A Sweeping Approach to Security

An IBM® Redbooks®
Point-of-View publication by the
IBM Academy of Technology

By **Chung-Sheng Li**, Ph. D., Director IBM Research, **Katsumi Ohnishi**, IBM Executive Architect, and **Josuyla R. Rao**, Director IBM Research

Highlights

Adopt a broad security approach that anticipates and stops attackers from infiltrating your system:

- Change your security paradigm from a traditional perimeter defense to a fine-grained, micro-perimeter security continuum.
- Employ micro-perimeter defense and security intelligence, which are the keys to addressing emerging threats in trending models of mobile, social, and cloud computing.
- Shift your solution from products to an integrated, comprehensive security intelligence approach.
- Implement security intelligence to mitigate risks from growing data volume, proliferation of clouds and mobile users, and web technologies.

Current security landscape

The security desktop icon on your computer, which is often depicted as a shield, represents a personal firewall. It protects against threats and attacks and searches your system for intruders that breached the wall. Although this safeguard is a good example of fine-grained security, organizations do not always establish similar safeguards within their enterprise boundaries. As a result, many servers that are critical to a business continue to rely on coarse-grained safeguards of corporate firewalls and intrusion detection and prevention mechanisms.

Businesses and governments today must take a broader approach to securing information from malicious attackers or infiltrators. This task is not easy when users demand fast and convenient access to information that they expect to be protected. Consequently, organizations increasingly need to implement a smarter approach that relies on fine-grained control of access privileges and far field detection of potential and seemingly unrelated threats. Such an approach must also rely on multitier containment methods to isolate intrusions and to minimize damage.

The dilemma for businesses is that they must allow access to their systems to enable tasks and services, while safeguarding information assets. However, the risks continue to grow. For example, data volumes are constantly growing. Cloud, mobile, and telecommuting users are accessing networks with various devices from multiple locations. Applications increasingly use the Internet to collaborate and communicate. And by using Web 2.0 technologies, users from outside the business can access data and controls. All of these risks illustrate that a security breach can occur anywhere and can potentially cascade into global reverberations.

The response to such risks was to build large firewalls to protect the entire enterprise. However, now the trend is to protect every resource within the network. Such resources include servers, middleware, storage, service-oriented architecture, applications, and information, each of which might have different strategic values.

Reacting to security breaches is not enough to protect the information, networks, and enterprise of a business. You must anticipate and protect against malicious attacks before they occur. To be prepared, you need to view security as a continuum that correlates between physical and virtual events, between seemingly harmless and suspicious events, and between local and global activities. You must adopt the security knowledge that is used in the intelligence and law enforcement communities. In these communities, clues of impending events, such as online terrorist chatter before an attack, are painstakingly gathered and analyzed.

Threat persistence at different levels

Businesses are at risk for internal and external security threats, as shown in Figure 1.

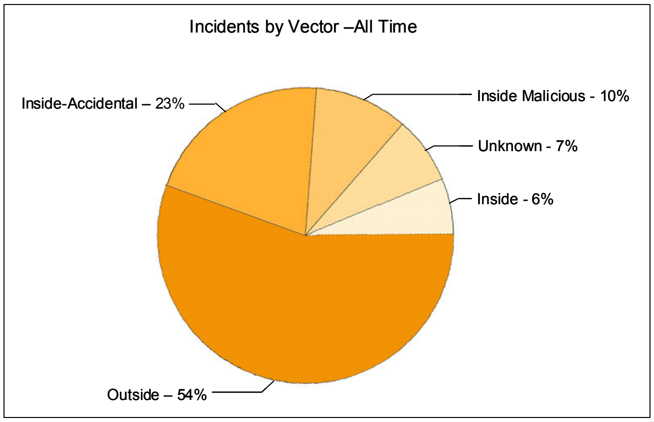


Figure 1 Attack incident percentages

Internal threats include insider malicious attempts and unintentional attempts to breach security with malcode, data leaks, or stealing valuable data, breaking through vulnerable points in the system. External threats include denial of service (DoS), web vandalism and propaganda, botnets (groups of compromised computers that run attack software), and equipment disruption. They also include attacks on critical infrastructure, such as power grids and fuel, communication, and transportation systems.

Security measures to avoid threats include user background checks, restricted access, physical monitoring, platform integrity monitoring, desktop controls, and profiling and auditing user interactions. Such measures also include detecting and preventing the transfer of sensitive data to an unauthorized external site.

Other threats include SQL injection, phishing, and advanced persistent threats (APT), which have been experienced by many well-known companies. An APT is the most severe attack on business assets because of its staged progression over time.

