VeriSign®
The Value of Trust℠

Intelligence and Control℠ Services:

The New Age of Information Security

CONTENTS

Introduction: The Maginot Line

They felt safe. The French army, devastated by World War I, based its national security on a system known as the Maginot Line. The system stretched along their northeast border from Belgium to Switzerland. It was made up of underground air-conditioned fortresses, artillery pillboxes, subterranean railroads and anti-aircraft guns—a defensive system so strong, the French considered it impenetrable.

After a history of war with the Germans, the French knew that they needed a new defense against their past enemy. This time, they planned to keep the attackers out using a fortified barrier. And the Germans did attack again in 1940. But this was not the last war. Instead of attacking full force at the barrier, the Germans invaded France through the Ardennes forest, a part of the border assumed to be impassable by Maginot and his colleagues in the French military establishment.

Historians believe that what actually doomed the French was not an insufficient defense, but a lack of intelligence beyond their own walls, and a basic inability to marshal strategic responses to a rapidly changing environment. Rather than controlling their own destiny, their mode of defense ultimately controlled them. In the past, entrenchment designed to outlast the opponent was the key to survival. But France's enemies had evolved, and the rules of warfare had changed. This stubborn "Maginot mentality," focusing on building massive defenses rather than a more agile approach that embraced real-time intelligence and control, had become obsolete in the new world.

Today, there are thousands of digital "Maginot Lines" that companies have invested in to protect their valuable online assets including sensitive customer, transaction, and employee records. These critical online assets sit behind seemingly impressive defensive infrastructures, but just as the French learned six decades ago, a defensive system alone is not enough. It must be coupled with an offensive system that provides real-time intelligence and control to ensure adaptability to an ever-evolving environment.

Today's Security Dilemma

We are living in a time of unprecedented promise and unprecedented uncertainty. The communications and technology sectors have been mired in a prolonged slump while Information Technology (IT) budgets have been drastically slashed. A recent *Harvard Business Review* article proclaimed that "IT Doesn't Matter," and that technology no longer provides a competitive advantage.[1] Yet it is incontrovertible that the commercialization of the Internet has fundamentally transformed how businesses operate. This revolution has opened up tremendous revenue opportunities and productivity improvements. Indeed, the Congressional Budget Office estimates that over 48 percent of the productivity gains over the next ten years will come through the applications of Internet technology.[2] Despite widespread perceptions that Internet-related activity has slowed down since the "bubble" burst, the Internet has, in fact, continued to grow at impressive rates. In just the last three years, daily Web interactions have shot up over 500 percent and e-commerce transactions have grown at an astounding rate of 74 percent annually.[3]

However, even this impressive growth has been outpaced by the increase in threats against corporate and national IT infrastructures. The number of security vulnerabilities and reported incidents has continued to rise at an unprecedented rate (figure 1). The enterprise network has been virtualized. Today, it includes not only connections to partners, but to the Internet infrastructure itself. The very openness of the Internet, which is the source of its vast power to affect positive change, has also proved to be a boon to would-be attackers.

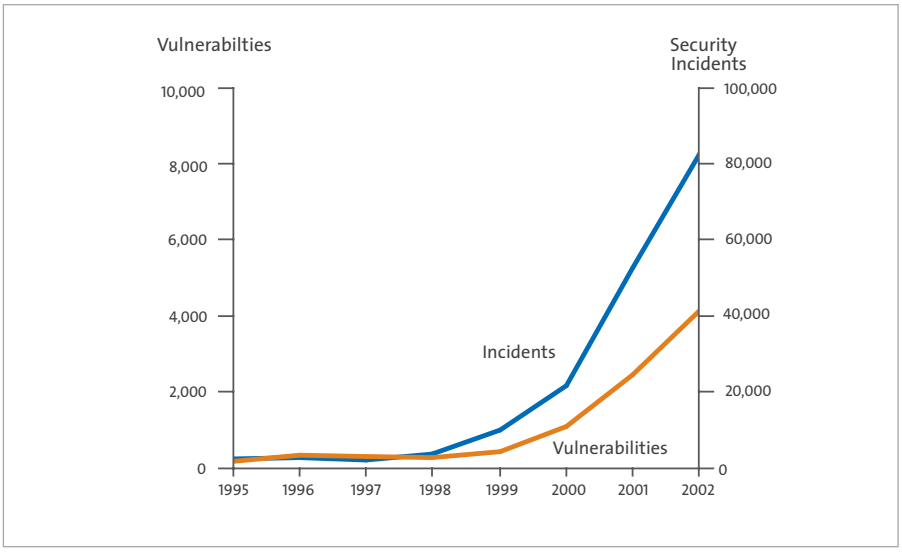

Figure 1: Rise in Known Security Vulnerabilities and Incidents
(CERT/Carnegie Mellon University 2003)

That being said, the Internet revolution marches on, with a new wave of emerging technologies promising to bring about even more transformational change including: Web services for partner integration; on-demand computing for capital expenditure efficiency; ubiquitous mobile computing for personal productivity from laptops to handhelds to smart phones; federated identity management across enterprises; and "IP Everywhere" for all voice and data communications. All of these developments will result in tangible benefits, yet each is fraught with security issues that inhibit adoption. *CSO* magazine found that at least one in ten businesses is not pursuing new business opportunities as a result of security concerns, primarily those associated with connecting to business partners, customers, and remote locations.[4]

This forms the fundamental security dilemma facing companies today: how to become more open, yet more secure. In trying to find the right balance some businesses tend toward progressive openness, while others concede freedoms in the pursuit of security. Why should corporations accept the limitations of this choice? The answer is they should not.

