

# The Evolution of Intrusion Detection Systems

Paul Innella 2001-11-16

## The Evolution of Intrusion Detection Systems

by Paul Innella, Tetrad Digital Integrity, LLC

last updated November 16, 2001

---

### Introduction

I am currently working with a client who asked me to choose an intrusion detection system (IDS) to deploy in their environment. I have been working with intrusion detection since it was virtually unknown, so it would seem the decision would be quite simple. On the contrary, with all of the different components and vendors to choose from, IDS offerings have become pretty complex. That led me to wonder how IDS technology has progressed to its current state. So, I invested some time trying to figure it out. Now that I have, let me tell you, it is enough to induce a headache. Nonetheless, I wrote this article to share my findings with you. If you are ready for a discussion about the evolution of IDS, then read on; however, be forewarned, the history of intrusion detection is as confusing as Greenspan's economic strategies.

### IDS Components

Before we get started, let me provide a layman's description of the primary IDS components:

#### Network Intrusion Detection (NID)

Network intrusion detection deals with information passing on the wire between hosts. Typically referred to as "packet-sniffers," network intrusion detection devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP. Once captured, the packets are analyzed in a number of different ways. Some NID devices will simply compare the packet to a signature database consisting of known attacks and malicious packet "fingerprints", while others will look for anomalous packet activity that might indicate malicious behavior. In either case, network intrusion detection should be regarded primarily as a perimeter defense.

NID has historically been incapable of operating in the following environments:

1. Switched networks
2. Encrypted networks
3. High-speed networks (anything over 100 Mbps)

Recently, however, Cisco released a module for their Catalyst 6000 switch that incorporates network intrusion detection directly in the switch, overcoming the first of these flaws. Additionally, ISS/Network ICE indicated that they are now capable of "packet-sniffing" at gigabit speeds.

#### Host-based Intrusion Detection (HID)

Host-based intrusion detection systems are designed to monitor, detect, and respond to user and system activity and attacks on a given host. Some more robust tools also offer audit policy management and centralization, supply data

forensics, statistical analysis and evidentiary support, and in certain instances provide some measure of access control. The difference between host-based and network-based intrusion detection is that NID deals with data transmitted from host to host while HID is concerned with what occurs on the hosts themselves.

Host-based intrusion detection is best suited to combat internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host. The majority of computer threats come from within organizations, from many different sources; disgruntled employees and corporate spies are just two examples. In fact, intrusion detection expert Richard Power states, "each year, we've asked the respondents [of the CSI/FBI survey] to rate the likely sources of [a network] attack. Invariably, disgruntled and dishonest employees have topped the list, with over 80% of respondents citing them as a likely source." (Power, 1999: 32.)

## Hybrid Intrusion Detection

Hybrid intrusion detection systems offer management of and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide the logical complement to NID and HID - central intrusion detection management.

## Network-Node Intrusion Detection (NNID)

Network-node intrusion detection was developed to work around the inherent flaws in traditional NID. Network-node pulls the packet-intercepting technology off of the wire and puts it on the host. With NNID, the "packet-sniffer" is positioned in such a way that it captures packets after they reach their final target, the destination host. The packet is then analyzed just as if it were traveling along the network through a conventional "packet-sniffer." This scheme came from a HID-centric assumption that each critical host would already be taking advantage of host-based technology. In this approach, network-node is simply another module that can attach to the HID agent. Network node's major disadvantage is that it only evaluates packets addressed to the host on which it resides. Traditional network intrusion detection, on the other hand, can monitor packets on an entire subnet. Even so, "packet-sniffers" are equally incapable of viewing a complete subnet when the network uses high-speed communications, encryption, or switches since they are essentially "without a sense of smell" (first and last NID joke, I promise.) The advantage to NNID is its ability to defend specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.

