Securing The Critical Infrastructure
Introduction

Following the September eleventh terrorist attacks on the United States last year, no issue has been on the minds of the American public more than national security and homeland defense. Transportation, power dissemination and financial systems – essentially all aspects of national security -- have come under incredible scrutiny in the month’s post 9/11, and cyberspace and the Internet are no exception. In October of last year, President George W. Bush created The President’s Critical Infrastructure Board by Executive Order 12321 and, on September 18, 2002, the Board released a draft of the much anticipated National Strategy to Secure Cyberspace.

As part of that executive order, President Bush called for “a public-private partnership, involving corporate and not-governmental organizations.” Reflective of President Bush’s call to action, Mr. Ronn H. Bailey, founder and CEO of Vanguard Integrity Professionals-Nevada, who had thoroughly examined the issues, found what he believed to be a significant hole in our nation’s security plan – the mainframe. Expressing his concerns to Howard A. Schmidt, Vice Chair of the President’s Critical Infrastructure Protection Board, Mr. Bailey was invited to the White House and was instrumental in creating new policies that put mainframe computers at the forefront of cyberspace protection discussions. As a result of his meetings with the White House and with government officials and critical infrastructure security policy makers, these policies were introduced into the national strategy listed above. This is a significant achievement for Vanguard, and a giant step forward for organizations and government agencies to realize and correct the potential danger that exists today on our nation’s mainframes.

The purpose of this White Paper is to demonstrate the significance of the mainframe to our nation’s critical infrastructure and highlight the serious decline of mainframe security practices within corporations and government agencies today. It is a direct result of Mr. Bailey’s discussions with the White House.
The National Strategy to Secure Cyberspace

Mr. Bailey met with Richard A. Clarke, CHAIR of the President’s Critical Infrastructure Protection Board, to discuss issues pertaining to mainframe security and was directly responsible for the inclusion of the new policies pertaining to mainframe computers, listed below:

Mainframe Computers

Mainframe computers continue to play important roles in large enterprises. However, security policies and practices tend to focus on desktop computers, network servers, network devices, the Internet, and pervasive computing devices – to the exclusion of mainframe computers. Mainframe security personnel have been redeployed or recruited toward new opportunities. Advances in mainframe technology and connection to the Internet have created new risks and vulnerabilities rendering existing mainframe security policies and practices obsolete. Furthermore, the frequency and rigor of qualified mainframe audits have deteriorated to the point they are no longer capable of identifying these threats. Organizations and government agencies must refresh their security policies, practices and technologies as vigorously as elsewhere or risk exploitation from new threats.1 (see footnote.)

Large Enterprises

(1) Enterprises should review mainframe security software and procedures to ensure that the latest effective technology procedural measures are being utilized; (2) IT vendors and enterprises employing mainframes should consider developing a partnership to review and update best practices of mainframe IT security and to ensure that there continues to be an adequate trained cadre of mainframe specialists; and (3) IT security audits should include comprehensive evaluations of mainframes.2 (see footnote)

1 National Strategy to Secure Cyberspace –Draft September 2002, Page 21
Securing The Critical Infrastructure
White Paper

The Myth and Reality of the Mainframe

The Myth

There is a pattern of common thinking that IBM® mainframes are just old legacy systems that are diminishing or going away, and being aggressively replaced by other platforms such as Unix® and Windows NT® servers. That is simply not true. The power, speed, capacity and performance to handle the millions of transactions required within our critical infrastructure exist only on mainframes.

Mainframes are at the very core of most of the businesses within the segments of the United States’ critical infrastructure. The vast majority of this nation’s Critical Information Infrastructure resides on – and is processed by – IBM mainframes. In general, these mainframes are less secure than they were just seven to ten years ago.

Enterprises running mainframe systems report that 80% to 85% of their mission-critical workloads still involve the mainframe. But mainframe information security funding has been cut or redirected, personnel have drifted to new opportunities, and most security policies are obsolete in the face of technological change. Mainframe host security, once a byword for high-quality, rigorous information security, has become an exercise in nostalgia. Organizations and government agencies must refresh their mainframe security policies and technologies as vigorously as they refresh technologies elsewhere, or risk intrusions from new threats and as yet unidentified areas. Without effective intrusion management processes, these mainframes can be penetrated from the outside by hackers, terrorists, and domestic antagonists. They are also vulnerable from threats inside the organization – whether from disgruntled employees or just plain human error.

