Top Website Vulnerabilities:

Trends, Business Effects & How to Fight Them

Rinaldi Rampen
Director, Solutions Architecture

OWASP Tampa
06.20.2011

WhiteHat
SECURITY

WhiteHat
SECURITY

450+ enterprise customers

- Start-ups to Fortune 500

Flagship offering “WhiteHat Sentinel Service”

- Thousands of assessments performed annually

Recognized leader in website security

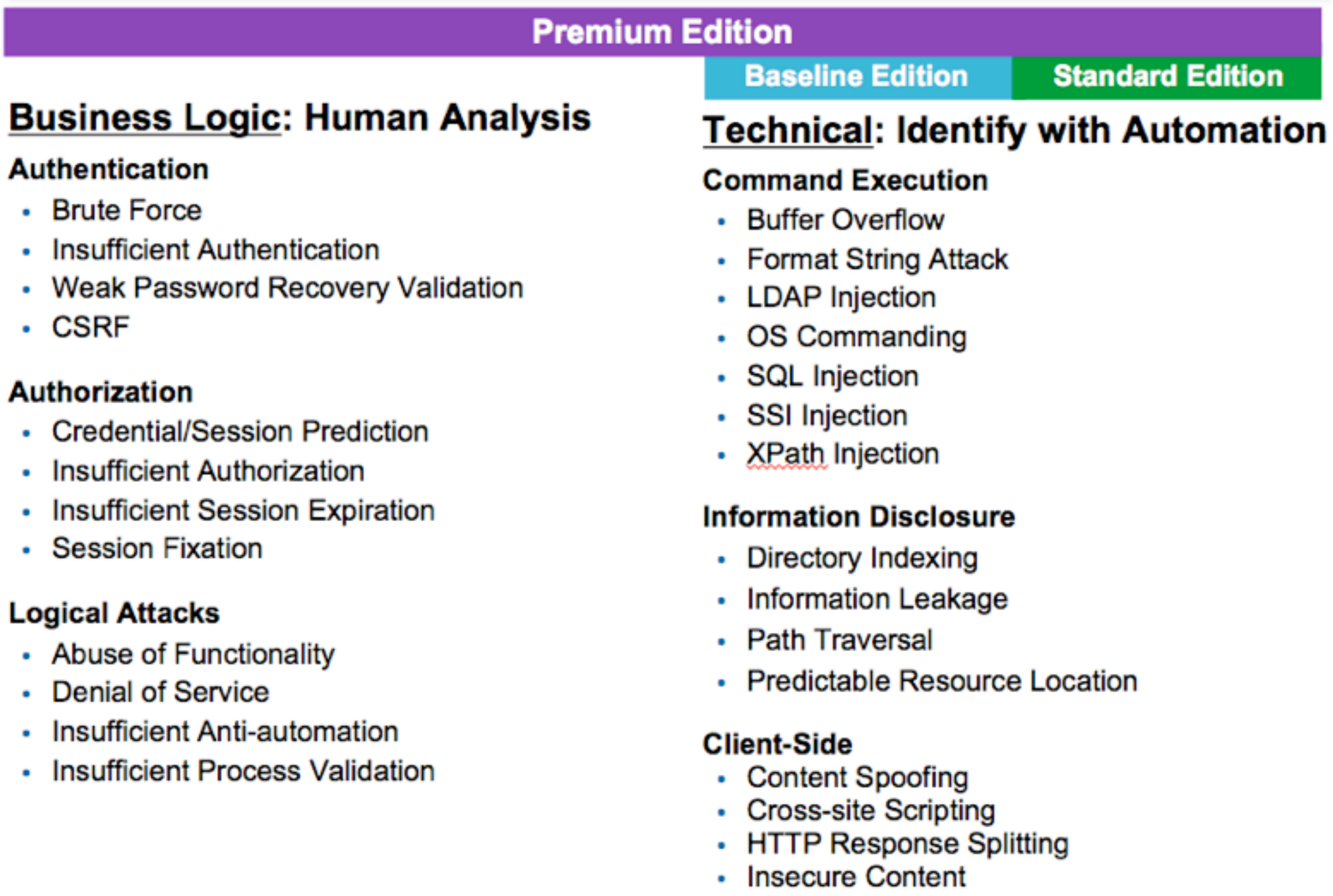
- Quoted thousands of times by the mainstream press

Inc.500

SC MAGAZINE AWARDS 2009 FINALIST Honored in the U.S.

