

IT Infrastructure  
Threat Modeling Guide

Release 1.0

Published: June 2009

For the latest information, please see   
[microsoft.com/technet/**SolutionAccelerators**](http://microsoft.com/technet/SolutionAccelerators)

Copyright © 2009 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, ActiveSync, Excel, Microsoft Press, MSDN, SharePoint, Windows, and Windows Mobile are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Overview 1](#_Toc231897051)

[Definition 2](#_Toc231897052)

[Purpose of this Guide 2](#_Toc231897053)

[Who Should Read this Guide 3](#_Toc231897054)

[Microsoft Operations Framework 4.0 3](#_Toc231897055)

[How to Use this Guide 4](#_Toc231897056)

[Preparing an IT Infrastructure Threat Model 5](#_Toc231897057)

[Chapter Summaries 5](#_Toc231897058)

[Support and Feedback 6](#_Toc231897059)

[Acknowledgments 6](#_Toc231897060)

[Chapter 1: IT Infrastructure Components 9](#_Toc231897061)

[Vision 9](#_Toc231897062)

[Use Scenarios 9](#_Toc231897063)

[Model the Component 10](#_Toc231897064)

[Data Flow 10](#_Toc231897065)

[Entry Points 11](#_Toc231897066)

[Trust Boundaries and Levels 11](#_Toc231897067)

[Protected Resources 11](#_Toc231897068)

[Identify Threats 12](#_Toc231897069)

[Mitigate Threats 14](#_Toc231897070)

[Threat Prioritization 15](#_Toc231897071)

[Validate 17](#_Toc231897072)

[Dependencies 17](#_Toc231897073)

[Implementation Assumptions 18](#_Toc231897074)

[Summary 18](#_Toc231897075)

[Chapter 2: The IT Infrastructure Threat Model Profile 19](#_Toc231897076)

[Add Component Threat Model Information to the Portfolio 19](#_Toc231897077)

[Prioritize Components 19](#_Toc231897078)

[Chapter 3: Applied Example – The Threat Modeling Process 21](#_Toc231897079)

[Vision 22](#_Toc231897080)

[Model the Component 22](#_Toc231897081)

[Entry Points 25](#_Toc231897082)

[Trust Boundaries and Levels 25](#_Toc231897083)

[Protected Resources 25](#_Toc231897084)

[Identify Threats 26](#_Toc231897085)

[Mitigate Threats 27](#_Toc231897086)

[Threat Prioritization 28](#_Toc231897087)

[Validate 29](#_Toc231897088)

[Summary 30](#_Toc231897089)

Overview

The threat modeling process for commercial software and Web applications has been widely discussed and is reasonably well understood, but little documentation exists for evaluating potential threats to IT infrastructure. The *IT Infrastructure Threat Modeling Guide* describes and considers the extensive methodology that exists for Security Development Lifecycle (SDL) threat modeling and uses it to establish a threat modeling process for IT infrastructure.

[Steve Lipner](http://blogs.msdn.com/sdl/pages/about-us.aspx#steve), Senior Director of Security Engineering Strategy at Microsoft, describes threat modeling as follows:

"At Microsoft we’ve made threat modeling a fundamental component of the Security Development Lifecycle—our process for improving the security of the software and services we develop. But threat modeling is a general approach to identifying the ways that the security of any system might fail and then identifying measures for preventing or mitigating those failures. The application of threat modeling to IT infrastructure is a natural extension of the concept, and this guide is a great resource for organizations that wish to improve the security of their IT systems."

For more information about SDL, see [Investigating the Security Development Lifecycle at Microsoft](http://download.microsoft.com/download/B/4/D/B4D74C4C-DE31-4536-84ED-BEAB135C6DB6/SDL%20Series%20-%201.pdf) (pdf) or [*The Security Development Lifecycle*](http://www.microsoft.com/learning/en/us/books/8753.aspx).

Why should you consider threat modeling for your IT infrastructure? The most important reasons include the viability and reputation of your organization. The consequences of a successful cyberattack would almost certainly affect your organization's ability to conduct its day-to-day business operations. Also, if such an attack exposed confidential information, your organization could be perceived as one that failed to do what was necessary to protect itself, which could affect its ability to conduct business in the future. In addition, failure to protect customer information could subject you and your organization to legal liabilities and potentially significant fines.

Threat modeling allows you to determine what threats exist that could affect your organization's IT infrastructure, helps you identify threat mitigations to protect resources and sensitive information, and helps you prioritize the identified threats so that you can manage your security efforts in a proactive manner.

Threat modeling for your IT infrastructure should immediately follow a well-conducted risk assessment that is fully supported by management. "Chapter 4: Assessing Risk" in the Microsoft® [*Security Risk Management Guide*](http://go.microsoft.com/fwlink/?linkid=30794) provides an excellent overview of the risk assessment phase, including planning, data gathering, and risk prioritization. Your output from this phase should be a detailed analysis and a list of significant risks that a team can use to make the appropriate business decisions. After you complete the first threat model for your IT infrastructure, you might find the information in "Chapter 6: Implementing Controls and Measuring Program Effectiveness" of the *Security Risk Management Guide* to be helpful.

# Definition

IT infrastructure threat modeling is the practice of considering what attacks might be attempted against the different components in an IT infrastructure. Generally, threat modeling assumes the following conditions:

* Organizations have resources (in this case, IT components) that they wish to protect.
* All resources are likely to exhibit some vulnerabilities.
* People might exploit these vulnerabilities to cause damage or gain unauthorized access to information.
* Properly applied security countermeasures help mitigate threats that exist because of vulnerabilities.

The IT infrastructure threat modeling process is a systematic analysis of an organization’s IT components that compiles component information into profiles. The goal of the process is to develop a threat model portfolio, which is a collection of component profiles.

# Purpose of this Guide

**Provide an easy-to-understand method that enables IT professionals to develop threat models for their environments and prioritize their investments in IT infrastructure security.**

IT infrastructure threat modeling should be incorporated into an organization's IT mindset as a matter of policy, much like any other part of the validation, implementation, and installation process. Threat modeling in the name of secure infrastructure should be performed throughout the technology implementation process, much like any other component that is measured for performance, usability, and availability.

The three pillars of IT security are confidentiality, integrity, and availability (CIA). One way to establish these pillars as a basis for threat modeling your IT infrastructure is through Microsoft Operations Framework (MOF) 4.0, a framework that provides practical guidance for managing IT practices and activities throughout the entire IT lifecycle.

The [Reliability Service Management Function (SMF)](http://technet.microsoft.com/en-us/library/cc506069.aspx) in the Plan Phase of MOF addresses creating plans for confidentiality, integrity, availability, continuity, and capacity, The [Policy SMF](http://technet.microsoft.com/en-us/library/cc543348.aspx) in the Plan Phase provides context to help understand the reasons for policies, their creation, validation, and enforcement, and includes processes to communicate policy, incorporate feedback, and help IT maintain compliance with directives. The Deliver Phase contains several SMFs that help ensure that project planning, solution building, and the final release of the solution are accomplished in ways that fulfill requirements and create a solution that is fully supportable and maintainable when operating in production.

Start the IT infrastructure threat modeling process from the onset of any new technology project, because doing so might reveal weaknesses in your architecture or implementation and design planning that could require significant changes to the project. Design changes early in the implementation process are significantly less expensive than a complete reimplementation after a failed attempt that wasn't well planned, or if an insufficiently secured system achieves production status.

Consider engaging in an IT infrastructure threat model portfolio review process annually, even if no major changes are made to the organization's IT infrastructure. Because threats and risks are dynamic, your threat modeling efforts should be as well. Attackers won’t stop their attempts to exploit vulnerabilities, and your efforts to mitigate potential threats will help make compromise less likely. The IT infrastructure threat modeling process might also improve an organization's audit profile by showing that the process is consistently practiced. In addition, mitigations achieved during the threat modeling process might prevent the need to undertake the same effort in the high-pressure spotlight of an audit and its potential mandates.

