A Discussion of Breach Reports

Ronald Woerner, CISSP

Cyber Security Forum, 20 May 09

NEbraskaCERT

What you need to know

- This is a discussion, not a lecture.

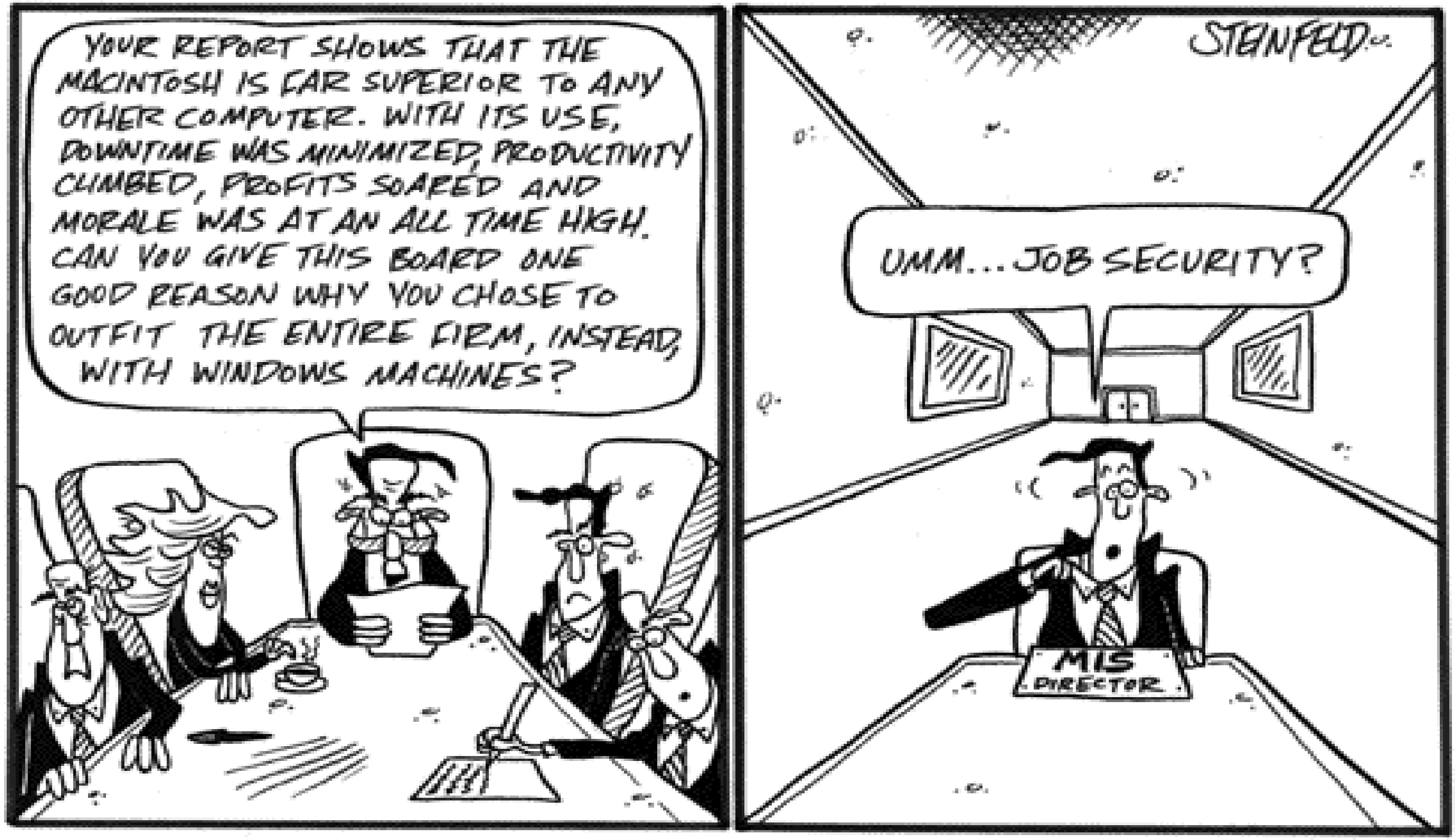
  ASK QUESTIONS!

  (but if you talk too long, you will be asked to speak at future CSF's or NebraskaCERT Conference)
- This is my interpretation, not anyone associated with me.
- I stole this material from many sources including:
  - Verizon Business Services and Dr. Peter Tippett's speech at RSA 2009.
  - Ponemon institute
  - WhiteHat Security

DOOMED

Please put your trays in the upright and locked position.