Effective security must not only react to attacks, but must be able to anticipate them, recognize patterns and trends, and correct weaknesses immediately without a compromise to operations. An active IT security stance should be a vital part of a new business model that makes the most of the vast productivity and opportunity already born of the Internet, and the advances yet to come. Technology does matter—and it will continue to have transformational benefits. Enterprises must not be paralyzed by fear. Security must not stand in the way.

Yet, many companies have retreated behind their own Maginot Lines, using IT resources to create virtual information fortresses—trying to protect themselves while risking the side effects of limiting access, isolating data, and prohibiting new forms of remote and wireless access.

They do so at their own risk. Companies that provide external access to customers, partners, and suppliers are more likely to experience greater revenue growth and lower costs than organizations that isolate their networks from the greater world. On average, more open companies experienced 2.9 percent greater revenue and 10.5 percent lower costs than companies that restricted access to only those within their physical walls.[5]

Key Business Challenge

COMPLEXITY

With so much attention paid to the slowdown in the IT marketplace, some have overlooked the many technology advances of the last three years—and with advancement has come complexity. Employees, partners, and customers are demanding ever greater access to information as their tasks become more and more complex. In turn, technology is evolving to meet those needs and develop new opportunities, along with new vulnerabilities. "By opening up the enterprise environment to improve information flow, the inherent risks and vulnerabilities significantly increase," write security analysts Alan Carey and Paul Johnson in a recent IDC report.[6] "Enterprises are increasingly forced to deal with a variety of potentially devastating attacks and vulnerabilities such as viruses, malicious code, Web defacement, insider abuse, and theft of intellectual property."

The people and organizations who take malicious advantage of the Internet are constantly working to stay one step ahead of technology. New tools developed to support an increasingly mobile workforce and the integration of disparate data systems mean that highly scalable and complex security systems—and the people to run them—are two of today's most pressing needs.

The Evolution of Information Security

Information security has evolved significantly over the past fifteen years. First came the Age of the Barrier where locking down data and restricted access were of paramount concern. More recently, came the Age of the Foot Soldier, where a proliferation of special-purpose devices and products have helped to move the balance a bit more toward access and productivity.

The Age of the Barrier

In the days when most of an organization's critical data resided on mainframes, and was accessed primarily through terminals and reports, security was primarily an isolated problem. IT professionals developed solutions that relied on physical security, encryption, and procedural controls. Security was achieved through obscurity, by putting up higher walls, tightly restricting access, and locking down data.

For years, data was not generally shared outside of tightly controlled, physically co-located teams. In a closed environment, this approach to security worked well, and benefits are still seen from the technologies and procedures that were developed. However, this purely defensive approach became insufficient in the early nineties, as the industry began progressing toward distributed groups with an imperative to share data. And it became fundamentally untenable as the Internet became a driver for increased productivity and revenue.

The Age of the Foot Soldier

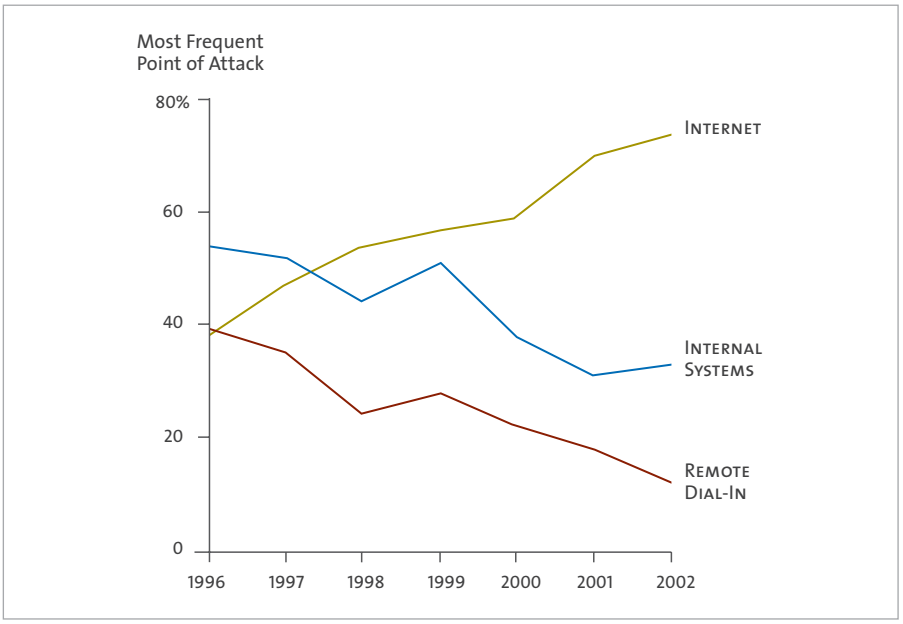

Figure 2: Change in Nature of Attacks
(FBI/CSI Computer Crime and Security Survey 2001)

The nature of attacks against businesses began changing dramatically as the Internet started to have an impact on IT architecture (figure 2). Physical proximity ceased to be a pre-requisite for accessing data. Viruses could be spread rapidly by e-mail, rather than relying on physical distribution means, such as shared floppy disks. Financial fraud could be perpetrated by criminal gangs operating thousands of miles away from their intended victims. And ever more sophisticated attacks could be launched, by ever less sophisticated attackers (figure 3).