The practice of threat modeling can be woven into the fabric of most ongoing IT infrastructure use scenarios. Consider involving administrators, engineers, architects, and project managers, preferably with managerial support as well. Project manager assistance can be especially helpful for focusing on the security aspects of each use scenario.

# Who Should Read this Guide

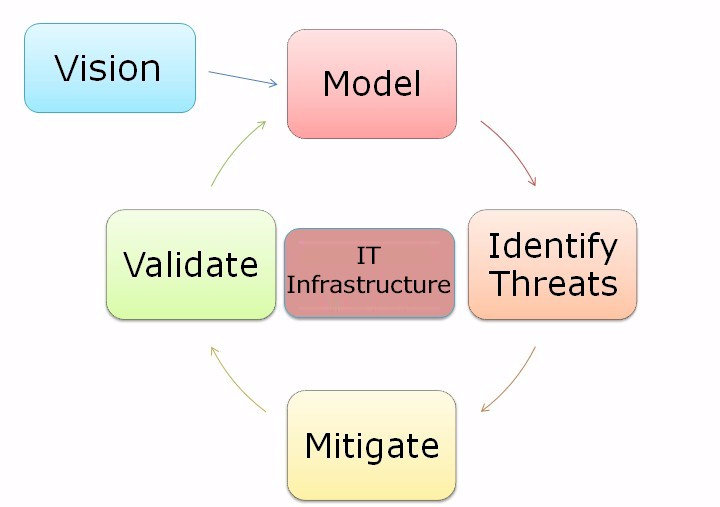
This guide is written for IT professionals, including administrators, analysts, architects, engineers, and managers who are responsible for the protection of specific critical resources for their organizations. It is meant for use by IT professionals who handle all aspects of IT for their organizations as well as IT professionals who have specific security-related duties as part of a much larger IT staff.

In addition, this guide is intended to be transparent to roles and applicable to all who wish to undertake the IT infrastructure threat modeling process.

# Microsoft Operations Framework 4.0

The *IT Infrastructure Threat Modeling Guide* is related to a series of materials for the cost effective management of IT services. As referenced earlier in the "Purpose of this Guide" section, this guide is related to the Plan and Deliver Phases of MOF 4.0. For more information about MOF and other helpful materials, visit the [Microsoft Operations Framework](http://go.microsoft.com/fwlink/?LinkId=130522) page on Microsoft TechNet.

# How to Use this Guide



A good threat model typically includes good documentation, including a defined process to help ensure that you avoid common pitfalls such as scope creep (a project management term for uncontrolled or poorly managed changes). Consider the following steps to frame the process:

1. **Establish a Vision**. Document what purpose or function the component provides to the organization. It is important to obtain as many perspectives as possible, so you should solicit input from anyone in the organization who has knowledge of the component.
2. **Model, or Create a Diagram**.The diagram should include processes, data stores, data flows, and trust boundaries that separate the components from each other and from external entities.The goal of the model (diagram) is to facilitate focused discussion by detailing just those parts of an IT infrastructure component that are relevant to the threat modeling process.
3. **Identify Threats**.For each component, consider what threats it faces. Use a malicious mindset from the perspective of an untrusted outsider as well as that of a trusted user. This guidance will map parts of the Microsoft STRIDE threat model approach to the security concepts of confidentiality, integrity, and availability as a way to provide a useful framework you can use to assess exploitability. For more information about STRIDE, see [Uncover Security Design Flaws Using the STRIDE Approach](http://msdn.microsoft.com/en-us/magazine/cc163519.aspx) on MSDN® (the Microsoft Developer Network).

STRIDE is an acronym for

* **S**poofing identity
* **T**ampering with data
* **R**epudiation
* **I**nformation disclosure
* **D**enial of service
* **E**levation of privilege

1. **Mitigate Threats**.Mitigation and prevention are key in this step. How and when will the infrastructure weakness be resolved? Part of this process should include determining your priorities—for example, addressing the most severe threats with the appropriate mitigation(s) first. Base this effort on both the likelihood of a threat being exploited and the potential impact of such an exploit on your infrastructure. The guidance focuses on a model of prioritization that follows a **High**, **Medium**, **Low** standard to avoid complexity.
2. **Validate**.It is essential that you validate the model, the threats list, the mitigations and their priorities, as well as all dependencies and assumptions.

This five-step process should be viewed as an ongoing cycle that is fueled by the purpose stated earlier in the guide—to establish a threat modeling process.

## Preparing an IT Infrastructure Threat Model

Each infrastructure *component* that is considered during the threat modeling process is documented separately in a *profile*. The threat modeling process results in an *IT infrastructure threat model portfolio*, which is a collection or repository of all the individual profiles.

The applied example in Chapter 3 of this guide makes use of the [SDL Threat Modeling Tool](http://msdn.microsoft.com/en-us/security/dd206731.aspx), whose output can be used to populate the profiles and resulting portfolio.

# Chapter Summaries

The IT Infrastructure Threat Modeling Guide consists of this Overview and three chapters. Brief descriptions follow for each chapter.

Overview

The Overview states the purpose and scope of the guide, defines the guide audience, and describes the guide's structure to help you locate the information that is relevant to you. It also describes the user prerequisites for the guidance.

Chapter 1: IT Infrastructure Components

This chapter focuses on understanding the details of the components that the IT infrastructure threat modeling process will consider, including diagramming, identifying threats, mitigating threats, and validating all the information that is acquired during the process. The chapter discusses use scenarios, dependencies, implementation assumptions, entry points, and trust levels.

Chapter 2: The IT Infrastructure Threat Model Portfolio

This chapter describes how to populate the IT infrastructure threat model portfolio with relevant data about your components. The chapter includes information about prioritization and is essential for helping you mitigate threats with the greatest potential impact to your organization.

Chapter 3: Applied Example – The Threat Modeling Process

This chapter uses a fictitious organization's communications system as an example for the IT infrastructure threat modeling process. The rapid introduction of mobile devices into IT infrastructure could make such a system an ideal target for an attacker. You can use the SDL Threat Modeling Tool as described in this guide or another of your own choosing.

## Support and Feedback

The Solution Accelerators – Security and Compliance (SA-SC) team would appreciate your thoughts about this and other Solution Accelerators. Please contribute comments and feedback to [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=IT%20Infrastructure%20Threat%20Modeling%20Guide). We look forward to hearing from you.

Solution Accelerators provide prescriptive guidance and automation for cross-product integration. They present proven tools and content to help you plan, build, deploy, and operate information technology with confidence. To view the extensive range of Solution Accelerators and for additional information, visit the [Solution Accelerators](http://go.microsoft.com/fwlink/?LinkId=51571) page on Microsoft TechNet.

We would appreciate your taking a few moments to complete this [short survey](http://go.microsoft.com/fwlink/?LinkID=132579). Doing so will help us continue to improve the quality of Solution Accelerators and ensure that they address customer needs. Thank you in advance for completing the survey, and thank you for purchasing Microsoft products.

