Frameworx Best Practice

Cyber Security Readiness Dashboard

TR213
October 2013

Latest Update: Frameworx Release 13.5	**Member Evaluation**
Version 0.3.1	**IPR Mode: RAND**

Notice

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Figures

List of Tables

Insert if applicable

Executive Summary

In keeping with our mission to help members protect their assets with Cyber Security best practices and guidance, the TM Forum held a workshop during TM Forum's Action Week Baltimore event in June 2013 to discuss how to provide an executive view of cyber readiness in near-real time.

While our requirements are simple at the high level - produce an at-a-glance dashboard that can effectively communicate to cyber situational awareness - it gets complicated when you consider combining threat information, compliance and network readiness into a single view. The team realized early on that producing a dashboard which contains not only the right level of content for an executive, but could also drill down to bring actionable information to decision makers is a critical hurdle.

The Cyber Security Readiness Dashboard uses newly defined metrics to communicate Cyber Security readiness for C-Level management. Using the metrics, CXOs can understand at-a-glance the status of their organization with respect to protective measures, emerging and active threats, and recovery.

The ability for executives to have this information rapidly is critical for understanding the need for short term actions, along with potential long term effects including lost business due to regulatory violations for example. The dashboard reduces risk to the organization by providing executives visibility into issues that could have financial, legal/compliance and human safety impacts.

The dashboard is industry agnostic, and leverages the TM Forum's Security Management Model to delineate functions for the purpose of categorizing key metrics.

The team encourages adoption and feedback from the Security Community.

1. Introduction

1.1. Document Structure

1.1.1. Introduction and Approach

In an effort to provide some categorization to the dashboard metrics, the team used the TM Forum's Security Management Model to categorize metrics. A Technical Report, TR172, details the Security Management Model.[1]

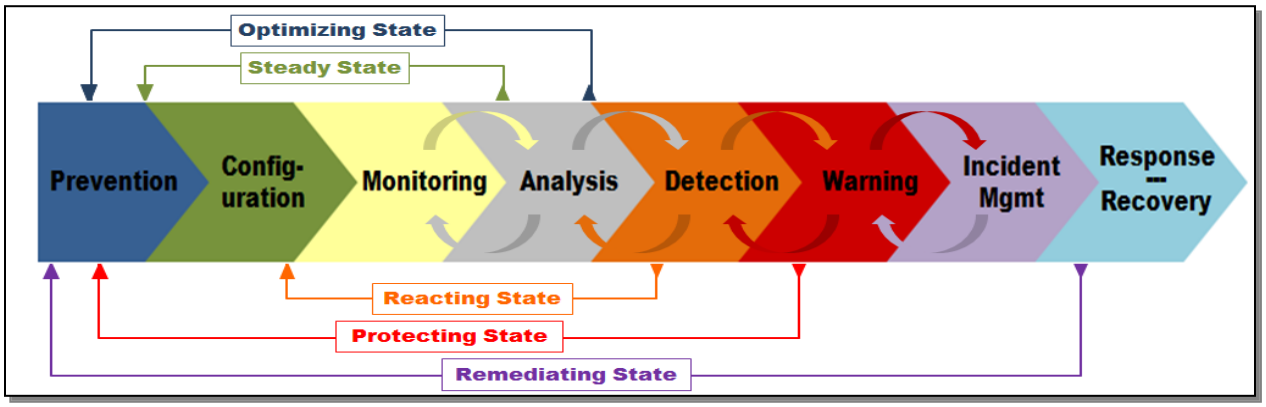

Figure 1: TM Forum's Security Management Model

The team used this model, and developed a series of questions that executives need answered in order to know the current state of cyber readiness for their respective organization. With the questions in hand, the team worked together to identify metrics that would answer those questions along with sources.

The remainder of this document will take the reader through each of the Security Management Model functions (above) and associate the questions, metrics, and sources.

