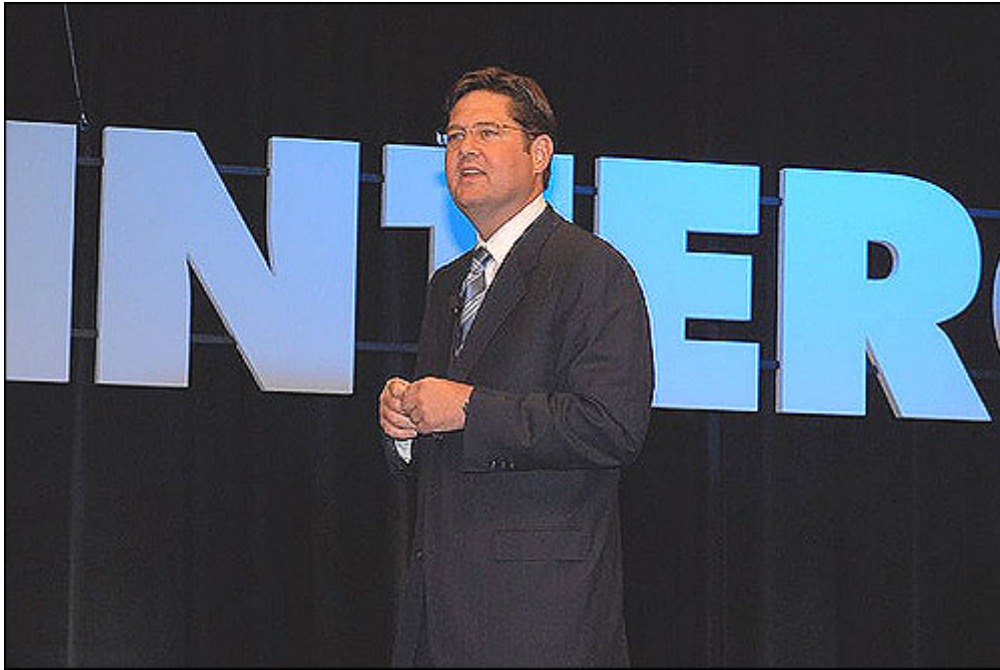




Security Innovation Drives Business Value



**Thomas E. Noonan
General Manager
IBM Internet Security Systems**

2007 Interop Las Vegas Keynote Address

May 22, 2007

First of all, I want to thank all of you for attending today. To tell you the truth, I was a little concerned about today's turnout, and I'll tell you why. It turns out that the people who run Interop are really crafty. They created this split session featuring two mortal competitors: my company -- IBM Internet Security Systems - - and McAfee.



Obviously they're expecting fireworks here today, and for good reason. As some of you may know, McAfee has been targeting our customers with "competitive switch" programs ever since IBM acquired ISS back in October. They've issued press releases offering our customers free software if they switch to McAfee. They've launched direct marketing campaigns offering free software and free appliances. To this day they offer free software to our customers on their home page.

Call me paranoid, but I figured they'd offer Interop attendees free software if they blew off my speech in favor of Dave DeWalt's!

But your presence here tells me one of two things: Either my concerns were unfounded, or you're all smart enough to know there's no such thing as free software. Either way, I'm really happy to be here with you today.

All joking aside...there really *is* no such thing as free software. And this is especially true in security. When the CEO calls you on the carpet to explain why there's been a database breach, I guarantee you that saying "Yeah, but I got the software for free" is not going to help your case. What *would* help your case would be to put in place a security infrastructure that ensures the CEO never needs to know your name.

Achieving that coveted level of anonymity is an extremely hard job. And to date, very few people have cracked the code. Most enterprises have invested enormous sums of money over the past few years in buying appliances, software, servers and systems to protect against every conceivable threat. And yet, most enterprises today are more vulnerable than ever before. Database breaches are in the news every day. Millions of PCs have been compromised



and co-opted for botnets and other purposes. And IT infrastructure has become so complex that enterprises have no idea if they're protected, because they don't know what they need to protect.

On top of this, networking and security personnel are often at odds within IT departments. The networking folks don't want yet another security appliance degrading their speeds and feeds. But the security folks are the ones who will be called on the carpet if there's a breach, or if the Web site goes down from a denial of service attack. And both groups live in constant fear of the dreaded regulatory audit.

