Business Process Framework (eTOM)

For The Information and Communications Services Industry

Addendum Z:

Application Note: Use Cases for Security Management

GB921 Addendum Z

Version 12.2

April, 2012

Notice

No recipient of this document and code shall in any way interpret this material as representing a position or agreement of TM Forum or its members. This material is draft working material of TM Forum and is provided solely for comments and evaluation. It is not "Forum Approved" and is solely circulated for the purposes of assisting TM Forum in the preparation of final material in furtherance of the aims and mission of TM Forum.

Although it is copyrighted material of TM Forum:

- Members of TM Forum are only granted the limited copyright waiver to distribute this material within their companies and may not make paper or electronic copies for distribution outside of their companies.
- Non-members of the TM Forum are not permitted to make copies (paper or electronic) of this draft material other than for their internal use for the sole purpose of making comments thereon directly to TM Forum.
- If this material forms part of a supply of information in support of an Industry Group Liaison relationship, the document may only be used as part of the work identified in the Liaison and may not be used or further distributed for any other purposes

Any use of this material by the recipient, other than as set forth specifically herein, is at its own risk, and under no circumstances will TM Forum be liable for direct or indirect damages or any costs or losses resulting from the use of this material by the recipient.

This material is governed, and all recipients shall be bound, by all of the terms and conditions of the Intellectual Property Rights Policy of the TM Forum (http://www.tmforum.org/Bylaws/1094/home.html) and may involve a claim of patent rights by one or more TM Forum members or by non-members of TM Forum.

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

Table of Figures

Executive Summary

The objective of this document is to gather Use Cases identified as significant for Security Management within enterprises. The contents have been developed by the Security Management project/team within TM Forum, and published as Technical Report TR173 “Security Management Use Cases”. This has now been contributed to the Business Process Framework to provide insight into how security management is handled, and as a stimulus for further work, e.g. the development of process flows that address these use cases, material to help refine and enhance existing process definitions, etc. It is being published here as part of the Business Process Framework document suite to further widen its visibility and to position it as a basis for further work, as noted above.

This document is an Application Note, aiming to document an approach based on industry experience that can be used by an organization to help address security management as an aspect of its overall business needs.

Note that, as an Application Note, this material should not be read as normative – i.e. a single standardised approach – but rather as a representative mechanism that provides a useful base for others to build on. Other approaches are also possible. It is the goal of work like this to assist convergence for the industry, but not to impose a single approach, where there are other variations and alternatives that make sense.

1. Introduction

This report is organized around three Use Cases in which Security Management processes play a key role. These Use Cases were identified by Defense and Service Provider Security Management community members, because of the risk that they pose to their respective organizations.

Denial of Service Attack (DoS)	Penetration Attack	Application Misuse/Abuse *(Future)*

Each of these Security-themed Use Cases is presented as a set of business process flows. These flows are captured from existing processes from the Business Process Framework (eTOM) - down to Level 3 process decomposition, and proposed L4 and L5 processes. *(Please note: The processes designated as "proposed" have been captured within this document for completeness. When they have been factored into a future eTOM release, this document will be synched with the model so that the names and process decomposition levels are in agreement.)* The intent is not to document the entirety of the complex process flow for each Use Case, but rather to exercise the eTOM for Security Management Use Cases in an effort to demonstrate its effectiveness and validate its completeness.

Please note that while Security Management is specifically captured as Level 2 process in the Enterprise Risk Management area of the eTOM, the Security Management Use Cases span Enterprise Management, Strategy, Infrastructure Lifecycle Management, and Product Lifecycle Management (SIP), and Operations as well.

