4 Years and 4 Thousand Websites:

What Have We Learned about Hacking Websites?

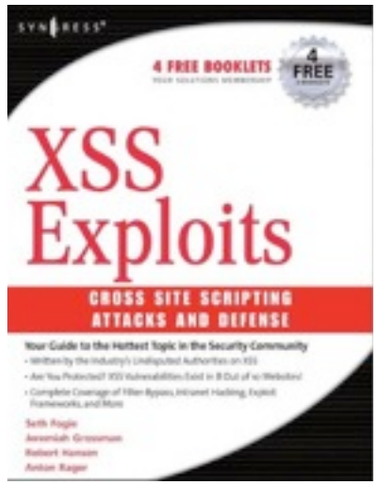
Jeremiah Grossman
Founder & Chief Technology Officer

WhiteHat SECURITY

© 2011 WhiteHat Security, Inc.

Jeremiah Grossman

- WhiteHat Security Founder & CTO
- An InfoWorld Top 25 CTO
- Co-founder of the Web Application Security Consortium
- Co-author: Cross-Site Scripting Attacks
- Former Yahoo! information security officer



© 2011 WhiteHat Security, Inc.

We shop, bank, pay bills, file taxes, share photos, keep in touch with friends & family, watch movies, play games, and more.

Cyber-war **Cyber-crime** **Hacktivism**

© 2011 WhiteHat Security, Inc.

How Data Breaches Happen

Verizon Business' 2010 Data Breach Investigations Report (DBIR):

“The majority of breaches and almost all of the data stolen in 2009 (95%) were perpetrated by remote organized criminal groups hacking "servers and applications."

Verizon Business' 2011 Data Breach Investigations Report (DBIR):

“The number of Web application breaches increased last year and made up nearly 40% of the overall attacks.“

And this was all before...

© 2011 WhiteHat Security, Inc.

at&t
Sun
microsystems
Kiplinger
zynga
Nintendo
AMERICAN
INTELLIGENCE
HACKED
SONY
HARVARD
UNIVERSITY
Moody's
citigroup
NYSE
GAWKER
BitTorrent

What we SHOULD be learning

1) Each and every one of these recent breaches could easily happen to any online business.

2) Exploitation of just one website vulnerability is enough to significantly disrupt online business, cause data loss, shake customer confidence, and more.

3) Attack techniques of choice are SQL Injection, PHP Local File Include, password reuse, denial of service, and malware; all of which cannot be defended against by firewalls or SSL. None should be considered ‘sophisticated’ by modern standards.

4) What makes some of these breaches unique, and why the hacks keep occurring, is that the victimized companies are ‘targeted‘ and their adversaries are relentless.

5) 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.

© 2011 WhiteHat Security, Inc.

Where to begin?

Hack Yourself First

WhiteHat Sentinel

400+
enterprises from start-ups to fortune 500
4,500
total sites assessed
357,000
vulnerabilities processed per day
7,700,000
tests per week
600,000,000
requests per month
10 Terabytes
data stored per week

Our infrastructure -- Assessing Over 2,000 websites
http://jeremiahgrossman.blogspot.com/2010/09/our-infrastructure-assessing-over-2000.html

© 2011 WhiteHat Security, Inc.