The progress of an APT advances in the following way:

1. Attackers use social media to send seemingly innocent email messages. This technique is known as *phishing*. The email messages contain attachments or hidden applications that break through security. Such applications are called *malware*.
2. Malware installs tools that allow the attacker remote access to control servers and computers behind the firewall.
3. The malware harvests user credentials. Then, it moves to privileged users, and finally it moves to high value targets.
4. The malware establishes access to staging servers at key points.
5. The attacker transfers sensitive data to an outside staging server at an external, compromised machine.

Traditionally, businesses responded to such threats by strengthening the defensive perimeter along the boundaries of the organization. This approach has become increasingly less effective because of the need to conduct business beyond the perimeter. Also, it does not address the threat of insider breaches.

In 2008, for the first time, insider breaches surpassed external breaches, challenging a traditional perimeter-based defense in cyber security.

How you prepare for and manage risks critically affects your bottom line, for example, in terms of costs, success, and effectiveness. Choosing the best protection for your data assets can be confusing considering the proliferation of security approaches and products.

The need for a far-reaching solution

For decades, businesses have trusted IBM with their networks, data, and systems, expecting quality, performance, and cutting edge technology. They now expect the same for asset security. To meet this security market demand, IBM shifts from a product approach to an integrated enterprise approach for security intelligence. This approach is based on key foundational elements that allow for active management, real-time information, analytical correlation, and predictive threat management.

The IBM security intelligence model covers the entire scope of security concerns, from compliance to infrastructure. The framework of this model helps to identify, predict, and remediate IT threats and enterprise risks and to achieve compliance. The security capabilities of the framework use plan-do-check-act (PDCA) cycles. These cycles are based on the principle of *defense-in-depth*, which is a structured, layered approach of security education, prevention, detection, and remediation. This IBM solution was built by thousands of researchers, developers, consultants, and subject matter experts on security initiatives. Plus, IBM has consulted on and implemented thousands of security projects, resulting in practical expertise in best practices and processes.

The security framework

Security intelligence, which is the art and science of anticipating, monitoring, and analyzing risks before they occur, is trending in the current market. Security intelligence provides unified visibility and real-time analytics from security and network devices to server operating systems, applications, endpoints, and infrastructure resources. Security intelligence involves the following key aspects, each of which evolves from a basic level to an optimum level, or from a reactive stance to a proactive stance:

- *People*, who move from a centralized directory to user provisioning with strong authentication, to role-based analytics, identity governance, and privileged user controls.
- *Data*, which evolves from encryption, access controls, access monitoring, and data loss prevention to data flow analytics and data governance. Social computing is increasingly important in intercepting both data leaks and spear phishing attacks.
- *Applications*, which move from application scanning, firewall, and source-code scanning to secure application engineering processes and fraud detection.
- *Infrastructure*, which evolves from a coarse-grained antivirus perimeter defense to asset management and endpoint and network security management (intrusion detection and prevention and deep packet inspection) to advanced network monitoring, forensics, and data mining.

Key solution points for security intelligence

IBM focuses on four key areas in delivering security intelligence: advanced threats, cloud computing, mobile computing, and regulation and compliance.

Advanced threats, or APTs, are sophisticated, targeted attacks that are designed to gain continuous access to critical information. These threats are growing to be more severe and more frequent. The solution is a strong network layer that integrates security, analytics, and threat intelligence, in addition to human and social factors because advance threats often begin as phishing attacks.

By consolidating massive data, security intelligence solutions provide deeper insight to defend against various threats, including APT. The IBM security information and event management (SIEM) solution helps you distinguish real threats from “noise.” It also helps reduce false-positive alerts by using more contextual data and smarter analytics.

Most businesses realize that they need to take advantage of cloud computing but remain concerned about potential risks. As both a service provider and security vendor, IBM is well-positioned to provide a secure infrastructure in the cloud and platforms to isolate information in secure data centers and clouds.

According to Gartner, Inc., 90% of businesses will support corporate applications on mobile devices by 2014.[1] To keep up with this expanded work environment, a top concern for most CIOs is providing employees wide access while securing their mobile devices. IBM focuses on secure access to corporate data while supporting privacy and offers broad security capabilities across endpoint, gateway, and application development. IBM also offers products to integrate and deliver mobile device management and provides access control and federated identity to user’s applications and systems.