Deloitte. 2008 Technology Fast 50 Silicon Valley

Vulnerability Coverage



Premium Edition

Baseline Edition | Standard Edition

Business Logic: Human Analysis

Authentication

- Brute Force
- Insufficient Authentication
- Weak Password Recovery Validation
- CSRF

Authorization

- Credential/Session Prediction
- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation

Logical Attacks

- Abuse of Functionality
- Denial of Service
- Insufficient Anti-automation
- Insufficient Process Validation

Technical: Identify with Automation

Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

Information Disclosure

- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

Client-Side

- Content Spoofing
- Cross-site Scripting
- HTTP Response Splitting
- Insecure Content

Data Set

- Data collected from January 1, 2006 to February 16, 2011
- ~500,000 verified Web application vulnerabilities (non-CVE)
- Majority of websites assessed multiple times per month
- Classified according to WASC Threat Classification

"When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts advanced to the stage of science."

- Lord Kelvin

Vulnerability Counting

- Vulnerabilities are counted by unique Web application and class of attack. If three of the five parameters of a single Web application (/foo/webapp.cgi) are vulnerable to SQL Injection, this is counted as 3 individual vulnerabilities (e.g. attack vectors). If a single parameter can be exploited in more than one way, each of those are counted as well.

*** Serious Vulnerabilities:** Those vulnerabilities with a **HIGH**, **CRITICAL**, or **URGENT** severity as defined by PCI-DSS naming conventions. Exploitation could lead to breach or data loss.

Lesson: 1

Software will always have bugs and by extension, security vulnerabilities. A practical goal for a secure software development lifecycle (SDLC) should be to reduce, not necessarily eliminate, the number of vulnerabilities introduced and the severity of those that remain.

Thank you Michael Howard (Microsoft)