Add this all up and you have a real mess. A mess that spans both technology and organizational dynamics. Cleaning it up is partly a question of strategy. Partly a question of technology. But mostly a question of human beings responding in a rational way to the challenge.

We're all familiar with that famous Benjamin Franklin quote about insanity. He said, "The definition of insanity is doing the same thing over and over and expecting different results." We're at that point in our industry – we can't keep approaching security in the same way we have for the past 10 years. If we do, we will guarantee ourselves a future of ever-increasing numbers of attacks causing ever-more severe damage to our businesses, our economy and our country.

The old way of security no longer works. The news headlines confirm that for us. Today we need a **new way**. And that's really what I want to talk about today.



The most important thing to understand about security today is that it is no longer just about protecting your IT assets from bad guys. Security today is about your brand. It's about preserving the ROI of your entire business.

Security used to be about preventing short-term business disruption. It was about stopping virtual vandalism. The bad guys were mostly ego-driven teenage malfeasants. They wanted to make a big splash and then read about it in the papers. That's why attacks were characterized by large distribution volume but low variant frequency. And the tactic worked – the headlines of the early 2000s were rife with the Slammer worm and other “big bang” attacks. In this environment we saw the rise of signature-based anti-malware systems. These are inherently reactive systems, simply because malware must already be in the wild before anyone can develop a signature for it.

In the last two years, however, we have seen a fundamental shift. Malware is no longer propagated by vandals whose goal is to annoy and disrupt. It is propagated by sophisticated criminals whose goal is to steal. And attacks have become much more frequent, with new variants appearing within minutes of each other. In 2006 alone, ISS's X-Force identified and analyzed more than 200,000 distinct malware samples. If you do the math, this means malcode developers unleashed roughly 22 attacks per hour, or about one every three minutes in 2006.

In this environment, the now-ubiquitous threat-signature-based security tools no longer work. They simply cannot react quickly enough to stem the constant assault of variants generated by today's sophisticated malcode developers.

This is a huge problem, because theft causes much graver business consequences than vandalism. In the old days, you could repair the damage



done by vandalism attacks with time and money. With theft, however, the damage runs much deeper. Take a customer database breach, for example. The costs associated with forensics, remediation and customer alerting and compensation are just the beginning. More imposing is the long-term damage resulting from lost customers and brand degradation. In a recent study from Javelin Strategy & Research, 77 percent of consumers surveyed said they will stop shopping at stores that suffer a database breach. Think about that – 77 percent. I can't think of another event that could be so catastrophic to a business.

The writing on the wall is about as clear as it can get: Security isn't just about protecting systems anymore. It's not just about stopping vandalism or even isolated acts of theft. Security is about business.

I've just painted a pretty bleak picture of the state of security. But, wouldn't we really rather focus on this as the glass being half full? Let me explain. History irrefutably shows us that security threats walk hand-in-hand with business opportunity. However, opportunity only smiles on the innovators.

The innovators think beyond the traditional constructs of security. In our industry, that construct is to secure the IT infrastructure. Today's innovators don't think about just protecting the infrastructure. They think about securing their processes. And when you think this way, you understand that network endpoints and process endpoints are not the same thing. You understand that your process endpoints usually reside outside of your network, but you must secure them anyway. Because even though security issues occurring outside of your network are not your fault, they are your problem.



One company that learned this lesson the hard way – but responded brilliantly to the challenge – was Johnson & Johnson. J & J makes Tylenol, and I'm sure all of you remember the big Tylenol scare of 1982. The Tylenol scare occurred in Chicago that year. Some maniac bought a few bottles of Tylenol from the store, put cyanide into some of the capsules, and then put the bottles back in the store. Seven people died from ingesting the tainted medicine and J & J had a huge problem on its hands.

Up to that time, security, as it pertained to Tylenol, was limited to the traditional construct of the manufacturing process. Once those Tylenol capsules were manufactured and bottled correctly, J&J had fulfilled its obligation to deliver a safe product to consumers. Security was no longer a concern.

But when the news broke from Chicago, security became a big concern. It was not J&J's fault that a lunatic tampered with its product and killed seven people, but it was J&J's problem. Tylenol's market share collapsed from 35% to 8% in the weeks following the tampering incident. The survival of the brand was in serious jeopardy.

