Network administrator

A network administrator maintains computer infrastructures with emphasis on networking. Responsibilities may vary between organizations, but on-site servers, software-network interactions as well as network integrity/resilience are the key areas of focus.

Duties

The role of the network administrator can vary significantly depending on an organization's size, location, and socio-economic considerations. Some organizations work on a user-to-technical support ratio,[1][2] whilst others implement many other strategies.

Generally, in terms of reactive situations (i.e.: unexpected disruptions to service, or service improvements), IT Support Incidents are raised through an Issue tracking system. Typically, issues work their way through a Help desk and then flow through to the relevant technology area for resolution. In the case of a network related issue, an issue will be directed towards a network administrator. If a network administrator is unable to resolve an issue, a ticket will be escalated to a more senior network engineer for a restoration of service or a more appropriate skill group.

Network administrators are often involved in proactive work. This type of work will often include:

- Network monitoring
- Testing the network for weakness
- Keeping an eye out for needed updates
- Installing and implementing security programs
- In many cases, E-mail and Internet filters
- Evaluating implementing network

Network administrators are for making sure that computer hardware and network infrastructure related to an organization's data network are effectively maintained. In smaller organizations, they are typically involved in the procurement of new hardware, the rollout of new software, maintaining disk images for new computer installs, making sure that licenses are paid for and up to date for software that needs it, maintaining the standards for server installations and applications, monitoring the performance of the network, checking for security breaches, and poor data management practices. A common question for the small-medium business (SMB) network administrator is, how much bandwidth do I need to run my business?[3] Typically, within a larger organization, these roles are split into multiple roles or functions across various divisions and are not actioned by the one individual. In other organizations, some of these roles mentioned are carried out by system administrators.

As with many technical roles, network administrator positions require a breadth of technical knowledge and the ability to learn the intricacies of new networking and server

software packages quickly. Within smaller organizations, the more senior role of network engineer is sometimes attached to the responsibilities of the network administrator. It is common for smaller organizations to outsource this function.

CH7

Network Security Concepts and Policies

Risk Analysis →

Evaluating and Managing the Risk

The security policy developed in your organization drives all the steps taken to secure network resources. The development of a comprehensive security policy prepares you for the rest of your security implementation. To create an effective security policy, it is necessary to do a risk analysis, which will be used to maximize the effectiveness of the policy and procedures that will be put in place. Also, it is essential that everyone be aware of the policy; otherwise, it is doomed to fail.

All design guidelines and principles, and the resulting security architecture, should be aimed at managing risk. Risk is, or should be, the building block of information security.

Levels of Risks

By its very nature, risk management is a tradeoff between the effort (cost) to protect organizational assets and the resulting level of exposure of those assets. This simple rule is a good starting point: the cost to protect an asset will likely not be greater than the value of the asset itself. There are obviously exceptions to the rule; for instance, cases that involve national security, or instances where the value of the asset is incalculable, such as cases where human life is involved.

The tradeoffs in risk management are based on its building blocks: assets and vulnerabilities, threats and countermeasures. Different values and scenarios for these components move the risk indicators up and down. Understanding these values and scenarios is critical in defining a risk management strategy.

For instance, would you use old, worn tires at high speed on a highway? The answer is obviously no. The asset that you are trying to protect (your life) is too valuable, and the countermeasure to mitigate the risk of navigating the highway, driving at a slow speed, is not good enough. It is inexpensive but not effective.

However, using a worn-down tire as a swing does not result in life-threatening risk in the majority of situations. The asset (your life) remains the same, but the threats that are able to exploit the vulnerabilities of the tire are mitigated or nonexistent. The premise changes again if you think that this worn-down tire will be used to swing your child. You may or may not risk using the old tire, but the value of the asset may prevent you from facing risk even if it is minimal.

The previous example is a simplistic view of information security risk. Imagine an organizational risk management effort, considering thousands of assets with different (and often subjective) valuation criteria, different (and often unknown) levels of vulnerability, and potentially exposed to an avalanche of threats that change by the minute. Risk

management becomes a delicate balance and involves constant tuning of countermeasures in the face of sophisticated threat vectors, exploiting assets that are often located outside of corporate control.

Information security risk management is a comprehensive process that requires organizations to frame risk (in other words, establish the context for risk-based decisions), assess risk, respond to risk, and monitor risk on an ongoing basis. The result is a dynamic process in nature, evolving along with internal factors (assets, vulnerabilities, security policies, and architectures) and external factors (threats, and business, legal, and compliance forces).

Other sections in this chapter will expand on these concepts and present commonly used risk management strategies, within the context of a security policy and a security lifecycle process.

