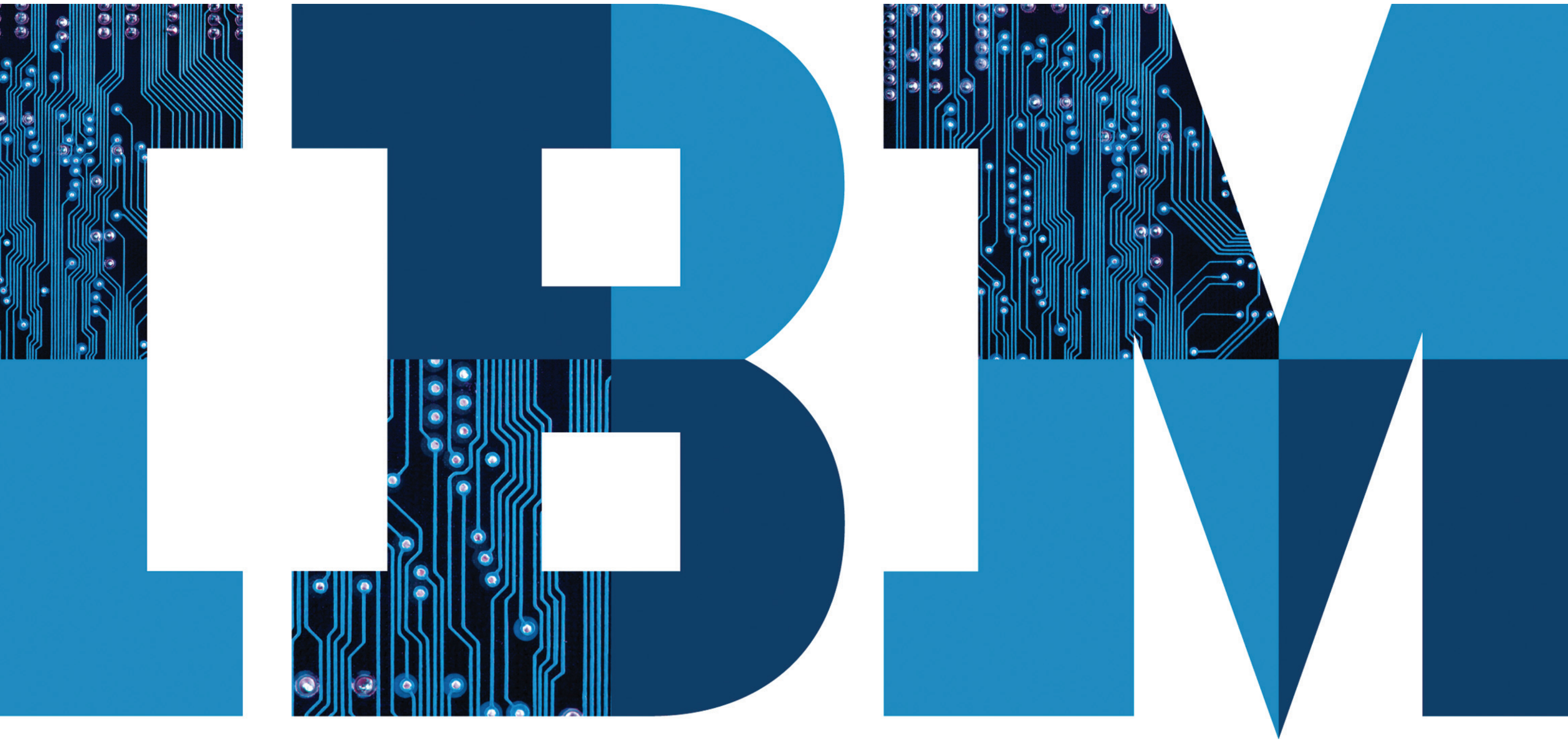
IBM Security
Thought Leadership White Paper

February 2010

IBM solutions for cybersecurity: Solutions for mitigating threats in the government sector



Contents

2 Executive summary

3 Introduction

3 Growing threats to government cybersecurity

4 "Deperimeterization:" Causes and effects

4 A charge for cybersecurity

5 IBM's holistic approach to cybersecurity

6 A closer look at IBM's cybersecurity approach

7 Trusted partners

7 Information assurance

7 Federated security management

9 Operational systems management

9 Governance, compliance, and risk management

10 Situational awareness

10 Layered defense for multitiered architectures

11 Conclusion

12 For more information

Executive summary

Governments around the world are making the protection of critical cyber infrastructures a top priority. These infrastructures play an essential role in the successful functioning of government, helping to ensure national security and economic stability.