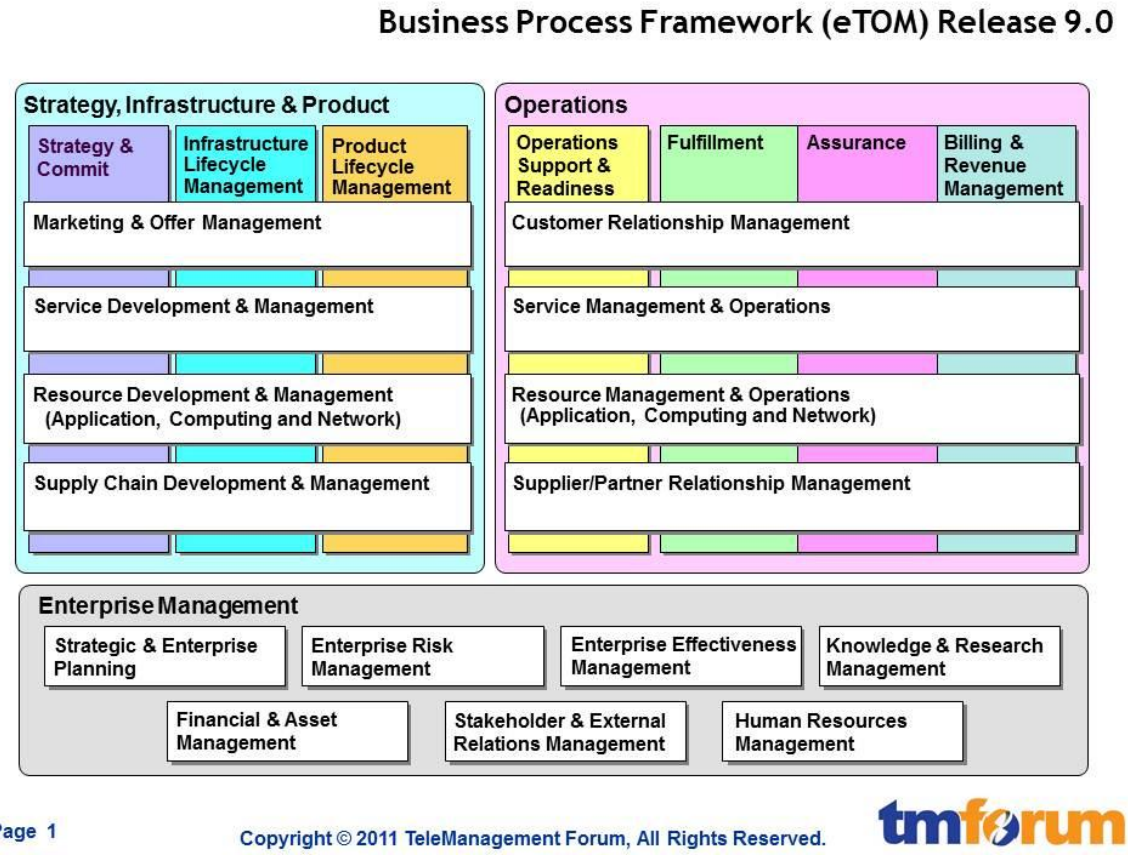

Figure 1: Business Process Framework (eTOM) Release 9.0

It is expected that additional Security Management Use Cases will be added over time, and that further eTOM decomposition (to Level 4 or 5) will be needed to support more specialized Security Management processes.

1.1. Use of the Security Management Model

To help organize the business process capture for each of the Use Cases, and flesh out Security Management L3 processes, the team applied the Security Management Model.