Risk Analysis and Management

Every process of security should first address the following questions:

- Which are the threats the system is facing?
- Which are the probable threats and what would be their consequence, if exploited?

The threat-identification process provides an organization with a list of threats to which a system is subject in a particular environment.

Risk Analysis

Risk analysis is the systematic study of uncertainties and risks. Risk analysts seek to identify the risks that a company faces, understand how and when they arise, and estimate the impact (financial or otherwise) of adverse outcomes. Risk managers start with risk analysis, and then seek to take actions that will mitigate these risks. Risk analysis tries to estimate the probability and severity of threats faced by an organization's system that needs protection, and then provides to the organization a prioritized list of risks that the organization must mitigate. This allows the organization to focus on the most important threats first.

Two types of risk analysis are of interest in information security:

- Quantitative: Quantitative risk analysis uses a mathematical model that assigns monetary values to assets, the cost of threats being realized, and so on. Quantitative risk analysis provides an actual monetary figure of expected losses, which is typically based on an annual cost. You can then use this number to justify proposed countermeasures. For example, if you can establish that you will lose $1,000,000 by doing nothing, you can justify spending $300,000 to reduce that risk by 50 percent to 75 percent.

- Qualitative: Qualitative risk analysis uses a scenario model. This approach is best for large cities, states, and countries to use because it is impractical for such entities to try to list all their assets, which is the starting point for any quantitative risk analysis. By the time a typical national government could list all of its assets, the list would have hundreds or thousands of changes and would no longer be accurate.

Qualitative risk analysis is straightforward provided you have the resources to document all the assets. However, quantitative risk analysis is more tricky, so we will take a closer look at it.

Quantitative Risk Analysis Formula

Quantitative risk analysis relies on specific formulas to determine the value of the risk decision variables. These include formulas that calculate the asset value (AV), exposure factor (EF), single loss expectancy (SLE), annualized rate of occurrence (ARO), and annualized loss expectancy (ALE). The ALE formula is as follows: ALE = (AV * EF) *ARO.

The AV is the value of an asset. This would include the purchase price, the cost of deployment, and the cost of maintenance. In the case of a database or a web server, the AV should also include the cost of development. AV is not an easy number to calculate.

The EF is an estimate of the degree of destruction that will occur. For example, suppose that you consider flood a threat. Could it destroy your data center? Would the destruction be 60 percent, 80 percent, or 100 percent? The risk-assessment team would have to make a determination that evaluates everything possible, and then make a judgment call. For this example, assume that a flood will have a 60 percent destruction factor, because you store a backup copy of all media and data offsite. Your only losses would be the hardware and productivity.

As another example of EF, consider data entry errors, which are much less damaging than a flood. A single data entry error would hardly be more than a fraction of a percent in exposure. The exposure factor of a data entry error might be as small as .001 percent.

CAUTION

One of the ironies of risk analysis is how much estimating (guessing) is involved.

The SLE calculation is a number that represents the expected loss from a single occurrence of the threat. The SLE is defined as AV * EF.

To use our previous examples, you would come up with the following results for the SLE calculations:

- Flood threat
  - Exposure factor: 60 percent

    - AV of the enterprise: US$10,000,000
    - $10,000,000 * .60 = $6,000,000
- Data entry error
    - Exposure factor: .001 percent
    - AV of data and databases: $1,000,000
    - $1,000,000 * .000001 = $10 SLE

The ARO is a value that estimates the frequency of an event and is used to calculate the ALE.

Continuing the preceding example, the type of flood that you expect could reach your data center would be a "flood of the century" type of event. Therefore, you give it a 1/100 chance of occurring this year, making the ARO for the flood 1/100.

Furthermore, you expect the data entry error to occur 500 times a day. Because the organization is open for business 250 days per year, you estimate the ARO for the data entry error to be 500 * 250, or 125,000 times.

Risk analysts calculate the ALE in annualized terms to address the cost to the organization if the organization does nothing to counter existing threats. The ALE is derived from multiplying the SLE by the ARO. The following ALE calculations continue with the two previous examples:

- Flood threat
    - SLE: $6,000,000
    - ARO: .01
    - $6,000,000 * .01 = $60,000 ALE
- Data input error
    - SLE: $10
    - ARO: 125,000
    - $10 * 125,000 = $1,250,000 ALE

A decision to spend $50,000 to enhance the security of our database applications to reduce data entry errors by 90 percent is now an easy decision. It is equally easy to reject a proposal to enhance our defenses against floods that costs $3,000,000.

