Keeping the Bad Guys Out- Safeguarding Applications and Data

Susann Ulrich – North America Security Practice Leader, Rational Software
sulrich@us.ibm.com

Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information

Smarter planet opportunities driven by Web-enabled applications

The Opportunity – smarter

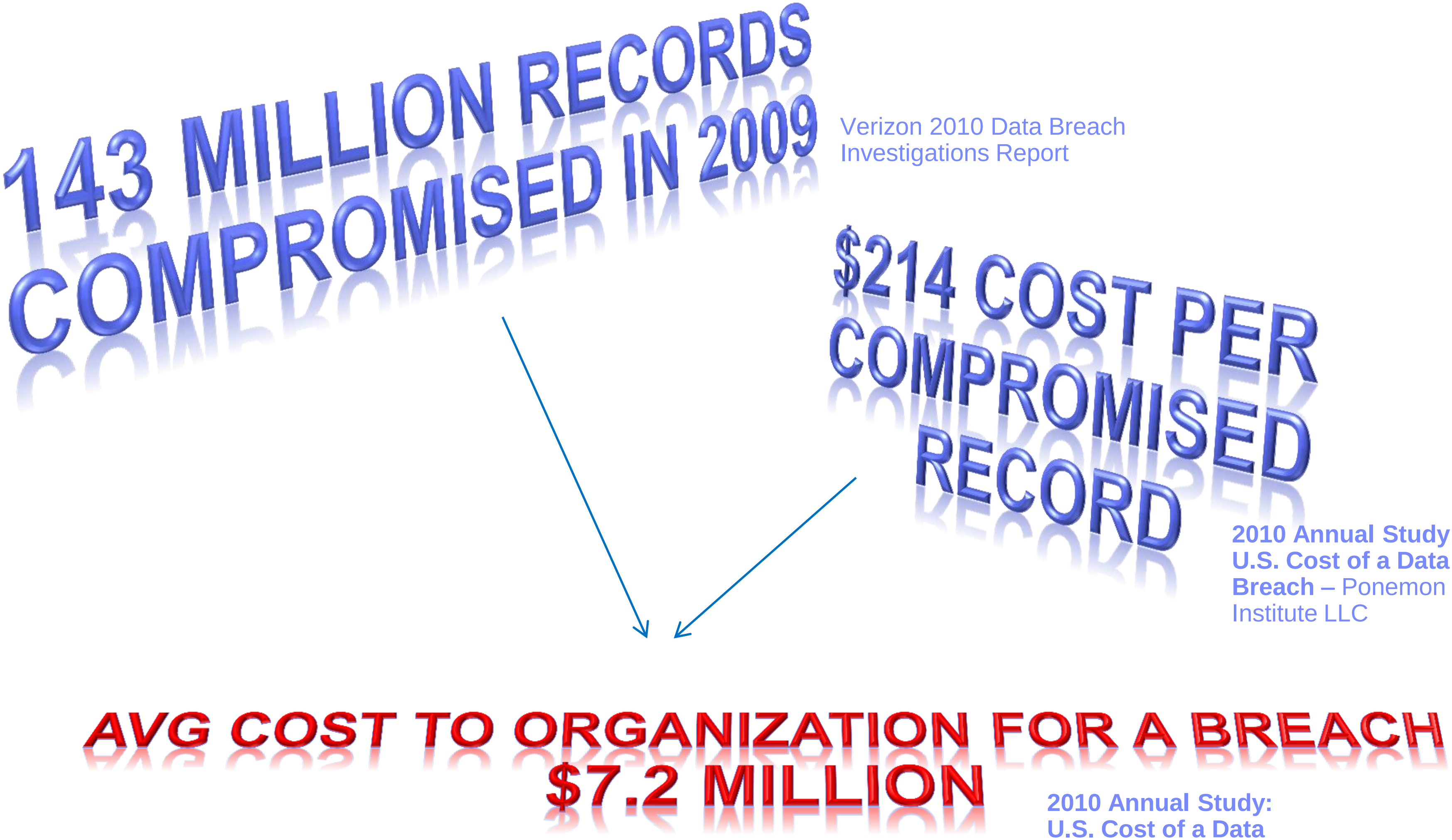
Globalization and Globally Available Resources

