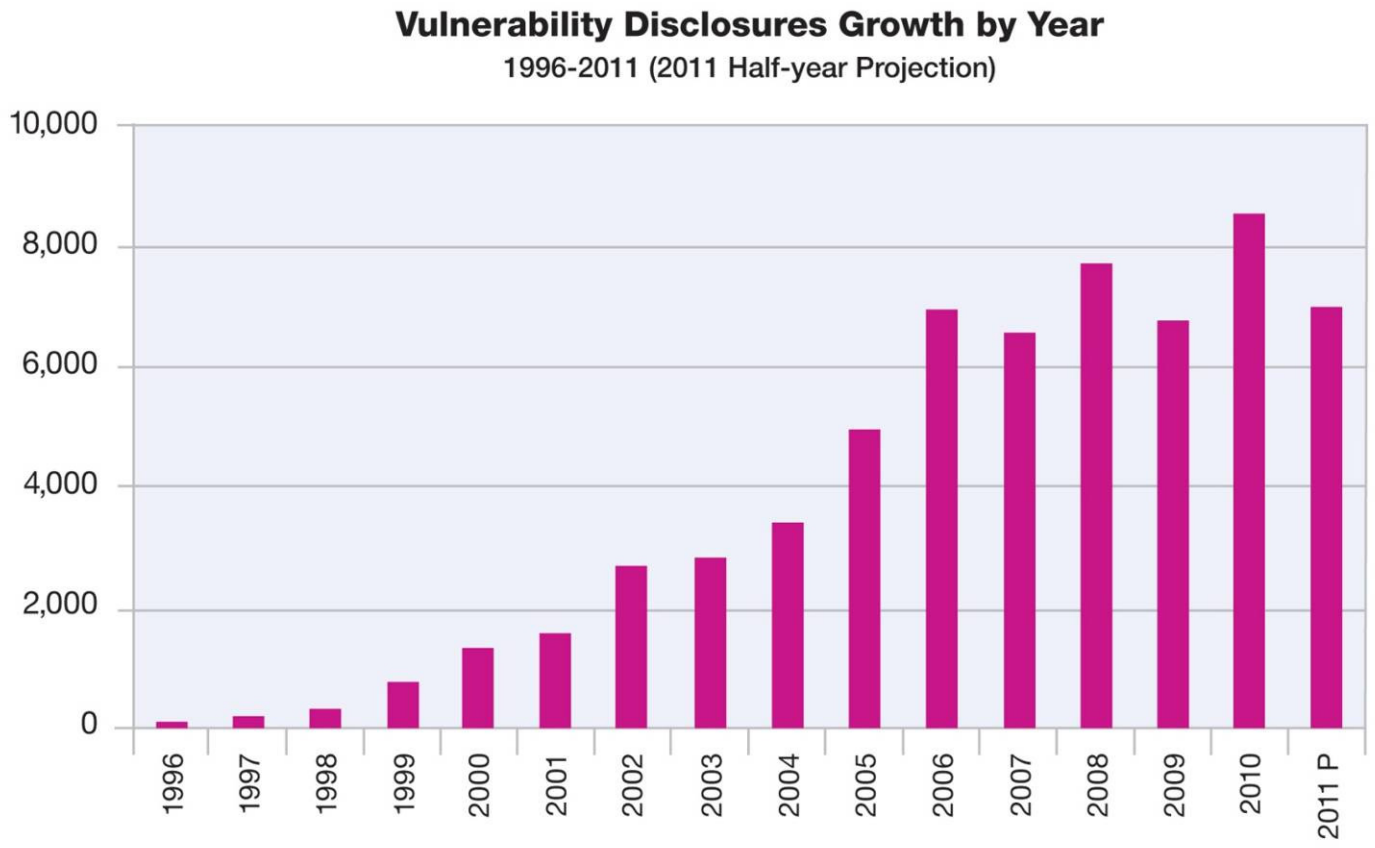
FAU Cybersecurity Presentation
Securing & Protecting the Enterprise

Don Kneitel, North America Security Consulting Services Leader
Kneiteld@us.ibm.com, 678-644-9053, October 28, 2011

Agenda & Discussion

- Security Vulnerabilities
- X-Force approach to finding them
- What is occurring in the Industry – types of hacks
- How do you start to address them
- What are the bigger business issues
- How do organizations need to address security
- Approaches to effective security

There are about 7,000 software vulnerability disclosures every year…



Source: IBM X-Force® Research and Development

We analyze them all…

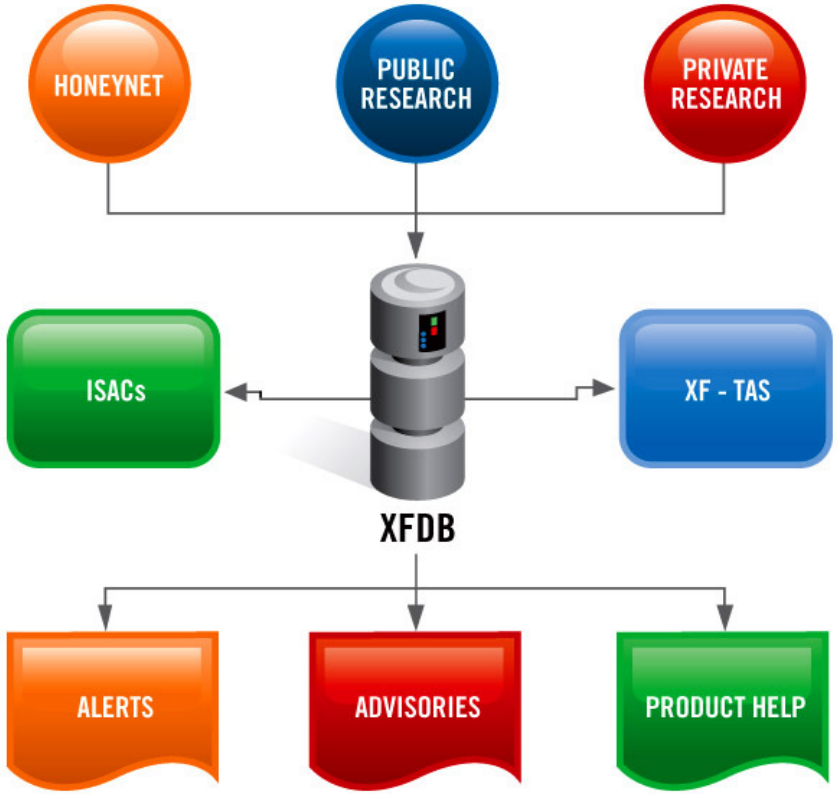
Most comprehensive Vulnerability Database in the world

- Over **50,000** unique vulnerabilities catalogued
- Entries date back to the 1990's

Updated daily by a dedicated research team

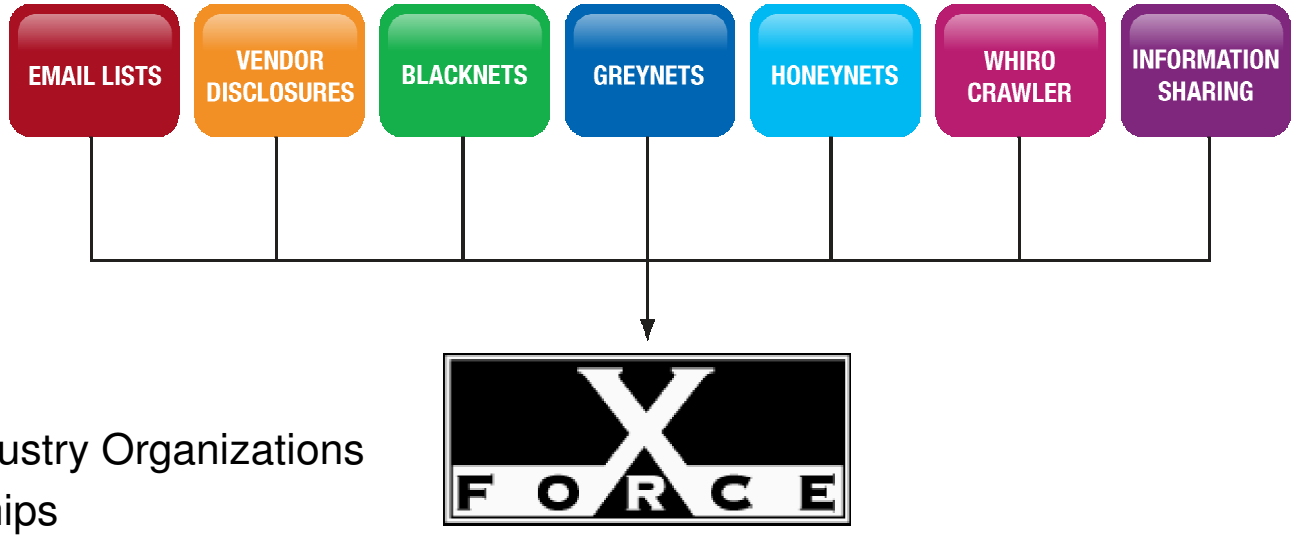
The X-Force database currently tracks over...

