Measuring the Efficacy of Cyber Security Controls

Invited Guest Lecture

Kingston University, London, UK

November 18, 2022

Dr. Cyril Onwubiko

Senior Director, Enterprise Security Architecture, Pearson

DrCyrilOnwubiko

cmricorg

c-mric.org

C-MRiC
CENTRE FOR MULTIDISCIPLINARY RESEARCH, INNOVATION AND COLLABORATION ®

Objective

Measure the Efficacy of Cyber Security Controls

1. Do Cyber Security Controls prevent, protect and/or detect cyber incidents?

2. How well do they - Effectiveness and Efficiency?

3. What Indicators/Metrics/KPIs might be best used when measuring whether Cyber Security Controls work or don’t?

Purpose

- Outline Cyber Security Controls
- Understand key Features / Metrics /KPI for measuring the effectiveness of Cyber Security Controls
- Discuss key Metrics of a Security Scorecard
- Understand business benefits

Cyber Security Controls

What are Cyber Security Controls?

People

Process

Technology

Cyber Security Scorecard - People

Role Descriptors – Analyst / Architect / Engineer / Administrator / Operator / Manager

People

- **Ability / Competency** – what are the competency levels or what levels of abilities e.g., Associates/Beginners, Intermediate or Advanced/Expert; Practitioner, Senior and Lead
- **Adaptability** – their potential and ability to adapt to the environment, culture and domain requirements
- **Curiosity** – their willingness to learn, ask questions and investigate, explore
- **Experience** – are the people experience on the role
- **Knowledge** – do they have knowledge of the domain or area
- **Skill -** what is the skills they possess
- **Training** – are the people trained, and what level of training

Certification/Education – Maybe used to assess or measure ability & competency

Cyber Security Scorecard - Process

Process – Documented procedure either manual or automated for operating the system or platform

Process

- **Accreditation / Certification** – is the system or platform certified or accredited to certain standards e.g., ISO27001, ISO31000, Cyber Essentials Plus etc
- **Automation** – are the processes for managing the system or platform automated, for instance, automation increases accuracy and pace, and hence reliability
- **Compliance** – does the system or platform align/hold industry best practice, standards and compliance regimes e.g., PCI DSS, GDPR, NIST CSF
- **Governance** – is there a governance process for managing the system or platform and/or is it a regular cadence
- **Playbooks / Runbooks** – are there playbooks and runbooks available to operation the system or platform, and are these automated or codified
- **Usability / UX –** are the processes usable and frictionless
- **Use Cases** – are there use cases document for the system or platform
- **Workflow** – is there a workflow to operate the system or platform, and how intuitive is the workflow

Cyber Security Scorecard - Technology

Technology

- **Accessibility*** – a measure of technical conformity of accessibility standards, inc. HCI, design aesthetics, UX
- **API Security** – a measure of the security of API (application programming interface), and API gateways
- **Architecture / Design** – is the system or platform architecture or design secure, and has security been baked-in from ideation through to design, development and deployment (DDD)
- **Data Security** – a measure of the security wrappers for securing the data, e.g., encryption, cryptography, certificate (PKI) etc
- **Hardware Security**– a measure of the security of the hardware or container housing the system or the platform, e.g., TPM, Chips, Endpoints, VMs, etc
- **Operational Security** – a measure of the security regime for operating the system or platform, e.g., security monitoring, vulnerability assessment & management, patching etc
- **Physical Security –** a measure of the security of physical infrastructures surrounding the system or platform, e.g., hosting, data centre, barriers, gates, cameras etc
- **Software & Code Security**– a measure of the security of the codes, software used to design and run the system or platform, e.g., SDLC, AppSec, DevSecOps etc

Security Scorecard Tools / Vendors

- **BitSight**
- **Cytegic**
- **FICO**
- **RiskRecon**
- **SecurityScorecard**

Cybersecurity rating services provide continuous, independent quantitative security analysis and scoring for organizational entities. The services gather data from a variety of public and semipublic sources via passive and active means; they then analyze the data using proprietary analysis and rate the entities using their own standard scoring methodologies [1].

[1] Gartner - Refreshed 13 July 2022, Published 30 April 2018 - ID G00259444

How do Security Scorecard or Rating works

- Use IP and Domains, and publicly available information to obtain data (passive and active).
- Use sinkholes and honeypots to glean vulnerability and threat data.
- Use commercial and privately purchased data.
- Leverage external-facing discoverable assets of an organization, the issues associated with those assets, and the severity of the threats that were found to determine a score for each organization.
- Use scoring algorithm based on a statistical framework that takes into account the 1,500,000+ rated companies on the SecurityScorecard platform [2].
- Scoring model is a continuous measure of the typical number of findings for an organization versus their size.

[2] https://support.securityscorecard.com/hc/en-us/articles/360059301992-How-does-SecurityScorecard-collect-data-and-calculate-security-ratings-

Summary / Benefits of measuring how well Security Controls Perform

- Helps the organisation manage internal or supply chain Cyber Risk.
- Helps the organisation gain insight into their cyber posture & security practices and that of their partners/vendors.
- Helps the organisation provide security assurance to existing and potential customers
- Helps the organisation benchmark security progress and compare to industry performance
- Assess controls and how well they perform

Cyber Science 2023

https://c-mric.org

3-4 July 2023
Copenhagen
University of Aalborg
Denmark

Call for Papers is Open

Cyber Science 2023

3-4 July 2023

Copenhagen, University of Aalborg

A. C. Meyers Vænge 15, 2450 København, Denmark

Theme: Multidisciplinary & Multidimensional Cybersecurity

Paper submission is Open

Q&A

Thank –You!

Follow me on Twitter
https://twitter.com/DrCyrilOnwubiko