RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-T07

No More Snake Oil:
Why InfoSec Needs Security Guarantees

Jeremiah Grossman

Founder
WhiteHat Security, Inc.
@jeremiahg

Ever notice how everything in the Information Security industry is sold “AS-IS”?

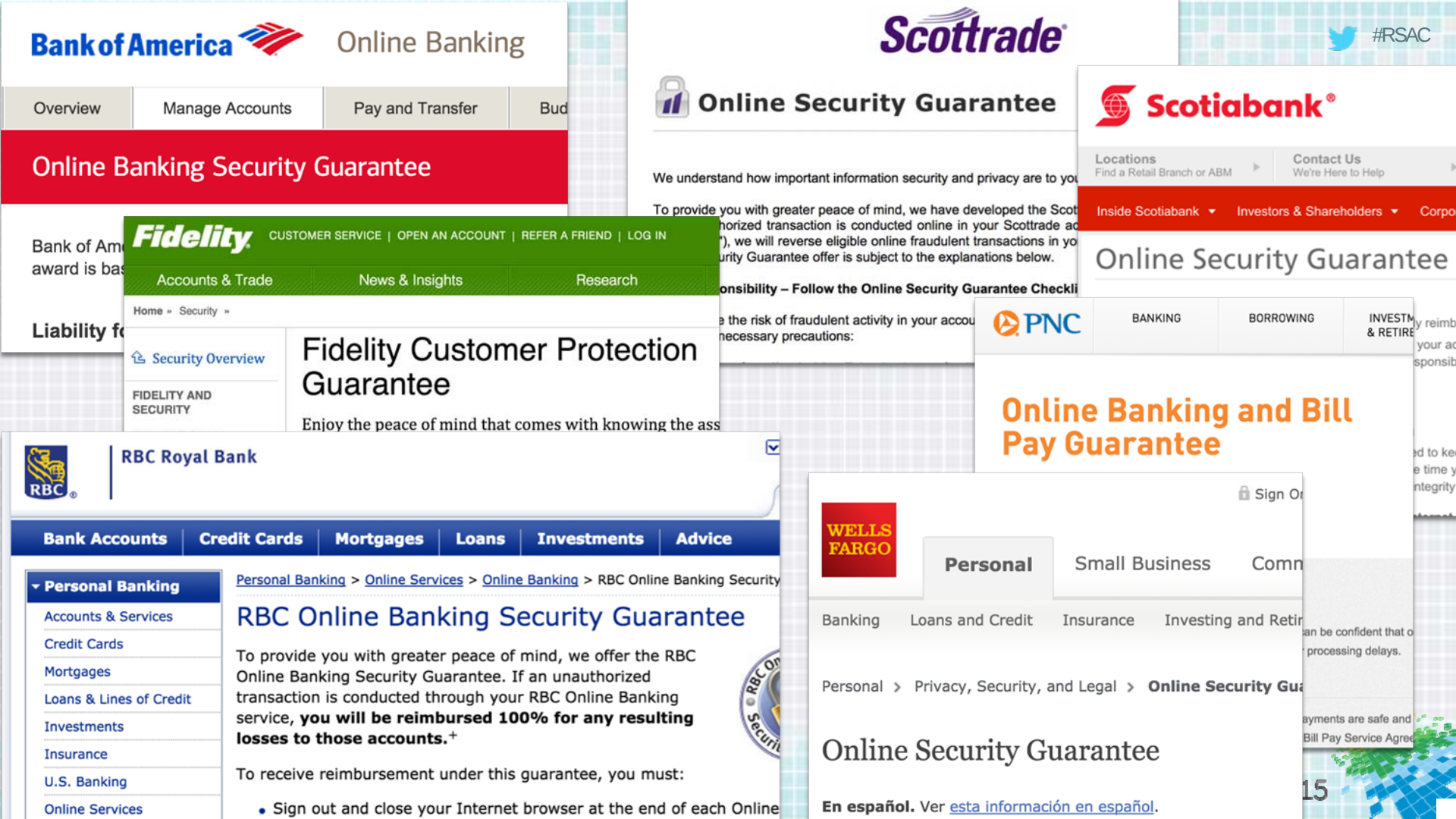
- No Guarantees
- No Warrantees
- No Return Policies