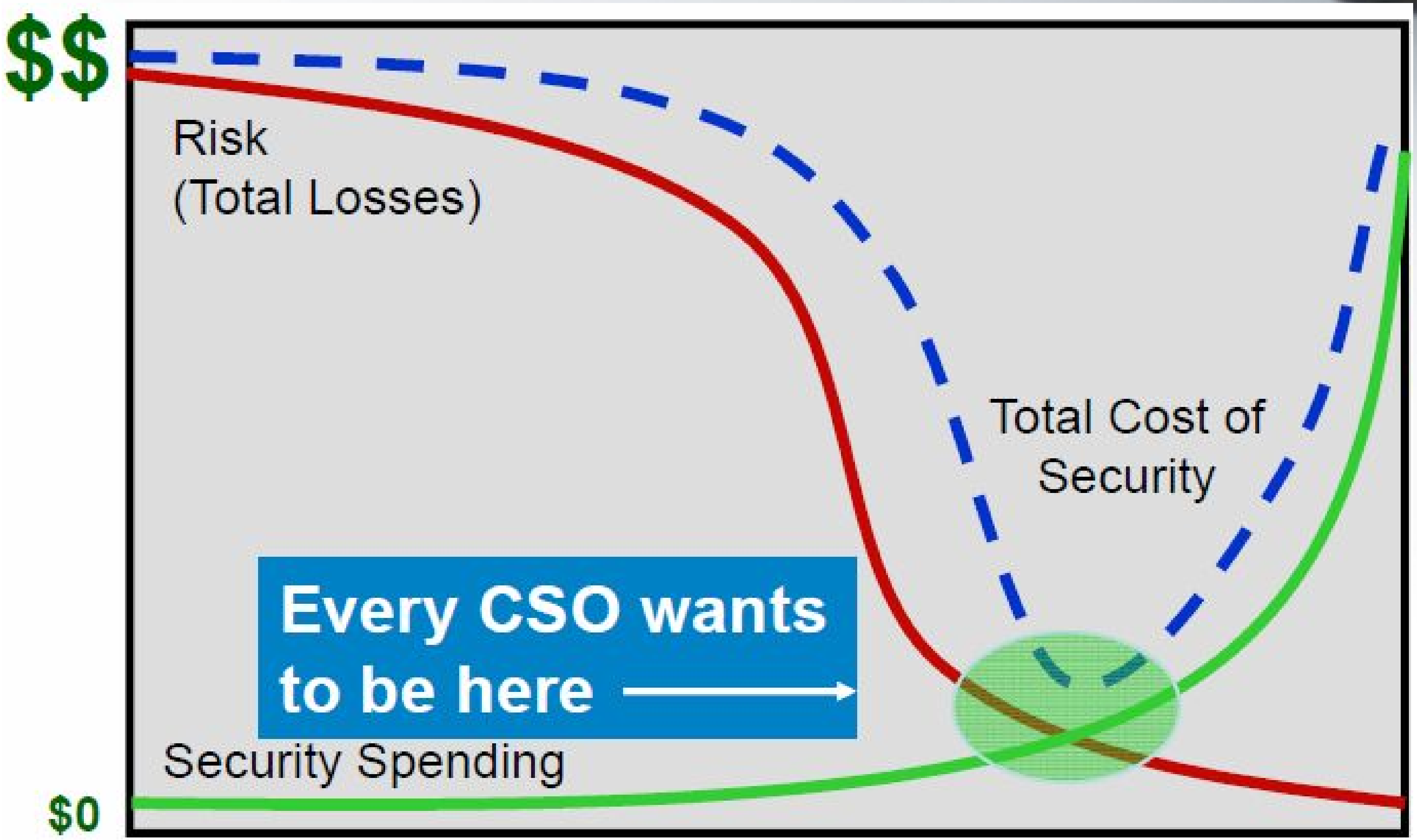
The Good News…


YOUR REPORT SHOWS THAT THE MACINTOSH IS FAR SUPERIOR TO ANY OTHER COMPUTER. WITH ITS USE, DOWNTIME WAS MINIMIZED, PRODUCTIVITY CLIMBED, PROFITS SOARED AND MORALE WAS AT AN ALL TIME HIGH. CAN YOU GIVE THIS BOARD ONE GOOD REASON WHY YOU CHOSE TO OUTFIT THE ENTIRE FIRM, INSTEAD, WITH WINDOWS MACHINES?
STEINFELD
UMM... JOB SECURITY?
MIS DIRECTOR

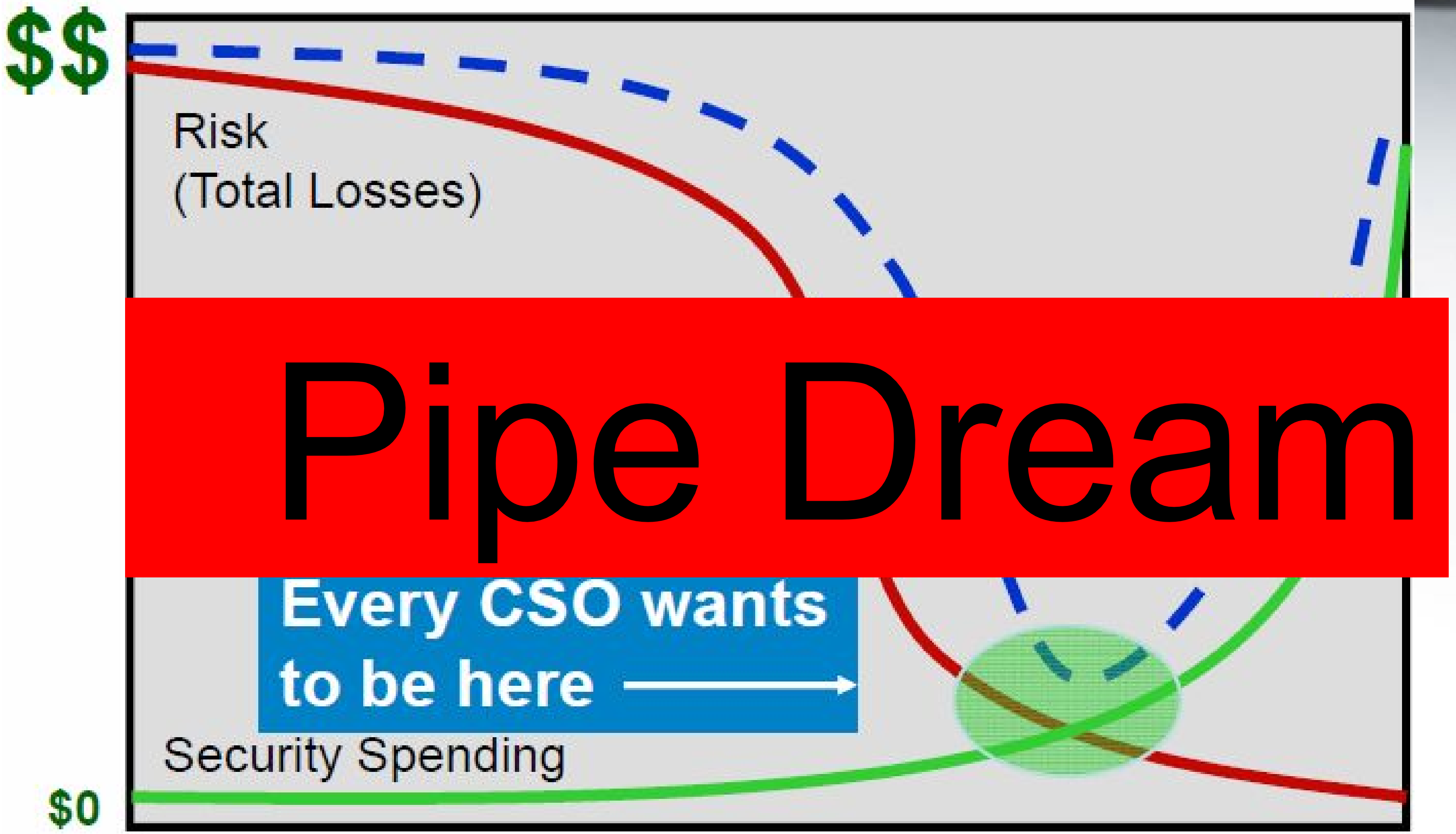
The Important Question

Can we improve decisions with imperfect data?