# Acknowledgments

The Solution Accelerators – Security and Compliance (SA-SC) team would like to acknowledge and thank the team that produced the IT Infrastructure Threat Modeling Guide. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Development Team

**Author**

Russ McRee

Contributors

Adam Shostack

Blake Frantz *Center for Internet Security*

Chase Carpenter

Steve Lipner

Developers

José Maldonado

Jeff Sigman

Editor

Steve Wacker *Wadeware LLC*

Product Manager

Shruti Kala

Program Manager

Kelly Hengesteg

Release Managers

Karina Larson

Shealagh Whittle *Aquent LLC*

Test Manager

Sumit Parikh

Tester

Bhavana Nema *Infosys Technologies Ltd*

Reviewers

Bob Fish

Don Lemmex

Doug Cavit

Enrique Saggese

Ernie Hayden

Joe Coulombe

John Steer

Kai Axford

Karen Scarfone *National Institute of Standards and Technology*

Kathy Lambert

Keith Pawson

Ray Pompon

Tony Noblett *Socair Solutions*

Chapter 1: IT Infrastructure Components

In this guidance, an IT infrastructure *component* is a single piece in the larger organizational IT puzzle. As shown in the process diagram in the Overview, you will identify threats to components, mitigate them, and validate your work during the IT infrastructure threat modeling process.

As you work through the process, you will populate a *threat model portfolio* with component *profiles* that contain information about network devices, servers, monitoring systems, and so on. This chapter will help you understand the different steps of the process.

# Vision

A clear vision should be developed for each IT infrastructure component that encompasses use cases, or what can be described as *use scenarios*. Developing such a vision should include as many relevant people as possible to ensure all perspectives are considered, and a security mindset should be applied to all of the perspectives.

As you create a vision for each infrastructure component, ask yourself questions such as “Where will the component be used?” or “What does the customer expect?” Additional considerations can include *assurances*, which are ways to express security goals as simple, positive statements that can be tested to help qualify a component's security status. For example “Only administrator can read this file” or “All data stored on mobile devices is encrypted.”

Security can also be considered a *feature property*. It is worthwhile to consider the security expectations your users have for the different features of components that you are threat modeling.

## Use Scenarios

As you document the pertinent details of the components for evaluation during the IT infrastructure threat modeling process, you should consider the *use scenarios* for the components. For example, consider how the following assertions relate to the various components:

* Our load balancer is essential because it manages all requests for our online products and ensures constant uptime and availability.
* Our Web proxy keeps employees productive, protects us from hostile workplace litigation, and prevents malware outbreaks.
* Our intrusion prevention system prevents external intrusion attempts and responds when attacks are attempted.
* Our e-mail system is the lifeblood of our organization because it manages communication among employees, customers, and partners.

These assertions, which are likely relevant to your vision, are important aspects of use scenarios.

The goal is to enumerate actions, actors, and resources for all use scenarios that are associated with in-scope IT components. You can prioritize use scenario generation by an IT component's criticality and any service level agreements (SLAs) that might be associated with the component.

For documentation and organizational purposes, each of the following use scenarios includes an alphanumeric prefix. Load balancer scenarios use LB followed by a sequential number; Web proxy scenarios use WP, and so on.

* **LB.1**. The load balancer helps external customers reach an available Web server.
* **LB.2**. The load balancer helps IT administrators manage the organization's Web presence.
* **WP.1**. The Web proxy prevents internal users (including employees and contractors) from accidentally visiting inappropriate sites or creating a hostile work environment by displaying inappropriate content on their screens.

Use scenarios help define the data flows, entry points, attack surfaces, and resources that should be included as part of the model. These aspects are critical for threat modeling components that are part of a larger service.

# Model the Component

During the IT infrastructure threat modeling process, diagrams help you gather information and develop threat models for different components.

## Data Flow

Data flow diagrams are essential to threat modeling during the software and application development process, and are no less important when creating a threat model for IT infrastructure.

Each diagram should include background information as well as a detailed, security-oriented description of the component. Details should include descriptions of the component's *entry points*, many of which could be potential attack vectors. In addition, the associated *trust boundaries* and each *protected resource* should be documented. It is equally important to document the actual data flow as it passes through entry points and past trust boundaries on the way to a resource. More information is provided about these terms in the following subsections.

Consider the example shown in the following data flow diagram, which identifies entry points, trust boundaries, and protected resources. Note how an accurate diagram helps identify the entry points and trust boundaries.

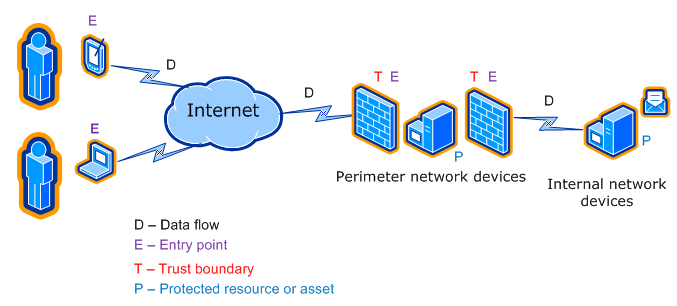
****

Figure 1.1. Data flow diagram with elements

## Entry Points

Entry points are those portions of data flows that cross a trust boundary. Because entry points present attack opportunities, they should receive careful attention. An IT infrastructure component's entry points include interfaces with other software, hardware, and users. If a component transmits data or receives data from an external resource in any way, consider it an entry point.

Consider the following partial list of entry points to a customer database server:

* Direct access at the console.
* Open Database Connectivity (ODBC) calls from an intranet sales application and an extranet partner application.
* Ports 1433 and 1434, which are exposed to the internal network.
* The database and transaction logs.

Although not complete, the purpose of this list is to encourage you to think about all the entry points to a database server. Don’t forget to include considerations for management methodology at both the software and host layers.

## Trust Boundaries and Levels

Trust boundaries are borders between realms, such as domains or networks. A common example of a trust boundary in an IT infrastructure is a firewall. Trust boundaries are attack surfaces, and construed broadly can include networks and devices of all types.

Consider the likelihood that items on either side of a trust boundary are either at different trust levels or are mutually distrustful. Also, consider how trust levels apply to each entry point and trust boundary for the component being reviewed during the IT infrastructure threat modeling process.

After you identify all the entry points to your component, label each one with a trust level that indicates the degree to which the entry point can be trusted to send or receive data. Note that trust levels apply to both people and devices.

Typically, there are three fundamental trust levels to consider:

* **Administrator**. Local or domain administrators have complete control over the component.
* **Untrusted**. The component is subject to external data files, network connections, or other potentially malicious input.
* **Trusted**. The component is subject to interactive users and any settings they might associate with the component (but not administrative users).

## Protected Resources

Protected resources are components or component aspects whose protection is critical, and might include protected assets that an attacker has reason to steal or copy. The Microsoft [*Security Risk Management Guide*](http://go.microsoft.com/fwlink/?linkid=30794) defines assets as anything of value to the organization.

An attacker’s motives might include the theft, modification, and/or disruption of a component to cause harm or gain a profit. Protected resources include:

* Customer databases
* Security Accounts Manager
* Contents of memory
* An organization's network connectivity

Each component should list the trust levels that are required to gain access to protected resources or assets.

# Identify Threats

Component threat acquisition is one of the most important steps in the IT infrastructure threat modeling process, and your perspective should be that of an attacker. To complete this step you should seek to answer the following question: What are all the possible threats a specific component is exposed to and how severe are those threats?

Consider facilitating a discussion that is open to feedback from as many people as you can involve, including administrators, analysts, architects, engineers, and managers. Someone else might have a significant perspective to offer about a specific component.

The Microsoft STRIDE threat model approach considers the following threats:

* **Spoofing**. An attacker pretends to be someone (or something) else.
* **Tampering**. An attacker changes data while in transit or at rest.
* **Repudiation**. An attacker performs an action that cannot be traced back to them.
* **Information Disclosure**. An attacker steals data while it is in transit or at rest.
* **Denial of Service**. An attacker interrupts the legitimate operation of a system.
* **Elevation of Privilege**. An attacker performs actions they are not authorized to perform.