Access to streams of information in the Realtime

Billions of mobile devices accessing the Web

New Forms of Collaboration

The Costs from Security Breaches are Staggering



143 MILLION RECORDS COMPROMISED IN 2009

Verizon 2010 Data Breach Investigations Report

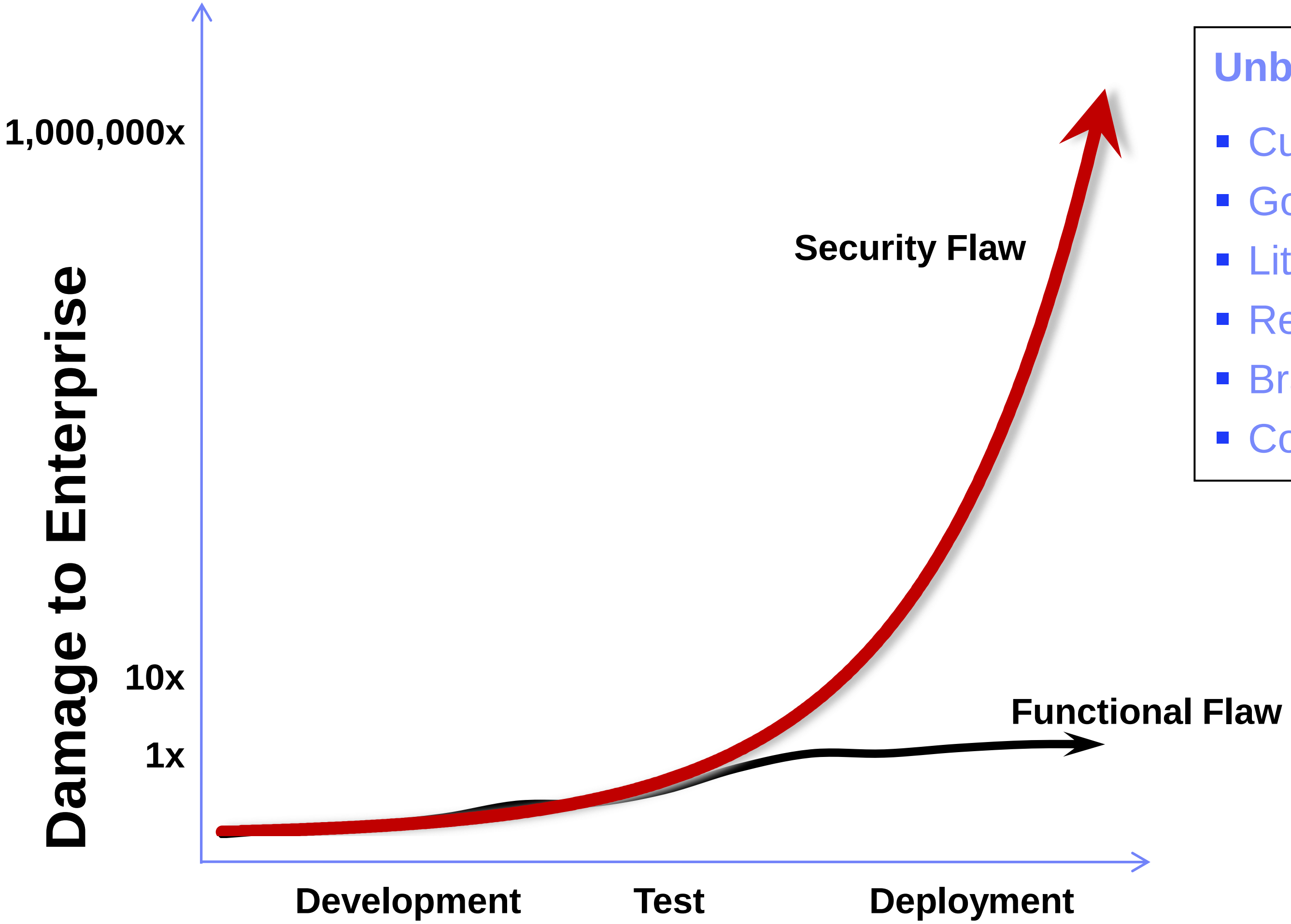
$214 COST PER COMPROMISED RECORD

2010 Annual Study: U.S. Cost of a Data Breach – Ponemon Institute LLC

AVG COST TO ORGANIZATION FOR A BREACH $7.2 MILLION

2010 Annual Study: U.S. Cost of a Data Breach – Ponemon Institute LLC

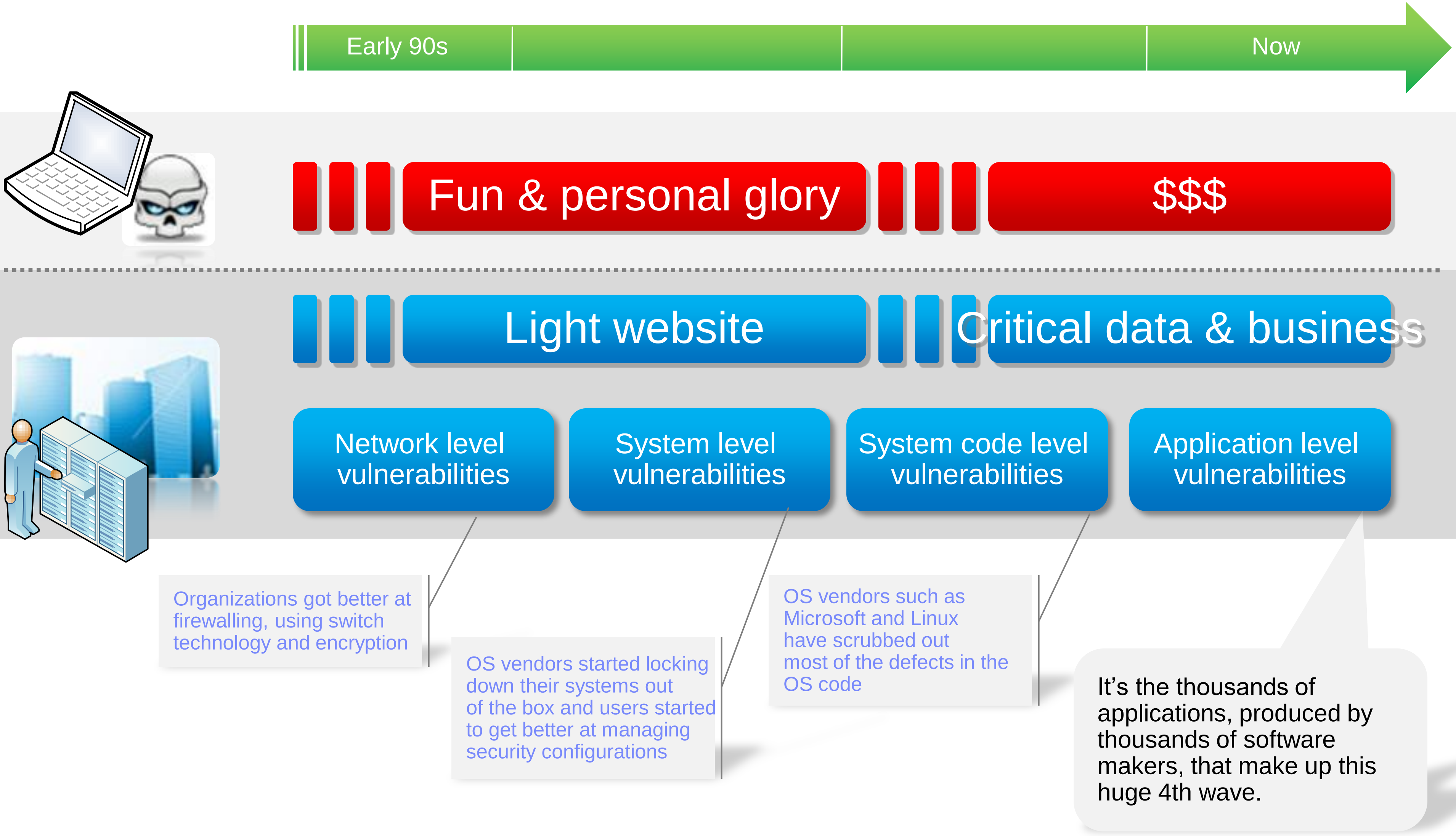
Sources of Security Breach Costs



Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

The Evolution of the Security Landscape



Early 90s

Now

Fun & personal glory

$$$

Light website

Critical data & business

Network level vulnerabilities

System level vulnerabilities

System code level vulnerabilities

Application level vulnerabilities

Organizations got better at firewalling, using switch technology and encryption

OS vendors started locking down their systems out of the box and users started to get better at managing security configurations

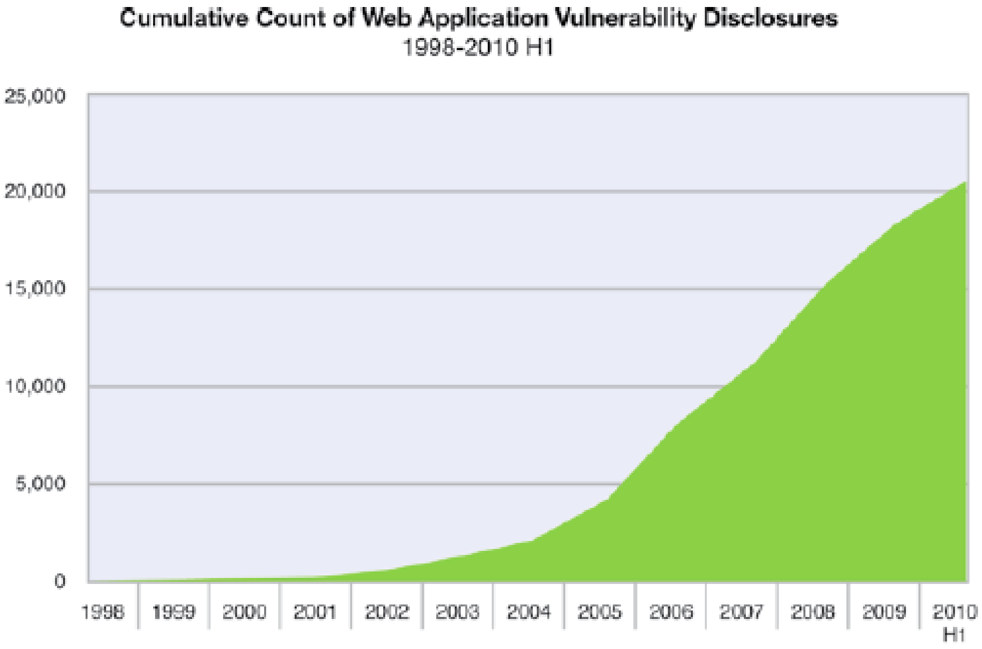
OS vendors such as Microsoft and Linux have scrubbed out most of the defects in the OS code

It’s the thousands of applications, produced by thousands of software makers, that make up this huge 4th wave.

Hackers Continue to Focus on Web Applications

… because they are easy points of entry and there is valuable of data exchanged in the business processes run by the applications

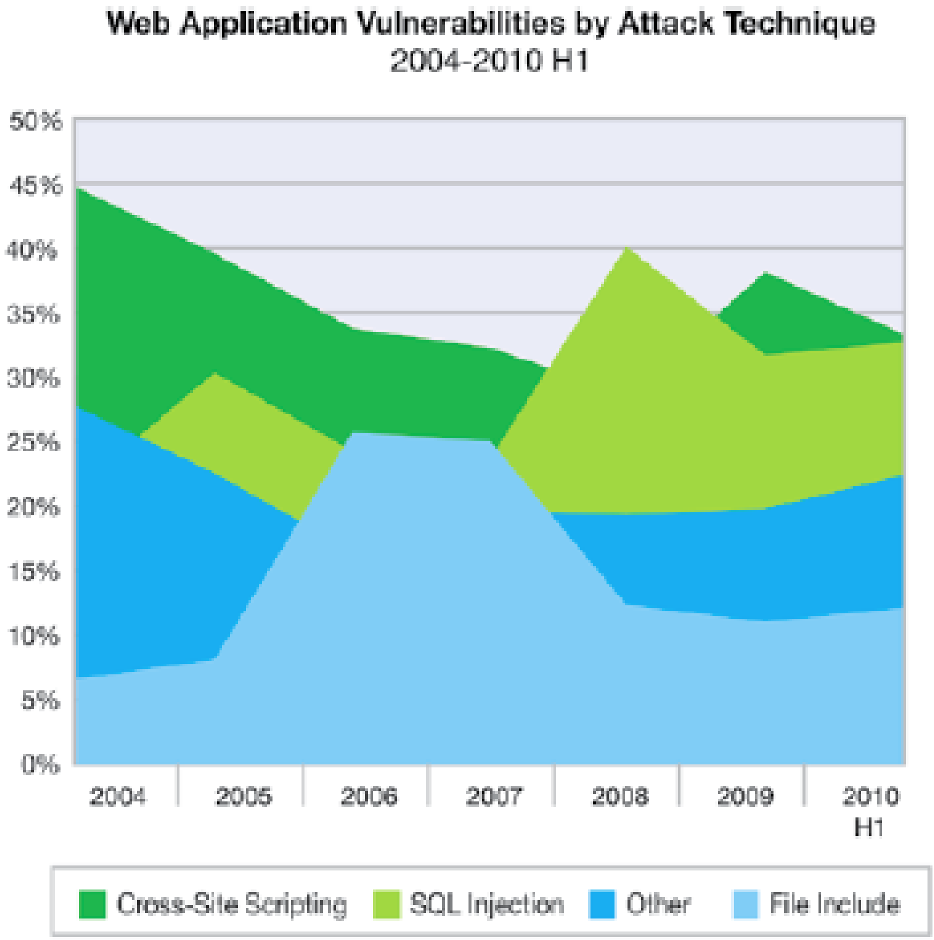
Web Application Vulnerabilities on the Rise