- 8000 Vendors
- 17,000 Products
- 40,000 Versions



Information Sources

- Email lists
- Vendor disclosures
- Blacknets
- Greynets
- Honeynets
- Whiro Crawler
- Information Sharing
  - ISACS, CERTs, Industry Organizations
  - Research Partnerships
  - Conferences
  - Online



Reasons for Vulnerability Analysis

- Avoiding false positives
  - Signature writers need to understand precise details about the vulnerability
    - legal buffer sizes
    - valid ranges for field values
- Avoiding false negatives
  - Signature writers need to emulate the product's protocol parsers as closely as possible
  - There may be multiple vectors to exploit a particular vulnerability
- Correctly evaluating risk
  - Is a particular vulnerability really a remote code execution issue or just a denial of service problem?
  - How hard is it to exploit? Are blackhat researchers likely to figure it out?
  - Are there other vulnerabilities

Some vulnerabilities require in depth analysis…

Vulnerability Details

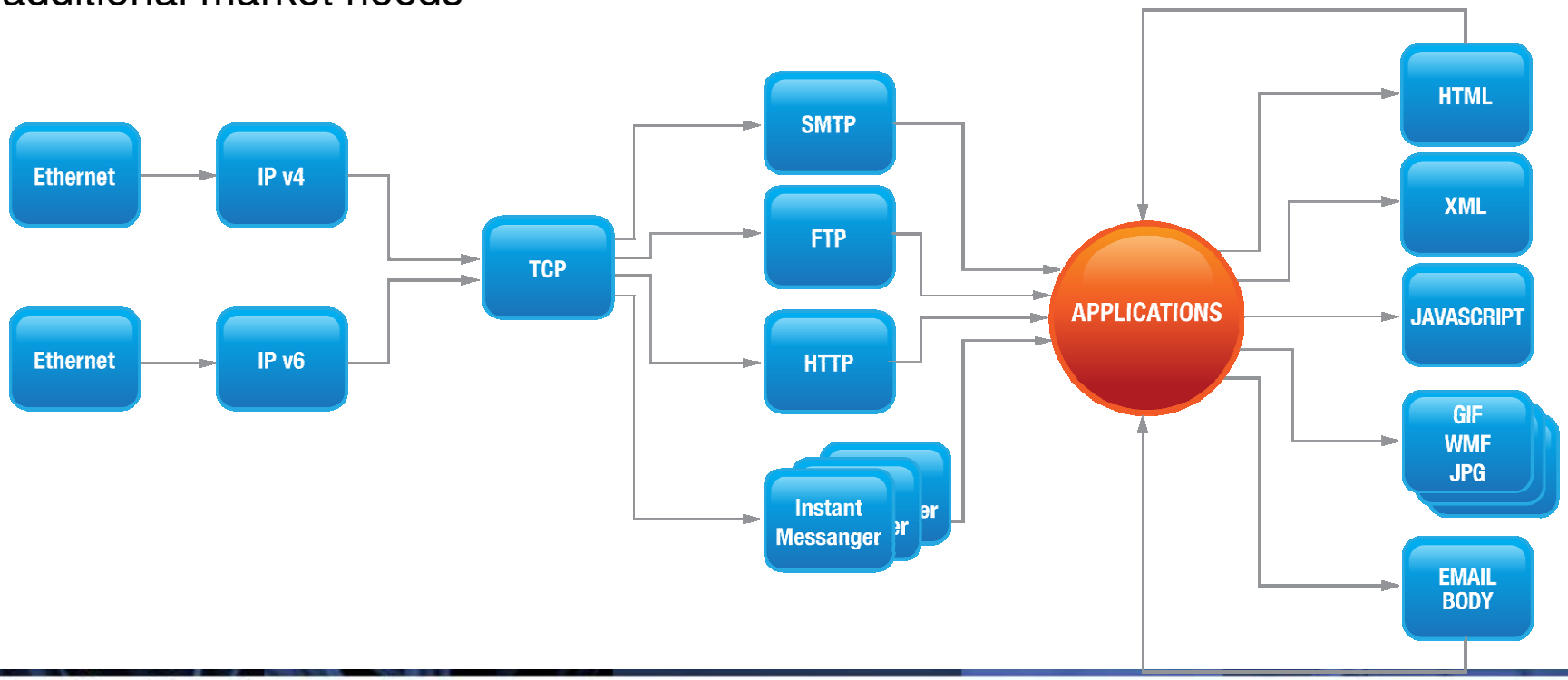
This vulnerability allows remote attackers to execute arbitrary code on vulnerable Symantec VERITAS NetBackup installations. Authentication is not required to exploit this vulnerability.

This specific flaw exists within the volume manager daemon (vmd.exe) due to incorrect bounds checking during a call to sscanf() that copies user-supplied data to a stack-based buffer. The vulnerable daemon listens on TCP port 13701.

```
.text:00435A64                push    edx
.text:00435A65                lea     eax, [esi+50h]
.text:00435A68                push    eax
.text:00435A69                lea     ecx, [esp+1A0h+var_34]
.text:00435A70                push    ecx
.text:00435A71                lea     edx, [esp+1A4h+var_70]
.text:00435A78                push    edx
.text:00435A79                lea     eax, [esi+12h]
.text:00435A7C                push    eax
.text:00435A7D                lea     ecx, [esp+1ACh+var_78]
.text:00435A84                push    ecx
.text:00435A85                lea     edx, [esp+1B0h+var_A0]
.text:00435A8C                push    edx
.text:00435A8D                push    esi
.text:00435A8E                push    offset aDSSHdSSHdHdS_2 ; "%d %s %s %hd %s %s %hd %hd %s %s %s %hd"...
.text:00435A93                push    ebp             ; char *
.text:00435A94                call    ds:sscanf       ; really???  --  who does this??
.text:00435A9A                add     esp, 110h
```

Protocol/Content Analysis at ALL Levels

- Simulate the protocol/content stacks in the vulnerable systems
- Normalize at each protocol and content layer
- Ability to shim in new technologies and grow with not only evolving threats but additional market needs

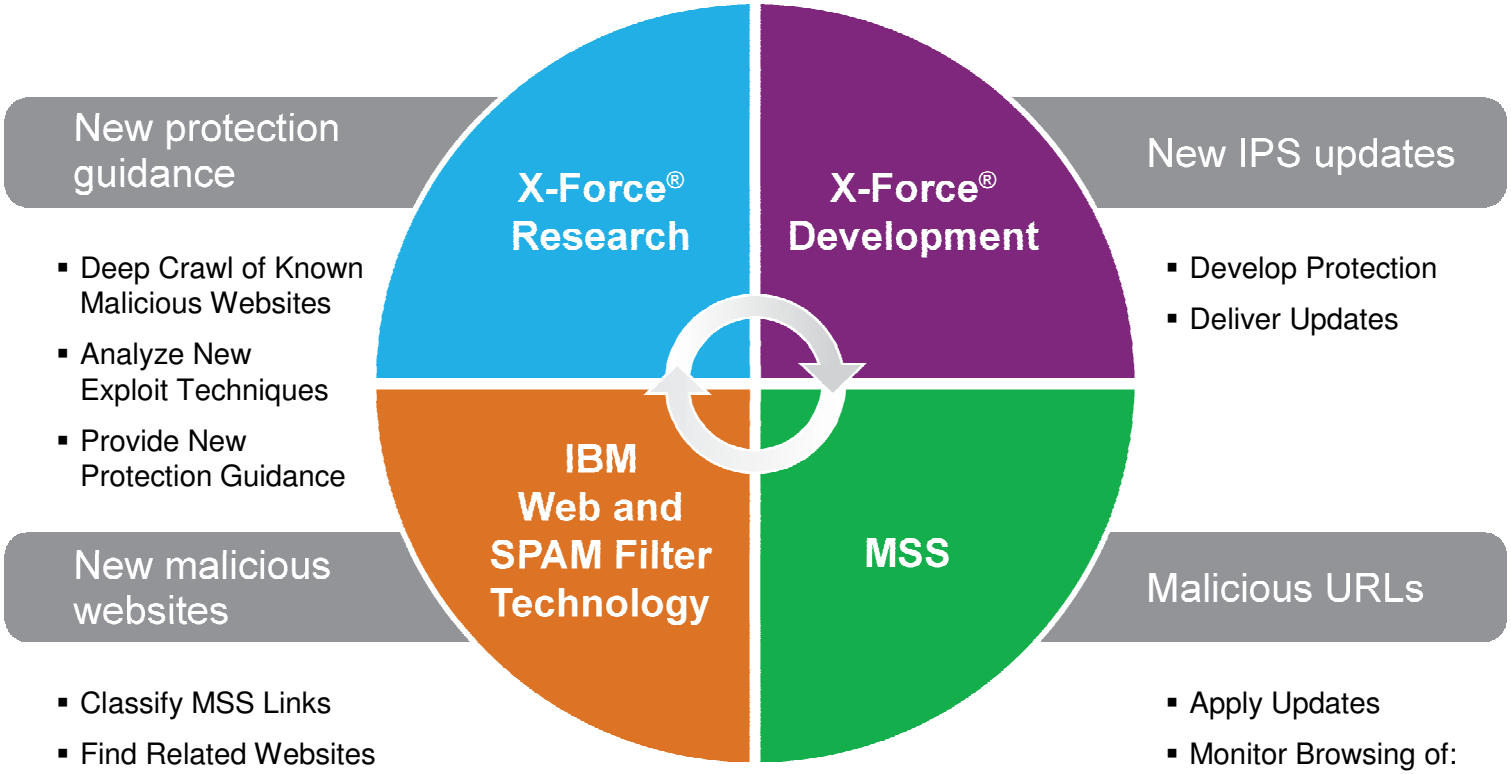


IBM Virtual Patch Technology

- At the end of 2010, **44%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability
- Shielding a vulnerability from exploitation independent of a software patch
- Enables a responsible patch management process that can be adhered to without fear of a breach
- IBM is a MAPP (Microsoft Active Protections Program) partner

