The Role of **Network Visibility** in IT Operational **Risk Management**

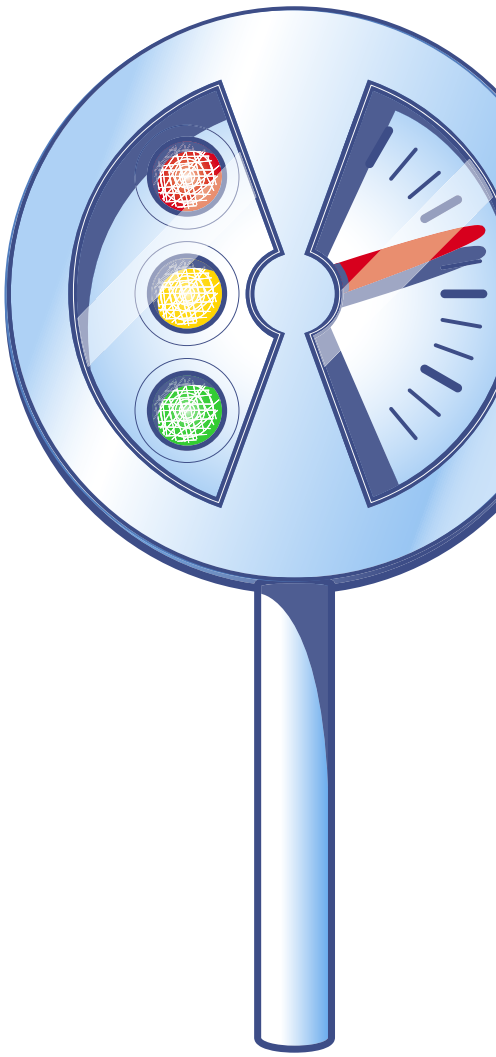
White Paper
Author: Dirk Paessler

Published: July 2008

www.paessler.com
info@paessler.com

PAESSLER®
the network monitoring company

CONTENTS



EXECUTIVE SUMMARY

Life is filled with risk. While it can never be eliminated, wise individuals and organizations dedicate resources to mitigate risk to keep potential losses under control.

In business, risk management has traditionally been synonymous with insurance. In IT the focus has been on a technological fix to a specific problem, often with little previous planning. Clearly such a shotgun approach to problem solving has major drawbacks including the potential for inefficient use of available resources.

Also in IT, there tends to be a focus on two subsets of risks – malware and data recovery. This can often lead to the exclusion of other risks that should also be focused on (see Gartner's recent report "IT Risk Management: A Little Bit More Is a Whole Lot Better" at www.gartner.com).

On the other hand, too much risk management can burn up resources better invested in other areas, so a balance needs to be struck. Resources need to be allocated carefully to achieve maximum risk mitigation at minimal cost.

The importance of network management to many areas of IT operational risk management is often neglected. Certainly its role in managing potential network problems such as switch failures and overloads is a major reason for investing in network management software. However, it also can have a role in identifying other potential problems including the download of inappropriate material on business networks and prioritizing various classes of network traffic for optimal business performance. In a world in which even sub-second delays in transactional traffic can cost, these can be crucial elements to address.

A comprehensive detailed examination of risks facing IT can be found in Control Objectives for Information and related Technology (CobiT) 4.1 available from the Information Systems Audit and Control Association (ISACA) at www.isaca.org/CobiT. This paper focuses on risks associated with IT and, in particular, network operations. It presents a three-step approach for identifying, rating and planning an overall IT operational risk mitigation strategy. In the process, it outlines the business case for network monitoring as a key player in that strategy.

Links

Gartner Group:
"IT Risk Management: A Little Bit More Is a Whole Lot Better"
www.gartner.com

ISACA:
CobiT-article on risk management
www.isaca.org/CobiT

CLASSIFYING IT OPERATIONAL RISKS

The bad news: it is impossible to eliminate risks. The goal of risk management is to identify the problems that can and should be managed and to reduce those exposures to a level that the business can accept. This leaves residual risks that can be accepted as a cost of doing business.

For small-to-medium sized enterprises (SMEs) some unlikely but potentially devastating risks might have to be accepted because the business lacks the resources to mitigate them.

Unfortunately, small to medium IT organizations often take a threat-based approach to security without any real forward-looking risk management. Network-borne computer viruses become a threat, so IT installs anti-virus software; intrusions become a threat, so IT installs a firewall to protect from the outside, and so on.