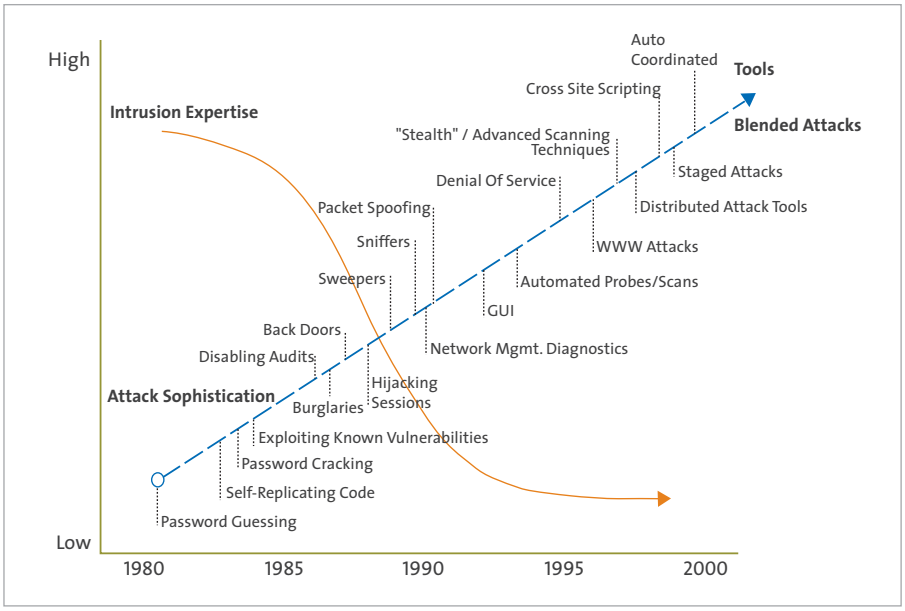

Figure 3: The Growth of Attack Sophistication Over Time
(CERT/Carnegie Mellon University 2001)

The industry has responded to each of these threats through a new generation of special-purpose security products: firewalls, network-based anti-virus software, access management, e-mail gateways, intrusion detection systems (IDS), and the like. The impact of deploying this wide variety of products, like the deployment of an infantry of foot soldiers, has helped organizations withstand many forms of attack. Not surprisingly, spending on these solutions has also continued to rise. Indeed, estimated spending on firewalls, secure content management software, IDSs, Virtual Private Networks (VPNs), and the like have formed the bulk ($8.9 billion) of $12.6 billion spent on security in the United States last year (figure 4).

Key Business Challenge

COMPLIANCE

As private information moves into the public space of the Internet, the government is acting to protect its people and their information. The *CSO Security Sensor IV* survey found that regulatory and compliance issues continue to be the biggest drivers behind investments in security.[9] And the challenges continue to rise with recently-enacted federal and state regulations, such as Sarbanes-Oxley, the Gramm Leach Bliley Act, California's Security Breach Notice Law, and the Health Insurance Portability and Accountability Act (HIPAA). These regulations are dramatically affecting the way companies protect financial, medical, and other private information. At the same time, they are forcing executives to fundamentally change the way they think about IT security. For example, under the new HIPAA Security Standards set to take effect in 2005, healthcare providers must be sure they can reconstruct every transaction and be able to show exactly who touched which patient records and when. "The government just says you have to do it," says a vice president of information services for a large medical services provider. "There is no template."[10]