Source: 2010 IBM ISS X-Force Mid Year Report

Hackers Continue to Focus on Web Applications

Web Application Vulnerabilities on the Rise

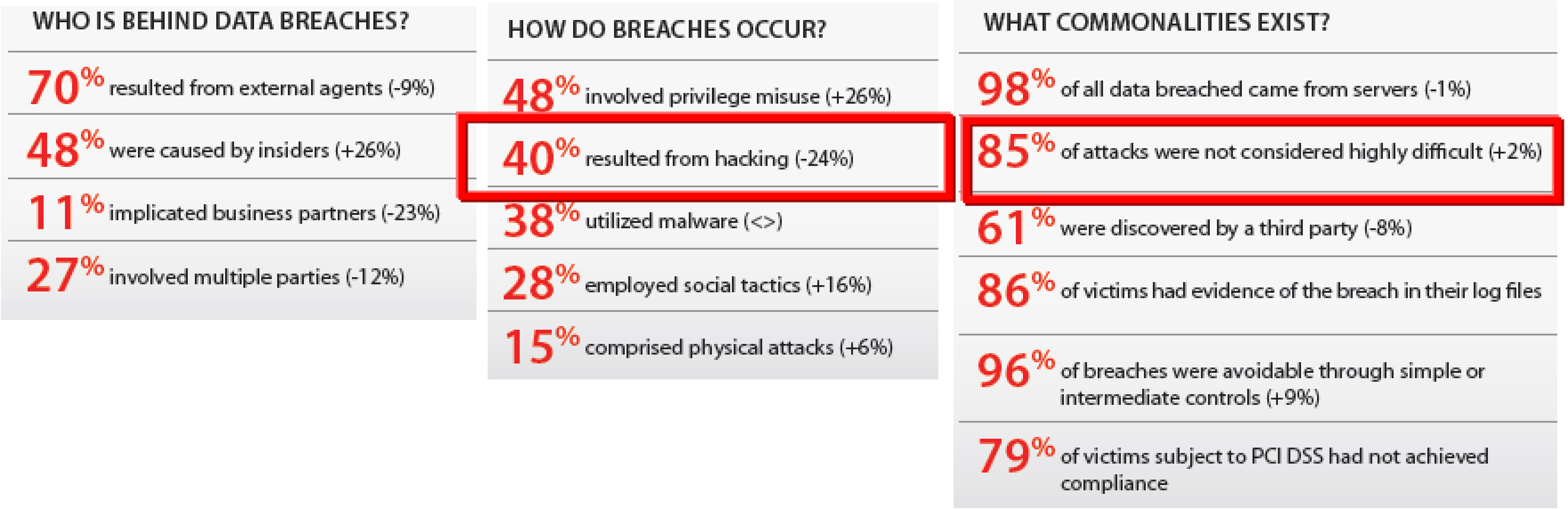


- Unfortunately, it appears that the volume of SQL injection disclosure is back up during the first half of 2010

•Over half (55 percent) of all vulnerabilities disclosed in the first half of 2010 have no vendor-supplied patch at the end of the period.

Source: 2010 IBM ISS X-Force Mid Year Report

2010 Breach Trends



WHO IS BEHIND DATA BREACHES?

70% resulted from external agents (-9%)

48% were caused by insiders (+26%)

11% implicated business partners (-23%)

27% involved multiple parties (-12%)

HOW DO BREACHES OCCUR?

48% involved privilege misuse (+26%)

40% resulted from hacking (-24%)

38% utilized malware (<>)

28% employed social tactics (+16%)

15% comprised physical attacks (+6%)

WHAT COMMONALITIES EXIST?

98% of all data breached came from servers (-1%)

85% of attacks were not considered highly difficult (+2%)

61% were discovered by a third party (-8%)

86% of victims had evidence of the breach in their log files

96% of breaches were avoidable through simple or intermediate controls (+9%)

79% of victims subject to PCI DSS had not achieved compliance

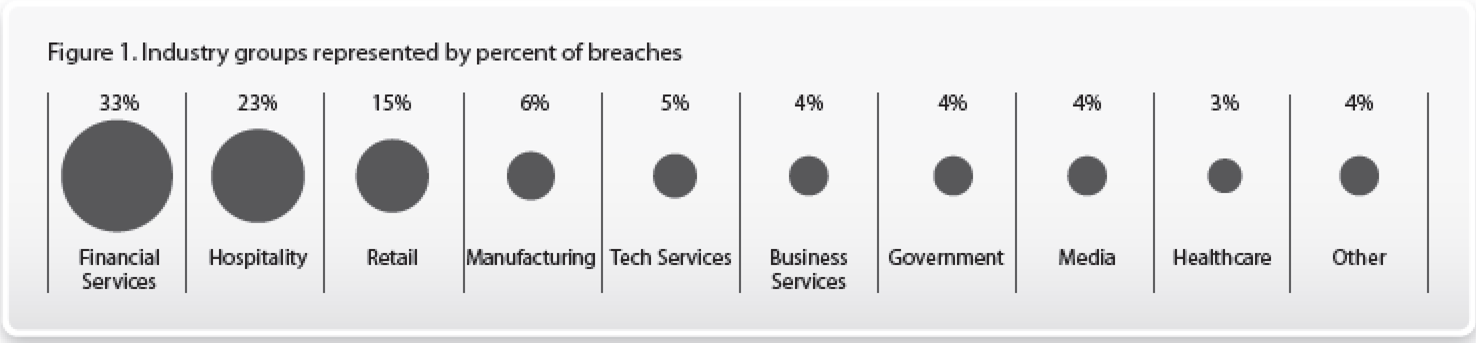
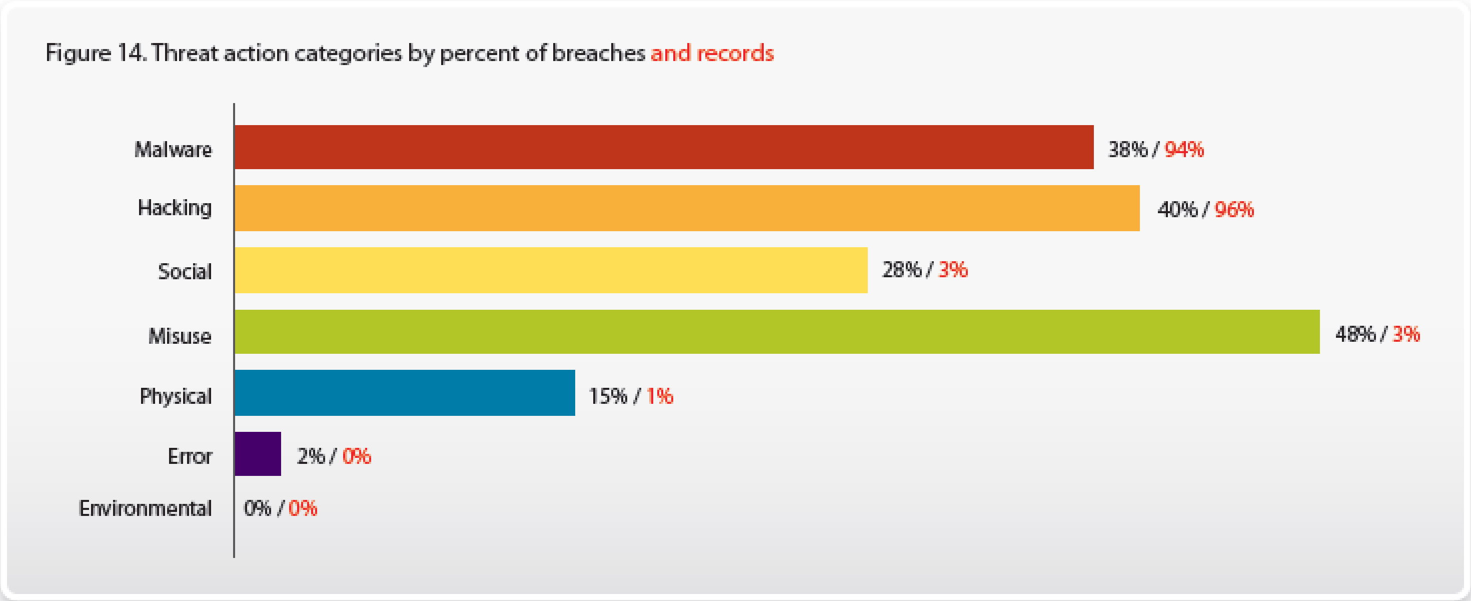


