New and Emerging Threats

Sukhdev Singh

IBM ASEAN

CISSP

CISM

XFE

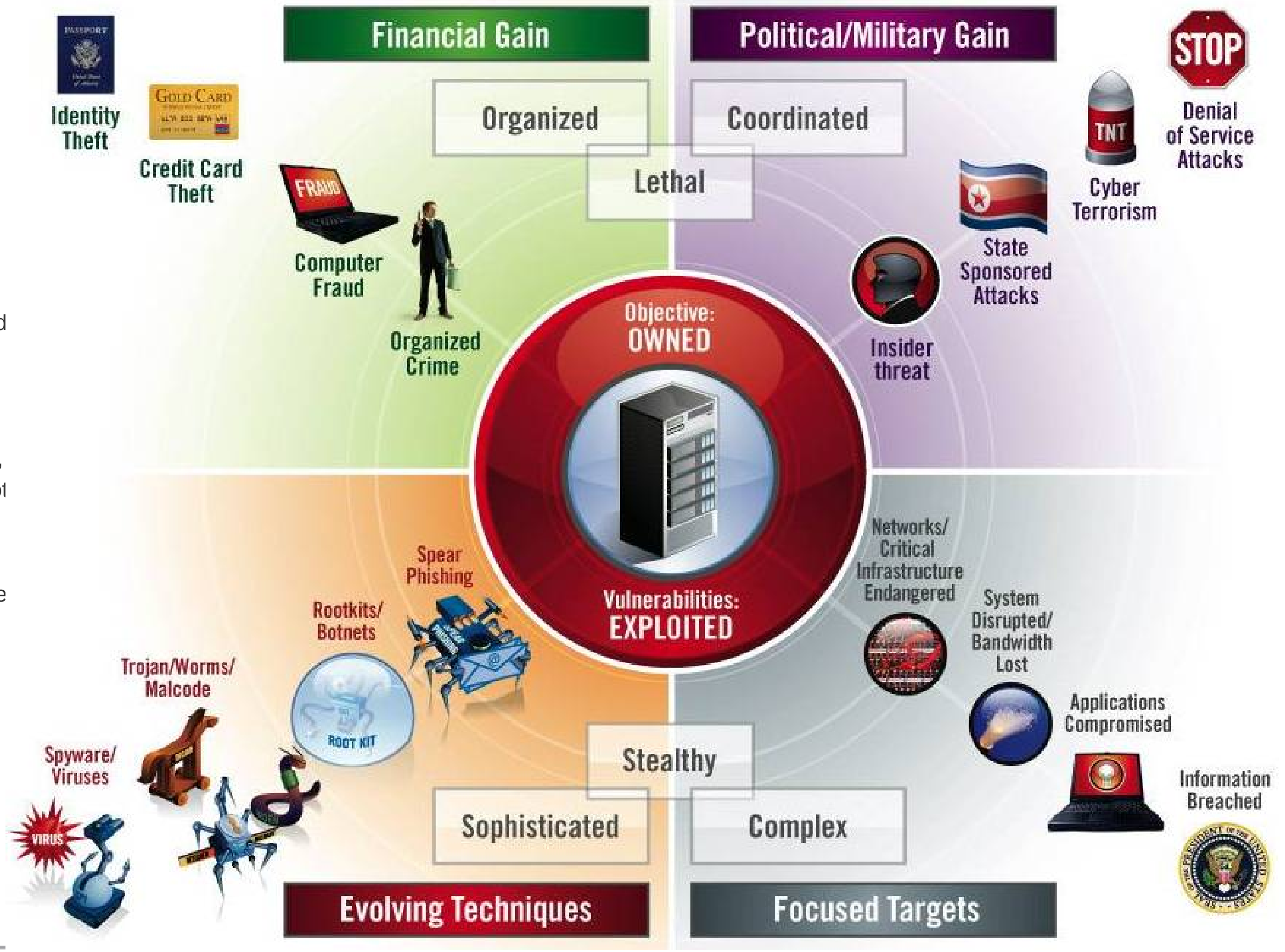
Certified Enterprise Architect (TOGAF®)

Agenda

- Basic Security Concepts – Today and tomorrow
- IBM’s vision of a Security Framework
- IBM Security Guidance
- Conceptual findings from Security Framework

“Amateurs Study Cryptography; Professionals Study Economics”

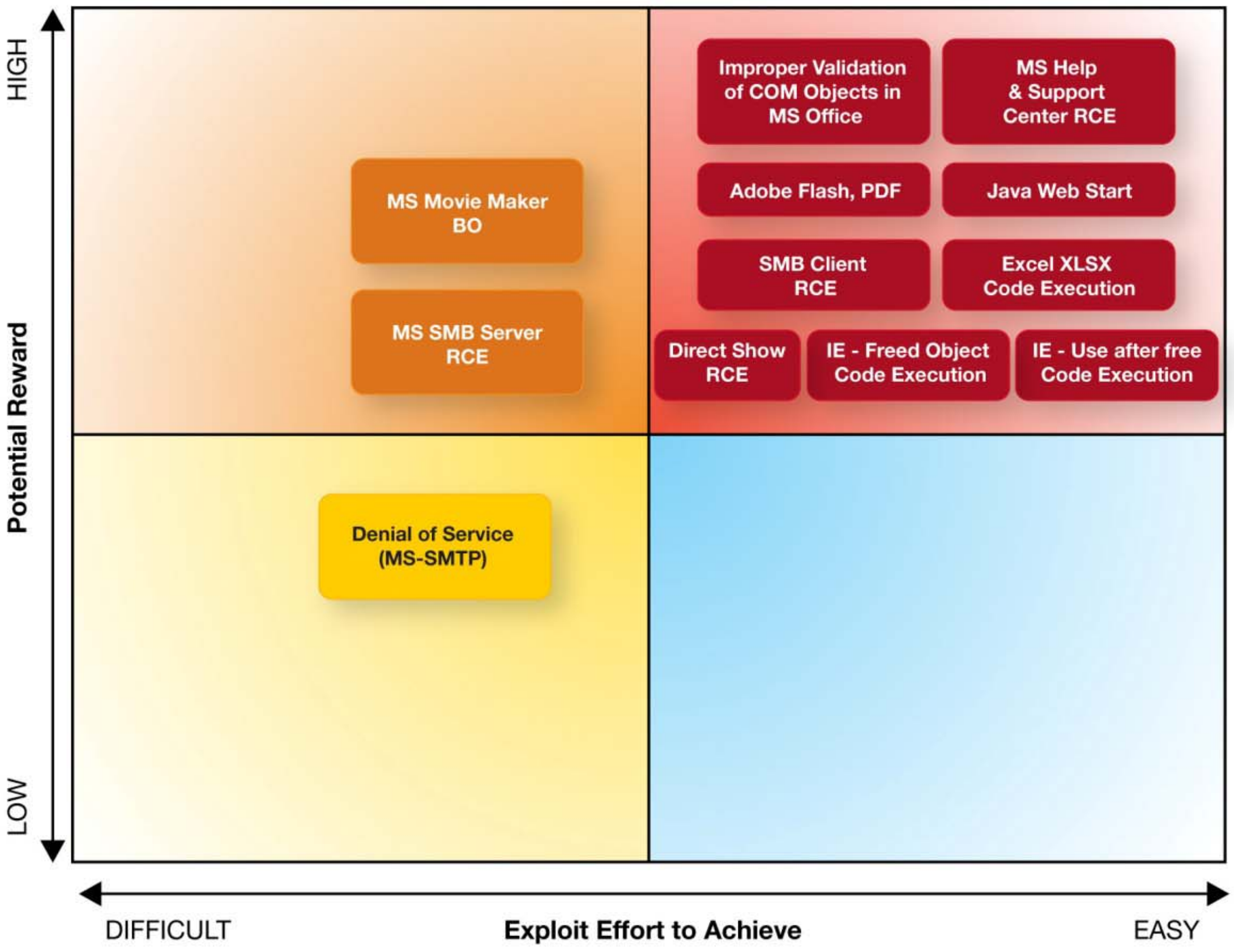
- **Threat Evolution:**
  - A flat world has brought about an unprecedented amount of criminals and cons
  - Attackers keep ROI in mind as well, and constantly evolve their wares in order to re-purpose it for the next flood of attacks
  - High profile vulnerabilities will still be the vehicles for new attacks, however, the low and slow attack vectors cannot be ignored
  - The economics of exploitation must be taken into consideration to better prioritize risk



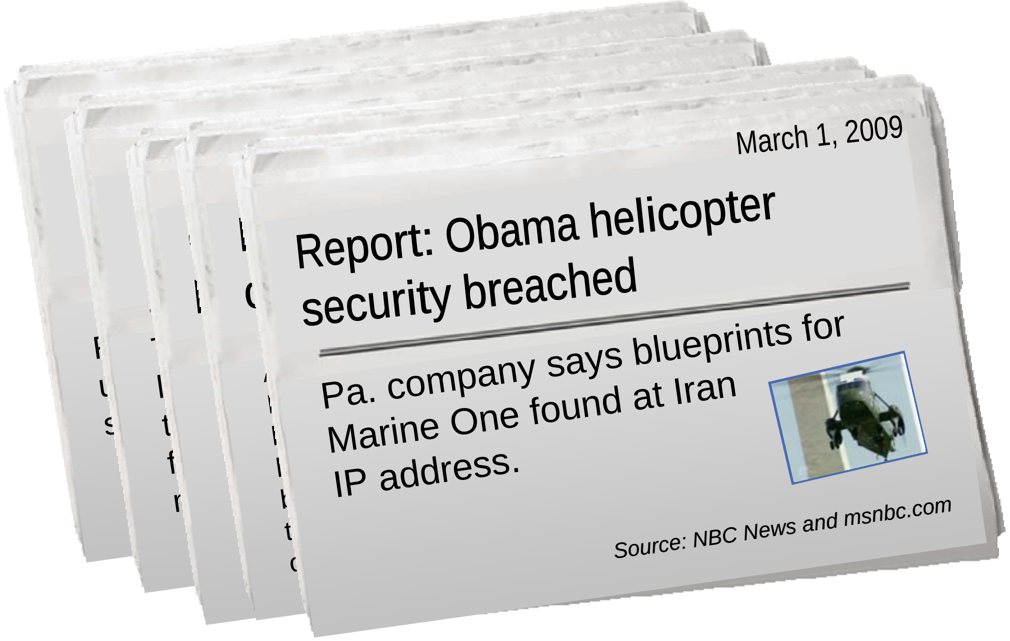
The Economics of Attacker Exploitation

- Economics continue to play heavily into the exploitation probability of a vulnerability.
- Web Browser and Document Reader and Office Document vulnerabilities are very profitable and easily executable.

Exploit Effort versus Potential Reward Matrix


HIGH
Potential Reward
LOW
Improper Validation of COM Objects in MS Office
MS Help & Support Center RCE
MS Movie Maker BO
Adobe Flash, PDF
Java Web Start
SMB Client RCE
Excel XLSX Code Execution
MS SMB Server RCE
Direct Show RCE
IE - Freed Object Code Execution
IE - Use after free Code Execution
Denial of Service (MS-SMTP)
DIFFICULT
Exploit Effort to Achieve
EASY

Impact of cyber security is becoming more apparent…



March 1, 2009

Report: Obama helicopter security breached

Pa. company says blueprints for Marine One found at Iran IP address.

Source: NBC News and msnbc.com

$226 Billion

Economic impact of cyber attacks on businesses has grown to over $226 billion annually.

Source: Congressional Research Service study

158% increase

Security breaches are on the increase: cyber attacks have increased 158% since 2006[1],

Sources: [1]US Department of Homeland Security,

52%

Private-sector statistics show that the insider threat is up more than 52% in the past year.

