****

**TM Forum**

**CyberOps Metrics**

**GB965 Quick Start Pack: Patch Management**

**April 2013**

**TM Forum Approved Version 0.11**

# Notice

Copyright © TeleManagement Forum 2013. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to TM FORUM, except as needed for the purpose of developing any document or deliverable produced by a TM FORUM Collaboration Project Team (in which case the rules applicable to copyrights, as set forth in the [TM FORUM IPR Policy](http://www.tmforum.org/IPRPolicy/11525/home.html), must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by TM FORUM or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and TM FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

TM FORUM invites any TM FORUM Member or any other party that believes it has patent claims that would necessarily be infringed by implementations of this TM Forum Standards Final Deliverable, to notify the TM FORUM Team Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the TM FORUM Collaboration Project Team that produced this deliverable.

The TM FORUM invites any party to contact the TM FORUM Team Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this TM FORUM Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the TM FORUM Collaboration Project Team that produced this TM FORUM Standards Final Deliverable. TM FORUM may include such claims on its website, but disclaims any obligation to do so.

TM FORUM takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this TM FORUM Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on TM FORUM's procedures with respect to rights in any document or deliverable produced by a TM FORUM Collaboration Project Team can be found on the TM FORUM website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this TM FORUM Standards Final Deliverable, can be obtained from the TM FORUM Team Administrator. TM FORUM makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

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](http://www.tmforum.org/)

Contents

[Notice 2](#_Toc352683916)

[Table of Figures 5](#_Toc352683917)

[Glossary of Terms 6](#_Toc352683918)

[Introduction 7](#_Toc352683919)

[Why Patch Management as a Cyber Ops Best Practice? 7](#_Toc352683920)

[Project Document Output 8](#_Toc352683921)

[Patch Management Security Metrics Overview 8](#_Toc352683922)

[Patch Management Process 9](#_Toc352683923)

[Identification Phase 9](#_Toc352683924)

[Evaluation Phase 11](#_Toc352683925)

[Testing Phase 12](#_Toc352683926)

[Implementation Phase 13](#_Toc352683927)

[Validation Phase 14](#_Toc352683928)

[KPI Meta-Data Collection Guide Detail 16](#_Toc352683929)

[In Practice 20](#_Toc352683930)

[Summary Suggested Patch Management Security KPIs 21](#_Toc352683931)

[Possible examples of commercially reasonable Patching SLA statements 21](#_Toc352683932)

[Variables 21](#_Toc352683933)

[Supply Base 22](#_Toc352683934)

[Recommended Use of the Quick Start Guide 23](#_Toc352683935)

[Appendix A: Metrics Derived from Bibliography Search 24](#_Toc352683936)

[Appendix B: Cyber Operations Metrics for Security Management – Prioritization in the Supply Base/Network and CNI 25](#_Toc352683937)

[Administrative Appendix 27](#_Toc352683938)

[About this document 27](#_Toc352683939)

[References 27](#_Toc352683940)

[Document History 28](#_Toc352683941)

[Version History 28](#_Toc352683942)

[Release History 28](#_Toc352683943)

[Company Contact Details 28](#_Toc352683944)

[Acknowledgments 29](#_Toc352683945)

# Table of Figures

[Figure 1 – Patch Identification for Security: a subset of all RFCs and of the Configuration Process 10](#_Toc352684542)

[Figure 2 – Evaluation Phase of Security Patch Management, Emergency Change 12](#_Toc352684543)

[Figure 3 – “Time to Complete Patch” Implementation Phase Scope 14](#_Toc352684544)

[Figure 4 – “Time to Complete Patch” Process Scope 17](#_Toc352684545)

# Glossary of Terms

|  |  |
| --- | --- |
| CAB | Change Advisory Board |
| CNI | Critical National Infrastructure |
| CVSS | Common Vulnerability Scoring System (scores) |
| CWE | Collaborative Work Environment |
| eTOM | Enhanced Telecom Operations Map |
| KPI | Key Performance Indicator |
| MTBF | Mean time between failures |
| NLT | Not Less Than |
| OS | Operating System |
| Parallel Mitigation | Temporary mitigations taken during to reduce risk until patching is complete. |
| RFC | Request for Change |
| SLA | Service Level Agreement |

# Introduction

The basic proposition put forward is that 80% of the root causes of security incidents from cyber-attack and risks can be mitigated with *doing the basics well*. By Pareto’s Rule, 20% of possible mitigations should give us an 80% impact. Since this proposition has emerged from the natural work of multiple worldwide security response teams, and, since the organizations that certify international security best practices have published work in material agreement with this proposition, the TM Forum Cyber Ops Metrics project team chose to address the question, “What *specific* 20% of all activities we could undertake to improve security can provide the most overall benefit, ideally 80% or more?”

The project champions recognized managing the response to security vulnerabilities and vendor software releases as a key risk mitigation strategy. The project team’s independent evaluation of multiple outside best practices and certification courses clearly justifies patch management as a best practice strategy within the 20% target. Requirements put forth by the project champions included defining KPIs that: could be instrumented systematically, encourage good behavior (process improvement), and are implementable across a supply industrial base[[1]](#footnote-2) with nested and networked connectivity, not only a traditionally simple cascaded supply chain[[2]](#footnote-3).

This Quick Start Pack intends to offer its audience best practice guidance with a set of KPIs that can be applied as is, or at least provide a starting point for discussion. The KPI’s prescribed within this document will not solve all patch management problems. They are intended to assist in identifying where you can probe deeper into your process and make improvements for security, specifically. Some metrics are also more broadly useful.