Unlike every day 'real world' products…

Customer challenges…

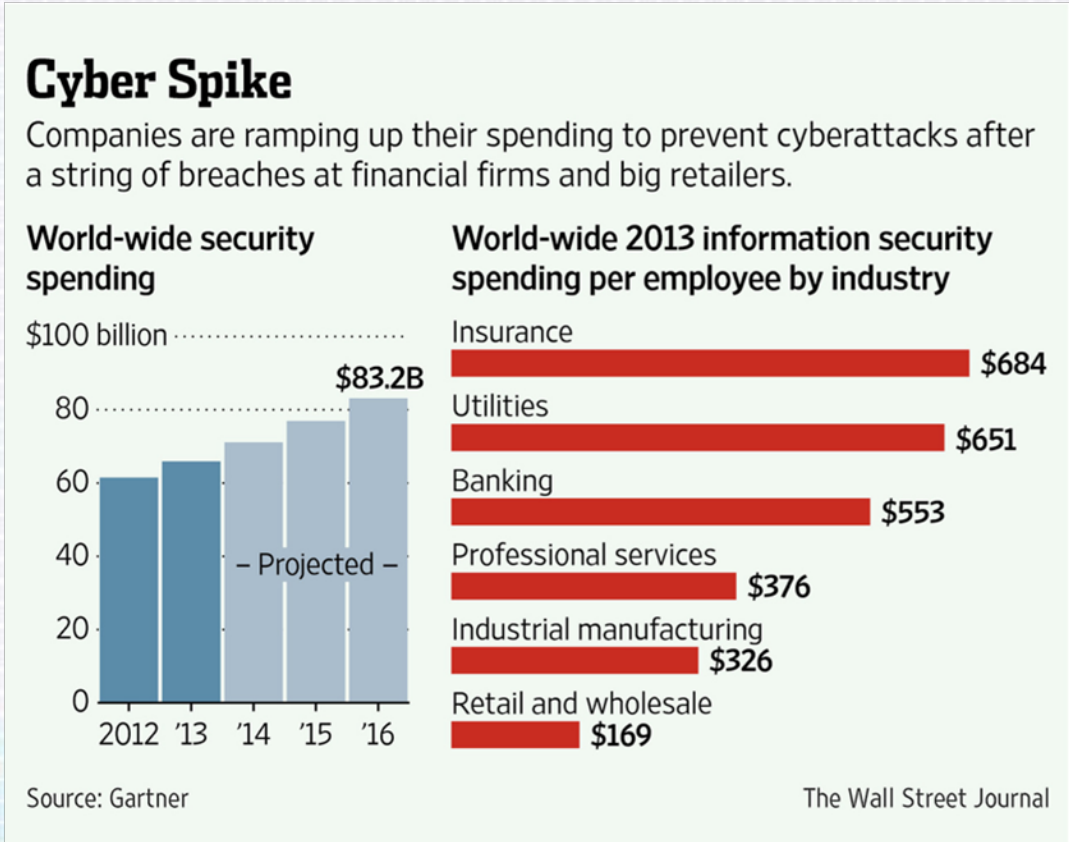
- Difficult telling security vendors apart.
- Justifying the business value of security products to management.
- Trusting security vendors since their interests are misaligned.

Answer: Security Guarantees


Bank of America
Online Banking
Overview
Manage Accounts
Pay and Transfer
Online Banking Security Guarantee
Scottrade
#RSAC
Online Security Guarantee
We understand how important information security and privacy are to you
To provide you with greater peace of mind, we have developed the Scot
Scotiabank
Locations
Find a Retail Branch or ABM
Contact Us
We're Here to Help
Inside Scotiabank
Investors & Shareholders
Online Security Guarantee
Fidelity
CUSTOMER SERVICE | OPEN AN ACCOUNT | REFER A FRIEND | LOG IN
Accounts & Trade
News & Insights
Research
Home » Security »
Security Overview
FIDELITY AND SECURITY
Fidelity Customer Protection Guarantee
Enjoy the peace of mind that comes with knowing the ass
PNC
BANKING
BORROWING
Online Banking and Bill Pay Guarantee
RBC Royal Bank
Bank Accounts
Credit Cards
Mortgages
Loans
Investments
Advice
Personal Banking
Accounts & Services
Credit Cards
Mortgages
Loans & Lines of Credit
Investments
Insurance
U.S. Banking
Online Services
Personal Banking > Online Services > Online Banking > RBC Online Banking Security
RBC Online Banking Security Guarantee
To provide you with greater peace of mind, we offer the RBC Online Banking Security Guarantee. If an unauthorized transaction is conducted through your RBC Online Banking service, you will be reimbursed 100% for any resulting losses to those accounts.+
To receive reimbursement under this guarantee, you must:
Sign out and close your Internet browser at the end of each Online
WELLS FARGO
Personal
Small Business
Banking
Loans and Credit
Insurance
Personal > Privacy, Security, and Legal > Online Security Gua
Online Security Guarantee
En español. Ver esta información en español.

