Using Network Monitoring Tools for Reducing IT Risks

A guide for IT professionals

wanstor

Contents

Introduction

Traditionally, risk management in IT has been focused on technological fixes to specific problems, often with little/no previous planning. In most organisations when you mention "risk management" to IT teams, a reactive process/approach is often demonstrated or used. Clearly a reactive approach to problem solving and risk management has major shortcomings including potential for inefficient use of personnel and computing resources.

Additionally in IT, risk management tends to focus on two subsets of risk - malware and data recovery. By only focussing on these two areas of risk IT teams are leaving themselves exposed to other security and data management risks. On the other hand, too much risk management can make the IT function inefficient by tying people up in unnecessary processes and procedures. This means a balance needs to be struck. Resources need to be allocated carefully to achieve maximum risk mitigation at minimal cost.

At Wanstor we often find the importance of network management to many areas of IT operational risk management is often neglected or overlooked. 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 can also 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. We now live in a society where even sub-second delays in transactional traffic can cost businesses money.

At Wanstor we always recommend before an IT manager starts designing a risk management programme that they read the Control Objectives for Information and related Technology (CobiT) report available from the Information Systems Audit and Control Association (ISACA) at **www.isaca.org/CobiT**. This report gives a comprehensive overview of the risks IT Managers should be aware of and plan for in their risk management strategy.

This whitepaper 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 a risk management strategy.