J&J responded with a brilliant strategy to secure the business process and restore customer trust. First, Tylenol became the first over the counter medicine to come in a triple-sealed package. This multi-layered defense made it almost impossible to access the capsules without making it obvious that tampering had occurred. J&J did not stop there, though. The company quickly innovated on the manufacturing front and replaced Tylenol capsules with caplets. Now, there was a hardened interior to go with the secured perimeter.

As a result of these efforts, consumers began buying Tylenol again. In fact, within one year Tylenol had recaptured its entire market share. And J&J had actually



strengthened consumer trust in its brand. So we see that in the face of a dire security problem, J&J actually turned it into a competitive advantage. How did they do it? By innovating!

The company took a process-centric view of security and found that its process end-point was not the shipping dock. It was the consumer. And to secure this end-point, J&J created the world's first tamper-proof over-the-counter medicine and changed an entire industry. Competitors had no choice but to follow suit, or else Tylenol and other J&J brands would have created an insurmountable competitive advantage.

Now, let's fast-forward to today. Many organizations today face a similar security crisis. For example, it's not a bank's fault if a customer's PC is compromised and their account is cleaned out, but it is the bank's problem. It's not eBay's fault if a consumer falls for a phishing attack and gives away their PayPal information, but it is eBay's problem. And moving forward it won't be carriers' fault when thousands of customers have their identities stolen via VoIP phishing attacks, but it will be their problem.

Each of these cases is remarkably similar to the challenge Johnson & Johnson faced in 1982. And, the opportunity to innovate is just as profound. The innovators will understand that by securing the process end-point, they can create competitive advantage.

Who will become our modern day Johnson & Johnson? Who will be first to understand that securing the entire process is not an expense – it is a competitive advantage? My company is working with these innovators right now. They are creating what we call “gated communities” where they can conduct business without fear of compromise. They are revamping their defenses to not



only secure their own systems, but those of the process endpoints -- the customers themselves. These are the innovators that will change the world, just as Johnson & Johnson did 25 years ago.

When I look across today's innovators, I see they all have one thing in common. They understand that complexity is the enemy of security. They see that enterprise infrastructures have become so unwieldy, with so many vendors, that they are almost impossible to secure. One of the best measures of complexity is to measure the number of people it takes to run the infrastructure. A recent study by IBM found that 45 percent of security spending by large enterprises is on people. This is a troubling statistic, for a couple of reasons. First, when you need that many people to run your security infrastructure, there is too much opportunity for human error. Second, security operations cost way too much money. Technology is supposed to reduce manual labor through automation. In the case of security technology, it is creating manual labor.

This trend simply is not sustainable. It's not sustainable because it is too expensive. More importantly, it's not sustainable because it doesn't work. Any infrastructure in which you need to invest almost half of your budget on human management is way too complex. The problem is, enterprises have been sold a bill of goods by security vendors. They believe spending half their budget on people is normal. They believe their security infrastructure is working when it isn't. And this creates an incredibly target-rich environment for today's cyber-criminals.

We see this every day through our professional security services organization. When our consultants engage a customer, the customer always thinks their



security infrastructure is functioning perfectly. Then the fun begins. For example, in one engagement, our consultants penetrated the defenses of a national electric utility in Latin America through a rogue wireless access point. I asked our lead consultant how critical the situation was. He said: “Incredibly critical. I could set it up so you could be sitting in a cyber café in China and shut off the electricity in Mexico. Give me a few days and I could spell my daughter’s name in lights in Mexico City so it’s visible from space.”

Another one of my favorite stories is an engagement we had with a county government in Florida. Their security team swore up and down that their systems were completely protected. Within a day or two, our consultants penetrated the county’s parole management system through an application vulnerability. They had complete access to the system – to the point where they could have started discharging criminals from county jails.

I’ll give you one more. A municipal organization in Atlanta saw that their IT budget was skyrocketing year over year. They asked us to assess their infrastructure to figure out why their networks were so slow and why they kept running out of capacity. We found one of the world’s largest pornography syndicates had co-opted their servers and was running operations out of their data center.

These stories might seem remarkable, but really, they’re the norm for us. Our consultants have hundreds of stories like this. And the root cause of the problem is always the same – the customer is trying to protect themselves with defenses that are easily bypassed by today’s modern cyber-criminals. I like to call this the Maginot Line school of security. You World War II buffs out there know what I’m talking about. The Maginot Line was a system of heavy artillery and fortifications



built by France in the 1930s. It stretched from Switzerland to Luxembourg and was designed to prevent another World War I.

