Cloudy with a chance of hack

Lars Ewe
CTO / VP of Eng.
Cenzic
lars@cenzic.com

OWASP
July, 2010

The OWASP Foundation
http://www.owasp.org

Agenda

- Weather Trends & 6-Day Forecast
- Clouds Everywhere!
- Why So Little Sunshine?
- How To Best Dress For Bad Weather
- Q & A

The First Hacked Site

Web Security Trends

75% of cyber attacks & Internet security violations are generated through Internet applications

Source: Gartner Group

87% of Websites are vulnerable to attack

Source: SearchSecurity – January 2009

75% of enterprises experienced some form of cyber attack in 2009

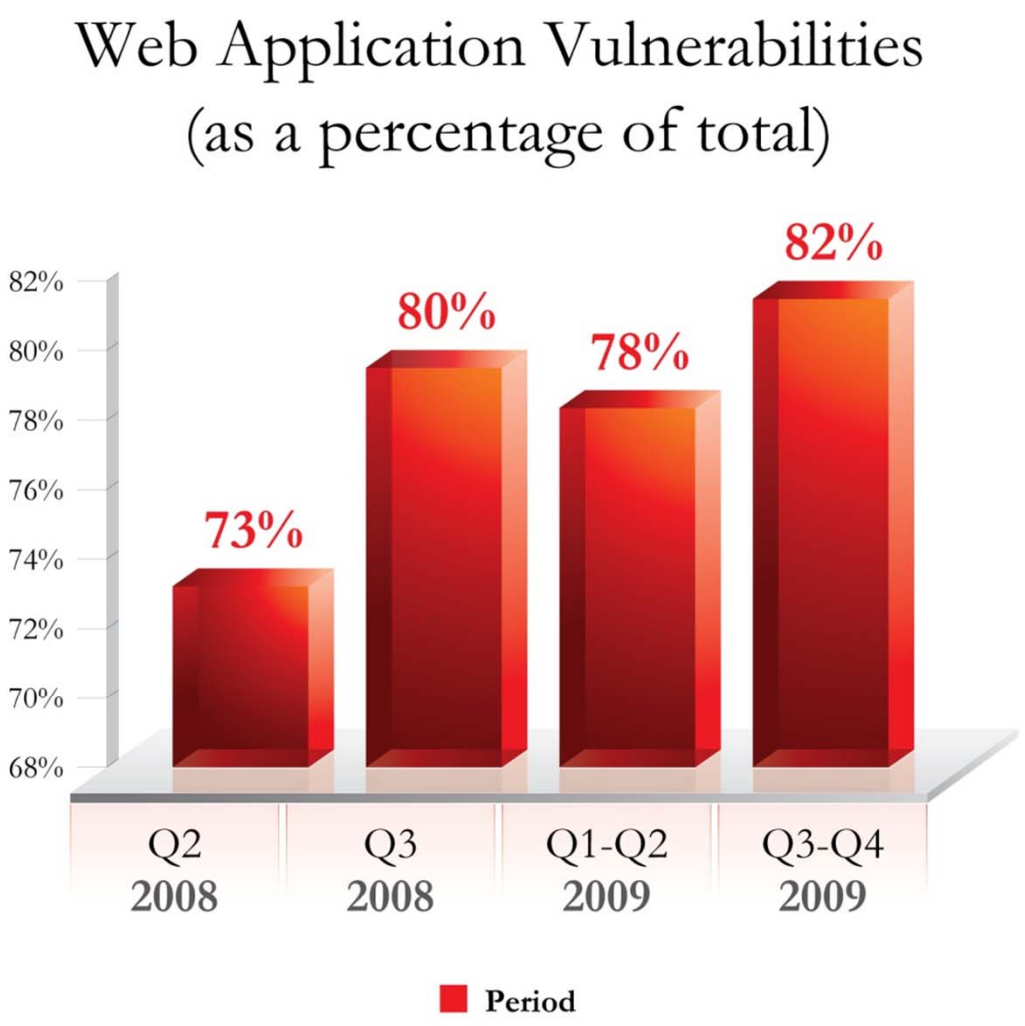
Source: Symantec Internet Security Report – April 2010

90% of Websites are vulnerable to attack

Source: Verizon Business Data Breach Report – April 2009

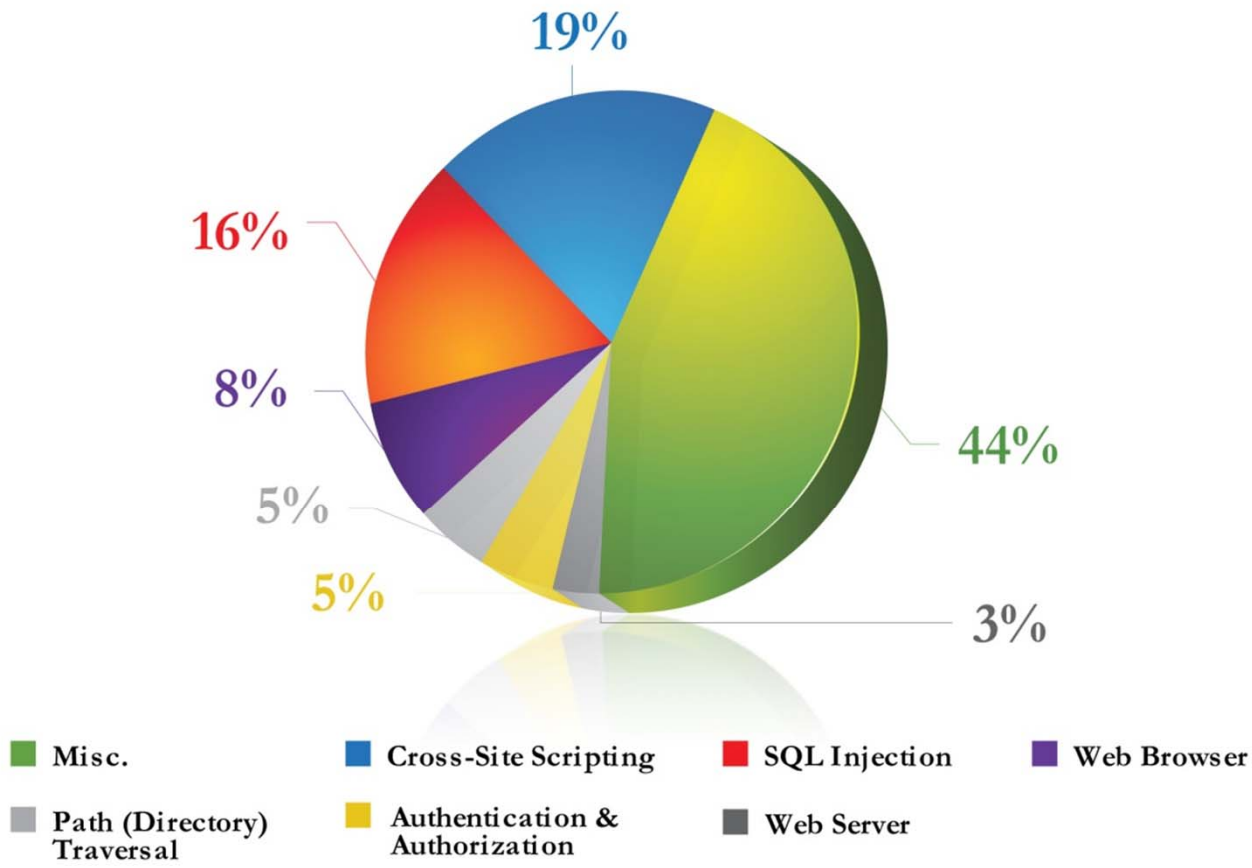
$6.6 Million is the average cost of a data breach

Source: Ponemon Institute – January 2009



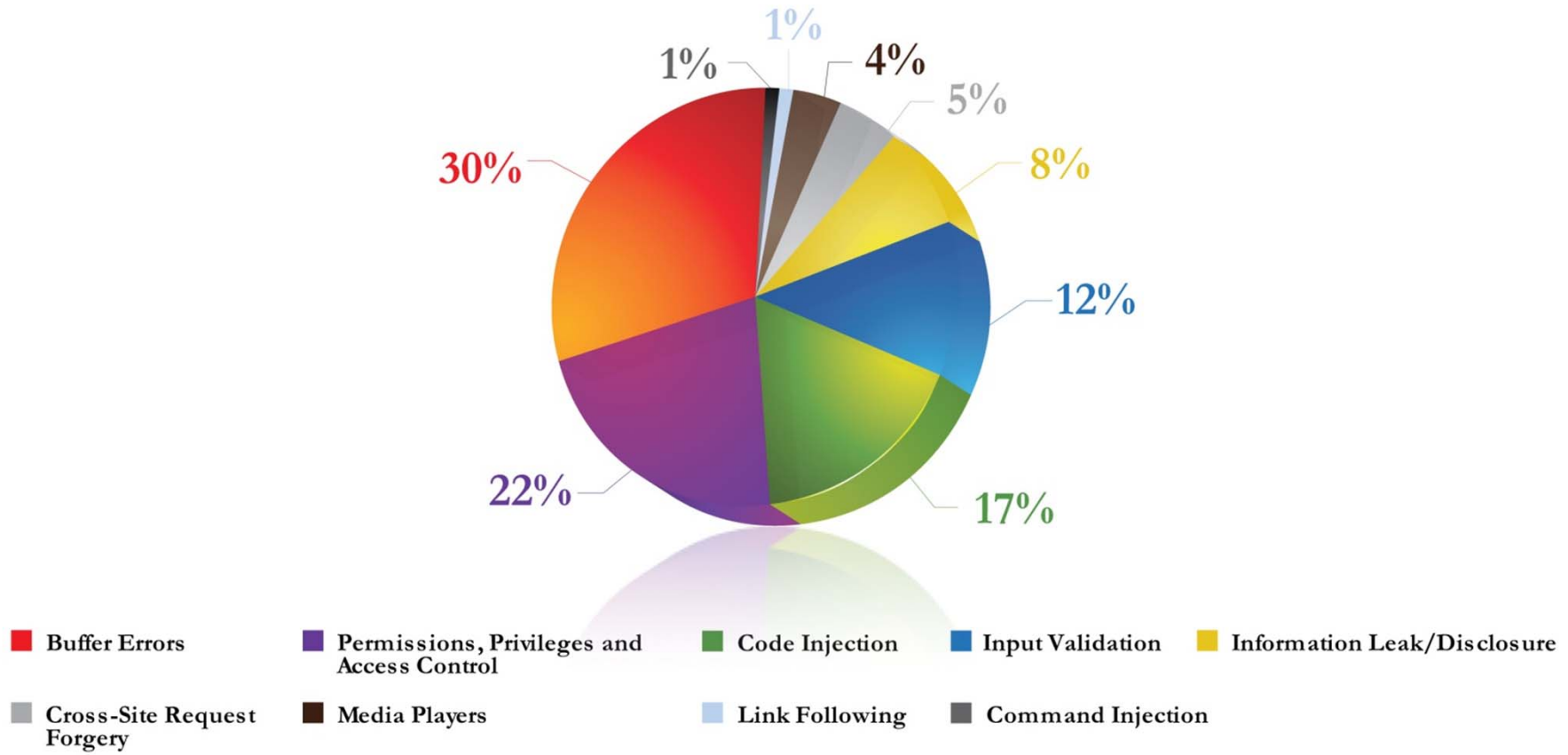
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Web Vulnerabilities by Class (commercial applications)