FEATURING VIRTUAL PATCH® TECHNOLOGY

IBM X-Force web intelligence lifecycle



New protection guidance

- Deep Crawl of Known Malicious Websites
- Analyze New Exploit Techniques
- Provide New Protection Guidance

New IPS updates

- Develop Protection
- Deliver Updates

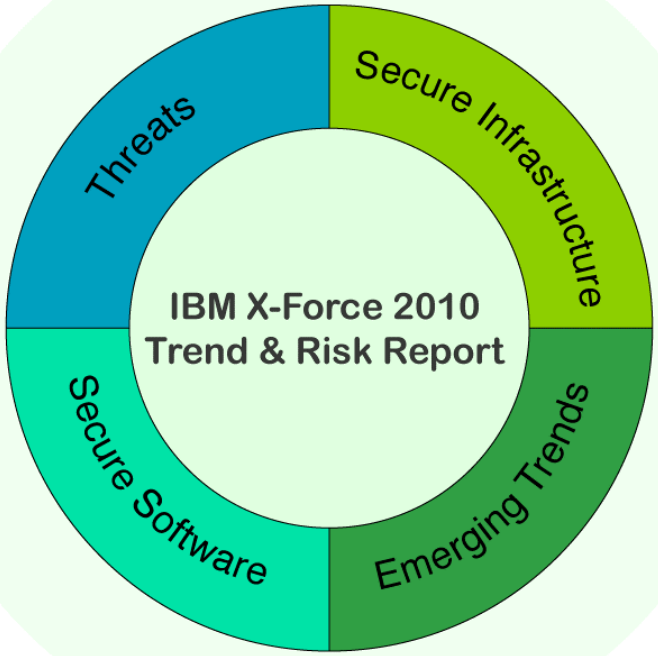
New malicious websites

- Classify MSS Links
- Find Related Websites (Deep Crawl)
- Search for Malware
- Find New Malicious Websites
- Block All Malicious Domains

Malicious URLs

- Apply Updates
- Monitor Browsing of:
  - Million of End-users
  - Thousands of Customers
  - Hundreds of Countries
- Block Malicious Links
- Send Links to X-Force

X-Force Trend Report



Section I–Threats

- Topics that comprise “Threats” and describe the attacks aimed at the enterprise that security specialists face.
- Latest attack trends as identified by IBM.

Section II—Operating Secure Infrastructure

- Topics surrounding the weaknesses in process software, and infrastructure targeted by today’s threats.
- Security compliance best practices, operating cost reduction ideas, automation, lowered cost of ownership, and the consolidation of tasks, products, and roles.
- Present data tracked across IBM during the process of managing or mitigating these problems.

Section III— Developing Secure Software

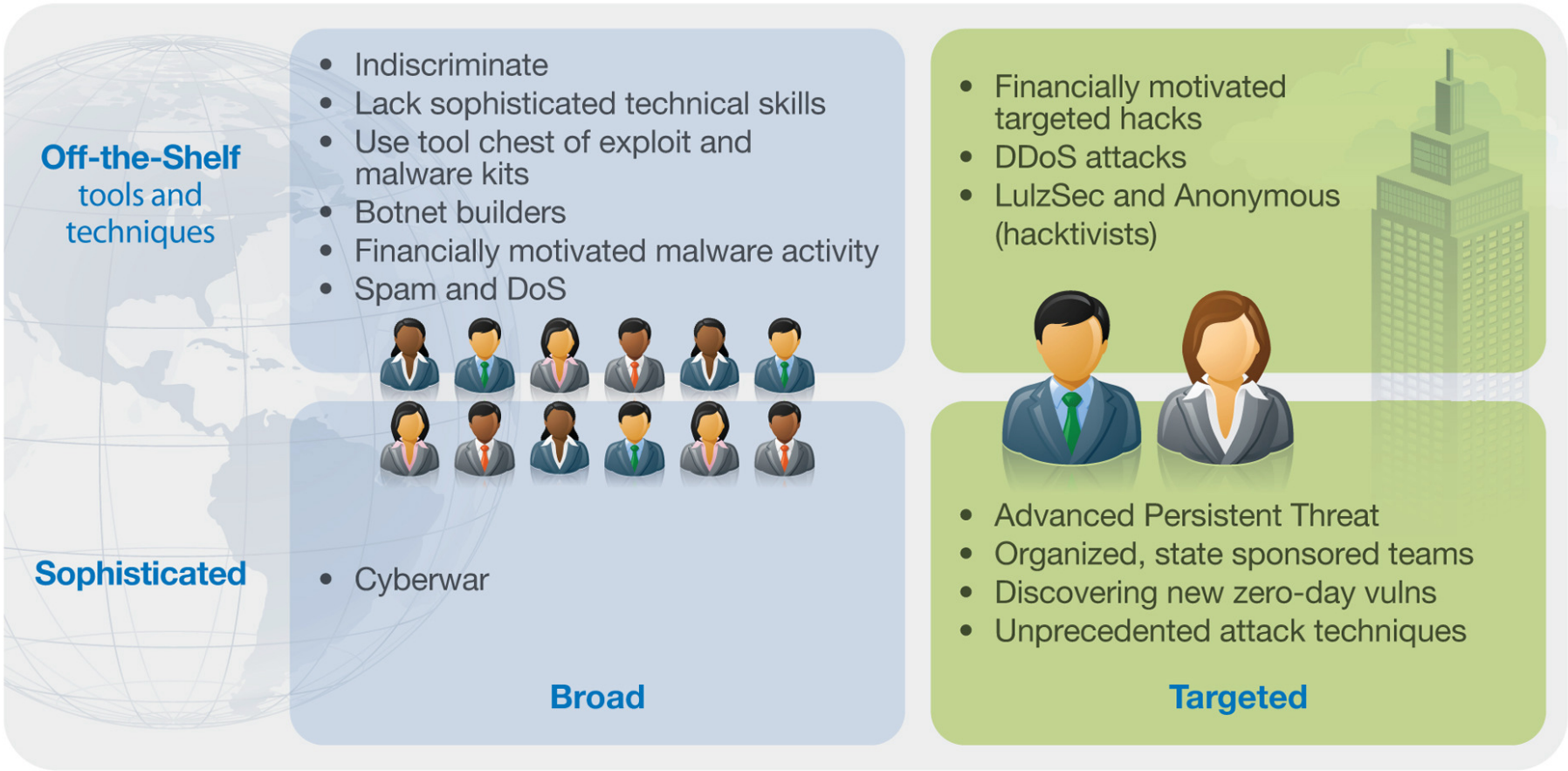
- Proven processes and techniques for developing secure software.
- Discussion on how enterprises can find existing vulnerabilities and help prevent new ones from being introduced.
- Static and dynamic security testing done by the Rational AppScan group in all stages of application development and share insights

Section IV—Emerging Trends in Security

- Developing technology that presses upon enterprises for future investments
- Explaining where threats and exploits are being utilized in these early technology adoptions and how enterprises can stay focused.

Who is attacking our networks?

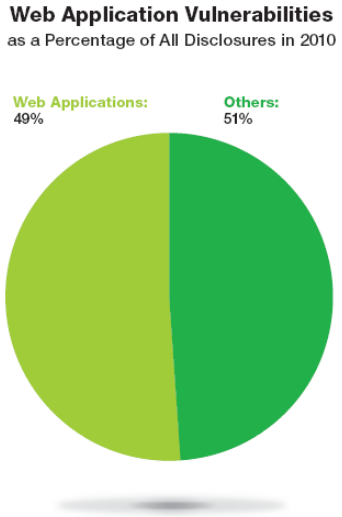
Attacker Types and Techniques 2011 H1

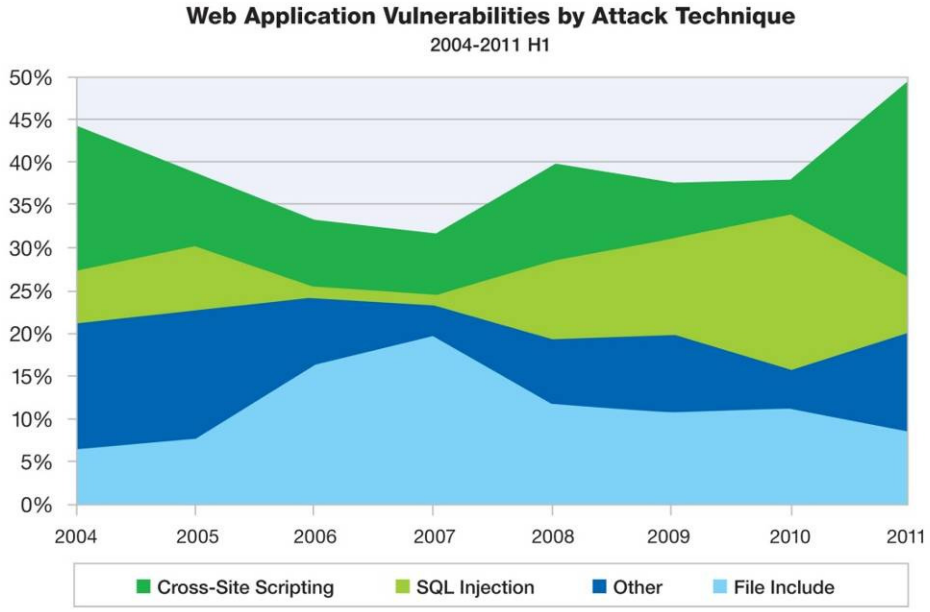


Source: IBM X-Force® Research and Development

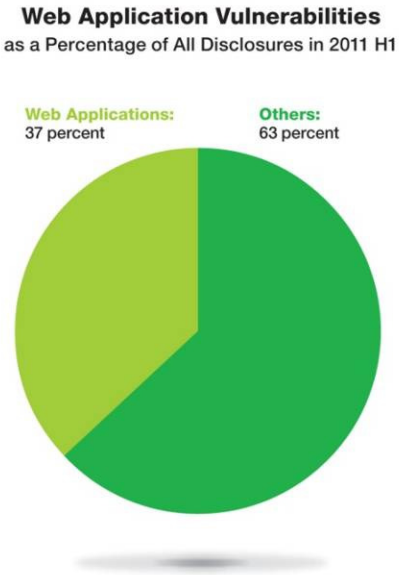
Decline in web application vulnerabilities in H1 2011

- In 2010 49% of security vulnerabilities affected web applications.
- In 2011 37% affected web applications.
- Big decline in SQL Injection vulnerabiliites.





