Network Intrusion Detection:

Know What You Do (Not) Need

By Tarlok Birdi, CCNP, CCSE, CISSP, and Kees Jansen, CISA, CISSP, PMP

Virus attacks, unauthorized access, theft of information and denial-of-service attacks were the greatest contributors to computer crime losses in 2005.[1] The three most popular security technologies implemented by organizations to reduce the exposure to these threats are firewalls, antivirus software and intrusion detection systems (IDSs); with 72 percent of companies using IDS technologies.[2] Despite the implementation of these security technologies, the number of organizations experiencing incidents from the outside has increased from 58 percent in 2000 to 65 percent in 2005.[3]

With the increase in information security incidents, and despite the application of IDS technologies, management needs to understand:

- The role of IDSs in reducing risks, and the alignment required with intrusion prevention and vulnerability management strategies
- The different technology, process and people components required to make an IDS effective
- The different types of technologies and how effectively they reduce the risk of certain threats
- The intrusion and detection features and capabilities in existing technologies that could be leveraged before investing in intrusion detection technologies
- The need for an enterprisewide intrusion detection strategy and vision based on a thorough understanding of the risks and control embedded in the existing environment
- The need to review the implementation and operational effectiveness after acquiring and implementing the intrusion detection technologies, or if the organizational risk and control environment changes

Organizations may have a false sense of protection from the investments made in their intrusion detection technologies because the solution implemented, for example, may be a point solution that does not alert the organization to risks that management expects to be reported; may be configured inadequately, resulting in too many false positives and diminished accuracy over time; may not have sufficient resources allocated to monitor the reports; or may lack supporting processes to identify and respond to incidents in a timely manner.

This article primarily focuses on network-based intrusion detection. It provides an overview of network intrusion detection components and summarizes a proven approach used to develop network intrusion detection strategies that helps business management to make technology-related decisions.

The Need for Intrusion Detection

The number of organizations experiencing information security incidents has increased, and these incidents contribute significantly to computer crime losses. In addition to the actual losses, there are a variety of business, regulatory and IT drivers that trigger organizations to pay attention to or revisit their network intrusion detection. These include:

- Strategic business changes—Organizations may have initiatives to improve competitiveness in the marketplace through increased web presence, e-commerce, integration with business partners, mergers and acquisitions, etc.
- Legal and regulatory requirements—Legal and regulatory requirements in the electronic environment have evolved over the last few decades and are anticipated to further develop as use of electronic systems evolves. Most recently, there have been accounting regulations (e.g., Sarbanes-Oxley and Bill 198), privacy legislation (e.g., the Health Insurance Portability and Accountability Act and the Personal Information Protection and Electronic Documents Act) and court rulings regarding forensic evidence.
- Managing public and stakeholder expectations—Many organizations have been affected by major or minor computer incidents. These incidents have resulted in exposure of confidential information, unavailability of systems and unreliable information.
- Dependency on information systems—Information systems have become more important and, as a result, the cost of an outage has increased. Timely detection of and response to an outage can save significant amounts of money.
- The increased number and sophistication of network threats—Network-based threats have increased significantly year after year. These threats include viruses, hacking, Trojan horses, unauthorized system changes, denial of service, brute force, social engineering, spyware and spam. The sources of these threats are either internal (e.g., employees, contractors) or external, and make use of system vulnerabilities and human errors (e.g., misconfiguration, lack of user education).

These drivers change the risk landscape of organizations; hence, the control environment needs to be reevaluated to adapt to the new environment. It is important for organizations to recognize when to (re)evaluate the need for an IDS and then revise the intrusion detection strategy. To develop a strategy that meets the organization's needs, the different components of an IDS need to be understood. This helps avoid a strategy that is too narrowly focused and that may not result in effective logging, monitoring and reporting.

Intrusion Detection Components

A comprehensive intrusion detection and prevention program relates to a wide variety of threats that may leverage weaknesses in different technology layers (e.g., business applications, operating systems and network), people (e.g., awareness regarding social engineering) and processes (e.g., incident identification and response processes). Network intrusion detection, however, is directed toward network-based attacks that come from outside and inside the organization. To have network intrusion detection functioning effectively, there are some people and process aspects that need to be established, but, where possible, the comprehensive intrusion detection and prevention program or business continuity plan should be leveraged.

Network IDSs must consist of technology, processes and people to function effectively. Although there is often emphasis on the technology component to increase the efficiency and effectiveness of network logging, monitoring and reporting, the technology will not function effectively without the supporting organizational infrastructure.