1.1.2. Top-View (Summary)

The team is of the opinion that a "top-view" dashboard (summary compiled from each of the sections below) would consist of the following:

1. Can we certify our security? (Prevention)
2. Are our configs secured? (Configuration)
3. What is at risk? (Monitoring)
4. What is the risk? (Analysis)
5. What revenue is threatened? (Detection)
6. What threats are current? (Warning)
7. What threats have happened? (Incident Management)
8. What are we doing to prevent first or re- occurrence? (Response/Recovery)

[1] http://www.tmforum.org/DownloadRelease13/14777/home.html

1.1.3. Issues and Appendices

Appendix A **Terminology, Acronyms and Abbreviations** (not defined in section 2)

Appendix B **References**

Administrative Appendix provides document revision history, acknowledgements for work completed and information about the TM Forum.

1.2. Terminology used within this document

All terms are defined where they are used.

2. Cyber Security Readiness Defined

Below are the security functions with a short definition from TR172, corresponding executive questions, metrics, and source/sample data. Also included is any helpful information, "general information", the team identified during the collaboration process.

2.1. Prevention

Prevention is the specification of baseline security controls and operational policies to be deployed into the network. In this process, the organization makes decisions (funding, staffing, R&D, testing, monitoring, etc. about what assets (tangible and intangible) to protect, using what particular means, and at what target assurance levels.

2.1.1. What questions do CXO's need answered?

Has our organization achieved the things necessary to auditably certify? Can our organization state and be certified to our chosen compliance standards under SSAE16 SOC II?

2.1.2. Metrics

1. Vulnerability assessments
2. Penetration tests
3. Auditor's certification or self-attestation to the chosen standards.
4. Social engineering tests
5. Results shared (with customers, partners or others on the period contracted. Such reports need not be made public.)

Each of the preceding must be assigned a period (not to exceed annual) and be certified either though independent certified/credible audit (preferred) or by attested self-evaluation (acceptable if attested by a fiduciary of the organization). Note: falsifying either attestation breaches SSAE16, which prevents the conduct of business.

Vulnerability & standard scans (complete)
Auditing (no reportable exceptions or qualifications)

2.1.3. Example Data / Potential Source

The list of prevailing, contractible standards as of the date of this release includes: ISO 270001, PCI-DSS, SOX, NIST 800-53, SSDLC (CERT), OWASP, COBIT, EUDPD/Safe Harbor, and ISF (Information Security Forum) self-assessment. For some specific industry segments in the TM Forum and NERC also applies.

2.1.4. General Information

The list of security standards applicable to each organization must be decided by that organization.

2.2. Configuration

Configuration is the application of baseline, optimized, and remediated secure configurations and policies on managed resources (directly or via proxies for those resources). Within the Configuration process the organization applies the baseline of secure configurations and operational policies, which were developed

during the Prevention process, to its managed resources and services. The application of baseline, optimized, and remediated secure configurations and policies on managed resources (directly or via proxies for those resources).

2.2.1. What questions do CXO's need answered?

Are our configurations verifiably secure?

Has a configuration put the organization at risk?

2.2.2. Metrics

1. Tested for security before being applied in Production (%)
2. Source verified before update (%)
3. Emergency changes tested and certified before being considered final (%)

Finding out that a configuration has put your organization at risk (this would typically be done as a 'post mortem' exercise.

2.2.3. Example Data / Potential Source

The list of independently verifiable configuration sources includes: OEMs/manufacturers, credible industry and user groups (by platform/type), certified experts (insured for E&O or some other mechanism whereby the contracting organization may recover losses in the event of an error), regulatory or legal compliance data, and your own testing data.

2.2.4. General Information

Note: executives will assume configurations to be properly applied in a timely fashion - metrics related to the operationalization of configuration are not part of an executive dashboard.

2.3. Monitoring

Monitoring is policy-based multimodal (active/passive, dynamic/scheduled) collection, filtering, aggregation, distribution, and retention of relevant data. Within the Monitoring process the organization collects and retains relevant data emanating from or associated with a given set of managed resources and services.

2.3.1. What questions do CXO's need answered?

What systems are at risk?