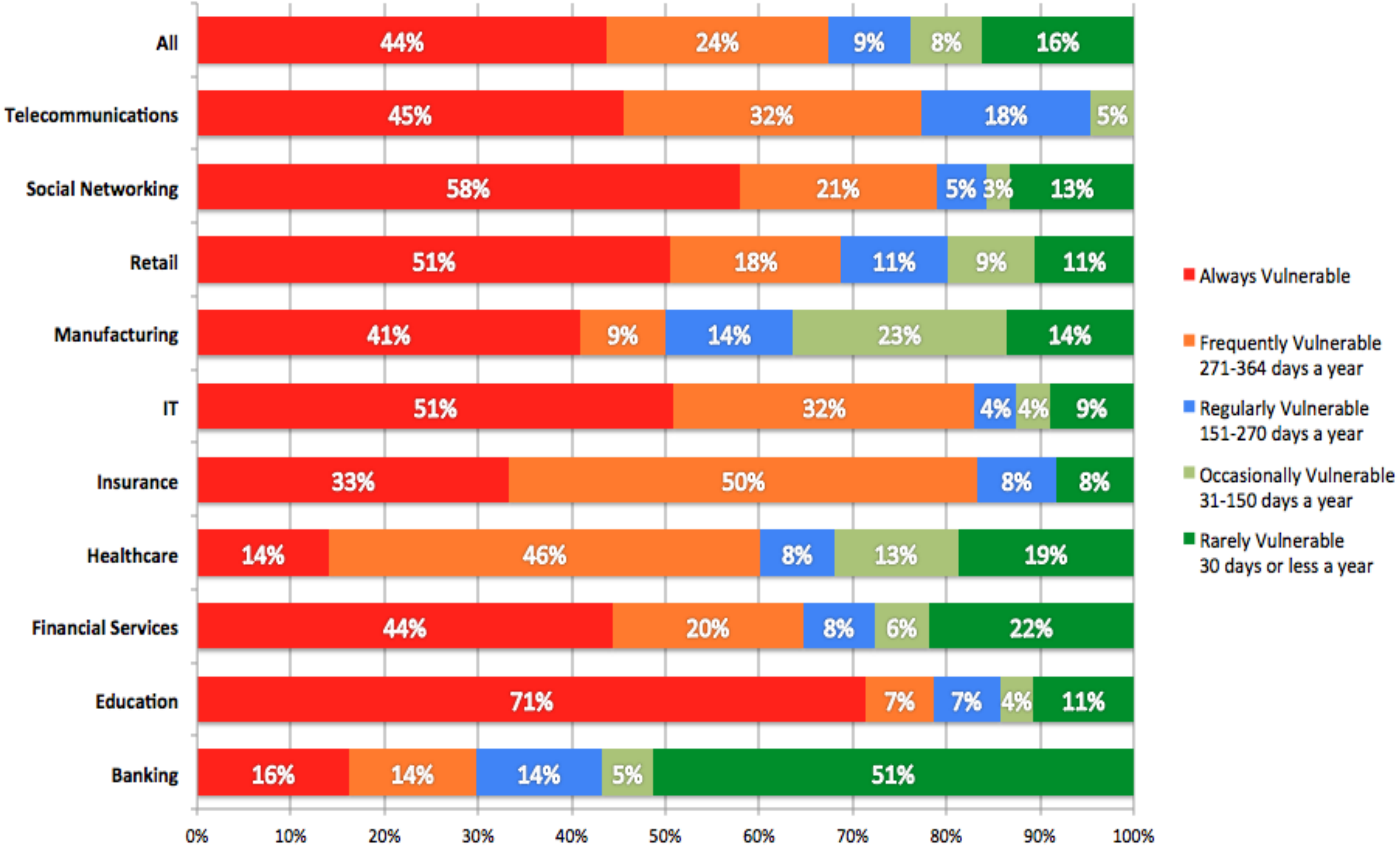
Lesson: 2

Exploitation of just one website vulnerability is enough to significantly disrupt online business, cause data loss, shake customer confidence, and more. The earlier vulnerabilities are identified and the faster they are remediated the shorter the window of opportunity for an attacker to maliciously exploit them.

The security posture of a website must not only be measured by the number of vulnerabilities, but also must take into account remediation rates and time-to-fix metrics.