Due to a variety of changes that have dissolved the IT perimeters that used to provide protection, today's cyber infrastructures are particularly challenging to secure. Global cybersecurity threats are on the rise, and the intensity and sophistication of attacks are increasing. Nations must embrace new technologies and processes to protect government entities and the citizens they serve.

This white paper discusses the unique features of today's cyber infrastructures and outlines the threats facing government enterprises. It then describes IBM's holistic approach to security and shows how the IBM Security Framework provides solutions for an organization's cybersecurity needs, as illustrated in Figure 2. IBM provides a multitiered containment strategy that addresses information assurance; federated security management; operational systems management; governance, compliance, and risk management; and situational awareness.

The highest levels of government rely on secure networks to provide essential constituent services and meet military and economic objectives.

Introduction

Net-centric technologies play an essential role in the successful functioning of a government's critical infrastructure. Highly linked and interdependent, these ubiquitous infrastructures are critical to a nation's security and prosperity. The highest levels of government rely on secure cyber networks to provide essential constituent services and meet military and economic objectives. These cyber infrastructures must be highly reliable for governments to meet mission-critical responsibilities, including providing information, protecting constituents, and ensuring national financial stability, even in the face of growing threats. Unfortunately, it takes only one adverse cyber event to threaten an organization's entire ecosystem.

Cybersecurity is more challenging than traditional IT security due to the magnitude of the landscape that must be secured. Securing net-centric computing is far more complex than securing traditional IT infrastructures, which have more clearly defined borders and access points.

Today's cyber infrastructures are more complex and vulnerable to attack—and therefore more difficult to protect. Decentralized, service-based computing and collaborative environments with shared touchpoints can increase infrastructure vulnerability. With organizational processes and data now distributed across very intricate infrastructures, it's no longer possible to secure cyberspace by simply setting arbitrary IT borders, centralizing all functions, or severely restricting access. Innovative new solutions are needed to help governments maintain cybersecurity while meeting today's critical IT requirements.

Today's cyber infrastructures are more complex and more vulnerable to attack – and therefore more difficult to protect – than traditional IT security infrastructures.

Growing threats to government cybersecurity

For nations across the globe, information systems are facing an increase in cybersecurity threats, and the attacks are more sophisticated than ever. In 2009, a number of high-profile cybersecurity threats made headlines around the world:

- On April 9, 2009, *The Washington Post* reported that the U.S. electricity grid had been penetrated by spies who left behind software programs that could be used to disrupt the functioning of the system.[1]
- In August of 2009, European news sources reported that hackers used social networking sites to help launch a cyber offensive in recent political conflicts.[2]
- In July of 2009, *The Washington Post* reported that several major government Web sites in the U.S. and South Korea were subjected to a distributed denial of service attack that brought them down for several days.[3]

Incidents such as these highlight the vulnerability of many critical cyber infrastructures. Vulnerabilities exist both internally and externally, and their exploitation can be inadvertent or deliberate. Threats may come from disgruntled employees, professional hackers, organized crime, other nation states, and terrorist groups. The impact of such attacks ranges from the compromise of sensitive information to the disruption of critical government or infrastructure operations.

Recent years have seen cyber attacks progress from small-scale, disorganized hacking to significant, highly organized, and well-financed attacks. The source of these attacks is increasingly international, making them harder to trace and neutralize. Central governments must adopt innovative approaches to counter the increasing frequency and intensity of cyber attacks, and protect the interests of government entities and the citizens they serve.

Recent years have seen cyber attacks progress from small-scale, disorganized hacking to significant, highly organized, and well-financed attacks.