This approach has two major problems:

- First, it is myopic: It focuses on just a subset of the total risk portfolio – usually those with technology fixes.
- Second, it is piecemeal and reactive: It results in a proliferation of devices and services, each focused on a single problem, with no central management, an IT group that is constantly "putting out fires" can never get ahead. It needs to take a step back and develop a risk plan.

RISK CLASSES

IT faces three major classes of operational risk:

Technology risks

These are traditional IT concerns ranging from equipment failures through network-borne computer viruses and worms to more exotic issues such as denial-of-service attacks, intrusion attempts and "war walkers" accessing wireless networks from outside the building.

Many of the remedies to these problems are also technology-based, but strong policies are also important. Enforcing a rule that portable devices run strong firewall and anti-virus systems is an obvious policy. Another could include a rule that employees cannot install their own uncontrolled, and often unprotected, WiFi nodes.

A strong network monitoring tool, such as Paessler's PRTG Network Monitor, can provide early warning of unusual, suspicious activity on the network and pinpoint the source of that traffic.

Legal and personnel risks

These include compliance issues such as preparing for possible legal discovery requirements which might include email collection for civil suits; employees downloading inappropriate material from the Internet which could create hostile workplace suits; and potential sabotage or espionage by employees.

These kinds of threats are harder to manage because technology cannot provide clear-cut solutions.

Strong personnel policies and good management are keys to mitigating these risks.

Managers should be trained in good management techniques. The presumption that a good employee can be promoted to management and automatically become a good manager is a common mistake.

However, network management can also provide clues to some potential problems. Some of them might be detected by a tool such as Paessler's PRTG Traffic Grapher, which provides live monitoring of network traffic and bandwidth usage classifications.

Natural and man-made disasters

Floods, earthquakes, large storms – while much less likely occurrences, can be devastating.

Defining adequate strategies for managing these risks is one of the most difficult tasks of risk management.

A variety of strategies are available at different prices and with varying levels of protection. They should be judged in the context of the overall situation of the business.

However, disaster management should start with common sense.

In today's networked world, even relatively small organizations can locate their data centers away from disaster-prone areas and in a modern, physically secure facility (possibly shared with other businesses) or can turn vital IT functionality over to outsourcers or Software-as-a-Service (SaaS) providers that can enable a greater level of security than the business can in-house.

Again, this makes network management tools such as those provided by Paessler an important tool in managing such risks. In both cases the importance of the network, including the Internet last mile, becomes central to delivering those IT services to the business.

A THREE-STEP PLAN

While many smaller IT shops are guilty of not planning at all, it is equally important to avoid over planning. For SMEs, and even some larger shops, risk management planning can be a fairly informal, spreadsheet-type exercise.

Step 1: List and rank risks according to business cost

The first step in this exercise is to identify the main risks under each of the three categories.

Standard risk lists are available and one of the most complete is part of the IT governance framework CobiT, but these could be overwhelming covering a wide range of topics beyond those that the IT organization might want to include.

Each project involves a range of risks of its own including the possibility that the job is never completed or that it is completed poorly, or runs over-budget and over-schedule.

While developing a comprehensive list of risks can be fairly easy, rating them according to potential busi-

ness cost and importance is much more difficult.

While lists of risks are universal, business costs can vary widely between organizations.

For instance, financial traders cannot tolerate even small delays in transmission of transactions, but a manufacturer might be tolerant of order processing delays and may need high performance from its ERP system. This means estimating the total business cost of each risk can be difficult.

Planners will want to consult business executives to discover what guidance could be offered from any associations in their industry and colleagues from other organizations in the same vertical market.

While the estimate does not have to be precise, having one is important. It will be the basis for determining how much should be invested in mitigation. It needs to be determined what focus should be applied to protecting the organization against the basic threats such as viruses and worms.

However, other important planning questions must be asked.

- How much should be spent on the basics compared with other risks?
- When does the investment reach a point of diminishing returns?

The answers to these vital planning questions depend, in part, on the cost of damage from these IT pests.

Event probability also must be factored into the picture. Viruses are a constant issue but individually have a small cost to fix and don't cause major disruption. A major disaster has a low probability, but can devastate a business.