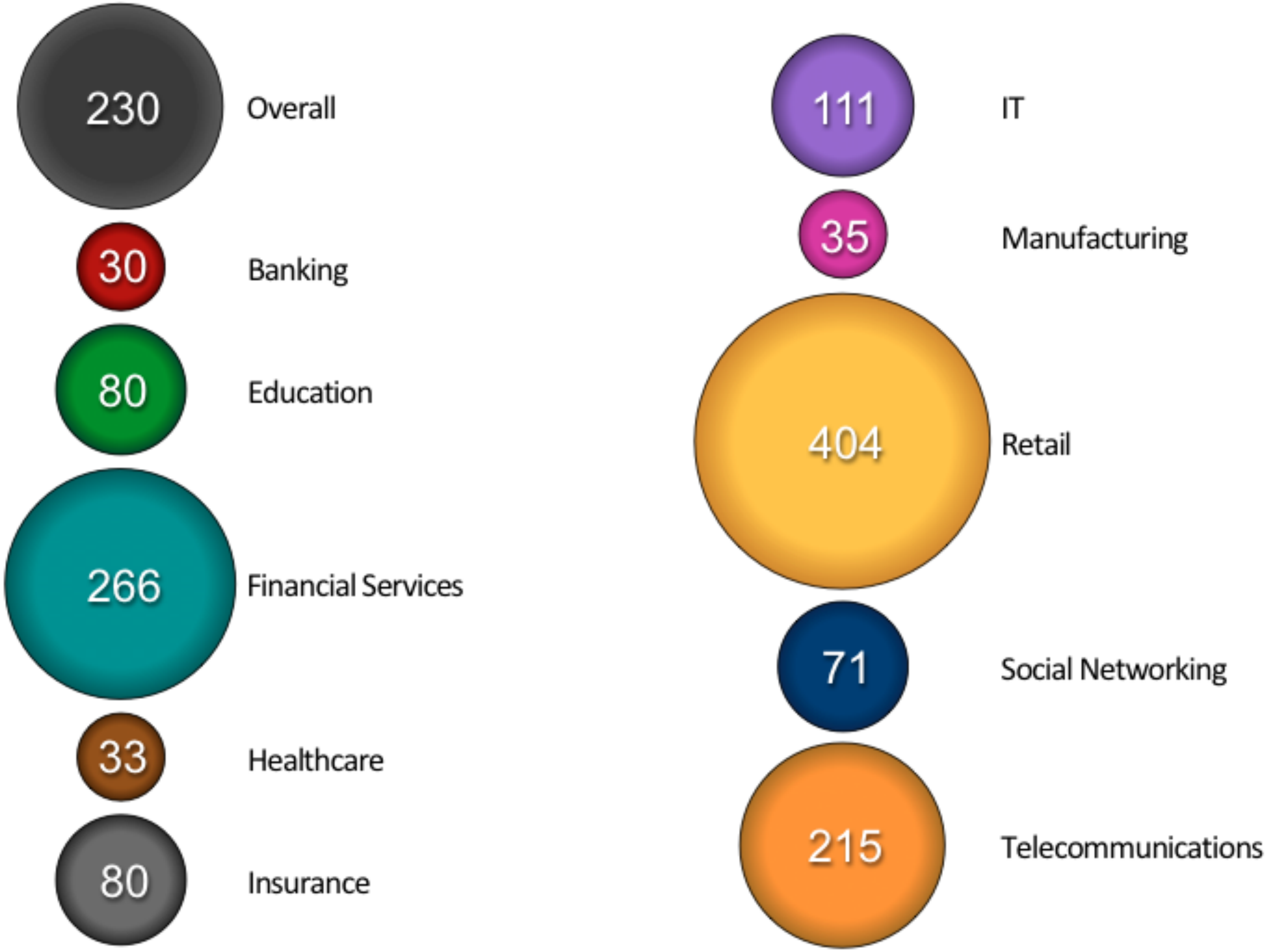
KPI: Window of Exposure

Number of days [in a year] a website is exposed to at least one serious* reported vulnerability.