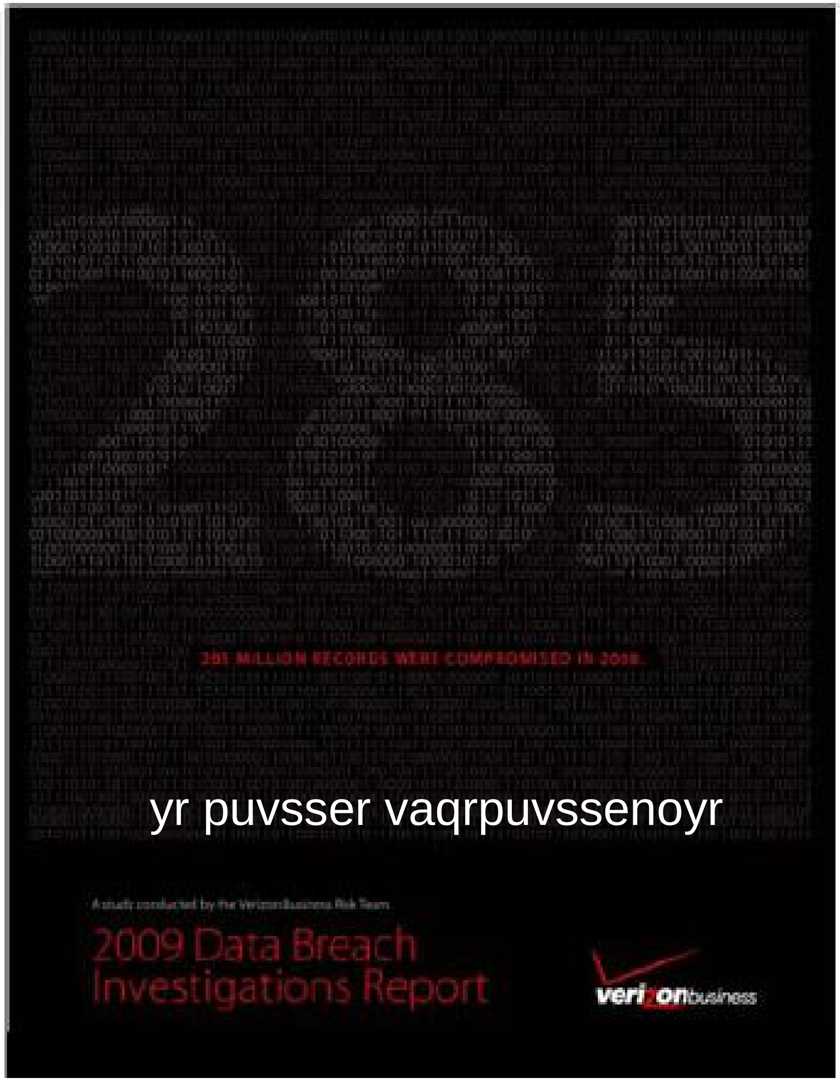
Managing Information Risk



Managing Information Risk



2009 Data Breach Investigations Report



285 MILLION RECORDS WERE COMPROMISED IN 2008.

yr puvsser vaqrpuvssenoyr

A study conducted by the Verizon Business Risk Team

2009 Data Breach Investigations Report

verizonbusiness

http://www.verizonbusiness.com/products/security/risk/databreach/

True Statement

The road to the (Verizon) Data Breach Investigations Report did not start out with the desire to create a report. It started with the desire to have data to better understand and manage risk.

2009 DBIR: Caseload Overview

All data collected during cases worked by the Verizon Business Investigative Response team during 2008

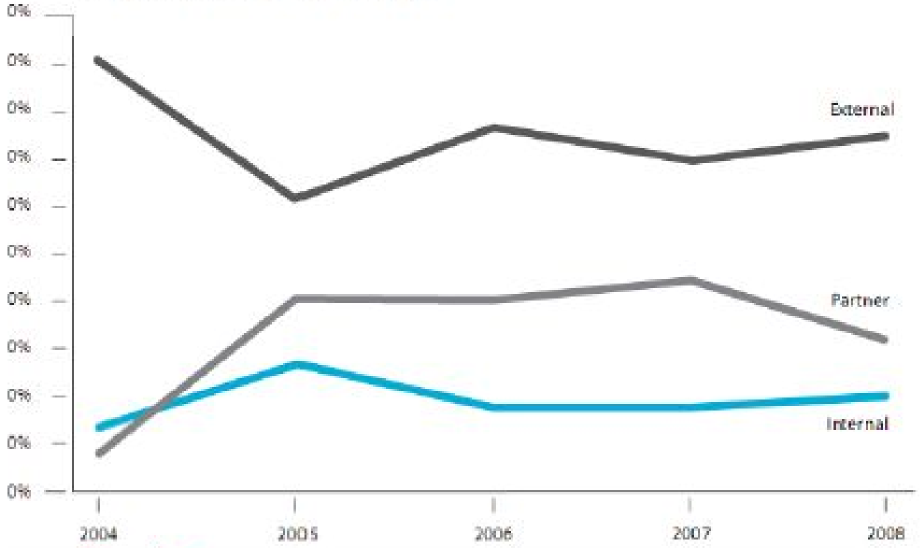
- Objective, credible, first-hand information on actual breaches

2008 Caseload:

- 90 confirmed breaches (>150 total engagements)
- 285 million compromised records (confirmed – not “data-at-risk”)
- 1/3 of these cases have been publicly disclosed (so far)
- About 50% of caseload comprised of sets of interrelated incidents
  - Same attacker(s), shared connections, identical circumstances, etc
- 15 arrests (and counting)
- 31% Retail, 30% Financial, 14% Food&Bev, Remaining mixed
- Over 1/3 of investigations conducted outside the US

Breach Sources

- External sources
  - Most breaches, nearly all records
  - 90+% of breached records attributed to organized crime activity
- Internal sources
  - Roughly equal between end-users and admins
- Partner sources



verizonbusiness

Likelihood

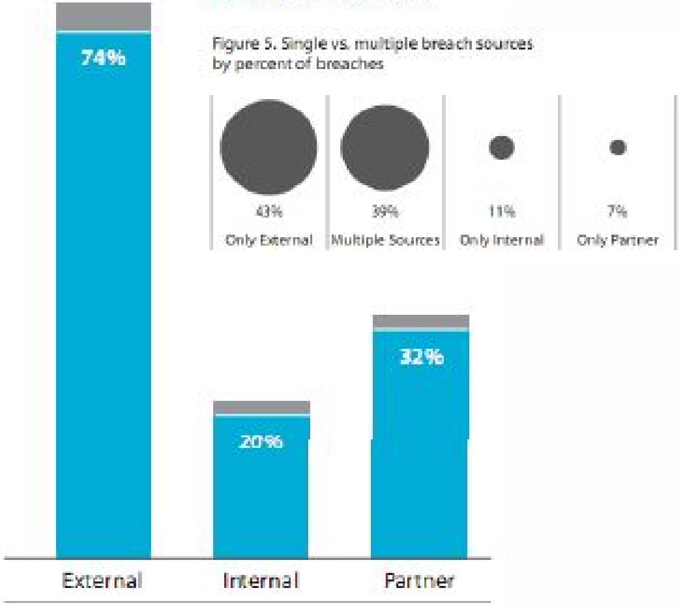
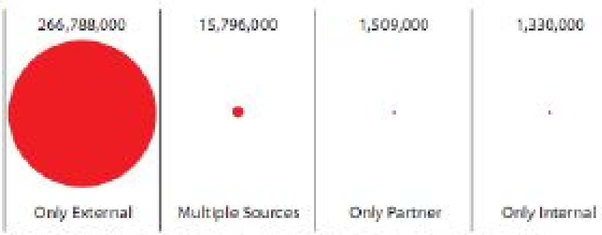