## Intrusion Detection Systems: A Brief History

The goal of intrusion detection is to monitor network assets to detect anomalous behavior and misuse. This concept has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity and incorporation into the overall information security infrastructure. Beginning in 1980, with James Anderson's paper, [Computer Security Threat Monitoring and Surveillance](#), the notion of intrusion detection was born. Since then, several pivotal events in IDS technology have advanced intrusion detection to its current state. Let's focus on how IDS has progressed since its inception.

James Anderson's seminal paper, written for a government organization, introduced the notion that audit trails contained vital information that could be valuable in tracking misuse and understanding user behavior. With the release of this paper, the concept of "detecting" misuse and specific user events emerged. His insight into audit data

and its importance led to tremendous improvements in the auditing subsystems of virtually every operating system. Anderson's conjecture also provided the foundation for future intrusion detection system design and development. His work was the start of host-based intrusion detection and IDS in general.

In 1983, [SRI International](#), and specifically Dr. Dorothy Denning, began working on a government project that launched a new effort into intrusion detection development. Their goal was to analyze audit trails from government mainframe computers and create profiles of users based upon their activities. One year later, Dr. Denning helped to develop the first model for intrusion detection, the Intrusion Detection Expert System (IDES), which provided the foundation for the IDS technology development that was soon to follow.

In 1984, SRI also developed a means of tracking and analyzing audit data containing authentication information of users on ARPANET, the original Internet. Soon after, SRI completed a Navy SPAWAR contract with the realization of the first functional intrusion detection system, IDES. Using her research and development work at SRI, Dr. Denning published the decisive work, [An Intrusion Detection Model](#), which revealed the necessary information for commercial intrusion detection system development. Her paper is the basis for most of the work in IDS that followed.

Meanwhile, there were other significant advances occurring at University of California Davis' [Lawrence Livermore Laboratories](#). In 1988, the Haystack project at Lawrence Livermore Labs released another version of intrusion detection for the US Air Force. This project produced an IDS that analyzed audit data by comparing it with defined patterns. In a telephone interview with the author, Crosby Marks, a former Haystack Project team member and Haystack Labs employee said that, "searching through this large amount of data for one specific misuse was equivalent to looking for a needle in a haystack."

The subsequent iteration of this tool was called the Distributed Intrusion Detection System (DIDS). DIDS augmented the existing solution by tracking client machines as well as the servers it originally monitored. Finally in 1989, the developers from the Haystack project formed the commercial company, Haystack Labs, and released the last generation of the technology, Stalker. Crosby Marks says that "Stalker was a host-based, pattern matching system that included robust search capabilities to manually and automatically query the audit data." The Haystack advances, coupled with the work of SRI and Denning, greatly advanced the development of host-based intrusion detection technologies.

To kick off the '90s, UC Davis's Todd Heberlein introduced the idea of network intrusion detection. In 1990, Heberlein was the primary author and developer of Network Security Monitor (NSM), the first network intrusion detection system ( see Heberlein, L. et al. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp. 296-303.) NSM was deployed at major government installations where network traffic analysis provided massive amounts of information. This new awareness generated more interest in the field of intrusion detection and investments in that market increased significantly. Heberlein's contributions also extended to the DIDS project where, along with the Haystack team, he introduced the first idea of hybrid intrusion detection. The work of the Haystack project and the introduction of the Network Security Monitor revolutionized the IDS field and brought it into the commercial world.

