Protecting the Evolving Infrastructure

Bhrigu Nagal

Product Manager – Security Services

We simply cannot be held back!

THE TIMES OF INDIA

Home | Cities | India | World | Business | Cricket | Sports | Health & Science | Info

US | Indians Abroad | Pakistan | South Asia | UK | Europe | China | Middle Ea

US electricity grid hit by cyber attacks: Report

8 Apr 2009, 2122 hrs IST, AFP

Share | Save | Comment | Text:

...an cyber-spies have hacked into the US ...mes that could be used to disrupt the system, a report said on Wednesday.

Quoting unidentified intelligence sources and homeland security officials, the Wall Street Journal said cyber-spies penetrated the system repeatedly last year, without disrupting it.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," the paper said quoting a senior intelligence official, and "so have the Russians."

China cyber attack: NIC most affected, 9 embassies hit

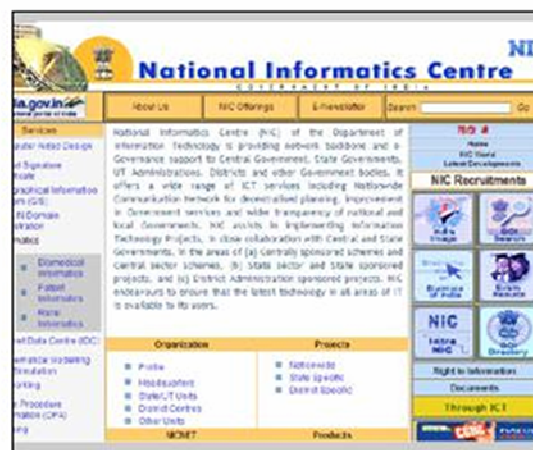9 Comments | Post Comment   BOOKMARK   A Larger | Smaller

Manu Pubby
Posted: Tuesday , Mar 31, 2009 at 0848 hrs IST

New Delhi:

Computers of nine key Indian embassies, including offices in the US, UK and Germany, were infected by the mysterious GhostNet, a China-based cyber espionage network that has been uncovered by a Canada-based research organisation.

More worryingly, the cyber investigation says that India's premier National Informatics Centre (NIC), which governs and hosts all government websites, was infected by the mysterious GhostNet at least 12 times in the past two years.

In this smarter world, we need our infrastructure to propel us forward, not hold us back.

Infrastructure that is instrumented, interconnected and intelligent.
Infrastructure that brings together business and IT to create new possibilities.

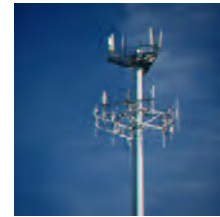| Mobility Infrastructure		Facilities Infrastructure		Production Infrastructure		Technology Infrastructure		Communications Infrastructure
	+		**+**		**+**		**+**	

We need a *dynamic* infrastructure.

Dynamic Infrastructure
Smart is: Managing Risk

Not only addressing today's security, resiliency, and compliance challenges, but also preparing for the new risks posed by an even more *connected* and *collaborative* world.

SMART IS
Connecting to the world securely with 100% availability.

SMART IS
Protecting your customer... and your brand with no loss of data.