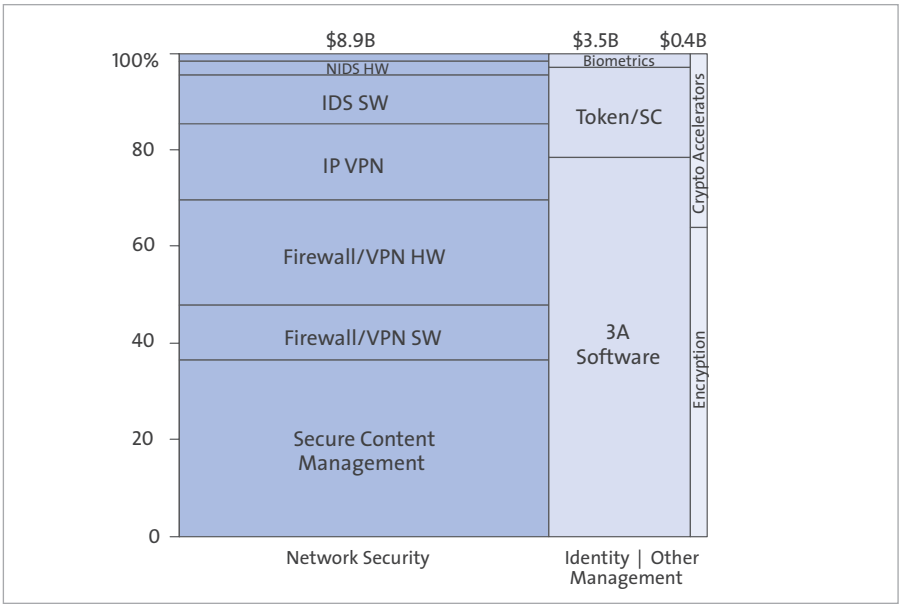

Figure 4: Estimated IT Security Spending, North America Only (2003)

(VeriSign extrapolation from IDC forecasts)

Yet even this large investment does not appear sufficient. The level of threats, vulnerabilities, and economic losses have more than doubled in the past year. John Pescatore, vice president and research director at Gartner, Inc., warns, "Every area of IT is getting more efficient except security. New security solutions need to replace the old, not just add up to more spending."[7]

Ironically, this point product proliferation has become a pain point in itself. The security environment is increasingly complex and unmanageable as IT staff are overwhelmed by unrelated consoles, alerts, and audit trails. They struggle with controlling divergent applications and networks, often made worse by organizational complexity. It is telling that, despite the widespread deployment of protective devices, over 90 percent of all successful attacks have been shown to be against vulnerabilities that have been well-known for at least six months. For many, just maintaining control has become an impossible challenge.

Similarly, the IT executive is challenged to evaluate the effectiveness of their investment. *Information Week's U.S. Information Security Survey* showed that only 40 percent of IT executive respondents have been able to actually review and measure the effectiveness of their security investments. And a full one-fifth of them said that they neither reviewed or measured efficacy.[8] So much time is spent fighting fires that few can focus on optimizing results and solving problems strategic to the business.

The Next Chapter: The Age of Intelligence and Control

Both the Age of the Barrier and the Age of the Foot Soldier brought significant advances to computer and network security. And each has introduced new challenges that can only be addressed by the technological, procedural, and philosophical advantages brought about by its successor. The enterprises that will thrive in the coming years, however, will be those best able to adapt to the dawning era: the Age of Intelligence and Control.

What's missing from the previous stages? Stated plainly, security solutions need to provide business people with the ability to "think outside the boxes." Michael Rasmussen, a director for Forrester Research, explains, "People approach info-security through products, but that only addresses the tactical side; it is much more of a business problem, and people are just starting to wake up to that."[11]

While smarter firewalls, better IDS signatures, and more comprehensive anti-spam filters will all continue to play critical roles, their full potential will be limited without a foundation of coherent policies developed by experienced people who understand the nuanced choreography of security technologies, intelligence, and control. Devices are the foot soldiers in defense, intelligence provides readiness, and control builds active protection—all three must work together to monitor threats, fight them, and continually improve the ability to safely use the Internet.

The next generation of security solutions will deliver real-time intelligence that allows the enterprise to regain control of their environment and take an offensive stance. These solutions can help realize the full value of existing investments, provide measurements and benchmarks for effectiveness, and establish service levels that are attuned to business needs. They can create order from chaos, and let an IT staff intelligently assess, monitor, manage, and respond to threats and changing needs. They can provide visibility beyond the corporate walls and act as an early warning system for business contingency planning. They can watch the flow of event and data across network, application, and transaction layers to enable business-relevant risk assessment. In other words, with *intelligence* and *control,* security can become a key asset and a competitive advantage for the progressive enterprise.

The New Model: Intelligence and Control℠ Services

VeriSign believes that a new model is evolving to meet today's security challenges, one aptly named **Intelligence and Control Services.** Properly implemented, the Intelligence and Control model will prove to be a powerful strategic weapon in the arsenal of today's progressive enterprises.

To gain its benefits, an Intelligence and Control strategy must embrace the following principles:

1. Device Independent Integration
2. Pervasive Security
3. Collective Intelligence
4. Conclusive Action

Principle 1: Device Independent Integration

The foundation of the Intelligence and Control model is *device independent integration*. It leverages a powerful combination of real-time information (the intelligence) and determinative tools (the control) to provide an integrated view and real control over a complex, heterogeneous environment. This allows organizations to accurately assess risk and take a proactive stance. This new model need not impose new software or hardware on the enterprise. Nor should it prescribe a particular suite of devices because most of today's enterprises have already deployed best-of-breed point solutions, and are operating in an inherently heterogeneous environment. As advances such as voice-over-IP (VoIP) and mobile computing become mainstream, the jigsaw puzzle of overlapping discrete products will become even more unmanageable. *Device independent integration* is the foundation for streamlined, consolidated management.

Principle 2: Pervasive Security

Intelligence and Control Services are not just about perimeter security such as firewalls and intrusion protection. They must also provide integrated intelligence about, and control of, the full range of security issues spanning activity at the network, application, and transaction layers. They must also incorporate information about the flow and access of data by employees, partners, and customers, as well as devices and applications.