Figure 5. Single vs. multiple breach sources by percent of breaches

Impac

Figure 8. Total records compromised by source



Ponemon Study:

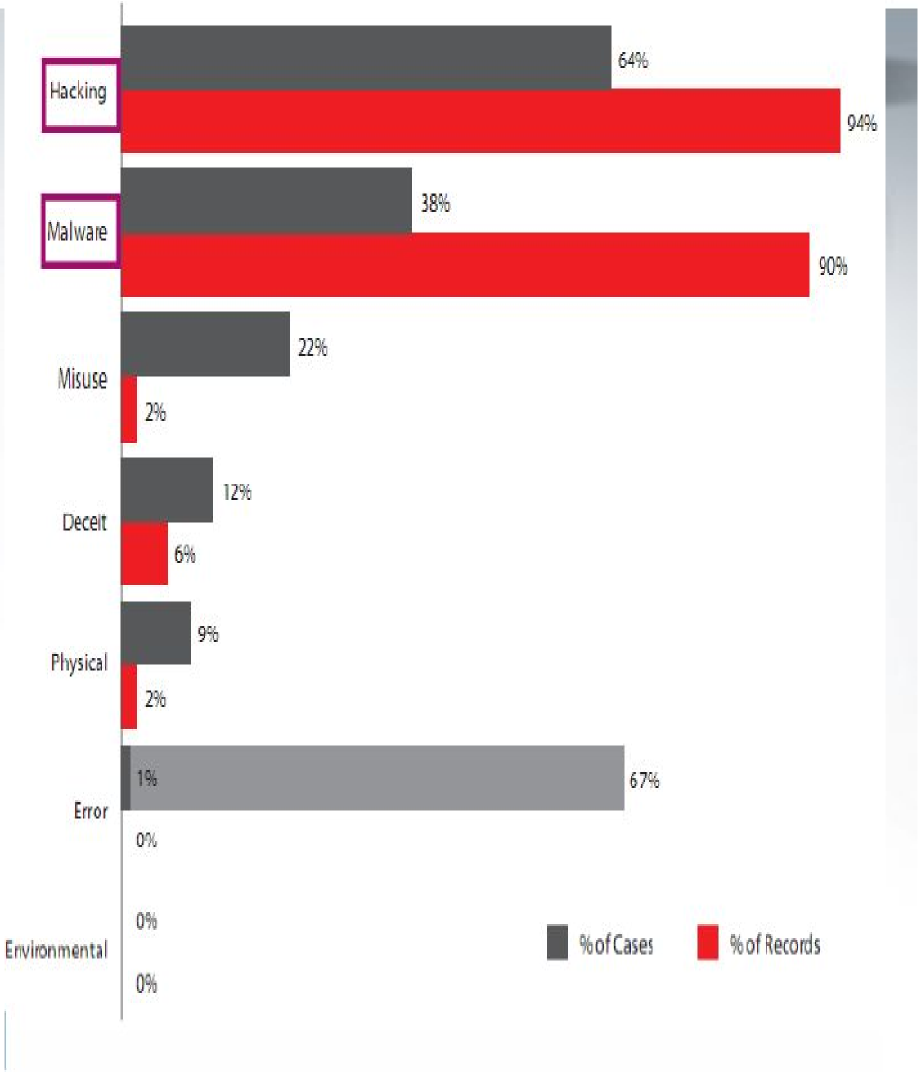
Data Loss Risks During Downsizing

- 59% of employees who leave or are asked to leave are stealing company data;
- 79% of these respondents admit that their former employer did not permit them to leave with company data;
- 67% of respondents used or are planning to use their former company’s information on a new job;