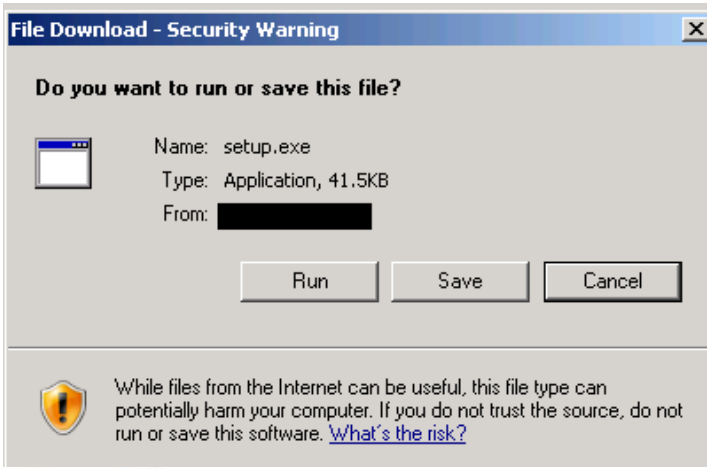
Source: IBM X-Force® Research and Development

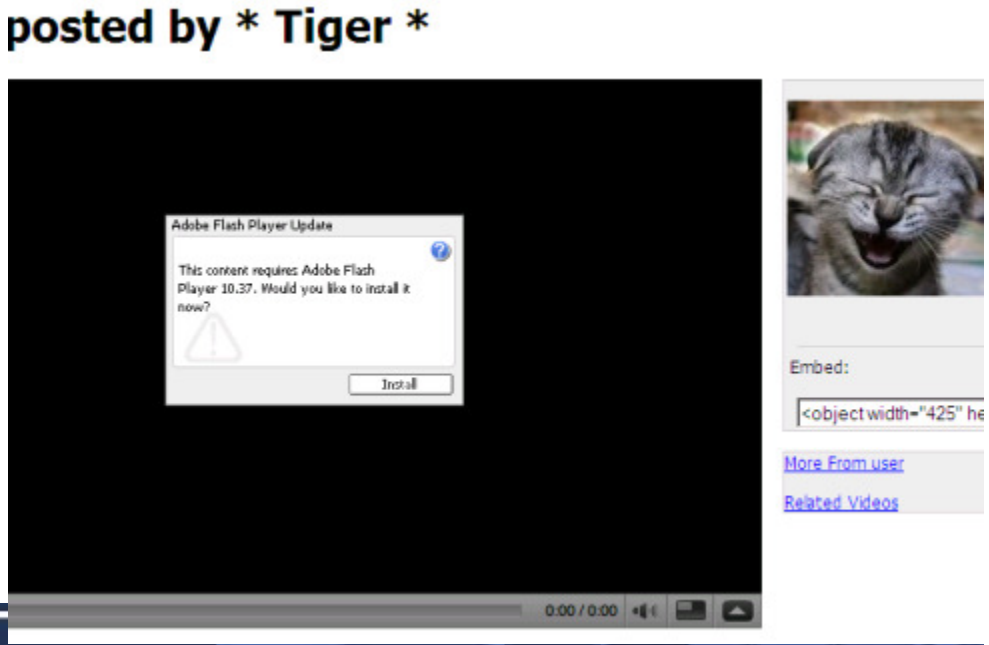


Source: IBM X-Force® Research and Development

Spear Phishing and Social Engineering on the Rise

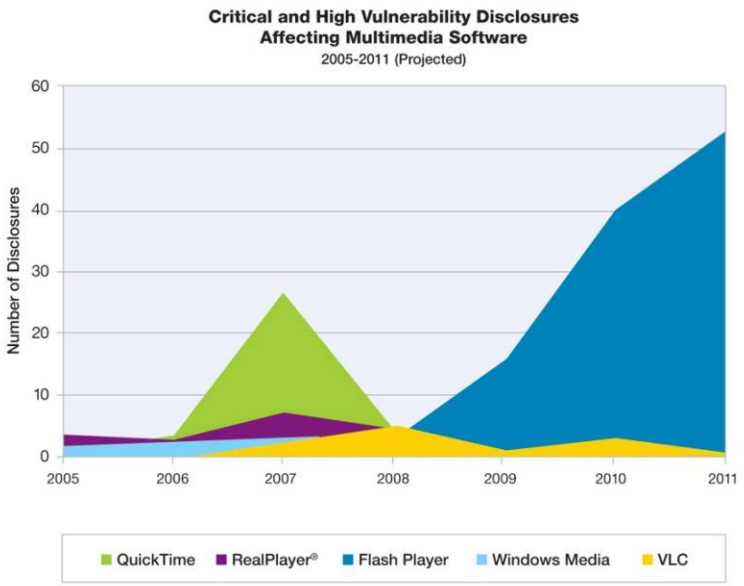
- Social networks represent a vehicle for malware authors to distribute their programs in ways that are not easily blocked. Examples include:
  - Antivirus 2009, which lures users into downloading a fake AV product.
  - The Koobface Worm which infiltrated Facebook, Myspace, and other social networking sites.
  - The Jahlav Trojan which used Twitter to infect Mac users.
- "There is no patch for stupid."



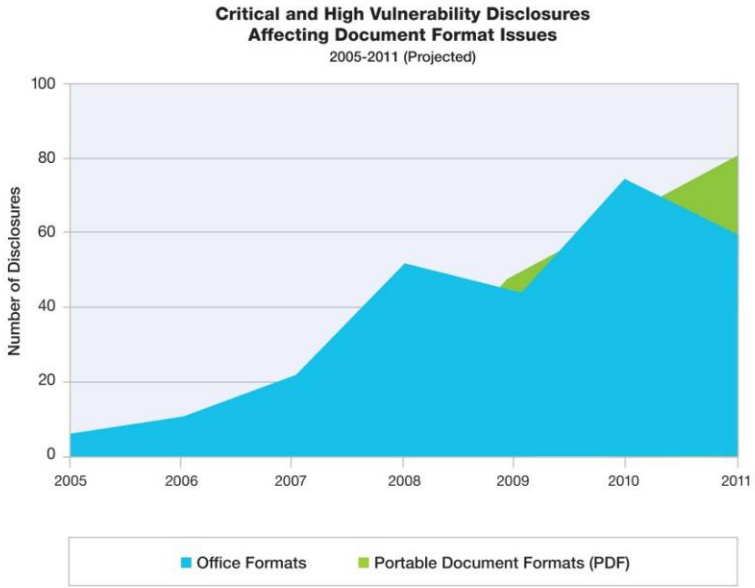


Multi-media & doc vulnerabilities increase

- Significant increases in both categories
- Attackers have zeroed in on software that consumers are running regardless of the browser
- Recent efforts to sandbox these applications are not perfect