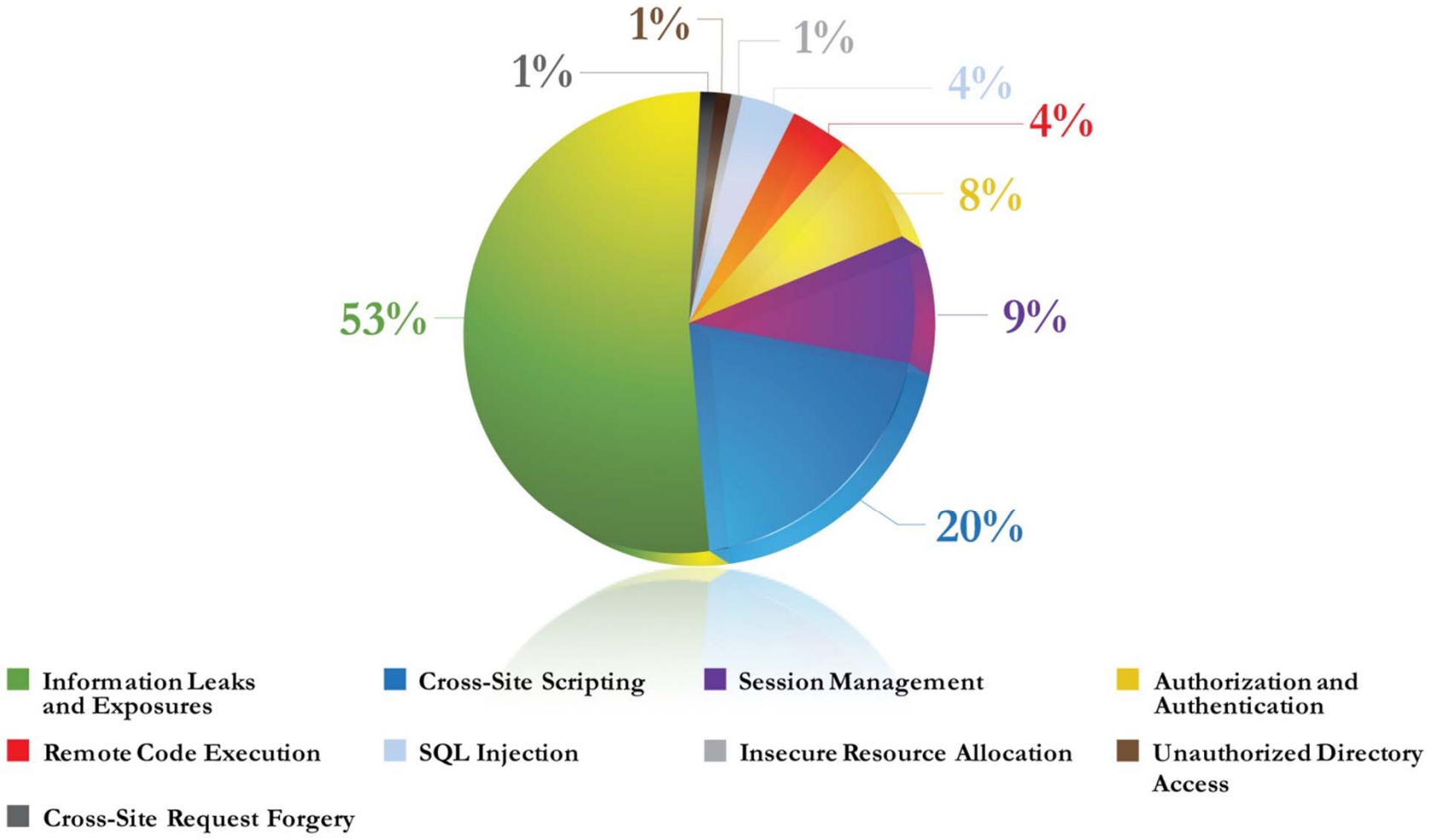
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Breakdown of the Miscellaneous Category



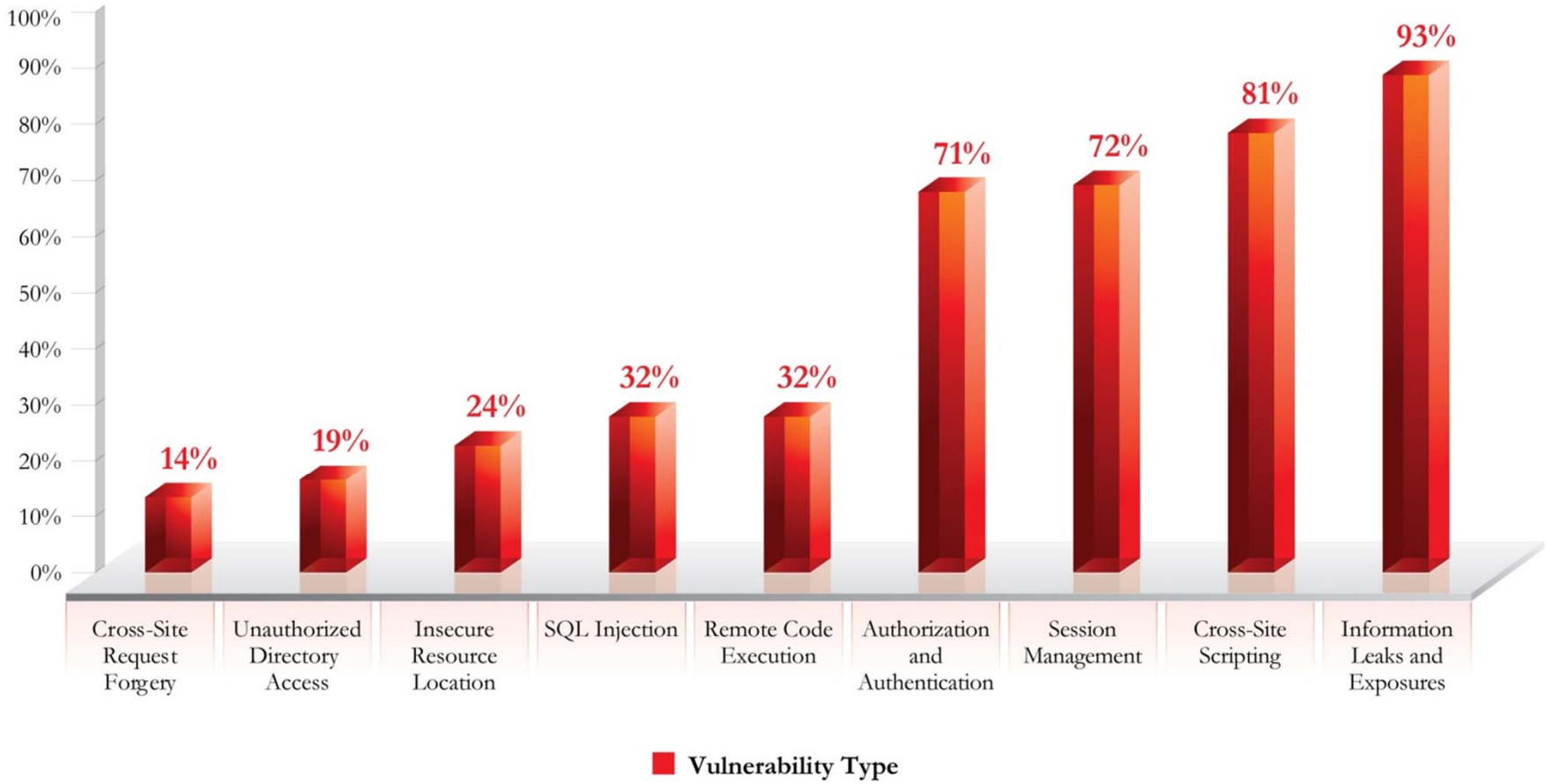
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Web Vulnerabilities by Class (proprietary applications)



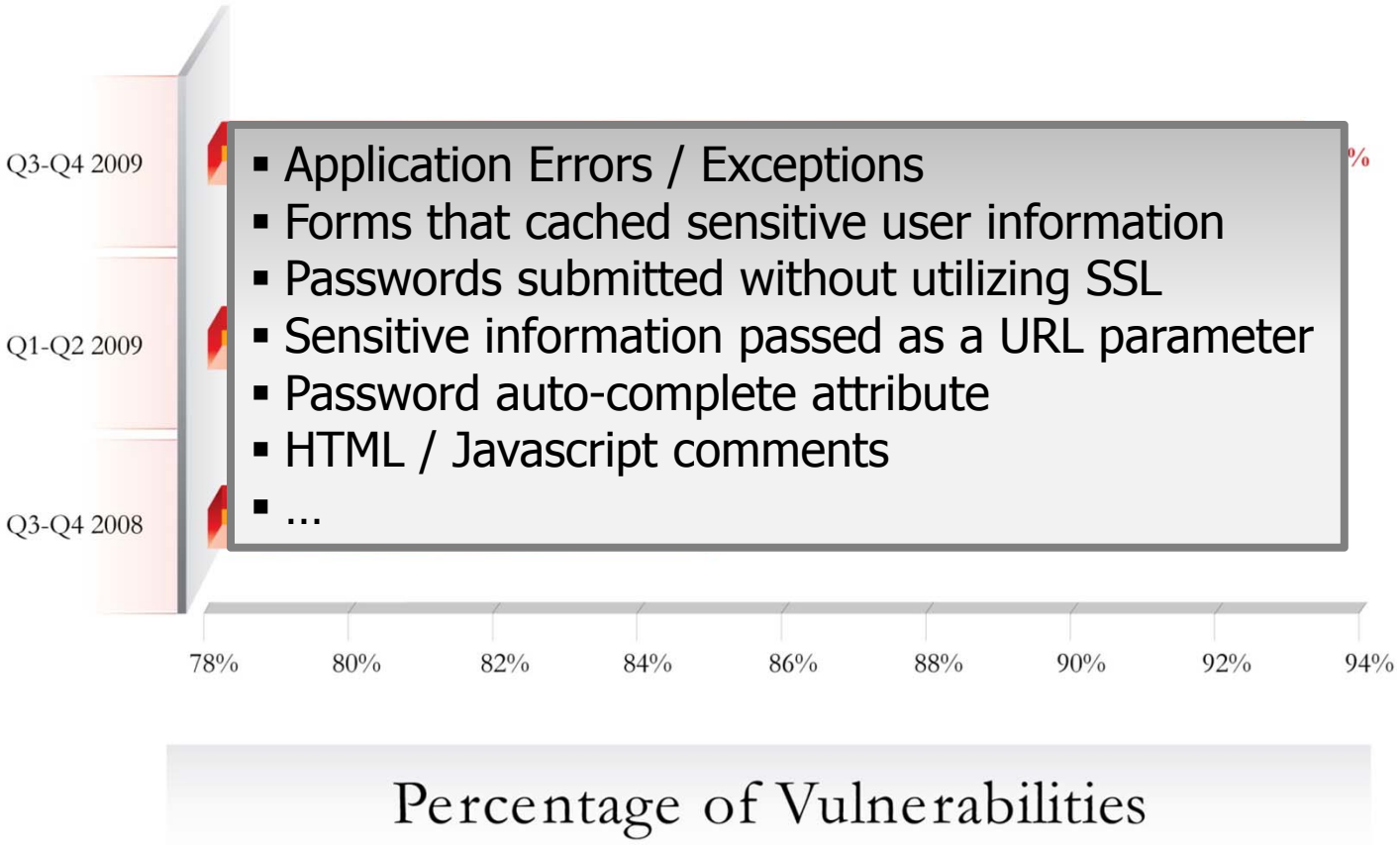
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Percentage of Applications with Vulnerability Type (proprietary apps)