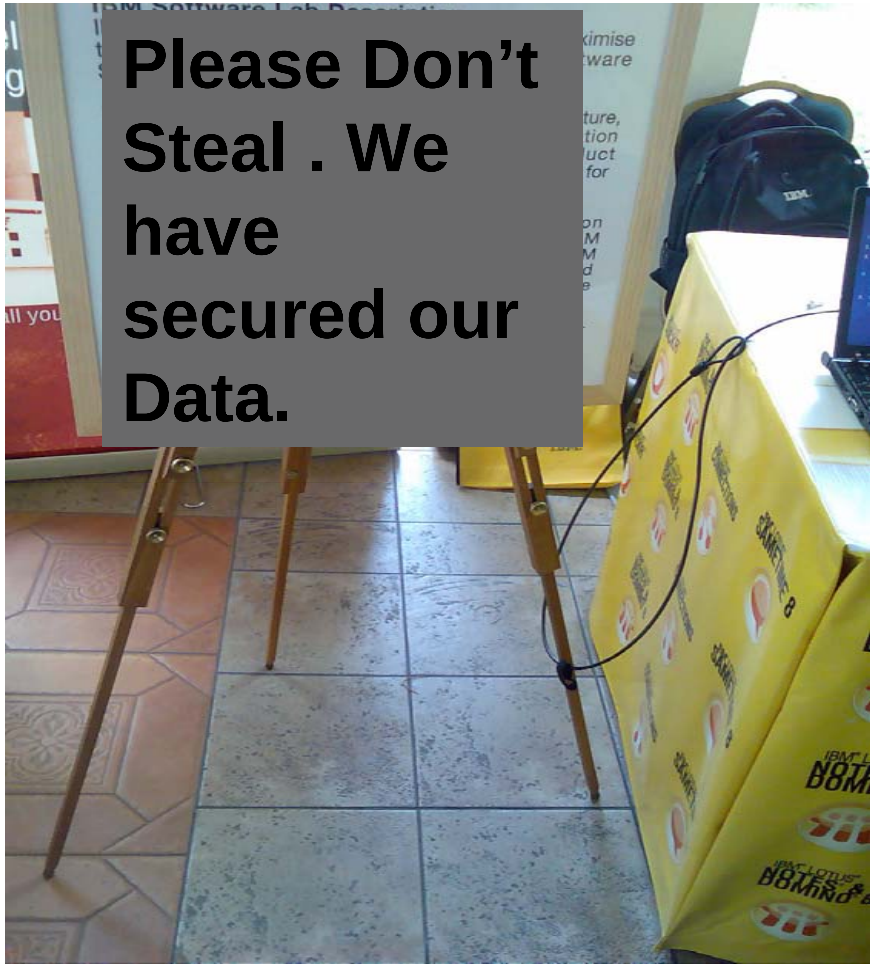
What is at Risk ?

- Interruption of business operations (Lost Revenues)
- Decreased productivity due to additional strain placed on network resources (Lost Revenues)
- Loss of confidential information (Lost Competitive Advantage)
- Increased recruiting and staffing costs (Lost Profits)

ปวดหัว !

You can't manage security by just locking down technology or data or restricting people's access….

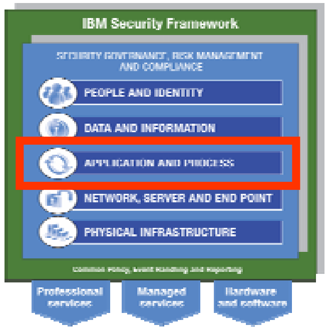
Are you feeling SAFE ? Are you Secure ?

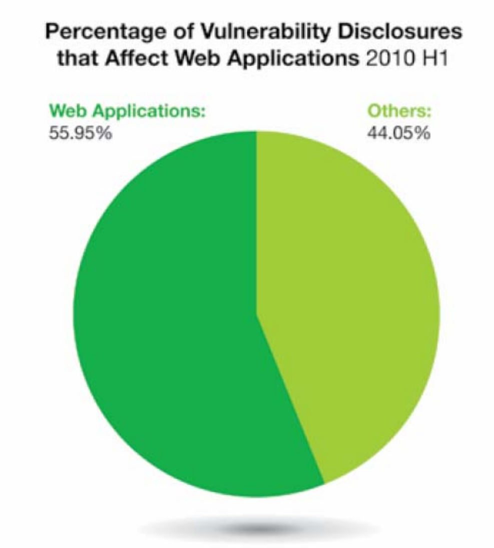


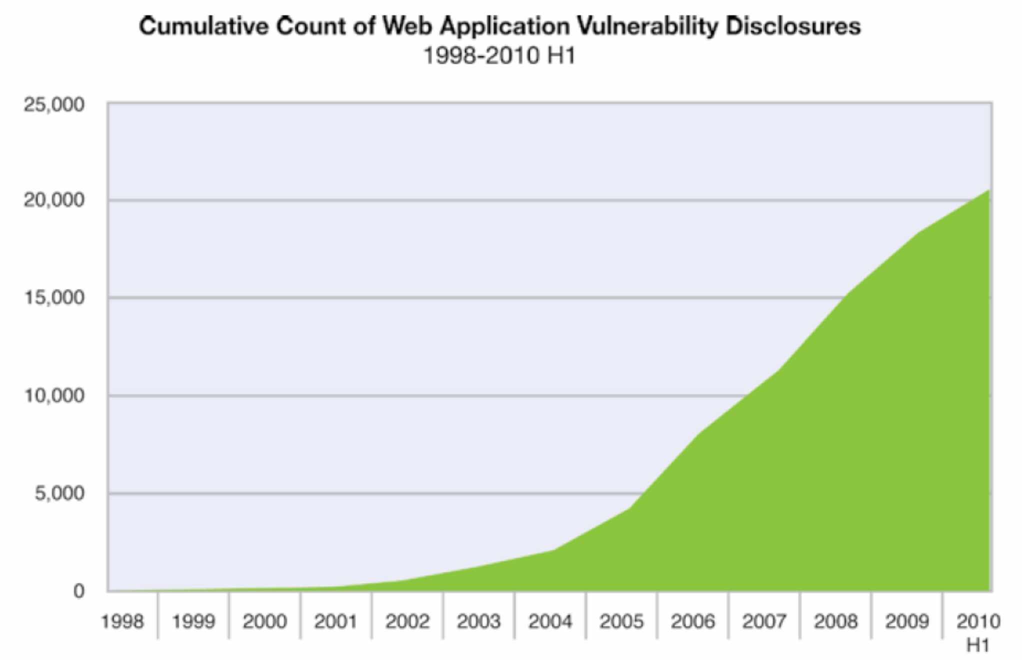
Please Don't Steal . We have secured our Data.

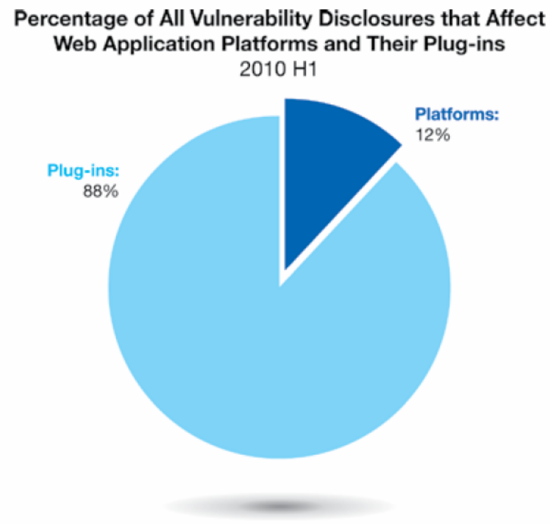
Web App Vulnerabilities Continue to Dominate

- **55%** of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.
- **88%** of web application vulnerabilities affect plug-ins and not the base platform



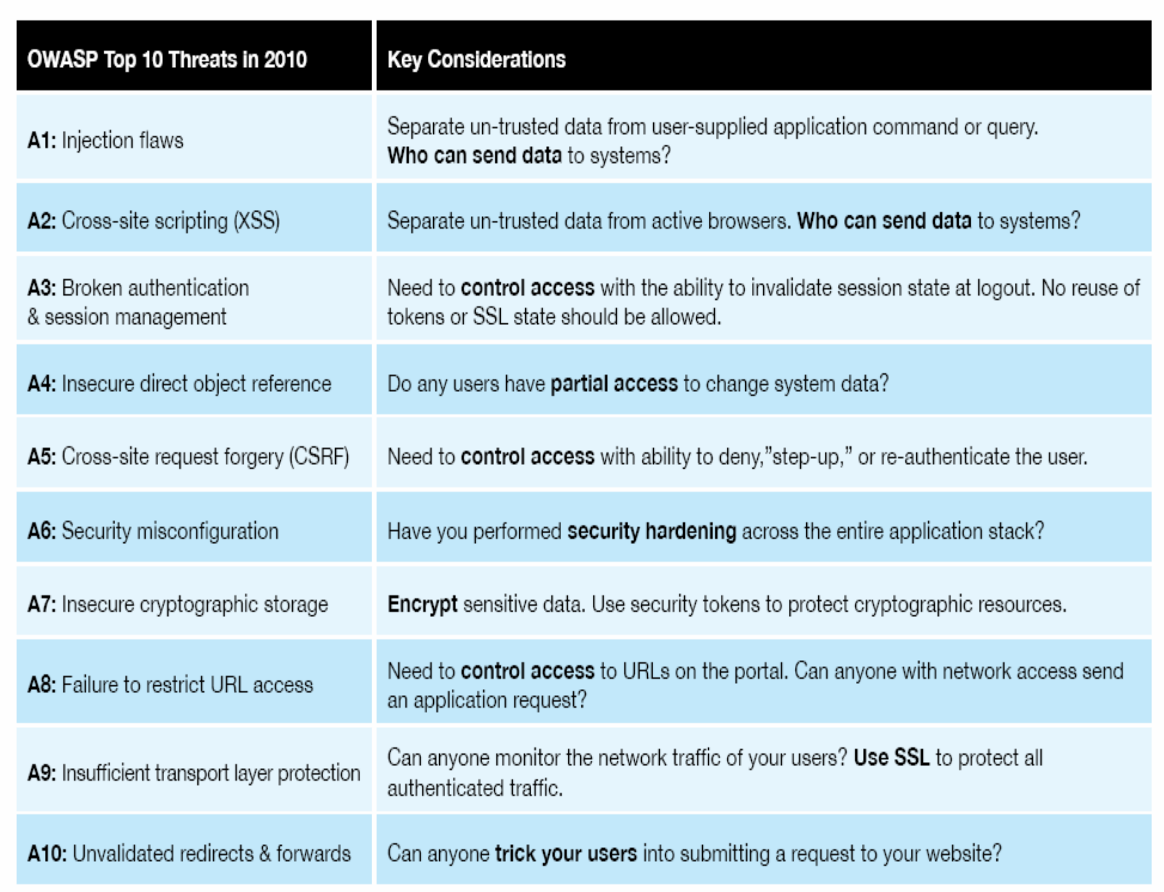

Percentage of Vulnerability Disclosures that Affect Web Applications 2010 H1


Cumulative Count of Web Application Vulnerability Disclosures 1998-2010 H1


Percentage of All Vulnerability Disclosures that Affect Web Application Platforms and Their Plug-ins 2010 H1

OWASP Top Ten Threats Impacting Web Applications

- Half of the vulnerabilities highlighted this year related to user-induced exploits.
- Vulnerabilities such as broken authentication and session management allow attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume user's identities.



OWASP Top 10 Threats in 2010	Key Considerations
A1: Injection flaws	Separate un-trusted data from user-supplied application command or query. **Who can send data** to systems?
A2: Cross-site scripting (XSS)	Separate un-trusted data from active browsers. **Who can send data** to systems?
A3: Broken authentication & session management	Need to **control access** with the ability to invalidate session state at logout. No reuse of tokens or SSL state should be allowed.
A4: Insecure direct object reference	Do any users have **partial access** to change system data?
A5: Cross-site request forgery (CSRF)	Need to **control access** with ability to deny,"step-up," or re-authenticate the user.
A6: Security misconfiguration	Have you performed **security hardening** across the entire application stack?
A7: Insecure cryptographic storage	**Encrypt** sensitive data. Use security tokens to protect cryptographic resources.
A8: Failure to restrict URL access	Need to **control access** to URLs on the portal. Can anyone with network access send an application request?
A9: Insufficient transport layer protection	Can anyone monitor the network traffic of your users? **Use SSL** to protect all authenticated traffic.
A10: Unvalidated redirects & forwards	Can anyone **trick your users** into submitting a request to your website?

Questions & Answers

Questions

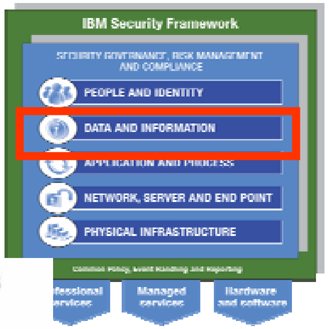
Do you have a vulnerability assessment process in place for web applications?

- Are you confident your home grown web applications are secure throughout the software development lifecycle?
- Do you know if your home grown web applications are secure? ie applications that can't be patched.
- Are your web applications used to send or receive sensitive information – including corporate IP, employee data, customer or partner information?
- Are your web applications secured against targeted attacks that exploit Web sites to gain access to sensitive information?
- Is your organization subject to federal or state legislative regulations or industry compliance stands? (PCI/HIPAA/SOX/GLBA) ?

