Application Security

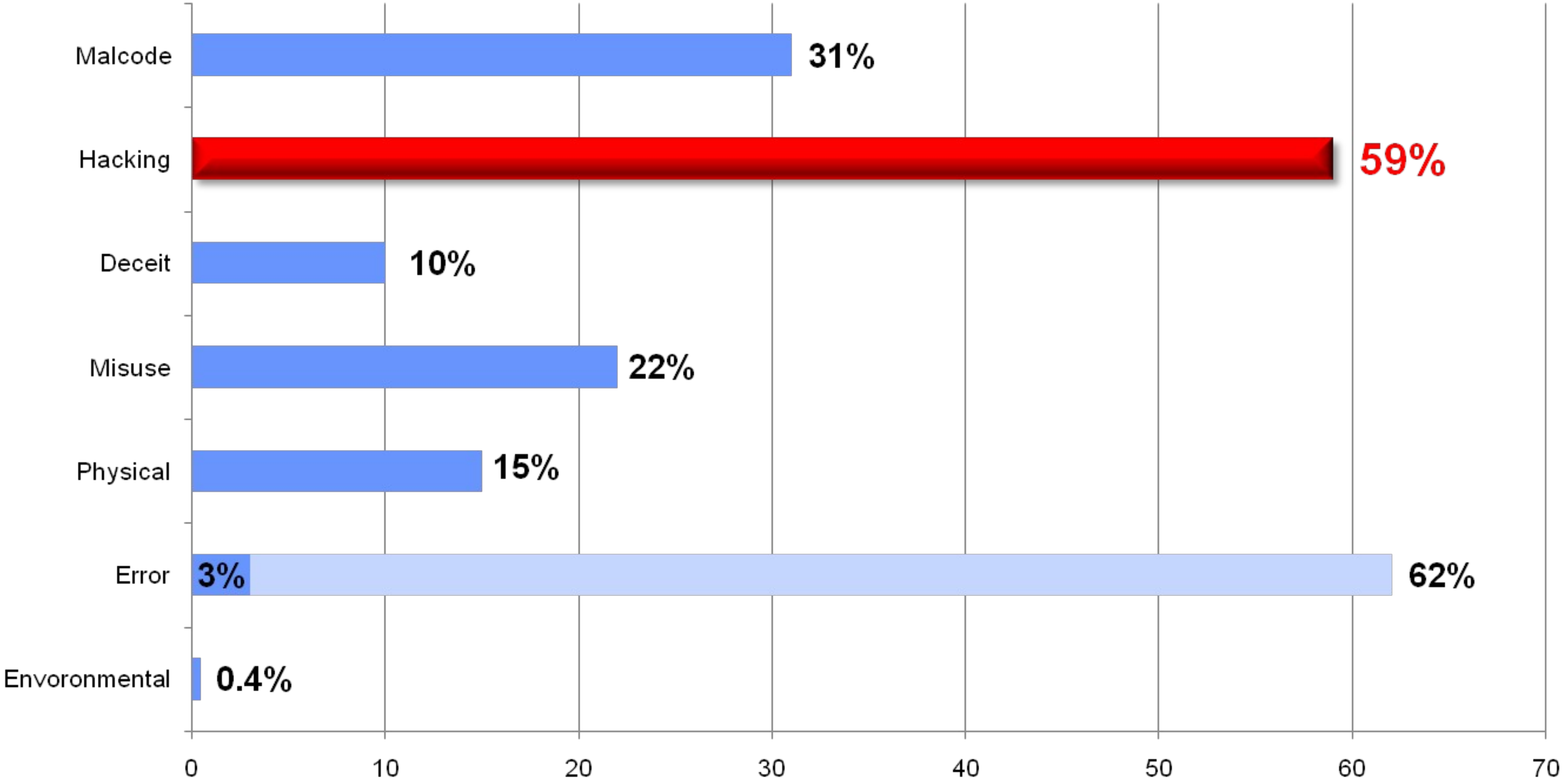
Doug Ashbaugh CISSP, CISA, CSSLP

It security

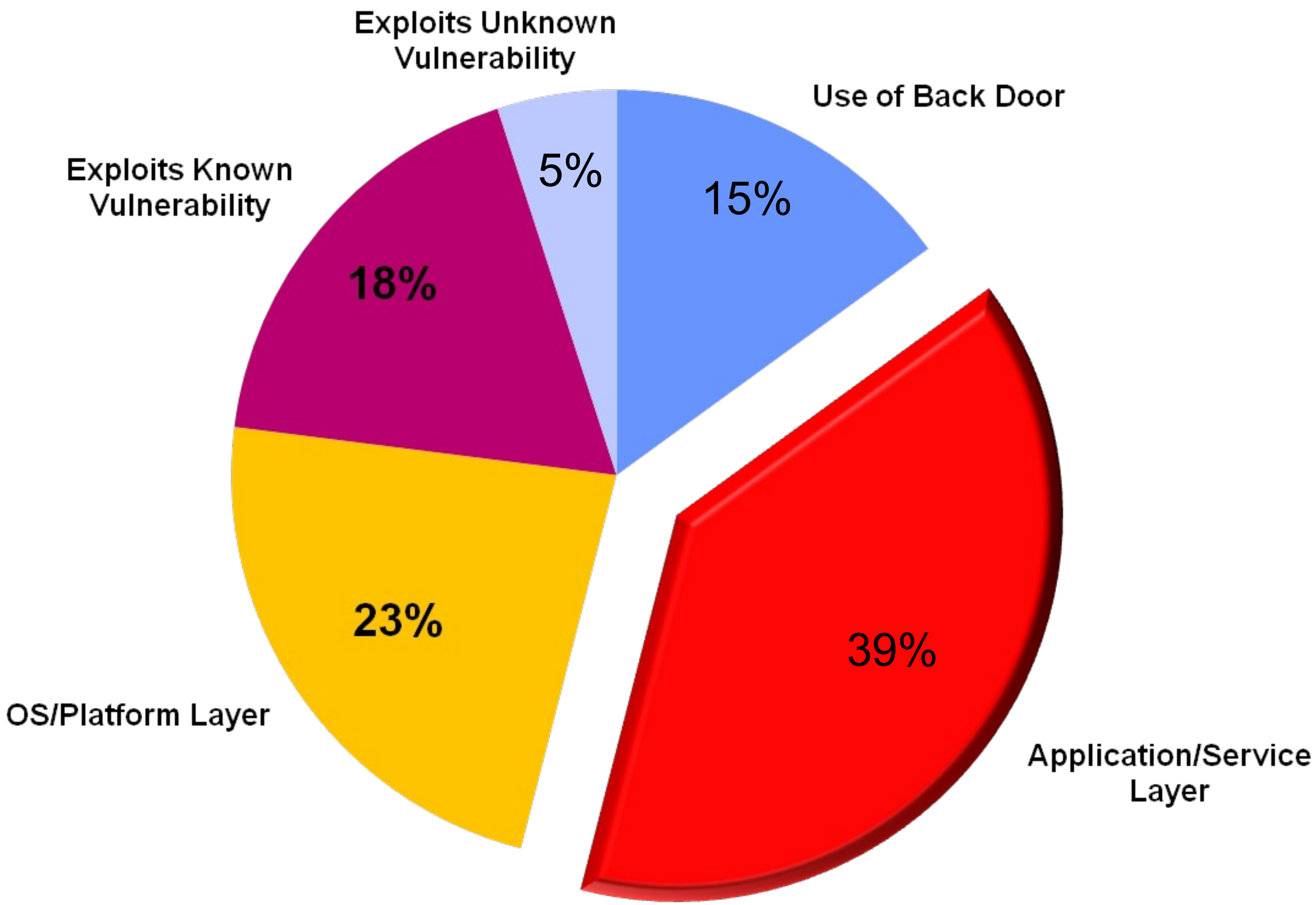
262,442,156

Records Lost Since Jan 2005

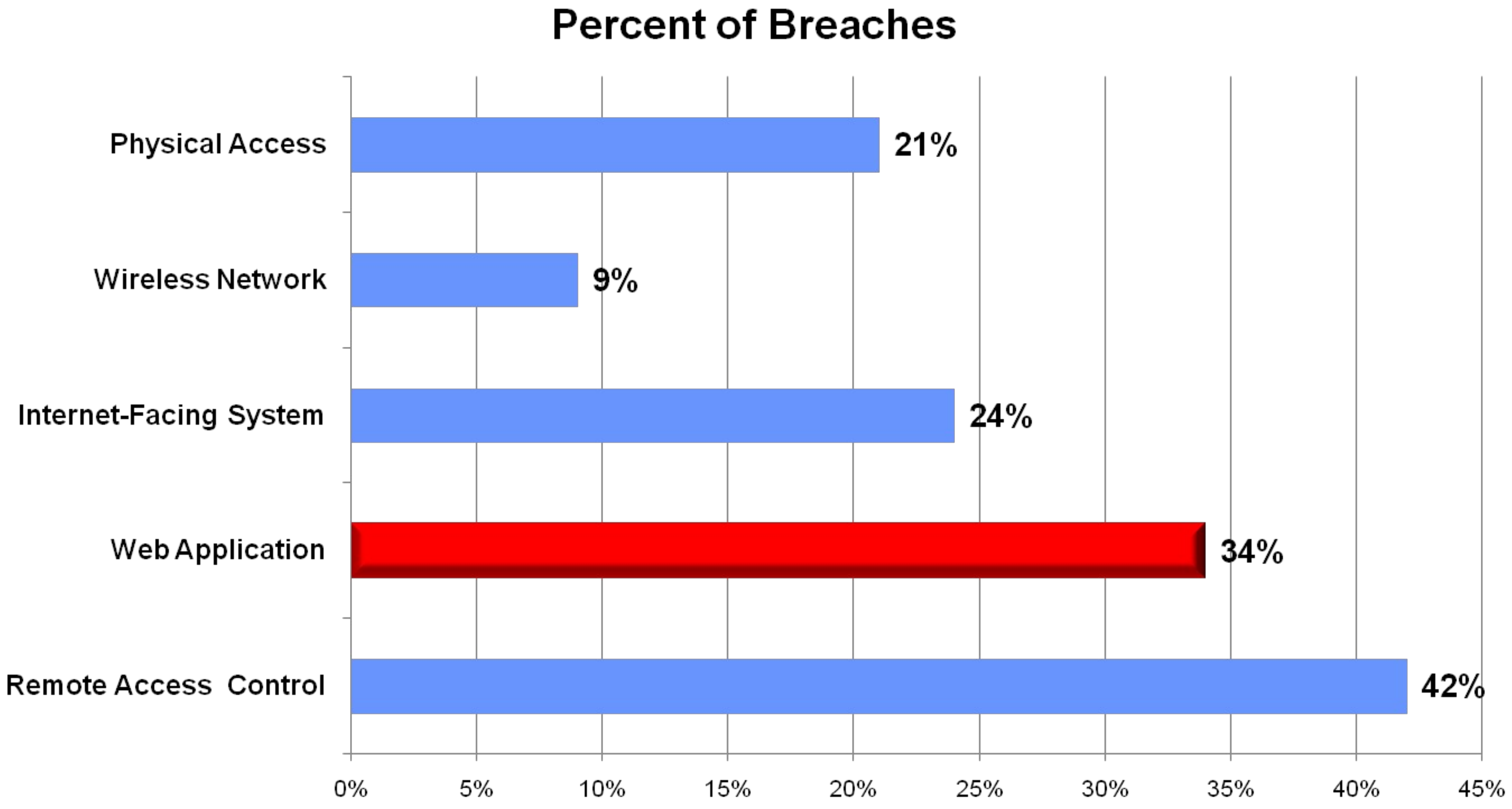
Percent of Breaches