## Why Patch Management as a Cyber Ops Best Practice?

Patch management[[3]](#footnote-4), a subset of configuration management, is vital to preventive security. Patch management was selected by the Cyber Ops Metrics team as an area of focus in part because it appears as one of the priority items from the Australian Defence Signals Directorate (DSD) Top 35 Mitigation Strategies[[4]](#footnote-5) list. Per the DSD, “At least 85% of the targeted cyber intrusions that the Defence Signals Directorate (DSD) responded to in 2010 could have been prevented by following the first four mitigation strategies listed in our Top 35 Mitigation Strategies.” Patch management is #1[[5]](#footnote-6) & #2[[6]](#footnote-7) in the DSD Top 35 list in terms of priority. The notion of patch management as critically important was also validated by its placement in the SANS 20 Critical Security Controls[[7]](#footnote-8) which lists audit guidelines for cyber defense. Further, the 2012 Verizon Data Breach Incident Report[[8]](#footnote-9) indicated that server, botnet, and hacker exploits targeted at unpatched vulnerabilities remains a threat vector of high priority, especially for organizations using insecure operating systems and non-hardened, or OEM, operating systems. It should be unsurprising that at the time of this report, strong correlations arguing for Patch Management to be included in the final selected ‘top 20%’ of available security remediation have also been found within works from NIST, CERT, Cloud Security Alliance and other credible and recognized sources[[9]](#footnote-10).

## Project Document Output

The Quick Start Guide for Patch Management (this document) is recommended as a guide and a reference. It documents a high level generic patch management process consistent with TM Forum Business Process Framework (eTOM), and then defines security key performance indicators (KPIs) as they relate to the process. These KPIs are not intended to completely address all important aspects of patch management, nor are some of these KPIs exclusive to security. There are a number of important aspects of a comprehensive patch management process that are deliberately not discussed in this document, with the specific intent of enabling a shorter and security-focused aid for security practitioners looked for a practical ‘short-list’ of things to measure in the real-world. For example, inventory management[[10]](#footnote-11) is distinct from, but related to, configuration management, of which this document considers patch management to a subset.

Wider patch management interests might include:

* maintaining any specific product’s general software level[[11]](#footnote-12);
* resolving a fault that has impacted a user / organization, or;
* introduce additional functionality;

all of which, when all combined with security patching greatly complicate patching policy overall. This document therefore does not cover the detailed issues around inventory or configuration management, or patching for reasons other than security[[12]](#footnote-13).

The document includes an overview of all the project outputs along with recommendations for use of each output artifact, and includes the inputs to this work as appendixes A (the original work list of metrics) and B (a high-level analysis of supply base considerations).

# Patch Management Security Metrics Overview

The goal of patch management security metrics is to support the overall improvement of the patch management process. It is intended that, as the metric improves, you can be reasonably certain your actual security is improved as well.

The team has found that balancing the need for speed with the need for quality presented a significant challenge to defining a small number of metrics that provide various levels of insight and precision, but at varying levels of cost and complexity. This report aims to clarify the minimum elements based on current best practice when considering what to measure about the security of patch management, solely, as a sub-set of Security Configuration.

You will not find a comprehensive list of key performance indicators in this guide, nor have we tried to create ‘our own new and improved list’, for which others have studied previously. We have instead drawn from some respected industry sources, and have sought agreement of direct participants from several sanctioning bodies, directly or indirectly. Chances are you have a pretty good idea what to measure, you just need a little help getting started, and a couple of concepts to stir healthy conversations.

Measurement is commonly more difficult than you initially expect. The data you need for good measurements may not be readily available, if at all. And, it is also common for the business rules of measurements to be heavily debated, with the 'truth' somewhat difficult to ascertain. Concessions may be required to move forward.

Measurement alone is not enough in most situations. People must be told and shown what to do in response to the measurements; compliance with the process must be enforced. Consider what to do about poor performance while creating each KPIs. Craft performance indicators with very granular detail: it is easier to aggregate from specific to general.

# Patch Management Process

In order to develop patch management KPIs, it was first necessary to understand the processes involved. The team described the general process of Patch Management as the following phases:

1. Identification Phase
2. Evaluation Phase
3. Testing Phase
4. Implementation Phase
5. Validation Phase

It is vital at all stages in the process to consider Parallel Mitigation (temporary mitigations taken during the patch management process to reduce risk until patching is complete).

## Identification Phase

As seen in Figure 1, the Patch Process for Security as a Business Process Framework (eTOM) level 4 process[[13]](#footnote-14) begins with the Identification of an RFC, driven by the need to Patch[[14]](#footnote-15). Working backwards, some TM Forum stakeholders, Defense members in particular, have more than the usual chances each period to discover new exploits. Their vulnerabilities are continually targeted. Measurement of the patch management process beginning ‘*When we find out’* is one working definition that covers, in general, the four specific sub-cases identified (see footnote 14). This ‘starts the clock’, so to speak, on the Identification Phase at this common-sense point.

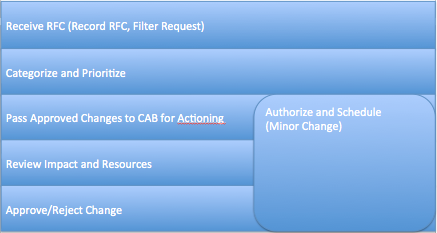


Figure – Patch Identification for Security: a subset of all RFCs and of the Configuration Process

So, in the Security Patch Management scenario, the RFC in Figure 1 is either the identification of the need to patch and/or the notifications of availability of the needed patch. Categorization and Prioritization occur in the Evaluation Phase. Passing the approved changes to the CAB for Actioning in this specific case is the process of verifying that the Security Patch is relevant[[15]](#footnote-16) to the operating environment. Review of impact and resources for the patch is addressing in the Testing Phase for Security Patch management, and as with all Changes, Approval must occur prior to the Implementation Phase, even in the case of an Emergency Security Patch change (please refer to Figure 2). So:

|  |  |
| --- | --- |
| **eTOM Change Management Process Step** | **Security Patch Management Phase** |
| Receive RFC | Identification |
| Categorize and Prioritize | Evaluation or Assessment |
| Review Impact & Resources | Testing |
| Approve Change | Implementation |

Table 1 – eTOM Change Management Mapping to Security Patch Management

## Evaluation Phase

An important aspect of the evaluation, or ‘assessment’, phase is to assess and confirm whether the patch applies in all particulars. This phase can be very complicated, but it’s acknowledged that the likelihood of a patch applying to a network is directly proportional to the degree to which systems are not hardened. Systems hardening is outside the scope of this document, being about configuration rather than patch management, but is among the best ways to improve patching security to avoid the need to patch as frequently or deeply.