Confidentiality, integrity, and availability (CIA) are foundational security considerations. In principle, CIA might also include authorization and non-repudiation. The following table shows how STRIDE and CIA align for the purposes of the IT infrastructure threat modeling process.

Table 1.1. STRIDE and CIA Alignment

| **Threat** | **Property** | **Definition** | **Example** |
| --- | --- | --- | --- |
| Spoofing | Authentication | Impersonating something or someone else | Pretending to be the CEO, or microsoft.com, or ntdll.dll |
| Tampering | Integrity | Modifying data or code | Modifying a DLL on disk or DVD, or a packet as it traverses a LAN |
| Repudiation | Non-repudiation | Claiming to have not performed an action | "I didn't send that e-mail." "I didn't modify that file." I *certainly* didn't visit that Web site!" |
| Information disclosure | Confidentiality | Exposing information to someone not authorized to see it | Allowing someone to read the Windows® source code; Publishing a list of customers to a Web site |
| Denial of service | Availability | Denying or degrading service to users | Crashing Windows or a Web site; Sending a packet and absorbing seconds of CPU time; Routing packets into a black hole |
| Elevation of privilege | Authorization | Gaining capabilities without proper authorization | Allowing a remote Internet user to run commands; Finding a way to run administrative commands despite being a limited user |

When you look for threats, realize that they can cluster on certain types of elements such as external entities, processes, data stores, and data flows. Processes include all running code. Data flows include all data that flows between processes and anything else, on host or off. Data stores include files, databases, and registries. External entities are anything outside the control of the system, such as people or Web sites.

The Microsoft SDL threat modeling process uses the following chart to help structure diagram analysis. The chart illustrates how different threats affect each type of element.

Table 1.2. SDL Elements and STRIDE

| **Element** | **S** | **T** | **R** | **I** | **D** | **E** |
| --- | --- | --- | --- | --- | --- | --- |
| C:\Documents and Settings\v-stewac\Local Settings\Temporary Internet Files\Content.Word\ExternalEntity.png | X |  | X |  |  |  |
| C:\Documents and Settings\v-stewac\Local Settings\Temporary Internet Files\Content.Word\Process.png | X | X | X | X | X | X |
| C:\Documents and Settings\v-stewac\Local Settings\Temporary Internet Files\Content.Word\DataStore.png |  | X | X | X | X |  |
| C:\Documents and Settings\v-stewac\Local Settings\Temporary Internet Files\Content.Word\DataFlow.png |  | X |  | X | X |  |

Chapter 22 of [*The Security Development Lifecycle*](http://www.microsoft.com/learning/en/us/books/8753.aspx) by Michael Howard and Steve Lipner (Microsoft Press®, 2006) discusses *threat trees* that were developed for STRIDE threats against each of the four standard SDL elements.

Threat trees are diagrams that show a hierarchy of threats or vulnerabilities to indicate the steps a malicious user would take to mount an attack. A portion of a sample threat tree (for only a single threat) is shown in the following figure. The ultimate goal of the attack is at the top of the tree. The "Finding Manifestations of Threats" section in the MSDN® article [Uncover Security Design Flaws Using The STRIDE Approach](http://msdn.microsoft.com/en-us/magazine/cc163519.aspx) is also a valuable threat tree resource.

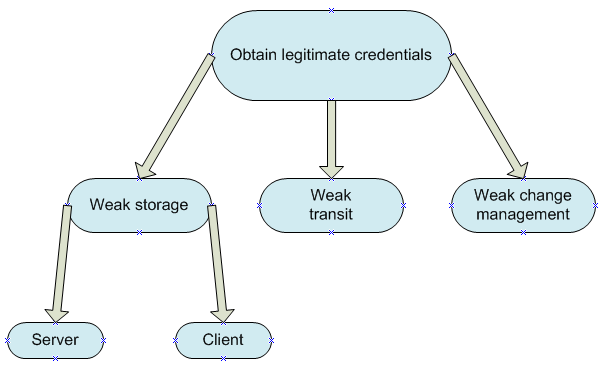
****

Figure 1.2. Portion of a sample threat tree for a spoofing attack

For example, a threat tree can explore how tampering might manifest itself against a data flow in a general sense. The leaf nodes on the threat trees suggest attacks that will realize the threat, and you can use these leaf nodes as leading questions to enhance discussion around threat enumeration. You might discover that a threat can be mitigated closer to the top of the threat tree.

When you look at a data flow, consider the ways it can be tampered with, how the information it contains could be disclosed, or how someone could deny service to it. The preceding chart works for Microsoft, and can work as a starting point for you. Microsoft has a separate privacy analysis within the Security Development Lifecycle, and so there is no check for “information disclosure by external entities,” which is a good description of some, but not all, privacy issues.

# Mitigate Threats

After you create a data flow for the component you’re modeling and compile a list of all the possible ways to attack it, you need to consider each threat and determine what steps will mitigate the threat.

Typically, threats will belong to one of the following five categories:

* **Not mitigated and requires mitigation**. No existing component or dependency provides any mitigation and the component is therefore at risk. Your prioritization process should obviously rank components that are affected by this threat category as your most immediate concerns and assign them a High priority rating. (The following "Threat Prioritization" section provides additional information about how to prioritize threats,)

*Example: This component is most at risk because it has no features to aid in mitigation, and no other component offers it any protection. Immediate mitigation required.*

* **Not mitigated, but is the responsibility of a dependency or other component**. Threats to components in this category will be mitigated by another dependency or component. For example, a threat in this category could be mitigated by another component, such as a firewall that is not yet installed or configured. However, although the dependency or component that provides mitigation might not be your responsibility, it is vital that you track implementation progress to its completion.

*Example: After it is installed, the Web application firewall (WAF) will mitigate the threats to this component.*

* Already mitigated by the component. What inherent functionality in a component might mitigate a specific threat? Can this functionality be invoked by a simple configuration change or is a significant upgrade required?

*Example: The component includes features to throttle bandwidth and block malicious IP addresses.*

* **Already mitigated by a dependency or other component**. What additional component might provide appropriate protection for the component that is currently being threat modeled? An example might be as simple as a Web server protected by a Web application firewall or a load balancer and configured as follows:

*Example: All requests for HTTP content served by Server A traverses our Web application firewall, all other traffic to Server A is denied.*

* **Not mitigated, but does not require mitigation**. This category consists of threats identified for a specific component, but because the component is considered relatively insignificant it does not require mitigation. For example, such a component might be a test or development resource that houses or traffics only test data with no connectivity to a production environment. The important question is: If this component is fully compromised, what additional damage can the attacker cause?

*Example: Layered defenses up the threat tree sufficiently protect this component so that its few minor vulnerabilities do not require mitigation.*

You might determine that additional categories are appropriate for your IT infrastructure or business model. The suggested categories are designed to help you implement the IT infrastructure threat modeling process; allow yourself the flexibility to adjust them as needed to suit your environment. Risk acceptance plays a role when mitigating threats. For example, your organization could determine that certain threats will remain unmitigated. Ensure that you clearly document this decision, because it might be subject to reconsideration in the future. Consider all these assumptions very carefully if you choose to accept unmitigated threats for any component.

Controls are often used to mitigate threats, both preventative and detective controls. Such controls might include policies, configuration changes, encryption, or event monitoring.

## Threat Prioritization

This guide discusses threat prioritization in two distinct ways. This chapter focuses on the need to appropriately prioritize each threat as it pertains to the component (also known as *resource*). This guide assumes that you understand the component’s significance to the organization.

For additional threat prioritization insights, see the *Security Risk Management Guide*, especially the risk prioritization discussion in Chapter 4.

The following figure is designed to help you visualize the analytical process for threat prioritization.