Business Critical systems should be monitored and or configured properly.
What is not being monitored (That is deemed mission Critical) As well could use FIM to ensure Integrity of file system.

2.3.2. Metrics

1. What is the volume of anomalies?
2. What is our technical monitoring coverage? (%)
3. What is our procedural monitoring coverage? (%)
4. What is our organizational monitoring coverage? (%)
5. For each of the preceding, what is our confidence in the data? (%).

2.3.3. Example Data / Potential Source

1. Output of technical systems including IDS/IPS, malware/virus scans
2. Last update of security definitions files, pattern files, white/black lists by platform/type
3. Last training/sample date/time
4. Results of any security assessments that were completed.

2.3.4. General Information

Note: executives will assume monitoring systems are verified for internal integrity, cross-referential and not themselves susceptible to attack - metrics related to integrity are not part of an executive dashboard.

2.4. Analysis

Analysis is policy-based assessment of collected/correlated data for events or trends of interest. Within the Analysis process the organization assesses the data it collects via Monitoring. Analysis may apply correlation and other functions over the collected data to form a more complete and accurate picture of events and conditions – for example, to detect patterns and trends that would not otherwise be visible.

2.4.1. What questions do CXO's need answered?

- What is the risk?
- What is happening to other organizations relevant to our business?
- What are our customers' areas of concern?
- What is the likelihood of threat/incident?
- Is there an impact to Customer service and/or a revenue impact?

2.4.2. Metrics

1. What is the potential exposure, measures either in monetary terms or some other quantifiable operational impact equivalent

2.4.3. Example Data / Potential Source

ISO/IEC 27003, Failure Modes and Effects Analysis, and TM Forum Frameworx provide guidance.

2.4.4. General Information

Note: executives are interested only in the objective conclusions of synthesis and trend data, not in the mechanics or work products of analysis

2.5. Detection

Detection is policy-based recognition of a possible incident. Within the Detection process the organization gains an awareness that Analysis has detected an anomaly – relative to expected results – and that a possible incident may be occurring or may have occurred. At this stage, automated policy-based remediation may still be possible – i.e., without invoking Incident Management.

2.5.1. What questions do CXO's need answered?

Is revenue being threatened? Would we know if it were (can we detect)?
There could be manual detection via review of logs, scans, contracts and automated functions.

2.5.2. Metrics

What is our delay between threat/exposure and detection? Confidence level that detection ability/coverage is complete.

2.5.3. Example Data / Potential Source

Credible industry sources like SNORT (IDS) and SQUID (proxy) provide guidance.

2.5.4. General Information

Critical for execs, long term impact includes lost biz/bids due to regulatory violations.
Risk items include: $, legal/compliance and/or saving lives

2.6. Warning

Warning is policy-based distributed notification of a probable incident. Within the Warning process the organization generates and distributes notifications that a probable incident is occurring or has occurred.

2.6.1. What questions do CXO's need answered?

- What security threats are current?
- Can they be prevented?
- What is the estimated time to complete prevention?
- If they cannot be prevented, how long after occurrence can they be remedied?

Warnings can come from many sources such as MITRE, NIST, Government agencies, commercially accepted groups, threat sharing, white hat hackers. The ability to remediate risks before they become an issue is easier the earlier you have the information.

2.6.2. Metrics

1. Volume of warnings.
2. Estimated time before each becomes an incident.
3. Confidence for each of the preceding.
4. What percentage of warnings are prevented from becoming incidents?

2.6.3. Example Data / Potential Source

Credible industry sources such as MITRE, SANS, Cloud Security Alliance and DBIR provide guidance.

2.6.4. General Information

Cyber Threat Intelligence Sharing ties into this potentially.

2.7. Incident

Incident is ITSM-based incident management practices. Within the Incident Management process the organization leverages ITSM-based incident management practices in response to a Warning. Incident Management will identify necessary Response & Recovery actions that may be required to repair damages incurred and/or to prevent further occurrences.

2.7.1. What questions do CXO's need answered?

What legal/contract (SLA) implications have occurred?
Have notifications been issued (as contracted or as needed to protect our brand)?