Figure 1. Industry groups represented by percent of breaches

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT

2010 Breach Trends



Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT

2010 Breach Trends

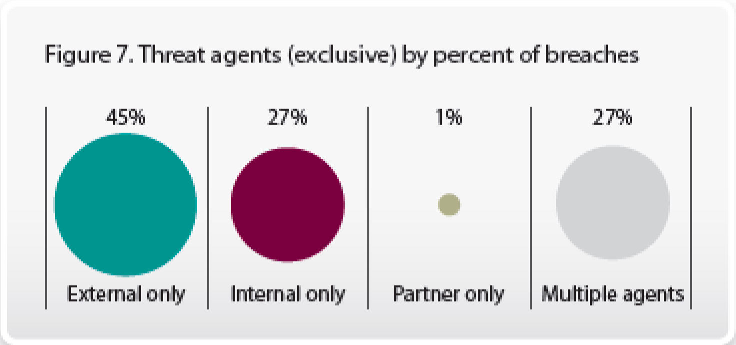


Figure 7. Threat agents (exclusive) by percent of breaches

Hacking (40% of breaches, 94% of records)

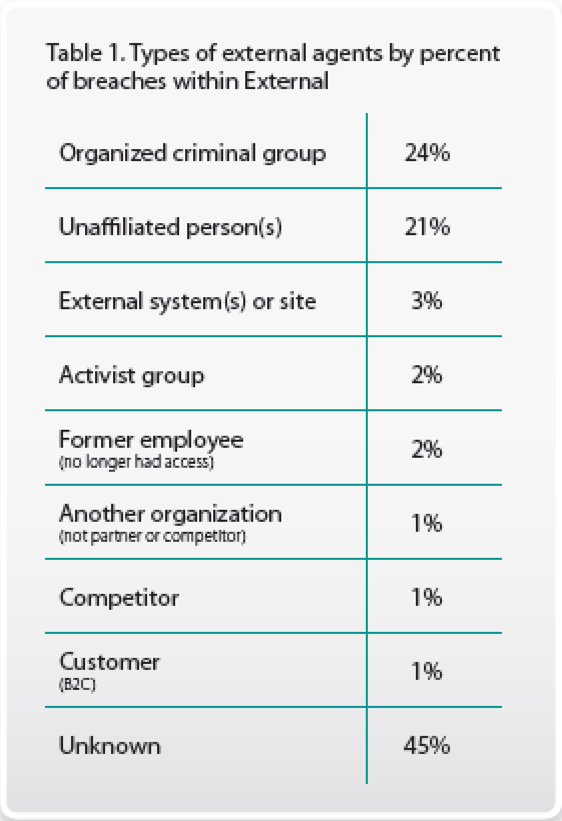


Table 1. Types of external agents by percent of breaches within External

Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT

2010 Breach Trends

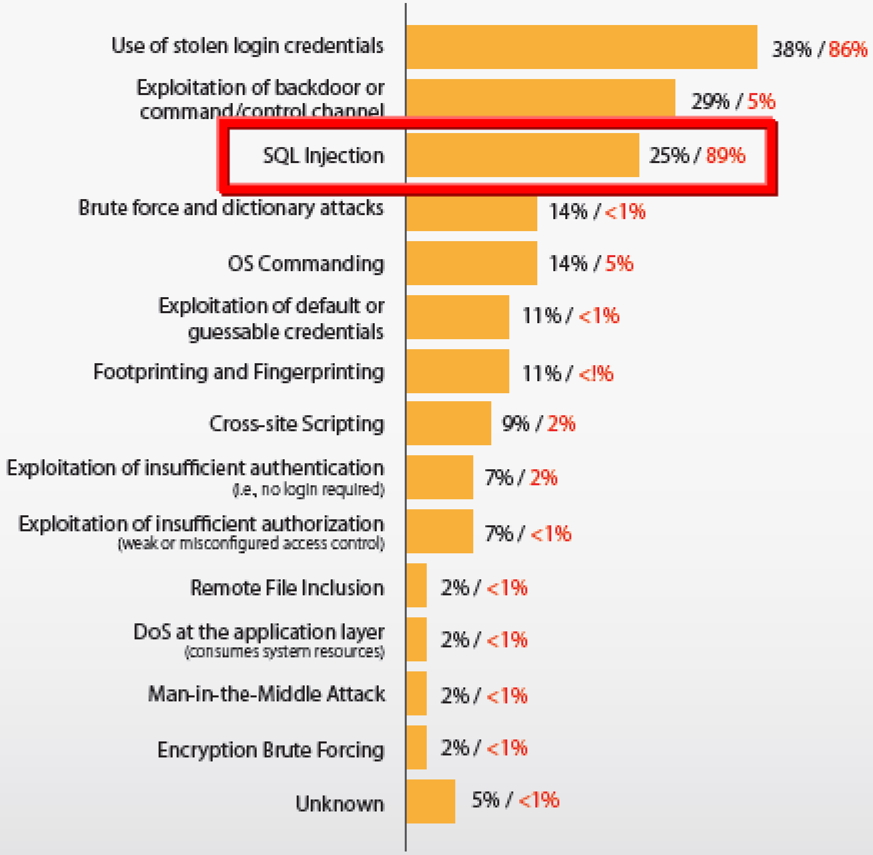
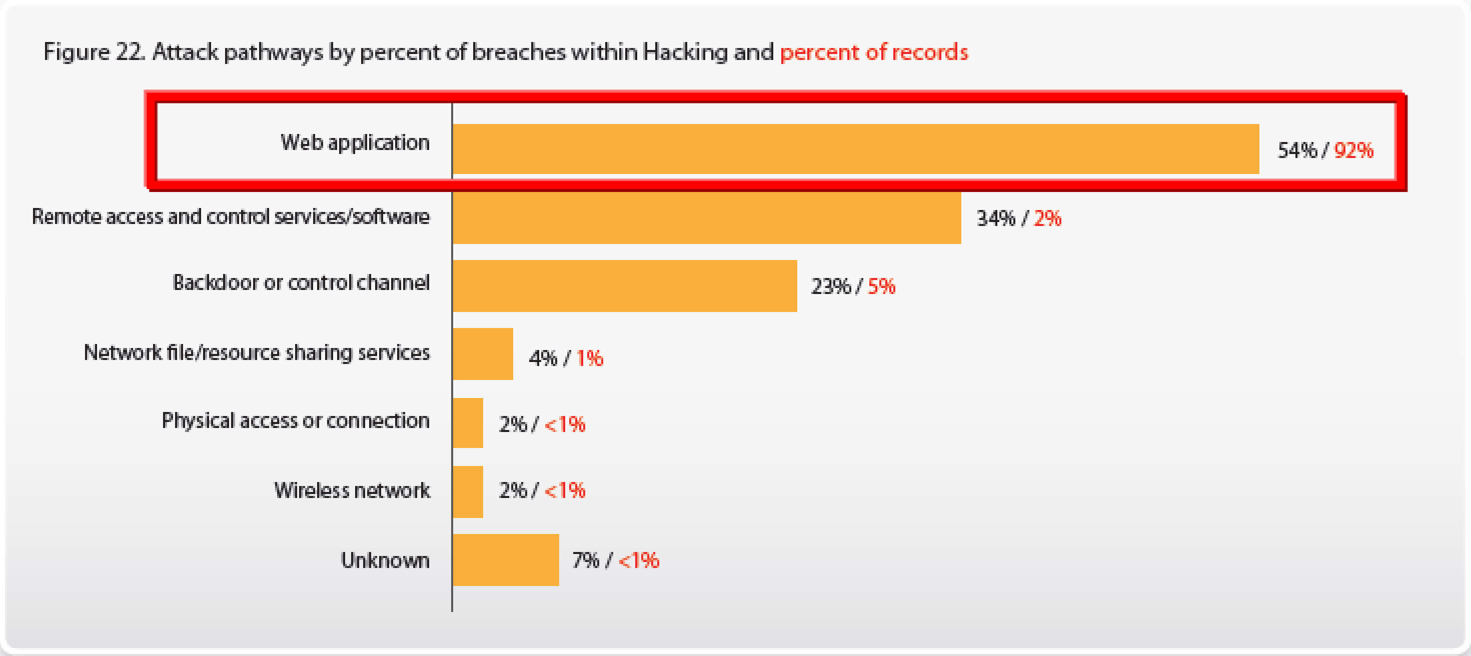


Figure 21. Types of hacking by percent of breaches within Hacking and percent of records