"Deperimeterization": Causes and effects

In order to develop effective new approaches to cybersecurity, we must first understand the forces at work in today's government organizations—forces that have erased the traditional IT perimeters enforced by traditional IT security approaches:

- Organizational dynamics: Department integration, agency mergers, outsourcing, and out-tasking have complicated traditional organizational and IT perimeters, redrawing them to include entities previously considered outside the organization. Combining multiple organizations with different security processes and policies makes it difficult to ensure consistent security management across the extended enterprise, regardless of whether the combination is organizational or operational in nature.
- Workforce dynamics: The number of contractors and temporary employees on government premises has increased dramatically in recent decades, complicating user management and access control, and increasing the potential threat.
- Technological dynamics: Rapid deployment and adoption of technologies like mobility, Web 2.0, and software as a service have changed the basic model of how business and infrastructure services are provisioned and accessed. Newer technologies such as cloud computing compound the exposures.

Security policies and technologies must span numerous different platforms such as clouds, data centers, service-oriented architectures, and collaborative communities.

As a consequence of these changes, the fundamental security model of the government enterprise has evolved, and the government enterprise itself has become deperimeterized. The focus of protection is shifting to individual business objects and key national resources—to concentrate scarce cybersecurity resources on protecting high-value assets. Security policies and technologies must therefore become more fine grained, and provide capabilities that span platforms, clouds, data centers, service-oriented architectures (SOAs), and collaborative communities.

A charge for cybersecurity

Protecting our cyber infrastructure is not an option—it's a requirement. Governments must respond effectively to new security threats and vulnerabilities. In order to improve the speed and accuracy of responses to threats, today's cybersecurity solutions must incorporate automation at every possible opportunity. These security solutions must protect deperimeterized IT environments without hindering work processes, collaboration, and information access, and without compromising the privacy and civil rights of constituents.

Cybersecurity controls must be developed and deployed within the context of multiple infrastructures and organizations in order to meet the needs of diverse government enterprises. There is no single solution that is designed to fit all environments. However, IT managers in the government sector rarely have all the resources required to implement multiple solutions and test how they work in each environment. As a result, organizations often turn to experienced IT security partners like IBM to help them navigate the complexities of cybersecurity.

IBM takes a holistic approach to cybersecurity, combining hardware, software, and services to address the existing threat landscape.

IBM's holistic approach to cybersecurity

IBM takes a holistic approach to cybersecurity, providing comprehensive solutions for the issues governments and the critical infrastructure sectors face today. This approach combines hardware, software, and services to address the existing threat landscape and better position the organization to take advantage of evolving technology and meet emerging threats.

As an organization builds security into and around its IT processes, care must be taken to ensure that all of the various security domains interoperate and are aligned with the organization's overall mission objectives. Without this coordination, the deployed security capabilities may fail to cover the mission priorities and the organization will be unprotected.

IBM has created a comprehensive IT security framework that can help ensure that an organization's essential security domains are properly addressed in a holistic fashion (see Figure 1). The key areas of this framework are:

- People and Identity – ensuring that the right people and systems have access to the right assets at the right time.
- Data and Information – protecting critical data in transit and at rest.
- Application and Process – ensuring application and business services security.
- Network, Server, and Endpoint – staying ahead of emerging threats across IT system components.
- Physical Infrastructure – leveraging digital controls to secure events in the physical world.

All of these domains are driven by the organization's operating principles and policies for managing risk and compliance.