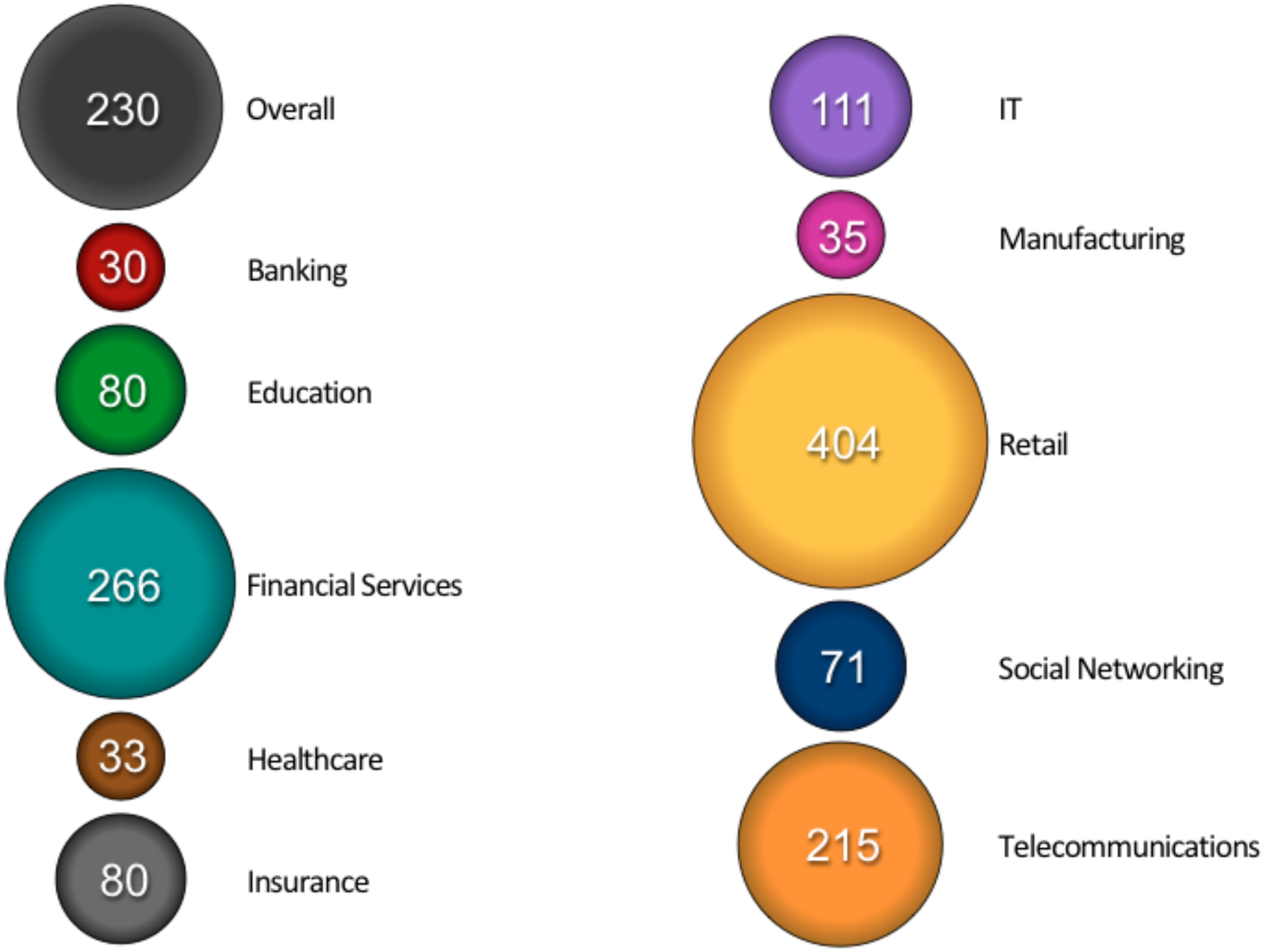
Average annual amount of new serious* vulnerabilities introduced per website by year

2007 2008 2009 2010 2011

*** Serious Vulnerability:** A security weakness that if exploited may lead to breach or data loss of a system, its data, or users. (PCI-DSS severity **HIGH**, **CRITICAL**, or **URGENT**)

© 2011 WhiteHat Security, Inc.