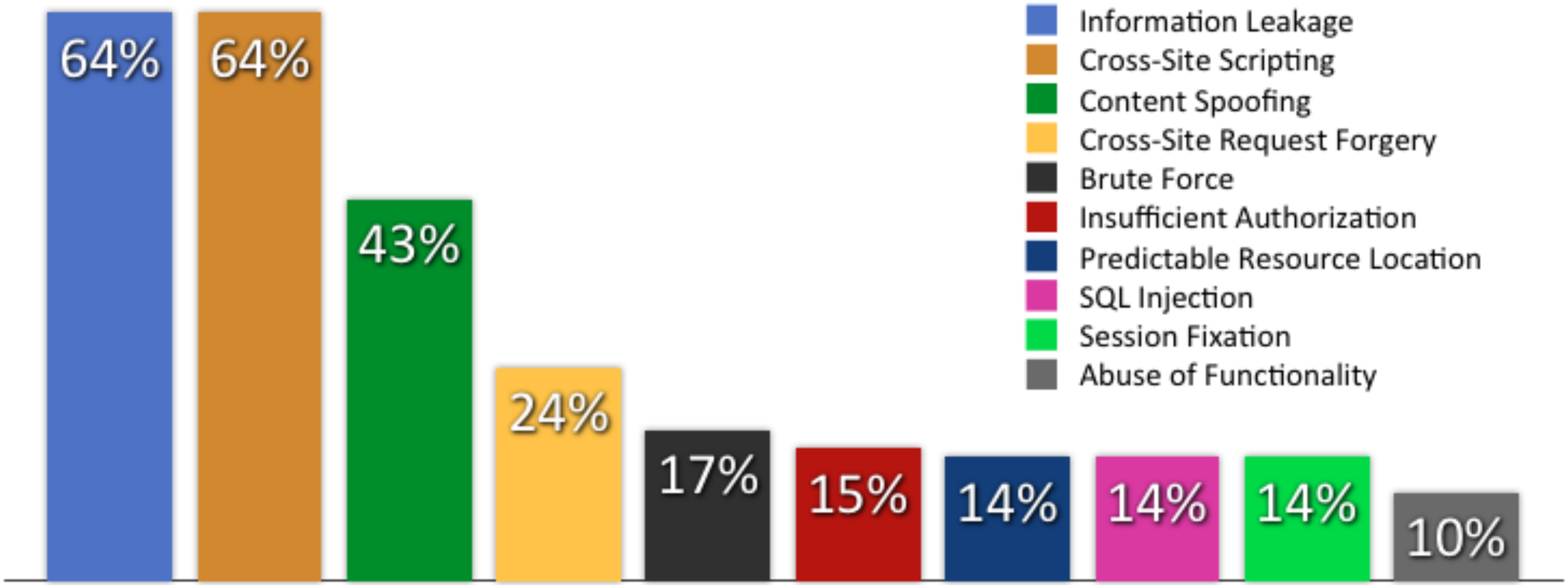


Most websites were exposed to at least one serious* vulnerability every single day of 2010, or nearly so (9-12 months of the year). Only 16% of websites were vulnerable less than 30 days of the year overall.

Average annual amount of new vulnerabilities introduced per website by industry (2010)