Unfortunately, it did not take into account the changing technology and tactics of warfare. The Maginot Line was built to stop the German army of World War I, with its horse-drawn artillery and plodding foot soldiers. It was not built to stop the German army of 1940, with its mechanized infantry, armored columns and air force. When the German army attacked, it simply went around the Maginot Line, through Belgium, and took France in a little more than a month. France had the right goal in mind, but made a huge strategic error. Instead of investing in systems to fight the next war – tanks and airplanes – they invested in a system designed to fight the last war. The results speak for themselves.

We see this same failed strategy being used today by enterprises trying to stave off the assault of modern cyber-criminals. Security infrastructure has grown at the component level – point solutions deployed to combat specific threats. Because of this, today's typical security infrastructure is a Maginot Line of expensive and complex point solutions.

And, the components behind the complexity are often powerless against today's threats. Vendors even admit as much. It always makes me laugh when I see anti-virus and malware prevention vendors issue press releases proudly proclaiming how many thousands of signatures they've added to their databases. I just think about the latency involved with each of those signatures. And how each period of latency represents time when the customer was not protected. As I noted, our ISS X-Force research organization analyzed more than 200,000 newly introduced malware samples in 2006. When you add it all up, it means their customers were not protected at all for the vast majority of the year. It's the Maginot Line all over again. And I wonder: "Does anyone get it? Does anyone



understand that the customers of these vendors are losing today's war by fighting the last war?"

And yet, these architects of the modern Maginot Line continue to flourish. They reinvent themselves to stay abreast of current trends. They acquire companies and talk about how consolidation will reduce operational complexity. But they don't tell you that their product offerings are not compatible on a system level. So what you have is brand consolidation, which does nothing to reduce complexity. And some of today's biggest brands are pushing complexity in a big way, to the detriment of customers.

IDC recently conducted a survey of IT security professionals. As part of the survey IDC asked respondents to rate 18 different security challenges facing them in 2007. Respondents said the no. 1 challenge facing them in 2007 is the growing sophistication of attacks. The no. 3 challenge is the increasing complexity of security solutions. The no. 1 challenge is not going to stop; bad actors have exploited the systems of commerce since ancient times. The no. 3 challenge must stop. We must enter an era of simplification, if we are to close the gap with the bad guys.

When I think about the current state of consolidation and simplification in the security industry, it reminds me of a story from the Reagan administration and the Tax Reform act of 1986. One of the people responsible for revising the code was a congressman from Ohio, Delbert Latta. When his task force finished its new draft of the tax code, he stood before the media and said "I hold in my hand 1,379 pages of tax simplification!" To someone working on his committee, reducing the code to 1,379 pages probably seemed like an accomplishment. But to those of us paying taxes, it was only a start.



The same dynamic applies to security. Yes, appliance consolidation and server consolidation have marginally reduced complexity. But true simplification is much greater than that. It requires a system-wide approach to security that accounts for everything from IT infrastructure to staffing to business process outsourcing.

The first step toward simplification is to understand what you have. You need to identify your critical assets. Identify vulnerabilities. And understand your business processes and how to secure them.

The second step is to simplify by innovating. No IT department can do it all anymore. Nor should they. Outsourcing has to be a key component of simplification. At a minimum, you should consider outsourcing your routine security functions and keep the critical ones in-house. You also should explore new service delivery models like in-the-cloud services. These are emerging services where service providers perform security functions on your network traffic, and then send clean traffic onto your network. My company recently conducted a survey of carriers, and 78 percent said in-the-cloud services will be a major source of revenue within five years. These services are coming, and they should be factored in as part of your simplification strategy.

Third, your in-house security infrastructure should be built from the ground up to be a fully integrated platform. And by that I mean a platform in which the different components are built to fit together in seamless interoperability. A platform that delivers a true single point of management and is extensible to address future security requirements. I don't mean a so-called integrated system that is really a bag of components, connectors, adapters, bailing wire and chewing gum, touted by a team of consultants. They'll tell you it's a platform. But really, it's a professional services engagement masquerading as a technology solution.



Only with a true platform can you achieve the level of manageability and cross-component synergy required to truly secure your business. Notice I said “your business,” not “your infrastructure.” That’s because when you think about simplifying and strengthening security, you need to frame your strategy around your business, not just your infrastructure.