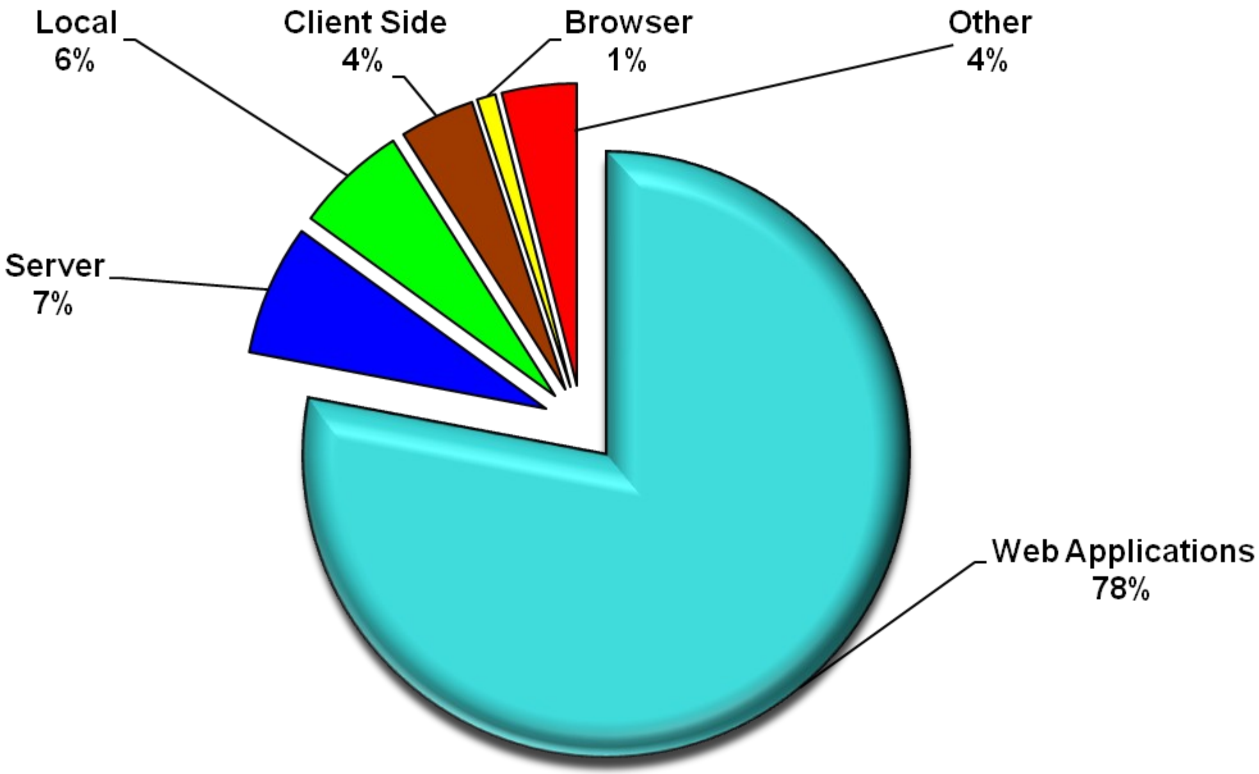
Hacking


Exploits Unknown Vulnerability
5%
Use of Back Door
15%
Exploits Known Vulnerability
18%
23%
OS/Platform Layer
39%
Application/Service Layer

Common Attack Pathways



Vulnerabilities /Weaknesses



Headlines

…software error exposes limited amount of personal information…

- Feb 23, 2009

…experienced a vulnerability on their website that compromised personal information…

- Feb 2, 2009

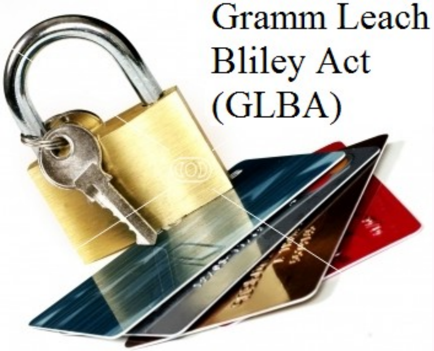
Banks warn customers as debit card processor acknowledges breach… “Larger than TJX?”