When you perform a quantitative risk analysis, you identify clear costs as long as the existing conditions remain the same. You compile a list of expected issues, the relative cost of those events, and the total cost if all expected threats are realized. These numbers are put into annual terms to coincide with the annual budgets of most organizations.

You then use these numbers in decision making. If an organization has a list of 10 expected threats, it can then prioritize the threats and address the most serious threats first. This prioritization enables management to focus their resources where it will do the most good.

For example, suppose an organization has the following list of threats and costs as the product of performing a quantitative risk analysis:

- Insider network abuse: $1,000,000 in lost productivity
- Data input error: $500,000
- Worm outbreak: $100,000
- Viruses: $10,000
- Laptop theft: $10,000

Decision makers could easily decide that it is of greatest benefit to address insider network abuse and leave the antivirus solution alone. They could also find it easy to support a $200,000 URL filtering solution to address insider network abuse and reject a $40,000 solution designed to enhance laptop safety. Without these numbers from a risk analysis, the decisions made would likely differ.

Building Blocks of Risk Analysis

Conducting a risk analysis starts with the gathering of pertinent information. The building blocks of the process follow the definition of risk used in this book: the organizational impact of threat vectors exploiting vulnerabilities of the assets you are trying to protect.

In that sense, the initial information gathering, in preparation for the risk calculations described in the previous example, should collect and define the following:

- Assets and their value: This information, shown in Table 1-1, is typically obtained from data classification, inventories of assets, and other sources. A general principle is to use discrete numerical values for the exposure factor (EF) based on discrete values that reflect the impact of losing the asset. These values are generally based on data classification techniques (confidential, secret, top secret, and so on), and the impact is based on organizationally relevant criteria (replacement cost, liability, and so on).

  Table 1-1. List of Assets and Their Value

	Confidentiality	Integrity	Availability
Low Value	Limited effect	Limited effect	Limited effect
Moderate Value	Serious effect	Serious effect	Serious effect
High Value	Severe effect	Severed effect	Severe effect

- Vulnerabilities: This information is typically gathered from vulnerability assessments, which will be discussed further later in this chapter. Several tools are available, like Nessus and other commercial vulnerability assessment products. The use of public- or platform-specific vulnerability classification databases is commonplace. They include the Common Vulnerabilities and Exposures (CVE) effort by MITRE, and the National Vulnerability Database (NVD) sponsored by the

National Institute of Standards and Technology (NIST),. An example of vulnerability categorization is shown in Table 1-2.

Table 1-2. Example of Vulnerability Categorization Headings

Risk Scores

With asset, vulnerability, and threat components defined, risk scores are obtained by applying formulas of quantitative risk analysis. Below illustrates the process.

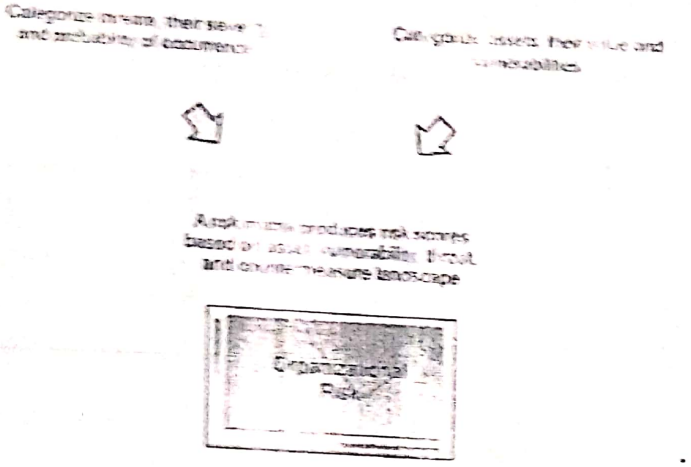

Figure Obtaining a Risk Score

A risk matrix is then calculated, including risk scores for assets and groups of assets and, ideally, an organization risk score that can be used in security monitoring, incident response, and policy reviews. These risk scores provide an idea of the landscape of assets, threats, vulnerabilities, and countermeasures, the components of risk, at a given point in time.