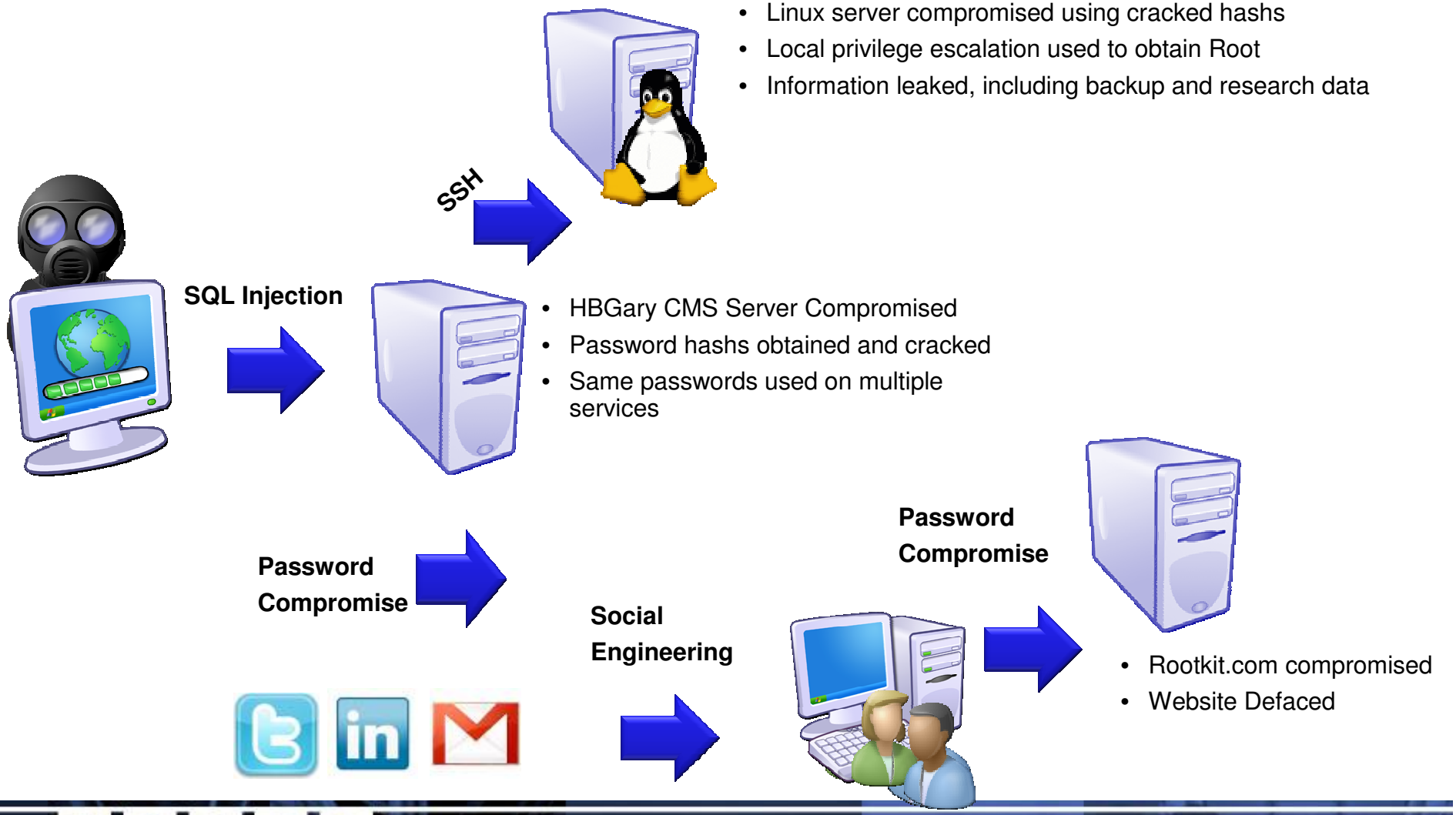


Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Well known, off the shelf attack techniques are all that it takes



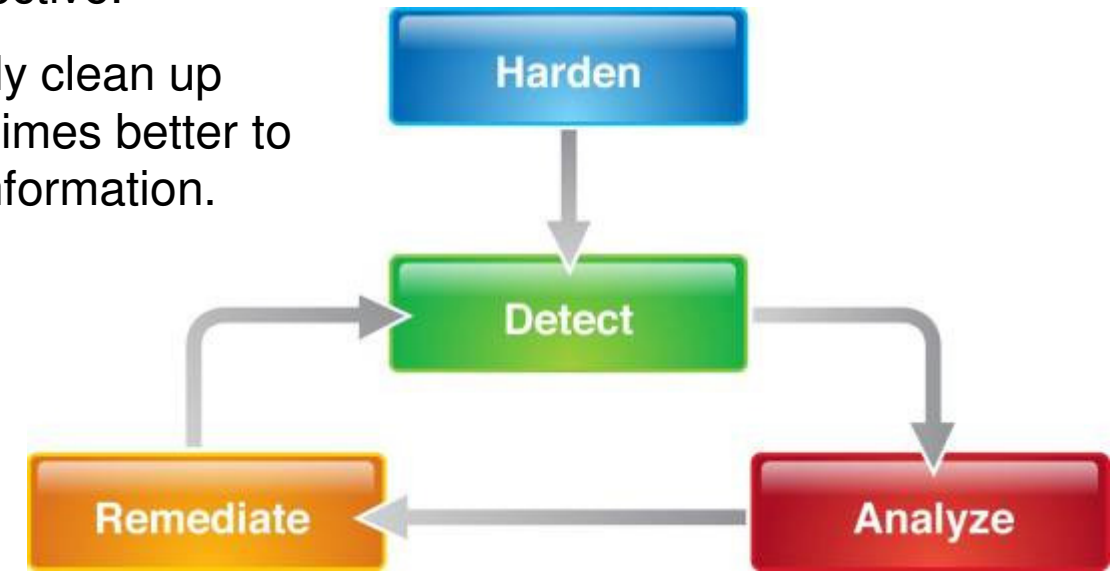
- Linux server compromised using cracked hashs
- Local privilege escalation used to obtain Root
- Information leaked, including backup and research data

- HBGary CMS Server Compromised
- Password hashs obtained and cracked
- Same passwords used on multiple services

- Rootkit.com compromised
- Website Defaced

Advanced Persistent Threats (APT) & Targeted Network Attacks

- Protecting a network from APT is a paradigm shift from the usual “audit and patch” approach to protecting a network from known threats.
- Sophisticated attackers may employ unknown attack techniques and 0day tools.
- Be willing to embrace approaches to detection that may not be 100 percent effective.
- You may not want to immediately clean up successful breaches. It is sometimes better to watch them unfold and collect information.

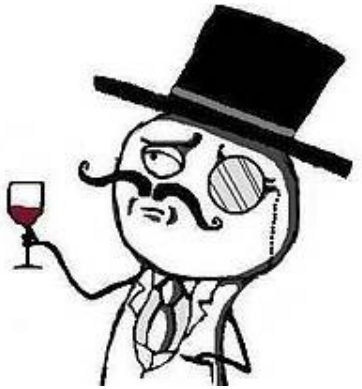


Hackers are politically & financially motivated

A member of Anonymous at the Occupy Wall Street protest in New York*

ANONYMOUS

One self-description is:
"We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."**

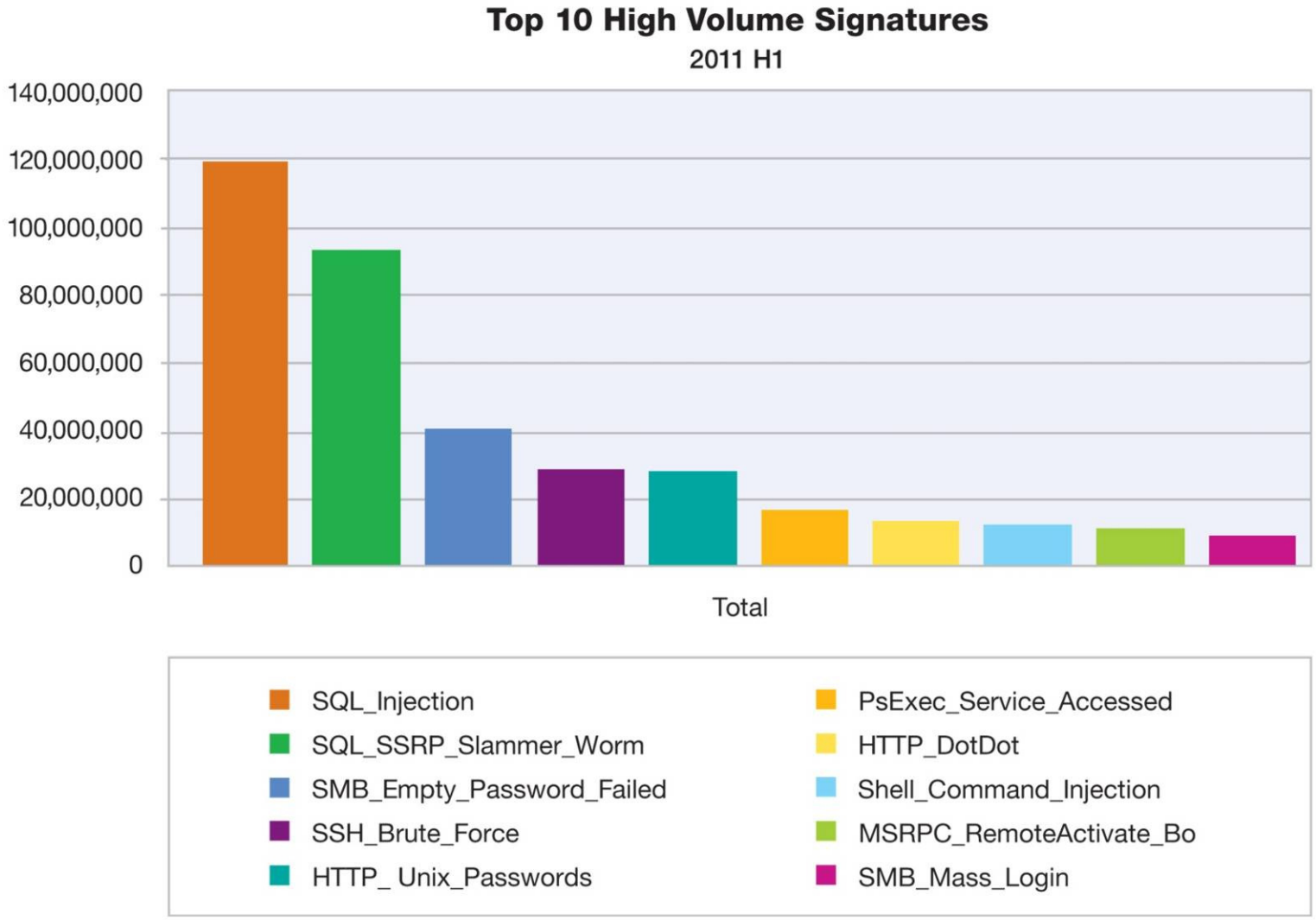


Lulz Security logo

"The world's leaders in high-quality entertainment at your expense."