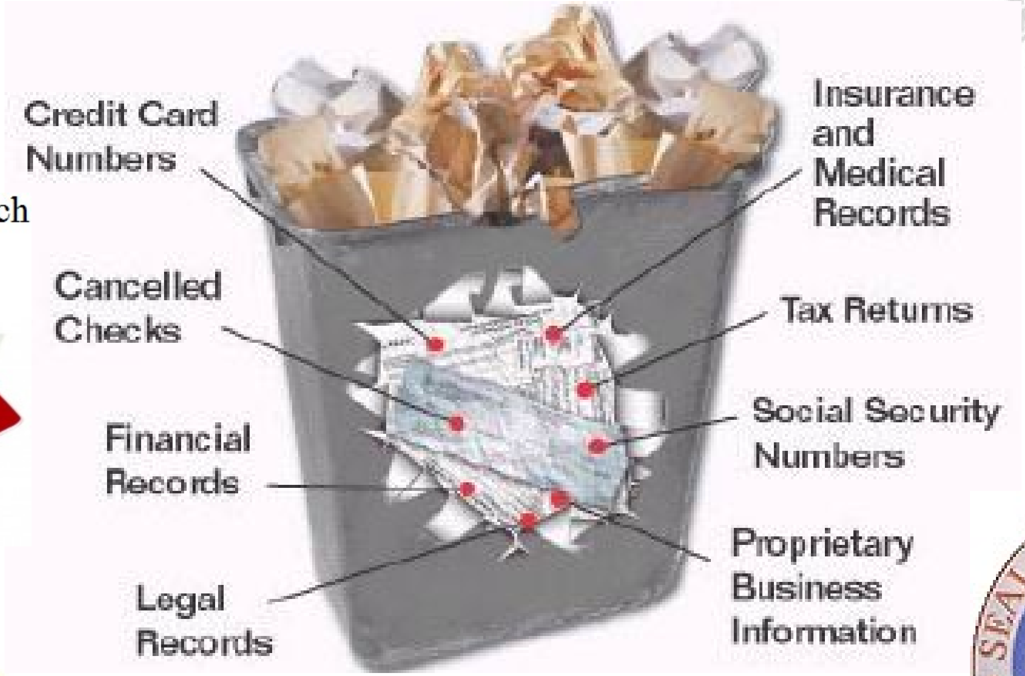
- Jan 20, 2009

LEGISLATION

HIPAA

Gramm Leach
Bliley Act
(GLBA)





Sarbanes
Oxley

PCi Security Standards Council ™
PARTICIPATING ORGANIZATION

NAIC
National Association of
Insurance Commissioners

SEAL OF THE SENATE OF THE STATE OF CALIFORNIA
LEGIS

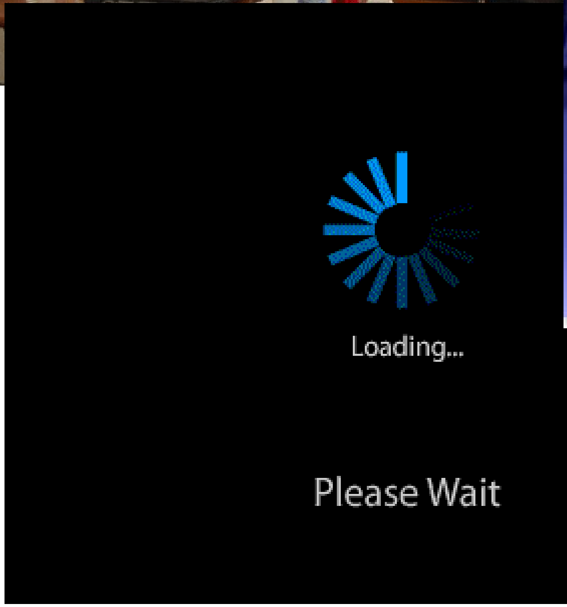
SB-1386

Cost / Customer Confidence

- $202.00 = Average cost of each record lost
- $268,000.00 = Average cost to inform customers
- $1,800,000.00 = Average annual cost to businesses suffering a major data breach
- $10,000,000.00 = Paid by Choice Point in Settlement
- $40,700,000.00 = Paid by TJX and Visa in Settlement
- A breach that exposes 46,000 identities will cost an organization $7.6 million on average
- Customer Confidence
  - 73% of consumers avoid online banking
  - 54% of consumers have curtailed online shopping
  - Higher privacy trust scores lead to higher revenues and marketing responses