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



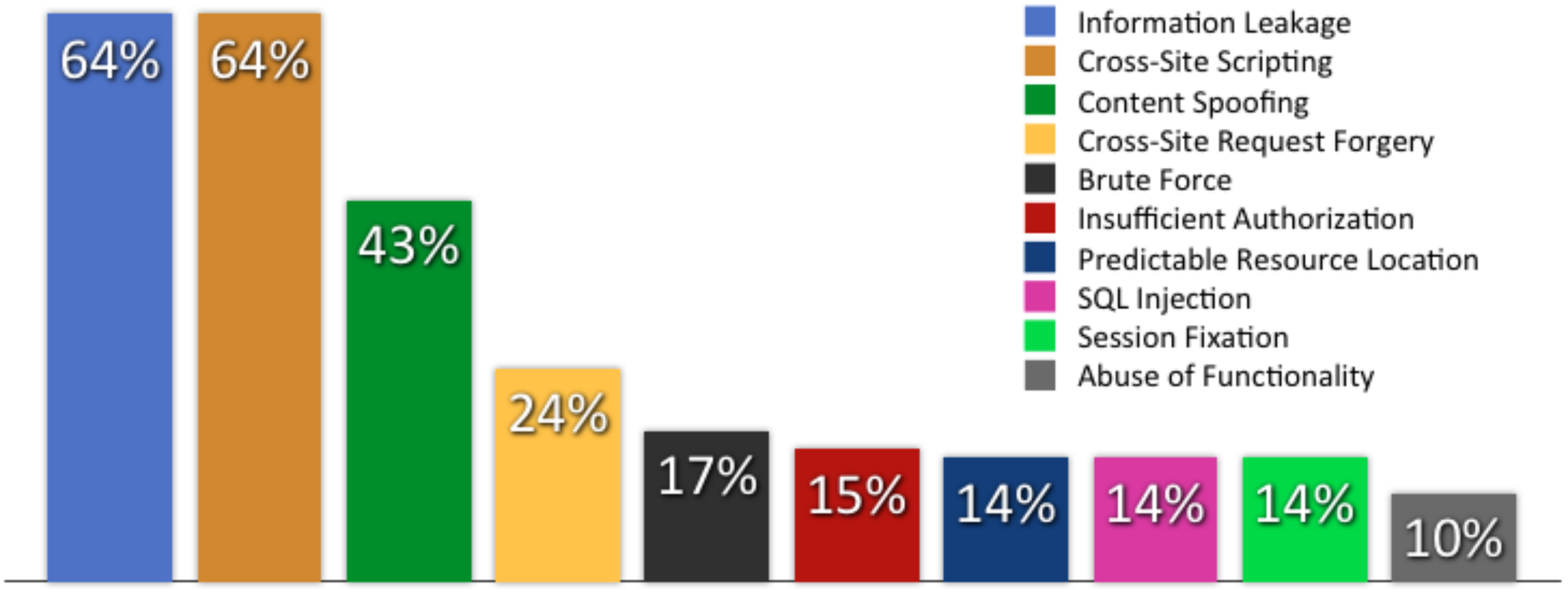
© 2011 WhiteHat Security, Inc.

Average annual amount of new serious* vulnerabilities introduced per website by industry by year

Banking	10	76	101	30	30
Education	10	144	107	80	86
Financial Services	361	361	303	266	140
Healthcare	20	109	112	33	104
Insurance	154	417	539	80	84
IT	328	300	178	111	126
Manufacturing	-	-	33	35	36
Retail	2471	1820	1000	404	238
Social Networking	113	143	129	71	57
Telecommunications	-	891	634	215	119
	2007	2008	2009	2010	2011

© 2011 WhiteHat Security, Inc.