Several factors contribute to this decline in mainframe security, and they can be verified. The biggest factor, of course, is the Internet and the many points of entry it offers intruders. An abundance of PCs, workstations, servers, laptop computers and peripheral devices can communicate with the mainframe via the Internet. In fact, industry research firm Gartner Group estimates that 90% of the nation’s mainframes are already connected to the Internet and 50% of them are doing some form of e-business today.
The following pages detail the conditions that have eroded – and continue to erode – mainframe security. Knowing the factors that adversely affect the mainframe is one thing. Doing something about them is something else entirely. To mitigate the risk to national security, there must be much more focus on IBM mainframes within the nation’s Critical Information Infrastructure Protection Plans and more emphasis on the intrusion management process within the many companies that rely on the mainframe as the core of their business operations.

**The Reality: Mainframes Are Alive and Healthy**

Mainframes have never been on the decline. To the contrary, they have continued to grow. In fact, in the three months following IBM’s announcement of its z800® entry level mainframe server in March 2002, 200 customers ordered it.

Admittedly, there has been a modest decline in actual physical mainframe sites (organizations with mainframes), but actual numbers used to measure the use, size, power and growth of mainframes have continued to grow by extraordinary rates.

Companies reliant on the mainframe have not abandoned the platform, and companies adopting a networking approach to business continue to look to IBM for mainframe based solutions.

As evidence, one need only review IBM’s Fiscal Year 2002 Second Quarter results for the period ended June 30, 2002. While announcing a 7% decrease in overall revenues from the second quarter of 2001, as well as a decrease of 16% in hardware revenues, IBM noted that shipments of its zSeries® (mainframe) line grew 4%, as measured in Millions of Instructions Per Second (MIPS). And IBM’s leading middleware product, WebSphere, grew 17% in the quarter. Even in a difficult economic environment, companies, organizations and agencies increasingly are looking to the IBM mainframe for data management and networking applications.

Over the last seven years, mainframes have grown significantly, as evidenced by increases in two key measurements: increase in yearly MIPS shipped (close to a 900% increase between 1994 and 2001) and the percentage of increase in installed MIPS for the same period (nearly 500%).
What is really interesting is the misconception that the growth of the Internet has eclipsed the deployment of mainframes. In actuality, the Internet has grown at a lower rate than IBM mainframe processing power over the last several years.

The Mainframe: Main Repository of the World’s Data
It has been estimated that between 70% and 80% of the world’s data resides on the mainframe. Just a few short years ago, some people projected that the Y2K issue and related concerns would serve as an impetus for mass migration off the mainframe and onto other platforms. This has not been the case. While there may have been some minor shifts, nothing significant occurred, and the preponderance of the world’s data remains exactly where it was on December 31, 1999 – on CMOS®, Multiprise®, S/390® and zSeries machines – in short, on the mainframe.

It is important to recognize that the mainframe continues to be the residence of choice for a preponderance of mission-critical applications and data for all categories of the Nation’s Critical Infrastructure.

Internet: The New Reality of the Mainframe

The Mainframe and The Internet
It seems that when most people think of cyberspace, they are thinking about PCs, network servers, network devices, the Internet and even pervasive computing devices such as Palm Pilots and cell phones. But not mainframes.

The truth is something else entirely. As noted earlier, Gartner Group estimates that 90% of the nation’s mainframes are already connected to the Internet and 50% of them are engaged in some form of e-business. The use of the Internet in mainframe computing provides many access points into the system, representing vulnerabilities. An intruder can exploit these vulnerabilities and pose severe risk.

There are five categories of risk associated with Internet access:

- Implementation Vulnerability;
- Design Vulnerability;
- Configuration Vulnerability;
- Unauthorized Use; and
- Unauthorized Access.
A system itself may have been designed to be safe; yet its installation and use may lead to multiple sources of risk.

