THE CYBER – HACKER'S DIARY

Implementing NIST CSF 2.0 at Strazmore University, Kenya

Introduction

Strazmore University, Kenya is mandated to strengthen its Information Security posture by leveraging the NIST Cybersecurity Framework (CSF) 2.0. This policy addresses recent cyber security breaches to the Institution’s Academic Registry; that have resulted to unauthorized adjustments of students’ grades.

1) Identify (ID):

- **Asset Management:** Inventory, classify and prioritize Academic Registry systems according to their criticality and business value
- **Business Environment:** Identify all the interested parties / stakeholders and document the process (SOPs) involved in the Academic Registry systems
- **Governance:** Monitor and review policies, controls and strategies that serve the Academic Registry systems
- **Risk Assessment:** Consider assets / issues: when identifying, evaluating and analyzing risks that have a potential of manipulating the grading systems
- **Risk Management Strategy:** Develop strategies for risk treatment

2) Protect (PR):

- **Identify Management and Access control:** Implement strong identification, authentication and authorization measures that suit the Academic Registry
- **Awareness Training:** Perform role - based cyber security awareness training to ensure that all the interested parties and stakeholders uphold best practices that safeguards the entire institution’s cyber security posture
- **Data Security:** Ensure that academic registry data is classified, prioritized and adheres to confidentiality, integrity and availability facets

Cyber Hacker's Diary

- **Information Protection Processes and Procedures:** Establish a secure cycle through which the Academic Registry's audits (internally or externally) and updates are frequently conducted
- **Maintenance:** Conduct regular reviews and updates of the Academic Registry assets and issues
- **Protective Technology:** Ensure that the Academic Registry has a list of devices, software and applications that are only authorized for use

3) Detect (DE)

- **Anomalies and events:** Monitor academic systems to detect potential adverse events
- **Security continuous monitoring:** Ensure constant auditing of the Academic Registry system within stipulated intervals (monthly or quarterly)
- **Detection process:** Outline the process of detecting and analyzing potential adverse events promptly to the Academic Registry systems

4) Respond (RS)

- **Response planning:** Validate, categorize and prioritize academic system breaches before escalation as required
- **Communications:** Utilize a customized communication map for adverse events affecting the academic systems
- **Analysis:** Analyze grading system breaches to determine the source and scope
- **Mitigation:** Implement controls to contain, eradicate or lessen the impact of academic system threats
- **Improvements:** Update response plan from the lessons learned as per the adverse events that have breached the Academic Registry information security

Cyber Hacker's Diary

5) Recover (RC)

- **Recovery planning:** Ensure that there are tested prompt plans to recover and secure the academic system after the occurrence of breaches
- **Improvements:** Consistently improve the recovery plan as per the past incidents' analyses
- **Communications:** Inform all interested parties / stakeholders during the recovery operations

Conclusion: Implementing the NIST CSF 2.0 at Strazmore University, Kenya, will ensures protection of the Academic Registry's cyber security posture. By strictly adhering to these guidelines, we aim at maintaining a secure system that holds confidentiality and integrity of students' grades. This policy is subject to undergo reviewing and updating in order to reflect changes in the Academic Registry's information Security posture

Signatory:

John Kimani
Chief Information Security Officer (CISO)
Strazmore University, Kenya.
Date: 5th June, 2024

Cyber Hacker's Diary