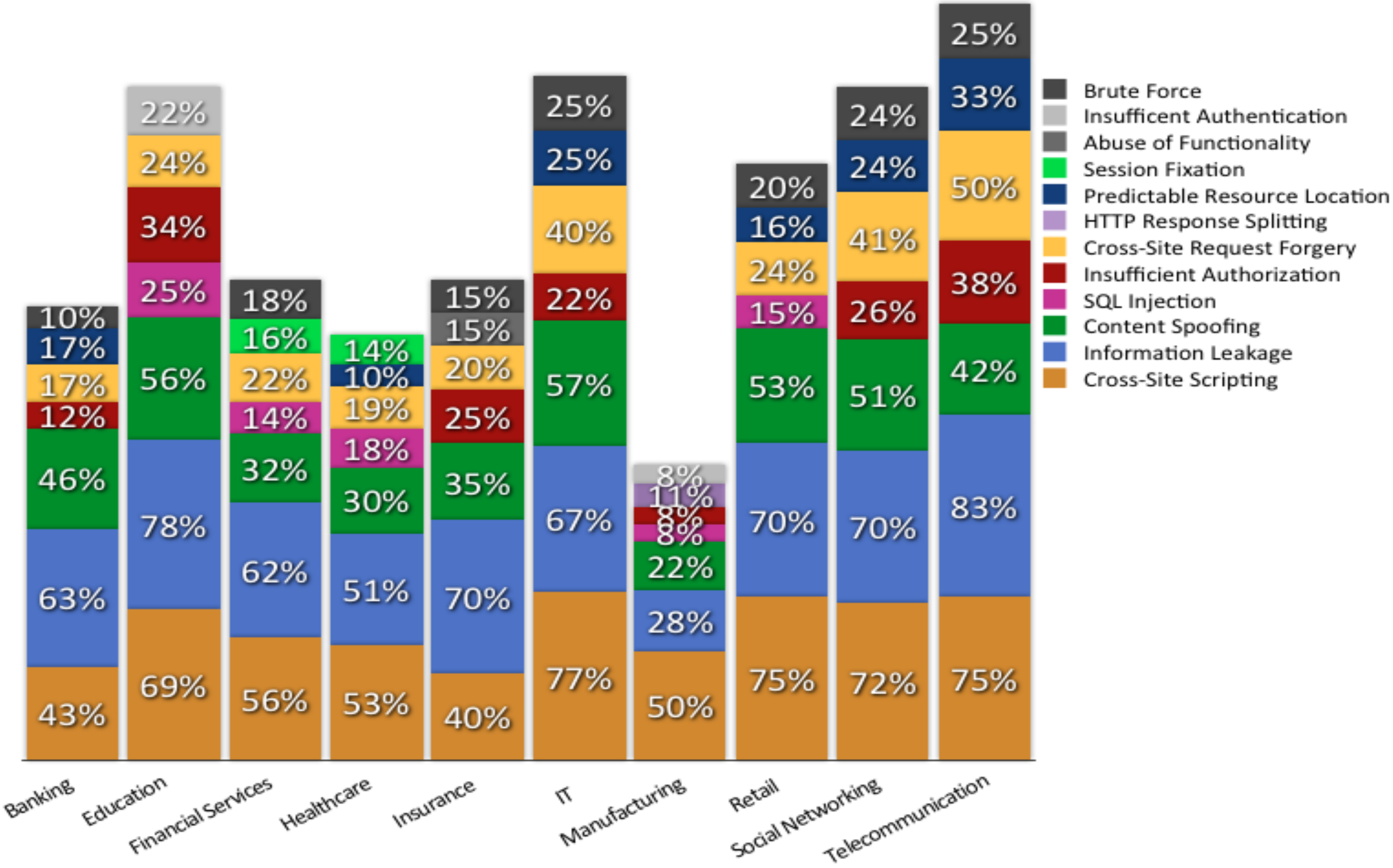


WhiteHat Security Top Ten (2010)



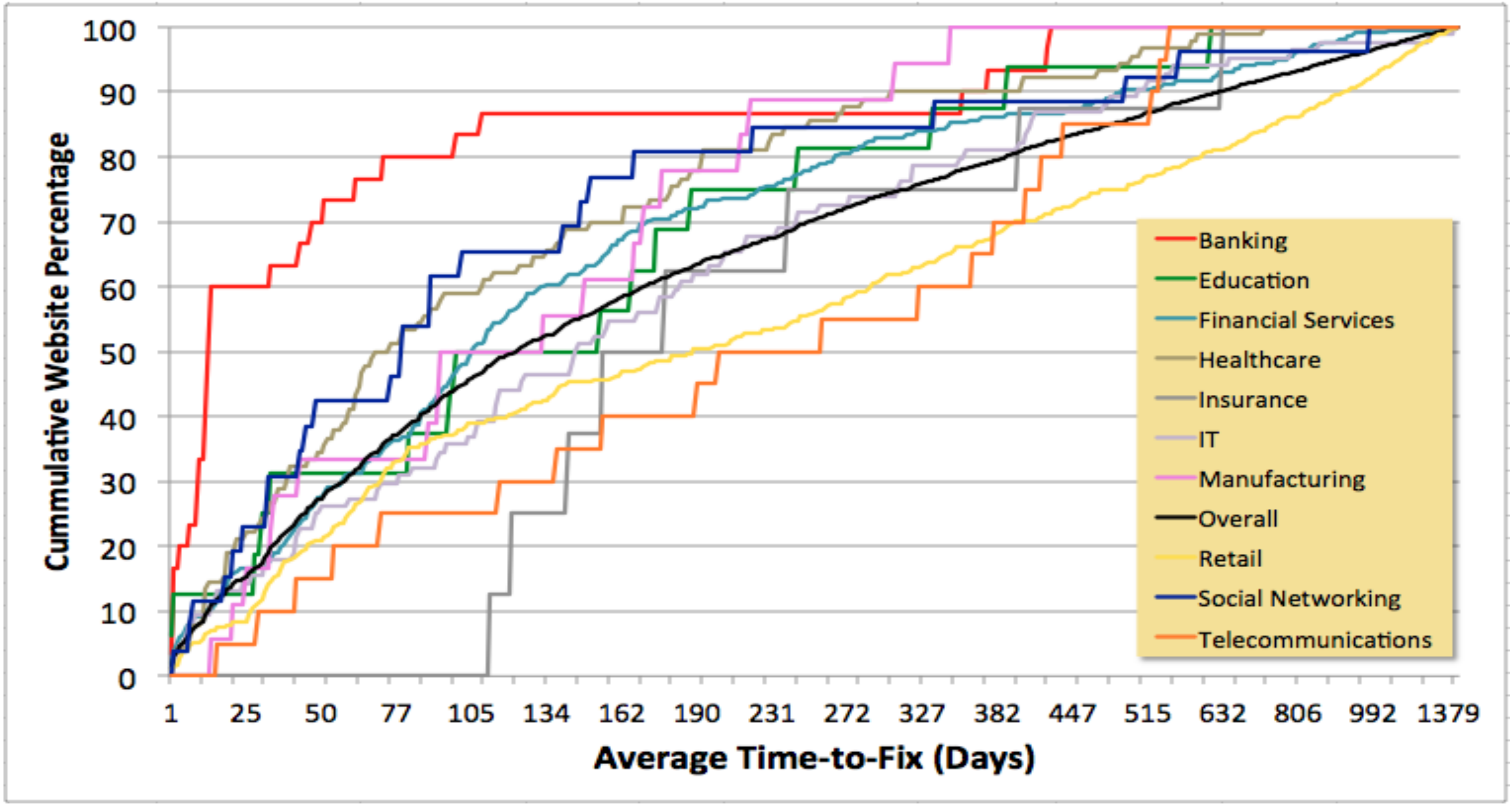
Percentage likelihood of a website having at least one vulnerability sorted by class