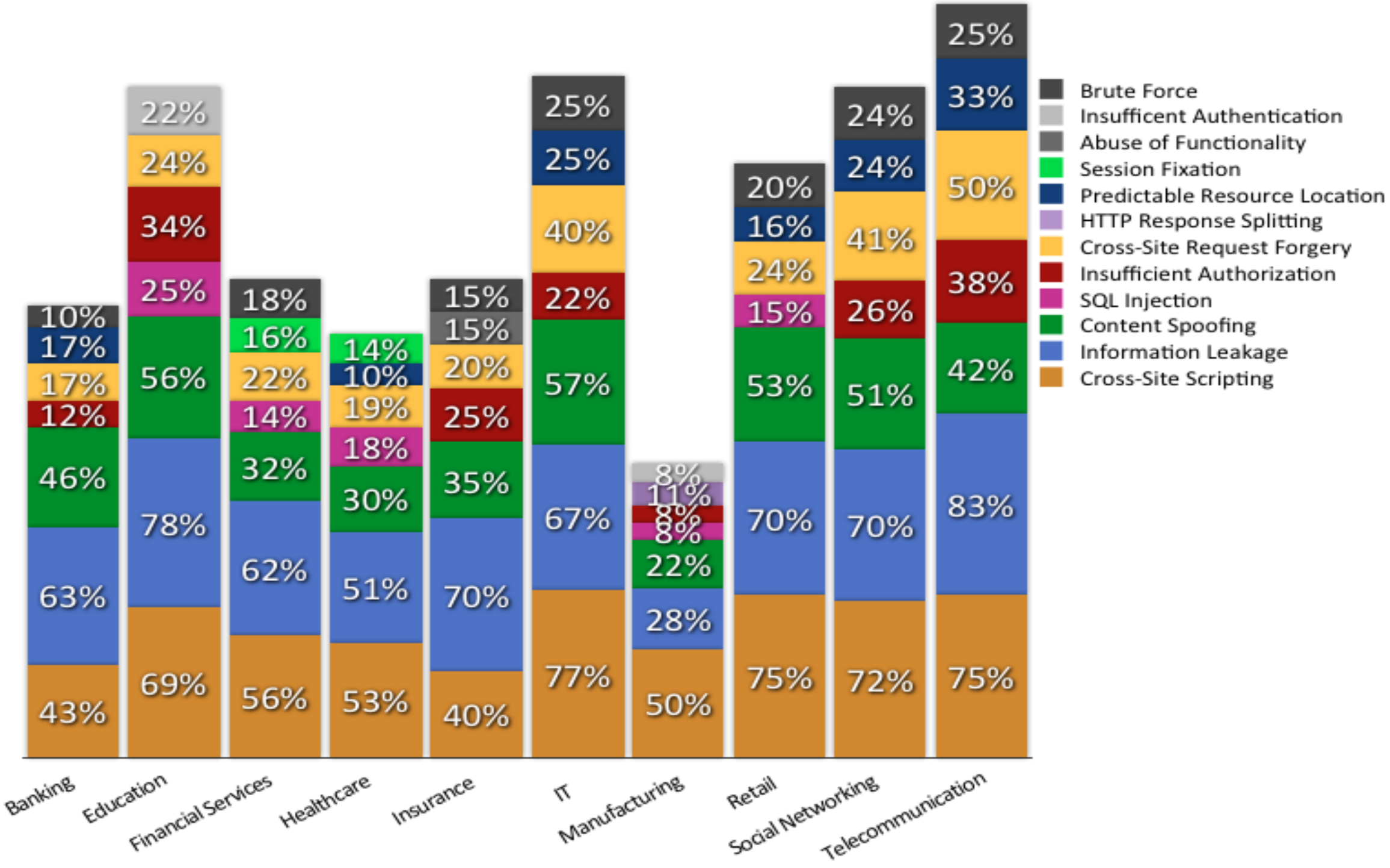
WhiteHat Security Top Ten (2010)



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

© 2011 WhiteHat Security, Inc.

Top 7 Vulnerabilities by Industry (2010)