Australian Open: Securely, resiliently provides scalable resources 100x normal scalability, real-time analysis and prevention of attacks and achieves 23% reduction in energy consumption, with 100% website availability.
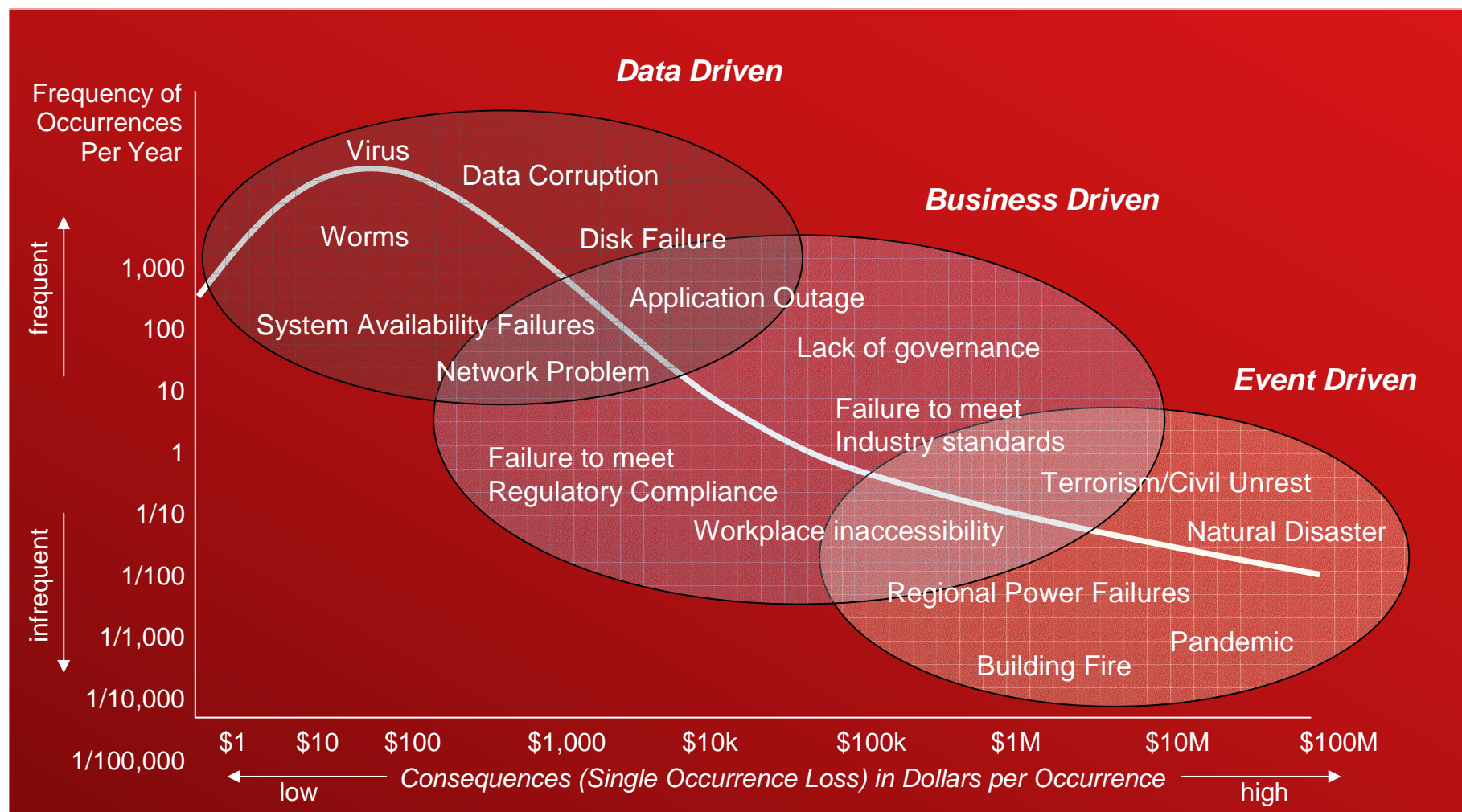
Bank of Montreal: Providing a recovery point of zero and a recovery time of 2 hours helps reduce operational risk, increase client trust, improve availability, and meet stringent regulatory compliance requirements.

Evolving Threats…

Frequency of Occurrences Per Year

Data Driven

Business Driven

Event Driven

frequent

- Virus
- Data Corruption
- Worms
- Disk Failure
- Application Outage
- System Availability Failures
- Network Problem
- Lack of governance
- Failure to meet Industry standards
- Failure to meet Regulatory Compliance
- Terrorism/Civil Unrest
- Workplace inaccessibility
- Natural Disaster
- Regional Power Failures
- Pandemic
- Building Fire

infrequent

1,000
100
10
1
1/10
1/100
1/1,000
1/10,000
1/100,000

$1 $10 $100 $1,000 $10k $100k $1M $10M $100M

low → *Consequences (Single Occurrence Loss) in Dollars per Occurrence* ← high

IBM Security Framework
Provides the Business Answers You Need in Uncertain Times

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

1. Lower the costs of applying the latest security expertise, processes and technologies

2. Mitigate, monitor and manage the latest security threats and vulnerabilities

3. Lower costs of limiting internal access to, and external release of, sensitive data

4. Identify and mitigate the risks of regulatory noncompliance

5. Lower the costs of identity and access management

6. Mitigate the increasing risks from application-level vulnerabilities

Professional Security Services

Security & Governance

- Information Security Assessment
- Vulnerability Assessment
- Penetration testing
- Application Security Testing
- Security Policy & Procedures
- Risk Assessment
- ISO 27002 Gap Analysis
- PCI Assessment Services
- Deployment Services
- Awareness & Training
- Emergency Response Services

Identity & Access Mgmt.