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT

2010 Breach Trends



Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT

Understanding the Web Application

Organization

Application Development

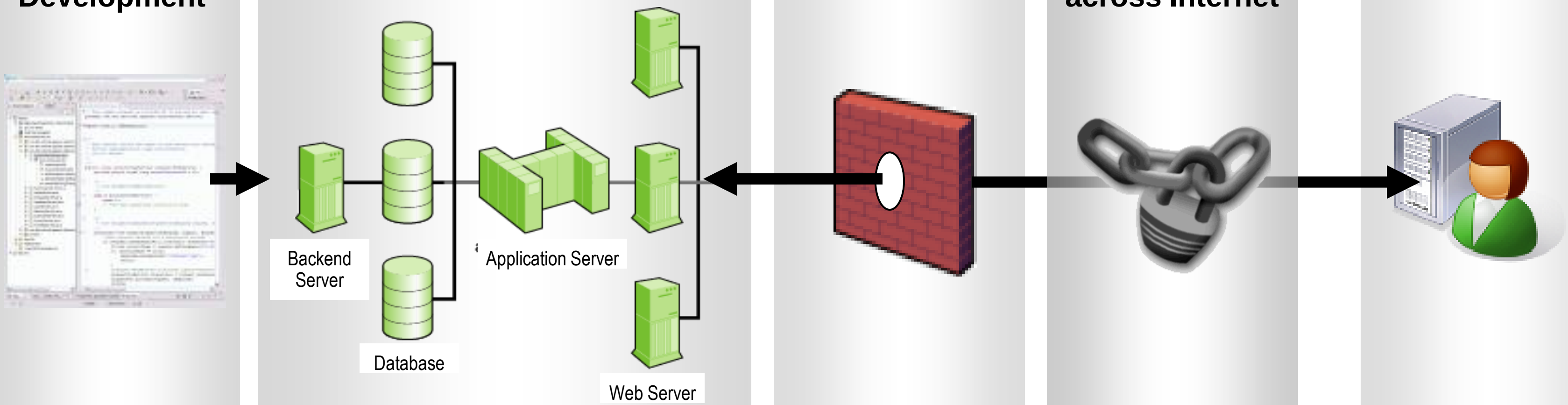
Secure Hosting Environment

Defend Network

Protect Data across Internet

Client

Desktop



Application Development

- **Requirements**
- **Secure Design**
- **Dynamic Analysis**
- **Static Analysis**

Secure Hosting Environment

- **Vulnerability management**
  - **Network**
  - **Host**
  - **Application**
- **Incident & event management**
- **Identity & access management**
- **Malware detection**

Defend Network

- **Firewall**
- **IDS / IPS**
- **Web App Firewall**
- **Anti-virus**

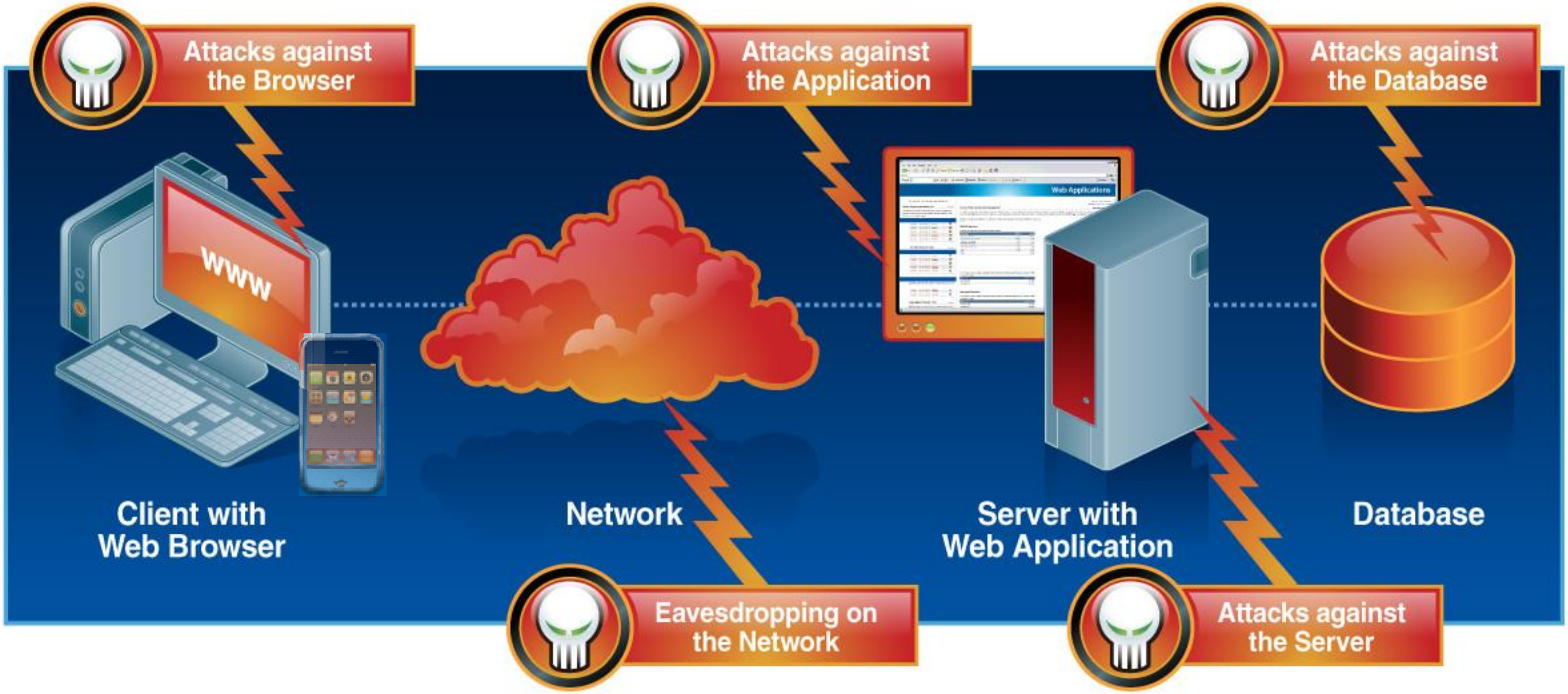
Protect Data across Internet

- **SSL Encryption**

Desktop

- **Anti-virus**
- **Anti-malware**
- **Personal firewall**

Attack Vectors


Attacks against the Browser
Attacks against the Application
Attacks against the Database
www
Web Applications
Client with Web Browser
Network
Server with Web Application
Database
Eavesdropping on the Network
Attacks against the Server

Why are Web Applications so Vulnerable?

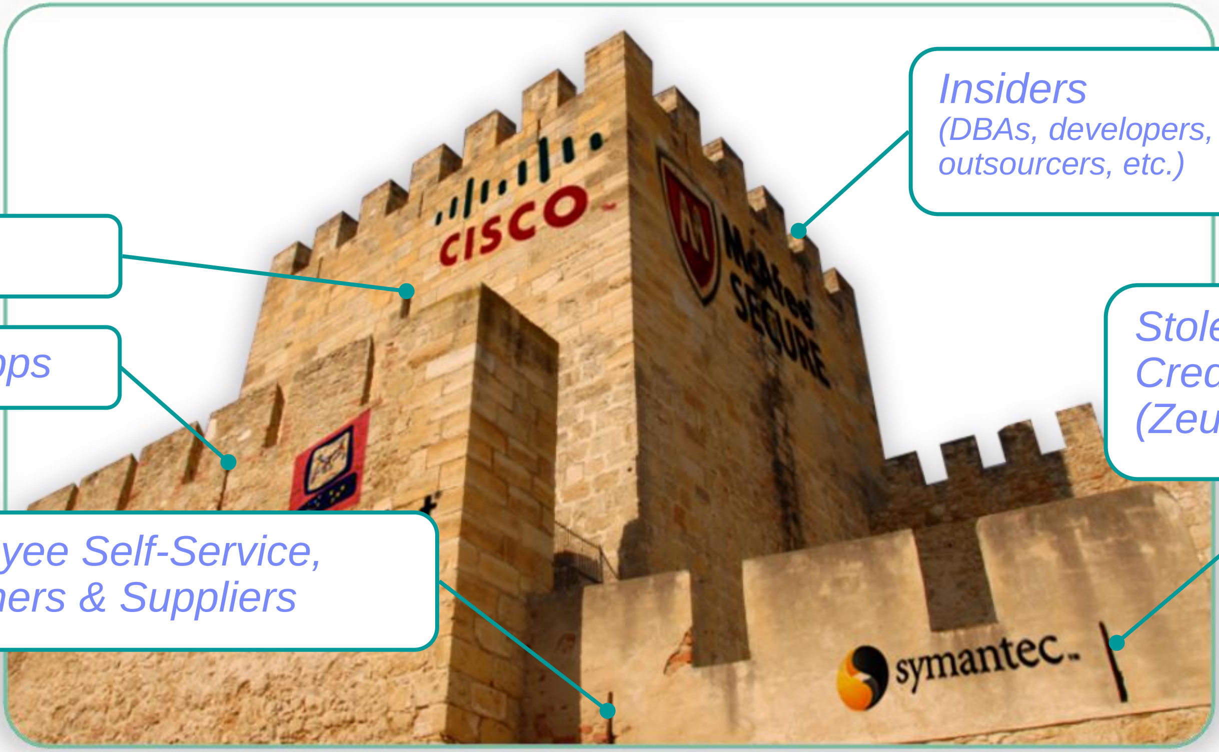
- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software for a Smarter Planet
- Network scanners won’t find application vulnerabilities and firewalls/IPS don’t block application attacks

Globalization and Globally Available Resources
Access to streams of information in the Realtime
INTERNET
facebook
myspace a place for friends
iTunes
Google
Billions of mobile devices accessing the Web
New Forms of Collaboration

Volumes of applications continue to be deployed that are riddled with security flaws…

…and are non compliant with industry regulations

Perimeter defenses no longer sufficient



Insiders
(DBAs, developers, outsourcers, etc.)