If the need to patch is verified in the Evaluation phase, additional assessment may be required regarding the need to implement parallel mitigation. Parallel mitigation is the act of implementing temporary measures for security while the appropriate permanent action is taken, in this case, a security patch[[16]](#footnote-17). Depending on the criticality of the vulnerability, parallel mitigation might be needed to minimize risk while implementing the patch. For example, in extreme cases it may be necessary to deactivate, quarantine, or isolate the affected[[17]](#footnote-18) system(s) until the patch is in place. In others, no parallel mitigation may be needed or cost-justified.

At the time of this report, the team has found only indirect ways of capturing this nuance within any sort of specific metrics, but mentions it as increasingly relevant in the real world. If other efforts being chartered now within the TM Forum are successful[[18]](#footnote-19), someday it might be performed via auto-negotiation between member networks in timescales of hours or minutes rather than days. At present, parallel mitigation is an important consideration during the Evaluation phase for more sophistication and larger networks where the ability to implement parallel mitigation, and its relevance are both most pronounced.

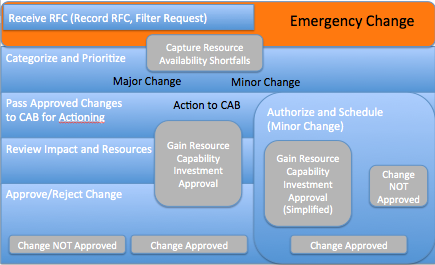


Figure – Evaluation Phase of Security Patch Management, Emergency Change

Notification of the results of the Evaluation Phase is presumed to gain Resource Capability Investment approval. (Please refer to Figure 2.) When reviewing the figures, please recall that this paper treats Security Patch Management as a subset of Patch Management, which in turn is a subset of Configuration Management, which itself is subject to the Change Management process requirements.

## Testing Phase

The Testing phase should be included in as many patches as possible[[19]](#footnote-20). A starting specific metric of 90-99% of all patches being tested prior to deployment is suggested as ‘good’.

Testing is critical to: a) ensure the patch does what it’s designed to do on the network being patched, and b) to ensure the patch doesn’t negatively impact critical functionality or possibly create a new vulnerability in the process of fixing the vulnerability it’s intended to patch. This is a complex task, especially in large and/or heterogeneous networks, with various security levels including insecure and/or unhardened operating systems.

As with all metrics where Testing is part of the critical path, there’s a natural urge to say ‘faster patching is better’, when in fact, setting targets too aggressively creates an artificial bias to reduce or eliminate testing of patches. While getting a patch in place fast may seem to be less risky, not testing a patch can create new unknown risks that may be worse than the known risk(s) being remediated.

## Implementation Phase

The team agreed that it was desirable to begin this Phase rapidly and in general complete it within 48-72 hours, a workable range of expectation for critical security patches. Of course, the rules must be flexible both for very large networks and for very small networks. For the very large, again, parallel mitigation and the notion of ‘what are we doing during the days we are patching to protect against the vulnerability’ are relevant – resources exist such that answers to these questions can be meaningfully contemplated. For the very small network, however, there are usually few realistic options aside from the patch itself.

Implementation may be performed wholly or partly by automation. As with all phases, the key is MTBF of the process, and not with what labor or technology it is performed. Increasing automation in security systems is necessary for quality, demonstration of compliance, and to make more cost-effective use of expensive security labor, which is in increasing demand. Important vulnerabilities said to be positively impacted by patching include: a) defense against intelligent guided exploits, b) defense against bot attacks or other low-intelligence automata, and c) server exploits.

Please refer to Figure 3 to see the transition from Test to Implementation Phase for Security Patching in context with the eTOM Change Management Process, which shows clearly how the ‘Time to Complete’ metric begins with a positive result of the Validation Phase, requiring the RFC be passed for Actioning (see Figure 1). The ‘Time to Complete’ metric ends when the Review of Change and Documentation are complete. Managing the Handover of Resource Operations in the specific case of Security Patch Management will include the appropriate steps to cease Parallel Mitigation if applicable before the Change can be Closed.

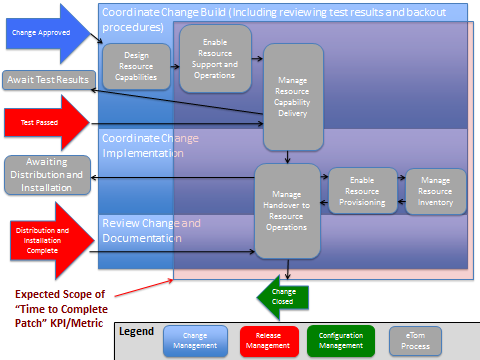


Figure – “Time to Complete Patch” Implementation Phase Scope

## Validation Phase

While several members of the team have expressed concerns about the cost, it is agreed to be preferable if a network can be tested after implementation of a patch to be sure of a ‘good’ outcome[[20]](#footnote-21). The simplest metric associated with patch management for security, or any other purpose is whether or not the patch needs to be rolled back; the team feels that the appropriate place to address rollback is within the larger scope of “Release Management” and not security.

Vulnerability scanning and code review automation exist adequate for the majority of security validation testing needs, though none is complete and all still require the input and oversight of human experts. In general, any Patch Management Program intended to include a Validation Phase should automated the design of Validation from the very beginning; otherwise, the error rates and costs of human labor alone performing such testing can quickly become prohibitive even for the most diligent organization, since statistically patches vary widely in effectiveness from operating system to operating system.