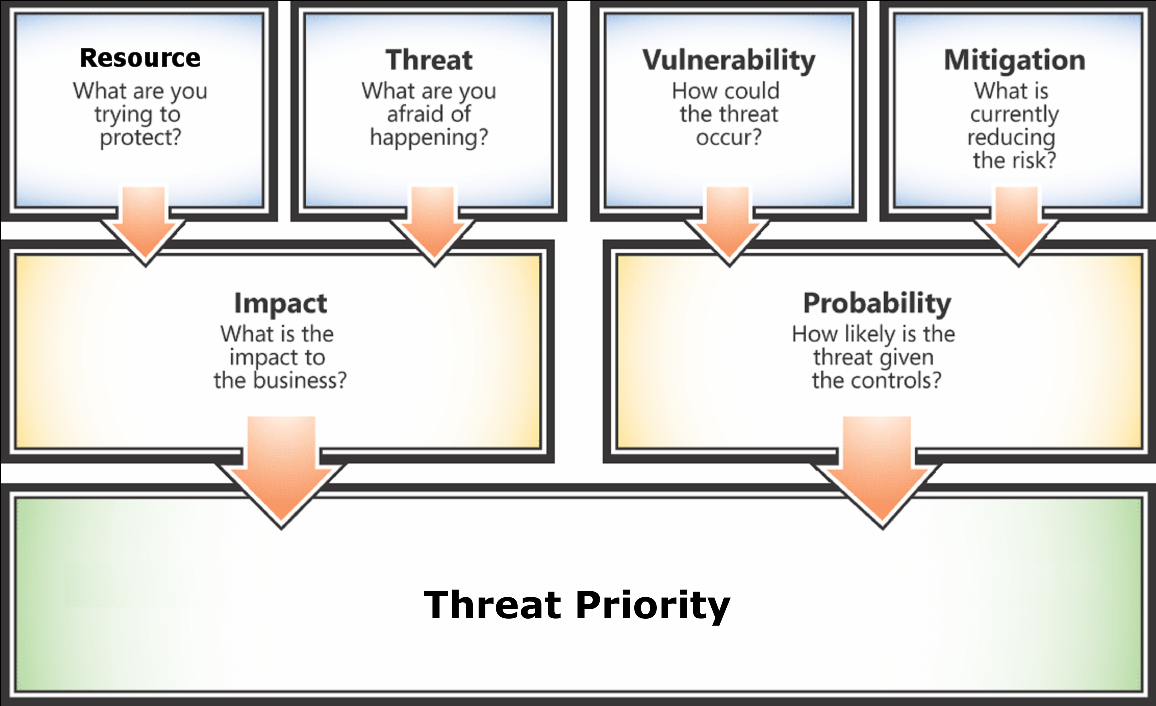
****

Figure 1.3. Threat prioritization process

As part of this process, you analyze resources and any threats to those resources to determine what the impact of a realized threat might be. Vulnerabilities and any related mitigations can help you determine the probability of a threat being exploited to the detriment of your organization.

Consider the following threat prioritization process example:

**Resource** A human resources application that includes employee PII (personally identifiable information). This application is made accessible by the Internet and is protected only by SSL and a username/password authentication scheme.

**Threat**. A successful attack could cause employee PII to be stolen or exposed.

**Impact**. The impact to the organization would be significant, resulting in probable litigation and employee dissatisfaction.

**Vulnerability**. Weak user credentials could be guessed by conducting a brute force attack against the authentication scheme.

**Mitigation**. No mitigations currently exist to protect the human resources application from brute force attacks.

**Probability**. Considering the lack of current mitigations and the high success rate for dictionary (brute force) attacks against weak user credentials, the probability of this threat being realized is high.

**Threat priority**. The threat prioritization process determines that the threat priority rating should be High. You can use the Detailed Level Risk Prioritization tool in the [*Security Risk Management Guide*](http://go.microsoft.com/fwlink/?linkid=30794) to help establish a consistent threat prioritization process.

In Chapter 2, the discussion is about how to appropriately prioritize each component based on its perceived threats. The priority rating for each component can then be used to calculate an overall threat posture that pertains to the threat model portfolio (the collection of threat models). The priority rating will also help you focus first on the components that are exposed to the most serious threats.

Regardless of whether the priority rating is applied to a threat or a component, this guide uses the following priority ratings:

* **High**. A High priority rating means that the organization has a considerable risk exposure, that threats urgently need mitigation, and that mitigation should be immediate. Components that are subject to clear and present danger because of exposed or actionable threats should be assigned a priority rating of High.
* **Medium**. A Medium priority rating means that the organization has a moderate risk exposure. Components that are subject to possible danger or potential harm but might soon be mitigated by a dependency or another component could qualify for the Medium ranking. Mitigation is needed as soon as possible.
* **Low**. Low priority ratings are for relatively minor threats that you intend to mitigate but that do not warrant High or Medium ratings. Threats with a Low priority rating have relatively low risk exposure to the organization. Mitigation should be scheduled so as not to disrupt normal business operations.

Creating an overall component priority rating by determining the median of all identified threats per component can be useful from a portfolio perspective (see Chapter 2), but High priority threats should always take precedence.

Components with a combined High priority rating should obviously take mitigation precedence. For example, if a component is subject to five threats—one High, three Medium, and one Low—the overall component threat priority rating would be Medium.

Conversely, if a component is subject to five threats—three High, one Medium, and one Low—the overall component threat priority rating would be High.

These distinctions are important in Chapter 2, which is designed to help you decide which components require mitigation first. From a service perspective, you could mitigate all High priority threats across all service components.

It's important at this phase to discern and address High priority threats first. Ten Low priority threats should not take precedence over two High priority threats.

# Validate

The validation process should include stringent review of steps taken so far. In addition to reviewing the model, the threats list, the mitigations, and their priorities, also review all dependencies and assumptions. We strongly suggest that the validation process include third-party perspectives, such as those of auditors and risk managers.

Be sure to analyze the effectiveness of mitigations as well.

## Dependencies

For the purposes of IT infrastructure threat modeling, a dependency is defined as the degree to which a component relies on other components. In keeping with Microsoft SDL threat modeling practices, it is important to consider how a failure in a dependency could lead to a security-related incident in your IT infrastructure.

To create an effective threat model, it's important to consider dependencies as you document the components in your IT infrastructure. Ask yourself what kind of impact a successful attack against a specific component might have. Consider the following example questions:

* If our firewall fails, what infrastructure is no longer protected?
* What does it mean to the organization's reputation if an attacker compromises our human resources system and obtains employee PII?
* If we experience a distributed denial-of-service (DDoS) attack, will our load balancer suppress the traffic appropriately or will the Web servers have to absorb the load?
* What does it mean to the organization's productivity if our e-mail server is damaged or compromised?

It's essential that you understand your data flows and network architecture when considering dependencies. Also, give due consideration to Defense in Depth, an essential concept that relates to enhanced security posture. For more information, see [Understanding Defense in Depth](http://technet.microsoft.com/en-us/library/dd365117.aspx) on Microsoft TechNet.

## Implementation Assumptions

Implementation assumptions are those you might make during the implementation / installation phase for a given component. It is very important to document these assumptions as well for verification purposes if their validity is questioned later. A quick review of the following sample assumptions will help you understand why they are important:

* This router will only handle internal traffic that is destined for the data store that holds credit card information.
* There is no need to encrypt any data on this file server because no one will ever store confidential data on it.
* This firewall will block all traffic except traffic destined for port 80 or 443.
* The vendor will keep all the signatures on our IPS current and our contract defines “current” in a way that is in agreement with our SLA.