IBM Security Offerings

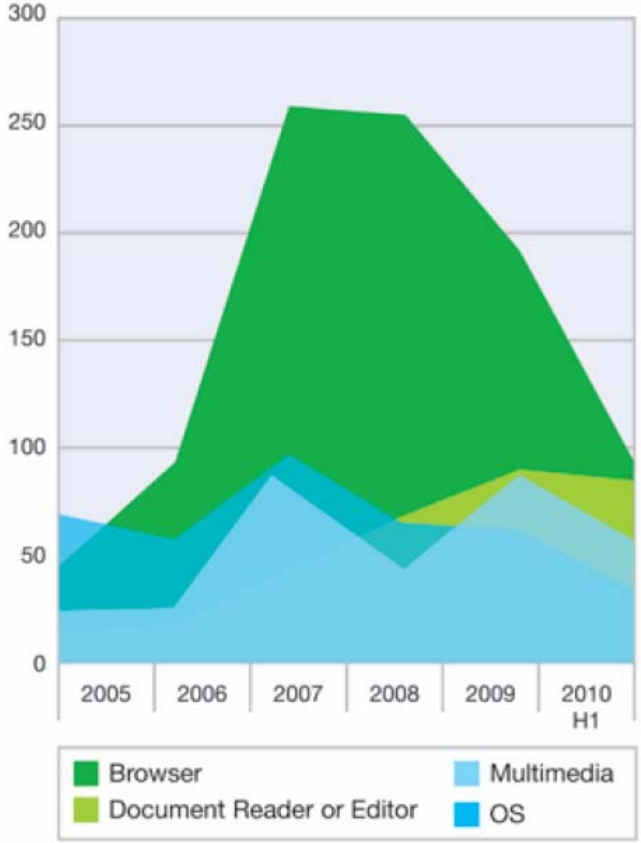
- Vulnerability Assessment
  - IBM Rational AppScan
  - IBM AppScan Source Edition
  - Application Security Assessment Services
- Identity & Access Management Solutions
  - IBM Tivoli Access Family
- Preemptive protection with the IBM Protocol Analysis Module (PAM) inside IBM Security protection products.
- IBM Web Application Security Solutions
- IBM Secure Web Gateway Service

Client-Side Vulnerabilities: Web Browser and Document Vulnerabilities Continue to Impact End Users

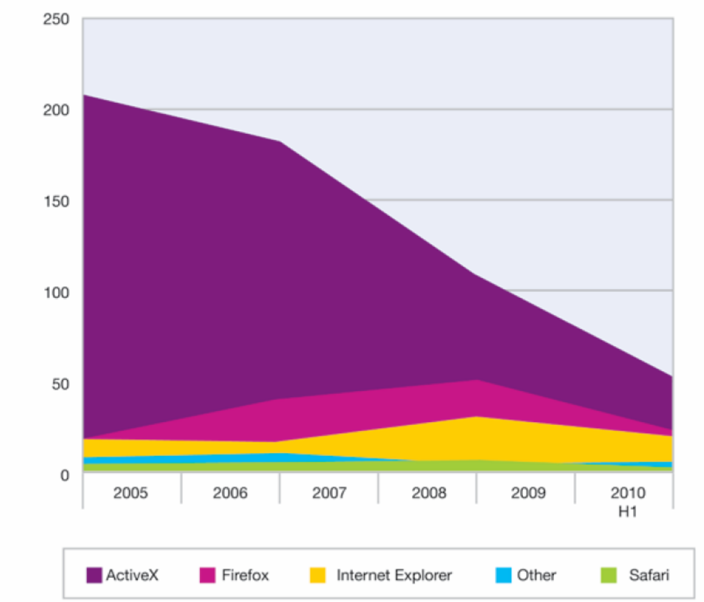


- Web browsers and their plug-ins continue to be the largest category of client-side vulnerabilities.
- Already in the first half of 2010, we see that document readers and editors, as well as multimedia applications, have almost surpassed 2009 year-end totals.

Critical & High Vulnerability Disclosures Affecting Client-Side Applications by Application Category
2005-2010 H1



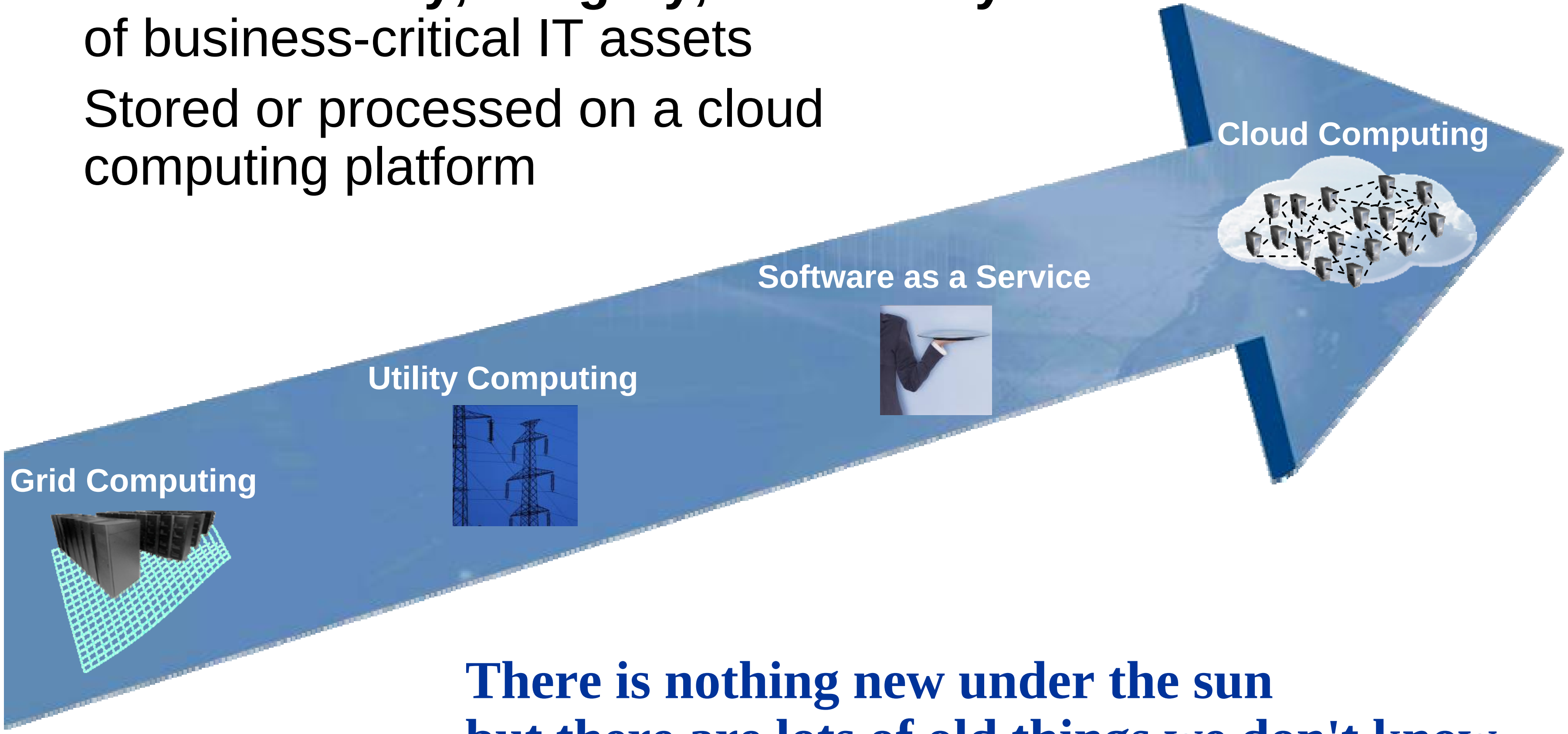
Critical and High Vulnerability Disclosures Affecting Browser-Related Software
2005-2010 H1



What is Cloud Security?

Confidentiality, Integrity, Availability
of business-critical IT assets

Stored or processed on a cloud computing platform



Grid Computing

Utility Computing

Software as a Service

Cloud Computing

There is nothing new under the sun
but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary

Cloud Security: Simple Example

Today’s Data Center

Tomorrow’s Public Cloud

We Have Control

It’s located at X.

It’s stored in server’s Y, Z.

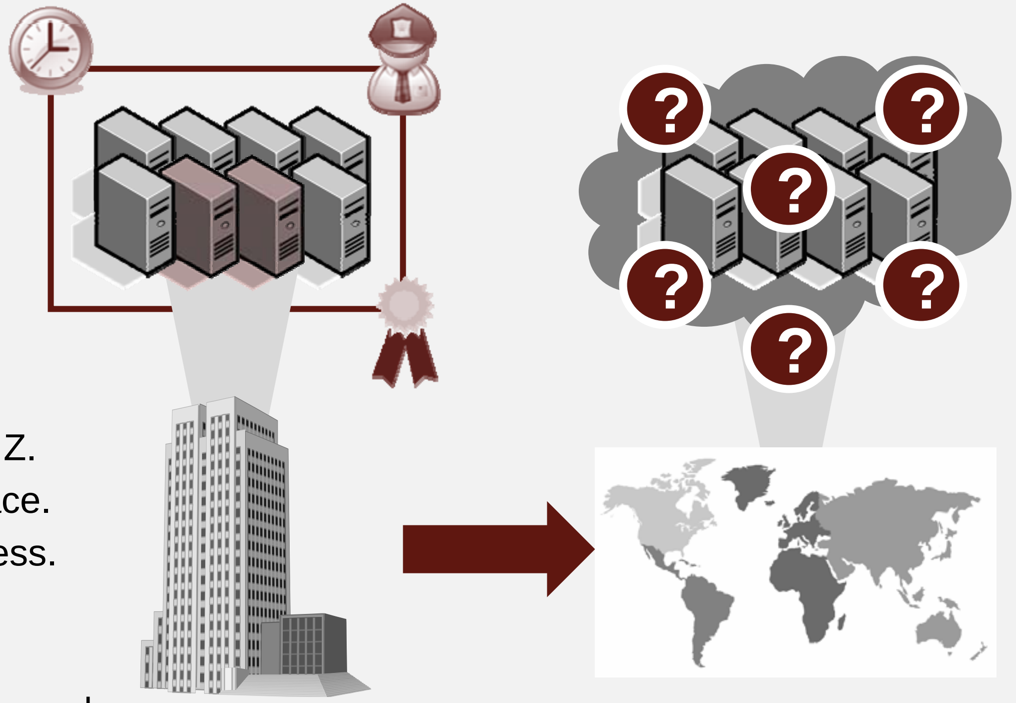
We have backups in place.

Our admins control access.

Our uptime is sufficient.

The auditors are happy.

Our security team is engaged.



Who Has Control?

Where is it located?

Where is it stored?

Who backs it up?

Who has access?

How resilient is it?

How do auditors observe?

How does our security team engage?