Top 7 Vulnerabilities by Industry (2010)



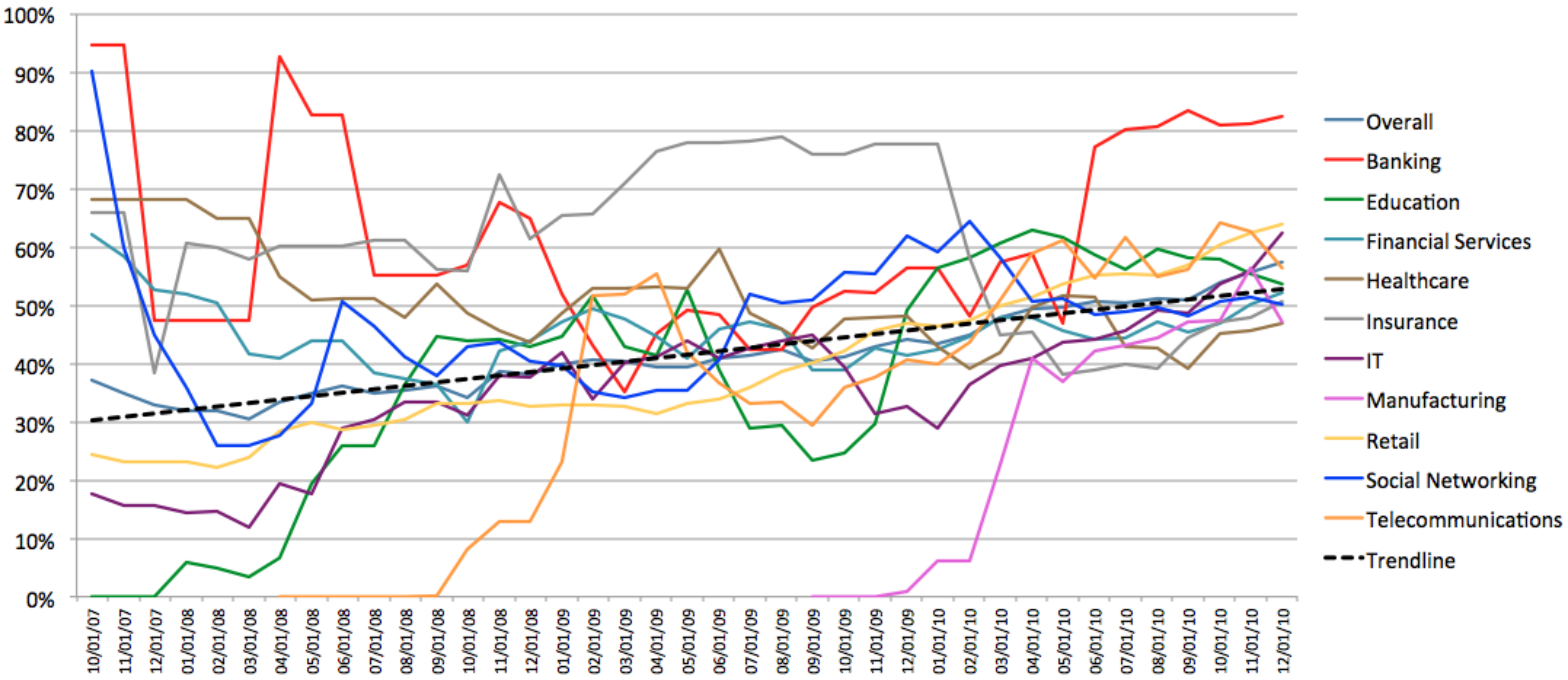
Percentage likelihood of a website having at least one vulnerability sorted by class