# Summary

For each component you should have compiled the following information:

* Vision
* Goals and use scenarios
* Model (Diagram) of the Component
* Entry points
* Trust levels
* Protected resources
* Dataflow
* Identified Threats
* STRIDE and CIA alignment
* Mitigated Threats
* Not mitigated and requires mitigation
* Not mitigated, but is the responsibility of a dependency or other component
* Already mitigated by the component
* Already mitigated by a dependency or other component
* Not mitigated, but does not require mitigation
* Prioritized Threats
* Validation
* Dependencies
* Implementation assumptions

Chapter 2: The IT Infrastructure Threat Model Profile

After you complete threat models for each component, organize the results into a *threat model portfolio*. It's very important to ensure proper prioritization of all component threat model results. A complete threat model portfolio lists all components that have been analyzed by the threat modeling process, preferably ranked by priority.

The portfolio summary should be an uncluttered, easy-to-read reference with an executive summary that describes your IT infrastructure threat posture. The portfolio summary will provide the needed detail if you properly complete each of the IT component threat models.

When you start the threat modeling process you might quickly realize that completing a threat model portfolio is more daunting than you expected. Some organizations start by focusing their efforts to ensure the security of those IT components that are most at risk and that are especially important to their business. This guide can help you evaluate both considerations and also to understand the importance of developing and perpetuating a threat modeling mindset within your organization.

Many good reasons exist for developing and maintaining a threat model portfolio. For example, such a portfolio can be an extremely useful knowledge base during security incidents. Also, a threat model portfolio contributes to better change management practices by providing pertinent documentation about changes made for threat mitigation purposes. In addition, such a portfolio can be a valuable reference during audits.

Organizational preferences are certainly subjective. Should your organization decide to threat model a number of components that make up a larger service, such as Secure Sockets Layer virtual private networking (SSL VPN) for home workers, it might make sense to maintain a threat model portfolio that is specific to that service.

The key consideration is this: a threat model portfolio helps you keep threat model information organized and useful in a manner that is conducive to enhancing your organization’s security posture.

# Add Component Threat Model Information to the Portfolio

Devise a system for organizing your threat model findings that is appropriate for your organization. For example, Microsoft® SharePoint® or some other collaborative Wiki is useful for storing component threat models, as well as for summarizing findings. At a minimum, Microsoft Excel® can provide a basic working structure, with each component threat model added as a worksheet to an overall portfolio workbook.

Reports exported from the SDL Threat Modeling Tool are in .MHT or .HTM/.HTML formats and will integrate well with SharePoint or other collaboration tools and services.

# Prioritize Components

The final prioritization process is perhaps the most important effort of the overall IT infrastructure threat modeling process, although it's also important to properly populate each IT component threat model. When you created each component threat model you rated each threat as it applied to the component to establish a threat priority rating. In the portfolio, you establish a priority hierarchy for all the component threat models. The same logic used in Chapter 1 to prioritize threats for each component can be applied to prioritize the components in your threat model portfolio.

The greatest priority should be assigned to components whose compromise would have the greatest impact and/or the greatest probability of being exploited. For example, if a specific component is subject to five High-priority threats but other components are subject to only one or two High-priority threats, the component with five High-priority threats should have the greatest threat priority rating.

Questions you might ask yourself as part of prioritization include:

* Which component has the highest value as a target?
* Which component is subject to the most High-priority unmitigated threats?

Prioritize components with an overall priority ranking of High first, followed by those ranked as Medium, and then those ranked as Low. If the median ranking for all components is found to be High, hopefully your management team will have all the justification it needs to dedicate resources and budget to immediate mitigation.

The threat prioritization methods described in Chapter 1 can be very useful, because they describe how to prioritize individual threats to a single component as well as how to prioritize numerous components with various priority ratings.

The following figure shows how the steps of the IT infrastructure threat modeling process help generate profiles, which are then assembled into a threat model portfolio.

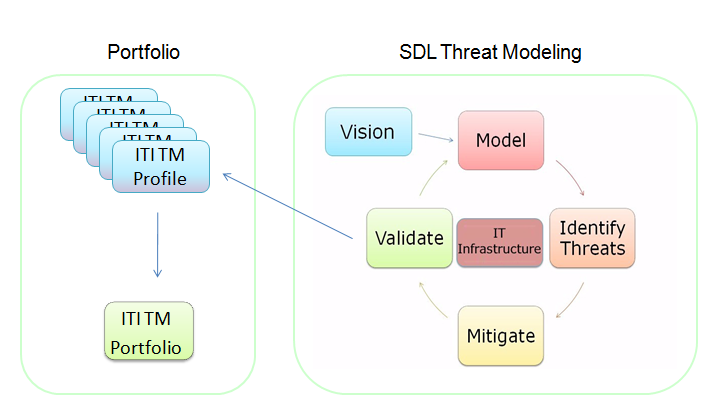


Figure 2.1. Creating the IT infrastructure threat model (ITI TM) portfolio

Chapter 3: Applied Example – The Threat Modeling Process

The goal of this applied example is to describe the practice of IT infrastructure threat modeling as environmentally transparent. Regardless of operating system, manufacturer, hardware/software type, or personal preference, the IT infrastructure threat modeling process must be unbiased. This guidance embraces the fact that IT infrastructures are typically hybrid environments. Creating a threat modeling practice that is limited by environmental conditions would defeat the very essence of that practice.

Mobile device connectivity to organizational e-mail systems is an increasing requirement. Whether this capability is considered a convenience or a necessity, it poses distinct risks to IT infrastructure. Unauthorized access, lost devices, data breaches, and information disclosure are some of the threats that must be considered when providing such connectivity. Therefore, mobile device connectivity is a good candidate for the IT infrastructure threat modeling process. Although single devices such as routers and core switches are typical IT infrastructure components, important processes and services-in-waiting are also excellent candidates for the IT infrastructure threat modeling process.

The arbitrary environment in this applied example is explored at three different levels, particularly during the diagramming phase. A Level 1 perspective provides context from a very high-level view. A Level 2 perspective drills a bit deeper, which one would do to consider a certain feature in more detail. Level 2 diagrams include infrastructure-specific details such as access points, servers, and security mechanisms. A Level 3 perspective is a close-in, detailed exploration that includes protocols and product specifics.

For this applied example, the IT component that is being threat modeled is referred to as Fabrikam Mobile Connectivity. Fabrikam Inc (a fictitious organization) is a major designer and manufacturer of plumbing fixtures. Fabrikam’s services include architectural design of bathrooms and kitchens, custom design and manufacture of plumbing fixtures, and installation and maintenance of plumbing fixtures. Fabrikam is a leader in plumbing-related work for large scale installations such as residential projects, commercial projects, and institutions. Fabrikam has 10,000 employees world-wide.

It's important to note that the applied example is not intended to be comprehensive or complete. Rather, the intention is to offer the reader guidance about how to conduct the IT infrastructure threat modeling process for a single infrastructure component. If you were to conduct the threat modeling process for mobile device connectivity in your environment you would almost certainly discover additional threats and mitigations. For the Level 3 exploration of Fabrikam Mobile Connectivity, the applied example will use the [SDL Threat Modeling Tool](http://msdn.microsoft.com/en-us/security/dd206731.aspx). This tool is available for free and is based on the SDL process. You can use its output to populate profiles and threat model portfolios.

The overall process model in the Overview illustrates how the IT infrastructure threat modeling process progresses:

* From **Vision**
* to **Modeling (diagramming)**
* to **Identifying** threats
* to **Mitigating** threats
* to **Validating** your work

This chapter is designed to help you understand the different steps in the process.

# Vision

Fabrikam management’s vision for mobile connectivity is simple:

**Allow connectivity to the Fabrikam e-mail system via mobile devices to increase productivity for mobile workers through increased efficiency and functionality.**

To achieve this vision, consider vision-related use scenarios that apply to infrastructure components. For example, Fabrikam has the following goals:

* All sales team members must have complete access to Fabrikam resources via their mobile devices, including e-mail and customer resource tools.
* Our e-mail system is the lifeblood of our organization, and it must be well protected because it facilitates communication among employees, customers, and partners.