X-Force R&D -- Unmatched Security Leadership

The mission of the IBM X-Force® research and development team is to:

Research and evaluate threat and protection issues

Deliver security protection for today's security problems

Develop new technology for tomorrow's security challenges

Educate the media and user communities

X-Force Research

10Billion analyzed Web pages & images

150Million intrusion attempts daily

40Million spam & phishing attacks

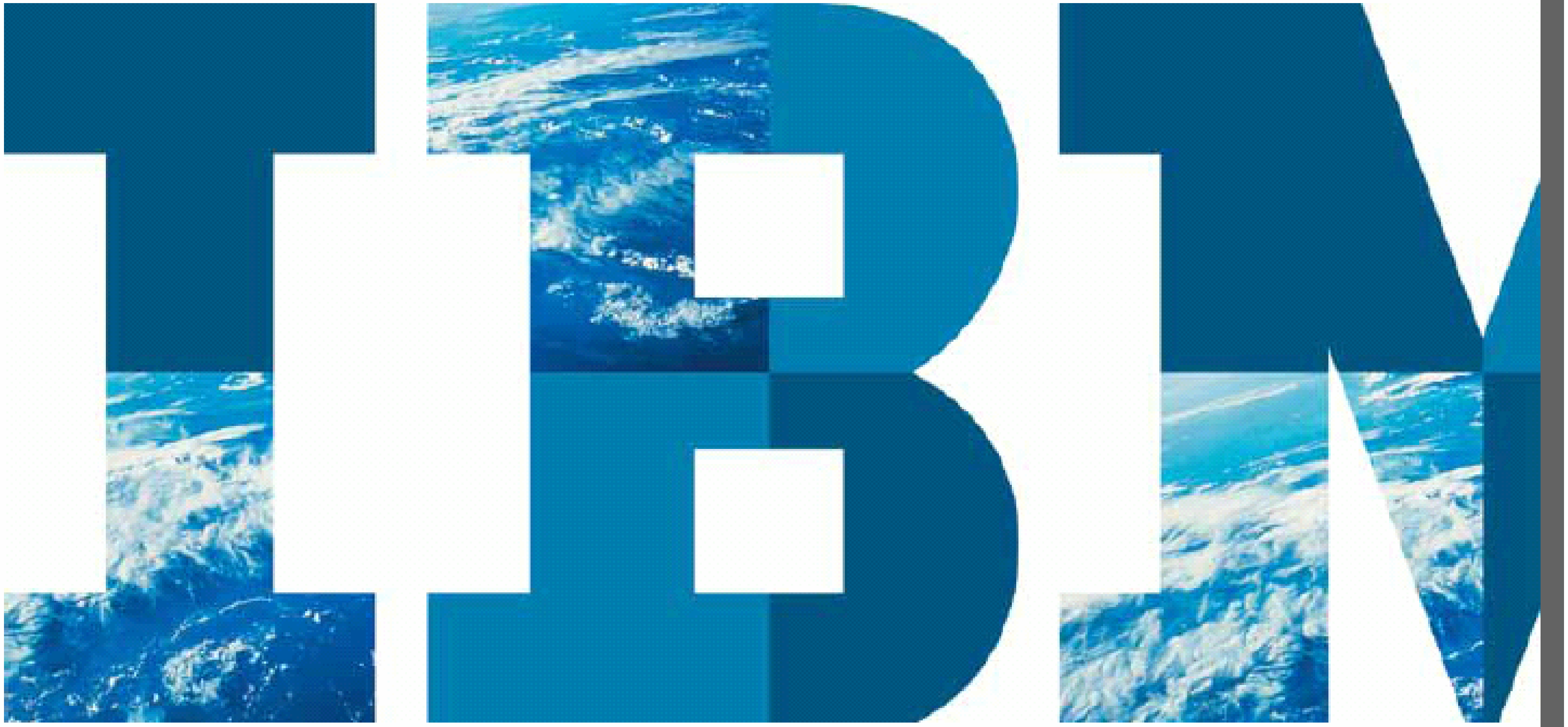
48,000 documented vulnerabilities

Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

IBM Security X-Force® 2010 Mid-Year Trend and Risk Report



Report Summary -- Attacks Continue Across all Security Domains

Application and Process

- Reported vulnerabilities are at an all time high, up **36%,** due to significant increases in public exploit releases and efforts by software vendors to identify and mitigate security vulnerabilities.
- **More than 55%** of all vulnerabilities disclosed are Web application vulnerabilities.
- **55%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of the 1st half of 2010.

Data and Information

- PDF attack activity continue to dominate the threat landscape. More than that, April 2010 had the most significant spike in PDF attack activity. Event activity for this month was almost **37%** higher than the average for the first half of 2010.
- The Zeus botnet toolkit continues to wreak havoc on organizations. Early 2010 saw the release of an updated version of the Zeus botnet kit, dubbed Zeus 2.0.
- Anonymous proxy websites continue to increase in volume, quadrupling since 2007.

Network, Server, and End Point

- Advanced persistent threats are groups of attackers that target and successfully penetrate well defended networks.
- Attackers are continuing to find new ways to hide or mask their malicious traffic to evade security technologies, i.e. Javascript obfuscation.
- **35%** of virtualization vulnerabilities impact the hypervisor.
- **7.2%** of the Internet is considered “socially” unacceptable, unwanted, or flat out malicious.

People and Identity

- Brazil, the U.S., and India account for more than one fourth of worldwide spam.
- Majority of spam **(more than 90%)** is still classified as URL spam—spam messages that include URLs that a person clicks to view the spam contents.
- Amount of URL spam using well-known and trusted domain names continue to increase.
- The top spam domains have moved from China (.cn) to Russia (.ru).
- More than two thirds **(66.8%)** of all financial phishing targets are located in North America, the remaining **32%** are in Europe.

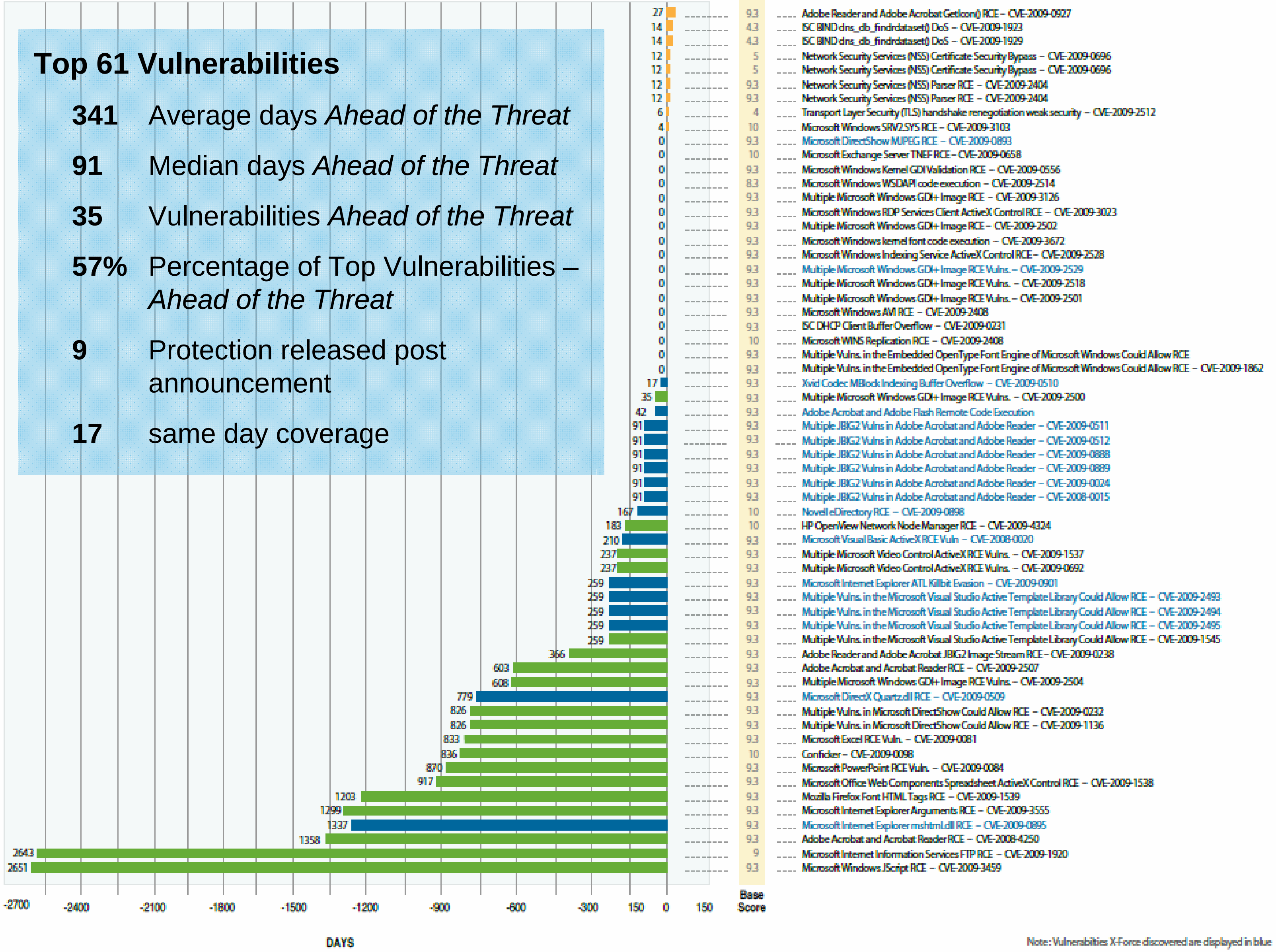
2010 X-Force Mid-Year Trend & Risk Report – Mapping to IBM Portfolio

Area of Risk	IBM Security Solutions
Vulnerabilities	- IBM Security Intrusion Prevention System (IPS) products: Network IPS, Server IPS, RealSecure Server Sensor, Desktop & Multifunction Security (MFS) - (Formerly IBM ISS Proventia products) - IBM Managed Protection Services for IPS - Tivoli Security Information and Event Manager (TSIEM)
Web Application Vulnerabilities	- Web application security for Network IPS, Server IPS and MFS - Managed Protection Services for IPS - Rational Appscan for assessment - IBM AppScan Source Edition - Rational Appscan Enterprise - Tivoli Security Information and Event Manager - Tivoli Security Policy Manager - IBM Secure Web Gateway Service
PC Vulnerabilities including Malicious Web Exploits	- IBM Security Intrusion Prevention System (IPS) product lines (see above list under vulnerabilities) - (Formerly IBM ISS Proventia products) - Managed Protection Services for IPS - Managed Security Services for Web Security
Spam	- IBM Lotus Protector/ Network Mail - IBM Multifunction Security (MFS) - Managed Security Services for Mail Security - IBM Security Content Analysis Software Development Kit (SDK)
Unwanted Web Content	- IBM Multifunction Security - Managed Security Services for Web Security -- IBM Secure Web Gateway Service
Malware	- IBM Desktop & Multifunction Security (MFS) - Managed Security Services for Mail and Web Security - IBM Lotus Protector/Network Mail

Security Effectiveness: Ahead of the Threat – Top Vulnerabilities of 2009

Top 61 Vulnerabilities

341	Average days *Ahead of the Threat*
91	Median days *Ahead of the Threat*
35	Vulnerabilities *Ahead of the Threat*
57%	Percentage of Top Vulnerabilities – *Ahead of the Threat*
9	Protection released post announcement
17	same day coverage



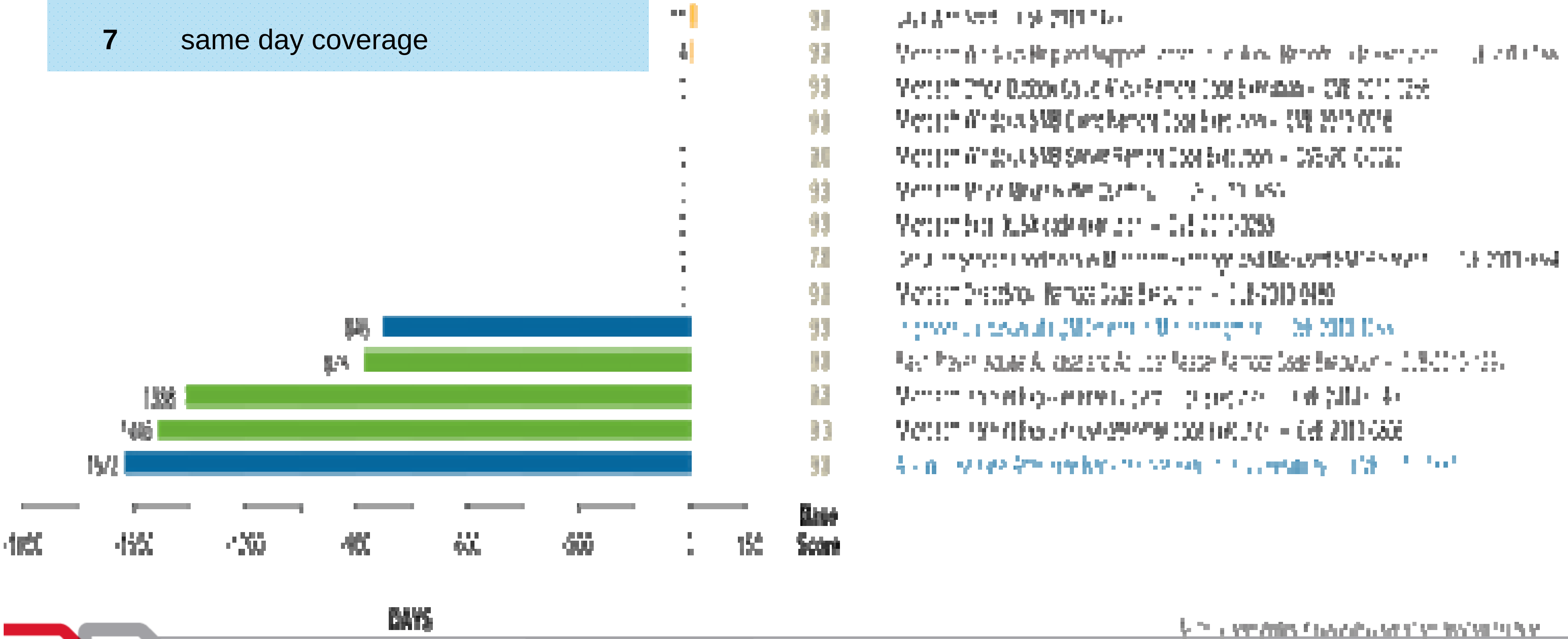
Note: Vulnerabilities X-Force discovered are displayed in blue