Mainframe

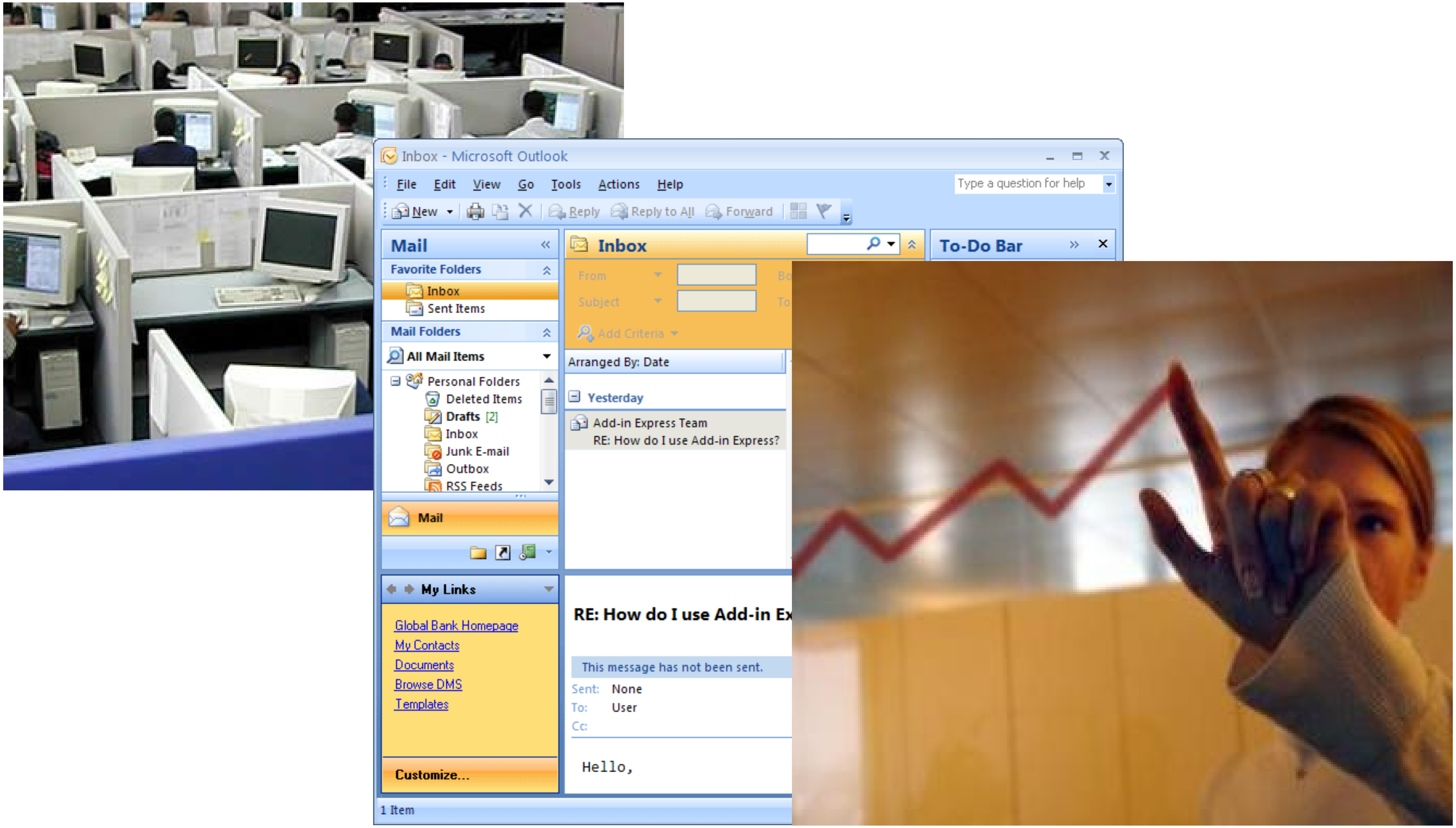
Client server



Loading...

Please Wait

Enterprise resource planning



Add-in Express Team
RE: How do I use Add-in Express?

RE: How do I use Add-in Ex

This message has not been sent.

Sent: None
To: User
Cc:

Hello,

World wide web

37,342

Known vulnerabilities in software

- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to restrict URL Access

Persistency

```
if (!(png_ptr->mode & PNG_HAVE_PLTE)) {
        /* Should be an error, but we can cope with it */
        png_warning(png_ptr, "Missing PLTE before tRNS");}
else if (length > (png_uint_32)png_ptr->num_palette) {
        png_warning(png_ptr, "Incorrect tRNS chunk length");
        png_crc_finish(png_ptr, length);
        return;}
...
png_crc_read(png_ptr, readbuf, (png_size_t)length);
```

