The Hague Centre for Strategic Studies

Stellenbosch University Iyunivesithi Universiteit

Ministerie van Buitenlandse Zaken

Deloitte.

Cyber Controls

Introduction

In today's digital landscape, organisations face an ever-evolving array of cyber threats, with an increasing frequency of cyber incidents highlighting the urgency for robust cybersecurity measures. Additionally, the concept of digital operational resilience has become crucial, as organisations must not only prevent and respond to cyber incidents but also ensure that they can maintain business continuity and recover quickly from disruptions. One effective way to defend against these threats is through the implementation of the NIST (National Institute of Standards and Technology) Cybersecurity Framework, specifically the updated version 2.0. This framework provides a comprehensive approach to managing cybersecurity risks, enabling organisations to protect their critical assets and promptly detect potential threats.

For this challenge, we will examine the fictional organisation, "Tech Solutions Ltd." This mid-sized technology firm provides software development services to various industries, including finance, healthcare, and retail. Tech Solutions Ltd. has recently recognised the need to enhance their cybersecurity posture, particularly in light of the increasing frequency of cyber incidents and the imperative of achieving digital operational resilience.

Background Information: Tech Solutions Ltd.

Tech Solutions Ltd. operates in a competitive environment where the protection of sensitive client data is paramount, necessitating a strong focus on maintaining confidentiality, integrity, and availability of information. While the company has a preliminary risk management strategy, it lacks a structured approach for regular assessment and updates. A cybersecurity team exists, but roles and responsibilities are not clearly defined or communicated, resulting in overlaps. Although basic incident response procedures are in place, they remain undocumented, complicating adherence during cyber incidents. The organisation lacks a formal oversight mechanism for regular review and improvement of cybersecurity practices. Basic annual cybersecurity awareness training is offered, yet there are no ongoing initiatives to keep employees current on emerging threats. While Tech Solutions Ltd. generates logs from monitored assets, there is insufficient analysis to detect adverse events or anomalies. Data backups of critical assets are performed regularly, but the restoration process during an incident is unclear. All assets are documented in a central repository and rated for criticality; however, without consistent updates or reviews, this information risks becoming outdated. Additionally, the organisation faces uncertainty regarding potential threats and their impacts, complicating incident response efforts.

Objective and key tasks

Utilise your understanding of the NIST 2.0 framework to demonstrate its application through analytical skills, showcasing your insights and conclusion based on the findings regarding Tech Solutions Ltd.'s cybersecurity posture and practices.

In your presentation, please cover the following questions:

1. How relevant is the application of NIST 2.0 to organisations, particularly in the context of Tech Solutions Ltd.?
2. Identify which categories of the NIST 2.0 framework are currently in place at Tech Solutions Ltd. based on the provided information.
3. Discuss which categories are lacking and provide specific suggestions on what the company should do to enhance their cybersecurity posture.
4. In conclusion, evaluate whether adequate prevention and detection measures for cyber threats are in place at Tech Solutions Ltd. and recommend next steps.

April 7th, 12:00PM SAST/CET is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

Contributor for this challenge is Africa Talent by Deloitte. Africa Talent by Deloitte is making an impact that matters by addressing high unemployment rates in South Africa while addressing talent shortages in Europe. Africa Talent professionals provide professional services to Deloitte clients as part of extended teams with European Deloitte firms. Remotely working from the comforts of South Africa. Key expertise areas consist of IT audit, Sustainability Advisory & Assurance, advisory services in Regulatory Risk, Cyber, Business Resilience, Digital Controls, Internal Audit and Internal Support. Guided by the Deloitte ethos of purpose beyond profit, Africa Talent specialists help drive our clients' needs for top class expertise to navigate global changes while supporting their local communities.