Outsourcing

Web-Facing Apps

Stolen Credentials (Zeus, etc.)

Employee Self-Service, Partners & Suppliers

> ***A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.***
>
> *-- William J. Lynn III, U.S. Deputy Defense Secretary*

Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information

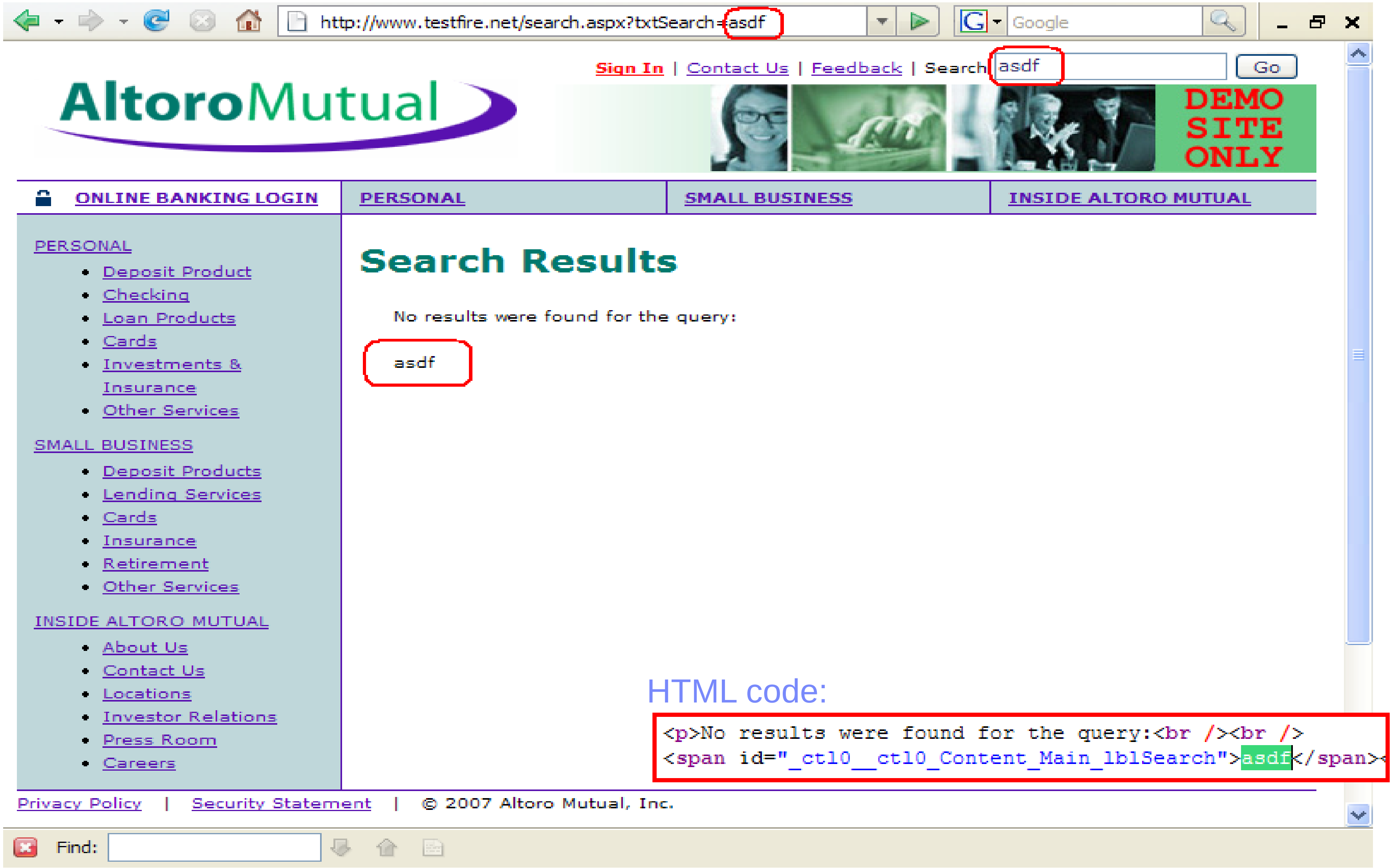
OWASP Top 10 Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, Browser control	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Execute shell commands on server, up to full control	Site modified to transfer all interactions to the hacker.
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Web application returns contents of sensitive file (instead of harmless one)
Cross-Site Request Forgery	Attacker can invoke "blind" actions on web applications, impersonating as a trusted user	Blind requests to bank account transfer money to hacker
Information Leakage and Improper Error Handling	Attackers can gain detailed system information	Malicious system reconnaissance may assist in developing further attacks
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly	Hacker can "force" session token on victim; session tokens can be stolen after logout
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted credentials "sniffed" and used by hacker to impersonate user
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access a page past the login page

www.owasp.org

Cross-Site Scripting (XSS)

- What is it?
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context
- What are the implications?
  - Session Tokens stolen (browser security circumvented)
  - Complete page content compromised
  - Future pages in browser compromised

XSS Demonstration



Search Results

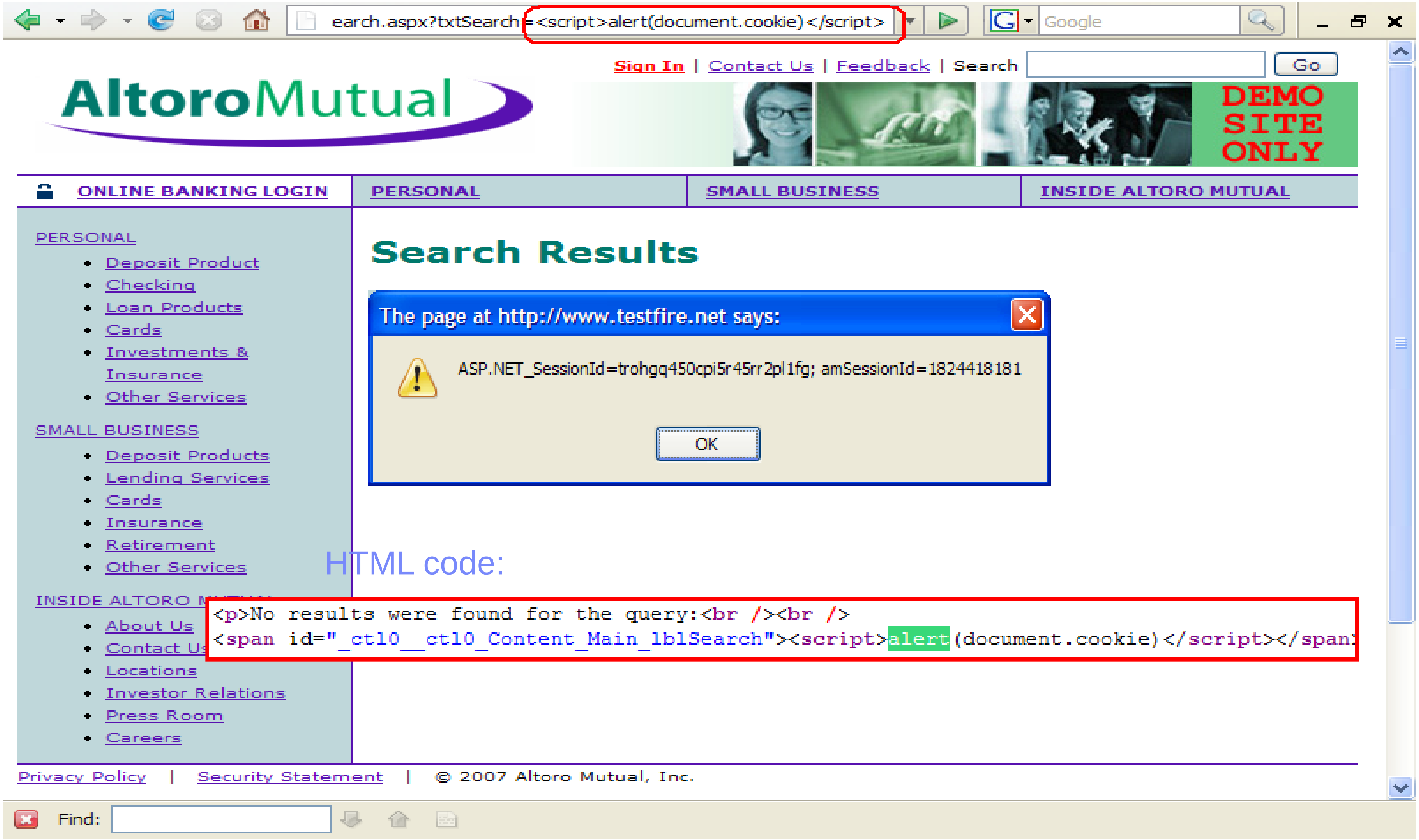
No results were found for the query:

asdf

HTML code:

```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch">asdf</span><
```

