

**TALKING**  
CREATES SECURITY PATCHES.  
**DOING**  
CREATES SECURITY SOLUTIONS.



**Mr. Thomas Noonan:** Today's enterprises see security as a growing burden, and one that distracts them from their core business. Just like us, our customers are in business to serve their customers and make money. Internet threats deter them from that goal. Threats take advantage of vulnerabilities. So they're constantly trying to patch. And now, patching, permissions, policies and the overall risk management are being governed by government regulations. IDC and AMR estimate that total spending on compliance in 2006 topped 27 billion dollars last year. That is an enormous amount of money diverted from core business initiatives. But spending on security is up. It's driven almost entirely by the cost of labor required to manage, monitor and integrate all of these stand-alone products.

We know that the threat spectrum will continue to change and evolve, so next generation's security cannot be based on a single threat fact or reactive signature architecture. It's got to be flexible and expand. We know that our infrastructure is going to be vulnerable to something, 7,242 last year. Next year it will be more. We must have systems that are continuously enabled by vulnerability assessment and detection systems that intelligently monitor all aspects of our infrastructure.

**“WHEN YOU PROVIDE A SECURITY PLATFORM THAT OFFERS CHOICE IN TERMS OF TECHNOLOGY AND SERVICE DELIVERY, THEN SECURITY BECOMES A SOLUTION, INSTEAD OF A BUSINESS PROBLEM.”**

Security platforms have to incorporate real-time vulnerability and threat intelligence from analysis gathered within the enterprise, and also from intelligence that's coming from the outside being fed from global monitoring of the Internet. These symptoms are preemptive. That means they're capable of detecting and preventing new threats, and this is

done through deep research. It's done through advance technologies, behavioral technologies and other things through unified management, and most importantly, through on-demand services, which provide a continuously updated source of information to these systems. The ultimate goal is a seamless automation system controlled from the top down and informed from the bottom up.

I'm extremely proud that ISS has become a part of IBM. But I know that it will create value for our industry and our customers. IBM recognized its potential not only to solve the complexity of enterprise security with these integrated solutions for access, identity, vulnerability and threat management, as well as data protection, business continuity, disaster recovery, the continuum of security. So what does this mean for our customers? It provides the first enterprise-wide blueprint for managing security as an integrated control system. It ensures that the system's view of making it all work is designed into the platform, and not left for our customers to figure out. It provides them with choice, and with choice comes control. When you provide a security platform that offers choice in terms of technology and service delivery, then security becomes a solution, instead of a business problem.

With IBM's acquisition of ISS, we are truly entering a period of renaissance, one defined by principled innovation and creativity, designed to solve real problems.

