The CYSFAM Questionnaire:

Assessing CYberSecurity Focus Area Maturity

Cybersecurity Focus Area Maturity Model (CYSFAM)					
Focus Areas	**Capabilities**				
	A	B	C	D	E
Organizational and Technical					
Server Protection					
End-user Controls					
Social Engineering Controls					
Network Security					
Application Security					
Cryptography					
Mobile Security					
Vulnerability Management					
Organizational					
Cybersecurity Incident Management					
Cybersecurity Awareness					
Cybersecurity Governance					

A companion publication of:

CYSFAM: The CYberSecurity Focus Area Maturity model

by Bilge Yigit Ozkan, Sonny van Lingen, and Marco Spruit

Marco Spruit
Sonny van Lingen
Bilge Yigit Ozkan

Technical Report UU-CS-2019-003
May 2019

Department of Information and Computing Sciences
Utrecht University, Utrecht, The Netherlands
www.cs.uu.nl

ISSN: 0924-3275

Department of Information and Computing Sciences
Utrecht University
P.O. Box 80.089
3508 TB Utrecht
The Netherlands

The CYSFAM Questionnaire

The following 144 yes/no questions cover 11 focus areas and constitute the CYberSecurity Focus Area Maturity (CYSFAM) model, version 1.0. Please refer to the main journal publication ”CYSFAM: The CYberSecurity Focus Area Maturity model” for further information.

i. Server Protection

Area	**Capability Maturity**	**Capability**
	A	The organization's baseline security configuration is described.
	A	Patch management is tool-supported (patch-management suites).
	A	A SIEM solution is in place.
	A	A technical compliance checking solution is in place.
	B	The baseline security configuration is based on an open standard.
	B	The deployment of patches is tested and approved at least once before deployment in the production environment.
	B	The SIEM implementation is based on a baseline set of events.
	B	Technical compliance checking is performed manually (supported by appropriate tools).
	C	The baseline security configuration is reviewed at least once a year.
	C	A process is in place that assures the organizations learns about patch releases as soon as possible.
	C	The SIEM implementation includes events that were identified during a risk assessment.
	C	Technical compliance checking is performed with the assistance of automated tools (with a reporting functionality).
	D	The baseline security configuration is updated after every significant configuration change or demonstrated vulnerability.
	D	The prioritization of patches is risk-based; the business-cruciality is taken into account.
	D	The SIEM solution is connected to a managed SOC for a correlation of events, and is connected to the organizations' incident management system.
	D	The technical compliance checking solution is connected to the organizations’ incident management system.

ii. End-user Controls

Area	**Capability Maturity**	**Capability**
	A	The organization has a policy on user authentication.

	A	The organization employs an enterprise-wide, standardized anti-malware protection solution.
	A	The organization employs an automated patch management solution.
	A	The organization makes a distinction in normal end-users and privileged end-users (local administrators).
	B	The organization employs one-factor authentication for all relevant assets.
	B	The organization employs multiple anti-malware protection solutions in an enterprise-wide manner.
	B	The organization employs a standardized, enterprise-wide automated patch management solution.
	B	Using local-administrator rights is an auditable event.
	C	The organization has the (in-house) capabilities to provide two- or three-factor authentication for relevant assets.
	C	The organization employs application control whitelisting.
	C	The organization has defined a Patch and Vulnerability Group (PVG) that is formally responsible for the organizations' patch management.
	C	The organizations' decision to provide local-administrator rights is taken risk-based, and provided by a formal end-user management committee.
	D	The organization employs a number of factors in the authentication process on a risk-based manner, based on their authentication policy.
	D	The organization has an anti-malware policy which describes the handling and escalation channels of a malware infection AND the organization tests the effectiveness of the anti-malware protection solution on a periodic basis.
	D	The organization evaluates the effectiveness of the patch management solution on a periodic basis, in a consistent manner AND a risk assessment of every patch is a common practice.

iii. Social Engineering

	A	The organization has implemented automated tools to circumvent poor, human-originated decisions.
	A	The organization has implemented social engineering defenses within the information security policies.
	B	The organization embraces management practices to foster a productive work environment (e.g. decreasing stress and increasing self-care).
	B	The organization undertakes risk management assessments in the context of Social Engineering.
	C	The organization has a training/awareness program in which employees are trained in both cognitive biases and historical accidents.