Step 2: Pricing mitigation

This does not have to be exact and should not involve writing request for proposal (RFP) documents. Estimates based on Internet research and past experience are good enough. Planners should keep in mind that costs will include staff availability and time as well as money spent. Some cases are straightforward where mitigation involves buying and installing a hardware or software solution. In others, and particularly in the case of disaster recovery, a variety of strategies with widely varying costs and effectiveness are available.

Determining which is best for any organization depends on a variety of factors:

- Tolerance for long periods of downtime
- Available resources for problem solving
- Ability to survive a major disaster

A small business unable to survive a disaster would be wasting money on a remote-site data recovery (DR) solution. Alternatively, if all the company can afford is tape backup and storage in a vault, then that becomes the company's DR solution, whether it fits the organization's true DR needs or not. However, more creative solutions such as using a SaaS provider or DR outsourcers are important options to consider.

Planners might also find that the cost of mitigating some risks is actually higher than the estimated potential loss. In this case, mitigation might not be worth the investment.

The company's relative tolerance to risk, as expressed by senior management, should also be taken into account in determining the mitigation strategy.

Step 3: Multi-year planning

Mitigation is an ongoing effort largely because available resources always fall short of needs, making multi-year planning a necessity. The risks change over time, so fresh approaches need to be considered constantly.

The risk of viruses is a constant, but the actual viruses change. So while an organization might be a veteran in dealing with such a risk, there is a need to be constantly vigilant.

New risk, such as wireless networks and war walkers can appear at any stage, and business activities such as expanding into new markets and industry segments or acquisitions will alter the basic risk picture.

THE LARGER PICTURE: RISK MITIGATION AND THE NETWORK

Risk management planners need to consider how the entire network functions when working on mitigation solutions and factor other in other IT planning issues.

More than costs need to be considered when thinking of risk mitigation, such as when choosing between using in-houses services or contracting out.

Often decisions are made on the basis of relative cost, availability of specific knowledge and skills or internal politics.

However, careful decision-making can be an effective way to change the overall risk exposure picture. The vendor takes on some risks, such as data security and DR, but in turn the company accepts the risk that the vendor may fail to meet service level agreements (SLAs) or that the agreed-to SLAs will not meet the organization's needs over time. If IT can reduce its investment in some areas of risk mitigation, it will need to invest in managing the services on which the business now depends.

Network management is another important tool that is often underutilized for risk mitigation. This technology's association with some areas of risk, primarily network component failures and management of hot spares and switchovers, is obvious and usually a main reason for installing a network management suite. However, it has

indirect uses for managing other areas of risk management as well.

One major area associated with network risk is transmission delay caused by traffic overloads.

VoIP is notoriously sensitive to delays, and the introduction of VoIP into a network is accompanied by traffic prioritization to ensure that voice packets are not delayed by other data movement.

Other applications can be just as sensitive to delays in data transmission. For instance, chronic delays in transmission of transactional traffic can add up to financial losses for some industries like airlines along with currency, stock and commodities trading.

In today's highly automated, real-time factories, chronic small delays in data transmission can slow production lines, causing production losses. The loss of automated order or shipping data in JIT (just-in-time) supply environments can be disastrous. So in many production environments, strong network management can achieve ROI simply by ensuring that vital data is not delayed.

Good network management can also help to identify the causes of data congestion and other issues in a system. In today's highly mobile environment, with management and increasing numbers of knowledge workers carrying laptops and other devices used outside the protection of the corporate network, the danger of malware being transported inside the enterprise firewalls by legitimate employees is escalating.

Often the first indication of the presence of such risks – a zombie sending out masses of spam or denial-of-service messages; or a worm propagating itself through the organization – is a spike in network traffic picked up by network management tools. These are also often the primary tools for tracking the problems to their sources so they can be shut down.

WiFi networks add several risks

IT loses a great deal of control over what devices are connected to the network, bringing risks ranging from incompatibility between applications and end-user mobile devices to network access by visitors and other unauthorized individuals.

The network often extends beyond the physical walls of the building which makes it potentially vulnerable to war drivers or walkers who access the network, and possibly corporate applications and data, from the sidewalk or parking lot.

WiFi modems are notoriously easy to attach to a network. Network administrators often discover unauthorized WiFi networks cropping up across an office as employees plug wireless modems into the network in their offices. Often these employees do not bother to activate the WiFi modem's access controls, opening a potential route for outsiders to bypass corporate firewalls and perpetrate intrusions or plant malware throughout the enterprise.