IBM last week rolled out a new set of governance and risk management initiatives designed to help companies develop just such a strategy. IBM did this because the market is screaming for new approaches to security governance. A recent IBM survey showed that 64 percent of CIOs see security compliance and data protection as one of the most significant challenges facing IT organizations today. Yet another data point showing that the Maginot Line school of security has failed, and that the time is ripe for innovation. Innovation from vendors and from enterprises. Successful innovation will have benefits that extend right to the bottom line. Likewise, lack of innovation will impact the bottom line, but not in the way you’d like. In a recent Unisys survey of nearly 1,800 consumers, 75 percent said they would switch banks for better protection of their personal information. 77 percent said they’d change for better protection of their money. Clearly, there is much to gain by being an early innovator in the banking industry. I believe the same opportunity exists across all industries.

Some people want you to believe that the security industry is mature and approaching commodity status. In this world, all products are equal and all problems have been solved. They point to consolidation as evidence of this. But consolidation can be deceptive. There is a profound difference between brand consolidation and technology consolidation. Brand consolidation adds to complexity. Technology consolidation reduces complexity. Brand consolidation takes a component-level approach to security. Technology consolidation takes a platform-level approach. Brand consolidation represents the old way; the failed



way...the way that administers a vaccine to a corpse and then calls it a cure. Technology consolidation represents the new way. The platform way. The way that enables companies to convert security into a competitive advantage.

Security is not a mature industry. Rather, it is an industry ripe for innovation. Innovation that moves us away from the disastrous Maginot Line strategy propagated by industry generals who to this day insist on fighting the last war. We're in a new war now – one where the stakes are too high to ignore. Just like they were for Johnson & Johnson in 1982.

Here's how we win this war:

First, enterprises need to step up to the plate and rethink their security strategy. Security is no longer an expense, or a necessary evil. It is a differentiator that can be more powerful than price, service or even product quality. The innovators will change the competitive landscape, just like J&J did in 1982.

Second, vendors need to step up to the plate and deliver true platform-level solutions. Not branded aggregations of point solutions, but true platforms that provide single point of management and control. And I don't just mean technical integration. I mean deployment and operational integration as well. Because winning the war requires a combination of on-premise and outsourced operations working together in unison.

Third, carriers must step up to the plate and deliver new, easily adoptable and highly scalable in-the-cloud services. This will radically reduce complexity by enabling enterprises to offload systems and their associated management to service providers. It will also enable enterprises to take a more strategic



approach to security operations. They will be able to deploy resources where they need them most – protecting critical assets.

The good news is, all of this is happening today. The early innovators are stepping up to the plate in all three categories. And that is why I am very optimistic about the future of security, and the future of business. And in that spirit, I'd like to leave you with one final story. This was actually one of President Reagan's favorites...

The parents of twin five-year-old boys were worried that their children had developed extreme personalities. One boy was a total pessimist, and the other was a total optimist. So, the parents took them to a psychiatrist.

First the psychiatrist treated the pessimist. To brighten the boy's outlook, he took him into a room piled to the ceiling with brand-new toys. But the boy burst into tears. "What's the matter?" the psychiatrist asked. "Don't you want to play with the toys?" "Yes," the little boy cried. "But if I did I'd only break them."

Next the psychiatrist treated the optimist. Trying to dampen his outlook, he took the little boy into a room piled to the ceiling with horse manure. Much to the psychiatrist's surprise, the little optimist cheered in delight. He climbed to the top of the pile, dropped to his knees, and began gleefully digging out scoop after scoop with his bare hands. "What do you think you're doing?" the psychiatrist asked. And the little boy replied, "With all this manure, there must be a pony in here somewhere!"

I encourage all of us here today to be that kid looking for the pony. Yes, today's threats are profound, and at times it may seem like the bad guys are winning. But, in these challenges lie opportunities. Opportunities to finally rid ourselves of



Maginot Line defenses so we may adopt modern strategies and platforms that provide true protection. Opportunities to challenge our vendors to live up to their promises by delivering true platform solutions – not grab-bag aggregations of acquired products branded as integrated solutions. Opportunities to simplify, strengthen and expand the way in which we secure our businesses, our economy and our country. We've created a vibrant industry with a strong heritage. But, without innovation, we risk becoming irrelevant. I challenge each of us here today to seize this historic opportunity.

Thank you for having me.