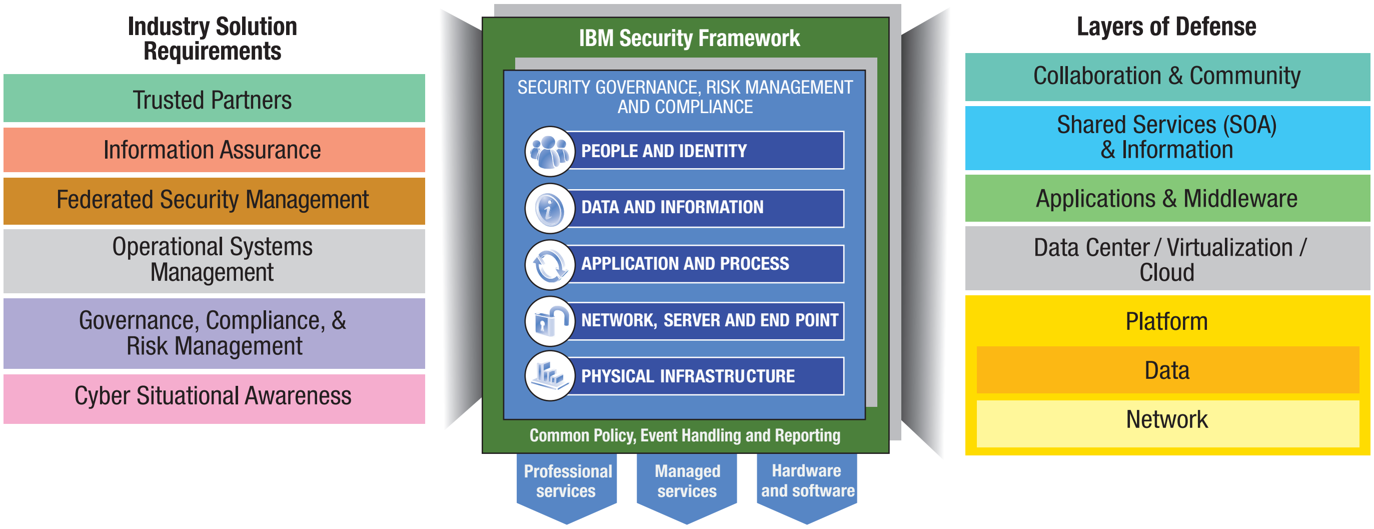

Industry Solution Requirements
Trusted Partners
Information Assurance
Federated Security Management
Operational Systems Management
Governance, Compliance, & Risk Management
Cyber Situational Awareness
IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software
Layers of Defense
Collaboration & Community
Shared Services (SOA) & Information
Applications & Middleware
Data Center / Virtualization / Cloud
Platform
Data
Network

Figure 1: The IBM Security Framework provides a foundation for addressing cybersecurity in a holistic fashion.

IBM's approach to cybersecurity builds upon this proven framework and is designed to help organizations meet the following key requirements:

- Protect each layer of the operational architecture
- Provide federated security management
- Ensure visibility into the operational environment
- Facilitate awareness and resiliency
- Enable effective governance, compliance, and risk management
- Provide assurance

IBM helps governments successfully mitigate threats from both within and outside the perimeter.

IBM offers a combination of proven, off-the-shelf products, coupled with industry-leading research and development capabilities in the field of cybersecurity. IBM delivers industry best practices in security policy and governance, development, engineering, implementation, and support. IBM helps governments successfully mitigate threats from both within and outside the perimeter with solutions that are carefully and securely configured, tested, deployed, tuned, and integrated to meet the unique requirements of each environment.

The IBM Security Framework forms the basis for addressing industry solution requirements across the different tiers of the infrastructure.

A closer look at IBM's cybersecurity approach

The focus of protection is shifting to protect high-value critical infrastructures including government, transportation, energy grids, and the food supply. The IBM Security Framework forms the basis for addressing cybersecurity industry solution requirements by providing risk-based assurance measures and intelligent insight into potential threats based on open standard technologies and industry best practices (see Figure 2).