A Lifecycle Approach to Risk Management

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization, including the following:

- Senior leaders and executives who provide the strategic vision and top-level goals and objectives for the organization
- Midlevel leaders who plan, execute, and manage projects
- Individuals who operate the information systems supporting the organization's mission and business functions

Figure below shows that risk management is a comprehensive process that requires organizations to do the following:

- Frame risk (that is, establish the context for risk-based decisions)
- Assess risk
- Respond to risk once determined
- Monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations

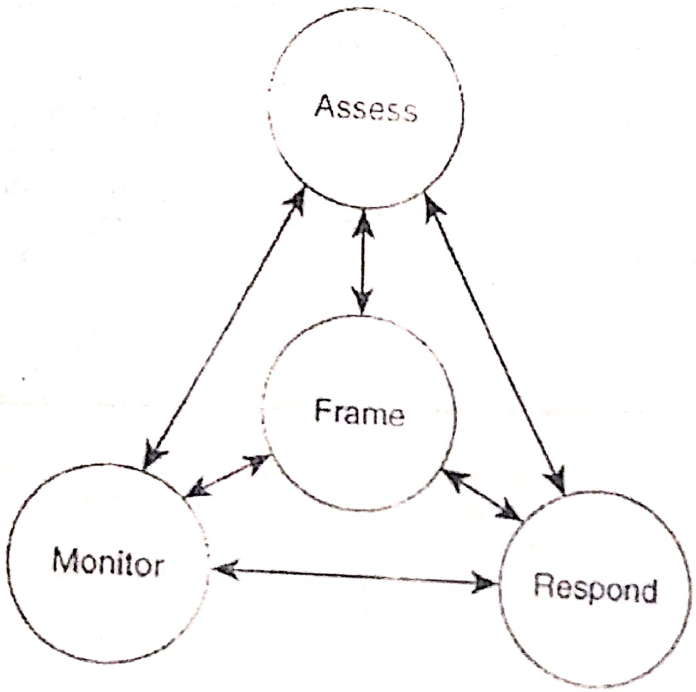

Figure. Lifecycle Approach to Risk Management According to NIST 800-39

Source: NIST 800-39, 2011

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level. Approaching risk management in this way ensures that risk-based decision making is integrated into every aspect of the organization.

Regulatory Compliance

Compliance regulations have been a major driver for security in organizations of all kinds, and the following trends have emerged over the past decade:

- Strengthened enforcement
- Global spread of data breach notification laws
- More prescriptive regulations
- Growing requirements regarding third parties (business partners)

- Risk-based compliance on the rise
- Compliance process streamlined and automated

The compliance regulation defines not only the scope and parameters for the risk and security architectures of an organization, but also the liability for those who do not comply. Recently there have been major shifts in the compliance landscape:

- Although enforcement of existing regulations has been weak in many jurisdictions worldwide, regulators and standards bodies are now tightening enforcement through expanded powers, higher penalties, and harsh enforcement actions.
- In the future, it will be more difficult to hide information security failings wherever organizations do business. Legislators are forcing transparency through the introduction of breach notification laws in Europe, Asia, and North America as data breach disclosure becomes a global principle.
- As more regulations are introduced, there is a trend toward increasingly prescriptive rules. For example, laws in the states of Massachusetts and Nevada, which went into effect in 2010, apply not only to companies based in these states but also to all external organizations that manage the personal information of these states' residents.
- Regulators are also making it clear that enterprises are responsible for ensuring the protection of their data when it is being processed by a business partner, including cloud service providers.
- For many organizations, stricter compliance could help focus management attention on security; but if they take a "check-list approach" to compliance, it will detract from actually managing risk and may not improve security.
- The new compliance landscape will increase costs and risks. For example, it takes time and resources to substantiate compliance. Increased requirements for service providers give rise to more third-party risks.
- With more transparency, there are now greater consequences for data breaches. For example, expect to see more litigation as customers and business partners seek compensation for compromised data. But the harshest judgments will likely come from the court of public opinion—with the potential to permanently damage the reputation of an enterprise.

CH7

V.V.I.

Physical security measures every organization should take

Every general computer networking class teaches the OSI and/or DoD networking models, and we all learn that everything begins at the bottom, with the physical level. Likewise, when it comes to IT security, physical security is the foundation for our overall strategy. But some organizations, distracted by the more sophisticated features of software-based security products, may overlook the importance of ensuring that the network and its components have been protected at the physical level.

In this article, we'll take a look at 10 of the most essential security measures you should implement now, if you haven't already done so.

#1: Lock up the server room

Even before you lock down the servers, in fact, before you even turn them on for the first time, you should ensure that there are good locks on the server room door. Of course, the best lock in the world does no good if it isn't used, so you also need policies requiring that those doors be locked any time the room is unoccupied, and the policies should set out who has the key or keycode to get in.

The server room is the heart of your physical network, and someone with physical access to the servers, switches, routers, cables and other devices in that room can do enormous damage.

#2: Set up surveillance → (Smart card, Camera)

Locking the door to the server room is a good first step, but someone could break in, or someone who has authorized access could misuse that authority. You need a way to know who goes in and out and when. A log book for signing in and out is the most elemental way to accomplish this, but it has a lot of drawbacks. A person with malicious intent is likely to just bypass it.