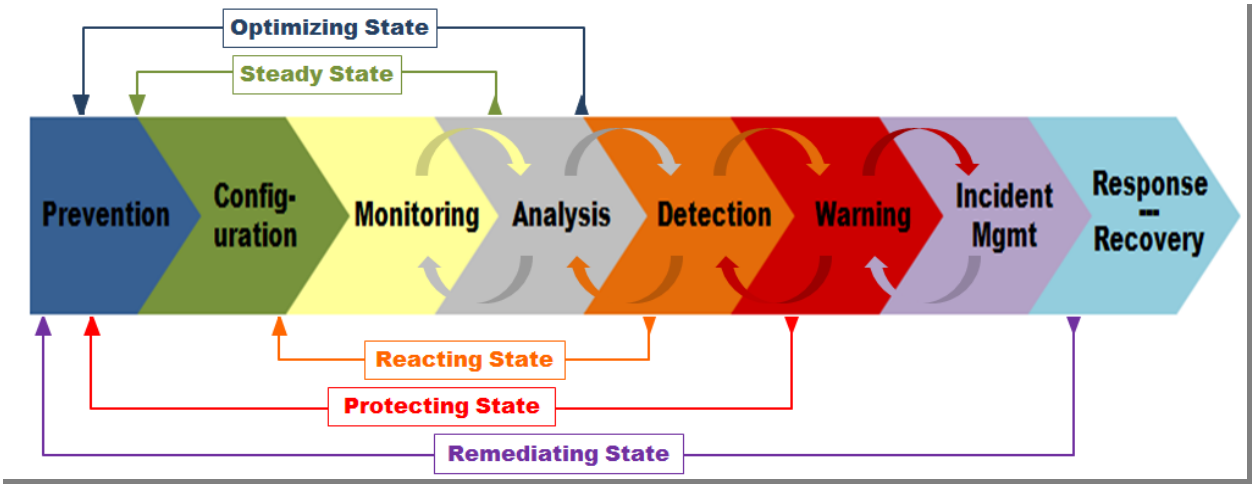

Figure 2: TM Forum Security Management Model

The TM Forum Security Management Model, illustrated in Figure 2, is an abstract model consisting of process flows and operational states. As an abstract model, it is a logical amalgam of multiple similar models and not intended as an exact representation of any specific actual system implementation. It is intended primarily as a tool to promote understanding, facilitate communication and collaboration, and guide coherent evolution across the complete TM Forum Frameworx.

2. Use Case 1: Denial of Service Attack (DoS)

Use Case 1: Denial of Service Attack

2.1. Characteristic Information

By definition, a Denial of Service Attack (DoS) is an attempt to make a computer or network resource unavailable to its intended users. A DoS can be executed in a number of ways including:

- Flooding the network with traffic
- Sending requests to a server intended to overload resources
- Sending data that causes a process or the entire server to crash.

Destruction of data also causes a denial of service. However, this type of attack is not usually thought of as a "DoS". One type of attack that is in the news frequently is a Distributed DoS (DDoS). A DDoS uses multiple systems to generate the necessary data traffic to cause the DoS.

Effective Security Management (eTOM L2 – Security Management) against a DoS occurs in two separate, but mutually supporting phases: Prevention and Operations.

Prevention (eTOM L3 - Prevention) activities are executed before an attack happens, and are intended to limit the vulnerability to attack, and enable rapid detection and response to an attack when it occurs.

Operations activities consist of monitoring, detecting, analyzing and responding to attacks (eTOM L3 – Monitoring, Detection, Analysis, Response & Recovery).

2.1.1. DoS Prevention

Effective blocking of a DoS attack requires the system owner/operator to have analyzed both the network and system resources to identify likely methods for attack and to design mitigations into the system.

Things like network traffic monitoring, firewall configuration, proper network segmentation and design, DMZs and load-balancers, installation of Intrusion Detection Systems (IDS) or Intrusion Prevention System (IPS) - either on the network, on the potential target systems, or both can assist with identifying and mitigation the effects of an attack, but will in no way prevent the attack. Attack effect prevention cannot typically be achieved without the aid of the carrier without a) adequate spare capacity to absorb the attack b) services of a 'scrubbing' service to quickly separate malicious from legitimate traffic and return it to the enterprise network or c) diversion of the attack without scrubbing or filtering. Carriers are in a far superior position to prevent DoS attacks by mitigating them for the entire affected IP space. Attack mitigation is usually, therefore, limited only to what can be achieved via firewall and load-balancer configuration, and by proactively ensuring proper network design and carrier overcapacity to absorb attacks.

Also, the system owner needs to monitor security bulletins for new vulnerabilities identified for the system configuration. When these bulletins are released, the system owner needs to analyze the

threat that the new vulnerability poses to the system, and determine if a new patch (or other change) is required.