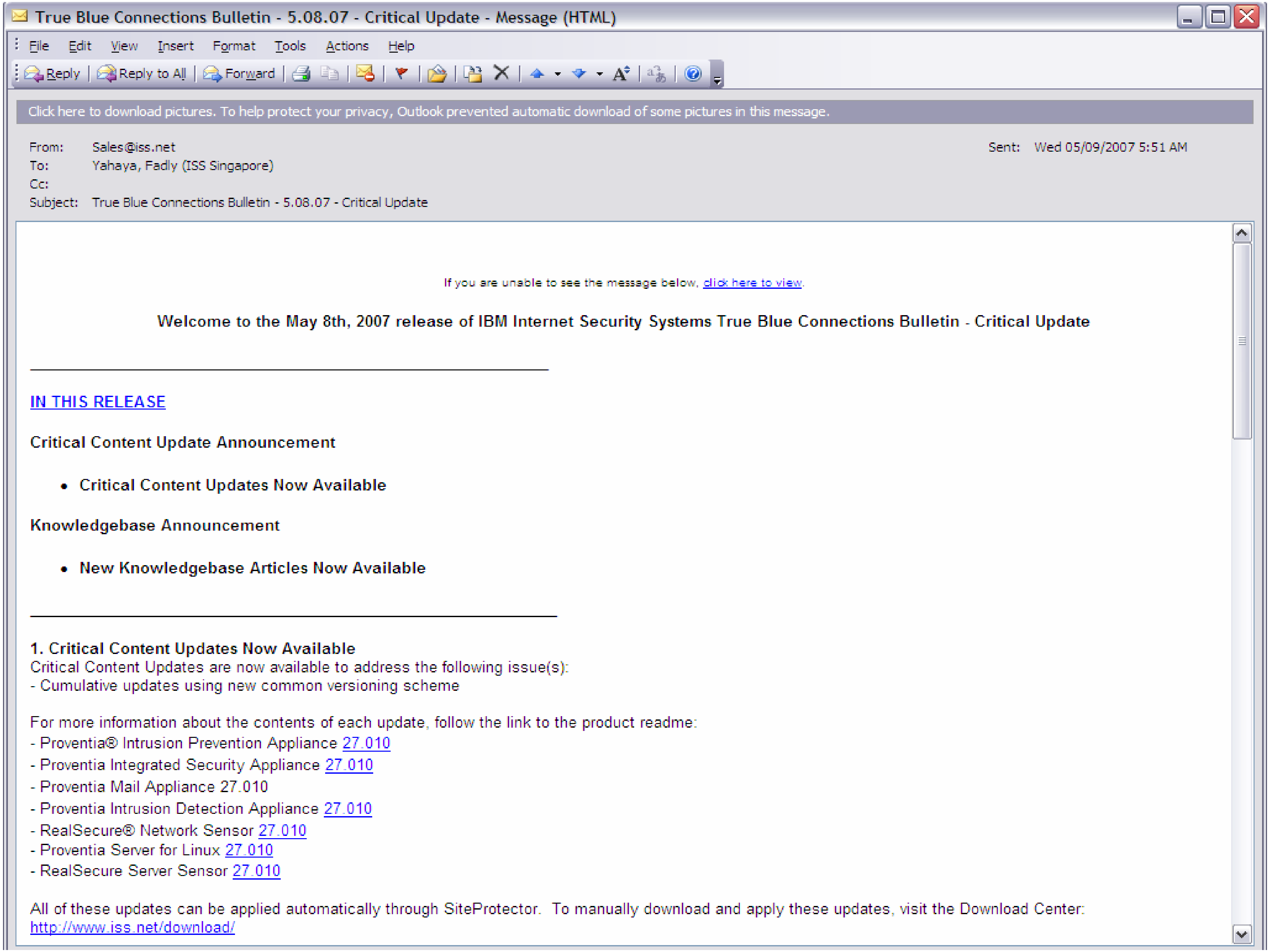
Note: RCE = Remote Code Execution

Security Effectiveness – Top Vulnerabilities of 1st Half 2010

Top 14 Vulnerabilities

437	Average days *Ahead of the Threat*
5	Vulnerabilities *Ahead of the Threat*
2	Protection released post announcement
7	same day coverage





True Blue Connections Bulletin - 5.08.07 - Critical Update - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Sales@iss.net

To: Yahaya, Fadly (ISS Singapore)

Cc:

Subject: True Blue Connections Bulletin - 5.08.07 - Critical Update

Sent: Wed 05/09/2007 5:51 AM

If you are unable to see the message below, click here to view.

Welcome to the May 8th, 2007 release of IBM Internet Security Systems True Blue Connections Bulletin - Critical Update

IN THIS RELEASE

Critical Content Update Announcement

- **Critical Content Updates Now Available**

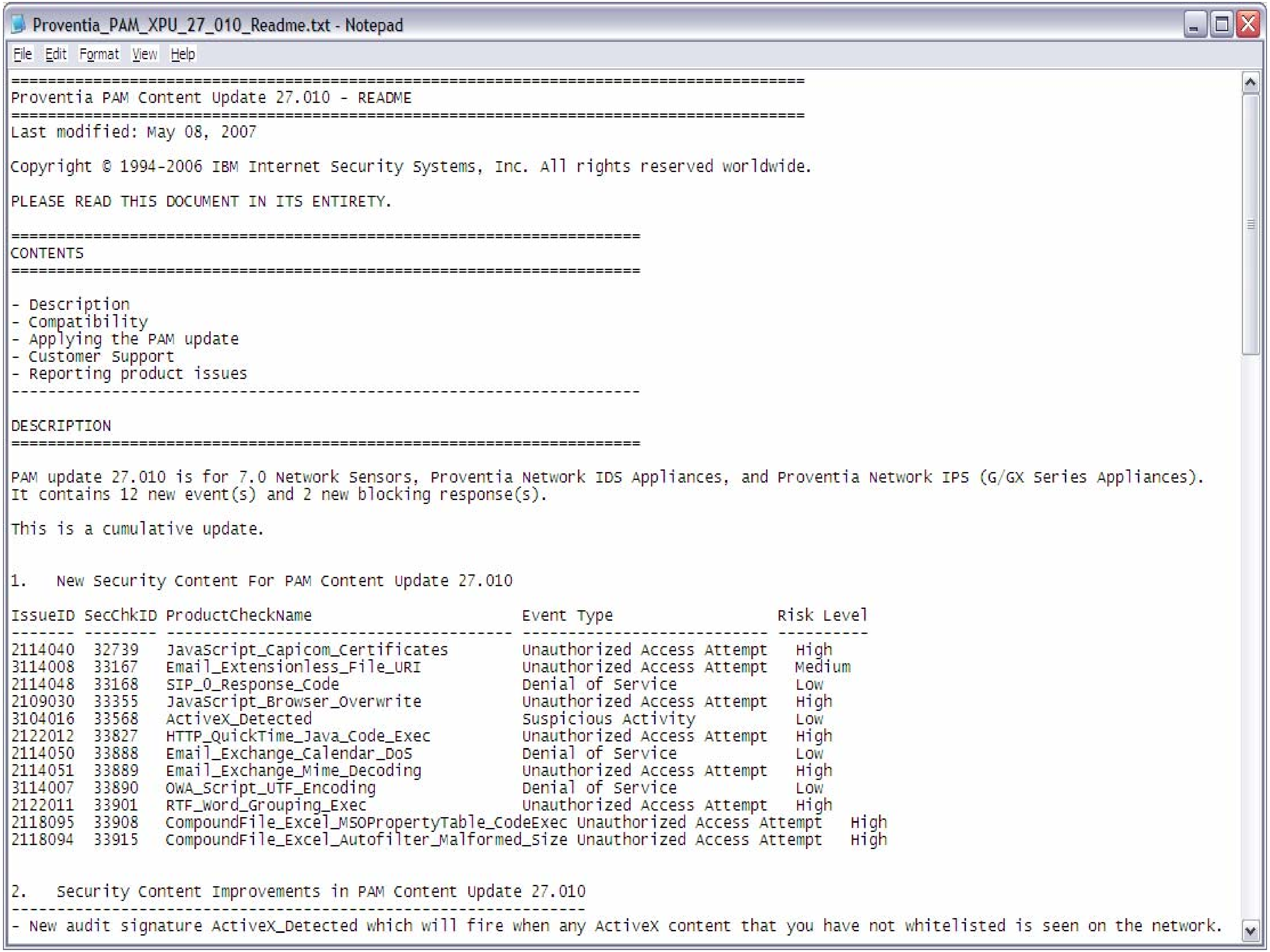
Knowledgebase Announcement

- **New Knowledgebase Articles Now Available**

1. Critical Content Updates Now Available
Critical Content Updates are now available to address the following issue(s):
- Cumulative updates using new common versioning scheme

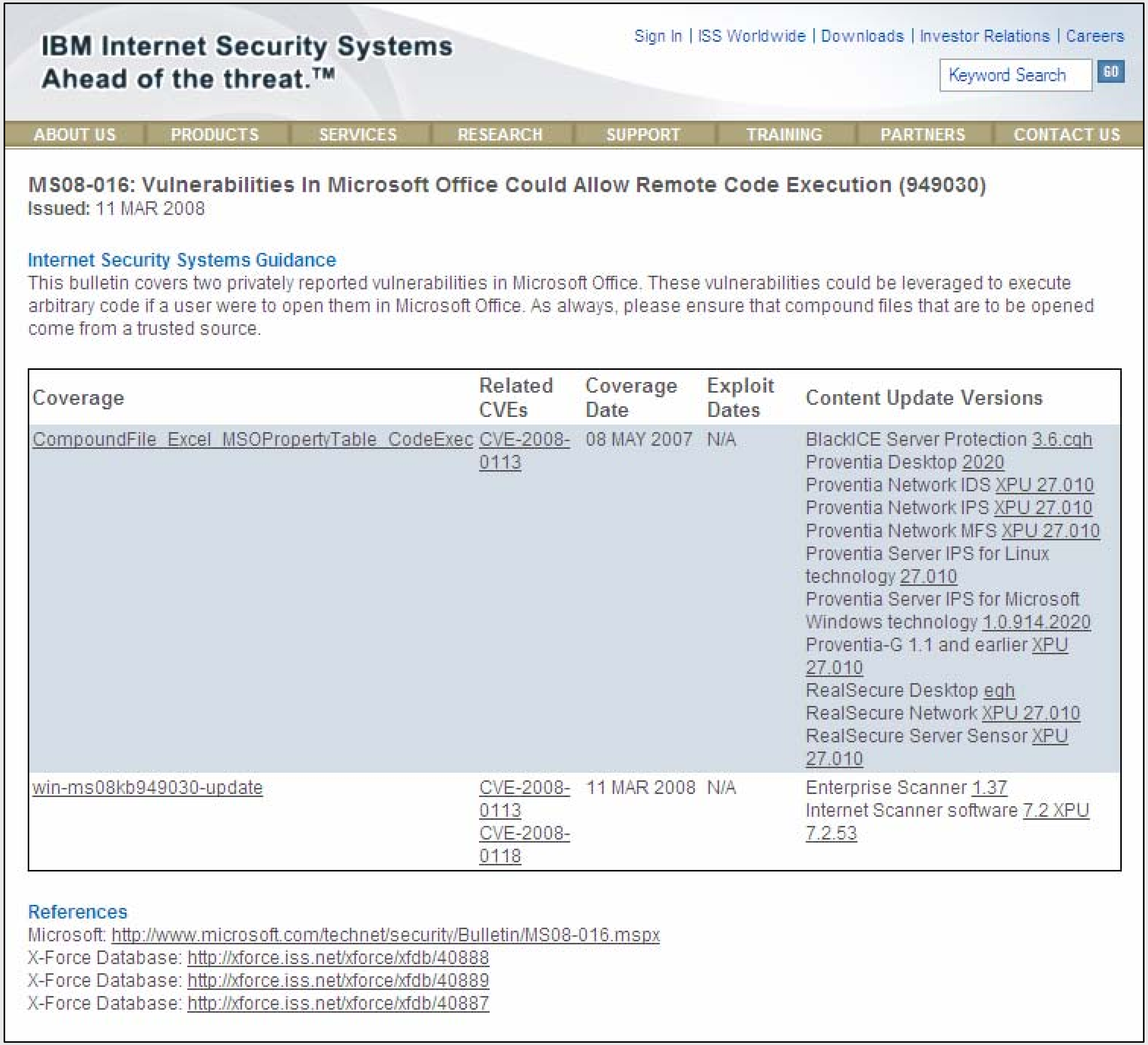
For more information about the contents of each update, follow the link to the product readme:
- Proventia® Intrusion Prevention Appliance 27.010
- Proventia Integrated Security Appliance 27.010
- Proventia Mail Appliance 27.010
- Proventia Intrusion Detection Appliance 27.010
- RealSecure® Network Sensor 27.010
- Proventia Server for Linux 27.010
- RealSecure Server Sensor 27.010