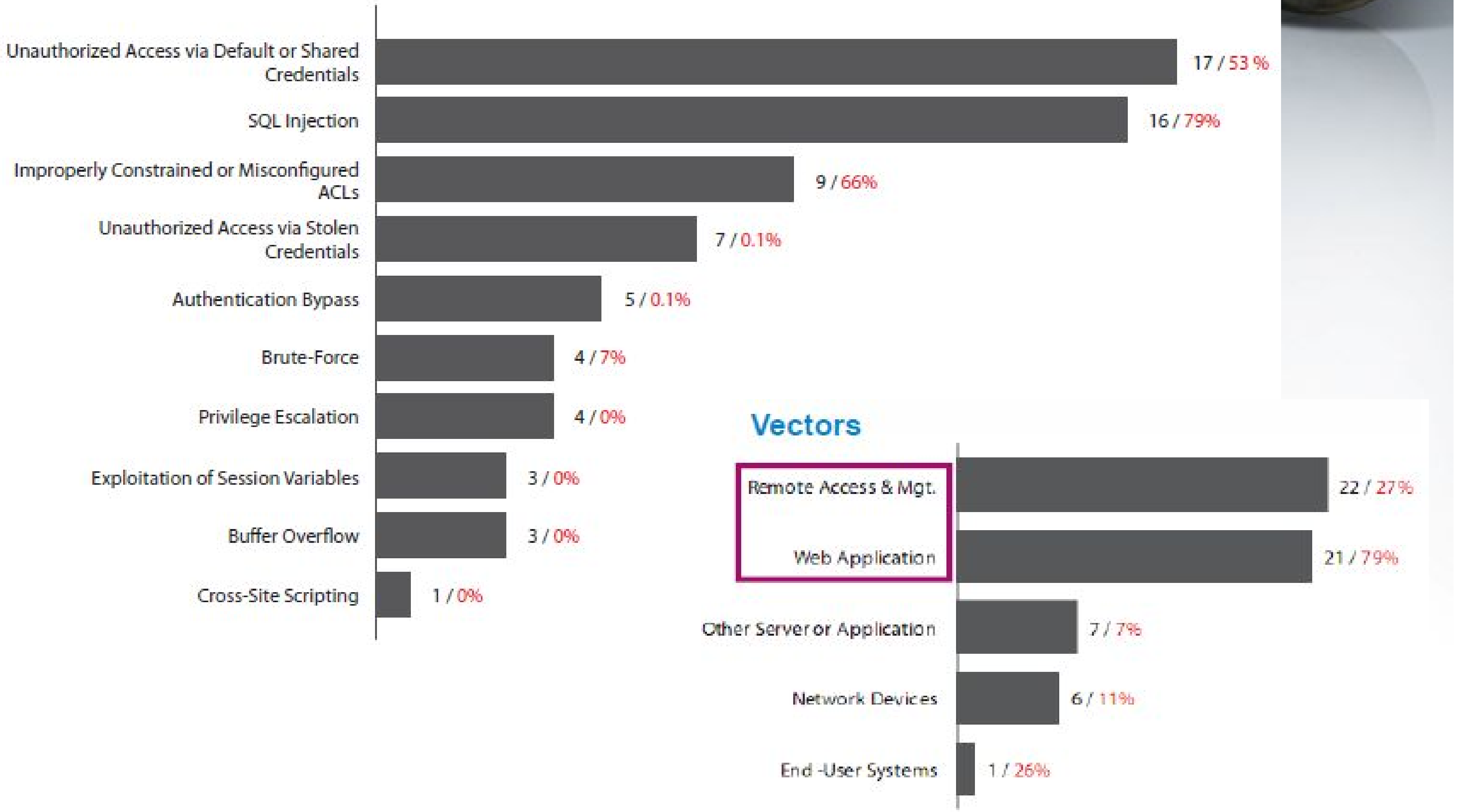
http://tinyurl.com/qecpgj

Threats and Attacks

- Similar to previous 4 years for breach percentages
- Most breaches and records linked to Hacking & Malware
- Misuse is fairly common
  - Mostly admin abuse
- Deceit and social attacks
  - Involved a range of methods, vectors, and targets
- Physical attacks
- Represent minority of caseload
- Portable media in one case (but not essential to breach)
- Error is extremely common
  - Rarely the direct cause
  - Usually contributing factor (67%)



Breakdown of Hacking (64%)



Misuse and Abuse

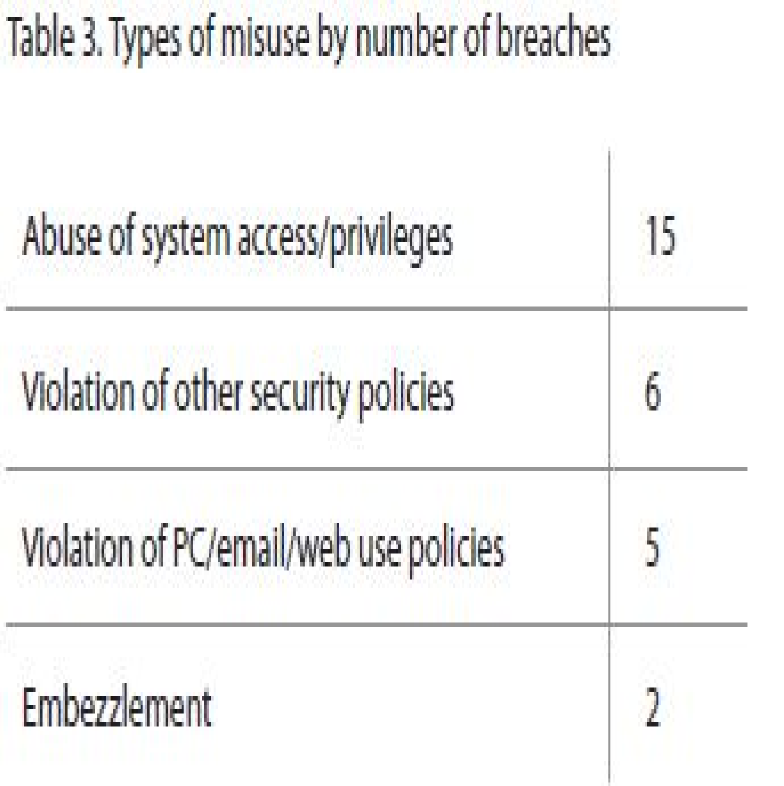


Table 3. Types of misuse by number of breaches

Abuse of system access/privileges	15
Violation of other security policies	6
Violation of PC/email/web use policies	5
Embezzlement	2

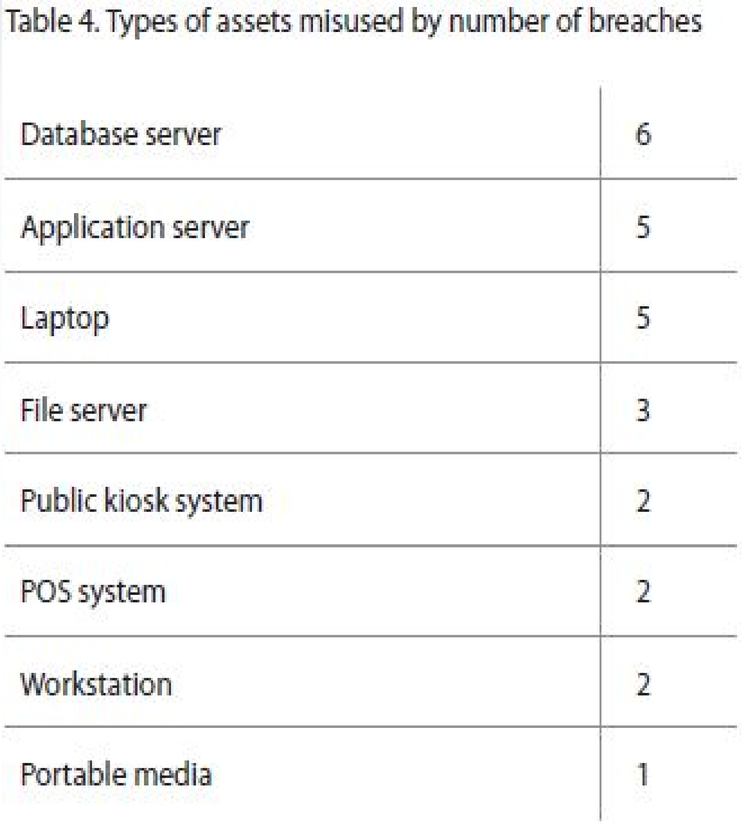


Table 4. Types of assets misused by number of breaches

Database server	6
Application server	5
Laptop	5
File server	3
Public kiosk system	2
POS system	2
Workstation	2
Portable media	1

Attack Difficulty & Targeting

- Targeted attacks doubled
- Highly difficult attacks did not increase but are responsible for nearly all breached records
- Message: Some attacks are difficult to pull off, but the payout appears worth it.