Business Process (eTOM) Steps Involved

Proposed L4: Conduct Vulnerability Management: Review new vulnerabilities to determine the applicability to the local environment. If the local environment is vulnerable, recommend changes to configuration to mitigate or eliminate the vulnerability.

Proposed L4: Conduct Threat Assessment: Review available information to determine the likelihood of attack from general or specific attack sources. Prioritize likely attackers and their methods.

Proposed L4: Conduct Risk Assessment: Based on the results of the threat assessment, review local computing environment configuration to identify potential weaknesses.

Proposed L4: Conduct Risk Mitigation: Based on threat and risk assessments, determine appropriate mitigation strategies (e.g., deploy additional Intrusion Prevention Systems (IPS), change firewall setting) to limit the potential for a successful attack. Check servers to make sure that corporate policies and security guidelines are being followed.

Proposed L5: Configuration: Modify (or direct modification of) network and/or systems to minimize vulnerability to attack.

(Note: Above is not specific to DoS and would be applicable in almost all attack user stories.)

2.1.2. DoS Operations

Security Management and Network Operations personnel have ISP or CSP Intrusion prevention system (IPS) and IDS sitting on the network in key places to watch what's going on in the network. These services[1] will alert if they see issues. Being signature-based, these systems are limited to responding to the unknown, but algorithmic and behavior sending adaptive technologies are rapidly emerging that are more adaptable. Carriers monitor systems via network devices and firewalls. Security is performed in-depth; perimeter-controls protect the integrity of the controlled IP space, while internally proper network design and segmentation[2] ensure that attacks originating internally from compromised resources are just as readily identified and that networks are zoned to protect recoverability and critical resources by isolating impacted resources until they can be recovered and shifting operations automatically to other portions of the infrastructure We're going to focus on the external DoS attach scenario, the most complex, least controllable and most to be feared scenario, with many diverse IP addresses attacking from multiple origins as is the case with Distributed Denial of Service using massive botnets. We will further assume for this case that our network is a Target of Intent, rather than a Target of Opportunity, such that the attacked will have anticipated the simpler strategies involving multiple points of presence and have done the research to identify all our points in ingress to the public internet, at minimum.

Business Process (eTOM) Steps Involved

L3: Analysis
- *Proposed* L4: Analyze Events
- *Proposed* L4: Analyze Data
- *Proposed* L4: Analyze Software

L3: Detection
- *Proposed* L4: Detect Anomalous Events
- *Proposed* L4: Detect Malware

[1] Form factor supporting solution may be standalone, component blade or service

[2] examples include VPNS (virtual private networks), sub-netting, tunneling and other forms of achieving abstracted and/or encrypted or otherwise secure channels for routing or other synchronous or asynchronous communications

L3: Incident Management
Proposed L4: Warning
Proposed L4: Response & Recovery

Monitoring

- In addition to security specific monitoring and detection devices, System Operations personnel monitor traffic flow and process states of systems in the course of ensuring appropriate quality of service. All of these inputs provide potential sources of information.
- DoS detection services watching for anomalies on the network.

L3: Monitoring (collecting and correlating data from diverse sources)
Proposed L4: Monitor Networks: System Operations automation[3] or personnel forward any anomalous network activity to security management automation or personnel for correlation with other information.
Proposed L4: Monitor Systems: System Operations personnel forward any anomalous system activity to security management personnel for correlation with other information.
Proposed L4: Monitor Security Sensors (IDS, IPS, etc.): Security Sensors forward events to Security Monitoring[4]

Analysis

L3: Analysis: Perform detailed analysis[5] of events, data, software, etc.
Proposed L4: Analyze Events: Evaluate events to determine how a specific event or set of events occurred. This includes conducting forensics analysis of systems if appropriate.
Proposed L4: Analyze Data: Evaluate data to determine if there has been any corruption. *Note: In some cases, A DoS can be caused by malformed or malicious data being received and then accepted by the system (causing processes to fail). That, in turn, could cause data corruption.*
Proposed L4: Analyze Software: Analyze software to identify malware, etc.
Proposed L4: Preserve Forensic Data: Collecting data to determine origin and reason for the attack, and support future Law Enforcement activities.