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

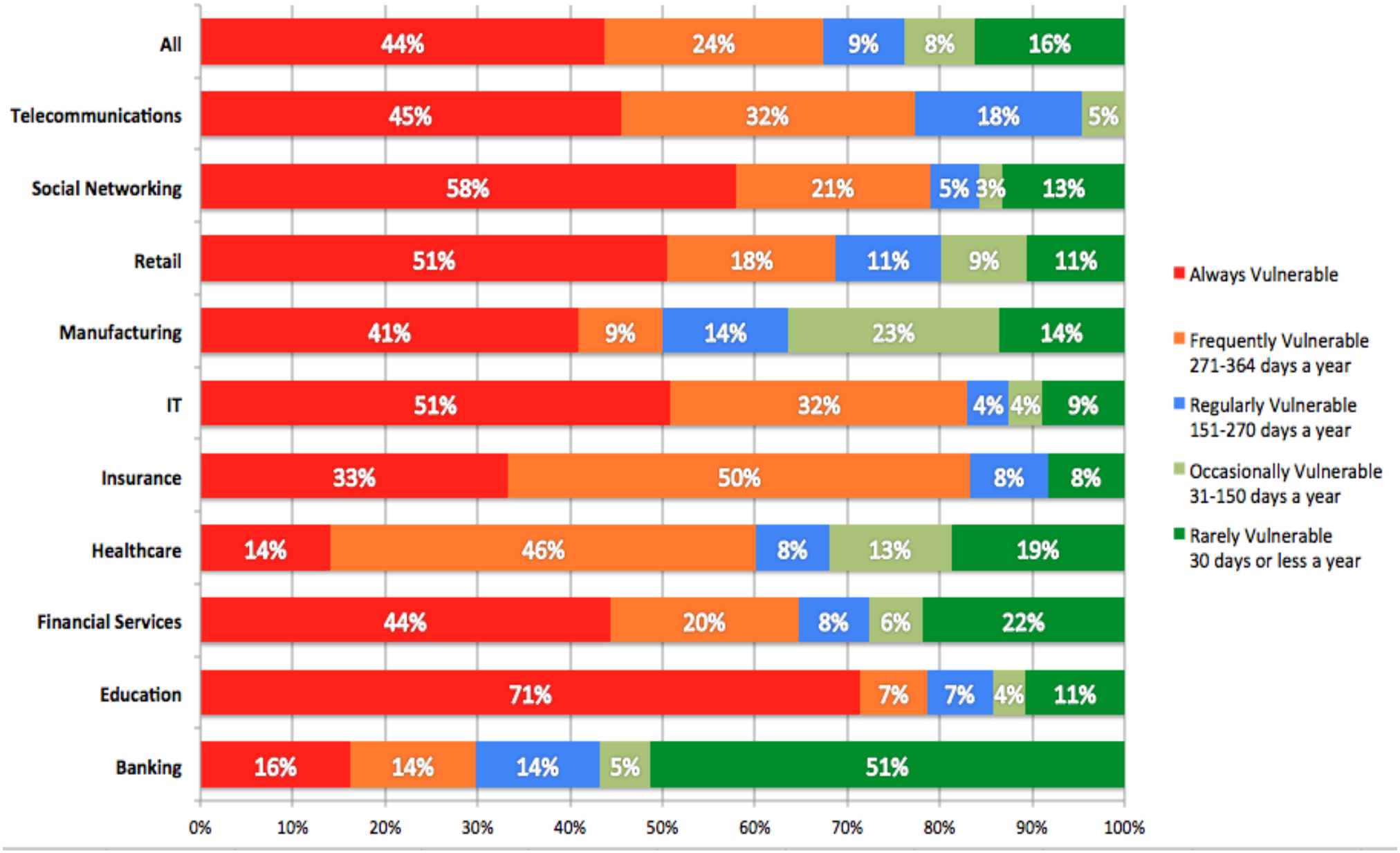
© 2011 WhiteHat Security, Inc.

The security posture of a website must take into account remediation rates and time-to-fix metrics.

© 2011 WhiteHat Security, Inc.

Window of Exposure (2010)