*Source: David Shankbone **Source: Yale Law and Technology, November 9, 2009

Highest volume signatures



Source: IBM X-Force® Research and Development

Evolution of the Enterprise threat

Late 90's-2000
Mass Mail viruses
-Highly visible
-Mostly harmless
-No significant information loss

Antivirus

2001-2005
Network Worms
-Very noisy
-Disruptive
-No significant information loss

Antivirus

Intrusion Prevention

2006-Present
Bots
-Silent, unnoticed
-Non-Disruptive
-Significant information loss

Antivirus

Intrusion Prevention

Anomaly Detection

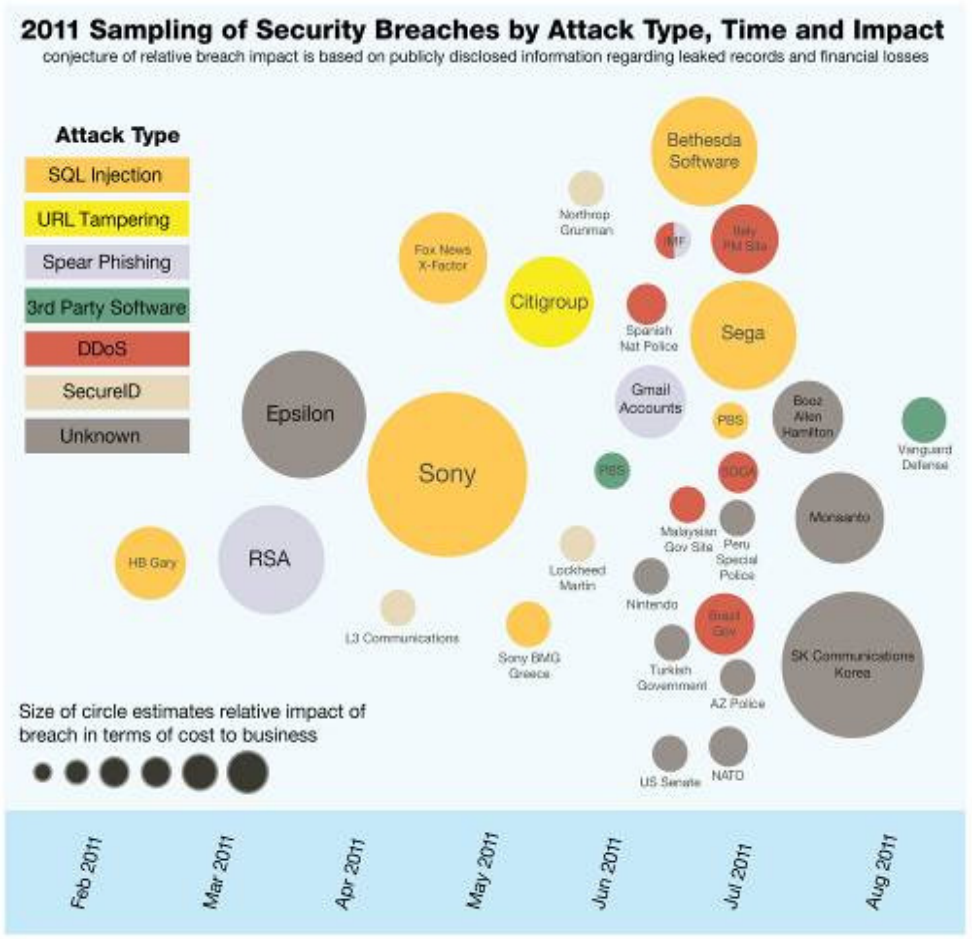
2009-
Targeted attacks
-Silent, unnoticed
-Very difficult to detect
-Targeted significant information loss

Antivirus

Intrusion Prevention

Anomaly Detection

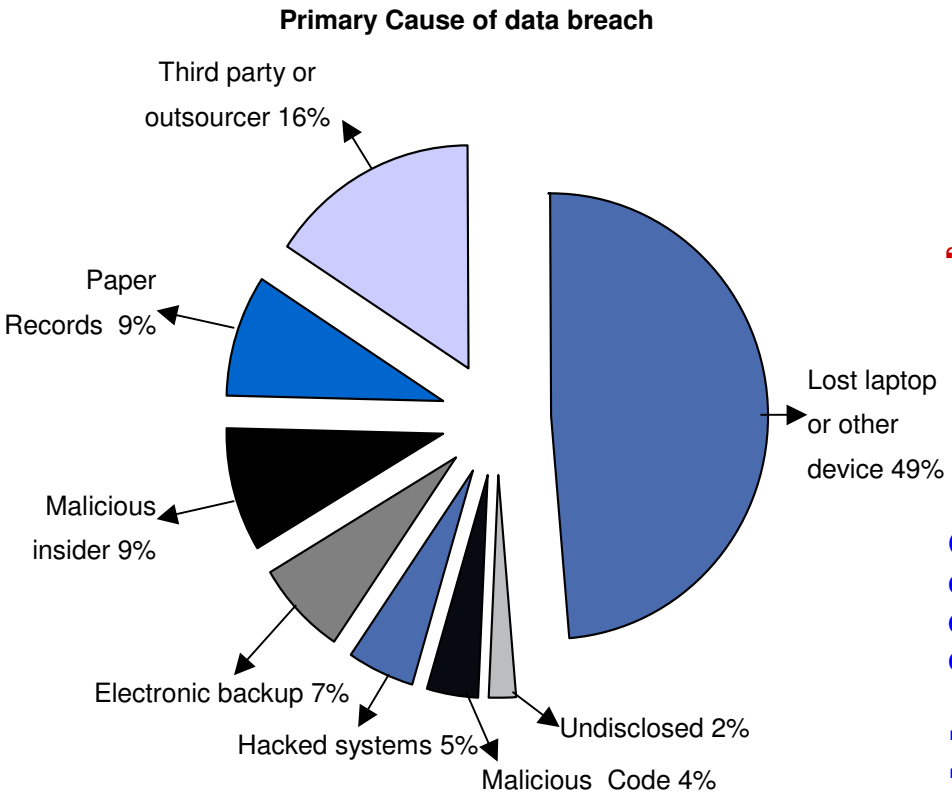
No company can effectively protect against everything, but how do you not end up in the news



- The first half of 2011 has been marked by a litany of significant, widely reported external network security breaches
- Notable not only for their frequency, but for the presumed operational competence of many of the victims
- The boundaries of business infrastructure are being extended – and sometime obliterated – by the emergence of cloud, mobility, social business, big data and more.
- Attacks are getting more and more sophisticated.

Source: IBM X-Force® Research and Development

As the risks expand and the cost of associated losses increase, data protection is top of mind



*Ponemon Institute, LLC; 2007 Annual Study: U.S. Cost of a Data Breach

"Security is evolving from the traditional, perimeter-centric model of protecting infrastructure to a data-centric model that protects information"

"…according to Gartner, insider threats are responsible for about 70% of security breaches"

Pervasive Security in a Connected World, Wachovia, April 2007

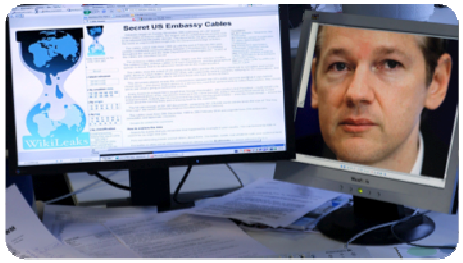
Gartner estimates a breach of customer information can cost a company from $50 to $1,000 per customer record depending on the number of accounts impacted. Typical costs include:

- **Brand reputation**
- **Lost customers**
- **Loss of revenue**
- **Audit Fees**
- **Call Center expenses**
- **Notification costs**

Litigation and regulatory fines drive the numbers even higher

Market Change 1: The impact and visibility of recent breaches calls into question the effectiveness of traditional security measures

Internal abuse of key sensitive information

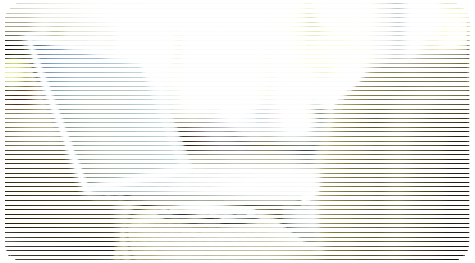


In spite of significant security policies, a single internal breach by an authorized user resulted in tens of thousands of classified records of the **US Army** leaked over Wikileaks**.** Impact to the Army is close to $100M

Complexity of malware, growth of advanced persistent threat

Stuxnet turned up in industrial programs around the world. The sophistication of the malware has led to beliefs that it was developed by a team of over 30 programmers and remained undetected for months on the targeted environment. Targeted to make subtle undetected changes to process controllers to effect uranium refinement

Business continuity interruption and brand image impact



Epsilon, which sends 40B e-mails annually on behalf of more than 2,500 clients, said a subset of its clients' customer information was compromised by a data breach. Several prominent banks and retailers acknowledged that their customers' information might be at risk

Market Change 2: Security challenges are impacting innovation

External threats

Sharp rise in external attacks from non-traditional sources

- Cyber attacks
- Organized crime
- Corporate espionage
- State-sponsored attacks
- Social engineering

Internal threats

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employee actions
- Mix of private / corporate data