All of these updates can be applied automatically through SiteProtector. To manually download and apply these updates, visit the Download Center:
http://www.iss.net/download/



Proventia_PAM_XPU_27_010_Readme.txt - Notepad
File Edit Format View Help

```
=========================================================================
Proventia PAM Content Update 27.010 - README
=========================================================================
Last modified: May 08, 2007

Copyright © 1994-2006 IBM Internet Security Systems, Inc. All rights reserved worldwide.

PLEASE READ THIS DOCUMENT IN ITS ENTIRETY.

=====================================================================
CONTENTS
=====================================================================

- Description
- Compatibility
- Applying the PAM update
- Customer Support
- Reporting product issues
---------------------------------------------------------------------

DESCRIPTION
=====================================================================

PAM update 27.010 is for 7.0 Network Sensors, Proventia Network IDS Appliances, and Proventia Network IPS (G/GX Series Appliances).
It contains 12 new event(s) and 2 new blocking response(s).

This is a cumulative update.


1.   New Security Content For PAM Content Update 27.010

IssueID SecChkID ProductCheckName                        Event Type                Risk Level
------- -------- --------------------------------------- ------------------------- ----------
2114040  32739   JavaScript_Capicom_Certificates         Unauthorized Access Attempt   High
3114008  33167   Email_Extensionless_File_URI            Unauthorized Access Attempt   Medium
2114048  33168   SIP_0_Response_Code                     Denial of Service            Low
2109030  33355   JavaScript_Browser_Overwrite            Unauthorized Access Attempt   High
3104016  33568   ActiveX_Detected                        Suspicious Activity          Low
2122012  33827   HTTP_QuickTime_Java_Code_Exec           Unauthorized Access Attempt   High
2114050  33888   Email_Exchange_Calendar_DoS             Denial of Service            Low
2114051  33889   Email_Exchange_Mime_Decoding            Unauthorized Access Attempt   High
3114007  33890   OWA_Script_UTF_Encoding                 Denial of Service            Low
2122011  33901   RTF_Word_Grouping_Exec                  Unauthorized Access Attempt   High
2118095  33908   CompoundFile_Excel_MSOPropertyTable_CodeExec Unauthorized Access Attempt   High
2118094  33915   CompoundFile_Excel_Autofilter_Malformed_Size Unauthorized Access Attempt   High


2.   Security Content Improvements in PAM Content Update 27.010
-----------------------------------------------------------------
- New audit signature ActiveX_Detected which will fire when any ActiveX content that you have not whitelisted is seen on the network.
```



MS08-016: Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (949030)

Issued: 11 MAR 2008

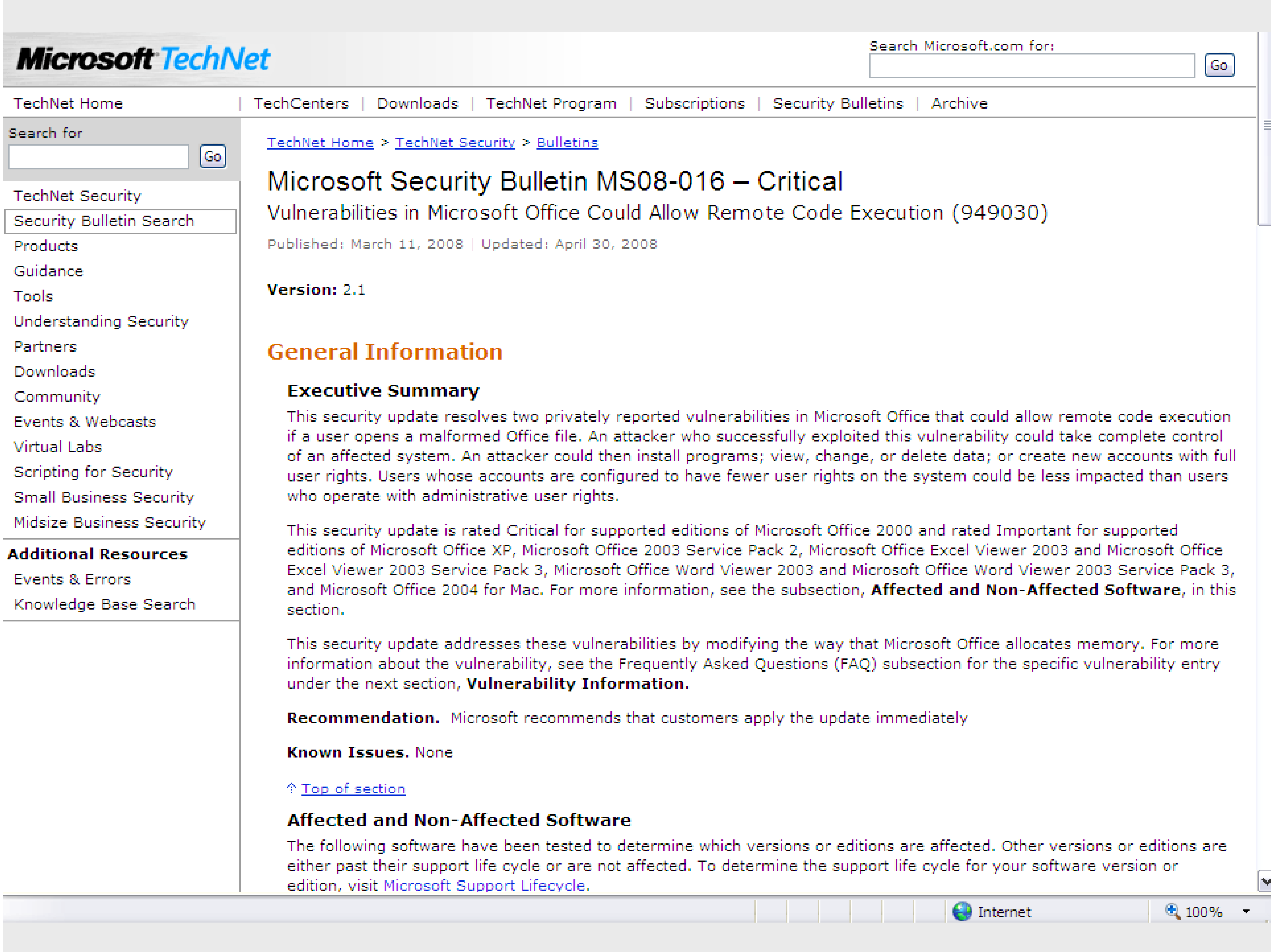
Internet Security Systems Guidance

This bulletin covers two privately reported vulnerabilities in Microsoft Office. These vulnerabilities could be leveraged to execute arbitrary code if a user were to open them in Microsoft Office. As always, please ensure that compound files that are to be opened come from a trusted source.

Coverage	Related CVEs	Coverage Date	Exploit Dates	Content Update Versions
CompoundFile_Excel_MSOPropertyTable_CodeExec	CVE-2008-0113	08 MAY 2007	N/A	BlackICE Server Protection 3.6.cgh Proventia Desktop 2020 Proventia Network IDS XPU 27.010 Proventia Network IPS XPU 27.010 Proventia Network MFS XPU 27.010 Proventia Server IPS for Linux technology 27.010 Proventia Server IPS for Microsoft Windows technology 1.0.914.2020 Proventia-G 1.1 and earlier XPU 27.010 RealSecure Desktop egh RealSecure Network XPU 27.010 RealSecure Server Sensor XPU 27.010
win-ms08kb949030-update	CVE-2008-0113 CVE-2008-0118	11 MAR 2008	N/A	Enterprise Scanner 1.37 Internet Scanner software 7.2 XPU 7.2.53

References

Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS08-016.mspx
X-Force Database: http://xforce.iss.net/xforce/xfdb/40888
X-Force Database: http://xforce.iss.net/xforce/xfdb/40889
X-Force Database: http://xforce.iss.net/xforce/xfdb/40887



Microsoft Security Bulletin MS08-016 – Critical

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (949030)

Published: March 11, 2008 | Updated: April 30, 2008

Version: 2.1

General Information

Executive Summary

This security update resolves two privately reported vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a malformed Office file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This security update is rated Critical for supported editions of Microsoft Office 2000 and rated Important for supported editions of Microsoft Office XP, Microsoft Office 2003 Service Pack 2, Microsoft Office Excel Viewer 2003 and Microsoft Office Excel Viewer 2003 Service Pack 3, Microsoft Office Word Viewer 2003 and Microsoft Office Word Viewer 2003 Service Pack 3, and Microsoft Office 2004 for Mac. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

This security update addresses these vulnerabilities by modifying the way that Microsoft Office allocates memory. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information.**

Recommendation. Microsoft recommends that customers apply the update immediately

Known Issues. None

↑ Top of section

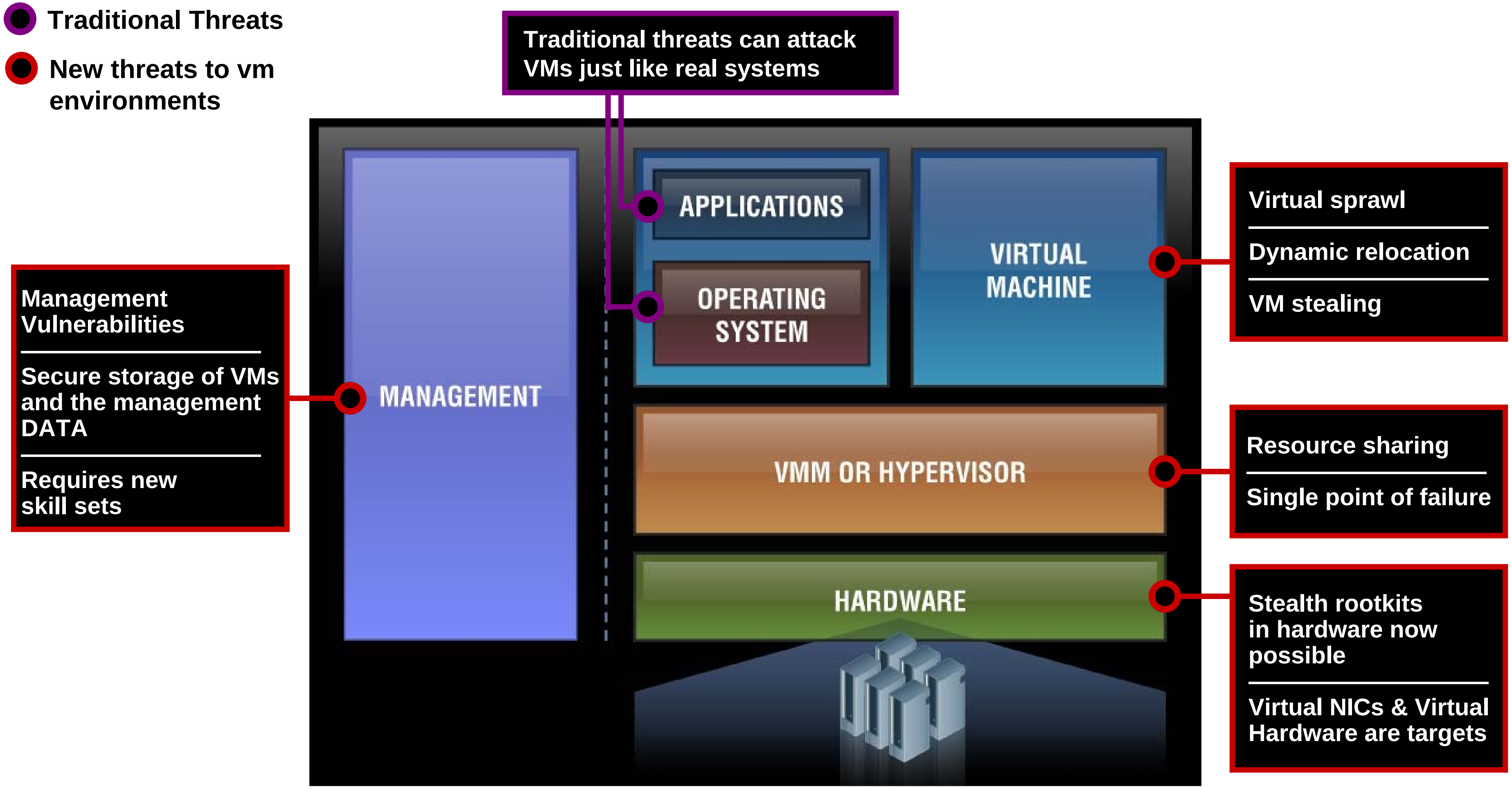
Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