Security Industry Spends Billions

"According to the IT research and advisory firm [Gartner], **global IT security spending will reach $71.1 billion this year [2014]**, which represents **an increase of 7.9% compared to 2013**. **Next year, spending will grow even more, reaching $76.9 billion.**"



WhiteHat SECURITY

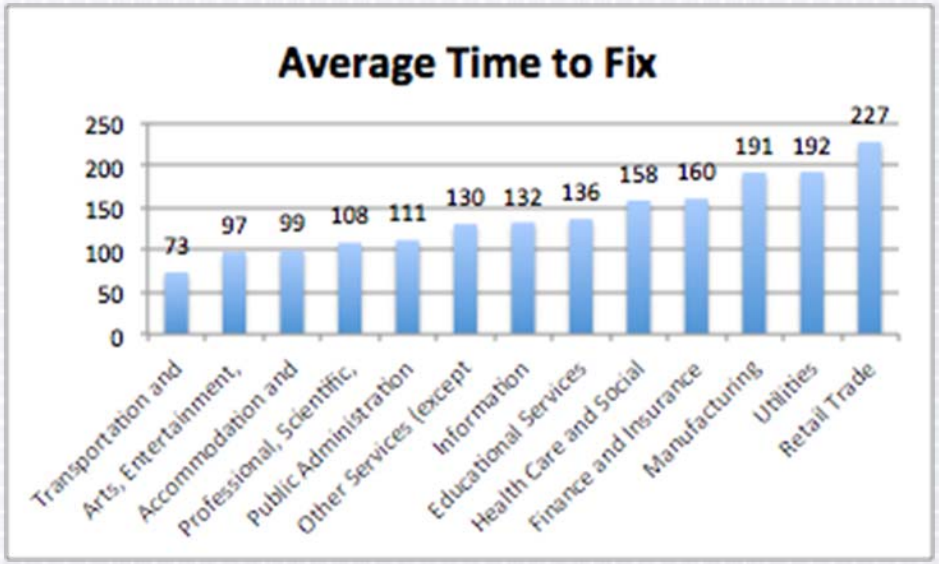
Result: Every Year is the Year of the Hack

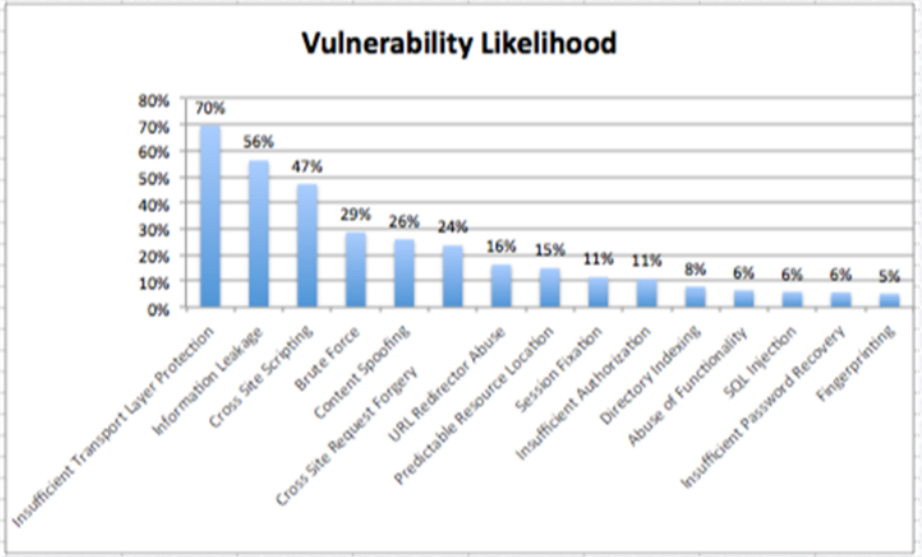
In 2014, **71% of security professionals said their networks were breached. 22% of them victimized 6 or more times**. This increased from 62% and 16% respectively from 2013.