- Assessment & Strategy
- Lifecycle Management
- Access Management

Data Security

- Encryption
- Data Loss Prevention
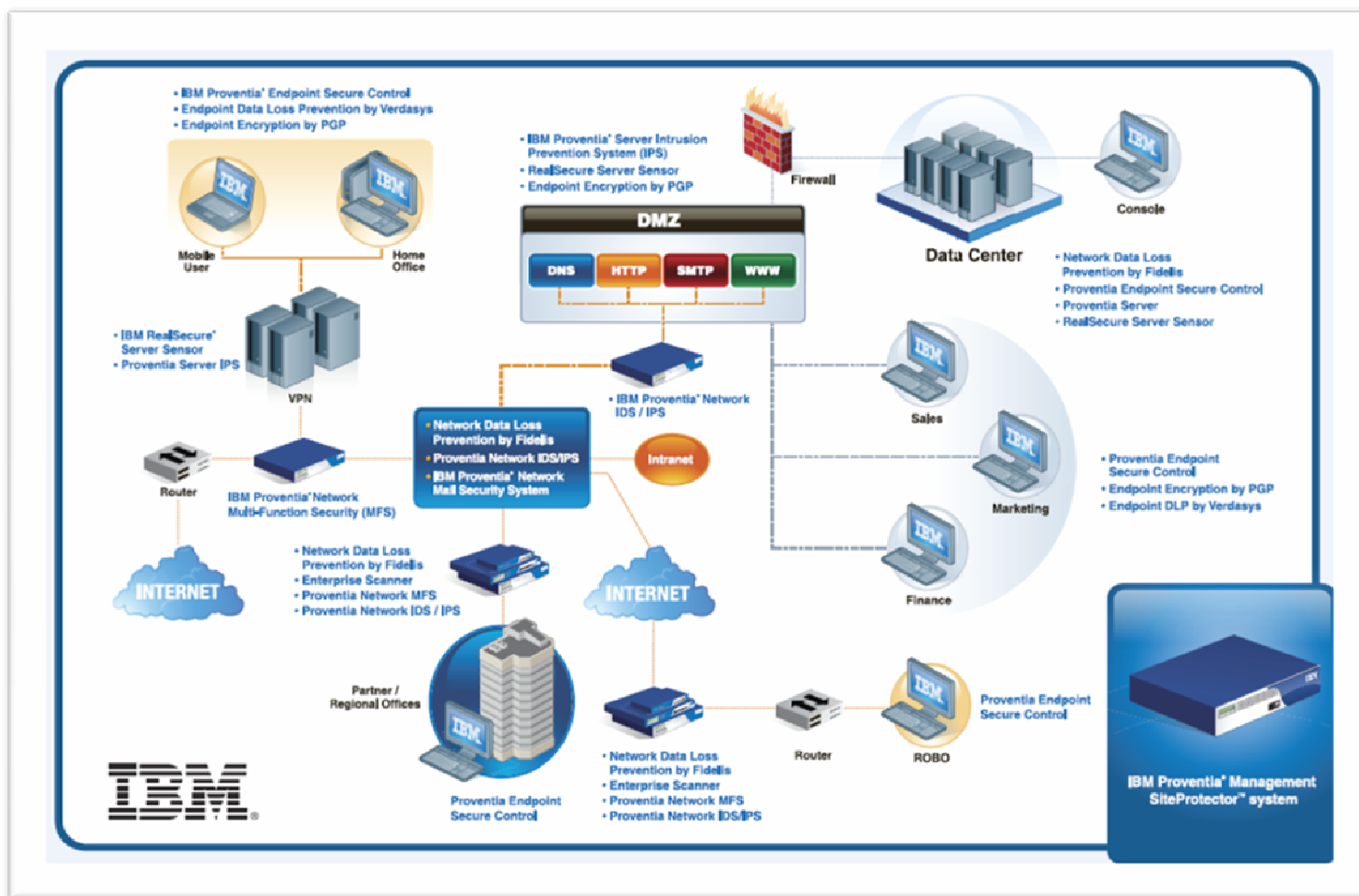- Log Analysis