- Inspect packets

Detection

L3: Detection: Using tools and sensors apply signatures and other methodologies to identify anomalous events, malware and other events which may indicate malicious activity. Detect denial of service impact on persistent connections and by noting deltas in transaction metrics.
Proposed L4: Detect Anomalous Events: Apply signatures and other methods to capture anomalous events to flag/alert (based on thresholds)
Proposed L4: Detect Malware: Detect malware signatures in network traffic. *Note:* While most people think of a DoS as a "flood" attack – there are DOS which use malicious code inserted into a process that causes the DOS.

Incident Management: The overarching process for incident management, including warning of component organizations, etc. as well as defining and executing appropriate response actions.

Warning

- Receive indications of malicious activity (DoS Attack)
- Security is notified of a possible problem

[3] Increasingly effective attack mitigation depends on defenses operating in synchrony at machine speeds

[4] also, law enforcement, black listing services and security service collaborators and partners
[5] all five steps may be performed in rapid sequence by automation instead of manually as implied

- Send appropriate warning information to Network Operations Center (assumes security management is separate from NOC)
- Send warning to business partners
- Network Operations looks for an alternate cause (change management (maintenance), an open ticket, or temporal surge has triggered the problem) → not our cause

Response & Recovery (this could be simultaneous with the step above)

- Based on analysis of the event (events) determine appropriate courses of action:
    - If you find out the origins, contact the ISP to turn off the IP addresses
    - Shut down the port on the firewall or another network element (router, load balancer, etc. depending on network set-up) if interrupting all network traffic is the best option
    - Null route or otherwise divert traffic away from the network space
    - Pass incoming traffic to a scrubbing or filtering service, incurring the delays for scrubbing and round trip but continuing operations with a defined latency delay
    - Burst available connectivity and bandwidth if that is the choke point to alleviate delays
    - Bring additional connection resources online in the affected service tiers(s)

3. Use Case 2: Penetration Attack

Use Case 2: Penetration Attack

3.1. Characteristic Information

Penetration attacks can take many forms, but essentially represent the penetration of a resource, device, or network by an unauthorized party with the intent to control the resource, view or extract data or instructions, facilitate further penetration into a network, or degrade, alter or destroy system data or performance. This kind of attack maybe and can be difficult to block. The attack can be automated or manual, and it generally utilizes flaws in the system environment (e.g. configurations, logic, etc.) as the means of penetration. Penetration attacks can occur anywhere, and will typically target the weakest link in the security of a customer can occur; e.g. a user with a weak password who has escalated privileges, using a rogue certificate, or exploiting cross scripting attacks (xss) on middleware product layers. These attacks can occur externally or internally.

Effective security Management related to Penetration Attack occurs in two separate but mutually supporting phases.

Prevention (eTOM L3 - Prevention) activities are executed before an attack happens and are intended to limit the vulnerability to attack and enable rapid detection and response to an attack when it occurs.

Operations activities consist of monitoring, detecting, analyzing and responding to attacks (eTOM L3 – Monitoring, Detection, Analysis, Response & Recovery).

3.1.1. Penetration Attack Prevention

Prevention is the best defense against a Penetration Attack because the attackers tend to try for stealth in executing the attack and it is very possible that the Intrusion Detection Systems will not alarm. A systemic implementation of policy to ensure conformance on all servers (includes authentication mechanisms, access control rules, limits on privileges, patching of vulnerabilities, audit log management, etc.) is the only effective defense. To be effective, this enforcement of policy must be integrated into the design of the network and would also include things like use of security hardening guidelines (e.g., ensuring that unused ports are turned off, segregating internal and externally facing systems, reducing or eliminating cross domain trusts, and making sure that the platform operations and security are checked when put into operation) to make it more difficult for an attacker to move between systems more difficult.