Source: Cenzic Q3-Q4, 2009 Application Trends Report

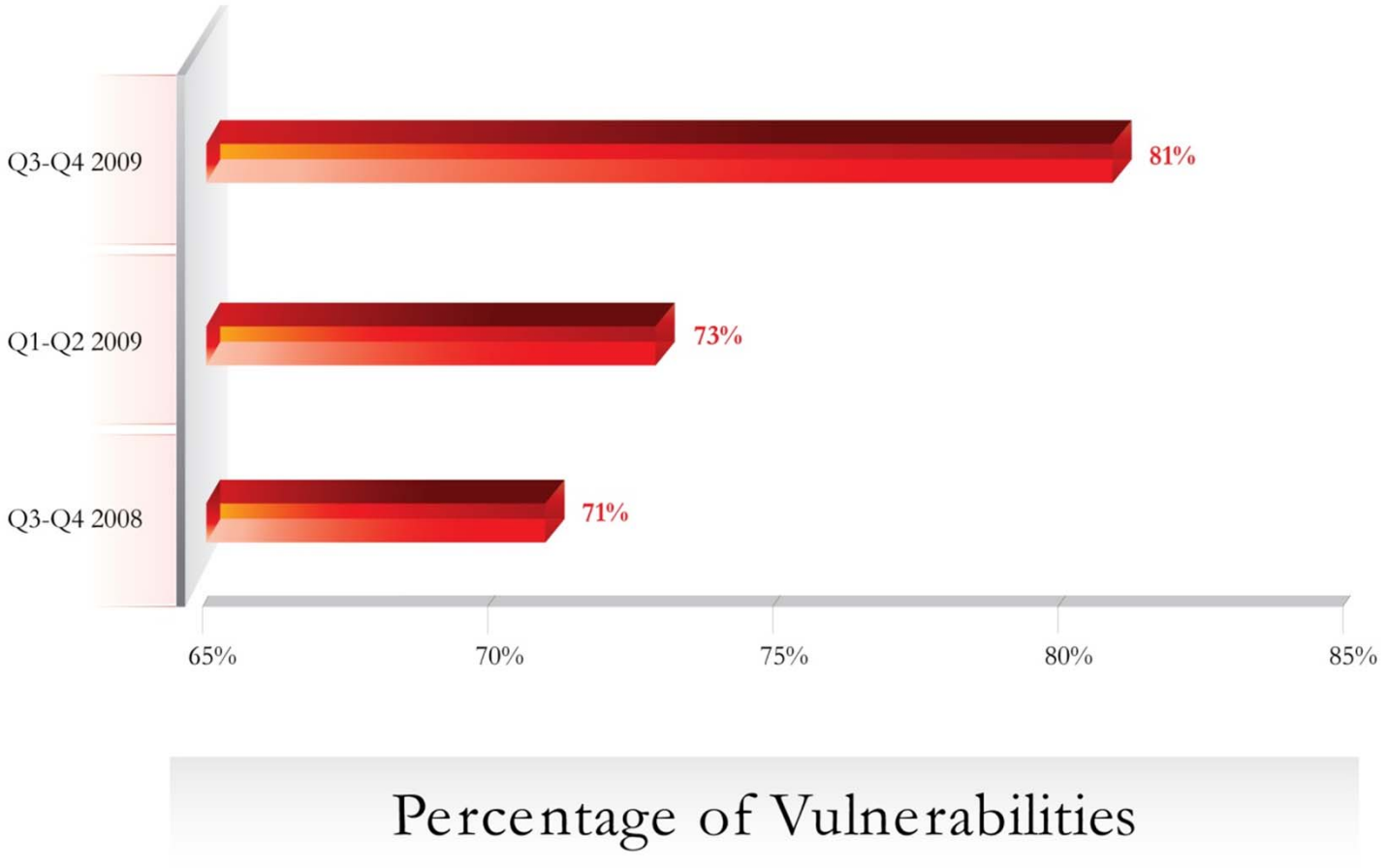
Information Leaks and Exposures (93%)



- Application Errors / Exceptions
- Forms that cached sensitive user information
- Passwords submitted without utilizing SSL
- Sensitive information passed as a URL parameter
- Password auto-complete attribute
- HTML / Javascript comments
- …

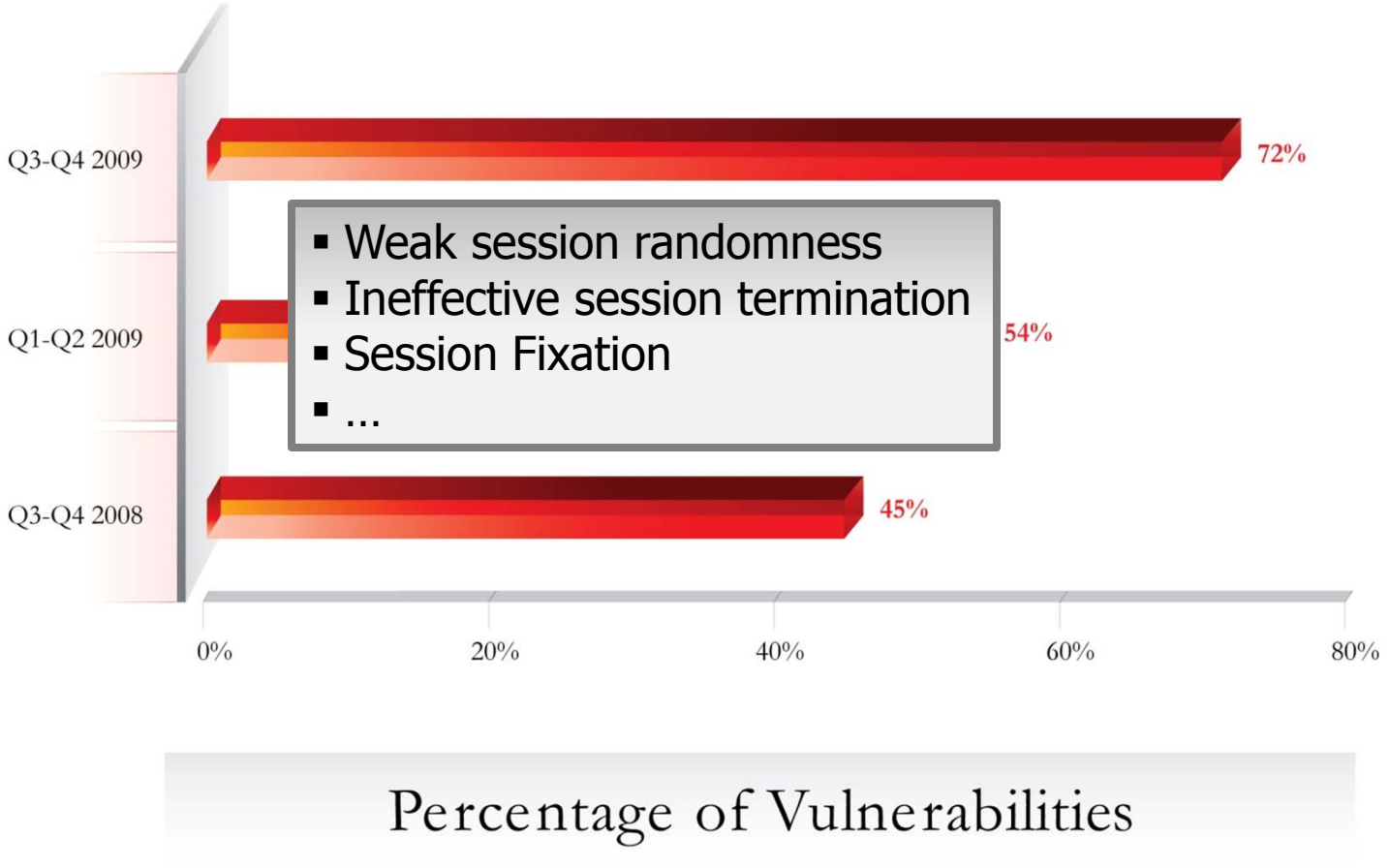
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Cross-Site Scripting (81%)