Processes: Incident Detection and Response

The processes for incident detection and response need to be closely aligned with the disaster planning processes that typically cover the five Rs:

- Risk analysis and management, to direct continuity plans to the highest risk areas and implement measures that balance cost and risk
- Response to an event, which confirms the occurrence of an incident and its significance
- Resumption of the critical function, which ensures that the impacted critical business functions can resume, often in an alternative way
- Recovery of the activity, which provides for running the business function through the regular set of processes and support of technology
- Restoration of the critical activities and other business functions, which provides for full restoration of operations, including elimination of backlog that occurred during the event

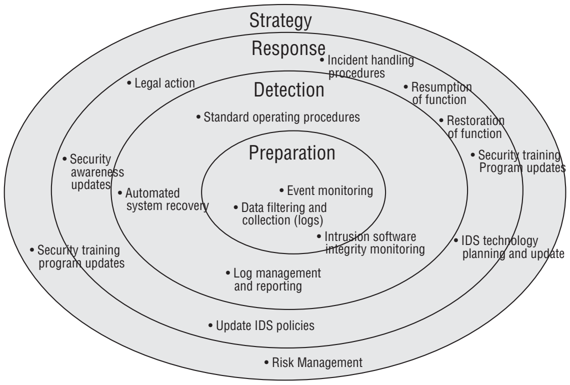
As the network-based threats are a subset of the threats considered during the disaster recovery process, leveraging and building upon processes developed for disaster recovery is recommended.

The processes for intrusion detection will focus on determining the strategy and architecture, developing processes to detect and respond to incidents, and preparing the technology environment (see **figure 1**).

Strategy

The intrusion detection strategy needs to be based on risk management analysis and practices. This includes conducting a threat and risk analysis and business impact assessment to provide direction for the intrusion detection strategy. The strategy process should be reinitiated based on changes in the IT or business environment, technology developments, or incidents that may have occurred. The tactical plans for intrusion detection software upgrades and updates should be established, as they are for any other technology. Finally, plans to enhance awareness and capabilities for end users and system administrators to, where possible, prevent incidents, identify incidents and respond in line with the organizational standards and procedures, are critical. The people aspect is often a weak link.

Figure 1—Processes for Intrusion Detection


Strategy
Response
• Incident handling procedures
• Legal action
Detection
• Resumption of function
• Standard operating procedures
• Restoration of function
Preparation
• Security awareness updates
• Security training Program updates
• Event monitoring
• Automated system recovery
• Data filtering and collection (logs)
• Intrusion software integrity monitoring
• Security training program updates
• IDS technology planning and update
• Log management and reporting
• Update IDS policies
• Risk Management

Detection and Response

The operational model for monitoring and reporting needs to be established. The basis will be an incident response policy that provides direction and management commitment toward adequate responses. Based on the policy, the organization must establish operating standards and procedures for:

- Logging—What needs to be logged, where will the log be kept, how often will it be backed up, how long will it be archived, etc.?
- Monitoring—What types of incidents or trends will be monitored, and how will information be correlated to identify potential threats?
- Reporting—What will be reported, how often, and what are the escalation procedures?
- Change management and access control—Who can configure changes on the IDS, and what mechanisms are in place to control changes?

In addition to the operational, day-to-day procedures, special procedures should be established to handle incidents. Incident procedures will cover areas such as:

- Determining the severity, extent and damage of an incident
- Establishing communication and escalation protocols
- Preserving evidence and establishing a chain of evidence
- Assessing whether law enforcement is required (Organizations often do not report intrusions to law enforcement. The two major reasons are that negative publicity could hurt stock prices and the company's image, and competitors could use it to their advantage.[4])
- Containing the incident by disconnecting systems and eliminating exposures
- Resuming and continuing business functions
- Restoring systems
- Undergoing postmortem analysis

Preparation

Intrusion detection technologies need to be configured based on organizational standards that relate to events that need to be logged and monitored and the type of correlation that needs to occur for reporting purposes. As part of the preparation, it is important that backup and recovery procedures for the IT systems be established and tested periodically. Often, the implementation of an IDS requires higher standards for capturing and storing log information. Hence, the requirements for backup and storage need to be defined as part of the intrusion detection architecture.

Although an IDS provides for capabilities to efficiently monitor systems, these systems still require capable resources to review reports and take appropriate follow-up steps. As many companies have not matured from a reactive level of monitoring (or none at all), the investment in IDSs will often result in additional resource efforts for monitoring activities. Without those resources to operate and review the IDS, the investment may not pay off.

