



INFORMATION AND NETWORK SECURITY (INS) MONTHLY REPORT

RISK AND RESPONSE: CRAFTING A RISK MANAGEMENT PLAN

The INS is based on a risk-based approach and outlines the following requirements in crafting a cybersecurity risk management plan:

Technology and cyber risk management

- Establish a TCRMF as an integral part of the organization's Enterprise Risk Management (ERM).
- Develop a technology and cyber risk management policies and practices with specific provisions on assessment, evaluation and integration of emerging technologies.
- Make available an enterprise-wide cyber risk management approach that reflects the collective responsibility of business and technology lines.

Third-party provider management

- Ensure that the board and the management exercise effective oversight and address associated risks when engaging a third-party provider.
- Establish a comprehensive cybersecurity third party risk management (CTPRM) function.
- Maintain and provide a list of third-party providers that have access to personal identifiable information (PII) data and its critical system to the Commission in a template as may be prescribed by the Commission from time to time.

Technology audit

- Establish a specialized internal technology audit function with a dedicated team, authority and resources.
- Ensure technology audits are dynamically aligned with the TCRMF and CRF objectives.
- Ensure the technology audits are designed to proactively identify vulnerabilities and assess the resiliency of the service provider's capability and capacity in managing cyber threats and recovering from cyber-attacks.

Security assessment and audit

Conduct security assessments and audits that include:

- Penetration testing
- Compromise and compliance assessments
- Data centre resilience
- Network risk assessment
- Cryptography audit
- Patch and end-of-line (EOL) assessment

- Assess control audit
- Cloud security assessment
- Third-party risk assessment
- Privacy impact assessment
- Information Security Management System (ISMS) audits

Collaborative intelligence and information exchange

Actively engage in sharing and exchanging information with the Commission and within the industry on a collaborative approach with the following considerations:

- Commission interaction
- Industry collaboration
- Threat intelligence exchange

Internal awareness competency building

Conduct cybersecurity and consumer or customer awareness and training programs at least annually that are tailored to specific roles and risks, reflecting the following:

- Phishing awareness
- Password hygiene
- Social engineering defence
- Data protection
- Incident reporting protocols

BUILDING INFORMATION AND NETWORK SECURITY

We focus on supporting organizations to develop robust information and network security. To protect the integrity of computer networks, organizations can develop the following components:

System development and acquisition	Ensure any changes to the source code of critical systems are subject to adequate reviews.
Security patching and end-of-life (EOL) system management	Ensure all critical vulnerabilities corrective measures and critical systems on EOL are reported to the board and management periodically for immediate rectification.
Identity management and access control	Implement an appropriate access controls policy for the identification, authentication and authorization of users and address both logical and physical technology access controls equal with the level of risk exposure of unauthorized access to systems.
Credential monitoring and protection	Establish monitoring processes to detect the exposure or theft of credentials on the dark web or other sources.
Data security and protection	Ensure data is protected and implement technical means to protect data.
Data storage	Ensure data stored is encrypted and protected by an adequate backup schedule, perform periodic testing and ensure data can be restored from backups.
Data disposal	Implement a clear data sanitization procedure to ensure the data is irretrievably destroyed from systems and devices.
Cybersecurity operations	Establish clear responsibilities for cybersecurity operations and implement appropriate mitigating measures that correspond to the cyber kill chain or threat actor management equivalent.
Security operations center	Establish clear responsibilities for cybersecurity operations and implement appropriate mitigating measures that correspond to the phases of cyber kill chain or threat actor management equivalent.
Incident response and recovery	Implement proactive measures to mitigate the impact of incidents on network and information system security, ensuring service continuity.

INCIDENT OVERVIEW

1. Cybersecurity Incidents

In the past month, our security team documented a total of 0 security incidents.

Type of Incident	Number of Cases	Severity Level
Phishing Attempts	0	None
Malware Detections	0	Low
Unauthorized Access Attempts	0	None

However, we only have malware detection data from last year . A sample is provided below :

[EGP Cloudblock RBL / 1731379202.48899] [probe/scan/virus/trojan] 103.131.135.246

(PTR: -) [<--- COMPROMISED HOST]

From EGP Abuse Dept. on 2024-11-12 10:40

Details

Headers

===== X-ARF Style Summary =====

Date: 2024-11-12T03:40:02+01:00

Source: 103.131.135.246

Type of Abuse: Portscan/Malware/Intrusion Attempts

Logs: 03:39:54.627287 rule 0/0(match): block in on vmx0: 103.131.135.246.59808 > 91.190.98.175.445: Flags [S], seq 597283308, win 0, options [mss 1460], length 0

To whom it may concern,

103.131.135.246 is reported to you for performing unwanted activities toward our server(s).

2. Cybersecurity Complaints

There are no phishing attempts, malware detections, and unauthorized access attempts from the previous month.

III. Conclusion

In conclusion, the absence of reported incidents this month reflects the effectiveness of our current security measures and proactive monitoring efforts. However, maintaining this positive trend requires ongoing vigilance and commitment to our security protocols. Continuous awareness training, timely system updates, and robust access control policies must remain a priority.