A better solution than the log book is an authentication system incorporated into the locking devices, so that a smart card, token, or biometric scan is required to unlock the doors, and a record is made of the identity of each person who enters.

A video surveillance camera, placed in a location that makes it difficult to tamper with or disable (or even to find) but gives a good view of persons entering and leaving should supplement the log book or electronic access system. Surveillance cams can monitor continuously, or they can use motion detection technology to record only when someone is moving about. They can even be set up to send e-mail or cell phone notification if motion is detected when it shouldn't be (such as after hours).

#3: Make sure the most vulnerable devices are in that locked room

Remember, it's not just the servers you have to worry about. A hacker can plug a laptop into a hub and use sniffer software to capture data traveling across the network. Make sure that as many of your network devices as possible are in that locked room, or if they need to be in a different area, in a locked closet elsewhere in the building.

#4: Use rack mount servers

Rack mount servers not only take up less server room real estate; they are also easier to secure. Although smaller and arguably lighter than (some) tower systems, they can easily be locked into closed racks that, once loaded with several servers, can then be bolted to the floor, making the entire package almost impossible to move, much less to steal.

#5: Don't forget the workstations

Hackers can use any unsecured computer that's connected to the network to access or delete information that's important to your business. Workstations at unoccupied desks or in empty offices (such as those used by employees who are on vacation or have left the company and not yet been replaced) or at locations easily accessible to outsiders, such as the front receptionist's desk, are particularly vulnerable.

Disconnect and/or remove computers that aren't being used and/or lock the doors of empty offices, including those that are temporarily empty while an employee is at lunch or out sick. Equip computers that must remain in open areas, sometimes out of view of employees, with smart card or biometric readers so that it's more difficult for unauthorized persons to log on.

#6: Keep intruders from opening the case

Both servers and workstations should be protected from thieves who can open the case and grab the hard drive. It's much easier to make off with a hard disk in your pocket than to carry a full tower off the premises. Many computers come with case locks to prevent opening the case without a key.

You can get locking kits from a variety of sources for very low cost, such as the one at Innovative Security Products.

#7: Protect the portables

Laptops and handheld computers pose special physical security risks. A thief can easily steal the entire computer, including any data stored on its disk as well as network logon passwords that may be saved. If employees use laptops at their desks, they should take them with them when they leave or secure them to a permanent fixture with a cable lock, such as the one at PC Guardian.

Handhelds can be locked in a drawer or safe or just slipped into a pocket and carried on your person when you leave the area. Motion sensing alarms such as the one at SecurityKit.com are also available to alert you if your portable is moved.

For portables that contain sensitive information, full disk encryption, biometric readers, and software that "phones home" if the stolen laptop connects to the Internet can supplement physical precautions.

#8: Pack up the backups

Backing up important data is an essential element in disaster recovery, but don't forget that the information on those backup tapes, disks, or discs can be stolen and used by someone outside the company. Many IT administrators keep the backups next to the server in the server room. They should be locked in a drawer or safe at the very least. Ideally, a set of backups should be kept off site, and you must take care to ensure that they are secured in that offsite location.

Don't overlook the fact that some workers may back up their work on floppy disks, USB keys, or external hard disks. If this practice is allowed or encouraged, be sure to have policies requiring that the backups be locked up at all times.

#9: Disable the drives

If you don't want employees copying company information to removable media, you can disable or remove floppy drives, USB ports, and other means of connecting external drives. Simply disconnecting the cables may not deter technically savvy workers. Some organizations go so far as to fill ports with glue or other substances to permanently prevent their use, although there are software mechanisms that disallow it. Disk locks, such as the one at SecurityKit.com, can be inserted into floppy drives on those computers that still have them to lock out other diskettes.

#10: Protect your printers

You might not think about printers posing a security risk, but many of today's printers store document contents in their own on-board memories. If a hacker steals the printer and accesses that memory, he or she may be able to make copies of recently printed documents. Printers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them.

Also think about the physical security of documents that workers print out, especially extra copies or copies that don't print perfectly and may be just abandoned at the printer or thrown intact into the trash can where they can be retrieved. It's best to implement a policy of immediately shredding any unwanted printed documents, even those that don't contain confidential information. This establishes a habit and frees the end user of the responsibility for determining whether a document should be shredded.

Summary

Remember that network security starts at the physical level. All the firewalls in the world won't stop an intruder who is able to gain physical access to your network and computers, so lock up as well as lock down.