Physical Security

- Smart Surveillance Solution

Managed Security Services

Managed Security Services

- IBM Managed and Monitored Firewall Services
- Managed IAM
- IBM Managed IPS and IDS Services
- Managed Data Security Services
- IBM Managed UTM Services
- Managed Protection Services

NORMALIZE • AGGREGATE • CORRELATE

Security Enablement Services

- IBM Vulnerability Management Services
- Security Event Management Services
- Secure Log Management Services
- IBM ISS X-Force® Threat Analysis Services
- Managed Email/ Web Security

ARCHIVE • ESCALATE • REMEDIATE
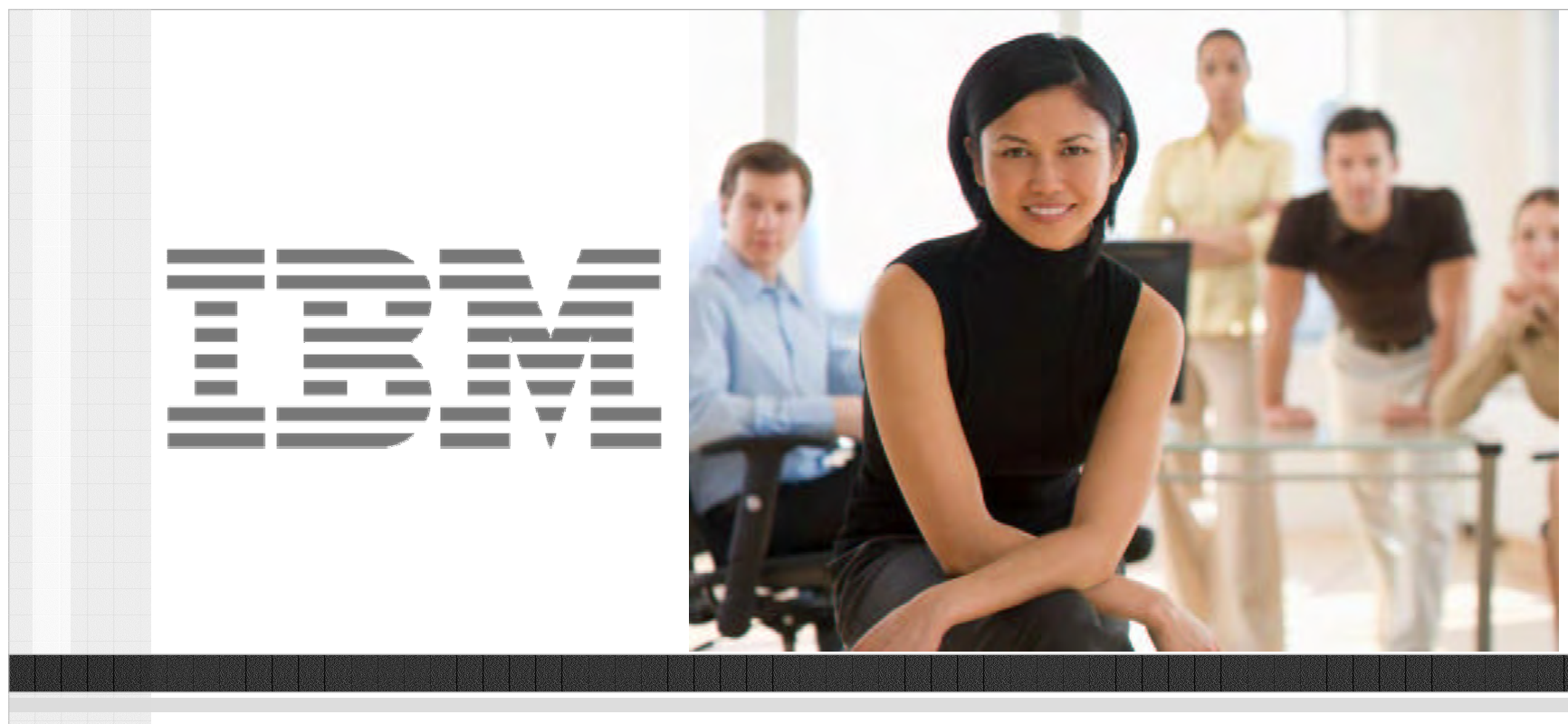
**Multiple Platforms & Products**