	C	The organization has developed a security management framework.
	D	The defense against Social Engineering threats is an integral part of the organizations' Security Management process.

iv. Network Security

	A	The organization uses relevant security documentation in configuring network components.
	A	By automated means, the organization ensures that only ports, protocols and services with validated business needs are running on each system.
	A	The organization designs its network using a minimum of a three-tier architecture (DMZ, middleware, private network).
	B	The organization uses a configuration management system to record and document the configuration files of network devices.
	B	The organization operates all critical infrastructural services (DNS, file, mail, web, database) on a separate physical or virtual machine.
	B	The organization has an (operational) method to quickly alter ACLs, rules, signatures, blocks and so forth in case of an attack.
	C	The organization manages the network infrastructure by using a separate VLAN for which the routing access is controlled.
	C	The organization has placed application firewalls in front of any critical servers.
	C	The organization segments the enterprise network into multiple, separate trust zones.
	D	The organization manages the network infrastructure on an entirely different physical stream of connectivity.
	D	The organizations' firewalls that protect critical components, have a functionality that automatically blocks unauthorized traffic, which in turn alerts about it.
	D	The organization assures that entering and leaving a trust zone is an audited event.

v. Web Application Security

	A	The organization has implemented Version Control in its Application Change Management process.
	A	The organization employs Secure Development Lifecycle activities on a manual, ad-hoc basis.
	B	The organizations employs Source Code or Web Scanning tools.
	B	The organization trains its staff specifically on Application Security (awareness-training, followed by technical training).
	C	The organization employs both Source Code and Web scanning Tools, and its results are adopted in a Defect Management System.

	C	The organization has assigned internal “Red Teams”.
	D	The organization automates all testing (not only security-testing, but also other test-disciplines, such as regression testing)
	D	The organization integrates its Application Security vulnerability-assessment process with relevant governing parties (such as IRM and Compliance).

vi. Cyber Security Incident Management

	A	The CIRT is mandated by upper management.
	A	There is a skillset description available describing the required skills to operate in the CIRT.
	A	The CIRT is able to get access to the complete IT resources list, but there is a process in place which regulates this access.
	A	The organization has a policy describing the security incident prevention, detection and resolution processes.
	B	The authority and responsibility of the CIRT is described in an official service description.
	B	The organization provides internal CIRT training (of any kind) AND the CIRT staffing pays attention to personal resilience (staffing during holidays, week-ends, et cetera).
	B	The CIRT receives their vulnerability/trend/scanning information from reliable sources.
	B	The CIRT has a way of handling "common mailbox names" (security@; cert@; abuse@) AND has a reporting process in place.
	C	The levels of service the CIRT offers is described in a service level description.
	C	The organization offers their CIRT's members external technical and communication training.
	C	On a regular basis, the CIRT receives the outcome of prevention, detection and resolution toolsets.
	C	The organization documented the CIRT emergency reachability process, which is also communicated and tested frequently.
	D	The organization has a security incident whistleblowers program in place which is mandated by upper management.
	D	External networking with other CIRTs or related knowledge sharing platforms is a CIRT habit.
	D	The CIRT has a robust and resilient (fail-safe) setup of all communication methods (Internet/email/phone) AND the CIRT incident management system is isolated from other incident management systems.
	D	The CIRT has a process in place which describes the different escalation scenario's (governance-level, press-function, legal-function, et cetera).

vii. Cyber Security Awareness

	A	The compliance or audit standards that the organization needs to adhere to are identified.
	A	The security awareness requirements for these standards are known – possibly coordinated by a compliance or audit officer.
	A	The organization possesses the security awareness training material to meet the compliance and audit demands.
	A	There is a process that tracks the security awareness trainings' participation.
	B	The security awareness program is actively promoted by stakeholders in the organization.
	B	The organization has conducted a security awareness level baseline measurement.
	B	The security awareness program is managed by a project charter – which in turn is governed by a steering committee.
	B	The security awareness training is tailored towards the needs of specific roles.
	C	The security awareness program is reviewed for effectiveness on a periodic basis.
	C	The organization activally surveys staff that has participated in the program for feedback.
	C	The security awareness program is updated when changes in the technology, theat-landscape, business processes or compliance standards occur.
	C	(Optional – provided that the data is available) The organization compares its current security awareness measurements to earlier baselines.
	D	The organization has identified metrics that relate to the business goals of the security awareness training.
	D	The organization documents how (and when) these metrics are measured.
	D	The organization has identified to whom the results are communicated, and in which manner.
	E	The organization executes its security awareness training metrics measurement.

viii. Cryptography

	A	Key generation is consistent within applications AND recipients are authenticated before the key is handed out.
	A	The access to key storage is defined in the application's individual processes AND key backup is consistent within applications.
	A	Updating and renewing keys is dealt with and is consistent throughout applications AND recovery processes are implemented per application.
	A	Key revocation is consistent within applications AND key disposal processes are implemented.
	B	Key generation follows a standard which has attention for symmetric and

		asymmetric standards AND the symmetric and asymmetric key distribution is always mutually authenticated and secured.
	B	Key storage containers are assuring authentication of the recipient AND key back-up containers are assuring authentication of the recipient.
	B	Key updating is dealt with by automated capabilities AND recovery processes per application are implemented.
	B	Key revocation is driven by a number of processes, namely key-notification, key-generation and key-distribution AND encrypted material is removed during the key disposal process.
	C	Key generation standards are managed at the organizational level AND all application in the enterprise comply to these standards.
	C	Key storage standards are managed at the organizational level AND key back-up standards are managed at the organizational level.
	C	Key update standards are managed at the organizational level AND key recovery processes are consistent with standards.
	C	Key revocation standards are managed at the organizational level AND key disposal standards are managed at the organizational level.
	D	Key generation endures continuous testing to ensure compliance AND there is a process in place to evaluate (new) standards for key generation.
	D	Key storage endures continuous testing to ensure compliance AND there is a process in place to evaluate (new) standards for key back-up.
	D	Key updating and the technology it supports is continuously evaluated AND there is a process in place for evaluating additions to the key recovery process.
	D	Key revocation and the technology it supports is continuously evaluated AND there is a process in place to evaluate (new) standards for key disposal.