Compliance

Growing need to address an increasing number of mandates

- National regulations
- Industry standards
- Local mandates

Impacting innovation

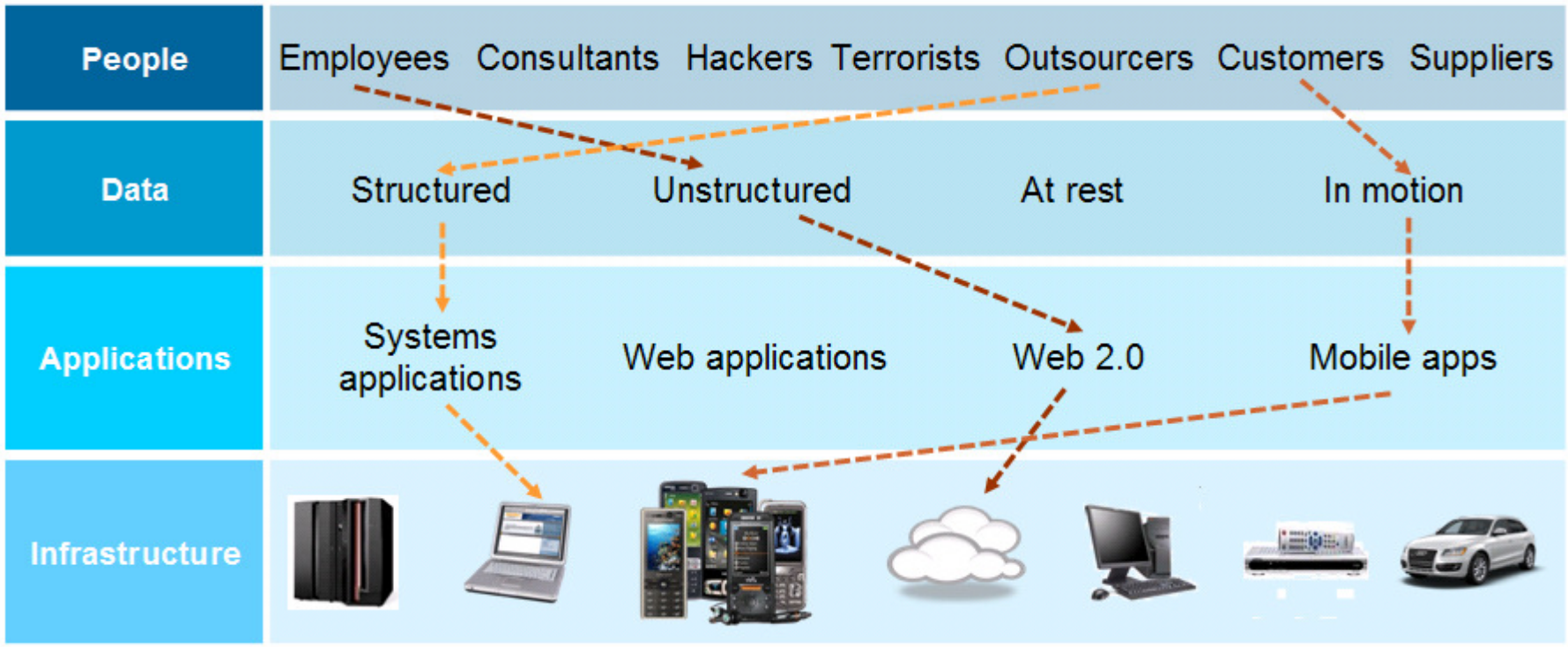
Mobility

Cloud / Virtualization

Social Business

Business Intelligence

Market Change 3: The attack surface for a typical business is growing at an exponential rate



- **77%** of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent
- **75%** felt effectiveness would increase with end-to-end solutions

Source: Ponemon Institute, June 2011

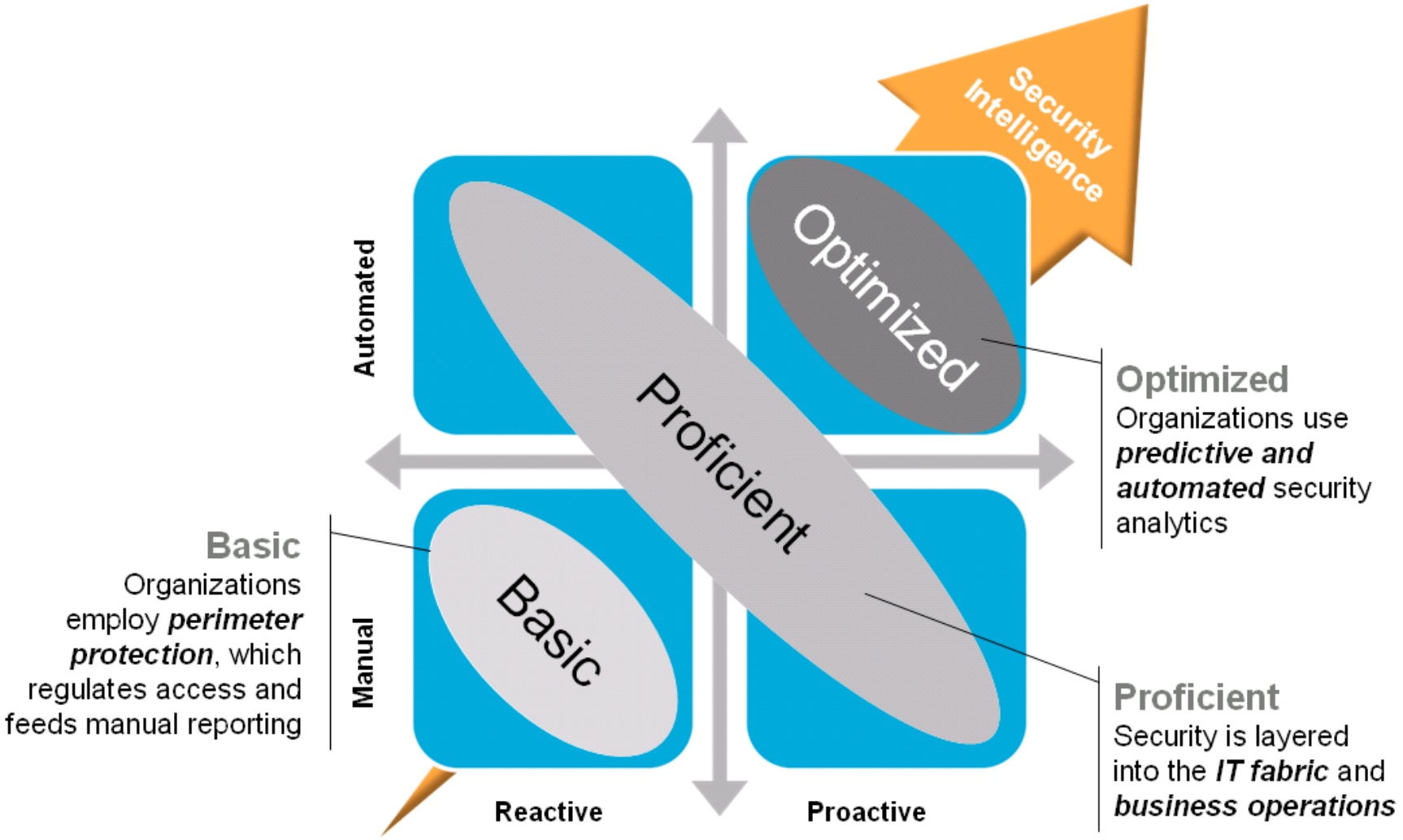
Market Change 4: The impact of a breach is now not contained to IT, but reverberates across the corporation

	CEO	CFO/COO	CIO	CHRO	CMO
CxO priority	Maintain competitive differentiation	Comply with regulations	Expand use of mobile devices	Enable global labor flexibility	Enhance the brand
Security risks	Misappropriation of intellectual property Misappropriation of business sensitive data	Failure to address regulatory requirements	Data proliferation Unsecured endpoints and inappropriate access	Release of sensitive data Careless insider behavior	Stolen personal information from customers or employees
Potential impact	Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Increasingly, companies are appointing CROs and CISOs with a direct line to the Audit Committee

*Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

In this “new normal”, IBM is helping organizations usher in an era of Security Intelligence



Some examples – Security Today vs. Tomorrow

Security will shift from a point product approach to an integrated enterprise approach, based on key foundational elements that allow for **active management, real time information, analytical correlation, and predictive threat management**

Security Domains	Today	Security Gap	Tomorrow	
People	Manage identities per application		Deploy role-based governance and privileged user management	Apply advanced correlation and deep analytics
Data	Deploy access control and encryption		Monitor usage and control leakage	
Applications	Scan for vulnerabilities		Build securely from day one	
Infrastructure	Block unwanted network access and viruses		Execute real time advanced threat detection and forensics	

Reactive ●----------▸ **Proactive**

The discussions we're having with customers…

People	1. To what extent have you rolled out an identity program? 2. How do you know what authorized users are doing? 3. What is your plan to automate identity and role-based management?
Data	1. In what ways have you classified and encrypted sensitive data? 2. How do you know if sensitive data leaves your network? 3. How do you monitor (privileged) access to data?
Applications	1. How secure is your application development process? 2. How do you regularly test your website for vulnerabilities? 3. What is your approach to test legacy applications for potential exposures?
Infrastructure	1. How do you promptly patch connected devices? 2. In what ways do you monitor in- and out-bound network traffic? 3. How are you building security into new initiatives (such as cloud, mobile and the like)?

Cross Domain

1.What is your plan to assess your security risks?

2.How do you detect threats and report compliance across domains?

3.Do you have a log retention and audit capability?

4.Which processes do you use to handle incident response and disaster recovery?