Integrated Products
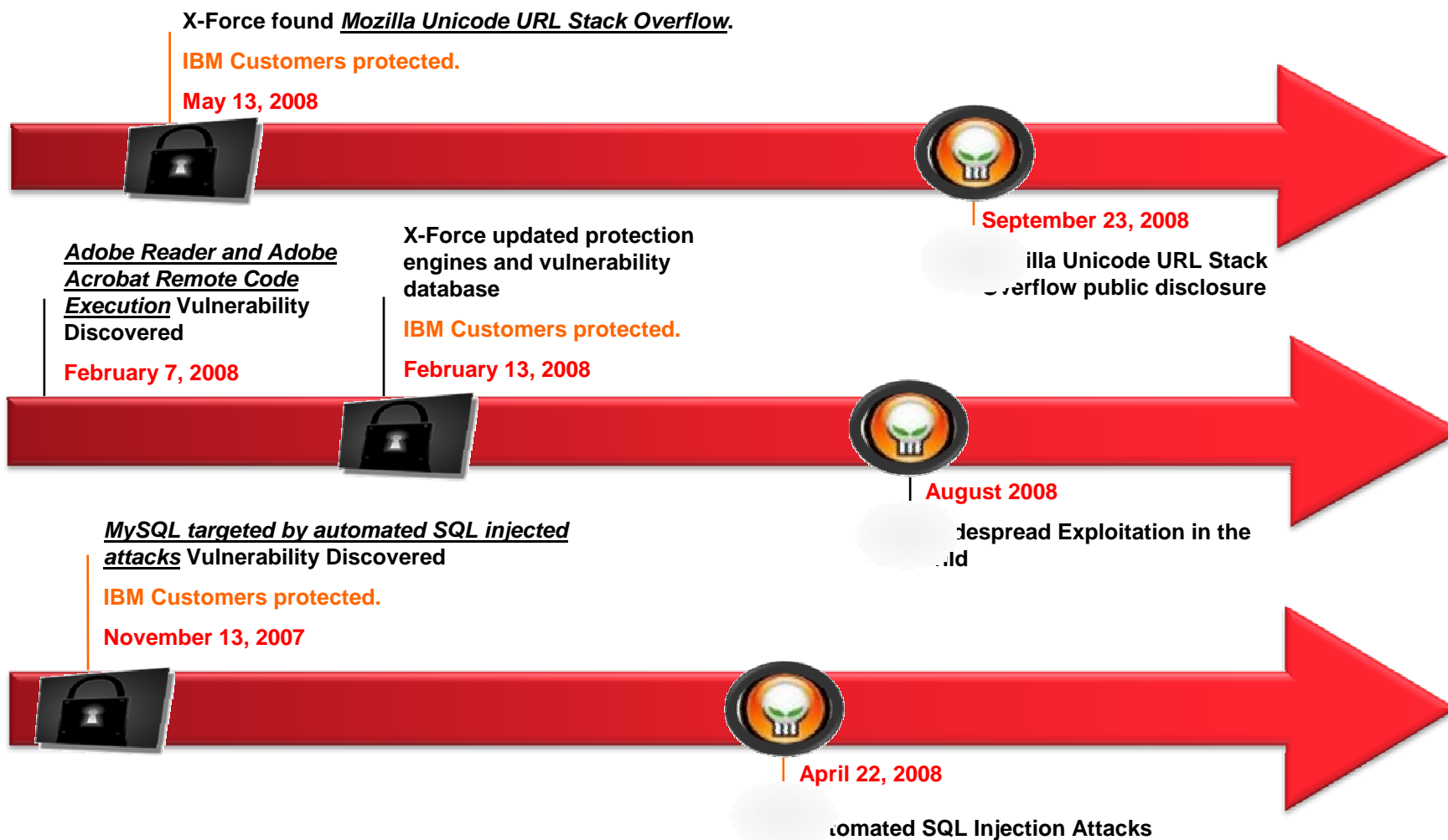
Why…

The IBM ISS X-Force Advantage

- The **CORE** of IBM Security
- Most comprehensive Vulnerability Database in the world
  - Over **38,000** unique vulnerabilities catalogued
  - Entries date back to the 1990's
  - 9.1B Web Pages & Images Analyzed
  - 150M Intrusion Attempts Daily
  - 40M Spam & Phishing Attacks