Network IDS Technology Components

Network intrusion detection features are present in the following components:

- Network IDS—Network-based attacks that are detected by a network IDS may be the result of router ACL misconfiguration, ineffectiveness or even compromise. Therefore, alerts from the network IDS should be taken seriously.
- Inline network IDS mechanism—Inline network IDSs are effective in protecting perimeter servers. As such, these devices are capable of detecting and dropping most common application-based attacks. Most common denial-of service-attacks, such as SYN attacks, will be detected and discontinued. Therefore, inline network IDSs are recommended as a first-line level of network and application protection for the network.
- File integrity—If configured correctly, file integrity sensors are effective in detecting tampering of the system, because they can detect changes to files or system files that should not normally undergo changes.
- Server security event monitors—Server security monitors (host IDSs) are effective at detecting misuse of a critical server. To provide "defense in depth," such systems provide effective monitoring of system tampering.
- Application/IPS gateway—Network layer devices, such as routers and switches, can look at only layers four and below. Application gateways are required so traffic can be inspected at upper layers (five to seven). This provides deep inspection of application and protocol fields, and ensures that the specific application is being used in conformance to RFC standards and does not contain any malicious code. Application/IPS gateways provide an additional level of defense for applications that cannot be inspected by network IDSs or inline network IDSs.
- Network/wireless IDSs—Network IDSs can be used to augment policy-based routing and access control. Since IDSs are effective at determining network traffic, such systems can be baselined to detect deviation from what is seen as "normal" traffic. Another component is a wireless LAN IDS. Such a system is capable of detecting rogue wireless LANs, wireless intruders and attackers, and network vulnerabilities.
- Router/access server logging—Logging on the router or access server is critical for monitoring remote access services. Access servers have the ability to record the telephone number of all incoming calls, although this also depends on the subscriber service provided by the public switch telephone network (PSTN) provider. As a result, most consistent attempts to war-dial these networks can be detected. If an organization subscribes to an applicable caller ID service, these attacks can be tracked to specific dial-up numbers, which becomes valuable for investigation efforts.
- Router logging—It is recommended that external choke routers be monitored for unauthorized changes, system utilization (for denial-of-service attacks) and attacks against itself. Typically, routers should have access lists to protect themselves. Protection of the internal and perimeter network should be entrusted to firewalls. Therefore, it is recommended that routers log only attacks against them. This will free up CPU cycles on the router to perform routing.

In addition to these specific network intrusion detection technologies, there may be a need to provide comprehensive correlation and reporting functions to detect threat trends and incidents. This will be of particular interest to management, which will not necessarily be interested in and familiar with the detailed data from the intrusion system components.