"Event correlation would be very useful to have at the perimeter," says a chief network architect at a global financial services company. "Currently we have too much information without a means of meaningfully harvesting or mining it." VeriSign's managed security business manages and monitors large numbers of firewalls, IDSs, and VPNs. Data from last year alone shows that, on average, VeriSign processed 6.4 million events per device. Of those events, approximately 100,000 are in some way anomalous. Through the use of advanced correlation, analysis, and automated intelligence activities, VeriSign was able to further distill that number to about 54 incidents that warrant further investigation by a trained security engineer. Of those 54 incidents, only two turned out to be true attacks (figure 5).

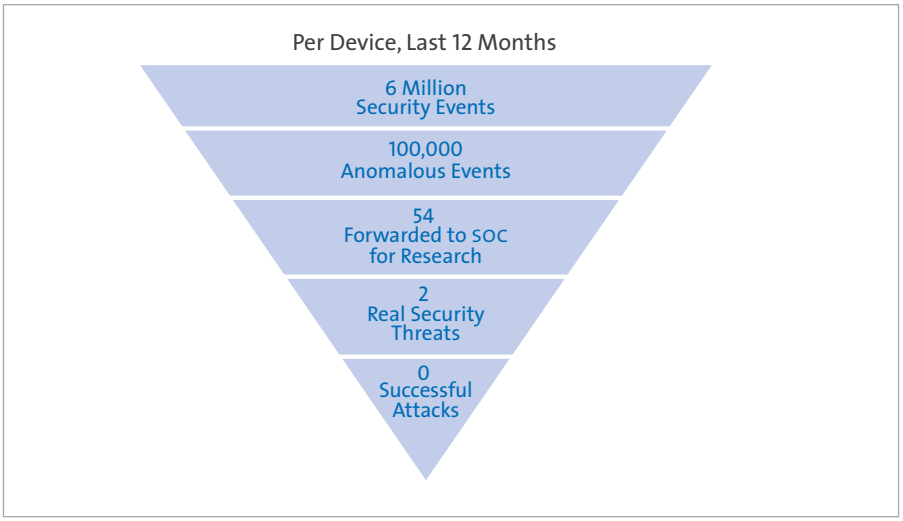

Figure 5: Determining Real Security Incidents

Without intelligence and control, the typical company would have to investigate 100,000 events multiplied by the number of devices in their facility (at five minutes per event, this would require several full-time staff). The more dangerous alternative would be to ignore events that could lead to major losses from the two real attacks.

But controlling the perimeter is not enough. Intelligence and Control Services should help control and manage risk from a business perspective. Detecting network attacks alone cannot truly quantify risk, conduct meaningful forensics, or assess loss. For example, to detect a fraudulent financial transaction, effective Intelligence and Control Services must examine events from the network, audit trails from the application, logs from data access, and transaction patterns. It must provide *pervasive security* from state-of-the-art correlation and inference engines to process events and find meaningful patterns across multiple networks and applications.

Principle 3: Collective Intelligence

As shown above, security must be designed with a comprehensive approach to the organization and its business goals. Trying to manage security is impossible if one's scope of vision is limited to a single point, such as a firewall. Similarly, as enterprise networks become increasingly interdependent, it is no longer adequate to limit one's visibility to a single network.

Intelligence and Control Services must also correlate and develop intelligence from data gathered between enterprises and across the Internet (figure 6). Even the most efficient, well-funded security organization will be at a significant disadvantage if it limits its sources of intelligence to those within its own four walls. Such an organization will not be able to see patterns of threats as they develop across the Internet. Nor will they be able to leverage the experience and knowledge of other organizations and develop appropriate solutions. And their response time will be dramatically shortened—unlike today, where enterprises can only initiate a response after the threat has already hit them. Fraud schemes perpetrated across large numbers of merchants, and worms such as Blaster and Sobig which attack by spreading rapidly without boundaries validate that leveraging the *collective intelligence* from network effects is critical to any successful security strategy.