Source: Cenzic Q3-Q4, 2009 Application Trends Report

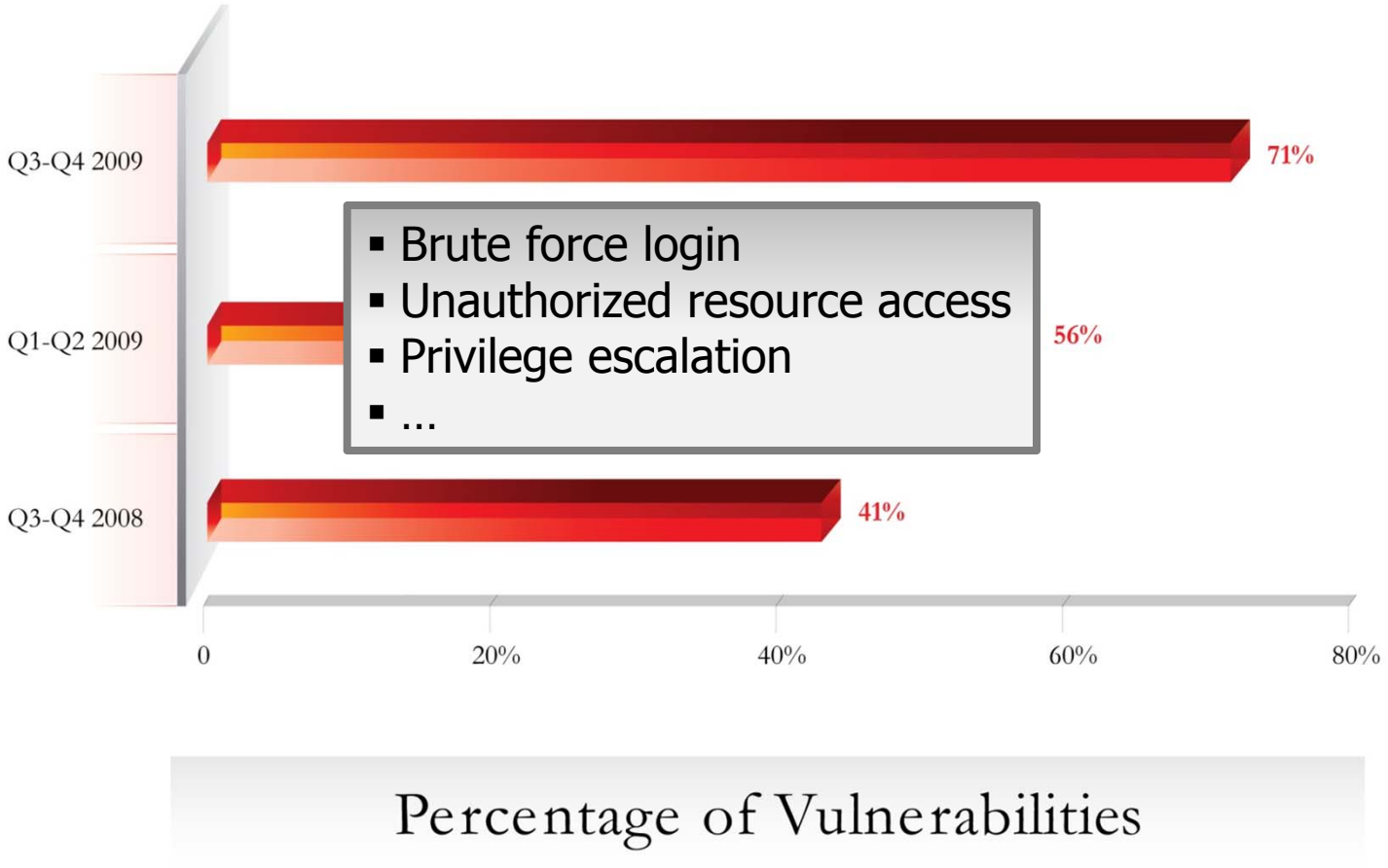
Session Management (72%)



- Weak session randomness
- Ineffective session termination
- Session Fixation
- …

Source: Cenzic Q3-Q4, 2009 Application Trends Report

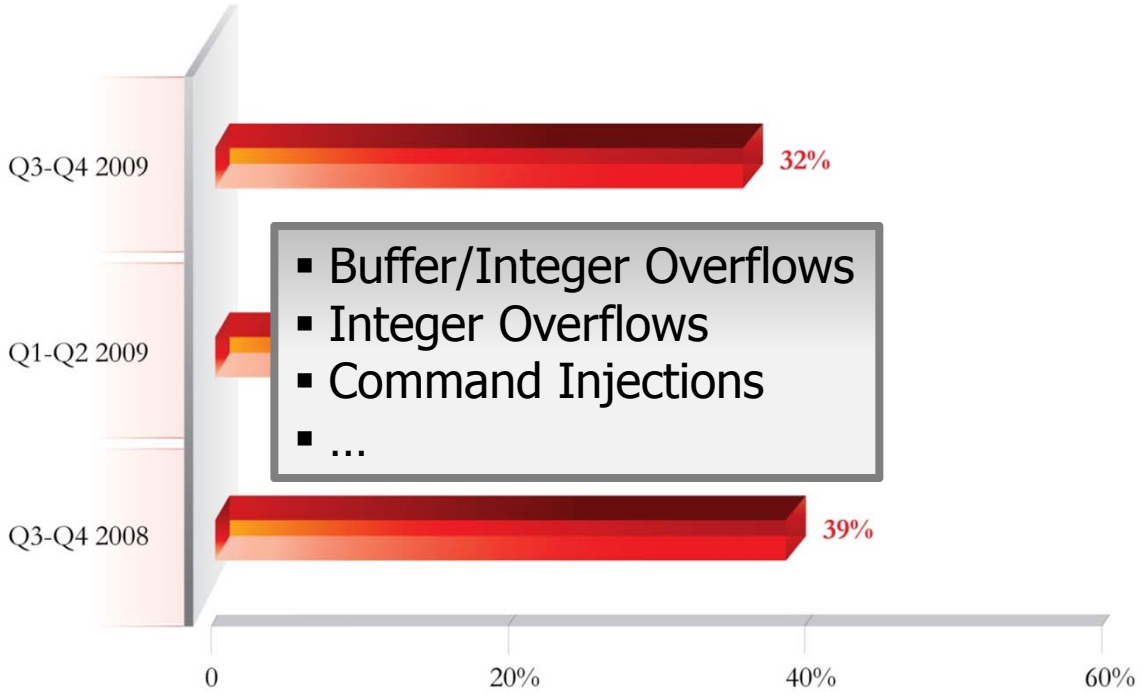
Authorization and Authentication Flaws (71%)



- Brute force login
- Unauthorized resource access
- Privilege escalation
- …

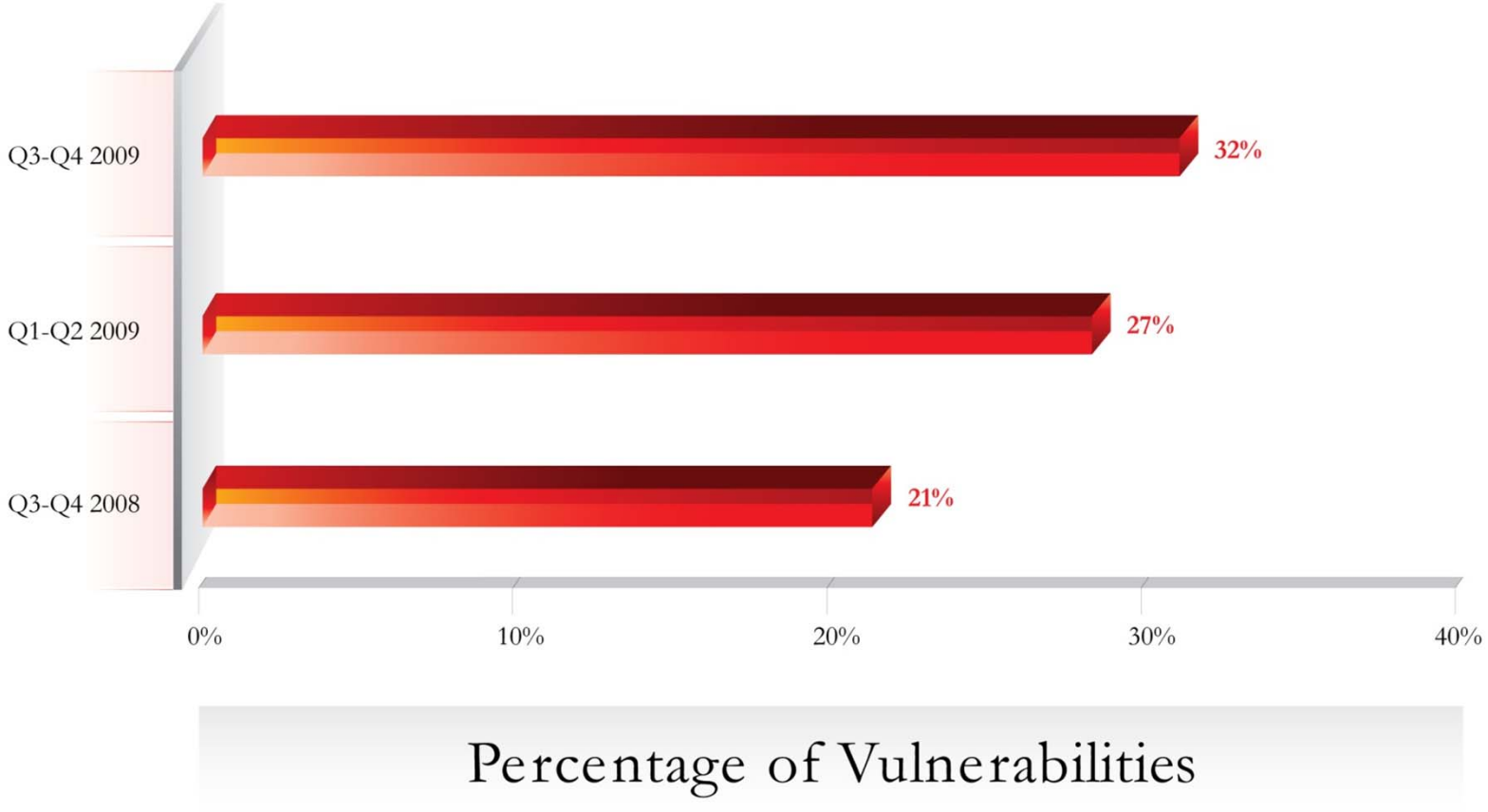
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Remote Code Execution (32%)



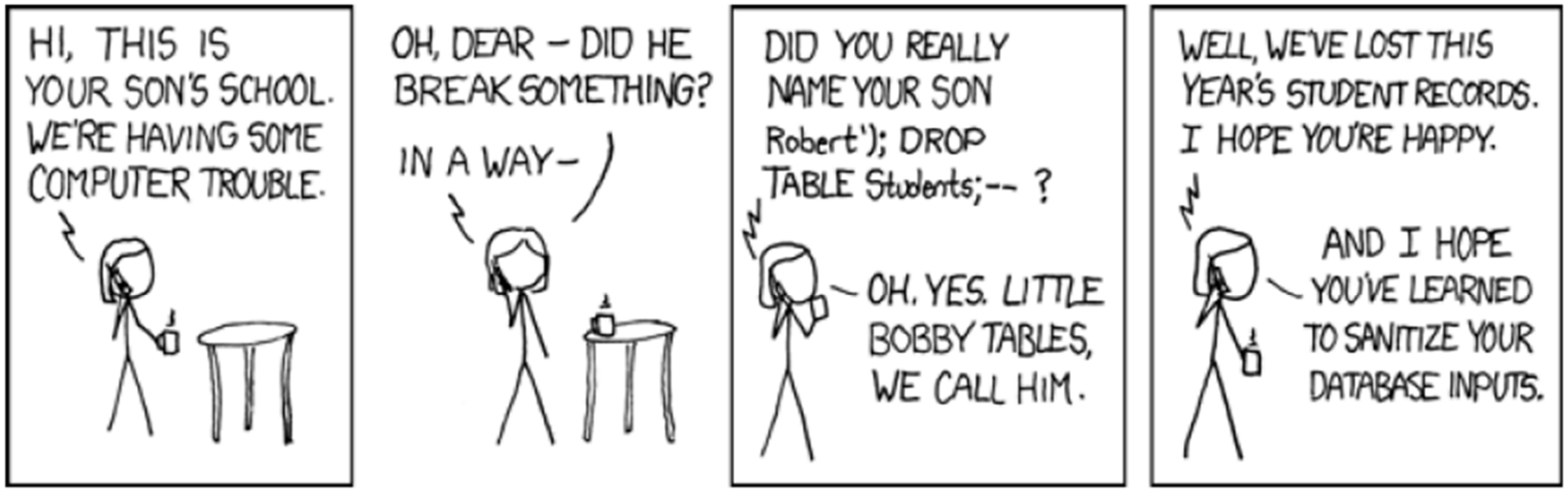
Source: Cenzic Q3-Q4, 2009 Application Trends Report