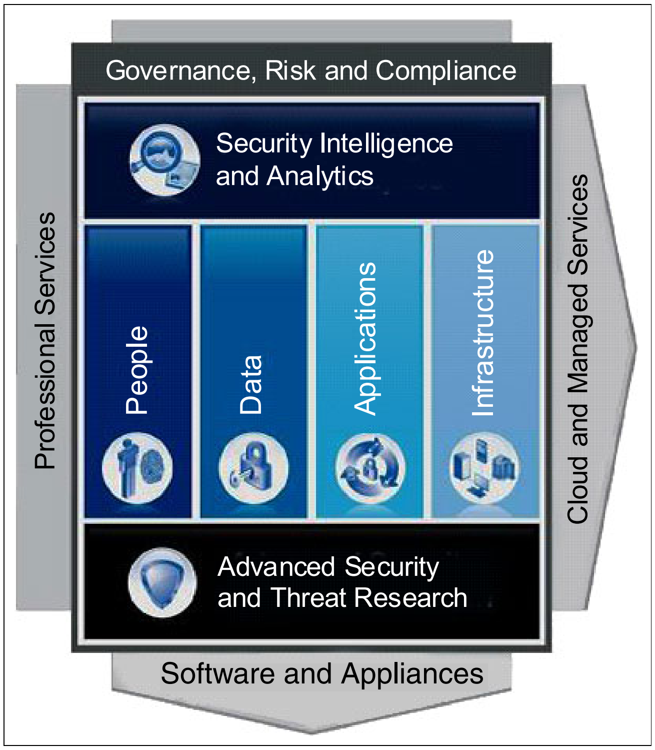
An expansive approach is needed that anticipates, monitors, and analyzes risks before they occur.

Businesses invest great efforts into complying with government and industry regulatory requirements, often at increasing costs. With help from IBM, businesses can map regulations to their IT and business infrastructure, which can reduce costs, streamline system complexity, automate configuration, and simplify monitoring, auditing, and reporting. IBM offers products that provide trusted logging and correlation and that perform orchestration, analytics, and dashboard functions.

[1] Gartner Newsroom
http://www.gartner.com/it/page.jsp?id=1480514

More on security intelligence

Merely building up your perimeter defenses does not secure your business. By using the products and services in the IBM security framework, illustrated in Figure 2, IBM can help you predict, identify, and remediate threats and achieve compliance. To accomplish these goals, IBM offers products and services for the IT infrastructure domains of people, data, applications, and infrastructure, in addition to compliance and security services.



Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Figure 2 IBM security framework

IBM offers end-to-end security intelligence with a full spectrum of services and products for the main business domains:

- People. IBM provides services for identity assessment, role-based analytics, user controls, deployment, and hosting by using the following products:
  - IBM Tivoli Identity and Access
  - IBM Tivoli Federated ID
  - IBM Tivoli Single Sign-on
- Data. IBM provides services for assessment, encryption, data loss prevention (DLP) deployment, flow analytics, and governance by using the following products:
  - IBM InfoSphere® Guardium®
  - IBM InfoSphere Optim™ Data Masking
  - Tape and disk encryption
  - IBM Tivoli® Key Manager
- Applications. IBM provides services for assessment, secure engineering processes, and fraud detection by using the following products:
  - IBM Rational® AppScan® Source Edition
  - IBM Rational AppScan Standard Edition
  - IBM Tivoli Security Policy Manager
- Infrastructure. IBM provides services for network security (intrusion detection and prevention, and deep packet inspection), forensics, data mining, penetration testing, firewall, intrusion prevention systems, vulnerability manager services, and managed mobile protection, by using the following products:
  - IBM Tivoli Network Intrusion Prevention
  - IBM WebSphere® DataPower® XML Gateway
  - IBM Tivoli Endpoint Manager (antivirus by using Trend Micro)
  - IBM Security zSecure™ mainframe security

What's next: How IBM can help

To help you implement security intelligence, IBM offers the services of the IBM X-Force® Research and Development team, which is one of the most renowned commercial security research and development teams in the world. This team studies and monitors the latest threat trends including vulnerabilities, exploits and active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising clients and the general public on how to respond to emerging and critical threats, the X-Force team also delivers security content to protect IBM clients from these threats.

The X-Force team bi-annually publishes the IBM X-Force Trend and Risk Report, which helps clients, researchers, and the public to understand the latest security risks and stay ahead of emerging threats. The report thoroughly explores the most significant challenges that are facing security professionals today. For IBM X-Force Trend and Risk Reports go to:

http://www.ibm.com/security/xforce/downloads.html

In addition to the IBM X-Force team, IBM services and products offer a full-spectrum solution that can help defend your data, applications, and infrastructure from attacks; protect your information assets; and allow secure access for your users.

Resources for more information

For more information about the concepts that are highlighted in this paper, see the following resources:

- IBM Redbooks publications about security

  http://www.redbooks.ibm.com/Redbooks.nsf/portals/Security?Open&count=20

- IBM X-Force Trend and Risk Reports

  http://www.ibm.com/security/xforce/downloads.html

- IBM Institute for Advanced Security

  http://instituteforadvancedsecurity.com/default.aspx·

- *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4944-00, was created or updated on November 29, 2012.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (or), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AppScan®
DataPower®
Guardium®
IBM®
InfoSphere®
Optim™
Rational®
Redbooks®
Redbooks (logo)
Tivoli®
WebSphere®
X-Force®
zSecure™

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.