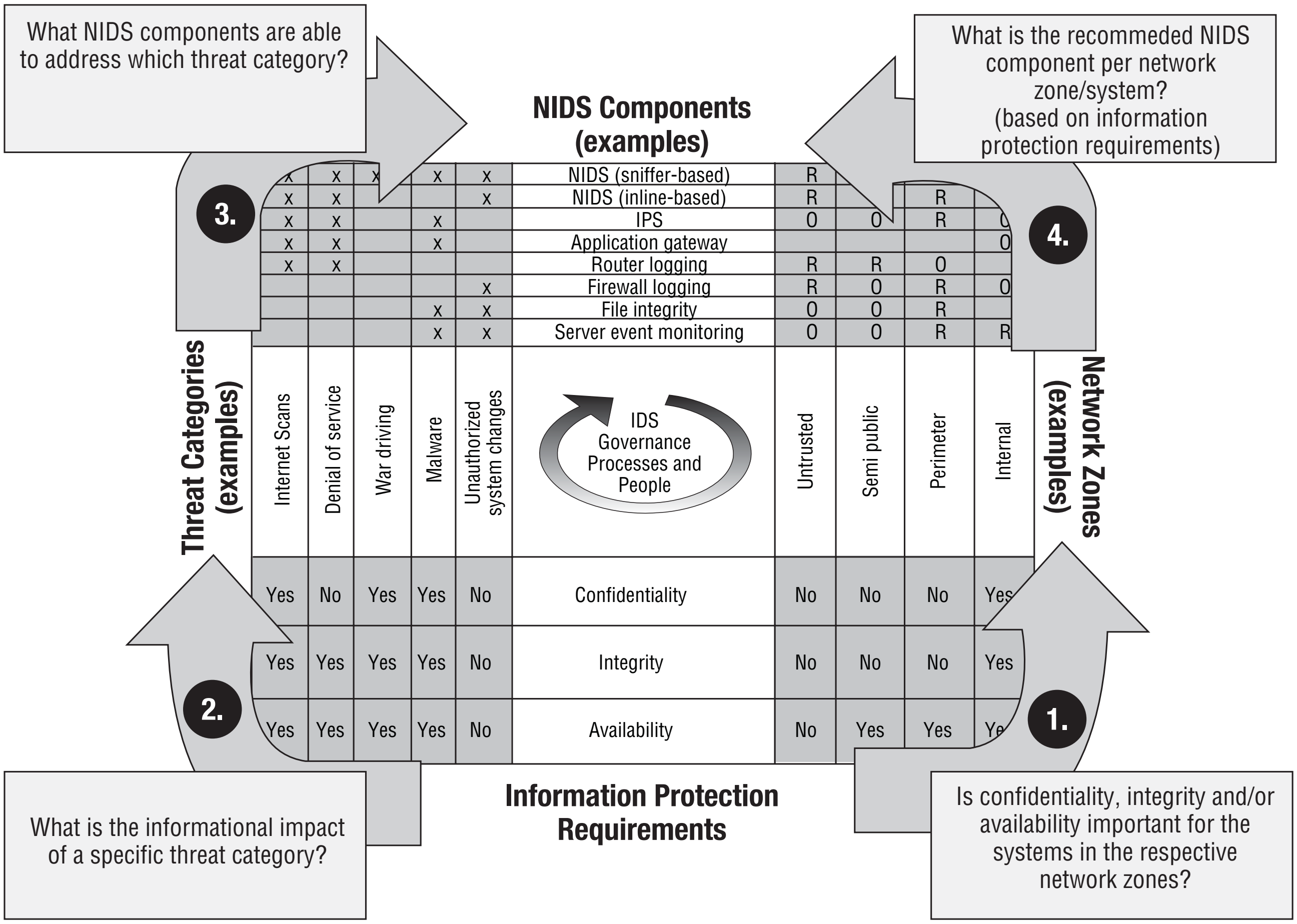
Defining the Intrusion Detection Strategy

With the wide variety of network intrusion detection technologies in the marketplace, organizations often do not know where to start, what to implement and how much to implement. Management often does not know the technical background of the network and most likely is not familiar with the breadth, depth and types of the intrusion detection technologies. This unfamiliarity does not stand in the way of developing an intrusion detection strategy. Actually, organizations should take a business-driven, rather than a technology-driven, approach. Using a business-driven approach to analyze the requirements and need for a network IDS will help determine the business needs and will also provide a mechanism to communicate more effectively with management.

Determining the right types of technology and placing them at key points within the network can be accomplished by a four-step proven approach that works from the information requirements to the network intrusion detection components (see **figure 2**). The steps are described in more detail below:

1. **Define information protection requirements.** A network IDS is primarily used to protect the availability, confidentiality and integrity of information for the network layer. Therefore, the business requirements for information protection need to be defined. Many organizations already have formal or informal requirements, or even a data classification control scheme established. Based on the business requirements for confidentiality, integrity and availability, networks can be zoned into segments. A zone contains a group of systems with a similar set of control requirements.

Figure 2—Network IDS Components (Examples)



NIDS Components (examples)
Threat Categories (examples)
Network Zones (examples)
Information Protection Requirements
IDS Governance Processes and People
1.
2.
3.
4.

Internet Scans	Denial of service	War driving	Malware	Unauthorized system changes		Untrusted	Semi public	Perimeter	Internal
x	x	x	x	x	NIDS (sniffer-based)	R			
x	x			x	NIDS (inline-based)	R		R	
x	x		x		IPS	O	O	R	O
x	x		x		Application gateway				O
x	x				Router logging	R	R	O	
				x	Firewall logging	R	O	R	O
			x	x	File integrity	O	O	R	
			x	x	Server event monitoring	O	O	R	R
Yes	No	Yes	Yes	No	Confidentiality	No	No	No	Yes
Yes	Yes	Yes	Yes	No	Integrity	No	No	No	Yes
Yes	Yes	Yes	Yes	No	Availability	No	Yes	Yes	Ye

What NIDS components are able to address which threat category?

What is the recommeded NIDS component per network zone/system? (based on information protection requirements)

What is the informational impact of a specific threat category?

Is confidentiality, integrity and/or availability important for the systems in the respective network zones?