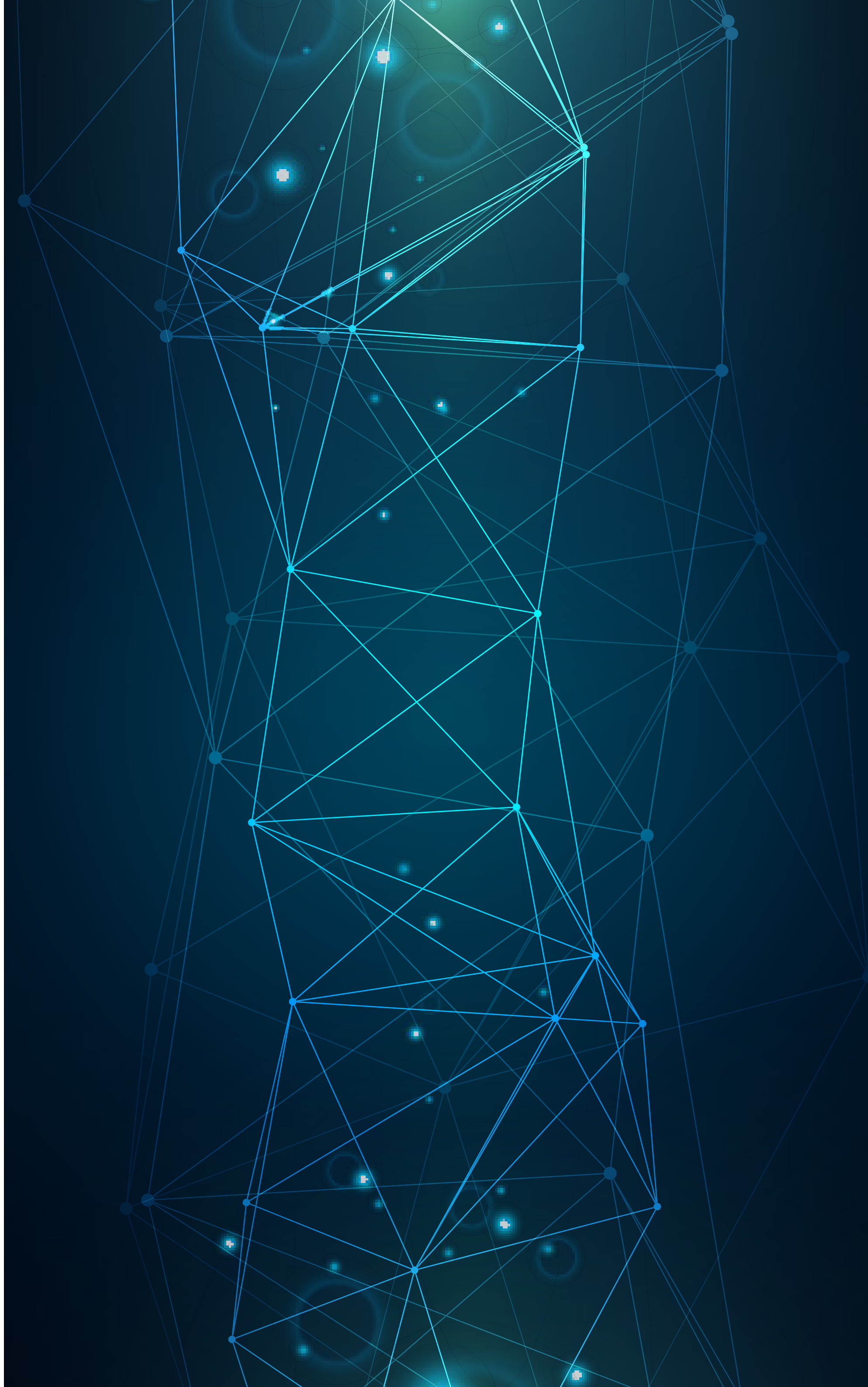
Classifying IT Operational Risks

Let's get the bad news out of the way first - it is impossible to completely eliminate all risks in IT. At Wanstor we believe the goal of risk management is to:

"identify the problems that can and should be managed and to reduce risk exposures to a level that a business or not for profit organisation can accept."

This leaves residual risks that can be accepted as a cost of doing business. For small-to-medium sized organisations 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 organisations 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 narrow-minded. It focuses on just a subset of the total risk portfolio - usually those with technology fixes.
- Second, it is reactive: It usually results in a proliferation of devices and services, each focused on a single problem, with no central management, and an IT group that is constantly "fire fighting" meaning it can never get ahead.

If you recognise this scenario it probably means the IT department needs to take a step back and develop a risk plan.

IT faces three major classes of operational risk:

Technology Risks

These are traditional IT concerns ranging from equipment failures through to network computer viruses and worms to more exotic issues such as denial-of-service attacks, intrusion attempts and unauthorised access to wireless networks. Many of the solutions to these problems are technology based, but strong policies, processes and procedures 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, Wi-Fi 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 legal challenges; employees downloading inappropriate material from the Internet; and potential sabotage or espionage by employees.

These kinds of threats are harder to manage because technology cannot provide clear and easy to use 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 Network Monitor, which provides live monitoring of network traffic and bandwidth usage classifications.

Natural And Man-Made Disasters

Floods, earthquakes, large storms can be devastating for IT equipment if it is not housed in a safe secure facility. Defining adequate strategies for managing these risks is one of the most difficult tasks of risk management for an IT Manager.

There are 100's of strategies, opinions and products available at different prices and with varying levels of protection to help mitigate these risks. Before you purchase any tools or software to help with risk management IT Managers should always ask the question - How does this solution fit within the context of my business? At Wanstor we believe disaster management should start with common sense.

In today's ever connected world, even relatively small organisations can locate their data centres 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 internally.

Again, this makes network management tools such as Paessler's PRTG Network Monitor 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 departments are guilty of not planning for disasters or the mitigation of risk, it is also important to avoid over planning as well. Here are 3 steps Wanstor recommends all of it's customers undertake when developing a risk management strategy:

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 as part of the IT governance framework CobiT (as mentioned on page 3 of this whitepaper). The COBIT report covers a myriad of IT risks.

Many IT departments will find the list of risk to cover overwhelming and covering a wide range of topics beyond those traditionally that the IT team are responsible for.

Each IT project involves a range of risks of its own including the possibility that the job is never completed, 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 business cost and importance is much more difficult.

While lists of risks are quite common, business costs can vary widely between different organisations depending on risk exposure.

For example, financial traders cannot tolerate 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.

Risk planners will want to consult business executives to discover what guidance could be offered from any associations in their industry and colleagues from other organisations 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 organisation against the basic threats.

However, other important planning questions must be asked including:

- 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 on the cost of damage from each IT risk. 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 if the right risk management process is not in place.

Step 2: Pricing Mitigation

This does not have to be exact and should not involve writing proposal 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 organisation depends on a variety of factors:

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

A 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 organisation'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 mainly because available resources nearly always fall short of needs, this makes 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 IT team may have a good track record in dealing with such a risk, there is a need to be constantly observant.

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

Risk Mitigation and the Network

IT 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 organisation‘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 is dependent on. Network management is another important tool that is often underused 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 tooling 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 banking, insurance and commodities trading.

In today‘s highly automated, real time retail stores small delays in data transmission can slow payment processing times and result in a poor shopping experience for customers.