The Mainframe’s False Sense of Security
Another misconception regarding the mainframe is that it is, by its very nature, secure – that it has innate integrity and offers unparalleled protection to its owners. People believe that the mainframe is, in fact, the most trustworthy system within a business, a fact that has been tested, proven and verified in the past – before the development of TCP/IP (i.e., the Internet). Since the mainframe has come to represent the benchmark of what secured computing should be (and because IBM markets it as a highly secure and reliable system), attention and resources have been diverted to other and newer technologies known to be less secure – to PCs, NT and Unix servers, networks and the Internet. In reality, this change in emphasis should not have been a question of “diversion.” Rather, it should have been a matter of “expansion.” Not a question of one or the other, but an issue of one and the other. Unfortunately, thanks to a number of factors, mainframe systems by and large are very vulnerable to unauthorized access, misuse and attack.

The Current Status of Mainframe Security

Mainframe Security Is Declining – Not Improving
While the technology to secure mainframes has increased significantly during the last decade, the level of applied security on mainframes is still far less than it was seven to ten years ago. This condition has been observed through the field experience of Vanguard’s professional services staff, and was confirmed through industry research by Gartner Group.

During the fourth quarter of 1998, Vanguard Integrity Professionals and Gartner Group completed research on the status and future of mainframe security. Garner Group subsequently issued an Advisory Services Technical Research Note with the following warning:

“In the vast majority of organizations, the overall quality of mainframe security will continue to deteriorate to early 1980s levels over the next two to three years (0.9 or 90% probability).” – Gartner Group Advisory Services Research Note
Many factors affect mainframe-computing systems after they are implemented. They do not remain in a static state. They are in a constant state of change; if not accommodated, such change causes the system to experience atrophy. A significant atrophy of security can occur in just a few short weeks and, in a matter of months, security can be completely out of control. The most significant factors eroding mainframe security over the past several years include the following:

1. Extending the mainframe outside the corporation;
2. A decrease in traditional audits;
3. Loss of skilled personnel;
4. Movement within the user work base;
5. Technology refreshes; and
6. Explosive increases in the numbers and types of users.

The Internet has created new access portals and a new class of users and, in so doing, has changed the risk factors. Some of the risk factors listed above have not yet been addressed by existing security measures. New and very different requirements must be addressed on the host, the mainframe, and within the domain itself.

Change must occur at that level. Host-based identification and authentication, access controls, logging, reporting, and intrusion management must be evaluated and improved to address new risk/threat scenarios. In order to minimize the number of information security breaches to mainframes and reduce financial loss, private businesses and government agencies must take a close look at the real threat to their Information Systems and deploy solutions accordingly.

**The Financial Costs of Mainframe Intrusions**

Researchers recently discovered a direct link between power poles and violent crimes. The survey on violent crimes showed there are far fewer incidents of such crimes in small mid-western towns with few power poles than in large metropolitan cities such as New York, Chicago and Los Angeles, which all have large numbers of power poles and statistically many more violent crimes.
Of course, many sane people reject the conclusion of these researchers. While there is a correlation between the number of power poles and violent crimes, the actual cause of more crime in large cities is likely the larger populations, rather than the power poles.

This demonstrates how careful one must be with statistical information. That is true of the FBI/CSI 2002 Computer Crime and Security Survey. The report concludes that viruses and worm outbreaks are the most frequent type of cyber attack, with 85% of respondents reporting such attacks over the last year. Since virus and worm protection devices are readily available, we also see more companies implementing such types of technologies. In addition, the report states that insider and outsider attacks are almost evenly divided – this represents a significant decline in insider attacks from previous years.

However, reviewing the true dollar amount of financial losses from security attacks, one can readily see that the theft of proprietary data and financial fraud -- $171 million and $116 million, respectively – greatly eclipse the financial losses of all other categories of loss added together, including insider net abuse; virus; laptop theft; denial of service; sabotage; telecom fraud; unauthorized insider access; and systems penetration.

The most interesting point is that these major dollar losses occur primarily on a host computer – a mainframe – behind the Internet, the firewalls and network access controls.

There is an additional piece of information that supports the above point. Vanguard Integrity Professionals’ security consultants work at numerous enterprises with mainframes across all industries and businesses. We have observed that most enterprises’ critical and proprietary assets reside on their mainframes. We have also observed that access controls on these mainframes have weakened and have moved from a need-to-know paradigm to more of an open-system-access model.