2.7.2. Metrics

1. $ Cost
2. Average age (incident)
3. Incidents undetected %
4. Severity
5. Volume of incidents
6. Notifications issued?

2.7.3. Example Data / Potential Source

ISO 20000/ITIL provides guidance.

2.7.4. General Information

In the United States, new SEC filings are required for certain types of Cyber "events".

2.8. Response & Recovery

Response and recovery is the application of solution measures, normally fed back into the Prevention posture. Within the Response & Recovery process the organization applies solution measures, either individually or collectively as appropriate, as indicated by Incident Management. Additionally, this process guides the flow of lessons learned, whether technical or non-technical in nature, back into Prevention.

2.8.1. What questions do CXO's need answered?

Do we prevent reoccurrence? If not, what is the incidence rate and action plan?

2.8.2. Metrics

1. # of TT's actioned & remediated
2. $ Actual exposure & $ Recovery (s/w, h/w, people, etc.)

2.8.3. Example Data / Potential Source

Certifiable root cause and lessons learned methods with credible academic sources including reason and Kepner-Tregoe provide guidance and close the loop with Prevention.

2.8.4. General Information

Where to invest?
The more you "share" (situational awareness) - higher confidence level.

3. Appendix A: Terms and Abbreviations Used within this Document

3.1. Terminology

Term	Definitions	TM Forum or Outside Source
# of TT's	Trouble Tickets	
SLA	Service Level Agreement	
SEC	Securities and Exchange Commission	
ITSM	IT Service Management	
OEMs	Original Equipment Manufacturer (s)	
R&D	Research & Development	
IDS	Intrusion Detection System	
IPS	Intrusion Protection System	
FIM	File Integrity Monitoring	

3.2. Abbreviations and Acronyms

Abbreviation/ Acronym	Abbreviation/ Acronym Spelled Out	Definition	TMF or External Source
NERC	North American Electric Reliability Corporation	Not-for-profit whose mission is to ensure the reliability of the Bulk-Power System in North America.	http://www.nerc.com/Pages/default.aspx

4. References

4.1. References

Reference	Description	Source	Brief Use Summary
Project Charter	Cyber Security Readiness Dashboard Project Charter		Targeted work is the design of the Cyber Security Readiness Dashboard. There is a strong need to produce a framework for effectively communicating cyber readiness in near-real time. The objectives behind this project include the identification of dashboard metrics, their definition, developing sample data and a prototype (potential) that would communicate Cyber Security readiness for C-Level management. It's expected that the project will leverage the TM Forum's Cyber Ops Metrics Guidebooks (best practices consumable and measureable) and Security Management Process. A workshop on this topic was held at Action Week Baltimore 2013 and a subsequent member contribution of a draft dashboard has helped to accelerate this project. It is expected that this project will use a rapid, iterative approach, and complete its work well in advance of the Frameworx 13.5 release.
A Technical Report, TR172	TR172, TM Forum Security Management Model, Version 0.2	http://www.tmforum.org/DownloadRelease13/14777/home.html	Details the Security Management Model.
ISO 270001	Published standard on security code of practice.	http://www.27000.org/iso-27001.htm	Referenced in "Prevention".
PCI-DSS	PCI Security Standards Council is a robust set of standards for the payment card data security	https://www.pcisecuritystandards.org/security_standards/index.php	Referenced in "Prevention".
SOX	Sarbanes-Oxley Act – Corporate and Auditing Accountability & Responsibility Act	http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act	Referenced in "Prevention".
NIST 800-53	National Institute of Standards and Technology (NIST) Security Content Automation	www.nist.gov	Referenced in "Prevention".