These goals generate numerous use scenarios. For documentation and organizational purposes, each of the following use scenarios includes an alphanumeric prefix. Mobile connectivity scenarios use MC followed by a sequential number:

**MC.1**. Fabrikam workers use mobile devices for "over-the-air" access to e-mail messages, schedules, contacts, task lists, and other mailbox data.

**MC.2**. Fabrikam management maintains control of mobile devices, including the ability to provision and enforce device security policies determine which devices can synchronize with the e-mail system, and conduct enhanced monitoring and logging.

# Model the Component

A view of Fabrikam Mobile Connectivity from a Level 1 perspective is shown in the following figure. Connection to a wireless LAN could be from a location that is external to Fabrikam (for example, from a coffee shop or through a home network) or while the user and device are physically at a Fabrikam location and within the boundaries of the organization's network.



Figure 3.1. A Level 1 perspective of Fabrikam Mobile Connectivity

A Level 1 diagram should be simple and show the obvious components. A written description of Fabrikam Mobile Connectivity as shown in the preceding figure might read as follows:

*User connects to Fabrikam via their mobile device, either through a cellular provider network and the Internet or directly through a wireless LAN connection.*

A Level 1 perspective provides the ability to make some immediate assumptions, For example, “a primary entry point to the Fabrikam e-mail server is the mobile device itself.”

A Level 2 perspective allows a closer examination that considers some of the technical details of the e-mail server architecture and the basic firewall design. This perspective is shown in the following figure.

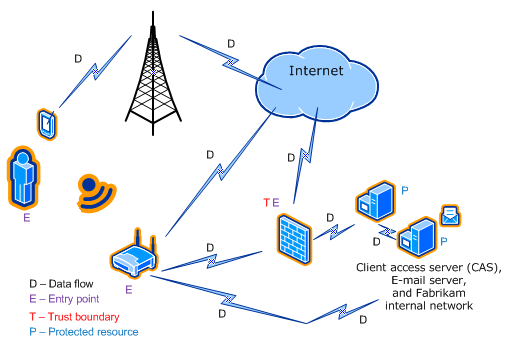
****

Figure 3.2. A Level 2 perspective of Fabrikam Mobile Connectivity

A written description of the preceding figure might read as follows:

*User connects to Fabrikam via their mobile device, either through a cellular provider network and the Internet or directly through a wireless LAN connection. After they connect to Fabrikam, the user connects to the client access server, which is located in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet). After they are authenticated by the client access server, the user's connection traverses the secondary firewall that protects the internal Fabrikam network and the e-mail server.*

When considered from a Level 3 perspective, an IT infrastructure threat model data flow diagram looks entirely different and is very product, technology, and protocol specific. An appropriate component to consider from a Level 3 perspective is Exchange ActiveSync®.

Exchange ActiveSync is a communication protocol that enables wireless mobile access to e-mail messages, schedules, contacts, tasks lists, and other Exchange Server mailbox data. Exchange ActiveSync is available on both Windows Mobile®–based devices and Exchange ActiveSync–enabled devices offered through Microsoft partners.

The following figure shows a data flow that is somewhat similar to the Level 1 and Level 2 perspectives of Fabrikam Mobile Connectivity.

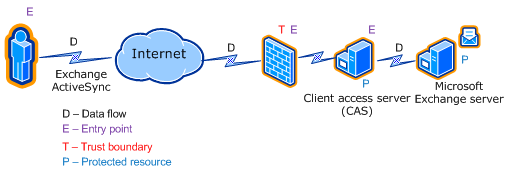
****

Figure 3.3. Exchange ActiveSync data flow

An analysis of Exchange ActiveSync provides an ideal opportunity to use the [SDL Threat Modeling Tool](http://msdn.microsoft.com/en-us/security/dd206731.aspx). You can use this tool from the Model step of the IT infrastructure threat modeling process to immediately enhance whiteboard discussion and stimulate additional discussion.

The preceding figure is a data flow visualization that incorporates Exchange ActiveSync. The ongoing discussion of the applied example in the rest of this chapter uses the SDL Threat Modeling Tool to generate data flow diagrams (DFDs) that use *elements*, including external entities, processes, data flows, data stores, and trust boundaries, as shown in the following figure.

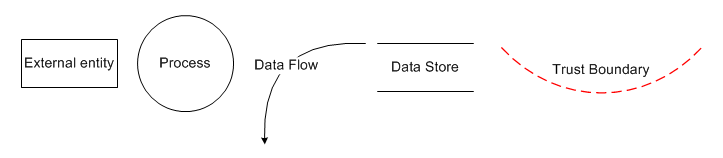


Figure 3.4. SDL Threat Modeling Tool elements

As indicated in Chapter 1, processes include all running code. Data flows include all data that flows between processes and anything else, on host or off. Data stores include files, databases, and registries. External entities are anything outside the control of the system, such as people or Web sites.

A Level 3 representation of Exchange ActiveSync use at Fabrikam as expressed via the Draw Diagrams feature in the SDL Threat Modeling Tool appears in the following screen shot.

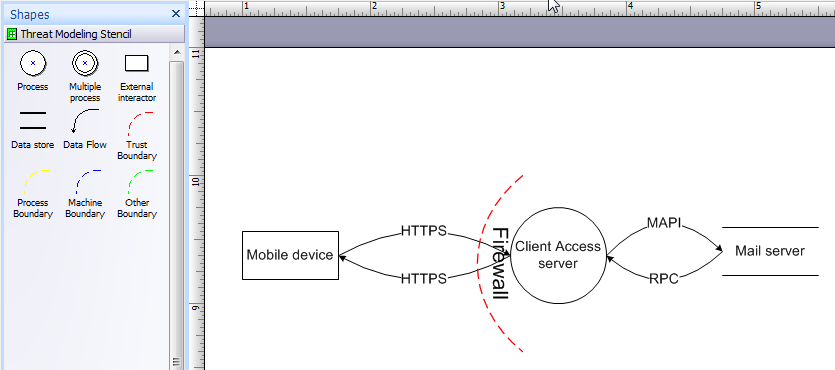
****

Figure 3.5. SDL Threat Modeling Tool Draw Diagrams feature

If the SDL Threat Modeling Tool determines that your diagram has validation errors, a message will display in the Diagram Validation pane of the tool. For example, if your diagram showed no connectivity from the mobile device to the client access server, the message would read “Firewall: No data crosses over the trust boundary.” Consider validator input as feedback, not critical errors that must be fixed.

## Entry Points

An entry point represents data or process flow that traverses a trust boundary. Any portions of an IT infrastructure in which data or processes traverse from a less-trusted zone into a more-trusted zone should have a higher review priority.

The preceding figure illustrates bidirectional data flow via HTTPS between a mobile device and a client access server. This data flow clearly traverses a trust boundary (denoted by a broken red line) that is in the form of a firewall. In addition, the mobile device itself could be considered an entry point. (This scenario is referenced in the "Identify Threats" section later in this chapter.)

## Trust Boundaries and Levels

Users, processes, and IT components all operate at specific trust levels that vary between fully trusted and fully untrusted. Typically, parity exists between the level of trust assigned to a user, process, or IT component and the level of trust associated with the zone in which the user, process, or component resides.

In the example shown in the preceding figure, the components to the left are outside the firewall and are considered less trusted than the components to the right, which are inside the firewall. There are two trust zones: components that are outside the firewall reside in an untrusted zone, and those that are inside the firewall are in a trusted zone.