Clearly, there is much work to be done in assuring true mainframe security and intrusion management. That work is being done by Vanguard Integrity Professionals – Nevada.
The Vanguard Approach to Mainframe Intrusion Management

Vanguard Integrity Professionals-Nevada provides the industry’s most comprehensive set of security add-on tools for the IBM Security Server (RACF) – the industry’s premier product for securing valuable corporate data on mainframes-making it easier than ever before for organizations to automate access, authentication and intrusion management of their mainframe environment. Our robust security management solutions minimize risk through a dynamic measurement and management process that strives to provide continuous improvement of security. Security administrators, managers, and CXO’s can get piece of mind through the knowledge that they are protecting critical resources, digital assets and adhering to industry Best Practices. Vanguard’s multi-tiered approach to comprehensive, integrated security management includes:

1. **Prevention** – Establish security policies and incorporate them into Information Systems.
2. **Access** – Policy-based infrastructure that allows management of access to sensitive or critical information assets.
3. **Monitoring** – Automate real-time monitoring and protection of critical assets and user activity. Provide detection and track activity that affects sensitive data, documents, and transactions.
4. **Analysis** – Provide data logs and analysis of security risks
5. **Response** – Immediately identify intrusions and respond quickly and efficiently with corrective action.
6. **Enforcement** – Facilitate compliance with standards, policies, rules and settings.
7. **Audit** – Ensure constant measurement of effectiveness in order to neutralize new risk and threat agents.
Vanguard Enablers

Vanguard's exclusive, context-sensitive Enabler™ technology links Vanguard's Security Solutions together. Seven powerful Enablers let the security administrator seamlessly move in and out of each product without missing a beat:

**SmartLink™**
Provides the process-driven backbone that links Vanguard Administrator, Analyzer, Advisor and Enforcer together.

**Find-it-Fix-it-Fast™**
Minimizes steps and keystrokes when using SmartLink or making corrections. Security administrators can quickly fix any exposure before it becomes a disaster.

**RiskMinder™**
The only available solution that continuously and automatically works in the background, even while the security administrator is performing other security management tasks, to uncover and immediately notify the administrator of risks found in the security system.

**SmartAssist™**
Explains identified risks, offers risk assessment, and explains how to fix the most common security problems.

**eDistribution™**
Sends key report findings via e-mail only to those who need to know. This may be done on a scheduled basis or in real-time when a specified event occurs.

**AutoPilot™**
Performs continuous, unattended operations, including monitoring and updating processes for scheduled events.

**QuickGen™**
Conveniently enables the user to generate free-form output (usually RACF command oriented) to produce RACF commands or ad-hoc customized reports. QuickGen can be run online or in batch mode.
Vanguard Integrity Professionals provides enterprise security software and services that solve complex security and regulatory compliance challenges for government agencies and large enterprises around the world. With solutions for Identity and Access Management, Audit and Compliance, Security Administration and Intrusion Detection, Vanguard automates processes necessary to identify and mitigate the risks customers face. Vanguard’s customers receive a rapid return on investment and are able to focus on other critical business needs thereby becoming more productive and more secure. For more information, visit www.go2vanguard.com.

For More Information

To learn more about the features and benefits of Vanguard enterprise security software solutions, visit www.go2vanguard.com.

Security Management Solutions:
- Vanguard Administrator
- Vanguard Advisor
- Vanguard SecurityCenter

Audit and Compliance Solutions:
- Vanguard Analyzer
- Vanguard inCompliance
- Vanguard Enforcer
- Vanguard Policy Manager

Access Management Solutions:
- Vanguard Authenticator
- Vanguard ez/SignOn
- Vanguard ez/Token
- Vanguard Tokenless Authentication
- Vanguard ez/Integrator
- Vanguard ez/AccessControl
- Vanguard Registration Manager
- Vanguard PasswordReset

Intrusion Detection Solutions:
- Vanguard Enforcer

©2007 Vanguard Integrity Professionals
All other copyrights, trademarks and/or service marks are the property of their respective owners.