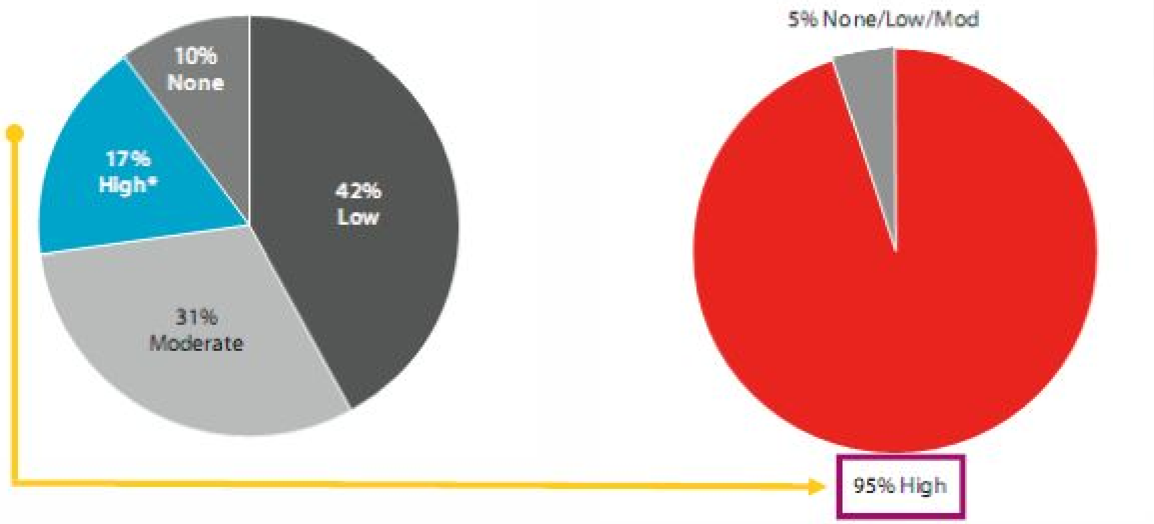


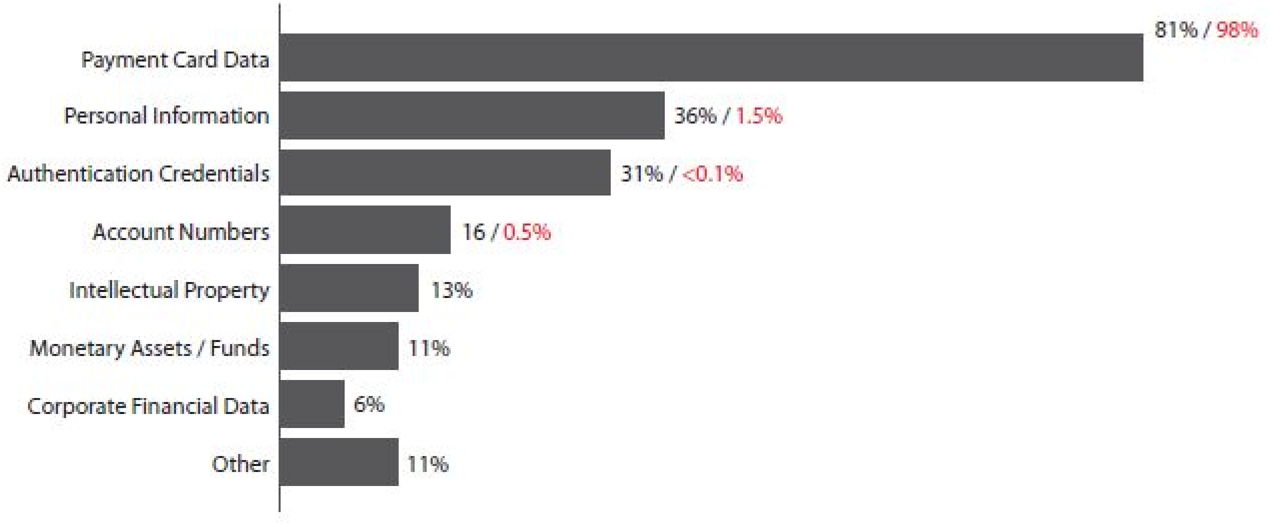
Figure 22. Attack difficulty by percent of breaches

Figure 23. Attack difficulty by percent of records

Compromised Assets and Data

- Most data breached from online systems
  - Different than public disclosures
- Criminals seek payment card data
  - Easily convertible to cash
- Other types common as well
  - Auth credentials allow deeper access
  - Intellectual property at 5-year high

Figure 29. Compromised data types by percent of breaches (black) and records (red)*



Breach Discovery

- Most breaches discovered by a third party
- Event monitoring caught few breaches