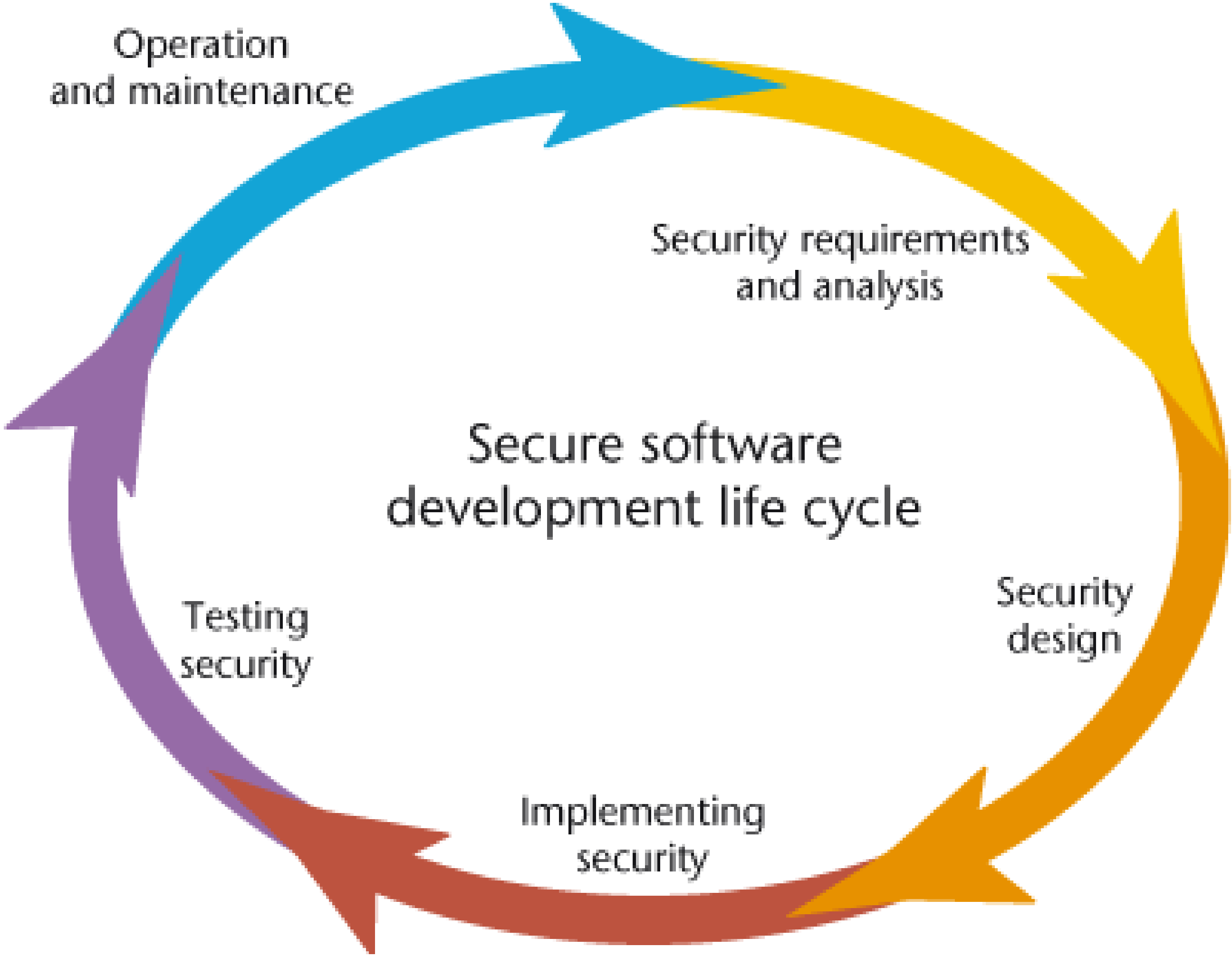
Top 5 Strategies

Find and Prioritize Websites

Find and Fix Website Vulnerabilities

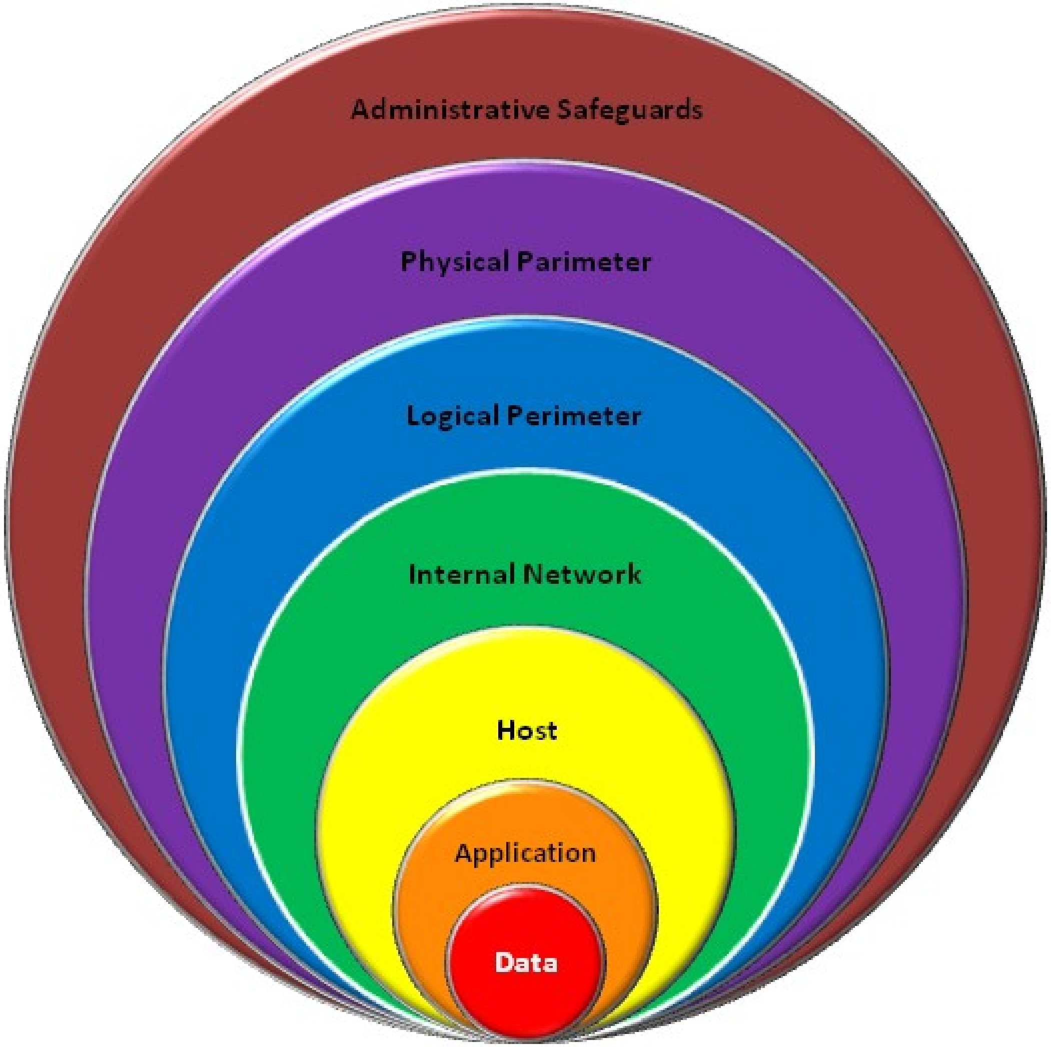
Remediate Vulnerabilities

Implement a secure SDLC