In many customer facing environments, strong network management can achieve ROI simply by ensuring that vital data is not delayed and can be easily accessed by staff.

The right network management approach can also help to identify the causes of data congestion and other issues in a system.

In highly mobile environments, 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 rising year on year.

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.

Wi-Fi Networks add several risks

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

The Wi-Fi network often extends beyond the physical walls of the building which makes it potentially vulnerable to outsiders who do not have authorised permissions to access the network.

Quite often network administrators discover unauthorized Wi-Fi networks appearing across an office as employees plug wireless modems into the network in their offices. Often these employees do not bother to activate the Wi-Fi modem's access controls, opening a potential route for outsiders to bypass corporate firewalls and allow intrusions or plant malware throughout the business.

Strong network management can help IT teams to identify and counter potential wireless network risks and keep the wireless environment under control. Close monitoring of network traffic levels is particularly important 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.

While sites such as YouTube are often the source of this traffic, an increasing amount is legitimate. E.g. businesses are replacing business travel with teleconferences and video conferencing, sometimes from office studios and 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 Network Monitor, is the first line of defence 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.

Wanstor's Network Monitoring Services

For any business, just one minute of network downtime can result in a poor customer experience, lost revenue and seriously impact staff productivity. Wanstor understands that no two businesses are the same. We offer a range of network monitoring services so you can choose the right mix for your business. Our most popular network monitoring services include:

Full Network Monitoring

Monitor every aspect of the network; PINGs, traffic, bandwidth, firewalls, routers and switches to make sure they have the right network infrastructure in place.

Bandwidth Monitoring

Identify potential bandwidth capacity and overloads, and where shortages are happening.

Hardware Monitoring

Allows the monitoring of all IT hardware at a glance – e.g. Computers, Printers, Servers, Hard Drives, Routers, and Switches.

IP Monitoring

Allows the monitoring of all IP addresses in your network, even remote and on Virtual Machines.

Update and Patch Monitoring

Makes sure updates and patch monitoring happens across all operating systems and applications.

Database Monitoring

Enables data centre teams to monitor availability, downtime, usage, alerts, Oracle SQL, MS SQL, MySQL, and PostgreSQL.

Application Monitoring

Allows engineering teams to monitor SQL, exchange and server software, cloud and virtualised applications and other standard business applications.

Wi-Fi Monitoring

Gives operational and IT teams access to what is happening across a Wi-Fi network, in terms of devices, load, traffic, signal strength, and last access.

Network Monitoring Benefits

By having the right network monitoring solution in place IT departments can benefit from:

Early recognition of potential hardware issues, meaning a proactive approach to IT can take place saving engineering time and costs to repair in the future.

Detect potential security threats earlier and put in place anti-virus software and patch management to stop attacks before they harm the business.

Enable the automation reboots of computers and other hardware saving engineers time and effort in their daily roles.

Make sure webpages are always available and set up alerts if they start to run slowly so customers receive a great online presence whenever they visit your company online.

Ensure your datacentre is running at the optimum temperature and is safely accessed by the people at the right time.

Make sure your business and guest Wi-Fi has the right bandwidth and user experience wherever users are accessing the service.

Wanstor Customers Using PRTG Network Monitoring Tools

wagamama
LOUNGES
YO!
D&D
LONDON
BFC Bank
WEXAS
TRAVEL MANAGEMENT
Lindt
MAÎTRE CHOCOLATIER SUISS
DEPUIS 1845
TEENAGE
CANCER
TRUST
Hestia
British
Lung
Foundation
LUC

Final Thoughts

Wanstor works with **PRTG Network Monitoring solutions** to offer a comprehensive network monitoring solution for companies of all sizes to provide more detailed visibility into critical parts of their networks. PRTG network monitoring tools are easy to use and help organisations monitor critical IT resources and detect systems failures or performance problems immediately, minimizing downtime and its economic impact.

Long-term usage trends for devices and applications can also be used to optimize IT environments. Remote network monitoring and management is possible via Web browsers and mobile apps for iOS, Android and Windows devices.

Ultimately there are no guarantees. IT will always have associated risks, and a certain amount of risk has to be accepted by any IT team. 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 the IT team can manage that, then it can consider its risk management approach successful.

For more information about Wanstor's IT Network Monitoring services please contact us on **0333 123 0360**, email us at **info@wanstor.com** or visit us at **www.wanstor.com**.

© Wanstor. All Rights Reserved.

wanstor