ix. Governance

	A	The organization has defined an organization-wide cyber security policy.
	A	The organizations' second line of defence addresses Root Cause Analyses for cyber security risk and mitigating controls.
	A	The organizations' internal audit capability is organized in a way that it can audit a broad range of cyber security domains.
	A	The organization has adequate funding to support the implementation of cyber security.
	B	The organization's cyber security policy contains the roles and responsibilities of the three lines of defence.
	B	The organizations' second line of defence asseses cyber security risk within the organizations' change management process.

	B	The organizations' internal audit capability determines the frequency of audits risk-based AND the organizations' internal audit capability carries out both a ToD (Test of Design) and a ToE (Test of Effectiveness).
	B	The organization has established a Senior Management committee that takes an active interest in cyber security matters.
	C	The cyber security policy is mandated in all of the organizations' groups and entities – including subsidiaries.
	C	The organizations' second line of defence challenges the cyber security risk assessments of the first line of defence on a periodic basis.
	C	The organization has defined processes for escalating serious breaches/cyber security incidents.
	C	The organization has conducted an external review of its cyber security policies.
	D	The organization has alsigned its cyber security strategy with its business strategy AND key cyber security initiatives and timelines are defined.
	D	The organizations' second line of defence actively monitors the identification and remediation of findings dealt with by the first line of defence AND the organizations' second line of defence incorporates cyber security risk in the operational risk appetite.

x. Mobile Security

	A	The organization has a repeatable process in place to identify smartphone system and data owners.
	A	The organization has a repeatable process in place regarding smartphone information (at least elaborating upon management of authentication, removable media, ownership, restoration and continuity and backup policies/schemes).
	A	The organization has a repeatable process in place regarding infrastructural affairs (at least elaborating on configuration policies, communication policies, physical threats, infrastructural system ownership and supplier/service delivery management).
	A	The organization has a repeatable process in place regarding people-matters (at least elaborating on user awareness programmes, control frameworks, rights and privileges and governance reporting).
	B	The organization has a defined process in place to identify smartphone system and data owners.
	B	The organization has a defined process in place regarding smartphone information (at least elaborating upon management of authentication, removable media, ownership, restoration and continuity and backup policies/schemes).
	B	The organization has a defined process in place regarding infrastructural affairs (at least elaborating on configuration policies, communication policies, physical threats,

		infrastructural system ownership and supplier/service delivery management).
	B	The organization has a defined process in place regarding people-matters (at least elaborating on user awareness programmes, control frameworks, rights and privileges and governance reporting).
	C	The organization has a managed process in place to identify smartphone system and data owners, in which metrics are defined.
	C	The organization has a managed process in place regarding smartphone information (at least elaborating upon management of authentication, removable media, ownership, restoration and continuity and backup policies/schemes), in which metrics are defined.
	C	The organization has a managed process in place regarding infrastructural affairs (at least elaborating on configuration policies, communication policies, physical threats, infrastructural system ownership and supplier/service delivery management), in which metrics are defined.
	C	The organization has a managed process in place regarding people-matters (at least elaborating on user awareness programmes, control frameworks, rights and privileges and governance reporting), in which metrics are defined.
	D	The organization has a fully optimized process in place to identify smartphone system and data owners, in which metrics are defined and respected.
	D	The organization has a fully optimized process in place regarding smartphone information (at least elaborating upon management of authentication, removable media, ownership, restoration and continuity and backup policies/schemes), in which metrics are defined and respected.
	D	The organization has a fully optimzed process in place regarding infrastructural affairs (at least elaborating on configuration policies, communication policies, physical threats, infrastructural system ownership and supplier/service delivery management), in which metrics are defined and respected.
	D	The organization has a fully optimized process in place regarding people-matters (at least elaborating on user awareness programmes, control frameworks, rights and privileges and governance reporting), in which metrics are defined and respected.

xi. Vulnerability Management

	A	The organization runs scheduled vulnerability scans on all production machines on their network.
	A	The organization has subscribed itself to vulnerability intelligence services, and this information is incorporated in the vulnerability management process.
	B	The organization runs scheduled vulnerability scans on all DTAP machines on their network.

	B	The organization measures the delay of the patching of vulnerabilities.
	C	The organization feeds a Vulnerability Management System (VMS) with the outcomes of the periodic machine scans.
	C	The organization has a process in which vulnerabilities are risk-rated based on the assets' characteristics.
	D	The VMS compares systems to configuration baselines automatically.
	D	There is a Role Based Access Control (RBAC) solution to regulate who has access to the vulnerability management platform