Figure 32. Breach discovery methods by percent of breaches

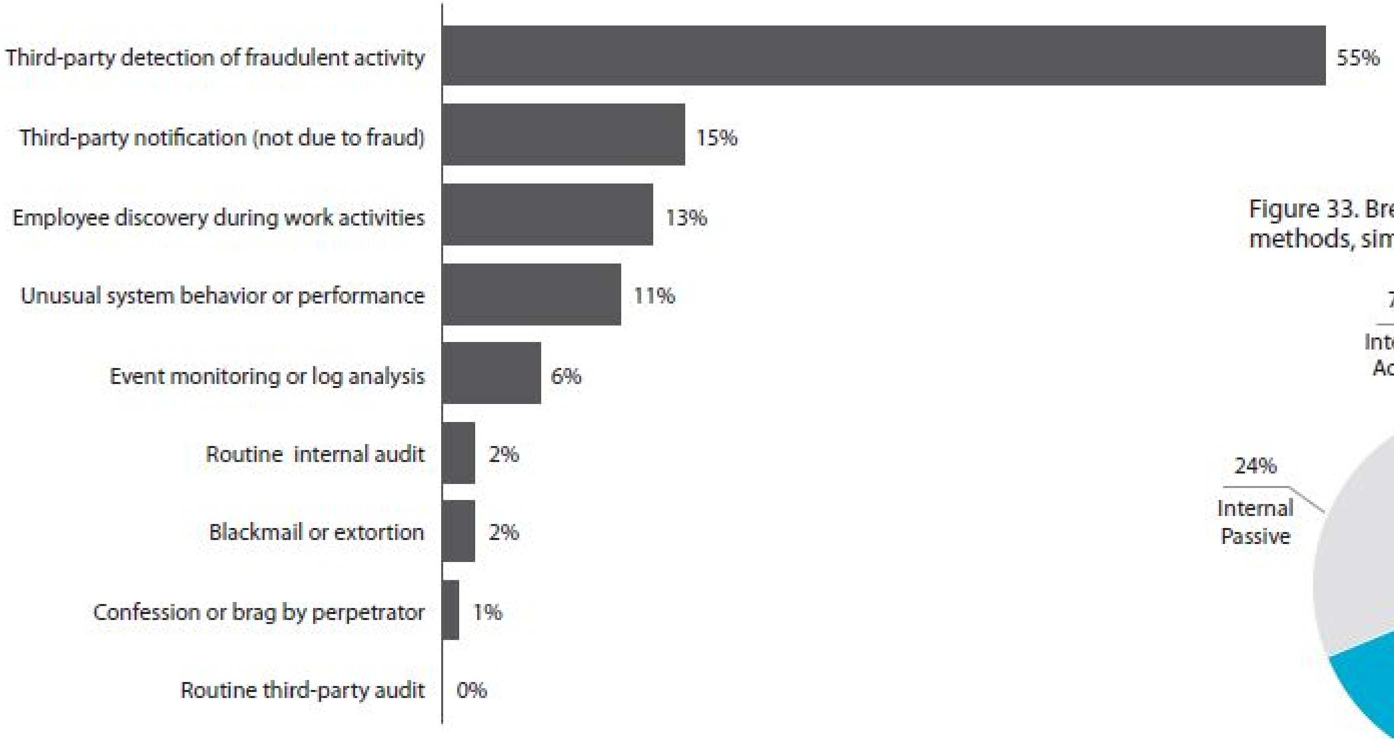
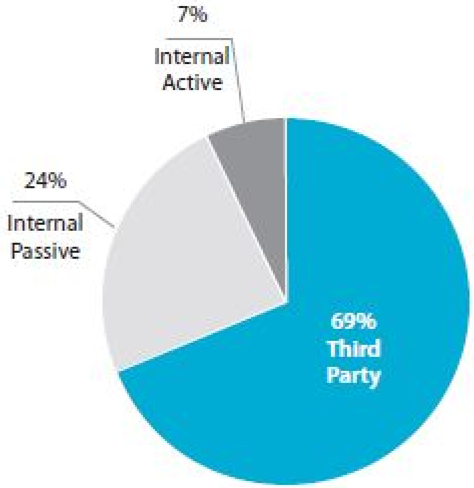


Figure 33. Breach discovery methods, simplified



Breach Discovery

On the whole, organizations discovered breaches slightly quicker in 2008. However, lest we confuse “quicker” with “quickly,” this statement needs some additional context. Breaches still go undiscovered and uncontained for weeks or months in 75 percent of cases. It is doubtful that any chief security officer anywhere would call this “quick”.

State of the Net 2009

	Spam	Viruses	Spyware	Phishing
	The incidence of heavy spam is as high as last year.	The frequency is the same as in last year's survey.	545,000 households had to replace computers in the past six months.	34,758 attacks in December 2008 alone.
National incidence	1 in 3 had heavy levels of spam.	1 in 7 had serious problems.	1 in 12 had serious problems.	1 in 90 lost money.
Total damage	N/A	$5.8 billion	$1.7 billion	$483 million

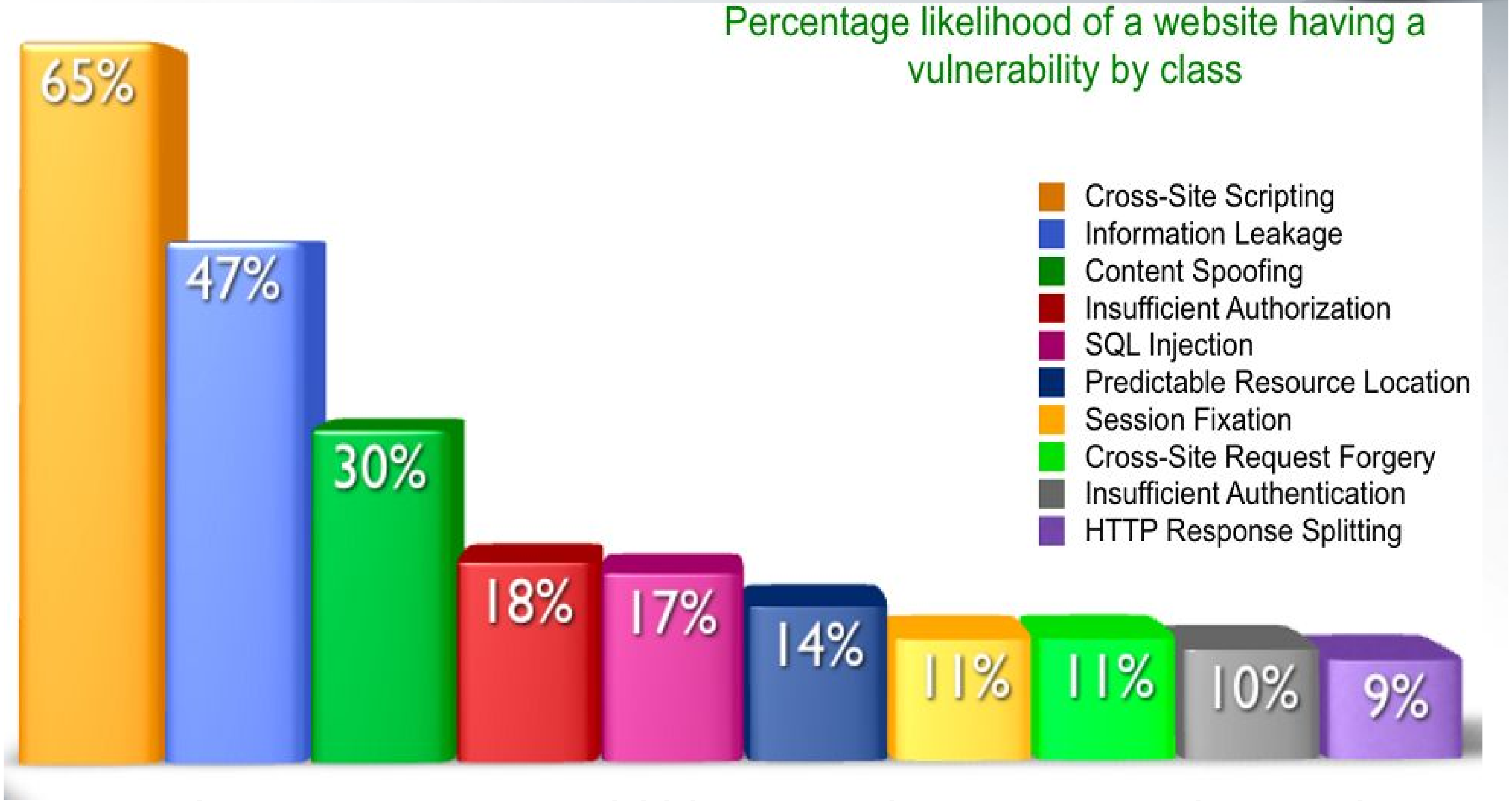
Consumer Reports magazine: June 2009

WhiteHat Security Report

- 70% of the top 100 most popular Web sites either hosted malicious content or contained a masked redirect to lure unsuspecting victims. (Websense 2009)
- 63% of websites currently have a high, critical or urgent issue
  - 31% have urgent issue
- Lifetime average number of vulnerabilities per website: 17
  - Current average of unresolved vulnerabilities per website: 7