Time-to-Fix in Days by Industry (2010)



On the average, 50% of organizations require 116 days or less to remediate their serious* vulnerabilities. The Banking industry being the fastest where 50% take under 13 days. The slowest is Telecommunications in that half need 205 days.

Remediation Rates by Industry (Trend)



A 5% improvement in the percentage of reported vulnerabilities that have been resolved during each of the last three years (2008, 2009, 2010), which now resides at 53%. Progress!

Why do vulnerabilities go unfixed?

- No one at the organization understands or is responsible for maintaining the code.
- Development group does not understand or respects the vulnerability.
- Feature enhancements are prioritized ahead of security fixes.
- Lack of budget to fix the issues.
- Affected code is owned by an unresponsive third-party vendor.
- Website will be decommissioned or replaced “soon.”
- Risk of exploitation is accepted.
- Solution conflicts with business use case.
- Compliance does not require fixing the issue.

Lesson: 3

Vulnerabilities do not exploit themselves. Someone or something, an attacker (or “threat”), uses an attack vector to exploit a vulnerability in a website, bypass a control, and cause a technical or business impact. Some attackers are sentient, and others are automated. Different attackers have different capabilities and goals in mind.

Lesson: 4

Some organizations are targets of opportunity, others targets of choice.

- Targets of opportunity are victimized when their security posture is weaker than the average organization and the data they possess can be converted easily into liquid currency.
- Targets of opportunity possess some form of unique and valuable information that is particularly attractive to an attacker.

If an organization is a target of opportunity, the goal of being at or above average with regard to website vulnerability numbers among your peers is reasonable.

If a target of choice, then the adversary is one who will spend whatever time is necessary looking for gaps in the defenses to exploit. In this case, an organization must elevate its website security posture to a point where an attacker’s efforts are detectable, preventable, and in case of compromise, survivable.

2010 at a Glance

Industry	Number of Vulns	Std. Dev	Remediation Rate	Std. Dev	Window of Exposure (Days)
Overall	230	1652	53%	40%	233
Banking	30	54	71%	41%	74
Education	80	144	40%	36%	164
Financial Services	266	1935	41%	40%	184
Healthcare	33	87	48%	40%	133
Insurance	80	204	46%	37%	236
IT	111	313	50%	40%	221
Manufacturing	35	111	47%	40%	123
Retail	404	2275	66%	36%	328
Social Networking	71	116	47%	34%	159
Telecommunications	215	437	63%	40%	260

Thank You

***Twitter**: http://twitter.com/Rinaldi2pt0*
***Email**: rinaldi.rampen@whitehatsec.com*