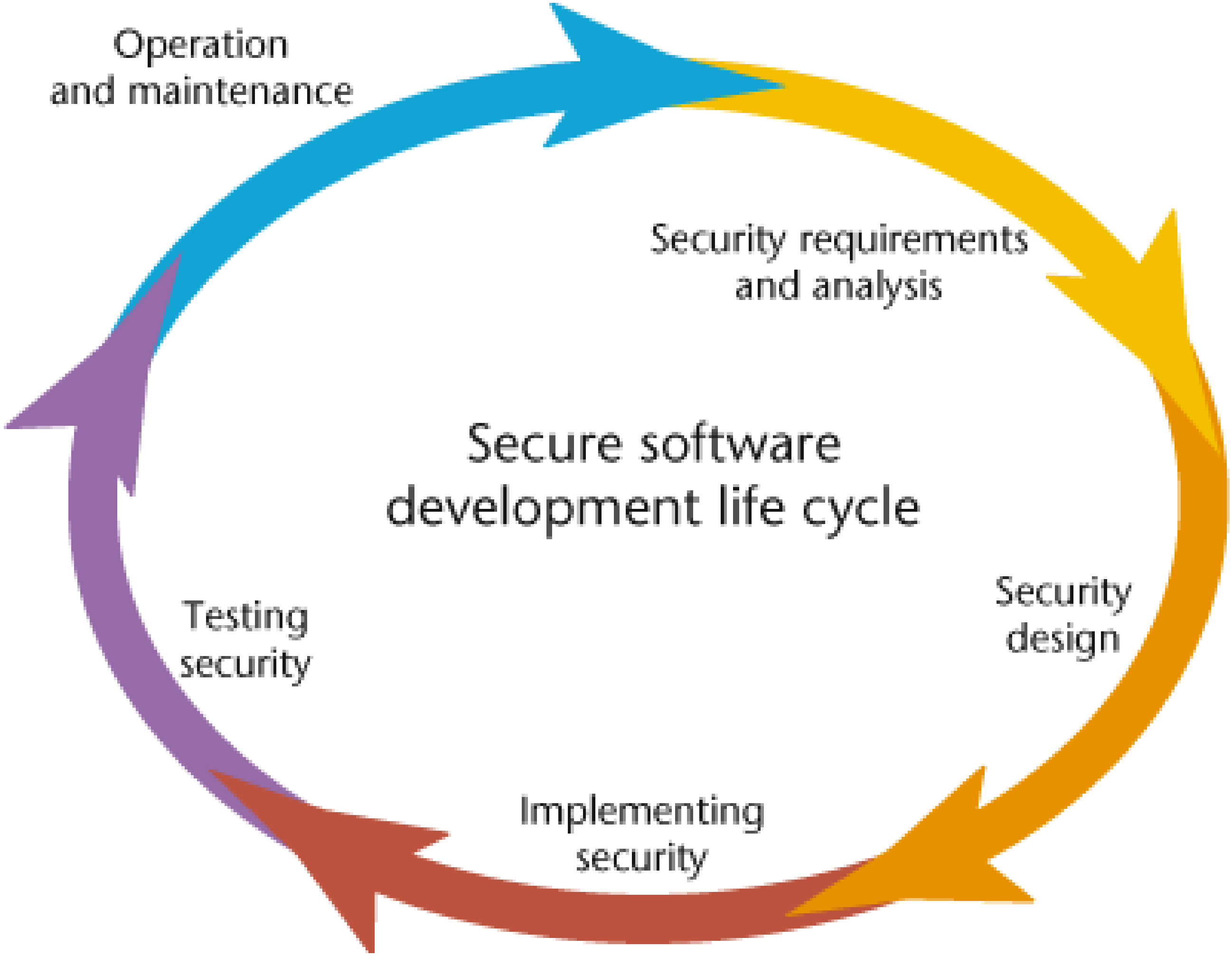


Operation and maintenance
Security requirements and analysis
Secure software development life cycle
Security design
Implementing security
Testing security

