cyberattack works;
- Understand the risks to the business;
- Best practices and tools to use (password management, advice on mobility, information transmission, handling sensitive data, responding to a suspected attack, etc.);

2) The best format for effective awareness-raising

- The benefit of an interactive format led by an expert;
- Maintain user knowledge.

CONCLUSION

Cyber resilience is a crucial concept in a world increasingly dependent on technology and where cyberattacks are increasingly frequent and sophisticated.

In short, our organizations must implement effective strategies to anticipate, prevent, detect, respond to, and recover from cybersecurity incidents.

THANK YOU FOR YOUR KIND ATTENTION

Depuis plus de 50 ans

L'Organisation Africaine de la Propriété Intellectuelle
Apporte son soutien et son expertise aux acteurs économiques

Dans ses 17 Etats membres

www.oapi.int

ORGANISATION AFRICAINE DE LA
PROPRIETE INTELLECTUELLE
OAPI