2. **Define threats**. A part of a threat and risk analysis, the network-based threats need to be identified, including their impact on confidentiality, integrity and availability. To understand the need for and value of a network IDS for the organization, the existing controls to mitigate the occurrence of a threat event and the business impact (e.g., impact on revenue, expenses, image) have to be identified. If mitigating controls exist for certain threat categories, the need for a network IDS control may be minimal unless control efficiencies can be gained through the implementation of a network IDS.

   IT auditors are uniquely positioned to play an important role during this stage of the network IDS strategy process, as they have a broad understanding of the threats and risks, potential business impacts, IT control environment, and mechanisms in place for and effectiveness of compensating controls.
3. **Identify which network intrusion detection system types will mitigate the threat categories.** Different types of network IDSs will mitigate risk exposures from different threat types. To evaluate the types of technology required, the threat categories need to be mapped to the network IDS component capabilities. Some vendor products will support multiple types of network IDSs, whereas others are focused on one type. The selection of actual products and vendors is during a later stage, after the network IDS strategy and architecture are defined.
4. **Identify the required network IDS for the organization.** Based on the threat categories a network IDS component covers, the potential business impact, the information protection requirements for a network zone and the existing controls in network zones, an organization can determine the types of network IDS components that are required (R), optional for the short term (O) or not required for the longer term (NR).

   In addition to determining the types of network IDS components, the number of network IDS agents needs to be defined. Dependent on the complexity, number of systems in a zone and criticality of those systems, the number of network IDS agents will vary and impact the budget.

Dependent on the risk appetite of an organization, an organization can choose to first select those components that address the highest risk threat categories.

As part of this step in the process the IT auditor should be aware of the risks that management is accepting and ensure that management is properly informed about those risks.

Closing Thoughts

Increasingly, organizations are experiencing information security incidents from the outside, despite 72 percent of organizations having implemented some form of intrusion detection mechanism. A variety of reasons contribute to this exposure, varying from increased sophistication of attacks to inadequate selection and implementation of a comprehensive IDS. A comprehensive IDS needs to consider the people and process components in addition to the technology aspect. The last thing an organization needs is another technology that is not implemented or is used ineffectively due to a lack of resources and supporting organizational infrastructure, and hence provides a false sense of control.

Intrusion detection strategies are often technology-driven without input and direction from the business. This will not only affect the effectiveness of the solutions, as it will most likely not consider the potential threats, the integration and place within the business and IT control environment (e.g., alignment with business continuity plans/disaster recovery plans and understanding of existing compensating controls), and their significance on business risks, but it will also inhibit the effective communication with management. Management will not necessarily understand how networks function and what the different types of intrusion detection technologies can do, but they will understand business risks and information protection requirements. Therefore, a business-driven approach will provide a solid foundation and buy-in for the intrusion detection strategy. The implementation of the strategy will be effective only if the process (e.g., operating and incident response procedures) and people (e.g., sufficient monitoring resources) aspects are integrated. If the organization's resources do not include time to monitor system logs in the current situation, do not expect that the implementation of intrusion detection technologies will enhance the protection of the organization. Resources will be required to proactively monitor the intrusion detection reports. Many companies are primarily reactive to incidents and make resources available to respond based on the severity of the incident. By the time of response, incidents have often impacted the organization and its business function significantly. The threat and risk analysis that is part of the business-driven strategy development approach will evaluate the risks vs. costs and provide justification for the level of investment required in the people, process and technology components of an IDS.

Tarlok Birdi, CISSP, CCNP, CCSE
is a manager in the enterprise risk service practice of Deloitte in Vancouver (Canada). Birdi is an experienced network security engineer with more than 11 years of experience in the IT field. He has been providing infrastructure and communication security solutions for enterprise, health and telecommunication markets throughout North America. For questions, he can be contacted at *tbirdi@deloitte.ca*.

Kees Jansen, CISA, CISSP, PMP
is a senior manager in the enterprise risk service practice of Deloitte in Vancouver (Canada). He has been an IT professional for more than 11 years and has in-depth experience as project manager and integrity and security consultant with technical infrastructure and application implementations. He has advised many medium-sized and *Fortune* 500 organizations in North and South America and Europe. For questions, he can be contacted at *kjansen@deloitte.ca*.

Endnotes

[1] Source: Computer Security Institute/Federal Bureau of Investigation (CSI/FBI), Computer Crime and Security Survey, USA, 2005

[2] *Ibid*.

[3] *Ibid*.

[4] *Ibid*.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal. Information Systems Control Journal* does not attest to the originality of authors' content.

www.isaca.org