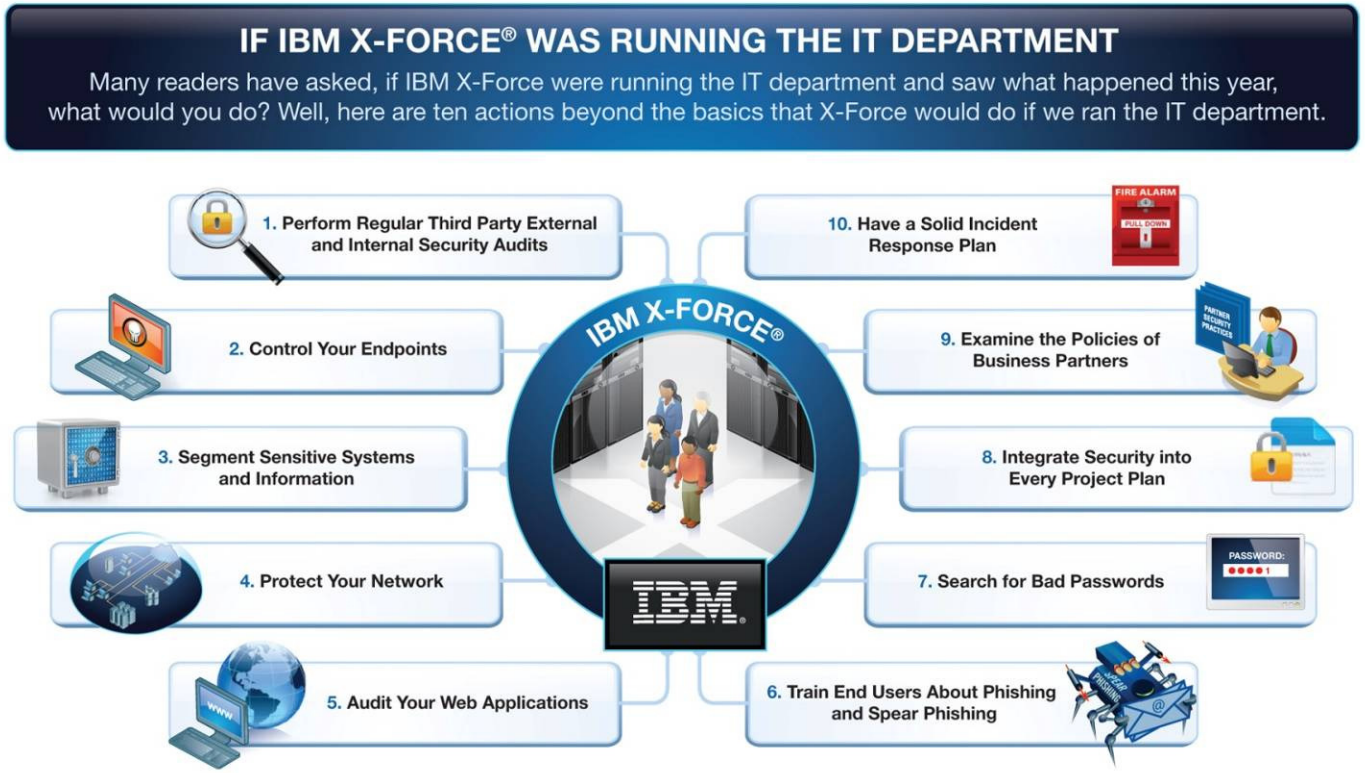
5.How do you involve key internal and external stakeholders in security matters?

Not a technical problem, but a business challenge

Many of the 2011 breaches could have been prevented

However, significant effort required to inventory, identify and close every vulnerability

Financial & operational resistance is always encountered, so how much of an investment is enough?



Source: IBM X-Force® Research and Development

The Security Challenge

Regulators

Board of Directors / Audit Committee

Theft of Client Records

CIO & Team

Theft of State Secrets

Intellectual Property Theft

Hactavists

Business imperatives:

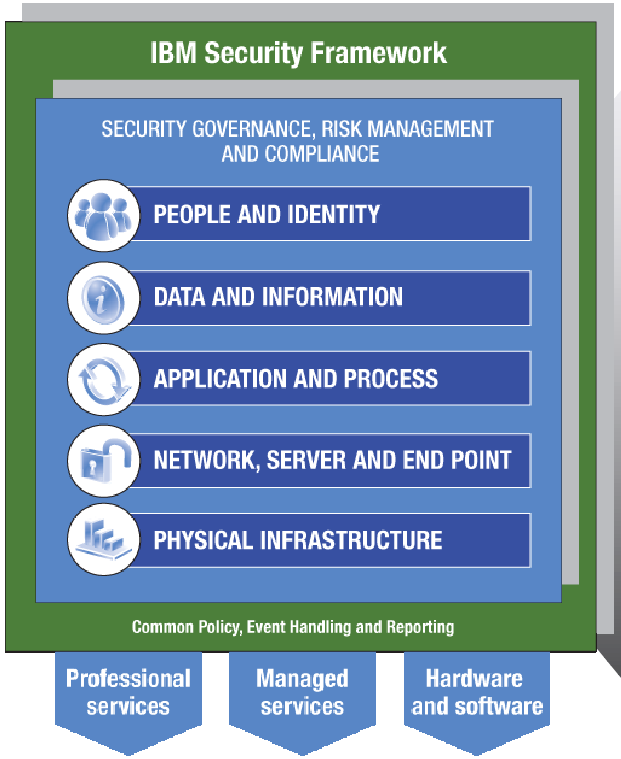
- Continuity of operations
- Protect sensitive client data
- Protect valuable IP
- Protect critical infrastructure
- Protect the Brand
- Support new, innovative and flexible business models
- Comply with policy and regulations
- Contain cost

Insider Fraud

Physical takeover of critical infrastructure

Enterprise Security Requirements

Addressed through the IBM Security Framework



GRC

GOVERNANCE, RISK MGMT AND COMPLIANCE

Ensure comprehensive management of security activities and compliance with all security mandates

PEOPLE AND IDENTITY

Mitigate the risks associated with user access to corporate resources

DATA AND INFORMATION

Understand, deploy, and properly test controls for access to and usage of sensitive data

APPLICATION AND PROCESS

Keep applications secure, protected from malicious or fraudulent use, and hardened against failure

NETWORK, SERVER AND END POINT

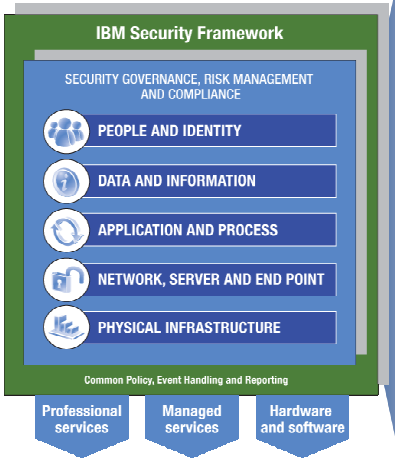
Optimize service availability by mitigating risks to network components

PHYSICAL INFRASTRUCTURE

Provide actionable intelligence on the desired state of physical infrastructure security and make improvements

IBM Security Solutions, Products & enhancements

- Professional Services
- Managed Services
- Products
- Cloud Delivered



GRC

Security Governance, Risk and Compliance

Security Information and Event Management (SIEM) & Log Management

Identity & Access Management

Identity Management

Access Management

Data Security

Data Loss Prevention

Data Entitlement Management

Encryption & Key Lifecycle Management

Messaging Security

E-mail Security

Database Monitoring & Protection

Data Masking

Application Security

Application Vulnerability Scanning

Web Application Firewall

Web / URL Filtering

Access & Entitlement Management

SOA Security

Infrastructure Security

Vulnerability Assessment

Virtual System Security

Endpoint Protection

Threat Analysis

Security Event Management

Managed Mobility Svcs

Intrusion Prevention System

Firewall, IDS/IPS MFS Management

Mainframe Security Audit, Admin & Compliance

Security Configuration & Patch Management

Physical Security

IBM has unmatched global and local expertise to deliver holistic security solutions across our entire portfolio

9 Security Operations Centers + 9 Security Research Centers + 11 Security Solution Development Centers + 133 Monitored Countries + 900+ Professional Services Security Consultants + 600+ field security specialists + 4,500 Security Delivery Experts + 400+ security operations analysts

- 16 Acquisitions in security space
- 3,700+ MSS clients worldwide
- 13 Billion+ events managed daily
- World class security research

Why IBM Security & Key Acquisitions:

Leadership

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

*IBM named **"Best Security Company"*** by SC Magazine*

Frost & Sullivan Names IBM North American Market Leader for Managed Security Services

RMONK, N.Y., Aug. 13 /PRNewswire-FirstCall/ -- IBM (NYSE: IBM) ..

Global Visibility

ALERTCON

Investment

MICROMUSE NETCOOL SOLUTIONS

INTERNET SECURITY SYSTEMS Ahead of the threat.

consul

watchfire

OUNCE LABS

Guardium SAFEGUARDING DATABASES

BIGFIX

1Q Labs Total Security Intelligence

Smarter Planet

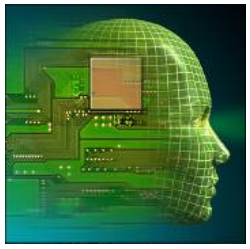
Industry Collaboration

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

INFRAGARD PARTNERSHIP FOR PROTECTION

IT ISAC INFORMATION TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Research



X FORCE

Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www-935.ibm.com/services/us/iss/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or Frequency X at http://blogs.iss.net/rss.php

Attend in-person events

http://www.ibm.com/events/calendar/

Join the Institute for Advanced Security

www.instituteforadvancedsecurity.com

Subscribe to the security channel for latest security videos

www.youtube.com/ibmsecuritysolutions

Thanks!

Questions?