XSS Demonstration



Search Results

The page at http://www.testfire.net says:

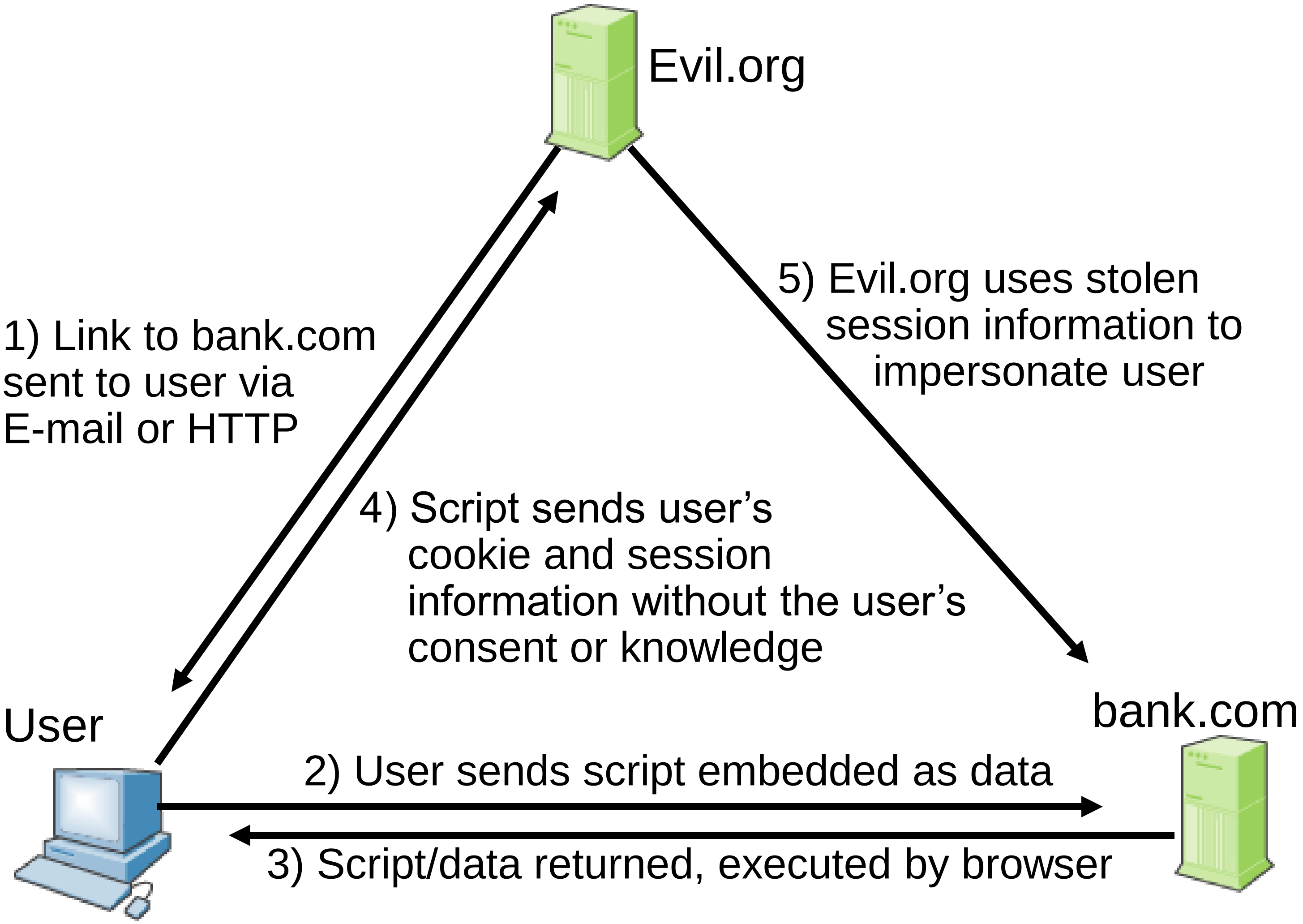
ASP.NET_SessionId=trohgq450cpi5r45rr2pl1fg; amSessionId=1824418181

OK

HTML code:

```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch"><script>alert(document.cookie)</script></span
```

Cross Site Scripting – The Exploit Process



Evil.org

1) Link to bank.com sent to user via E-mail or HTTP

5) Evil.org uses stolen session information to impersonate user

4) Script sends user's cookie and session information without the user's consent or knowledge

User

bank.com

2) User sends script embedded as data

3) Script/data returned, executed by browser

Injection Flaws

- What is it?
  - – User-supplied data is sent to an interpreter as part of a command, query or data.

- What are the implications?
  - – SQL Injection – Access/modify data in DB
  - – XPath Injection – Access/modify data in XML format
  - – SSI Injection – Execute commands on server and access sensitive data
  - – LDAP Injection – Bypass authentication
  - – MX Injection – Use mail server as a spam machine
  - – HTTP Injection – Modify or poison web caches
  - – Etc.

SQL Injection Illustrated

Account: 876398' or '1'='1

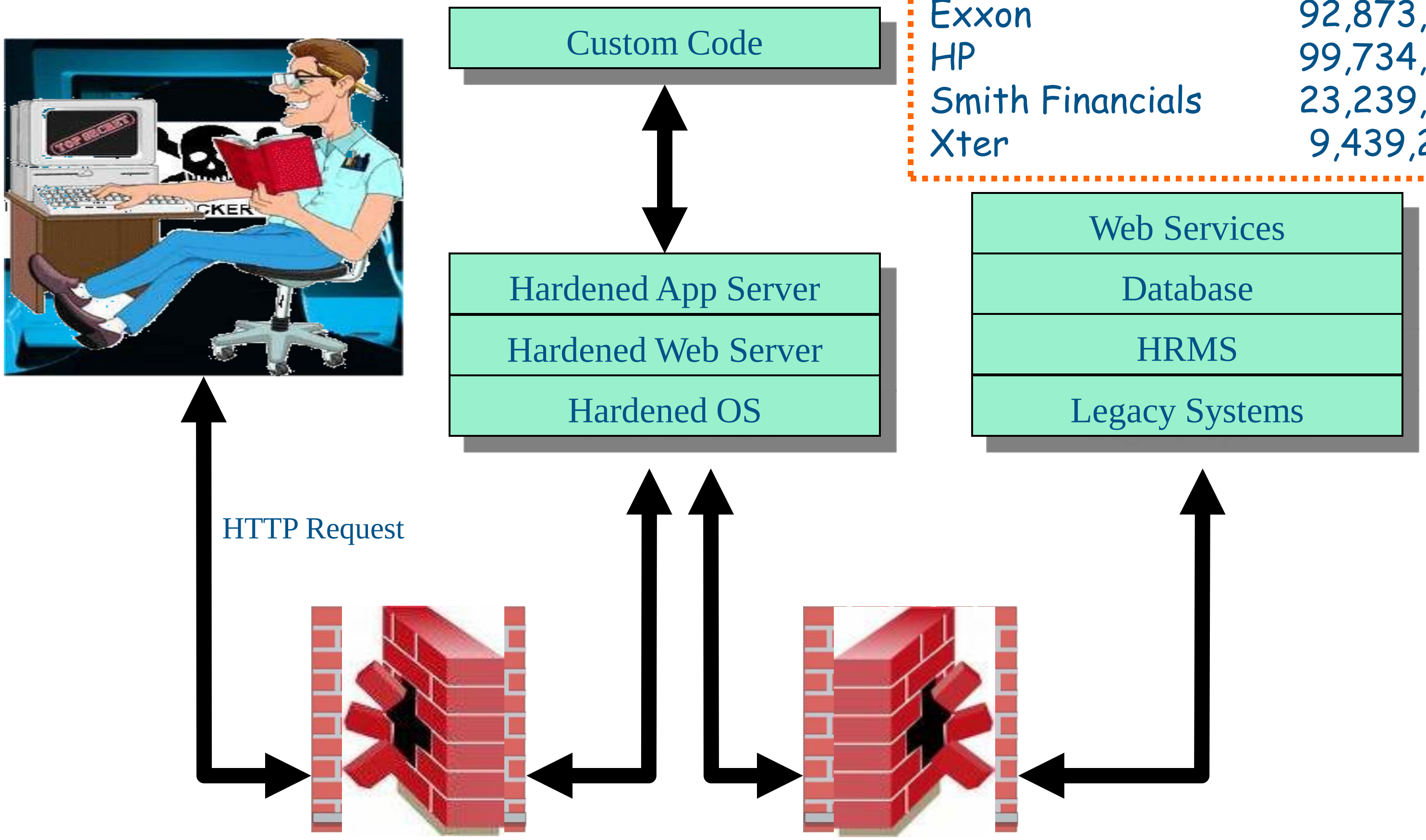
All records are returned

Account: 876398' or '1' = '1

Account: 876398' or '1' = '1

Select * from Account where acct = '876398' or '1' = '1'