- Updated daily by a dedicated research team
- The X-Force database currently tracks over...
  - **7,600 Vendors**
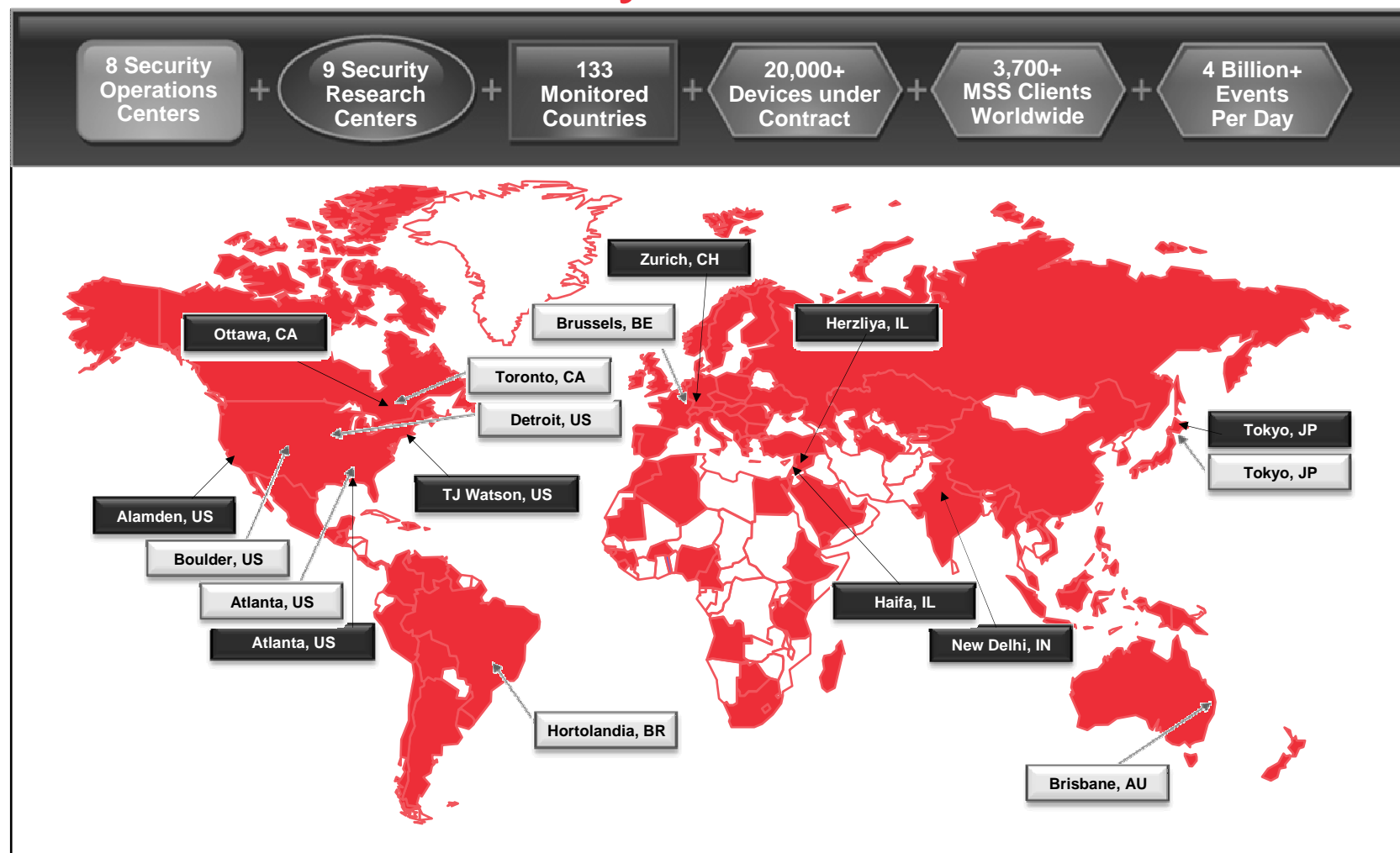 - **17,000 Products**
  - **40,000 Versions**
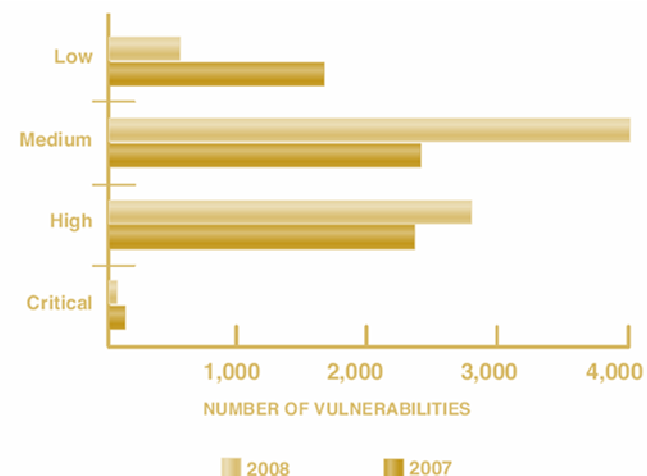
X-Force® Research and Development - The world leaders in security intelligence