Business Process (eTOM) Steps Involved

- *Proposed* L4: Conduct Vulnerability Management: Review new vulnerabilities to determine the applicability to the local environment. If the local environment is vulnerable, recommend changes to configuration to mitigate or eliminate the vulnerability.
- *Proposed* L4: Penetration attack against a given network to identify potential attack methods that can provide access.

Proposed L4: Conduct Threat Assessment: Review available information to determine the likelihood of attack from general or specific attack sources. Prioritize likely attackers and their methods.

Proposed L4: Conduct Risk Assessment: Based on the results of the threat assessment, review local computing environment configuration to identify potential weaknesses.

Proposed L4: Conduct Risk Mitigation: Based on threat and risk assessments, determine appropriate mitigation strategies (e.g., deploy additional Intrusion Prevention Systems (IPS), change firewall setting) to limit the potential for a successful attack. Check servers to make sure that corporate policies and security guidelines are being followed.

Proposed L5: Configuration: Modify (or direct modification of) network and/or systems to minimize vulnerability to attack.

3.1.2. Penetration Attack Operations

Security Management and Network Operations personnel install, operate and maintain ISP or CSP (Intrusion prevention system (IPS) & IDS sitting on the network in key places to watch what's going on in the network. These boxes will alert if they see issues. However, as these devices are primarily signature-based, they may miss an attacker that uses a method not recognized by the IPS & IDS signature. Operations personnel periodically collect and review log data from systems. This data is fused and correlated with data from other systems across the network in order to identify malicious activity not detected by signature based analysis.

Business Process (eTOM) Steps Involved

Monitoring

- In addition to security specific monitoring and detection devices, System Operations personnel monitor traffic flow and process states of systems in the course of ensuring appropriate quality of service. All of these inputs provide potential sources of information.

L3: Monitoring (collecting, fusing and correlating data from diverse sources)

Proposed L4: Monitor Networks: System Operations personnel forward any anomalous network activity to security management personnel for correlation with other information. Chances are that a penetration attack is not going to be picked up by Operations.

Proposed L4: Monitor Systems: System Operations personnel forward any anomalous system activity to security management personnel for correlation with other information. Audit log collection and review may provide a means to identify unauthorized behavior. Log systems that offload collection, correlation and fusing of log data can support human review of logs. Setting thresholds (e.g., number of failed login attempts) to enable automated alerting while not overwhelming network operations staff with false negative reports is also useful.

Proposed L4: Monitor Security Sensors (IDS, IPS, etc.): Security Sensors forward events to Security Monitoring

Analysis

- L3: Analysis: Perform detailed analysis of events, data, software, etc.
- *Proposed* L4: Analyze Events: Evaluate events to determine how a specific event or set of events occurred. Includes conducting forensics analysis of systems if appropriate.
- *Proposed* L4: Analyze Data: Evaluate data to determine if there has been any corruption.
- *Proposed* L4: Analyze Software: Analyze software to identify malware, etc.
    - Collecting and analyze data to determine origin and method of the attack
        - Inspect packets
        - Capture of compromised systems to facilitate deep forensics analysis
-

Detection

- L3: Detection: Using tools and sensors (IDS/IPS, etc) apply signatures and other methodologies to identify anomalous events, malware and other events which may indicate malicious activity.

- *Proposed* L4: Detect Anomalous Events: Apply signatures and other methods to capture anomalous events to flag/alert (based on thresholds). Also, alert system administration personnel responding to trouble calls because a device behaving incorrectly should be aware of and looking for potential intrusions which may alter device behavior. Many penetration attacks are found because an administrator noticed an unauthorized configuration change while performing routine system management tasks.
- *Proposed* L4: Detect Malware: Detect malware signatures in network traffic and on systems.

Incident Management: The overarching process for incident management, including warning of component organizations, etc. as well as defining and executing appropriate response actions.