Name:	Balance
ACME Bank	21,234,345
Exxon	92,873,739
HP	99,734,123
Smith Financials	23,239,329
Xter	9,439,231



Intrusion detection, firewalls, and hardened OS's won't
detect or prevent most application attacks

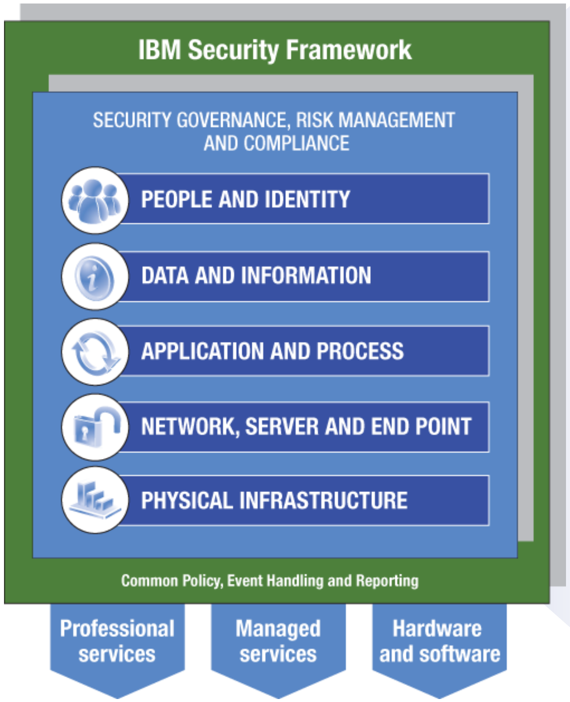
Night Dragon

- Successful attacks on 5+ global oil & gas co's
- Attacks began with SQL-injection, which compromised external web servers
  - Common hacking tools were then used to access intranets, giving attackers access to internal servers and desktops
  - Usernames and passwords were then harvested and after disabling Internet Explorer proxy settings
  - Hackers were able to establish direct communication from infected machines to the Internet.

Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information

The Framework identifies five security focus areas as starting points



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

Click ⓘ for more information

IBM Security portfolio can help you meet challenges in each security focus area

Framework	Challenges	
PEOPLE AND IDENTITY	▪ Manage identities ▪ Control access to applications	▪ Audit, report and manage access to resources
DATA AND INFORMATION	▪ Protect Critical Databases ▪ Messaging Security and Content Filtering	▪ Monitor & manage data access ▪ Prevent Data Loss ▪ Encryption
APPLICATION AND PROCESS	▪ Ensure Security in App Development ▪ Discover App Vulnerabilities	▪ Embed App Access Controls ▪ Provide SOA Security
NETWORK, SERVERS & ENDPOINTS	▪ Protect Servers, Endpoints, Networks, Mainframes	
PHYSICAL INFRASTRUCTURE	▪ Video Surveillance ▪ Command and Control	▪ Video Analytics

Click ℹ for more information

Protect your most valuable information

Continuously monitor access to high-value databases to:

1. Prevent data breaches

Mitigate external and internal threats

2. Ensure the integrity of sensitive data

Prevent unauthorized changes to sensitive data or structures

3. Reduce cost of compliance

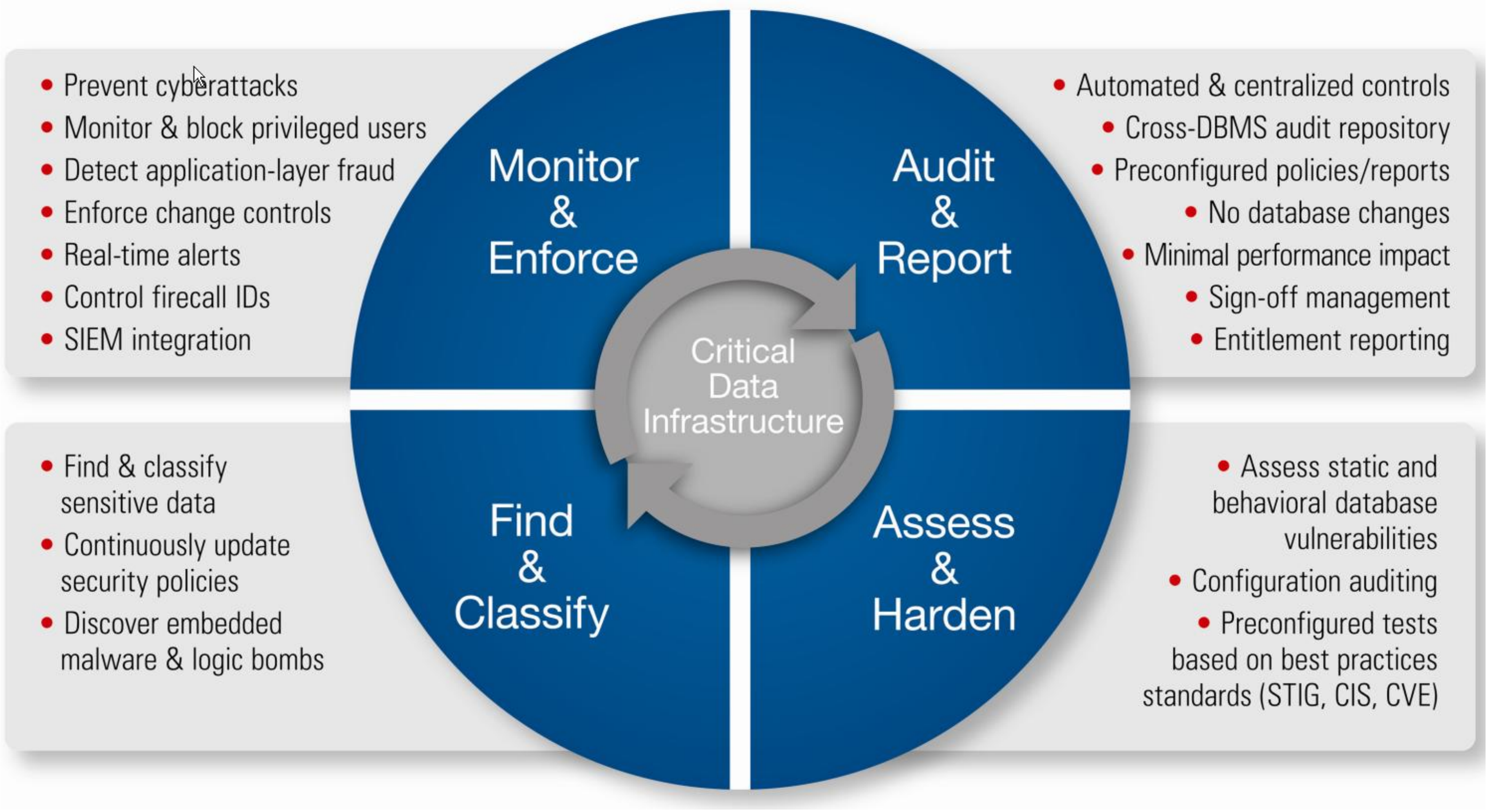
Automate and centralize controls

1. Across PCI DSS, data privacy regulations, HIPAA/HITECH, …
2. Across databases and applications

Simplify processes

92% of all breached records originate in database servers *(2010 Data Breach Report)*

Addressing the full database security lifecycle



- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

Monitor & Enforce

Audit & Report

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

Critical Data Infrastructure

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

Find & Classify

Assess & Harden

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

Thank
You

Trademarks and notes

IBM Corporation 2010

- IBM, the IBM logo, ibm.com, AppScan, DataPower, Rational, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), these symbols indicate 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 "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
- Other company, product and service names may be trademarks or service marks of others.
- References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.