Included in this Phase is the notion of ‘released after patching’ or ‘approval’ or similar wording. In other words, the security work of patch management is not complete at the end of the Implementation phase and whether the system is again ‘released’ for Production use (ITIL) or simply ‘approved’ the logical work to be performed is the same, and in Validation. In Figure 3, the eTOM process mapping of Implementation, the Change would be ‘Closed’.

Note on Patch Severity

Severity is a consideration in determining the urgency, scope and other decision factors that drive the speed versus testing decision in patch management. Rather than suggesting a new definition of severity, the team offers examples of appropriate guides to this complex topic:

<http://cve.mitre.org/>

<http://nvd.nist.gov/>

<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>

<http://www.kb.cert.org/vuls/>

# KPI Meta-Data Collection Guide Detail

What are metrics to Patch Management as it relates to security? The KPI meta-data collection guide created for the TM Forum provides a structure for business units to use and modify as needed. The metrics in this guide are designed to be:

* Extensible (takes into consideration future growth)
* Scalable (is still cost[[21]](#footnote-22)-effective and practical as growth occurs)
* Agnostic (applicable independent of the specific technology chosen)

In general the following convention is used in the formal statement of the metrics:

Hours from ‘when we know’ about the need to patch to deployment time.   
Formula:        B - A

A=Time at which the existence of the patch is known

B=Time at which the patch is fully deployed

We can readily define several other times:

A’= Time at which the need for a patch is known

B’= Time at which the patch begins deployment

The Duration of each Phase can then be stated as follows:

Identification: A – A’

Evaluation: B’-A’

Testing: B’-A (if not skipped, it begins with confirming a need to patch)

Implementation: B – B’

Validation: A’new – B (next patch, or MTBP for that particular system)

The measures can be complicated by one or more of the following:

1. Start Event (noting that there is no clear definition in all cases for what constitutes an ‘immediately critical’ patch versus something that can take longer. For example: a critical patch may not be that critical to an unclassified desktop with no external network connection, if only used in a secure location);
2. Hold Event (e.g. insufficient evaluation of the patch available, or devices offline);
3. Completion Event (e.g. enterprise deployment – achieved to x%);
4. Inclusions (e.g. out of cycle critical patches released during the measurement period);
5. Exclusions (e.g. functionality patches);
6. Mitigations (e.g. what rules govern adjusting the metric and compliancy);
7. Process and Communications Methodology (e.g. how the metric will be reported and presented).

The TM Forum Patch Management workgroup identified the following six general measures:

1. Time to apply the patch: this implies steps 1-4 of the process. (See Figure 3 which is repeated for convenience below)

1a. Time exposed: instead of measuring the time to patch, measuring the time unpatched and exposed. Exposure begins at the same time as the Identification Phase (A). No effort has been made in this paper to suggest also determining A^, the time when the actual vulnerability existed versus when it was known, since the measure of the time spent vulnerable without knowing it is more closely related to the Use Case for Vulnerability Management rather than Patch management.

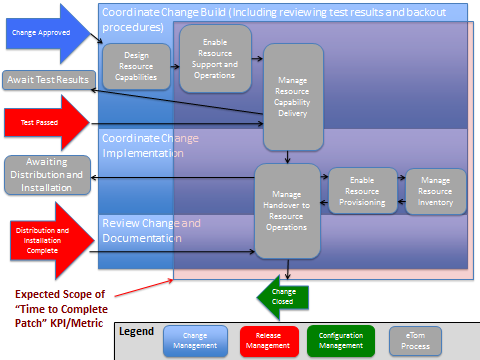


Figure – “Time to Complete Patch” Process Scope

1. % of devices by % patched (which is closely related to 3)

Alone, % of devices patched is of little actual use and did not make the list of essential measures. When accompanied at least by a sense of to what degree patching is complete degree up to 100%, then the % of devices ‘exposed’ (as with Time Exposed) is revealed by this measure. This leads many team members to prefer 1a to 1, so as to have Time Exposed (1), Devices Exposure (2), and % Exposed (3).

Otherwise, with 1 “Time to Patch”, there is the potential to trade off metrics 1 and 2 as required by delaying patches and lowering metric 1 and improving 2 and vice versa.

1. Criticality of Patch Exposure (presumed to be somehow objective)

This is a valid metric, but difficult to achieve and cost-prohibitive unless automation for this is designed in. A simple % of patches not applied for devices not fully patched, or ‘Devices Exposed’, as in 2, above, does not carry the desired meaning for security purposes without also saying that patching deviations are, on some scale, important.

If an organization has a robust Evaluation and Testing process, then this metric can realistically be supported. If, however, the extent of the patch management evaluation is ‘It was released by the OEM vendor and they say we should do it’, then resources to granularly define criticality of exposures are properly not well-invested. Not all programs need to have this level of security to be considered effective or to actually be effective.

One method suggested that offered consensus objectivity was to assess patches utilizing CVSS metrics. Patches remediating vulnerabilities with a CVSS score > CVSS-threshold need to be applied to high-priority systems in X time, medium-priority in Y time, and so on. This paper does not suggest one particular objective system over another, just notes that unless such a ‘standard’ is available for comparison, this measure loses some value.

1. Audited degree of systems susceptibility to attack

The security value is offset by cost and complexity for adding this metric to the “Validation” step in the process. One example of how to mitigate the cost and complexity is the common ‘Qualys’ scan, but this is neither directly related to Patch Management nor comprehensive, and would offer only a partial technical solution to the challenges of adding this measure.

Some team members noted that the Evaluation phase assumes this metric is including by analysis to some degree, as well as in Testing prior to implementation of the patch.

1. What % of patches result in further security problems, or MTBF of patch security

What percentage of patches result in either a) an incomplete solution to the vulnerability intended to be patched and b) a new vulnerability caused by the patch or patching process interaction with the actual environment (that was not revealed in the Testing phase of the process).