SQL Injection (32%)



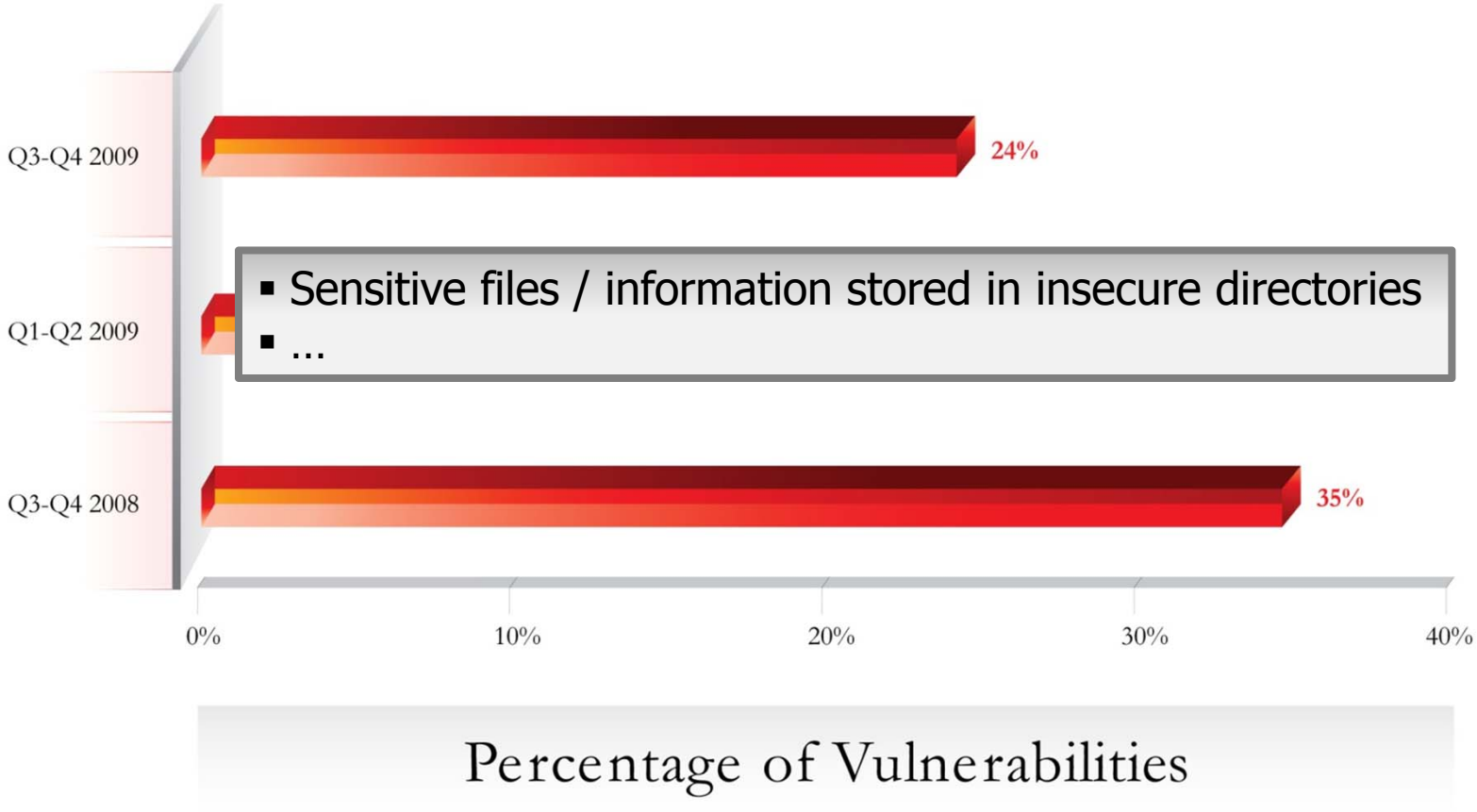
Source: Cenzic Q3-Q4, 2009 Application Trends Report

Robert'); DROP TABLE Students;--



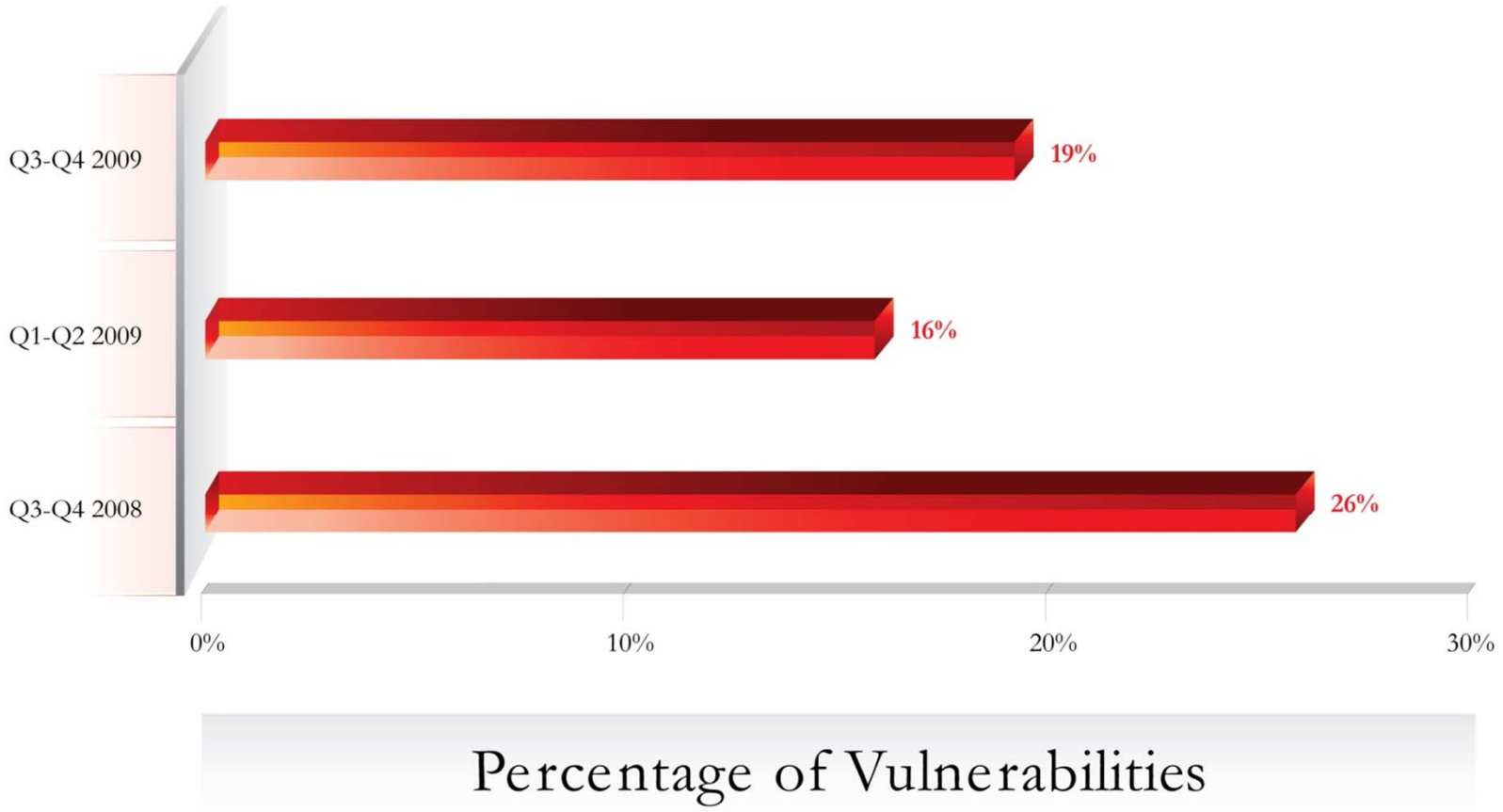
http://xkcd.com

Insecure Resource Location (24%)