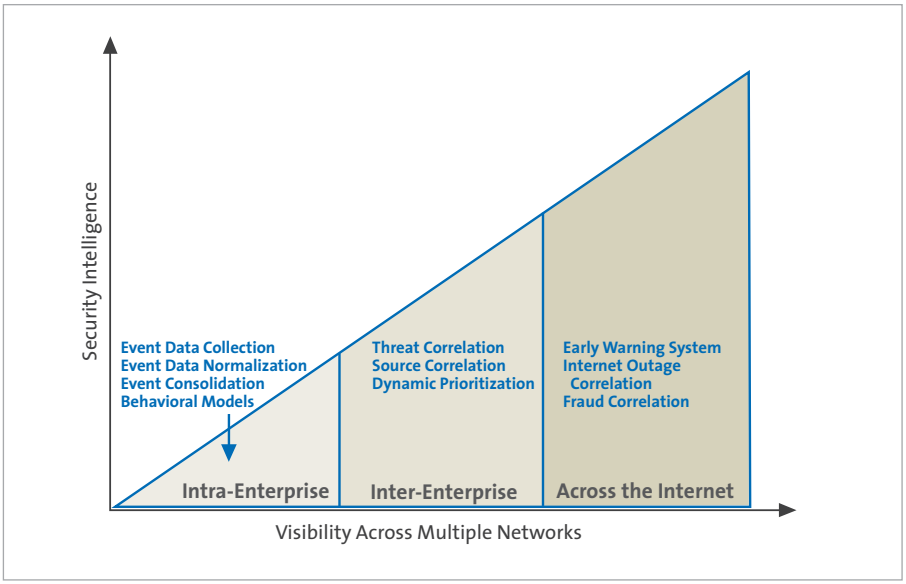

Figure 6: Visibility Across Multiple Networks

Principle 4: Conclusive Action

For Intelligence and Control Services to be valuable, they must provide intelligence that supports conclusive policy and design decisions. Public and private organizations must design systems with global sources of data and intelligence. This requires methods that help experts measure risk, prioritize remediation steps, and proactively design their policies, networks, and defenses around business goals.

For example, in the past twelve months, over 70 different security bulletins were issued by Microsoft alone.[12] The total number of known vulnerabilities is now over 8000 and that number is likely to rise for 2003 (figure 1). Clearly, there is a cost associated with deploying each new patch and correcting each vulnerability. Administrators cannot simply bring down the network every time there is a new patch to deploy, they must weigh the cost against the risk. The same principle holds true for decisions around granting remote access to employees, sharing information with partners, and expanding to serve new categories of online customers. For Intelligence and Control Services to be useful, they must present the enterprise with enough information to make informed decisions, weigh risks, and take *conclusive action* rooted in business logic.

Ultimately, the extent to which an organization is in control of its destiny is a function of its intelligence. As shown (figure 7), an enterprise needs to be able to readily correlate:

1. The *value* of unique information assets, both to themselves and to attackers.
2. The level of organizational *vulnerability*. This is itself a function of the enterprise's IT architecture, exploitable system vulnerabilities, and the extent to which those vulnerabilities have been addressed through patching or other activities.
3. The level of *threat*. This requires understanding, in real time, potentially threatening activity within the enterprise, activity across enterprises, and across the Internet.

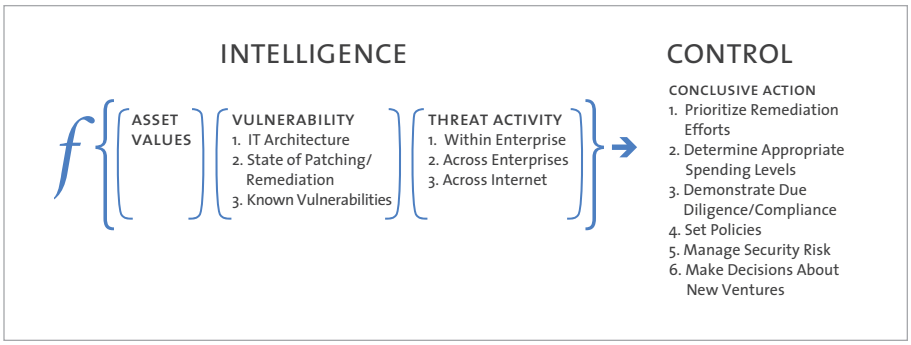

Figure 7: Control is a Function of Intelligence

Intelligence and Control Services seek to intelligently correlate all three categories of information, and present the resulting intelligence to the enterprise in a way that permits the enterprise to take conclusive steps, such as: prioritizing remediation activities, demonstrating compliance to regulations, establishing appropriate security service-level agreements, and determining whether to invest in a particular security initiative.

Perhaps most importantly, Intelligence and Control Services allow organizations to assess and manage the security risks associated with any new venture, be it automating supply chains, moving off of leased lines, or collaborating with outside parties.

It is this combination of real-time information (intelligence) with the determinative tools (control), that allows organizations to take a proactive stance in their security strategy, thus differentiating the Intelligence and Control approach from prior approaches to security.

Evolving Security Needs

Ultimately, organizations will have to evolve beyond framing decisions about security designs and expenditures in the context of a largely unquantifiable horde of threats. Without the intelligence to form a productive business strategy, security environments will continue to be shaped in reaction to budgetary constraints, perceived regulatory mandates, and fear of the unknown.

As an analogy, consider the way in which financial risk is treated. Interest rates change, poor market conditions, wars, weather, and a hundred other factors impact the financial community, and all pose risks. However, the most successful insurance companies, brokerages, and banks leverage their approach to risk as a competitive weapon, intelligently managing risk in relation to return. Companies that are best able to gain intelligence about the environment—and control their responses to it—stand to benefit from the most financial gain.

Key Business Challenge

COST

Perhaps the most unavoidable facet of our current economy is cost cutting. Overspending on technologies that seemed indispensable in the late nineties is still shackling today's IT budgets. Companies are now under great pressure to slash capital spending as well as operational expenses. Staffing has not escaped the knife which means fewer people within organizations are capable of managing and securing information.

Now business finds itself in a catch-22. At the very moment that companies need to migrate more of their critical operations to the digital infrastructure to cut costs, they find themselves without the available resources to protect the required migrations. Meanwhile, the threats to existing security systems do not rest while the economy stagnates. On the contrary, threats and attacks are becoming more frequent, more sophisticated, and more successful.