This metric is notionally simple and provides a mechanical view of the quality achieved in security patching without presuming the root cause. For example, a small MTBF (mean time between failures) of patching of a particular platform, component or device might mean ineffective patching process, poor patch quality or poor component or platform quality. This metric tells use where to look, but investigation as to cause is still required.

To be avoided is the seemingly closely related metric ‘which patches CAUSE security issues’. This is a poor metric because of the costs of gathering the data, including complicating factors like:

Over what time interval is the measurement to be taken?

What amount of time must pass before it’s decided the patch won’t cause issues?

Should problem severity created by the patch be factored in? (i.e. patches that cause minor problems for isolated systems to patches that shutdown a whole enterprises for days?)

Should problem localization be factored in? (What if the patch only causes a problem that affects one very important customer versus a problem that introduces a minor delay for online job applicants?).

1. Number of patches

The group concurred that too many patches is representative of a recurring problem, but is that really a metric for Patch Management? Control over the number of patches needed originates outside the Patch Management process, and so this metric might be appropriate as a measure of selection of systems architecture components or the quality of systems design and execution, but a patch being needed is an input to the Patch process, not controlled by Patch Management.

These preceding six metrics were found to have well-founded security benefits, and are the result of consolidating the larger list of metrics found in Appendix A. Wider benefits as a consequence of using the 6 metrics but in service delivery operational performance improvement would be anticipated though are not covered by this document.

## In Practice

In practice, there may be difficulties in consistently gathering data to support these metrics.

Depending on the configuration of a system, a patch on a specified vulnerability may open additional vulnerabilities in a corresponding software module. As all system configurations will vary, patches cannot necessarily be assessed in isolation. For example, the same piece of software, such as Java Runtime Environment (JRE) on two different platforms, e.g. X and Y, may behave differently after the application of the same patch. Applying the patch to the software on the X platform resolves the vulnerability. Applying the same patch to the Y platform closes the known vulnerability but due to the underlying framework configuration it creates another. This could lead to an inaccurate and diluted representation on the quality of a given patch.

# Summary Suggested Patch Management Security KPIs

The target for our work group was to produce a short list of the relevant metrics for security as related to Patch Management only, and specifically not for the larger question of Configuration Management. The full detail of this list is available in a separate spreadsheet and the summary list is presented here.

|  |  |  |
| --- | --- | --- |
| **ID** | **Business Unit** | **KPIs** |
| 1 | Configuration Management | Time to apply patches/Time unpatched |
| 2 | Configuration Management | Completeness of patching across and on devices |
| 3 | Security | Criticality of deviation from patching standards |
| 4 | Security | Audited Degree of Systems Susceptibility |
| 5 | Security | After-patch vulnerabilities |
| 6 | Architecture | Number of patches needed |

## Possible examples of commercially reasonable Patching SLA statements

a. Provider will promise Customer that patching for security emergency (where the term ‘emergency’ shall be specifically agreed contractually between parties) items will occur in not more than \_24\_ hours, with ≥ \_90%\_ tested  
b. Provider will promise Customer that patching for security critical (where the term ‘critical’ shall be specifically agreed contractually between parties) items will occur in not more than \_72\_ hours, with ≥ \_99%\_ tested  
c. Provider will promise Customer that patching will be successful in ≥ \_99%\_ of all cases at remediating the vulnerability identified  
d. Provider will promise Customer that patching will not create new vulnerabilities ≥ \_99%\_ of the time   
e. Provider will demonstrate via 3rd party auditor certification and attestation it's (security) patching practice via SSAE16, ISO27000, TM Forum (which), itSMF/ITIL v3.0 and/or PCI-DSS v2.0 or acceptably equivalent international standard NLT \_annually\_

Normally in an SLA these may not be wholly separated from overall patching requirements and configuration requirements. Patching schedules for critical feature/function patches are often on the same schedule as security patches, because they often have a real and immediate financial impact instead of a potential security impact). As a basis for contractual agreement, one or more of the industry-accepted standards of criticality may be agreed by both parties.

## Variables

Patching metrics vary based on factors including:

Device types, noting especially that mobile devices provide new challenges that at best are only incompletely addressed so far because they are still in part unknown. Regardless; the intent of the team at the time of this Quick Start is that any type of device that is patchable in any sense is within the scope of our intent. It’s likely that within the next few years new form factors of devices will emerge in the market, perhaps including Google Glass. These devices, too, if they are in way part of the enterprise or are allowed to come in contact with the data, systems or access of our networks, must obey the same expectations and metrics of patch management. However, more previously ‘excluded’ devices, those of the power grids supporting our facilities both internally and in our supply base (see below), may also be subject to increased patching requirements. “Household” devices allowed in the workplace, perhaps as simple as appliances, will provide additional threat vectors; these, too must be considered to be in scope, and this point gives new meaning to the Supply Base Appendix.

http://gizmodo.com/5910798/electric-imp-wants-to-connect-your-everything-to-the-internet

Network vs. application, a distinction that has only grown more complex as virtualization has increased our powers of abstraction in networking, applications and many other elements of computing. While it is true that ‘networking’ device OS historically require fewer patches than applications or ‘insecure’ operating system, under virtualization and proper network abstraction, the criticality of a network patch for security may exceed that many application patches. The annually updated Data Breach Incident reports show server exploits, most fully or partially counter-acted by patching, as one of the top threat vectors for enterprise networks.

Network perimeter vs. non-perimeter, always a vital security element, has only become a stronger bar to malicious activity, provided that inside networks no ‘open paths’ are allowed to exist once the perimeter is breached. It’s clear that in comes cases, systems or devices that do not have access to insecure networks or resources, especially those on isolated networks, may be excluded from patching consideration with a high degree of security for longer periods of time, provided of course that asset management exists to prevent the movement of devices without proper authorization and is enforced with automation ( a subject for the broader use case of Configuration Management, of which Patch Management is one facet )

OS – the most common subset of device patches would have to be either Application or OS, so it is with a degree of irony that the team notes here that not all devices have operating systems, just as not all operating systems have devices, at least not in the traditional sense, and it’s in these new “boundary zones”, where the rules are muddled, that risks are highest.