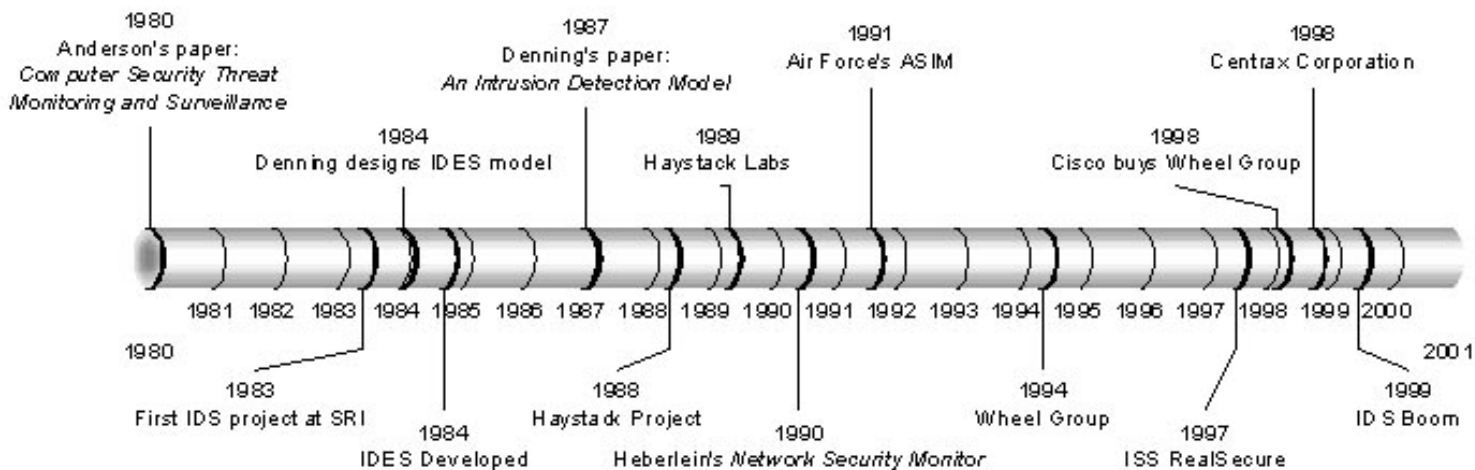
Commercial development of intrusion detection technologies began in the early 1990s. Haystack Labs was the first commercial vendor of IDS tools, with its Stalker line of host-based products. SAIC was also developing a form of host-based intrusion detection, called Computer Misuse Detection System (CMDS). Simultaneously, the Air Force's

Cryptologic Support Center developed the Automated Security Measurement System (ASIM) to monitor network traffic on the US Air Force's network. ASIM made considerable progress in overcoming scalability and portability issues that previously plagued NID products. Additionally, ASIM was the first solution to incorporate both a hardware and software solution to network intrusion detection. ASIM is still currently in use and managed by the [Air Force's Computer Emergency Response Team \(AFCERT\)](#) at locations all over the world. As often happened, the development group on the ASIM project formed a commercial company in 1994, the Wheel Group. Their product, NetRanger, was the first commercially viable network intrusion detection device. Nonetheless, commercial intrusion detection systems developed slowly during these years and only truly blossomed towards the latter half of the decade.

The intrusion detection market began to gain in popularity and truly generate revenues around 1997. In that year, the security market leader, ISS, developed a network intrusion detection system called RealSecure. A year later, Cisco recognized the importance of network intrusion detection and purchased the Wheel Group, attaining a security solution they could provide to their customers. Similarly, the first visible host-based intrusion detection company, Centrax Corporation, emerged as a result of a merger of the development staff from Haystack Labs and the departure of the CMDS team from SAIC. From there, the commercial IDS world expanded its market-base and a roller coaster ride of start-up companies, mergers, and acquisitions ensued. (The next section, *Players*, discusses these developments.)

Currently, market statistics show that IDS is amidst the top selling security vendor technologies and should continue to rise. Furthermore, government initiatives, such as the Federal Intrusion Detection Network, (FIDNet) created under [Presidential Decision Directive 63](#), are also adding impetus to the evolution of IDS. Advancements in IDS will ultimately push security technology into a whole new arena of automated security intelligence.

So what's next? Well, there's application intrusion detection, heuristics and rules-based intrusion detection, incorporation of artificial intelligence, and who knows what else. (If I did I would be working on that instead of writing this article.) Regardless of how intrusion detection technology evolves, one thing is for sure - it is now an important and integral component of information security.