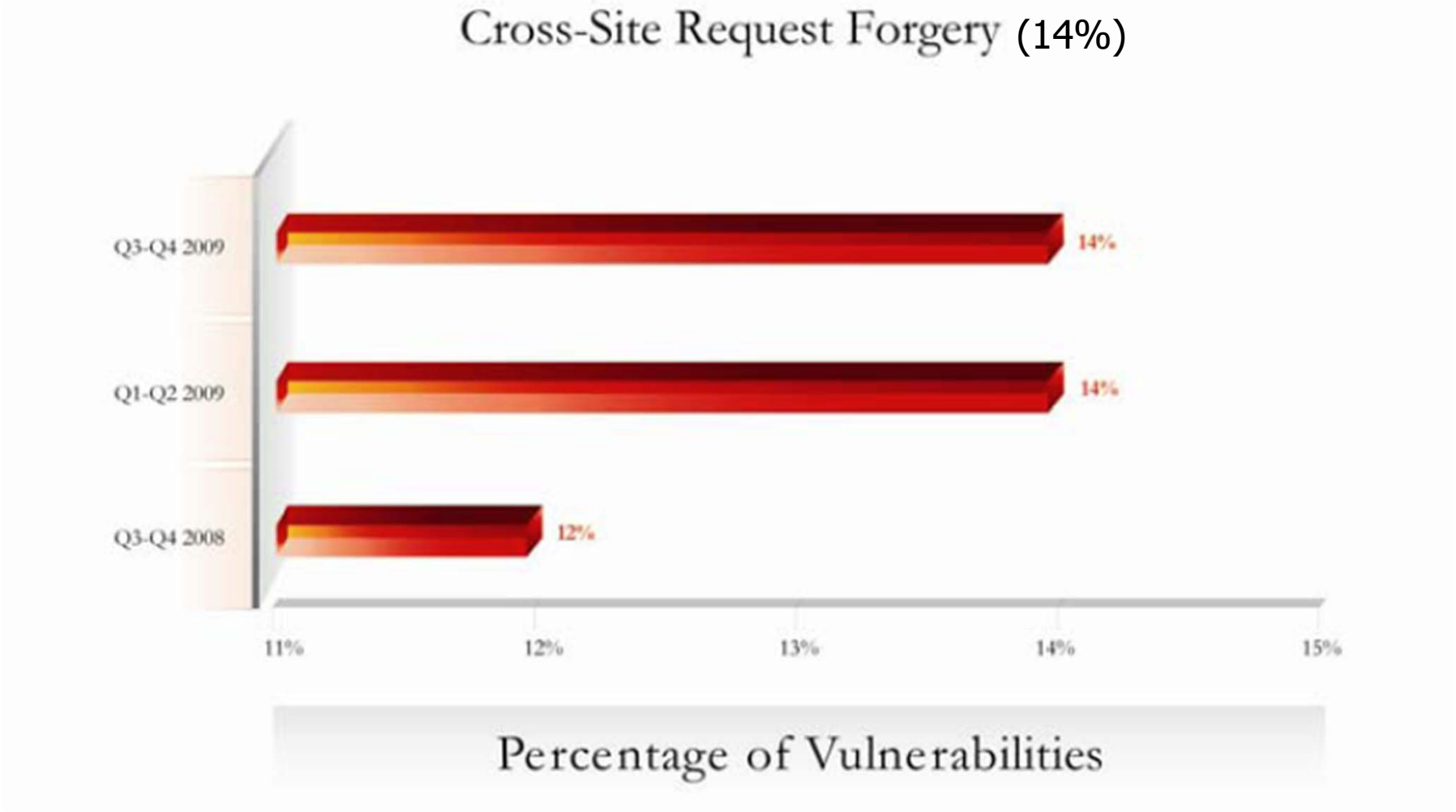


Source: Cenzic Q3-Q4, 2009 Application Trends Report

Unauthorized Directory Access (19%)



Source: Cenzic Q3-Q4, 2009 Application Trends Report

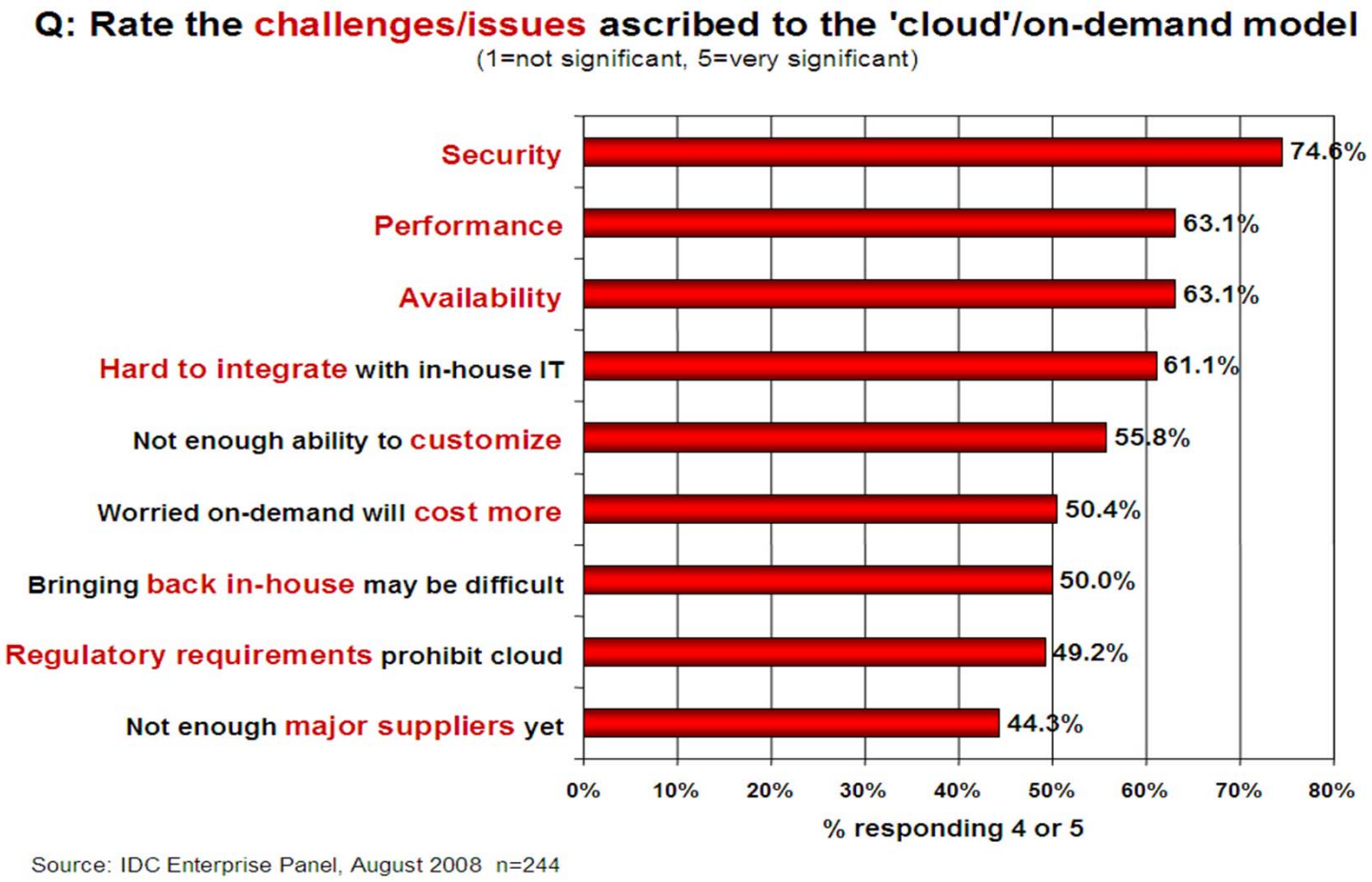


Source: Cenzic Q3-Q4, 2009 Application Trends Report

And The 6-Day Forecast?

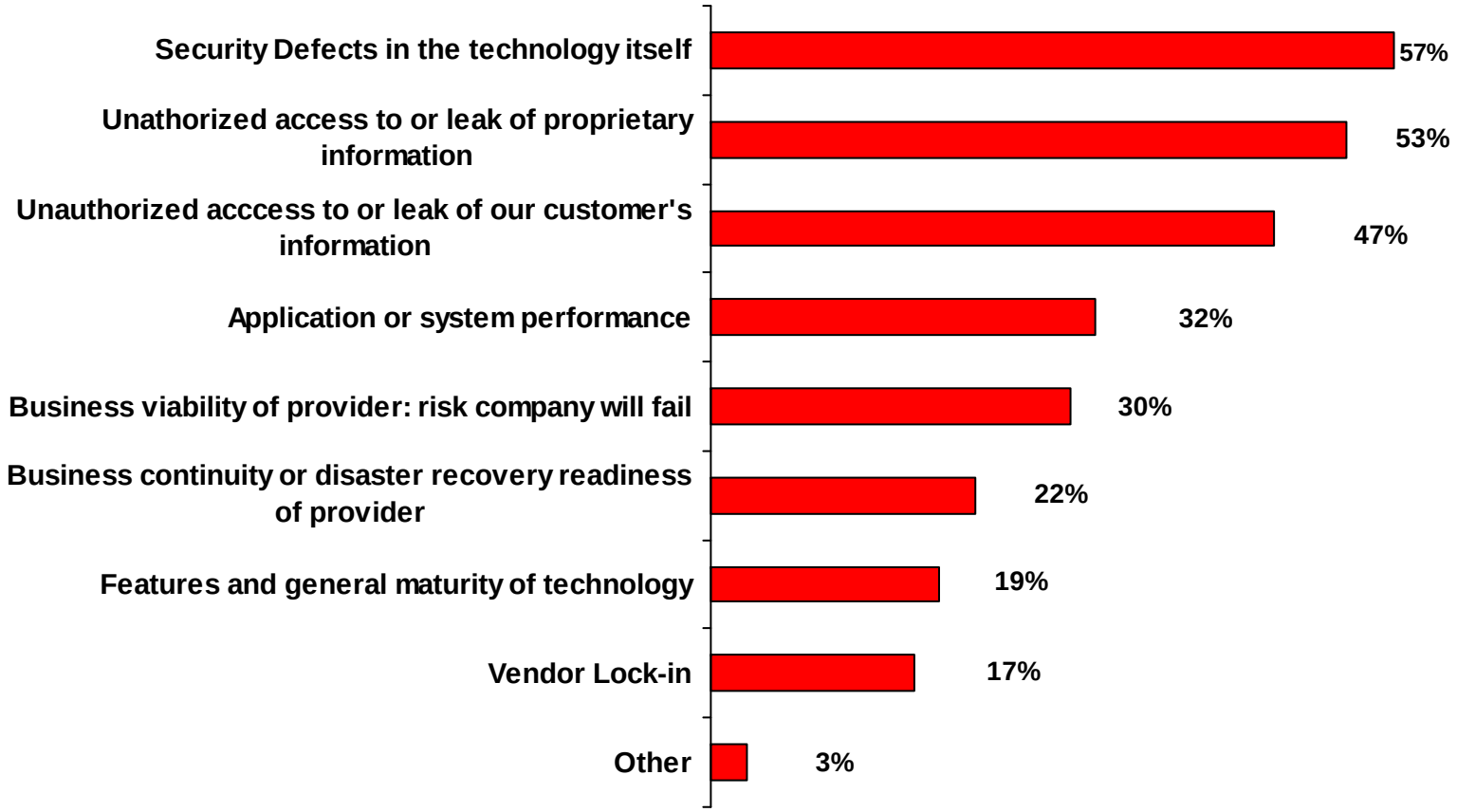
Cloud Security

Cloud Security – A Big Issue



Source: IDC Enterprise Panel, August 2008 n=244

Cloud Security – A Big Issue



Source: Information Week Analytics (547 respondents)

Cloud And Security

- Exposure is similar to any Web apps – but on a potentially massive scale
- Security boundaries and attack surfaces are often only partially understood
- Proliferation of Mashups and 'open' APIs that favor 'experience' over security
- Does security ownership transfer to the cloud infrastructure / platform provider?
- What happens in case of a breach? Who's responsible?
- Often organizations are still figuring out the "Functionality / Usability" aspects of their cloud strategy…