The X-Force Difference

X-Force found _Mozilla Unicode URL Stack Overflow_.

IBM Customers protected.

May 13, 2008

September 23, 2008

illa Unicode URL Stack
verflow public disclosure

Adobe Reader and Adobe Acrobat Remote Code Execution Vulnerability Discovered

February 7, 2008

X-Force updated protection engines and vulnerability database

IBM Customers protected.

February 13, 2008

August 2008

despread Exploitation in the
ld

MySQL targeted by automated SQL injected attacks Vulnerability Discovered

IBM Customers protected.

November 13, 2007

April 22, 2008

tomated SQL Injection Attacks

IBM Global Security Reach

8 Security Operations Centers	+	9 Security Research Centers	+	133 Monitored Countries	+	20,000+ Devices under Contract	+	3,700+ MSS Clients Worldwide	+	4 Billion+ Events Per Day

Zurich, CH

Brussels, BE

Herzliya, IL

Ottawa, CA

Toronto, CA

Detroit, US

Tokyo, JP

Tokyo, JP

Alamden, US

TJ Watson, US

Boulder, US

Atlanta, US

Haifa, IL

Atlanta, US

New Delhi, IN

Hortolandia, BR

Brisbane, AU

Why Partner with IBM?

IBM LEADERSHIP

- Security Leadership for **12+ Years**

- **Consult** as well as **remediate**

- **15,000** researchers, developers and SMEs on security initiatives

- **3,000+** security & risk management patents

- 40+ years of proven success securing the zSeries environment

- **X-Force® R&D** – the unequivocal world authority in vulnerability and threat research

- $6.0B+ in R&D per year, **$1.5 Billion in Security - 2008**

- IBM is the **only security vendor** in the market today with end-to-end coverage of critical controls

- **Leadership in Managed Security Services** 2007 and 2008: Gartner Magic Quadrant, Forrester Wave, Frost & Sullivan

- Experience with clients of all sizes, industries, all over the world

- **8 Security Operations Centers + 9 Security Research Centers**

So show me the money…

Customer Speak

"Meeting the PCI DSS regulations was mandatory, but IBM provided us with more than just compliance. Sensitive data is secure, systems are monitored closely for performance issues, and our IT staff can <u>*focus on more mission-critical activities.*</u>*"*

A Retail Company

"The real key is that we have the education in place and now implement security early in the application development lifecycle, so we <u>*have less overall vulnerabilities to manage.*</u>*"*

A Financial Services Firm

"We looked at the TCO and it <u>*made more sense to outsource to IBM ISS.*</u>*"*

A Telecommunications Company

"Using Managed Protection Services instead of paying for 24/7 onsite staff with no guarantee of consistent expertise was <u>*slam dunk ROI*</u>*"*

A Wealth Management Firm

"<u>*IBM allowed us to meet business goals*</u> *while strengthening our security systems and improving the efficiency and effectiveness of our security operations"*

A Manufacturing Organization

"The Proventia Intrusion Prevention Appliance and SiteProtector management system have <u>*saved me time and money*</u> *- I have saved substantial costs in hiring extra staff and lots of time in managing the 20 appliances in place today."*

An Insurance Group

Thank You

Bhrigu Nagal
bhrnagal@in.ibm.com
+91-9717200133