### Supply Base

This enormously complex topic is only suggested in Appendix B. The table included represents the prioritized activities for each of these industries based specifically on a defense world-view during a security cyber-event, such as the interdiction of Estonia by DDoS attack some years back. Other organizations can use this guide and reprioritize it as best suits their individual business needs and aims. Priority 3 activities would include non-critical functions deemed to have a position impact on operational readiness if assured within 24 hours, and Priority 4 activities those functions that are comfort functions with operational impact only if not assured after 72 hours or some other interval reasonable in the event.

One of the main goals of this project is to use the metrics from this quick start guide to give end-to-end assurance across the supply base.

# Recommended Use of the Quick Start Guide

This team’s recommended use of this guide is as a minimum sanity check for the Patch Management of any organization. In an organization has not addressed the minimum considerations in this document, it may be exposed to one or more of the most common threat vectors for security in the world today. As noted in this team’s business agreement, this is not just our opinion – sources specifically including SANS, AUS DSD, and the Verizon Data Breach Incident Report were compared to validate the choice of this and the other Cyber Ops Metrics quick start guides and the highest apparent priorities worldwide chosen.

As one of the expressed goals of this project is to use the metrics from this quick start guide to give end-to-end assurance across the supply base, it is recommended that each catalyst should trial these metrics both internally and across their supply base, focusing on those suppliers deemed to be critical suppliers. As logistics can be fraught with other risks, decisions can’t be made solely based on cyber-attack considerations alone. Cyber-attack threats must be considered in the context of enterprise risk management and mitigation overall, potentially affecting the entire enterprise. For additional references, this team recommends the TM Forum Insight Research Report “Enterprise Risk Management”, GB952[[22]](#footnote-23), as well as ISO/IEC 31000 and ISO/IEC 22301 (BS25999).

# Appendix A: Metrics Derived from Bibliography Search

|  |  |
| --- | --- |
| **Metrics covered** | |
| 1 | “Half life” for applying patches |
| 2 | Amount of time or effort involved in mitigating the vulnerability: 1.) Amount of time it takes for defects within an organization to be mitigated after the vulnerability is identified, 2.) Comparison of “time to patch” averages for proprietary commercial software vs. open source software |
| 3 | Average time to patch |
| 4 | Configuration Management Coverage |
| 5 | Cost of program failures |
| 6 | Cost of PVG |
| 7 | Cost of software |
| 8 | Cost of system administration support |
| 9 | Current Anti-Malware Coverage |
| 10 | CVSS: Common Vulnerability Scoring System, Version: 2, Specification: NIST IR 7435. Web site: http://www.first.org/cvss/ |
| 11 | Emergency configuration response time |
| 12 | Mean Cost to Mitigate Vulnerabilities; |
| 13 | Mean Cost to Patch |
| 14 | Mean Time to Patch |
| 15 | Meantime to deploy critical patches |
| 16 | Mean-Time to Mitigate Vulnerabilities; |
| 17 | Meantime to patch |
| 18 | Measure a system’s susceptibility to attack |
| 19 | Measure mitigation response time |
| 20 | Measure the cost of patch and vulnerability management |
| 21 | Network services ratio |
| 22 | No. of Applications with problems after patching |
| 23 | No. of Devices having problems after patching |
| 24 | Number of Applications |
| 25 | Number of known open, closed, or novel vulnerabilities |
| 26 | Number of known vulnerabilities |
| 27 | Patch management coverage |
| 28 | Patch Policy Compliance |
| 29 | Patch response time (critical) |
| 30 | Patch response time (noncritical) |
| 31 | Patches missing per device |
| 32 | Percent of Systems without Known Severe Vulnerabilities; |
| 33 | Percentage Critical Patch Coverage per IP Subnet |
| 34 | Percentage of Configuration Compliance |
| 35 | Percentage of systems with no known severe vulnerabilities |
| 36 | Percentage Patch Coverage for IP Subnet |
| 37 | Percentage Patch Coverage for Latest Critical Patch |
| 38 | Response time for vulnerability and patch identification |
| 39 | Security Patch Release Speed(time) |
| 40 | Unapplied patch ratio |
| 41 | Vulnerability ratio |
| 42 | Vulnerability scanning coverage |

# Appendix B: Cyber Operations Metrics for Security Management – Prioritization in the Supply Base/Network and CNI

Risks to the operation of top-level customer organizations from suppliers and sub-contractors are diverse and increasing. This document identifies the primary types of prioritized risk in a number of sectors in a framework that is ISO29115 compliant for risk mitigation, which can then be re-used as a guide. Key points:

* The notion of a supply base being a clean hierarchy of supplier companies operating at Tier 1, 2, 3 etc. feeding into a government customer organization is misleading and inaccurate. For reasons of globalization and market forces, the supply base in most sectors is a mesh or network. Companies can be Tier 1 and 2 and 3 at the same time, even in the same contract.
* Re-use of information sharing services and capabilities is essential to the minimization of risks and costs, and for competitive advantage for a company. It can’t afford different information sharing solutions for different customers. They require one standards-based approach.
* Supply bases are not unique to a sector, but are blurred and thus highly interconnected and interdependent. For example, power affects everyone but it can’t operate without transport. A high proportion of companies operate in more than one sector and supply base. Internationally, supply bases are a mesh of meshes.
* Government can often be a supplier, particularly for the provision of accurate user data to enable the service provider to provide a Just In Time service – e.g. the operational maintenance of military helicopters by Westlands depends on usage data from the military at first and second line.
* Each organization (including Government) has to consider Enterprise Risk and Shared Risk. Enterprise Risk is the internal set of risks that are managed by the organization’s directors at their discretion in accordance with the law. Shared risk is the set of external, collective risks that every member of the supply base shares, including the customer, and the collective mitigation is normally defined in the (federation) Common Policy, which includes:
  + Standard contract language for shared risk mitigation in commercial arrangements
  + Reference to mandatory standards
  + Additional policies, procedures and mechanisms for multi-jurisdictionally
  + A binding risk assessment model
  + A set of mitigations for trusted interactions in normal business operations, including collaborative working arrangements (e.g. in collaborative working environments or collaborative cloud services) and information management (e.g. multi-mastering management, version control, information quality, archiving, purging)
  + Third party audit policies and procedures
  + Enforcement policies and procedures
  + Other policies and procedures e.g. for dispute resolution and trust restoration.