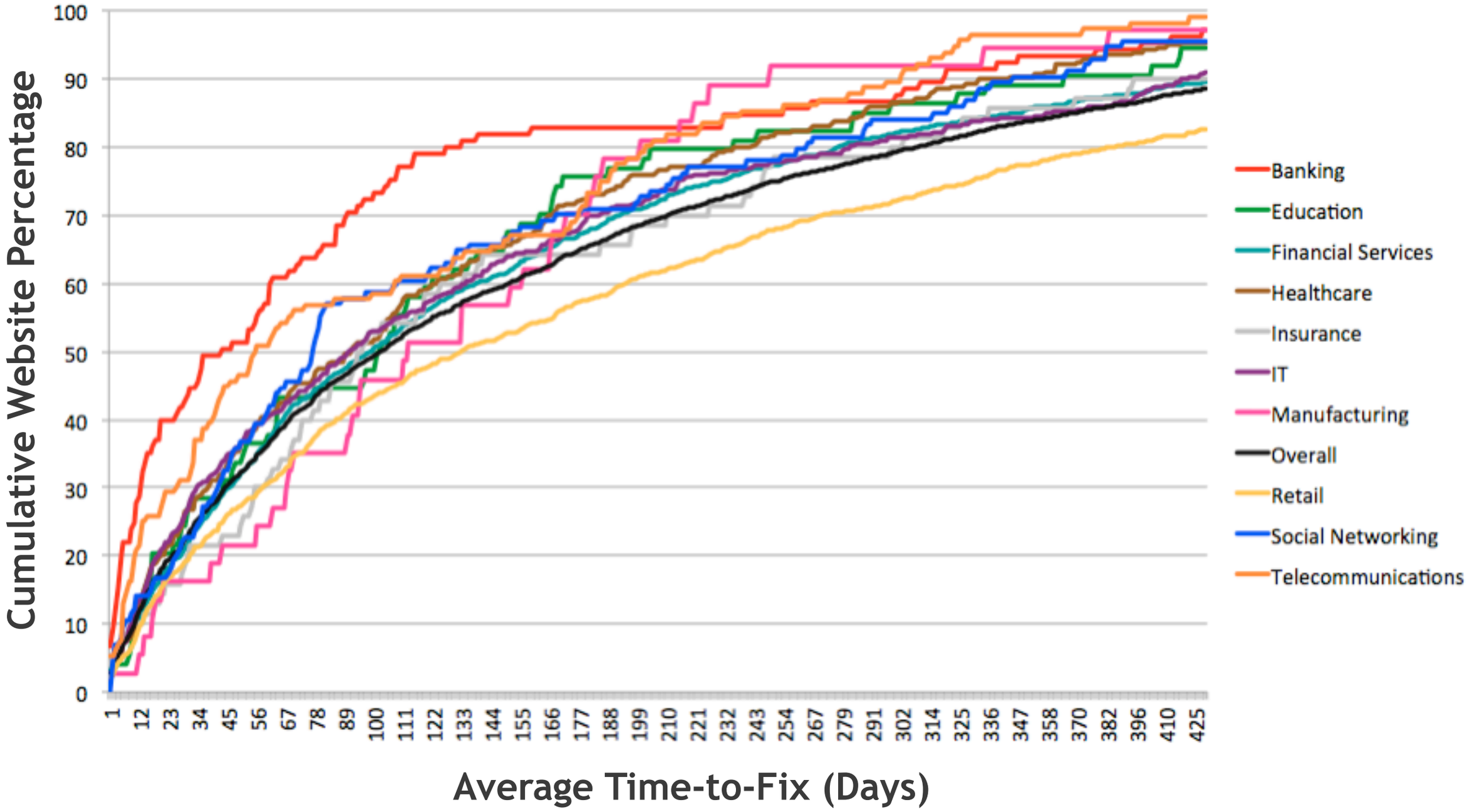
Number of days [in a year] a website is exposed to at least one serious* reported vulnerability.



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.