52% said their organizations will likely be successfully hacked in the next 12 months. This is up from 39% in 2013.

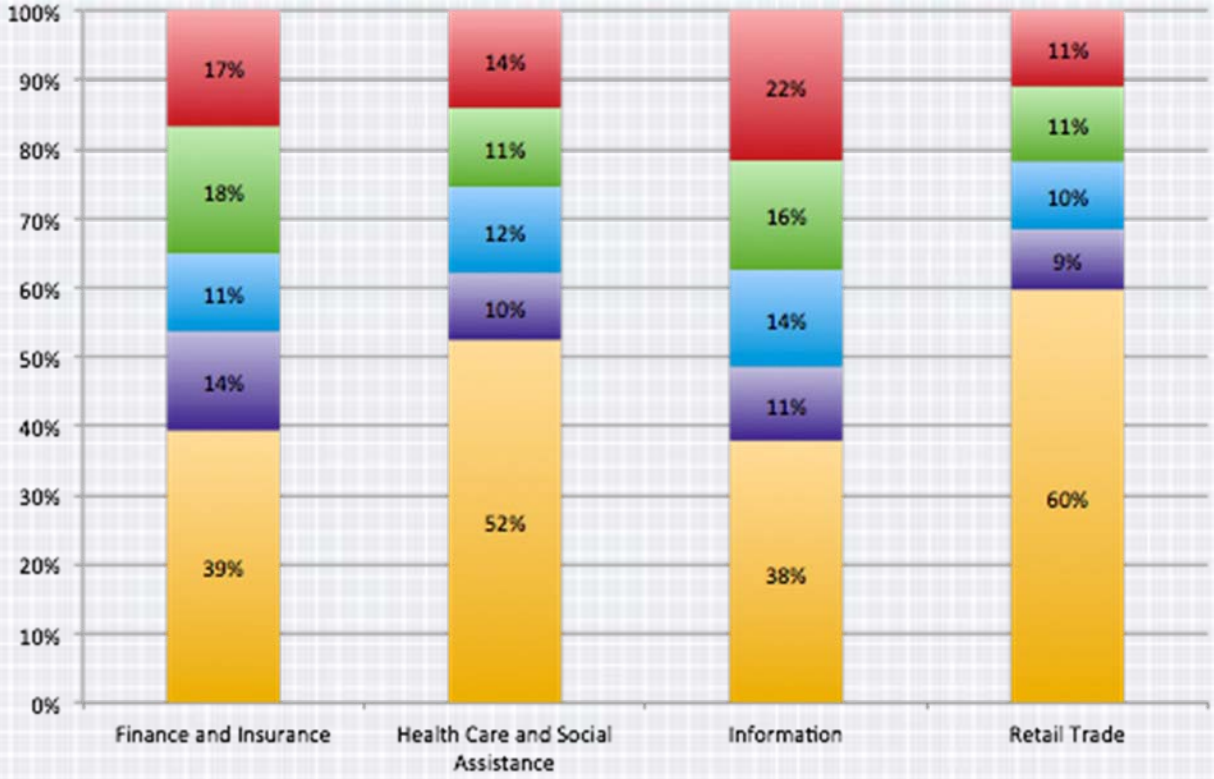
Survey of security professionals by CyberEdge Group