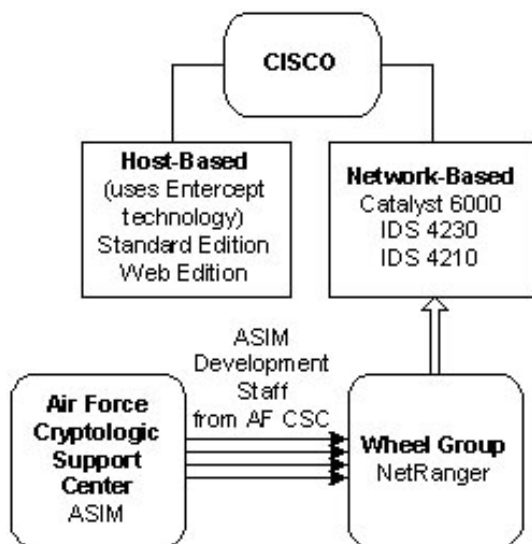
## Players

The IDS market appears to grow and shrink with the stock market. In the February 2000 timeframe there seemed to be a gaggle of IDS vendors, but there are now only a few serious ones remaining. Most have faded away or been

gobbled up by the bigger fish. It is important to note how different intrusion detection vendors' technologies came to be. So, let's review the current players in the market and discuss how they got here.

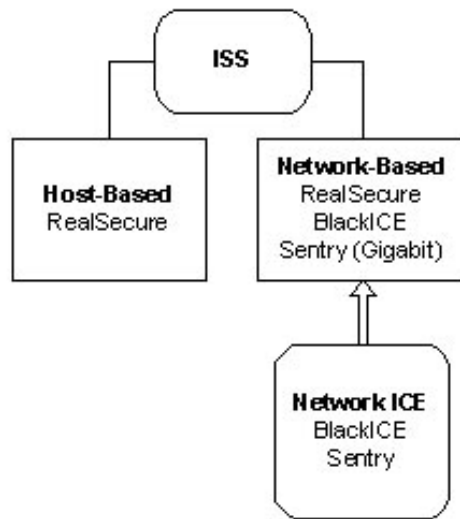
## Cisco

Cisco currently provides both host-based and network-based intrusion detection products. They first entered the IDS market in 1997 by acquiring the Wheel Group and their NetRanger technology for \$124 million. Their IDS 4230 and 4210 series provide typical NID solutions while the Catalyst 6000 module is the first switched-integrated NID offering on the market. On the host-based intrusion detection side, they use Enterccept's technology instead of having developed their own.



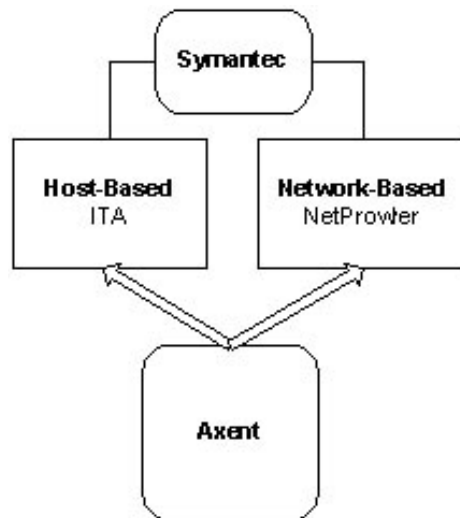
## Internet Security Systems (ISS)

ISS provides both a proprietary hybrid intrusion detection solution and an additional NID system that functions independently of their hybrid offering. ISS ventured into NID with the release of RealSecure, virtually at the same time that CISCO purchased NetRanger. Only two years later, they introduced a host-based component that made their hybrid IDS offering complete. ISS recently made another move towards conquest of the IDS market with the acquisition of Network ICE and their highly respected NID solutions, including their new gigabit NID system.