From the trusted zone perspective, there are three general trust levels for users: Mail Administrators, Authenticated Mobile Users, and Anonymous Untrusted entities. IT components that are in the trusted zone and accessible by Anonymous Untrusted entities should have a higher review priority. In the preceding figure, the HTTPS interface should have a higher review priority because it is exposed to unauthenticated mobile devices.

## Protected Resources

As defined in Chapter 1, protected resources include data stores. In the current scenario, the e-mail data source that contains e-mail and personal information (the mail server) is clearly a protected resource.

If you choose to use the SDL Threat Modeling tool, you have the opportunity to add assumption notes during the Draw Diagrams phase. If the data store (the mail server) is considered protected, it might be relevant to indicate assumptions such as “Current policy might not be adequate to protect this resource.” To do so, right-click the Mail server element in the drawing and click **Note Assumption**, which will cause the dialog box shown in the following screen shot to display.



Figure 3.6. The Assumptions dialog of the SDL Threat Modeling Tool

# Identify Threats

Given what has been learned so far about Fabrikam Mobile Connectivity, which threats should be considered the most dangerous?

* An approved, allowed Fabrikam mobile device is lost or stolen.
* An unauthorized, unapproved device or unauthorized user connects and gains access to Fabrikam.
* Data is intercepted or stolen in transit between a mobile device and Fabrikam that was connected via unencrypted wireless (802.11) connectivity.

If you use the SDL Threat Modeling Tool, the Identify and Mitigate steps of the IT infrastructure threat modeling process will auto-populate the appropriate threats for you based on the STRIDE model discussed in Chapter 1. Based on the data flow diagram created with the Draw Diagram feature for a Level 3 view of Fabrikam Mobile Connectivity, the STRIDE-based threats include Information Disclosure as relevant to the e-mail server. You will see a number of questions to consider regarding this threat type. You can drill deeper into each question by clicking **more**, and you can populate both the Impact and Solution forms. This applied example will examine impact and solution in the "Mitigate Threats" section later in this chapter.

The SDL Threat Modeling Tool allows you to choose the option to “Certify that there are no threats of this type.” You might choose this option based on reasons such as *within a trust boundary* (behind firewall), *mitigated elsewhere* (another component mitigates the threat), or *accepted risk*. Do so only after very careful consideration of the threat, and ensure that you keep detailed records that explain your reasoning. You can use the SDL Threat Modeling Tool to help capture this information.

However, for this applied example, there are threats that remain to be mitigated. The following screen shot shows all the features mentioned in the preceding text.



Figure 3.7. The Analyze Model feature of the SDL Threat Modeling Tool

# Mitigate Threats

The "Mitigate Threats" section in Chapter 1 described the following five mitigation categories to which threats typically belong:

* **Not mitigated and requires mitigation**
* **Not mitigated, but is the responsibility of a dependency or other component**
* Already mitigated by the component
* **Already mitigated by a dependency or other component**
* **Not mitigated, but does not require mitigation**

It's important to weigh each threat very carefully and consider all possible mitigations.

If you use the SDL Threat Modeling Tool, you can populate its Impact and Solution forms during the Identify and Mitigate steps of the process.

Declare your priority rating (High, Medium, or Low) in the Impact form along with a description of the specific threats. The specific threats indicated during the Identify Threats step were as follows:

* An approved, allowed Fabrikam mobile device is lost or stolen.
* An unauthorized, unapproved device or unauthorized user connects and gains access to Fabrikam.

The Solution form is the ideal place to populate your mitigations. For this applied example, the mitigations that were identified for the preceding threats were as follows:

* Mobile devices must be password protected/locked and an inactivity timer must be enforced.
* Data storage on the device must be encrypted.
* Remote wipe (the ability to delete all data on a mobile device from a remote location) must be available.
* To ensure policy enforcement via Exchange ActiveSync, only approved, provisioned Windows Mobile 6.1 devices will be allowed to connect to the Fabrikam e-mail server.

The following screen shot provides examples of how these threats and mitigations appear in the SDL Threat Modeling Tool.



Figure 3.8. The Impact and Solution forms in the SDL Threat Modeling Tool

The information you provide during this portion of the process indicate how many green bars you see in the "Completion" section. Simply populating the Impact and Solution forms will cause two green bars to display. You can check **Finished** if you believe all threat and mitigation information has been populated, which is indicated by a third green bar.

Note that when you populate the Impact and Solution forms during the Analyze Model step, you can choose to file a bug via Microsoft® Product Studio to see the mitigation through to completion, which will result in a fourth green completion bar.

## Threat Prioritization

After you identify all possible threats and determine what mitigations exist or need to be implemented, consider prioritizing the identified threats. Based on this applied example, common sense indicates that threats that result from a lost or stolen mobile device should be mitigated first.

Consider the following threat prioritization process example:

**Resource**. Fabrikam's internal e-mail system, approved mobile devices, and various customer resource tools that are accessible via the devices.

**Threat**. An approved mobile device that is lost or stolen could allow an attacker to gain access to Fabrikam e-mail system resources.

**Impact**. The impact of a successful attack by lost or stolen mobile devices on the organization could be significant and could result in a data breach.

**Vulnerability**. Mobile devices are not password protected, no inactivity timer is enforced, and data that is stored on the mobile devices is not encrypted.

**Mitigation**. No mitigations currently exist to protect Fabrikam's internal e-mail system from attacks by lost or stolen Fabrikam mobile devices.

**Probability**. Considering the lack of current mitigations and the likelihood of approved Fabrikam mobile devices being lost or stolen, the probability of this threat being realized is high.

**Threat priority**. The threat prioritization process determines that the threat priority rating should be High.

The priority rating chosen for each threat can be used to prioritize all of the overall threats. If you use the SDL Threat Modeling Tool, the priority rating should be added to the Impact form during the Identify and Mitigate steps of the process. Of course, threats that have the greatest impact and High priority ratings should be mitigated first.

# Validate

As mentioned in Chapter 1, part of validating the entire IT infrastructure threat modeling process can include examining dependencies and assumptions. Dependencies are key in determining threat mitigations, because any specific threat might actually be mitigated by a dependency. For example, there’s an obvious dependency in this chapter's applied example that requires mobile devices to connect to a client access server before they can access the e-mail server. If access to the client access server is only allowed over a secure protocol (HTTPS), the threat of e-mail server information disclosure (unauthorized viewing of e-mail) via sniffing is mitigated by the dependency.

Dependencies and assumptions can be populated during the Describe Environment phase in the SDL Threat Modeling Tool as shown in the following screen shot. Remember that a dependency is defined as the degree to which a component relies on other components. The tool allows you to clarify and organize dependencies and assumptions, including notes and origins.



Figure 3.9. The Describe Environment (validate) screen of the SDL Threat Modeling Tool

As part of the validation phase, the SDL Threat Modeling Tool allows you to make use of External Security Notes and Document Header Information, found under Describe Environment.

External Security Notes can include information relevant to the component’s users or customers while Document Header Information is excellent for tracking the details about who is involved in the threat modeling process.

# Summary

When you use a structured method like the one in this guidance to develop a threat model for your IT infrastructure, you identify and mitigate threats to your environment in an efficient and effective manner. Validate every assumption, threat, and mitigation. Create complete data flow diagrams. Leave no detail unconsidered. The closer your attention to detail, the better your threat model will be. The more components that you add to your IT infrastructure threat model portfolio, the stronger your security posture will be. Well-developed threat models that identify mitigations that are implemented will help improve security in your organization.

Remember, the threats identified in this guidance are cited as possible examples and are not to be considered complete or comprehensive. You should apply all due diligence when considering threats; failure to do so in an appropriate manner can be costly in the future.

It is the intent and hope of this guidance that the benefits of choosing to develop a threat model portfolio for your IT infrastructure will be many, and that a holistic state of security becomes commonplace for those who undertake the process.