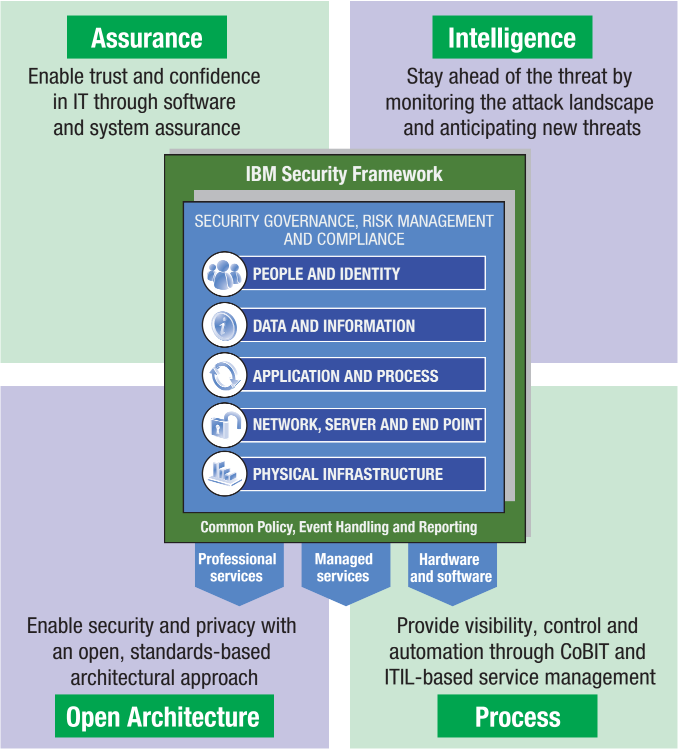

Assurance
Enable trust and confidence in IT through software and system assurance
Intelligence
Stay ahead of the threat by monitoring the attack landscape and anticipating new threats
IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software
Enable security and privacy with an open, standards-based architectural approach
Open Architecture
Provide visibility, control and automation through CoBIT and ITIL-based service management
Process

Figure 2: The IBM Security Framework forms the basis for addressing industry solution requirements across the tiers of the infrastructure, and for providing multiple layers of defense.

The next sections of this document describe these industry solution requirements and layers of defense in more detail.

Trusted partners

A trusted partner is one who requires integrity in supply chain practices and policies. Effective supply chain management practices focus on successful management of partners, product design, manufacturing, transportation, fulfillment, import/export, intellectual property, and customer support. These are necessary to protect against the threat of malicious components, loss of confidential information, and insider threats. IBM supply chain practices address each of these items. IBM has led the global focus on supply chain security and is a founding member of the Electronic Industry Supplier Code of Conduct, ICASI, and IT-ISAC.

Information assurance

Information assurance is the practice of managing risk within or across information systems or instrumented critical infrastructure. Certification and Accreditation (C&A) is a systematic procedure for evaluating, describing, testing, and authorizing these systems prior to making them operational. When faced with the challenges of achieving system C&A in a net-centric environment, organizations face a new set of challenges that includes deperimeterizaton, implementation of shared services, and federated cloud-based environments. These federated components require varying degrees of assurance levels across multiple boundaries and stakeholders.

While previously established C&A practices may be appropriate for systems that have well-defined operational boundaries, a fine-grained multitiered approach to C&A is better suited to today's service-based environments. Focusing the C&A process on more fine-grained discrete layers of the architecture allows for greater visibility into assurance practices employed within a tier and the perimeter defense necessary between each tier. IBM has developed a practical implementation C&A process known as Assured Design. Assured Design is a service-based systems engineering process that facilitates C&A throughout the life cycle of the capability.

IBM offers solutions to ensure the integrity of each tier, providing capabilities to help governments prevent and defend against internal and external cybersecurity attacks.

Federated security management

To secure a multitiered architecture, IBM offers solutions to ensure the integrity of each tier, providing capabilities to help governments prevent and defend against internal and external cybersecurity attacks. These solutions include:

- Intrusion detection/prevention.
- Vulnerability detection.
- Auditing.
- Visualization.
- Data leakage prevention.
- Encryption.

Intrusion detection/prevention: IBM focuses on identifying attacks in progress and alerting the system of the attack and/or preventing the attack from continuing. IBM delivers intrusion detection and intrusion prevention on the same platform, protecting systems through:

- Host intrusion prevention (HIPS).
- Network intrusion prevention (NIPS).
- Endpoint security (desktop protection).
- Web services protection.
- Data leakage prevention.