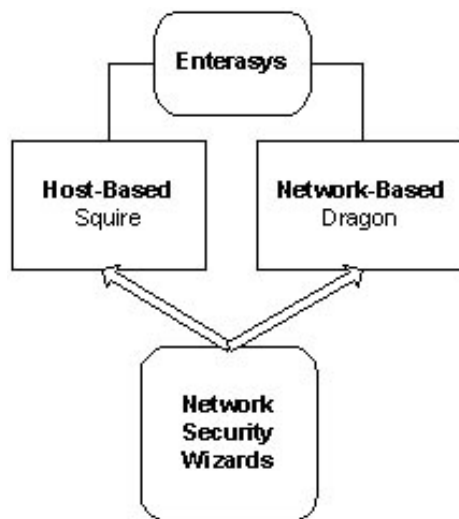
## Symantec

Symantec recently acquired Axent and thus gained their Intruder Alert and NetProwler technologies, bringing them into the IDS market. Symantec offers both NID and HID solutions and a method of providing hybrid integration as well.



## Enterasys

Like Cisco, Enterasys/Cabletron realized that providing bridges and routers was a viable means of subsequently offering intrusion detection. Consequently, Enterasys purchased Network Security Wizards and their Dragon NID solution and Squire HID system.



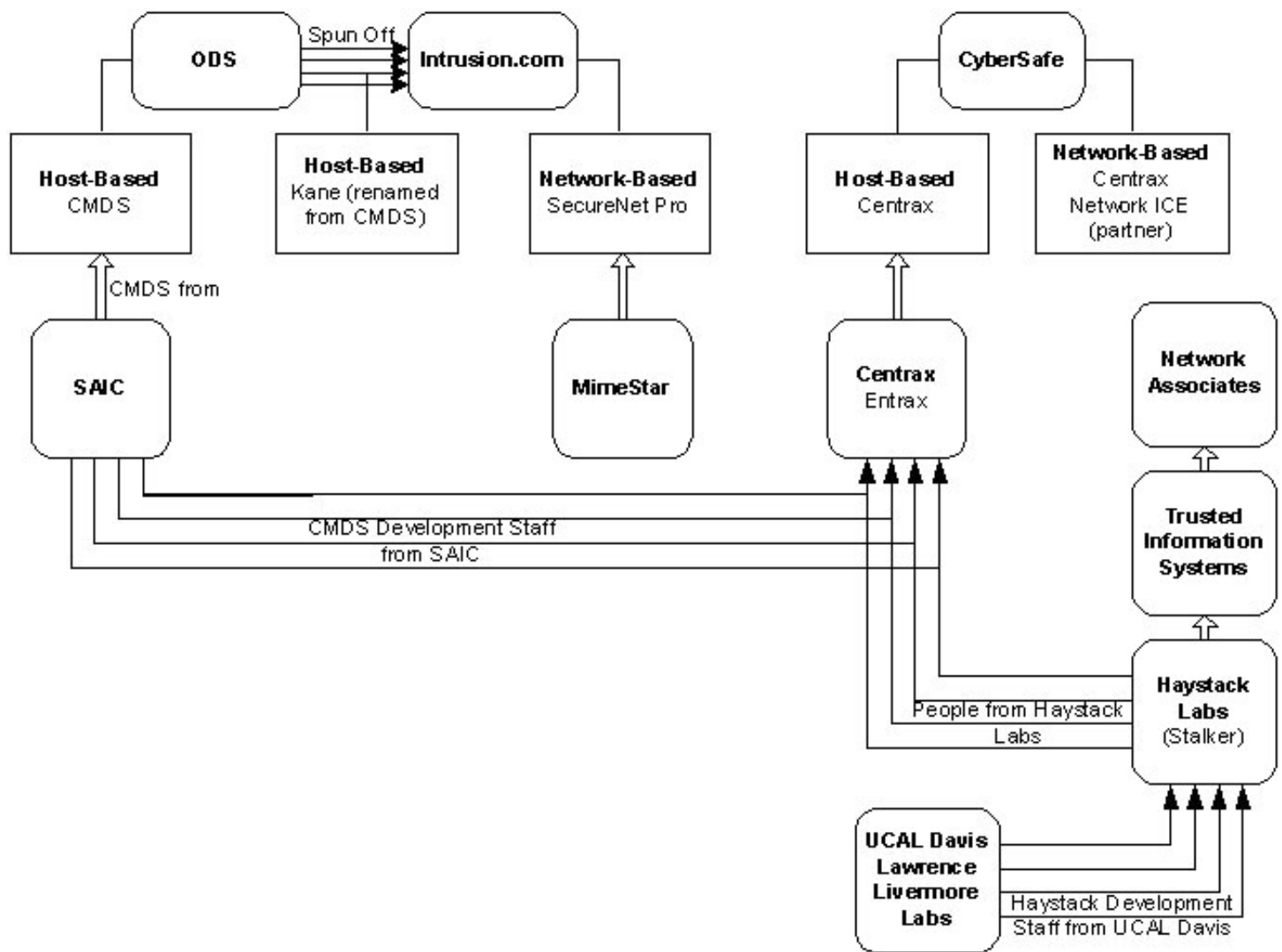
## The Rest

Now, let's discuss the rest of the IDS field. Okay, ready, take a deep breath, and here we go.

We start with the merger of the CMDS development staff from SAIC who went on to start Centrax Corporation along with the people from Haystack Labs. Incidentally, the remainder of Haystack was purchased by Trusted Information Systems, which was then acquired by [Network Associates](#). Centrax Corporation was purchased by CyberSafe Corporation and changed the host-based product, Entrax, into Centrax. Centrax then became the first commercially viable host-based intrusion detection product. CyberSafe later introduced NID followed by NNID technologies into their Centrax product; they even partnered with Network ICE to round out the solution - until ISS bought Network ICE and ended that relationship.

Meanwhile, CMDS moved to its new home when SAIC sold it to ODS, who renamed it to Kane Security Enterprise and then spun off Intrusion.com to better market the product. Intrusion.com then purchased MimeStar, and its SecureNet Pro NID solution, to provide its customers with a total IDS offering.

Okay, you can let it out now - the long and short of this series of spin-offs, acquisitions, mergers, and failures is that the strong seem to get stronger and the number of IDS competitors continue to decrease.