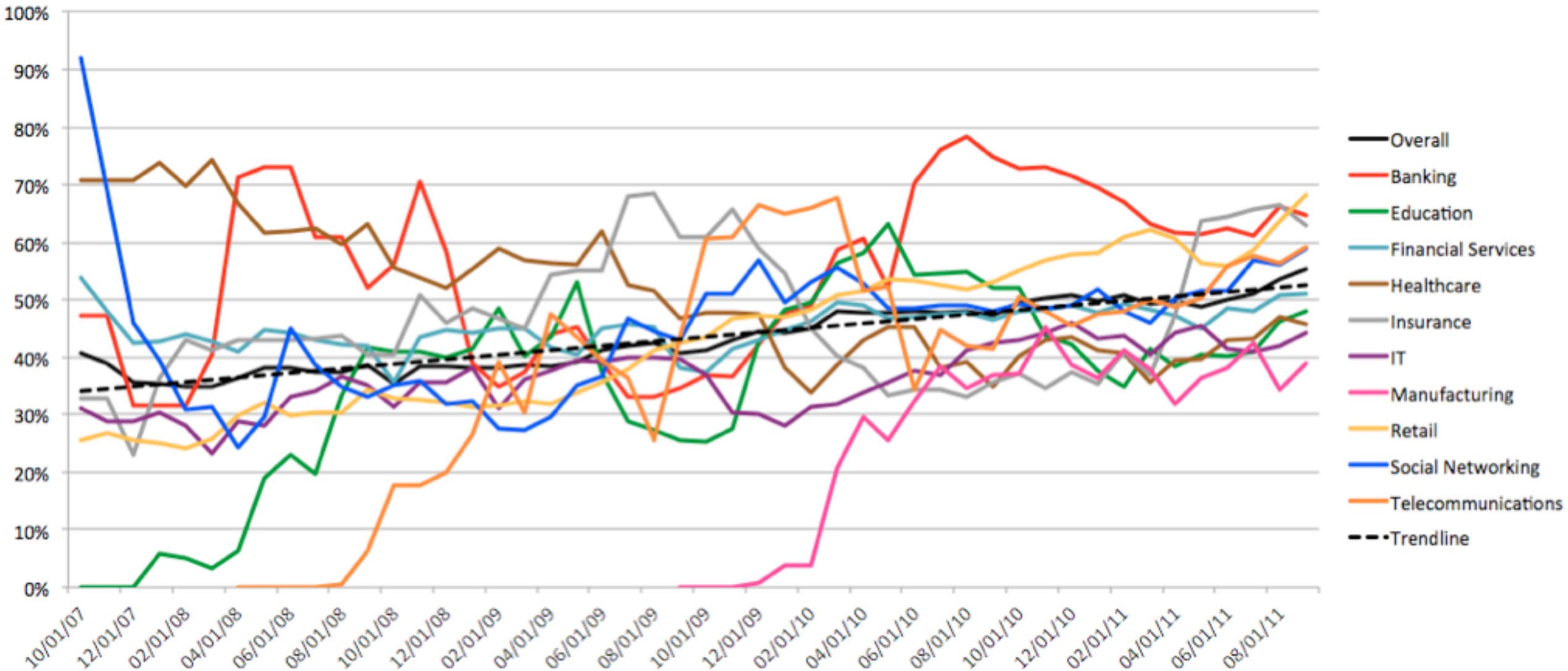
© 2011 WhiteHat Security, Inc.

Time-to-Fix in Days



© 2011 WhiteHat Security, Inc.

Remediation Rates by Industry (Trend)



A steady improvement in the percentage of reported vulnerabilities that have been resolved during each of the last three years, which now resides at 53%. Progress!

© 2011 WhiteHat Security, Inc.

Why do vulnerabilities go unfixed?

- No one at the organization understands or is responsible for maintaining the code.
- Development group does not understand or respect the vulnerability.
- 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.
- Feature enhancements are prioritized ahead of security fixes.

© 2011 WhiteHat Security, Inc.