More Components = More Exposure

● Traditional Threats

● New threats to vm environments



Traditional threats can attack VMs just like real systems

Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

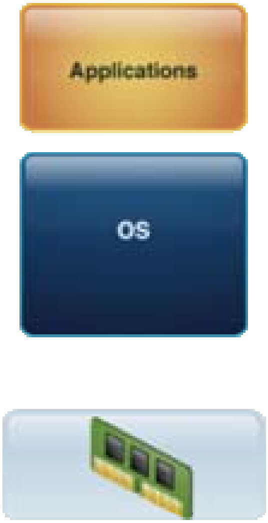
Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

Security complexities raised by virtualization

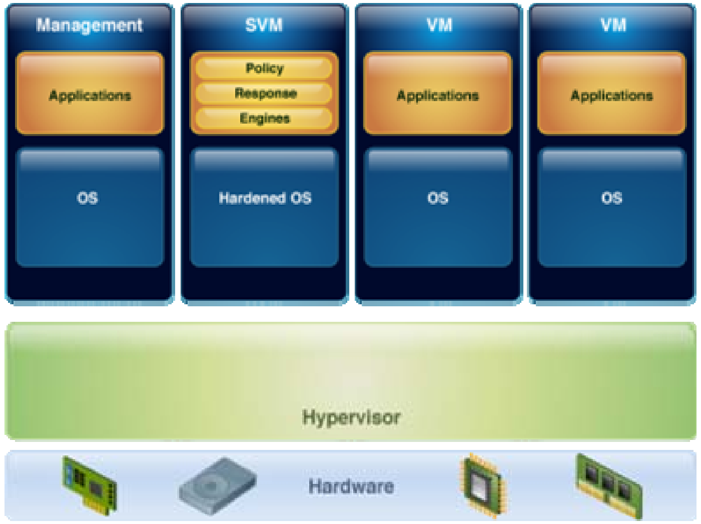
- Complexities
  - –Dynamic relocation of VMs
  - –Increased infrastructure layers to manage and protect
  - –Multiple operating systems and applications per server
  - –Elimination of physical boundaries between systems
  - –Manually tracking software and configurations of VMs
  - –Maintenance of virtual images
  - –Backup/Disaster recovery
  - –Geographic location of images, data
  - –Demonstrating compliance using shared data

Before Virtualization



- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

Proventia GX Hardware Refresh 2Q 2010
(Performance Enhanced)

- GX4004-V2
- GX5008-V2
- GX5108-V2
- GX5208-V2

✷Multi-Core CPU's
✷Next Generation hardware design
✷Content Analysis performance headroom Performance Optimization
✷Significant price/performance improvement
✷64 Bit PAM

Categories of Cloud Computing Risks

Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control.

Providers must offer a high degree of security transparency to help put customers at ease.

Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

Authentication and access technologies become increasingly important.

Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

Mission critical applications may not run in the cloud without strong availability guarantees.

Compliance

Complying with regulations may prohibit the use of clouds for some applications.

Comprehensive auditing capabilities are essential.

Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

Providers must supply easy controls to manage security settings for application and runtime environments.

The right tools for the job?

IBM Security Framework – Business-oriented framework used across all IBM brands that allows to structure and discuss a client’s security concerns

Built to meet four key requirements:

- Provide *Assurance*
- Enable *Intelligence*
- Automate *Process*
- Improve *Resilience*

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

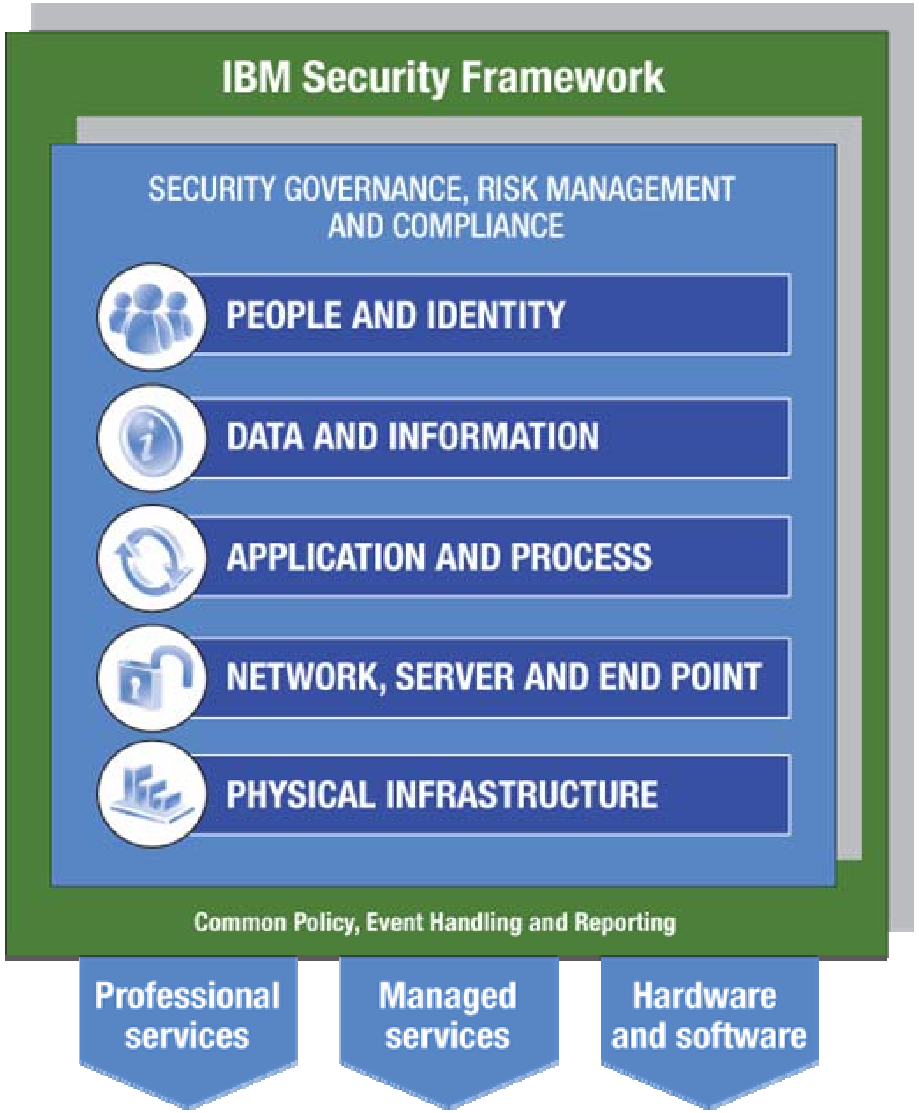
Redguides
for Business Leaders

Axel Buecker
David Crowther
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

- Building a Business Security Reference Model based on standards and common practices
- Connecting business drivers with IT security and risk management disciplines
- Employing the IBM Security Framework and the IBM Security Blueprint in real-world business scenarios

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009



Typical Client Security Requirements

Governance, Risk Management, Compliance

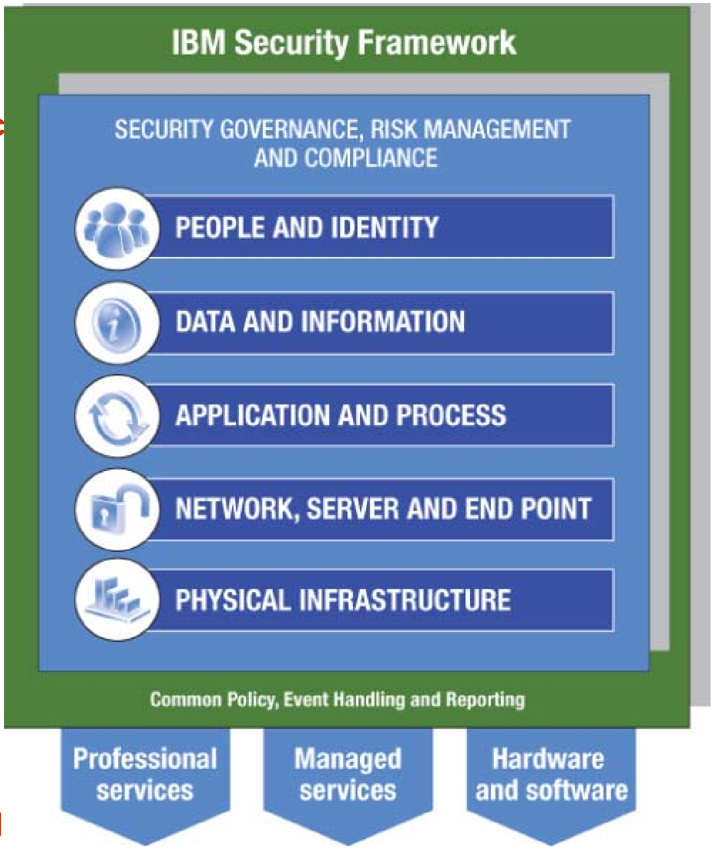
- **3rd-party audit** (SAS 70(2), ISO27001, PCI)
- **Client access to tenant-specific log and audit data**
- **Effective incident reporting for tenants**
- Visibility into change, incident, image management, etc.
- SLAs, option to transfer risk from tenant to provider
- Support for forensics
- Support for e-Discovery

Application and Process

- Application security requirements for cloud are phrased in terms of image security
- Compliance with secure development best practices

Physical

- Monitoring and control of physical access



People and Identity

- **Privileged user monitoring,** including logging activities, physical monitoring and background checking
- **Federated identity / onboarding:** Coordinating authentication and authorization with enterprise or third party systems
- **Standards-based SSO**

Data and Information

- **Data segregation**
- Client control over geographic location of data
- Government: Cloud-wide data classification

Network, Server, Endpoint

- **Isolation** between tenant domains
- **Trusted virtual domains:** policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability Management
- Protect machine images from corruption and abuse
- Government: MILS-type separation

Based on interviews with clients and various analyst reports

IBM is the Trusted Partner of Choice

- 2008: Most trusted IT company

  Ponemon Institute and TRUSTe study
- Thought leadership
- Commitment and customer insight
- Industries/sectors expertise
- Comprehensive capabilities, products, services and research
- SC Security Company of the year 2010 RSA Security

Cloud Computing Quotes

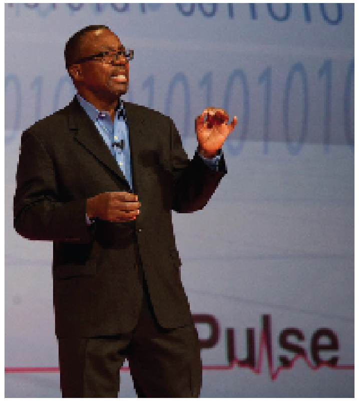
> *"IBM is an international company. It has a good brand and status in the industry.* ***We will be comfortable with IBM in terms of data security"***

> ***"IBM is a trusted supplier of information security****…"*
>
> *"Yes I think* ***they can offer secured services****"*

Source: Oliver Wyman Interviews

enresa
Empresa Nacional de Residuos Radiactivos, S. A.
Borregaard
NAYANA
COMMUNICATION
Australian Open
GLOBAL DATA VAULTING
AGENTRICS
Washington Trust Bank
cmc
community medical care
arek
DukeMedicine
GODIVA
Chocolatier
bp
CONVERGENCE CT
IBM
BAYLOR
UNIVERSITY
Mercantil
Trillium
HEALTH CENTRE
Mn Services
AVIYA
Clinical Research and Development
HUGHES
DTCC
ZOO ATLANTA
WestLB
THE INTERNATIONAL BANK OF MIAMI, N.A.
STADTWERKE ILMENAU GMBH
STROM • ERDGAS
P&G
NORTHWEST HOSPITAL & MEDICAL CENTER
Hbc

BEST SECURITY COMPANY



WINNER
IBM Corporation
www.ibm.com/security

Founded in 1911, IBM has been a security industry leader for nearly 50 years, helping CxOs and IT professionals secure their corporate infrastructures with solutions that go beyond just collections of niche products. Customers rely on IBM for the planet's most secure databases, applications, operating systems, storage and servers.