Security Today

This new way of thinking is gaining traction within the enterprise security space. Just five or six years ago, many companies viewed security as a checkbox task for IT managers and a necessary evil for IT budgets. As the Internet grew and networks became more complex, companies recognized a need for hiring specialists who could focus their energies on nothing but IT security. Almost 60 percent of companies now have at least one employee dedicated to security, and 32 percent of these companies have senior titles including chief security officer, chief information officer, or vice president.[4] In the past decade, it has become clear that the Internet offers companies valuable business opportunities, but with significant risks. As a result, IT security has made its way into boardrooms and executives suites.

These C-level executives, who sit on the fence between IT security and business efficiency, are a new breed. They are well aware and concerned about what can happen if a hacker penetrates a network perimeter or a virus takes down an e-mail system for a day. Instead of acting as fear mongers, they are more interested in pursuing strategic partners who understand how security can actually provide them with a competitive advantage. They want partners who focus on business issues that matter most to them: controlling costs, managing complexity, and complying with regulatory requirements.

"What top managers of enterprises need to find is a balance between security that can protect their businesses and free communication that can stimulate growth. Success depends on it," says Richard Hunter, vice president and director of research at Gartner, Inc. "They need to think in terms of what Gartner calls the 'Resilient Virtual Organization' in which security is the ability to survive and prevail, not just hunker down and resist intrusion."[13]

Today, forward-looking companies are considering a new perspective, the idea that security can set you free—free to pursue opportunities in commerce, communication, and collaboration.

The next section highlights examples of three organizations using the Intelligence and Control approach. While these are VeriSign customers and partners, it is important to stress that this model transcends any one provider.

Freedom to Communicate

Merrill Lynch is one of the largest financial services firms on Wall Street, posting $18.6 billion in revenues for its 2002 fiscal year. As a company with offices around the globe, Merrill Lynch makes huge investments in technology, connecting everything from branch offices in small towns to bustling trading floors in the world's financial capitals. With such a far-flung network, security and reliability of data and transactions are paramount.

With trillions of dollars in customer assets under management, Merrill Lynch built a sprawling computer security operation. But according to Merrill Lynch, there was a problem. Despite large investments in the latest network security devices, such as firewalls and intrusion detection

systems, the company still could not gain a good perspective on the seriousness of a particular cyber-threat—whether it was affecting the Internet as a whole, or just an isolated attack on Merrill Lynch. They had plenty of data to review internally, but like many companies, lacked a broader view of cyber-threats and appropriate security responses, according to officials.

With Intelligence and Control Services acting as an early warning system, it actually helps an enterprise take steps to mitigate the impact or stop an attack altogether. That ability to see beyond the firewall and beyond the network turns a defensive fortress into an active protection system. This is why Merrill Lynch is using the Intelligence and Control approach as the underpinning of its financial systems security.

"It's all about being the best that we can possibly be," says David Bauer, Merrill Lynch's chief information security officer, in a recent interview with *InformationWeek*.[14] "Now we're going to get analysis of all our activity in context with what else is going on in the world. It's not just about data, it's about intelligence. We can get analysis of events going on with us in context as to what's going on in the rest of the world. That allows us to make better decisions. It also gives us early warning. We can be better by having the kind of intelligence network we couldn't possibly have on our own."

Freedom to Collaborate

Law enforcement organizations like those that make up the Commonwealth of Pennsylvania Justice Network are increasing their ability to collaborate and communicate using the Intelligence and Control model. That was not always the case. In the past, the Commonwealth's various law enforcement agencies, such as the police department and the justice department, locked their information in very strict silos. It was not possible for one agency to access the criminal data of another agency without getting manual permissions and completing hours of paperwork. They were afraid that their data would fall into the wrong hands.

Deploying Intelligence and Control Services gave Pennsylvania the confidence to build a Web-based solution known as JNET. This system includes over 11,000 users, and provides secure access for the FBI, the DEA, the IRS Criminal Investigative Service, and hundreds of district justice offices across 36 counties. "Data integrity and data security are essential to all aspects of homeland security," says Linda Rosenberg, executive director of JNET. "If criminal activities and the resulting data are not shared it could have an adverse impact on critical decisions, and ultimately on public safety."

JNET allows each individual agency to convert their data to an XML format, creating a common online environment where authorized users can access offender records and other justice information such as driver's license photos, mug shots, and RAP sheet information. "This information, which has historically lain dormant in legacy systems is key to all aspects of criminal investigation, apprehension, and crime prevention," says Rosenberg. Using VeriSign's Intelligence and Control Services, authorized agencies throughout Pennsylvania are now able to query and exchange sensitive and protected information.

"Access to the most accurate, timely, and dependable justice information on the justice network is the essence of the JNET vision and represents one of the greatest needs of the justice system and homeland security," Rosenberg continues. "This has dramatically changed the nature of the justice system and has provided technology solutions to age-old information barriers."