The next page shows two tables combined into one. The first table concerns the priority for maintaining the electronic business interactions between organizations. The second concerns the priority for ensuring the availability of shared information sources, such as Collaborative Work Environments (CWE), information hubs and secure email. The majority of CWEs and information hubs are operated by prime contractors and Tier 1 companies, however a significant proportion are also held at Tier 2 and Tier 3. Most importantly, the master data that feeds these CWEs and hubs is usually held in the data-owning companies, so timeliness of data can be an issue. Government holds relatively little data.

These are not distinct sectors and there is high degree of multi-layer inter-dependence – nearly every sector has a shared risk dependency on every other sector in the majority of situations, to some degree. Some verticals (e.g. telecoms, power, transport) are also horizontals.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Aerospace & Airlines | Air Traffic Management | Power | Health | Finance | Telecoms |
| Priority 1 | - Flying aircraft  Maintaining aircraft  - Passenger handing systems (e.g. PNR)  - Airside and passenger side security systems  - First responder incident management  - Manufacturing military aircraft  - Providing spares for use within a 12 hour period  - Holding shared data for the above. | - Flight planning  - Flight plan management  - Air navigation systems  - Air communications systems  - Staff credential management systems  - Backup power and communications systems support  - Emergency management systems  - Physical and logical security systems  - Providing spares for use within a 12 hour period  - Holding shared data for the above. | - Safety monitoring systems  - Power generation monitoring systems  - Power generation management systems  -Grid usage monitoring systems  - Grid availability monitoring systems  - Providing spares for use within a 12 hour period  - Holding shared data for the above. | - Ambulance management services  - Bluelight coordination  - SPINE core systems  - Drug dispensing systems in hospitals and local pharmacies  - Hospital patient record management systems  - Summary care record systems  - Providing spares for use within a 12 hour period  - Holding shared data for the above. | - Payments system (BACS, IBAN etc)  - ATM system  - Horizon network  -Internal access control systems  - Audit systems, particularly for regulatory compliance  - Trader monitoring systems  - Account management systems  - Money supply systems with the Bank of England | - Core infrastructure management systems  - Core infrastructure monitoring systems  - Usage and load management  - IDS  - Access control management  - Providing spares for use within a 12 hour period  - Holding shared data for the above. |
| Priority 2 | - Manufacturing civil aircraft  - Inflight catering  - Essential ground transport  -Providing spares for use within 24 hours | - Staff HR systems  - Staff rostering  - Maintenance management systems  - Providing spares for use within 24 hours | - Demand forecasting systems  - Maintenance management systems  - Job management systems  - Providing spares for use within 24 hours | - Drug supply base ordering and management systems  - Contractor and contract management systems  -Providing spares for use within 24 hours | - Payments credential management systems (Identrust etc.)  - Customer enrolment systems | - User account management systems  - User billing systems  - Web hosting services  - Job management systems  - Providing spares for use within 24 hours |
| Priority 3 | - Ground transport  - Terminal passenger services  - Certification systems  -Providing spares for use within 48 hours | - Certification systems  - Training systems  - Providing spares for use within 48 hours | - Mapping systems  - Certification systems  - Training systems  - Providing spares for use within 48 hours | - Providing spares for use within 48 hours |  | - Providing spares for use within 48 hours |
| Priority 4 | - Providing spares for use within 72 hours | - Providing spares for use within 72 hours | - Providing spares for use within 72 hours | - Providing spares for use within 72 hours |  | - Providing spares for use within 72 hours |

# 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.

## About this document

This is a TM Forum Guidebook. The guidebook format is used when:

The document lays out a ‘core’ part of TM Forum’s approach to automating business processes. Such guidebooks would include the Telecom Operations Map and the Technology Integration Map, but not the detailed specifications that are developed in support of the approach.

Information about TM Forum policy, or goals or programs is provided, such as the Strategic Plan or Operating Plan.

Information about the marketplace is provided, as in the report on the size of the OSS market.

## References

|  |
| --- |
| Australian Defence Signals Directorate Top 35 Mitigation Strategies: <http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm> |
| SANS 20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines: <http://www.sans.org/critical-security-controls/> |
| Verizon 2011 Data Breach Investigations Report: [www.verizonbusiness.com/about/events/2012dbir/index.xml](http://www.verizonbusiness.com/about/events/2012dbir/index.xml) |
| TM Forum’s Business Process Framework (eTOM): [www.tmforum.org](http://www.tmforum.org) |
| Security Compliance Audit Automation: <http://www.tmforum.org/BusinessAgreements/SecurityCompliance/48393/article.html> |
| MITRE Common Vulnerabilities and Exposures (CVE): <http://cve.mitre.org/> |
| National Vulnerability Database: <http://nvd.nist.gov/> |
| The Open Web Application Security Project: <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project> |
| US-CERT Vulnerability Database: <http://www.kb.cert.org/vuls/> |
| TM Forum Insight Research Report “Enterprise Risk Management”, GB952: <http://www.tmforum.org/Guidebooks/GB952RiskManagement/46926/article.html> |