IBM offers comprehensive security solutions and services addressing compliance, applications, data, identity and access management, networks, threat prevention, systems security, email, encryption, virtualization and cloud security.

Through an end-to-end approach to security across people and identity, data, applications, compliance, networks, servers and the physical infrastructure, IBM offers security capabilities that are among the top in the industry. With multiple leadership awards in market presence and technology innovation, IBM is able to offer more than 120 security products and the experience of over 15,000 researchers, developers and SMEs focused on security initiatives.

IBM clients around the world gain the benefit of integrated, security solutions that reduce the cost and complexity of managing security solutions from multiple vendors.

World-class security support services from IBM provide the technical and operational expertise needed to maximize security investment. By providing a global network of support centers to assist customers worldwide, often in their native language, IBM partners with its customers around the clock to solve any implementation and technical issues.

This support is available regardless of client location or implementation method of hardware, software and/or managed security services. IBM provides a variety of support levels – from self-help to tiered levels – enabling customers to choose the one that best meets their needs. IBM is recognized for its outstanding customer support and consistently high customer satisfaction.

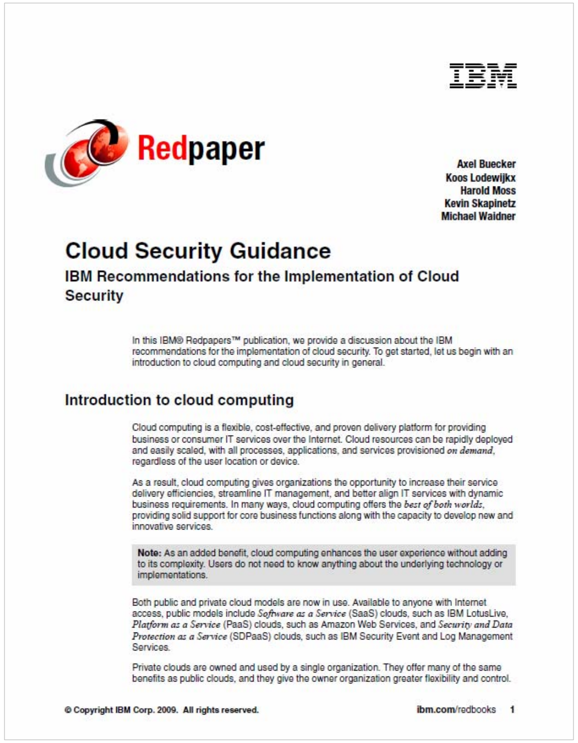
The company has staked a firm claim in the security marketplace and emerged as a market leader capable of meeting any global organization's security needs through an integrated, diverse and flexible portfolio of products and services across key industries.

With a strong, deep and broad security portfolio, IBM is in a strong position, able to leverage its considerable assets and reputation and provide innovative technologies and intellectual property that address both today's vulnerabilities and newly emerging threats.

SC MAGAZINE
AWARDS
2010
WINNER
Honored in the U.S.

IBM Cloud Security Guidance document

- Based on cross-IBM research on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:
  - *Building a Security Program*
  - *Confidential Data Protection*
  - *Implementing Strong Access and Identity*
  - *Application Provisioning and De-provisioning*
  - *Governance Audit Management*
  - *Vulnerability Management*
  - *Testing and Validation*



Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

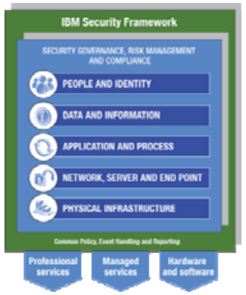
Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

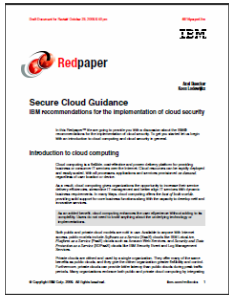
© Copyright IBM Corp. 2009. All rights reserved.

ibm.com/redbooks 1

Network, Server and End Point



IBM Security Framework


IBM

Redpaper

Secure Cloud Guidance

IBM recommendations for the implementation of cloud security

[illegible]

Introduction to cloud computing

[illegible]

IBM Cloud Security Guidance Document

Customers expect a **secure** cloud **operating environment**.

Maintain environment testing and vulnerability/intrusion management

- Implement vulnerability scanning, anti-virus, intrusion detection and prevention on all appropriate images
- Ensure isolation exists between tenant domains
- Trusted virtual domains: policy-based security zones
- A secure application testing program should be implemented.
- Develop all Web based applications using secure coding guidelines.
- Ensure external facing Web applications are black box tested

Network, Server, and Endpoint

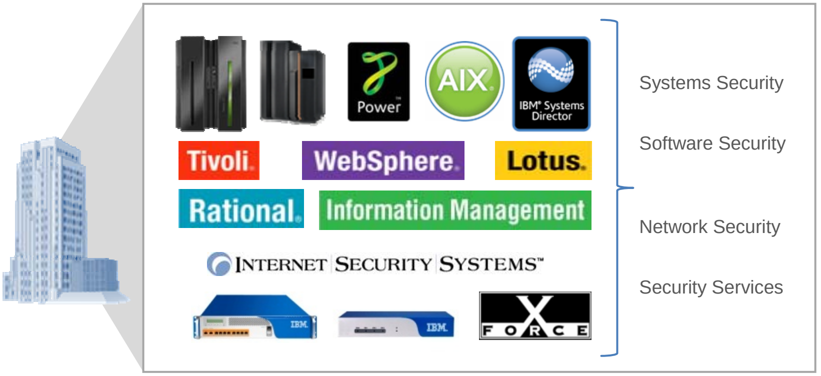
Enterprise Security

Security for existing IT infrastructure as it extends to the cloud

IBM Enterprise Security Solutions

Summary: IBM security products and services driven by X-Force research, Tivoli Security Software to reduce cost and risk, and IBM Systems work together to create a highly secure computing environment that minimizes the potential risk posed by security threats.

Cloud Use Case: Our end-to-end solutions allow customers to build a strong security posture - positioning them to reap the rewards of emerging trends such as cloud computing.



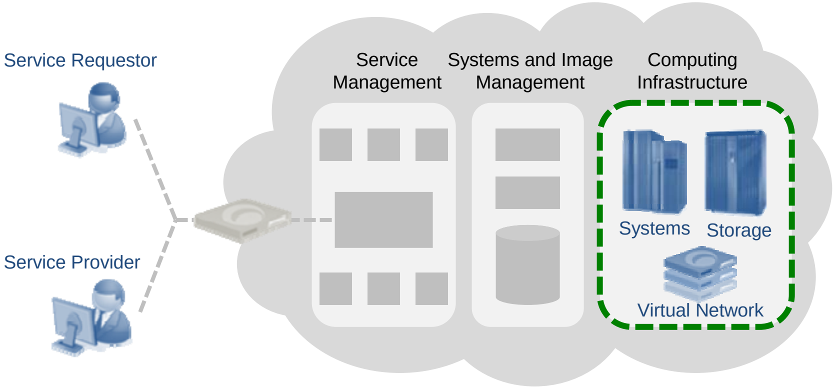
Virtualization Security

Security for pools of high performance virtualized resources

IBM Systems and IBM Virtualization Security

Summary: IBM offers the industry's broadest set of virtualization capabilities. Relying on over 40 years of heritage and attention to security, IBM virtualization platforms are built with security as a requirement, not an afterthought. Solutions from IBM ISS, such as Proventia Server and virtual appliances, strengthen defenses by eliminating additional threats.

Cloud Use Case: Security of the virtualization stack - enabling flexible, rapid provisioning across heterogeneous servers and hypervisors.



Cloud computing also provides the opportunity to *simplify* security controls and defenses

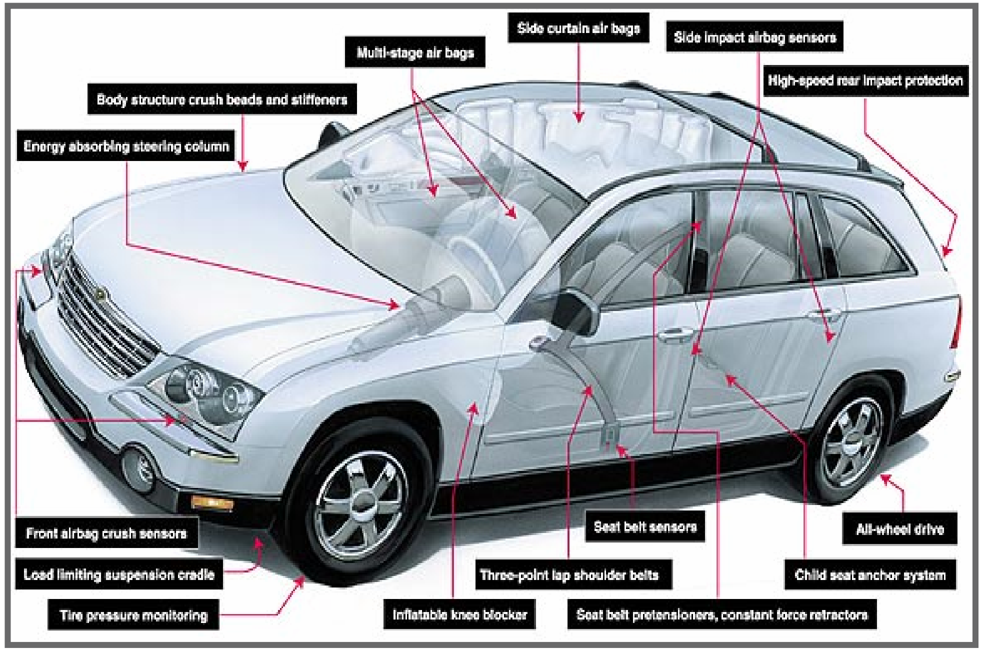
	Cloud Enabled Control(s)	Benefit
People and Identity	• Defined set of cloud interfaces • Centralized repository of Identity and Access Control policies	• Reduced risk of user access to unrelated resources.
Information and Data	• Computing services running in isolated domains as defined in service catalogs • Default encryption of data in motion & at rest • Virtualized storage providing better inventory, control, tracking of master data	• Improved accountability, Reduced risk of data leakage / loss • Reduced attack surface and threat window • Less likelihood that an attack would propagate
Process & Application	• Autonomous security policies and procedures • Personnel and tools with specialized knowledge of the cloud ecosystem • SLA-backed availability and confidentiality	• Improved protection of assets and increased accountability of business and IT users
Network Server and Endpoint	• Automated provisioning and reclamation of hardened runtime images • Dynamic allocation of pooled resources to mission-oriented ensembles	• Reduced attack surface • Improved forensics with ensemble snapshots
Physical infrastructure	• Closer coupling of systems to manage physical and logical identity / access.	• Improved ability to enforce access policy and manage compliance

Summary

- “Cloud” is a new consumption and delivery model inspired by consumer Internet services.
- Security Remains the Top Concern for Cloud Adoption
- One sized security doesn’t fit all
- Take a structured approach to securing your cloud environment
- Documented guidance is available for download to assist you in securing your cloud environment
- IBM has a view from End to End when it addresses your security needs

Pillow Safety ?

Think of X-Force as the Safety Component Engineers


Side curtain air bags
Side impact airbag sensors
Multi-stage air bags
High-speed rear impact protection
Body structure crush beads and stiffeners
Energy absorbing steering column
Front airbag crush sensors
Seat belt sensors
All-wheel drive
Load limiting suspension cradle
Three-point lap shoulder belts
Child seat anchor system
Tire pressure monitoring
Inflatable knee blocker
Seat belt pretensioners, constant force retractors

IBM provides Enterprise-grade Security

Who can do this better than IBM?

IBM
IBM Systems Director
Power
AIX
Tivoli
Information Management
WebSphere
Rational
Lotus
INTERNET SECURITY SYSTEMS
GTS
ITS
GBS
Smart Planet
Dynamic Infrastructure
IBM Research
X FORCE

…Nobody

Thank you!