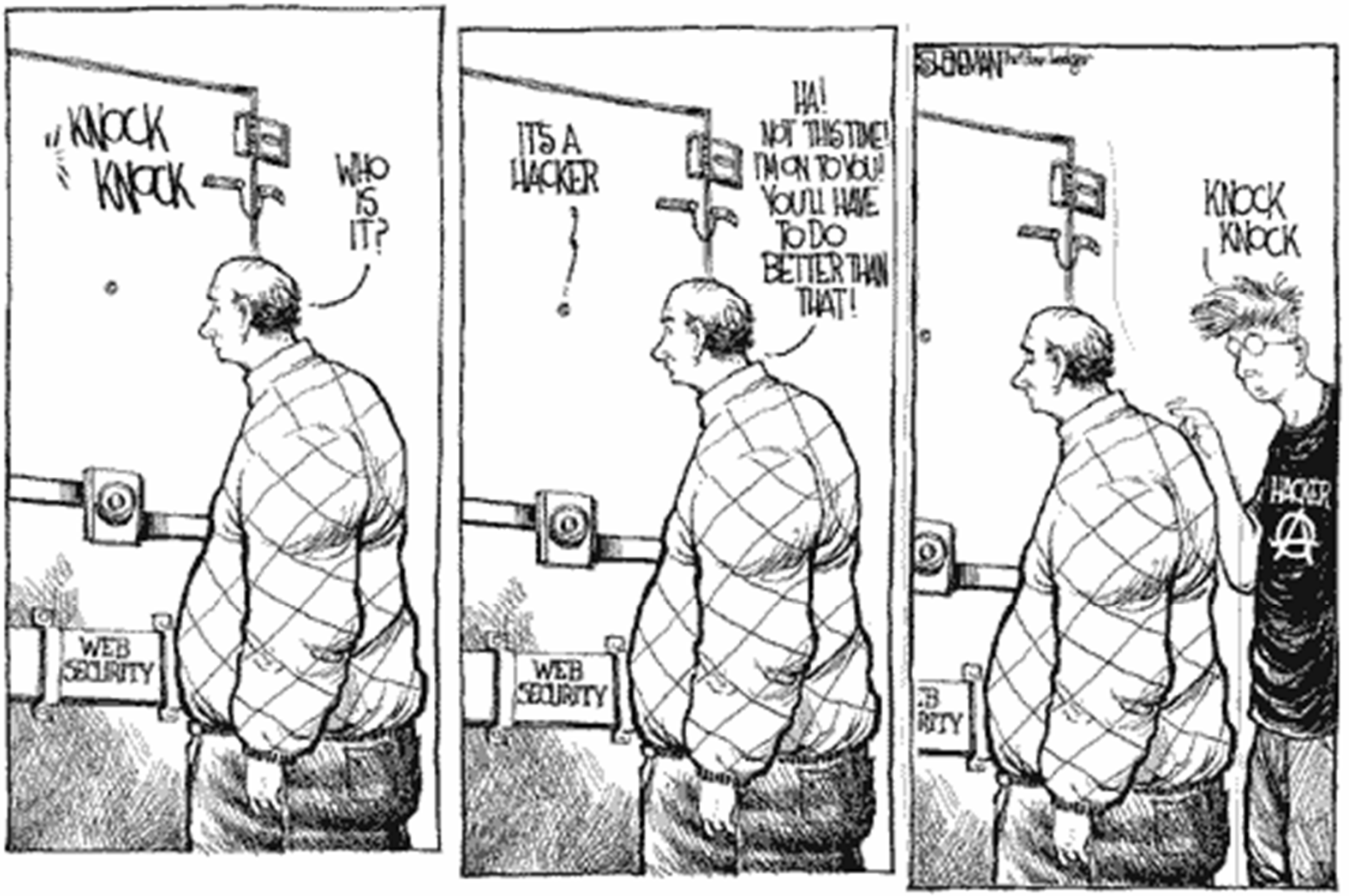
"Security is usually the last component added to any new technology, and cloud computing is no exception." – ***Mark Nicolett, Gartner***

Top 5 Myths of Web Application Security

1. **We use SSL so that'll protect my Web site**
   - SSL ≠ App Security
2. **We have never been hacked**
   - How do you know?
3. **We're PCI compliant**
   - Heartland, Hannaford…
4. **We test some of our Web applications once a year**
   - Any vulnerable site is your weakest link
5. **Too expensive**
   - Many flexible options to get you jump started

Learn more: App Security MythBusters Videos
http://www.cenzic.com/resources/videos/mythbusters/

The Hacker World



Hackers: What Motivates Them?

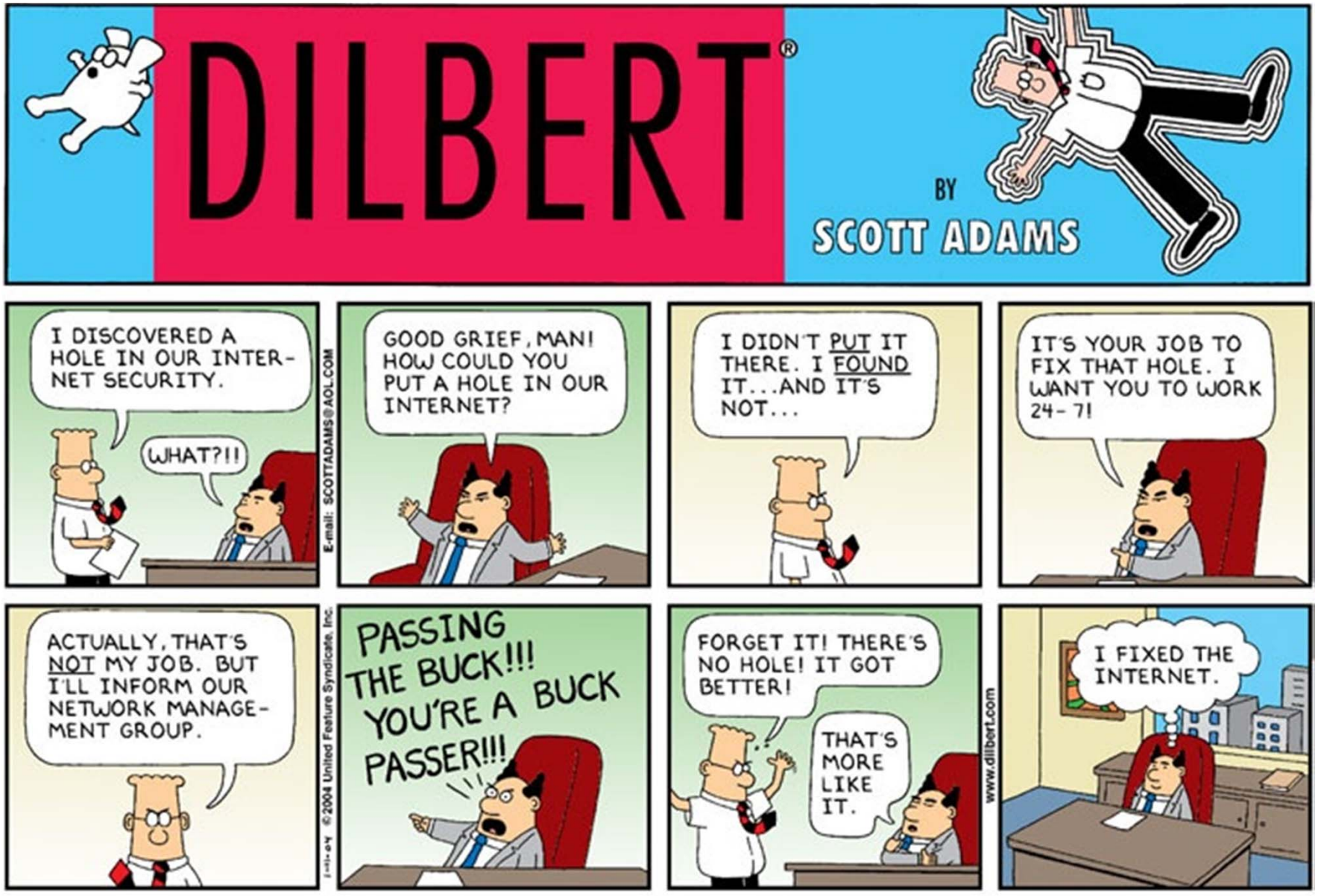
- Hackers stole $1.2 million in 30 minutes from Sugarland Corporation & $9M in a few hours from RBS World Pay
- Hackers get paid ~ $10,000 / week

Avg Rates Hackers Get for Stolen Information, Symantec Threat Report – 2009

Overall Rank 2009	2008	Item	Percentage 2009	2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Why So Little Industry Progress?

- Functionality & Usability tend to almost always win over security
- Time-to-market is the name of the game
- Security continues to be an afterthought
- Very limited security related education
- Experts are still hard to find (compared to other disciplines)
- Many organizations still struggle to find a scalable and persistent security approach
- Stakeholders still "don't always get it" …


DILBERT®
BY
SCOTT ADAMS
I DISCOVERED A HOLE IN OUR INTERNET SECURITY.
WHAT?!!
E-mail: SCOTTADAMS@AOL.COM
GOOD GRIEF, MAN! HOW COULD YOU PUT A HOLE IN OUR INTERNET?
I DIDN'T PUT IT THERE. I FOUND IT...AND IT'S NOT...
IT'S YOUR JOB TO FIX THAT HOLE. I WANT YOU TO WORK 24-7!
ACTUALLY, THAT'S NOT MY JOB. BUT I'LL INFORM OUR NETWORK MANAGEMENT GROUP.
©2004 United Feature Syndicate, Inc.
PASSING THE BUCK!!! YOU'RE A BUCK PASSER!!!
FORGET IT! THERE'S NO HOLE! IT GOT BETTER!
THAT'S MORE LIKE IT.
www.dilbert.com
I FIXED THE INTERNET.

How To Best Dress For Bad Weather

Best App Security Practices

- Analyze and know your security boundaries and attack surfaces
- Beware of reliance on client-side security measures
  - Always implement strong server side input & parameter validation (black & whitelisting)
  - Test against a robust set of evasion rules
  - Remember: The client can never be trusted!
- Assume the worst case scenario for all 3rd party interactions
  - 3rd parties can inherently not be trusted!

Best App Security Practices (contd.)

- Implement anti-CSRF defenses
- Escape special characters before sending them to the browser (e.g. < to `<`)
- Leverage HTTPS for sensitive data, use `HTTPOnly` & `Secure` cookie flags
- Use parameterized SQL for any DB queries
- Implement a comprehensive, solid exception handling architecture
- Don not disclose any stack trace, debug log, or path information or failed SQL statements to users
- Use strong tokens with strong randomness

Best App Security Practices (contd.)

- Implement a comprehensive, solid exception handling architecture
  - Default error handler which returns sanitized error message for all error paths
  - Do not disclose any stack trace, debug log, or path information or failed SQL statements to users

Best App Security Practices (contd.)

- Beware of weak / faulty session management
  - Use strong authentication mechanism (e.g. two factor)
  - Implement strong session termination / logout mechanism
  - Avoid weak passwords & weak change / forgot password mechanisms
  - And always remember: The strongest authentication won't help if session management vulnerabilities exist!