Strong network management can help IT identify and counter potential wireless network risks and keep the wireless environment under control.

Close monitoring of network traffic levels is particularly important

today because of a major shift in business data types and volumes. Alphanumeric data, which, until recently has dominated knowledge worker traffic, is now being supplemented with increasing amounts of graphic and digital audio and video. This can easily overload networks sized for alpha-numeric office data. It is difficult to identify legitimate business traffic from simple amusement or worse, something that might create a hostile workplace situation.

While sites such as YouTube are often the source of this traffic, an increasing amount is legitimate. For instance, businesses are replacing business travel with teleconferences and video conferencing, sometimes from office studios and also directly from individual desks. This can save the company large amounts of money spent on travel, boost employee productivity by eliminating travel time, boost employee morale, and reduce the corporate carbon footprint.

The fast growth in such traffic, which will only accelerate as fuel prices and the real costs of traveling rise, can increase the risk of network traffic spikes that can degrade service across the network. A good network management tool which can project growth patterns in use of network devices, such as Paessler's PRTG Traffic Grapher, is the first line of defense against this kind of risk and can plan an important role both in monitoring fast network traffic growth and providing data for planning increases in network capacity.

RISK MANAGEMENT AND PAESSLER

Paessler offers four applications that comprise a complete network monitoring suite for small-to-medium businesses and is also used by large and very large enterprises to provide more detailed visibility into critical parts of their networks. Unlike some of its competitors, Paessler has recently re-architected all its tools, putting them on the optimal technological base and improving their overall functionality, efficiency and usability.

Paessler's tool suite consists of

PRTG Network Monitor (www.paessler.com/prtg) is an easy-to-use Windows application for uptime-monitoring and classifying network traffic and usage. It combines the capabilities of Paessler's former products, IPCheck Server Monitor and Paessler Router Traffic Grapher into one offering. PRTG helps organizations monitor critical network resources and detect systems failures or performance problems immediately, minimizing downtime and its economic impact. Live readings and long-term usage trends for network devices can also be used to classify bandwidth usage, memory and CPU utilization.

SNMP Helper (www.paessler.com/snmphelper) enables PRTG to collect detailed performance information on Windows servers and workstations. Up to several thousand parameters and performance counters on a PC can be monitored with just a few mouse clicks.

Paessler products

PRTG Network Monitor:
Network availability and usage monitoring:
www.paessler.com/prtg

SNMP Helper:
Windows performance monitoring:
www.paessler.com/snmphelper

Webstress Server Tool:
Load and Stress testing of websites:
www.paessler.com/webstress

Webserver Stress Tool (www.paessler.com/webstress) is a powerful HTTP-client/server test application designed to pinpoint critical performance issues on a Web site or Web server that may obstruct delivery of an optimal user experience. By simulating simultaneous access by hundreds or thousands of simultaneous users, it tests Web server performance under normal and extreme loads to ensure that critical information and service are available at response times that users expect. Detailed test logs and several easy-to-read graphs make analyzing results a snap. Webserver Stress Tool for Windows can benchmark almost any HTTP server (static pages, JSPs/ASPs, or CGIs) for performance, load, and stress response.

Each tool comes in commercial versions. However freeware editions are available to allow users to test main features before making the purchase decision. To download free and commercial editions, please visit at www.paessler.com/download/.

CONCLUSION

Ultimately there are no guarantees. Life is risky, and a certain amount of risk has to be accepted by any organization. Risk management is not about guaranteeing that nothing bad can happen, because even the most secure environments experience problems. Instead, the aim of risk management is to reduce exposure to an acceptable level that is both affordable and survivable. If IT can manage that, then it can consider its risk management program successful.

About Paessler AG

Founded in 1997 and headquartered in Nuremberg, Germany, Paessler AG builds cost effective software that is both powerful and easy to use. The product range is specialized on Network Monitoring and Testing as well as Website Analysis. Its products are used by Network Administrators, Website Operators, Internet Service Providers and other IT-Professionals worldwide. Freeware and Free Trial versions of all products can be downloaded from www.paessler.com.

PAESSLER®
the network monitoring company

Paessler AG • Burgschmietstrasse 10
90419 Nuremberg • Germany
www.paessler.com • info@paessler.com