http://www.whitehatsec.com/home/news/09pressarchives/NR_051809stats.html

WhiteHat Security Top Ten



The top ten vulnerabilities remain largely unchanged

Operationalizing Website Security

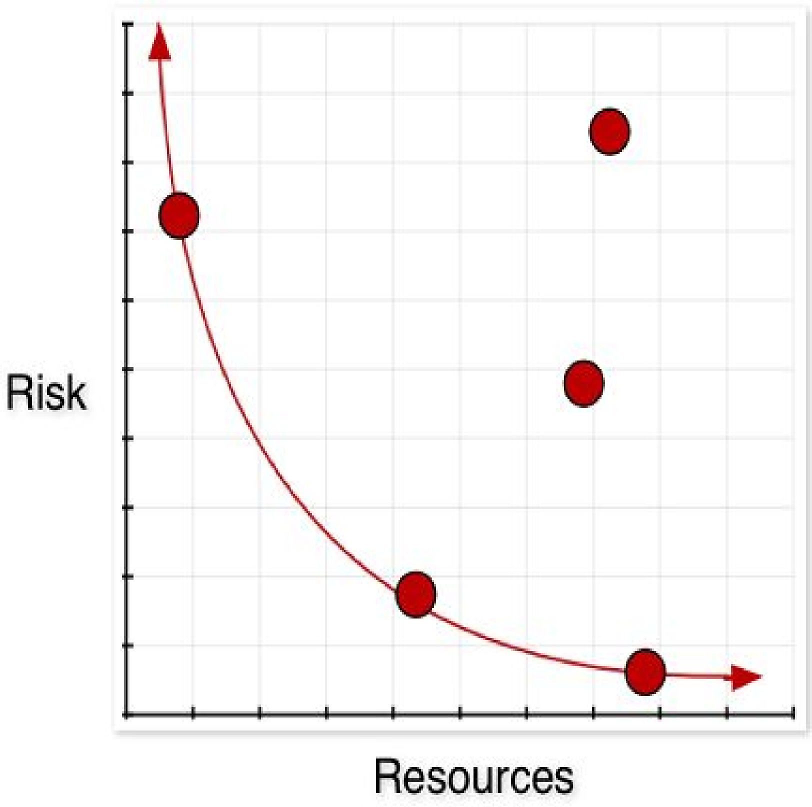
1) Where do I start?
Locate the websites you are responsible for

2) Where do I do next?
Rank websites based upon *business criticality*

3) What should I be concerned about first?
Random Opportunistic, Directed Opportunistic, Fully Targeted

4) What is our current security posture?
Vulnerability assessments, pen-tests, traffic monitoring

5) How best to improve our survivability?
SDL, virtual patch, configuration change, decommission, outsource, version roll-back, etc.



What is your organizations tolerance for risk (per website)?

Recommendations

Recap from previous report (they still apply)

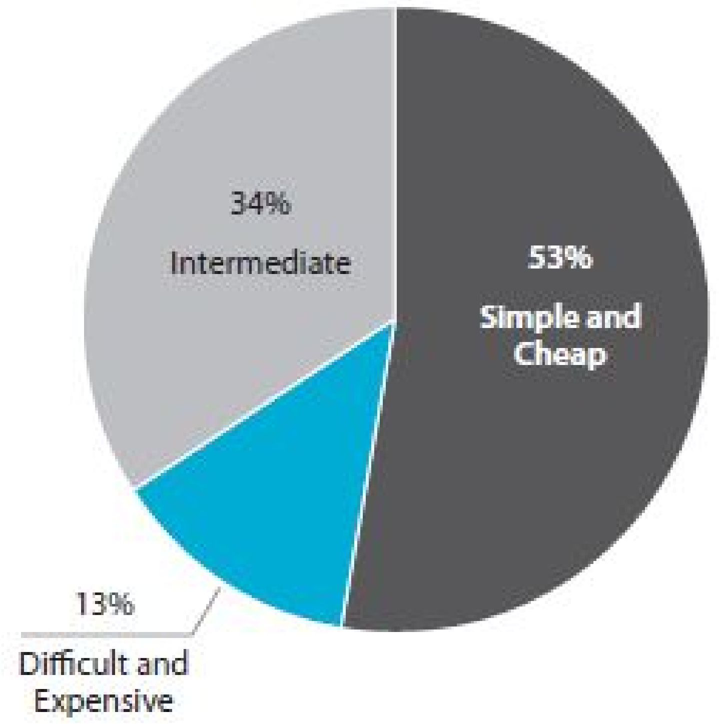
- Align process with policy
- Achieve “Essential” then worry about “Excellent”
- Secure Business Partner Connections
- Create a Data Retention Plan
- Control data with transaction zones
- Monitor event logs
- Create an Incident Response Plan
- Increase awareness
- Engage in mock incident testing

Recommendations

New Recommendations

- Changing default credentials is key
- Avoid shared credentials
- User Account Review
- Application Testing and Code Review
- Smarter Patch Management Strategies
- Human Resources Termination Procedures
- Enable Application Logs and Monitor
- Define “Suspicious” and “Anomalous” (then look for whatever “It” is)

Figure 38. Description of the effort and expense of recommended preventative measures by percent of breaches



Summary

Sources: Similar distribution; organized crime behind most large breaches

- Organized criminal groups driving evolution of cybercrime

Attacks: Criminals exploit errors, hack into systems, install malware

- 2008 saw more targeted attacks, especially against orgs processing or storing large volumes of data
- Highly difficult attacks not common but very damaging
- Large increase in customized, intelligent malware

Summary

Assets and Data: Focus is online cashable data

Prevention: The basics–if done consistently–are effective in most cases

- Increasing divergence between Targets of Opportunity and Targets of Choice
  - ToO: Remove blatant opportunities through basic controls
  - ToC: Same as above but prepare for very determined, very skilled attacks
    - Initial hack appears the easiest point of control

My Summary

We're not really doomed.

We just have a lot of work to do.

By working together, we all become stronger.

Ron Woerner

Email: ronw2007 (at) gmail.com

Twitter: ronw123