Warning

- Receive indications of malicious activity - e.g., penetrations of other networks, identification of new penetration techniques, etc.
- Send appropriate warning information to Network Operations Center (assumes security management is separate from NOC) – when a penetration attack is identified (successful or unsuccessful) provide notice internal organizations identifying the method used, source of the attack (as best it can be determined,) etc.
- Send warning to business partners - when a penetration attack is identified (successful or unsuccessful) provide notice partner organizations identifying the method used, source of the attack (as best it can be determined,) etc.
- Network operations is informed of a possible problem
    - Looking for an initial cause (change management (maintenance), an open ticket, or temporal surge has triggered the problem) → not our cause
- Security is notified of a possible problem

Response & Recovery (this could be simultaneous with the step above)

- Based on analysis of the event (events) determine appropriate courses of action:
    - If you find out the origins, contact the ISP to turn off that IP address
    - Shut down the port on the firewall or another network element (router, load balancer, etc. depending on network set-up)

4. Use Case 3: Application Abuse/Misuse

Use Case 3: Application Abuse/Misuse

4.1. Characteristic Information

Application abuse and misuse can be classified into two broad categories, those acts perpetrated by authorized personnel, insider threat, and those perpetrated by external personnel, external threat. In both cases, the critical concepts are defined in Sarbanes-Oxley Section 404 as well in other regulatory instruments and standards.

Insider threats are those acts where, although a person is an authorized user of the application, they are able to perform actions and access information that are an abuse or misuse of the application. This can be a function of the person's privileges not being defined with sufficient granularity or insufficient controls being in place to enforce the intended limits of the person's access privileges. One of the critical controls is known as "Restriction of Access" or "Least Privilege", which is the concept that a person's usage privileges should be the minimum required to achieve their role. This has proven a challenging criterion because as the role of an individual changes, their application privileges must change with it.

Many of the most grievous examples of application abuse have occurred where a person has retained privileges from former roles and indeed temporary roles, Although these privileges should have been revoked when the person's role changed, they were retained and were subsequently abused, for example to be both the actor and auditor of a transaction. This leads and must be considered in parallel with a second concept called "Separation of Duties", which requires that a person's privileges should not allow conflicts of interest or the avoidance of internal controls. This applies to both the transactional capabilities of the person's privileges but also a limitation on the information they may access and distribute. In many organizations, demarcations between what classes of information each person can access and distribute have profound commercial, national security or privacy implications and the taxonomy and classification of information become critical. However the classification and control of this information is reliant upon proper controls being in place within the application.

Where an application does not have proper controls in place, their potential exposure to external threat is significantly greater. There is an increased probability that information boundaries will not be properly defined and that there will be fewer controls on the actions of users of the application. External threat techniques known as "Privilege Acquisition" are where an external threat actor or group is able to gain access with very basic privileges to an application. The weaknesses in the internal controls of the application allow the external threat to increase the privileges of their access to the application and either gain more valuable information or even assume total administrative control of the application.

4.1.1. Application Abuse/Misuse Prevention

The prevention of abuse and misuse of applications is reliant upon the control of both information and restriction of access privileges. Restriction of access includes:

- Privileged users: Personnel who have a role in administering an application should not be able to use the same credentials to make use of the application and its information.

Where a person has a need to both manage and use an application, these two roles should require separate credentials. The actions of personnel with highly privileged roles should be subject of heightened scrutiny. This measure is known to both significantly limit internal threat but also significantly restricts privilege acquisition by external threat actors.

- Taxonomy and classification: The organization should prepare a clear taxonomy of its information and conduct an analysis of the value of this information. In particular, it must ensure that information is kept demarcated when its availability to a single person creates conflict of interest of or increased security risk.
- Restriction of Access: The access privileges of a person should be restricted to the minimum required for their function. When a person's role changes, their access privileges should be reviewed and those privileges not required for the new function should be revoked.
- Separation of Duties: All actions and information's that are identified as requiring audit or management should have an approval function that is separated from the initiator of the transaction. An individual should never have the ability to authorize their own transaction. An individual or team's function should not require access to information that has been identified as creating a potential conflict of interest or heightened security risk. An organization development exercise should be undertaken to divide and redesign roles to remove the potential conflict or risk.