## Conclusion

Summing up, the work of Anderson, Heberlein, and Denning spawned the concept of IDS. Government funding and corporate interest helped to develop their concept into a tangible technology that eventually found its way into the mainstream of network security. Intrusion detection has indeed come a long way, becoming a necessary means of monitoring, detecting, and responding to security threats. From theory to practice, and finally to commercially viable tools, IDS technology has gone through countless iterations and numerous owners. Nonetheless, the use of intrusion detection as a means of deterring misuse has ultimately become commonplace. Moreover, IDS has become essential.

## References

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E., State of the Practice of Intrusion Detection Technologies. CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, January 2000.

Anderson, James P., Computer Security Threat Monitoring and Surveillance. James P. Anderson Co., Fort Washington, Pa., 1980.

D. E. Denning, "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2): 222-232, Feb. 1987.

Heberlein, L. et al. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp. 296-303.

Marks, Crosby, former Haystack Project team member and Haystack Labs employee, telephone interview, September 3, 2001.

Mchugh, J. et al. "Intrusion Detection: Implementation and Operational Issues," Software Engineering Institute Computer Emergency Response Team White Paper, January 2001.

Power, Richard, "1999 CSI/FBI Computer Crime and Security Survey," Computer Security Journal, Volume XV, Number 2, 1999, pp. 32.

Proctor, Paul, The Practical Intrusion Detection Handbook, Prentice Hall, 2001.

Sans Institute, "Intrusion Detection and Vulnerability Testing Tools: What Works" Feb 2001.

Shipley, Greg, "Watching the Watchers: Intrusion Detection," Network Computing, November 13, 2000.

[Paul Innella](#), CISSP, is President of [Tetrad Digital Integrity, LLC](#) a Washington, D.C. based information security services company. Mr. Innella has nearly ten years of experience in the computer industry working at several commercial and government companies as a security engineer, developer, integrator, systems administrator, program manager, and sales engineer. Mr. Innella is a member of the Gerson Lehrman Group Council of Advisors, the CISSP Speakers/SME Bureau, ISSA, and CSI.

[Privacy Statement](#)

Copyright 2006, SecurityFocus