	Protocol (SCAP) suite of interoperable specifications		
SSDLC (CERT)	Secure Software Development Life Cycle Processes	https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes	Referenced in “Prevention”.
OWASP	The Open Web Application Security Project is a not-for-profit org focused on improving software security.	https://www.owasp.org/index.php/Main_Page	Referenced in “Prevention”.
COBIT	IT Governance Framework and supporting toolset to bridge gaps between control requirements, technical issues and business risks.	http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx	Referenced in “Prevention”.
EUDPD/Safe Harbor	European Personal Data Protection (EUDPD) Law regulates “personal data”.	http://www.s3security.com/safeHarborAssessment.html	Referenced in “Prevention”.
SSAE16 SOC II	Statement on Standards for Attestation Engagements Reporting on Controls at a Service Organization	http://ssae16.com/SSAE16_overview.html	Referenced in “Prevention”.
ISO/IEC 27003	Information technology, Security techniques, Information Security Management System Implementation Guidance	http://www.iso27001security.com/html/27003.html	Failure Modes and Effects Analysis
ISO 20000 /ITIL	Certification (formerly managed by itSMF).	http://www.isoiec20000certification.com/	Referenced in “Incident”.
MITRE	MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through **registries** of baseline security data, providing standardized languages as means for accurately communicating the information, defining proper usage, and helping establish community approaches for	http://measurablesecurity.mitre.org/	Referenced in “Warning”.

	standardized processes.		
NIST	*NIST* is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.	www.nist.gov	Multiple references.
SNORT (IDS)	A lightweight intrusion detection system developed by Sourcefire.	http://www.snort.org/	Referenced in “Detection”.
SQUID (proxy)	A caching proxy for the Web.	http://www.squid-cache.org/	Referenced in “Detection”.
SANS	A trusted source for computer security training, certification and research.	http://www.sans.org/	Referenced in “Warning”.
Cloud Security Alliance	Not-for-profit organization that develops the use of best practices for providing security assurance within Cloud Computing.	https://cloudsecurityalliance.org/	Referenced in “Warning”.
DBIR	Data Breach Investigations Report produced by Verizon.	http://www.verizonenterprise.com/DBIR/2013/	Referenced in “Warning”.

4.2. IPR Releases and Patent Disclosures

This document may involve a claim of patent rights by one or more of the contributors to this document, pursuant to the Agreement on Intellectual Rights between the TM Forum and its members. Interested parties should contact the TM Forum office to obtain notice of current patent rights claims subject to this document.

5. Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document. In general, sections may be included or omitted as desired, however a Document History must always be included.

5.1. Document History

5.1.1. Version History

<This section records the changes between this and the previous document version as it is edited by the team concerned. Note: this is an incremental number which does not have to match the release number and used for change control purposes only>

Version Number	Date Modified	Modified by:	Description of changes
0.1	19/Sep/2013	Jenny Rottinger	Converted Excel spreadsheet to TR format.
0.2	7/Oct/2013	Christy Coffey	Added Executive Summary & general clean-up
0.3	10/Oct/2013	Christy Coffey	Updates for top 8 summary questions, comments from champion & team lead, & updated references.
0.3.1	15/Oct/2013	Alicja Kawecki	Updated cover, header & footer prior to posting

5.1.2. Release History

Release Number	Date Modified	Modified by:	Description of changes
<<Release Number >>	DD/MMM/YY	<<name>>	Description e.g. first issue of document

5.2. Company Contact Details

Company	Team Member Representative
TM Forum	Christy Coffey
Bell Canada	Blake Lindsay

Ministry of Defence, DSTL	Martin Huddleston
TOA Technologies	Mike Carpenter

5.3. Acknowledgments

This document was prepared by the members of the TM Forum Cyber Security Readiness Dashboard team:

- Christy Coffey, TM Forum, **Editor**
- Blake Lindsay, Bell Canada, Sponsor
- Mike Carpenter, TOA Technologies, team leader

Additional input was provided by the following people:

- Martin Huddleston, Defence Science and Technology Laboratory
- Jason Boswell, Symantec Corporation
- Harry Perper, MITRE
- Clive Reeves, Telstra Corporation
- Brian Rexroad, AT&T Inc.
- Joseph Alleman, Ideas That Work, LLC
- Ward Cobleigh, Edge Technologies
- Donald Hart, Edge Technologies
- Ron Roman, Applied Communication Sciences
- Pamela Abbott, Brunel University