Business Process (eTOM) Steps Involved

4.1.2. Application Abuse/Misuse Operations

The operational misuse and abuse of applications requires that both the usage of the application and the information that it accesses be actively monitored and also made the subject of regular review. Much of this operational activity requires effective planning in both the classification and categorization of information. These measures are critical because in order to detect misuse, the proper usage must first of all be clearly be understood, defined and agreed.

Business Process (eTOM) Steps Involved

Monitoring

- L3: Monitoring
    - *Proposed* L4: Monitor Systems
        - Access to the application must be recorded and any actions of persons while using the application must be auditable.
        - Audit logs should themselves be secured and a copied continuously to a location external to the application environment.
        - Monitoring should include whether information accessed during the application session is appropriate to the role and privileges of that person's role. Particular interest should be made of movement between information classification levels or between privilege levels during a user session.
        - The use of different user identities from the same point or similar points of origin may also be indicative of application abuse.
        - Virtual and cloud computing environments present particular challenges for both the management of users with administration privileges. Virtual environments

require particularly careful monitoring for external threat privilege acquisition techniques.

Analysis

- L3: Analysis
  - *Proposed* L4: Analyze Data (log records)
    - Analysis and audit records should include both the user identity that accesses the application and provide the ability to cross-reference record between identity and information.
  - *Proposed* L4: Preserve Forensic Data
    - Analysis should be possible for information in transit and also information in storage.

Detection

- L3: Detection
  - *Proposed* L4: Detect Anomalous Events
    - It should be possible to reconcile any mismatch between the privileges of the user identity and the classification of the transaction and information can be detected and alarms created to prevent its continuance.
    - Failed access attempts for an identity or information record should be able to be cross-referenced with successful attempts.
    - Detection should be correlated across multiple sources of information, as many sophisticated forms of external threat also tamper with detection methods. Externally measured indicators such as power and bandwidth should be considered.

Incident Management: The overarching process for incident management, including warning of component organizations, etc. as well as defining and executing appropriate response actions.

- L3: Incident Management
  - *Proposed* L4: Response & Recovery
    - Methods of authentication may need to be reset and in in dire circumstances, some or all users may be required to re-enroll before usage of the application and information can resume.
    - During an incident and in advance of forecast incidents, methods of authentication should be more stringent or access to the application suspended
    - Response should include the ability to increase authentication requirements in reaction to suspected attempts to inappropriately access the application or information.
    - During the response period some classes of user activity and access to more sensitive information may be rendered more difficult or be made unavailable.
    - Recovery should include analysis of whether the integrity of information has been compromised or if sensitive information has been inappropriately distributed.

5. Administrative Appendix

5.1. About this document

This document is an Application Note, aiming to document an approach based on industry experience that can be used by a company and adapted to its business needs.

Note that it repackages the content from the Security Management project/team within TM Forum, and published as Technical Report TR173 "Security Management Use Cases."

5.2. Document History

5.2.1. Version History

Version Number	Date Modified	Modified by:	Description of changes
12.0	Mar 2012	Mike Kelly	Document launch – repackaging of TR173 from Security Management as Business Process Framework Application Note
12.1	Mar 2012	Mike Kelly	Addition of a further Use Case provided in the updated TR173 from Security Management
12.2	Apr 2012	Alicja Kawecki	Minor formatting, cosmetic corrections prior to posting for Member Evaluation

5.2.2. Release History

Release Number	Date Modified	Modified by:	Description of changes
12.0	Mar 2012	Mike Kelly	Document launch - repackaging of TR173 from Security

			Management as Business Process Framework Application Note

5.1. Acknowledgments

This document reproduces use cases documented in TR173 “Security Management Use Cases, Business Process Framework (eTOM) Mapping”. Please see that document for acknowledgements on the work.