Best App Security Practices (contd.)

- Beware of weak / faulty session management (contd.)
  - Implement strong logout functionality (with invalidation of session tokens & deletion of session & state on server
  - Implement session expiration with same results as strong logout (after e.g. 5 or 10 minutes)
  - Ideally do not allow concurrent logins
  - Terminate sessions when attacks are detected
- **Also see owasp.org and OWASP dev guide**

Security In The Real World ...

It's true, you might not be able to outrun the bear, but let's not forget, all you have to do is outrun your competition!

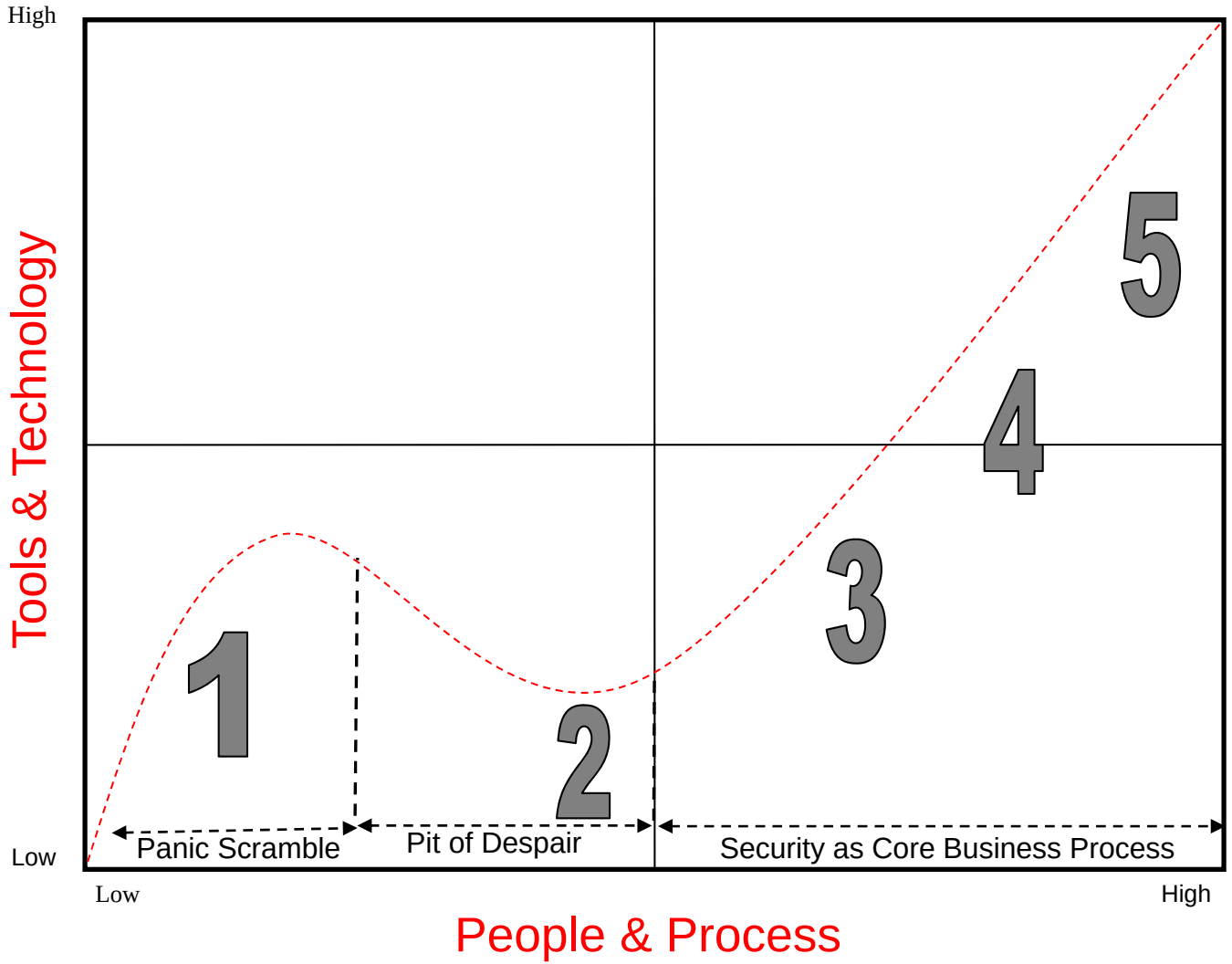
Things to Remember

- Attackers can be extremely creative and overcome various defense mechanisms
- Never assume you're safe just because you've implemented a few basic defenses
- Never underestimate your opponent!

Web Security Matrix - Goal: Attain Stage 5

	Areas of Testing / People involved	# of Attacks	Testing Freq
1	No areas tested > No People	N/A	N/A
2	Intermittent testing of Dev, QA >> InfoSec (or just 1 person)	Basic 5 – 10 attacks	Test once or twice
3	Dev / QA Tested, Testing pre-prod apps > InfoSec, Mgmt (few people)	Intrusive attacks	Test every year
4	Dev, QA & Safe testing of Production apps > Execs, InfoSec, Dev (more people, but no standardization)	Infrastructure + (non)-intrusive	Testing every 6 mo
5	Dev, QA, and full production Tested > Execs, InfoSec, Dev, QA (most of the company is security driven)	Application logic tests + all others	Continuous Testing / monthly

Application Security Maturity Model

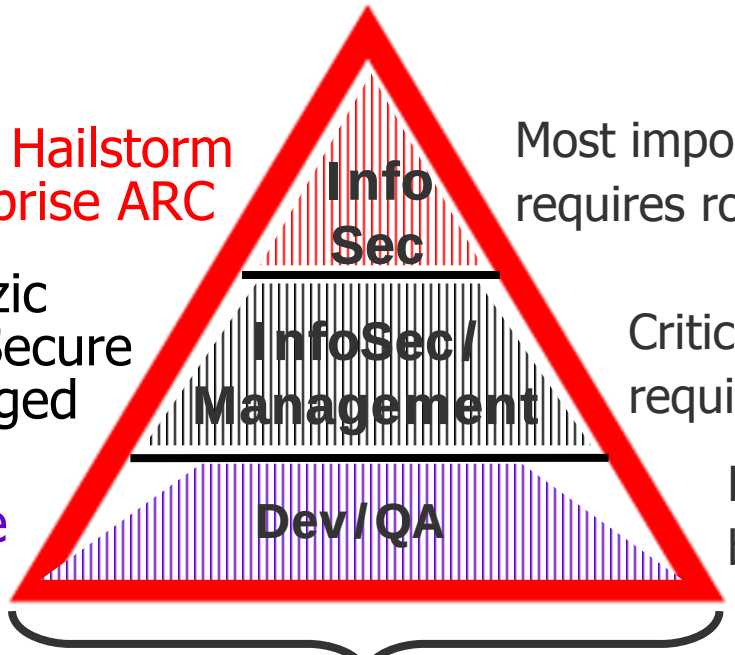


3 Products
1 Risk Management Dashboard

Cenzic Hailstorm Enterprise ARC

Cenzic ClickToSecure Managed

Cenzic ClickToSecure 'Self-Service'



Most important & complex apps; requires robust testing

Critical apps that are less complex; requires medium testing

Less critical apps (i.e. internal), but still require basic testing

Persistent security approach saves money and reduces risk

All results viewed in the ARC Dashboard

Risk Management Dashboard

Tells which apps have been tested

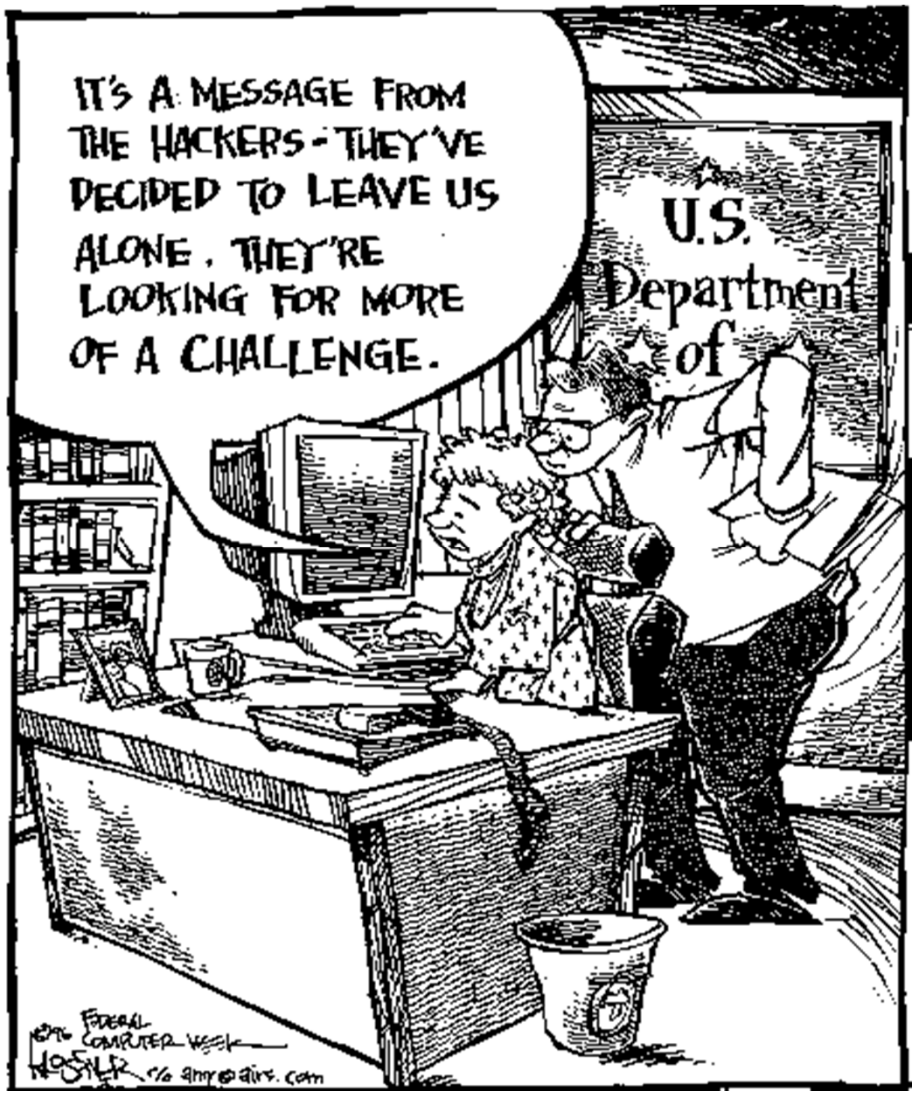
Web Interface

Tells vulnerability levels

Finds and lists all applications

Quantitatively tells how severe the risk is for each app

Sophistication of Hackers ...



Meets Unprepared Users ...