Freedom to Conduct Commerce

A major security challenge to online commerce is the growing incidence of Internet fraud. According to Avivah Litan, director for Gartner, Inc., the amount lost in online fraudulent activity is expected to grow to over $1 billion for 2003.[15] A pervasive problem, fraud is more than using false credit card numbers; it can also include stolen identity or unauthorized transfers between cash accounts. Fraud occurs not only at the level of individual transactions, but also can affect entire merchant accounts as well as the overall integrity of a network.

Fraud was a particular threat to Anaconda Sports which supplies sports equipment to wholesalers, mass merchandisers, and consumers. Because of their wholesale sales, international fraud perpetrators target Anaconda and attempt to buy large amounts of equipment for resale overseas. "We stood to lose tens of thousands of dollars per month in bad debt," said Robert Meyer, director of Internet services for Anaconda. "With fraud protection, we've saved significant time and more than $10,000 in just three weeks."

Based on the Intelligence and Control model, VeriSign's fraud solutions are not merely defensive, they make use of aggregate information gathered from payment and domain name directory services to recognize and score risk. Triggers can include unusual volume; geographical discrepancies; or transactions linked to IP addresses, e-mail addresses, or credit card numbers associated with fraud. Transactions that appear fraudulent are stopped before any money changes hands, and the merchant is alerted. Like other security threats, fraud can be approached with a proactive stance strengthened by real-time intelligence and real-world experience.

Security That Sets You Free

The rise of the Internet and related technologies has brought with it both unprecedented promise and unprecedented peril. Enterprises are facing a new strategic dilemma in a business environment that requires being both more open and more secure. All while dealing with increasing cost, compliance, and complexity issues.

The answer to this challenge will not be found by retreating into a Maginot-like defensive posture, by deploying additional point solutions, or by limiting one's intelligence to proprietary networks. Rather, what is required is a new approach for the enterprise through the Intelligence and Control model. As organizations such as Merrill Lynch, the Commonwealth of Pennsylvania, and Anaconda Sports have discovered, services which are rooted in the principles of *Device Independent Integration, Pervasive Security, Collective Intelligence,* and *Conclusive Action* provide the best solution to security and opportunity.

"Rather than join the chorus of fear mongers focused on sounding alarms, VeriSign believes security actually sets you free," argues Stratton Sclavos, VeriSign chief executive officer. "Security is a strategic weapon that, when applied and managed properly, enables an organization to grow in a digital economy—reliably, securely and profitably."

As history has shown, those who do not adapt to meet evolving security concerns will not succeed. The Maginot Line is viewed as a tragic example of a flawed defensive strategy. However, from this failure was born a new construct for active security; the result of which was illustrated in the Allies' victory on D-Day. Using highly secured intelligence, the Allies secretly amassed the largest amphibious offense in history and controlled the fearsome German assault despite nearly impossible odds. The Allies' efforts led to the eventual liberation of Europe.

Today, corporations must also break out of the fortresses of the past. The more interconnected organizations become, the more critical it is that the concept of intelligent, controlled security be embraced by the global marketplace. When provided with the tools to have control over their dynamic networks and the visibility to see beyond their own walls, enterprises will be free to conquer the complex challenges of today's business environment and explore new models and markets instead.

"The core idea is that if you have the real-time intelligence about security at the user, device, and network level, then you have the real-time ability to successfully control your environment. VeriSign offers solutions including strong authentication, network security, application security, and commerce security that deliver on the Intelligence and Control model."

Stratton Sclavos, CEO, VeriSign

Sources

1. "IT Doesn't Matter," Nicholas G. Carr, May 2003 *Harvard Business Review,* © 2003 by the President and Fellows of Harvard College

2. *2003 Net Impact Study:* "Driving Networked Business Productivity," © 2003 Momentum Research Group

3. From VeriSign as measured by top level domain name servers for .com and .net. The daily DNS queries rose from 1.5 billion in June 2000, to over 9 billion in August 2003. .com and .net registrations exceeded 2001 levels in July 2003.

4. *CSO Security Sensor IV*, July 2003: "Corporate Risk Management and Security," © 2003 CXO Media Inc.

5. *2003 Net Impact Study:* "Driving Networked Business Productivity," © 2003 Momentum Research Group

6. Security Report for VeriSign, Alan Carey, Paul Johnson, © 2002 IDC

7. *The Future of the Internet Security Market,* John Pescatore, © 2002 Gartner, Inc.

8. *U.S. Security Survey 2003,* © 2003 *Information Week* Media Network

9. "Security Immaturity," *CSO Survey,* © 2003 CXO Media Inc.

10. "Washington Watch," by Elana Veron, *CIO* June15, 2003, © 2003 CXO Media Inc.

11. "Secure Insecurity," Derek Slater, *CSO* magazine, April 2003, © 2003 CXO Media, Inc.

12. "Patch as Patch Can," Baroudi Bloor, *Small Business IT World,* 5/16/03, © 2003 Accela Communications

13. "Enterprises and Employees: the Growth of Distrust," Richard Hunter, © 2003 Gartner, Inc.

14. "Merrill Lynch's Chief Information Security Officer Speaks Out About The Benefits of Outsourcing Network Security," George V. Hulme, 5/21/03, © 2003 *InformationWeek*

15. "2002 Internet Fraud Report," © 2002 National White Collar Crime Center