Testing Speed & Frequency Matters

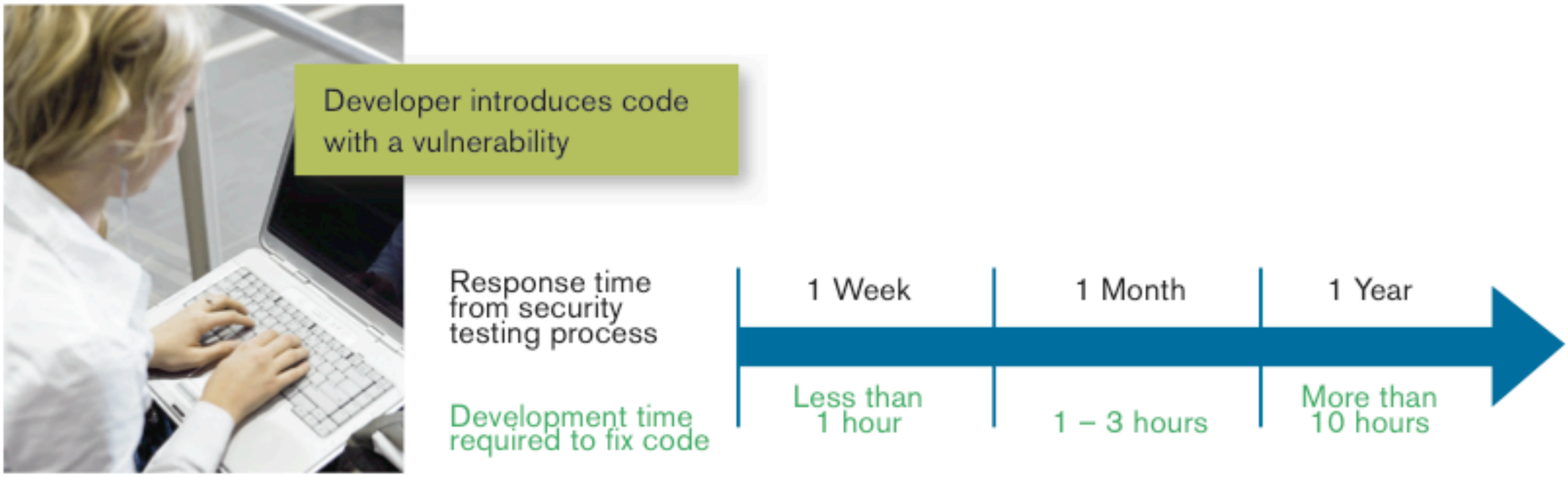


Figure 1. Relationship between the time that passes between testing for vulnerabilities and the time required to fix them:

© 2011 WhiteHat Security, Inc.

Why Do Breaches

(*and vulnerabilities*)

Continue to Happen?

I don’t think the answer is technical

© 2011 WhiteHat Security, Inc.

The IT Budget Game

Ask the CFO where the business invests

Applications

Software, development, CRM, ERP, etc.

Host

Servers, desktops, laptops, etc.

Network

Routers, switches, network admins, etc.

© 2011 WhiteHat Security, Inc.

Typical IT Budget Allocation

Applications

Software, development, CRM, ERP, etc.

Host

Servers, desktops, laptops, etc.

Network

Routers, switches, network admins, etc.

© 2011 WhiteHat Security, Inc.

Ask the CISO

Security investment to protect the IT assets

Applications

Software architecture, trainings,testing, etc.

Host

Vulnerability management, system config,patching, etc.

Network

Firewalls, Network IDS, SSL, monitoring, etc.

© 2011 WhiteHat Security, Inc.

Typical IT Security Budget

Applications

Software architecture, trainings,testing, etc.

Host

Vulnerability management, system config,patching, etc.

Network

Firewalls, Network IDS, SSL, monitoring, etc.

© 2011 WhiteHat Security, Inc.

Budget Prioritization

The biggest line item in [non-security] spending **SHOULD** match the biggest line item in security.

	IT	IT Security
 Applications	1	3
 Host	2	2
 Network	3	1

© 2011 WhiteHat Security, Inc.

Empirical Data

Survey [2010] of IT pros and C-level executives from 450 Fortune 1000 companies (FishNet Security)...
*“Nearly 70% [of those surveyed] say **mobile computing** is the biggest threat to security today, closely followed by **social networks** (68%), and **cloud computing platforms** (35%). Around 65% rank mobile computing the top threat in the next two years, and 62% say cloud computing will be the biggest threat, bumping social networks."*

The report goes on to say...
*“45% say **firewalls** are their priority security purchase, followed by **antivirus** (39%), and **authentication** (31%) and **anti-malware tools** (31%)."*

http://www.darkreading.com/security-services/167801101/security/perimeter-security/227300116/index.html

© 2011 WhiteHat Security, Inc.

Big Picture

"Market-sizing estimates for network security range anywhere from $5-8bn, whereas our calculation for the aggregate application security market is about $444m. Despite the spending boost on application security mandated by the Payment Card Industry Data Security Standards (PCI-DSS), it's still not commensurate with the demonstrated level of risk."

The Application Security Spectrum (The 451 Group)

"...we expect this revenue will grow at a CAGR of 23% to reach $1bn by 2014."

© 2011 WhiteHat Security, Inc.

Difficult Choices

1) Reallocate resources away from firewalls, IDS, anti-virus, etc. towards application security.

2) Justify brand-new application security spending.

3) Keep the status quo -- breaches continue and get worse.

Security is optional, but then again, so is survival.

© 2011 WhiteHat Security, Inc.

Thank You!

I was not in your threat model.

1:53 PM Apr 28th via TweetDeck
Retweeted by 1 person

jeremiahg
Jeremiah Grossman

Blog: *http://blog.whitehatsec.com/*
Twitter: *http://twitter.com/jeremiahg*
Email: *jeremiah@whitehatsec.com*

© 2011 WhiteHat Security, Inc.