Defense in Depth



Securing the SDLC



Requirements Phase

Make Security Requirements Explicit

Perform Threat Modeling when doing Use Case analysis

How the customer explained it

Design Phase

Centralize security-critical functions into subsystems

Explicitly define "trust" relationships between subsystems

Evaluate the use of cryptography

How the Analyst designed it

Development Phase

Perform code reviews with security in mind

Integrate verification of security measures into unit testing

How the Programmer wrote it

Testing Phase

Use automated application scanners to test major functional areas

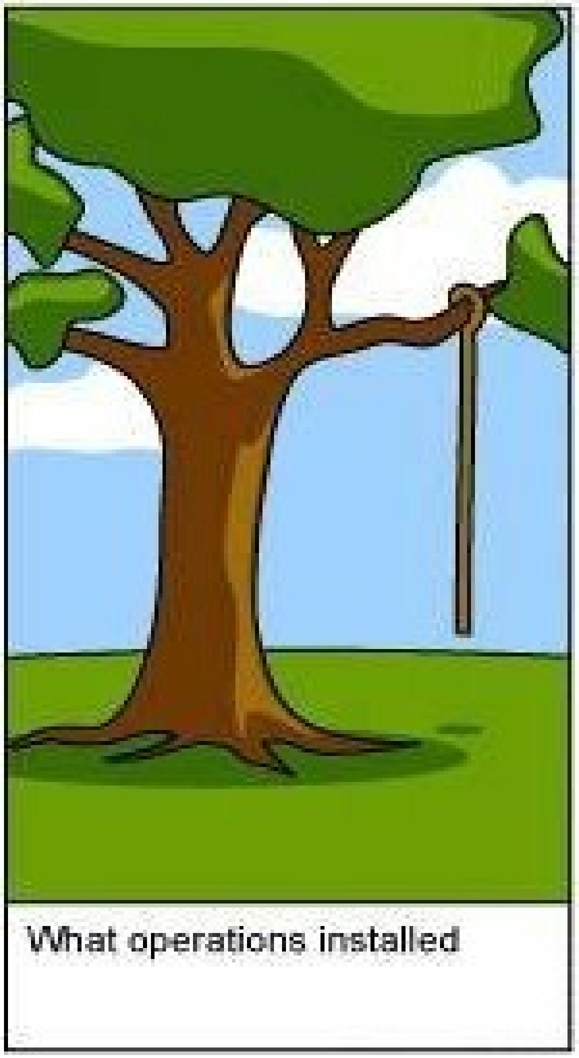
Perform application penetration testing

How the Business Consultant described it

Deployment Phase

Use automated server and application scanners to verify deployment servers are correctly secured

Consider the use of application and database firewalls



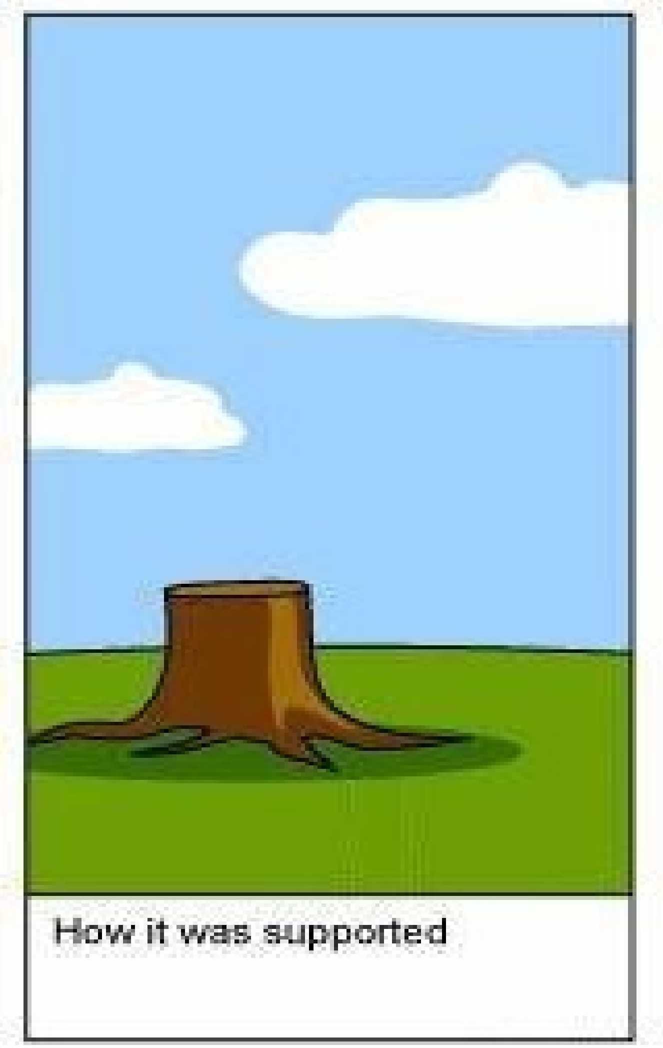
What operations installed

Maintenance Phase

Conduct periodic security reviews and scans

Consider certification and accreditation

Integrate security impact reviews into normal change management processes



Next Steps…

"The security of commercial software will improve when the market demands better security. At a minimum, every software request for proposal should ask vendors to detail how they test their products for security vulnerabilities. This step will start convincing vendors of off-the-shelf software and outsourced developers that enterprises value security." -- John Pescatore, research director with Gartner

Doug Ashbaugh

Software Engineering Services

dashbaugh@sessolutions.com