## Document History

### Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 0.1-0.4 | May 4-16, 2012 | Mike Carpenter, TOA Technologies | Draft |
| 0.5 | May 17, 2012 | Mike Carpenter, TOA Technologies | Draft |
| 0.6 | May 18, 2012 | Alex Hamerstone , TOA Technologies | Draft |
| 0.7 | May 21, 2012 | C. Coffey, TM Forum | Draft |
| 0.8 | May 30, 2012 | Mike Carpenter, TOA Technologies | Updates from walk-though with Project Champion. |
| 0.9 | June 7, 2012 | C. Coffey, TM Forum | Final preparation for team review and vote. |
| 0.9b | July 9, 2012 | Mike Carpenter, TOA Technologies | Edits for comments from team review |
| 0.10 | Sep 14, 2012 | Alicja Kawecki, TM Forum | Minor cosmetic corrections prior to web posting for Member Evaluation |
| 0.11 | Apr 2, 2013 | Alicja Kawecki, TM Forum | Updated to reflect TM Forum Approved status |

### Release History

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

## Company Contact Details

|  |  |
| --- | --- |
| **Company** | **Team Member Representative** |
| Ministry of Defence, DSTL | Martin Huddleston |
| TOA Technologies | Mike Carpenter |
| MITRE | Susan Schreiner |
| BBFA | Patrick Curry |
| BT | Hugh Payton |
| Bell Canada | Blake Lindsay |
| TM Forum | Christy Coffey |
| TM Forum | Jenny Rottinger |
| Booz Allen Hamilton | Larry Frank |
| UKCeB Liaison | Simon Croall |

## Acknowledgments

To Martin Huddleston, DSTL, our executive sponsor, ***many thanks for your guidance, leadership, and support.***

This document was prepared by the members of the TM Forum Cyber Ops for Security Management project team:

Mike Carpenter, TOA Technologies, Editor and Team Leader

Patrick Curry, British Business Federation Authority

Christy Coffey, TM Forum

Jenny Rottinger, TM Forum

Additional input was provided by the following people:

Luke Forsyth, CA Technologies

Hugh Payton, BT

Simon Croall, UKCeB Liaison

Susan Schreiner, MITRE

Alex Hamerstone, TOA Technologies

Pamela Abbott, Brunel University

Blake Lindsay, Bell Canada

Larry Frank, Booz Allen Hamilton

Clive Reeves, Telstra

1. Please refer to Appendix B for a short summary treatment of some considerations for larger organizations [↑](#footnote-ref-2)
2. e.g. a simple “tree” of providers with no cross-branch connections and few sub-levels (“flat” structure) [↑](#footnote-ref-3)
3. The full scope of Patch management includes security, failure, business function change, end-of-life, end-of-software, and release management among others; this document deals only with patching security metrics. Please refer to the larger body of work available from TM Forum for details on other aspects of patch management, which would include non-security technical impacts, customer and product management impacts, and others. [↑](#footnote-ref-4)
4. Australian Defence Signals Directorate Top 35 Mitigation Strategies: <http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm> [↑](#footnote-ref-5)
5. patching of office automation, e.g. .pdf viewers, Flash player, word processors, spreadsheets [↑](#footnote-ref-6)
6. patching of operating systems [↑](#footnote-ref-7)
7. SANS 20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines: <http://www.sans.org/critical-security-controls/> [↑](#footnote-ref-8)
8. Verizon 2011 Data Breach Investigations Report: [www.verizonbusiness.com/about/events/2012dbir/index.xml](http://www.verizonbusiness.com/about/events/2012dbir/index.xml) [↑](#footnote-ref-9)
9. Please see ‘Note on Patch Severity’ for examples of specific references for the organizations noted [↑](#footnote-ref-10)
10. to collect, record, and report the software and settings on each managed device [↑](#footnote-ref-11)
11. for continuity of supplier supportability [↑](#footnote-ref-12)
12. performance, reliability, contractual requirements, homogeneity, supportability, integration, etc. [↑](#footnote-ref-13)
13. Readers unfamiliar with Business Process Framework (eTOM) should please see appropriate references [www.tmforum.org](http://www.tmforum.org) [↑](#footnote-ref-14)
14. which presumes ongoing Monitoring or some other means of discovery of the need to Patch. This can be based, for example, on: a) the announcement from the patch provider, b) announcement of the exploit, c) confirmation of the exploit [which may coincide with (b)], or d) discovery of the exploit. [↑](#footnote-ref-15)
15. i.e., is not obviated by systems hardening or other exclusion of elements that would otherwise need patching [↑](#footnote-ref-16)
16. on less sophisticated networks this concept may not be applicable. On smaller networks easily patched quickly, this concept may not be practically relevant regardless of the degree of network sophistication. [↑](#footnote-ref-17)
17. Finding the affected systems is a complicated process without software/packet versions (e.g. a repository) [↑](#footnote-ref-18)
18. specifically including <http://www.tmforum.org/BusinessAgreements/SecurityCompliance/48393/article.html>  [↑](#footnote-ref-19)
19. smaller organizations may have to outsource testing, or accept patches as adequately tested by the source [↑](#footnote-ref-20)
20. e.g., the patch works, and the patch does not cause new issues [↑](#footnote-ref-21)
21. While intended to be used in the real world, cost was specifically NOT a primary consideration in the selection of security metrics for this Quick Start. Ideally, a good metric costs less to collect as it scales and works as well for large networks and small. In reality, organizations often accept compromises between data quality and cost of collection. [↑](#footnote-ref-22)
22. The specific notion to be taken from GB952 is that included in the list of risks to be addressed is whether the entirety of the supply base consistently addresses patching for security, so as not to allow a single entity to compromise the business, whether via supply base, fraud or any other of the two dozen risk areas included in GB952. Cyber-attacks changing this data can cause the basis of risk decisions to be wholly compromised. [↑](#footnote-ref-23)