Vulnerability detection: IBM focuses on edge devices and internal systems that are reachable by potential attackers via the Internet. Vulnerability detection takes two forms:

- Black-box detection, where scheduled or continuous scans monitor network and server devices and application software stacks, looking for known vulnerabilities
- White-box detection, where software is checked during the software development lifecycle for vulnerabilities in the software code

Auditing: IBM focuses on the logging of security events such as administrator, privileged user, and user interactions on a variety of devices, including network switches, routers, servers, and firewalls. This data can be instrumental in understanding the effect of security attacks, access control events, and authorized and unauthorized changes to the system. Audit data can be combined with other data to provide a broader security operations perspective.

Visualization: IBM provides dashboards that convey the overall security posture of the critical infrastructure through analytic visualization systems and security event viewers. A variety of technologies can be employed in this area, including business intelligence systems and mashup technology that allow users to visualize and analyze combinations of data and even create their own applications without changing code.

Data leakage prevention: One of the emerging areas of concern for any enterprise is the loss of sensitive business-critical information, either intentional or accidental. IBM addresses data leakage prevention (DLP) through enhanced visibility and real-time control of network ports and internal traffic, even on multigigabit speed networks.

Encryption: From the Data Encryption Standard (DES) to the Hash Message Authentication Code (HMAC), IBM has been at the forefront of advanced encryption development.
IBM recently announced another cryptographic breakthrough—fully homomorphic encryption—which allows encrypted information to be analyzed without compromising the confidentiality of the data. This advancement has dramatic implications for strengthening cybersecurity, particularly in cloud computing environments.

These solutions support a truly distributed approach that allows data to be securely shared and processed. While intrusion prevention and detection systems are important elements of the overall protection approach, they must be combined with other capabilities in order to provide a complete operational solution.

IBM offers a full range of cross-platform operational systems management, virtualization, and cloud computing solutions.

Operational systems management

A robust network and systems management infrastructure is the foundation for monitoring, managing, and securing the technology infrastructure and operational environment. IBM's network and event management capabilities use agent-based and agentless mechanisms to gather performance and fault information from computing and network devices throughout the infrastructure. This gathering of information is an ongoing process to build a knowledge base of the network topology, assets, and defenses. This information is critical during an attack, providing an understanding of the system's operating baseline. Correlating this data with security sensor and vulnerability information from other areas of the infrastructure can help identify the source and the targets of the attack. System monitoring also provides historical performance and fault information which can be critical data during event triage. IBM offers a full range of cross-platform operational systems management, virtualization, and cloud computing solutions.

> ***IBM's compliance strategy is distinguished by the fact that it addresses all stages of the IT lifecycle, rather than only one point or several points.***

Governance, compliance, and risk management

IBM has developed a strategy of comprehensive security through governance and risk management. This strategy is designed to maximize business resilience and continuity. Compliance is the practice of ensuring that governance and risk management practices are appropriately maintained. IBM's strategy is distinguished by the fact that it addresses all stages of the IT lifecycle, rather than only one point or several points. IBM's strategy is a holistic, integrated approach to IT governance as a whole, which also applies straightforwardly to the problem of IT security. IBM's solution is characterized by a number of elements:

- A process-centric, policy-driven approach to governance, which drives accountability at the process owner level to unlock domain expertise and ensure that policies are enforced consistently
- Improved visibility into varying forms of risk—and their potential business impact—throughout the organization
- The incorporation of critical information uncovered through key performance and process metrics
- Shared processes, risks, and controls across business units to reduce complexity, eliminate duplication of efforts, and demonstrate interdependencies between key business processes
- Enhanced change management for organizational structures and business processes to improve business agility

Situational awareness

In-depth analysis of network traffic data (dynamic real-time deep packet inspection, or DPI) is necessary to identify and characterize attacks on the network. IBM integrates these capabilities into networks and IT infrastructures, scales them to support the network traffic data rates of small offices all the way to the largest government enterprises, bases them on industry standards, and employs proven commercial off-the-shelf (COTS) products. This approach can help organizations continue to protect themselves against increasingly sophisticated attacks.

Many government organizations have deployed numerous security controls including intrusion prevention and detection systems, enterprise security management systems, and sensors that can capture traffic in real time for analysis. While these tools enable organizations to improve their security posture, they can also result in an overwhelming volume of event alert streams, logs, and audit records that contain precious intelligence that is not exploited. IBM's solutions enable organizations to consolidate and correlate these events and data automatically, at line speeds, and present them to the security analyst in a semantically meaningful way, providing security operators, security intelligence analysts, and system administrators with valuable information for defending their cyber infrastructures.

In conjunction with addressing industry solution requirements for cybersecurity, the IBM Security Framework also provides layers of defense for a multitier containment solution.

Layered defense for multitiered architectures

In conjunction with addressing industry solution requirements for cybersecurity, the IBM Security Framework also provides layers of defense for a multitier containment solution that spans platforms, cloud computing/data centers, middleware and SOAs, and collaboration communities (see Figure 2). This strategy protects assets and processes within each tier and provides containment (defense in-depth) to safeguard the tiers from one another.

Collaboration and Community: Traditional security controls (such as groups, roles, and role-based access control) are ill-suited for collaborative Web 2.0+ environments. End users choose security controls in the context of their tasks with usability in mind. Finely integrated compliance processes are necessary, as the lack of natural perimeters leaves no place for bump-in-the-wire security solutions. IBM's assets at this tier include a suite of middleware tools for managing business processes and communities of interest, including the capability to extract, formulate, and analyze social networks.

Shared Services (SOA) and Information: IBM's offerings at this tier include mashup technologies that enable the quick composition of situational applications at a fraction of the time and cost of traditional IT applications, enabling clients to "plug into" existing core internal enterprise information infrastructures. Advanced capabilities include security analytics, stream-based network security, and intrusion detection and prevention, including the ability to do deep content inspection both at the network and platform levels to detect the leakage of sensitive information.

Applications and Middleware: IBM has a significant security presence at the applications and middleware tier, providing tools that help ensure the security and compliance of Web applications throughout the software development lifecycle. IBM also offers automated source code analysis technology that provides precise details and remediation advice on software vulnerabilities, including coding errors, design flaws, and policy violations. New middleware offerings provide the ability to perform analytics and forensics on high-bandwidth streams in an efficient and scalable fashion.

Data Center/Virtualization/Cloud: With IBM's industry-leading systems management and security solutions, systems administrators can quickly and easily detect malware and vulnerabilities while managing and monitoring system and application health from a central location. IBM automated provisioning, virtual machine security, and cloud management solutions help customers effectively manage highly virtualized environments.

Platform (OS, Data, Network): IBM's security assets include advanced technologies for inspecting network traffic and analyzing information flows at carrier speeds. IBM also offers high-assurance platforms that enable reliable, secure, and automated data sharing at different assurance or classification levels. IBM has a complete portfolio of assets aimed at protecting data at rest and in transit over the network. This includes advanced multilevel security (MLS) information management and MLS Enterprise Service Bus technologies.

IBM automated provisioning, virtual machine security, and cloud management solutions help customers effectively manage highly virtualized environments.

Conclusion

The IBM Security Framework provides the foundation for IBM's cybersecurity coverage, reflecting IBM's belief that a fine-grained, multi-tiered strategy is the most effective way to meet the challenges of securing today's cyberstructures. IBM has solutions in every key area of this model that satisfy each layer of the underlying strategy. These solutions can stand alone or be combined into an integrated, holistic architecture designed to meet the specific needs of a particular government organization or site.

For more information

To learn more about how IBM cybersecurity solutions can help you prevent and defend against cyber attacks, contact your IBM sales representative or IBM Business Partner, or visit **ibm.com**/security.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2010
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.
IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

Please Recycle

[1] Nakashima, Ellen, and R Jeffrey Smith, "Electric Utilities May Be Vulnerable to Cyberattack," *The Washington Post*, April, 9, 2009. www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040803904.html

[2] "Social networks used for Georgia cyber attacks," Euranet, August 18, 2009. www.euranet.eu/eng/Archive/News/English/2009/August/Social-networks-used-for-Georgia-cyber-attacks

[3] Nakashima, Ellen, Brian Krebs, and Blaine Harden, "U.S., South Korea Targeted in Swarm Of Internet Attacks," *The Washington Post*, July 9, 2009. www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html