AppSec: Too Many Vulns, Too Little Time

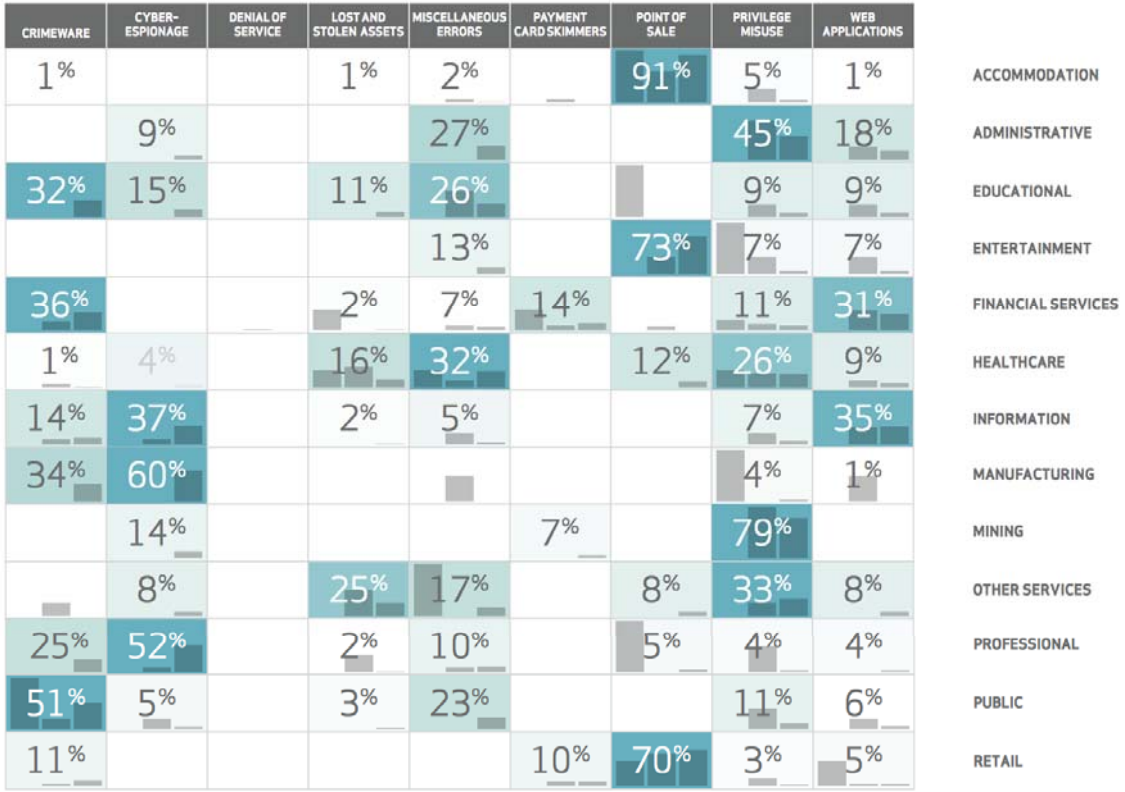




Window of Exposure



WhiteHat SECURITY



	CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	LOST AND STOLEN ASSETS	MISCELLANEOUS ERRORS	PAYMENT CARD SKIMMERS	POINT OF SALE	PRIVILEGE MISUSE	WEB APPLICATIONS
ACCOMMODATION	1%			1%	2%		91%	5%	1%
ADMINISTRATIVE		9%			27%			45%	18%
EDUCATIONAL	32%	15%		11%	26%			9%	9%
ENTERTAINMENT					13%		73%	7%	7%
FINANCIAL SERVICES	36%			2%	7%	14%		11%	31%
HEALTHCARE	1%	4%		16%	32%		12%	26%	9%
INFORMATION	14%	37%		2%	5%			7%	35%
MANUFACTURING	34%	60%						4%	1%
MINING		14%				7%		79%	
OTHER SERVICES		8%		25%	17%		8%	33%	8%
PROFESSIONAL	25%	52%		2%	10%		5%	4%	4%
PUBLIC	51%	5%		3%	23%			11%	6%
RETAIL	11%					10%	70%	3%	5%

Figure 29.

Frequency of data disclosures by incident patterns and victim industry

For this reason, some may wish to refer back to the 2014 DBIR for a primer on the incident patterns. In the following sections, we aim to highlight new, interesting, insightful, and instructive nuggets of wisdom rather than restate the basics. It's our hope that this to-the-point approach strikes a good and useful balance.[39]

Downside Protection

As of 2014, American businesses were expected to pay up to **$2 billion on cyber-insurance premiums**, a **67% spike** from $1.2 billion spent in 2013.

Current expectations by **one industry watcher suggest 100% growth in insurance premium activity, possibly 130% growth**.

It's usually the firms that are best prepared for cyber attacks that wind up buying insurance.

"**Premiums for a $1 million plan are generally $5,000 to $10,000 annually**, though that can vary based on several factors, including the company's revenue, cyber-risk management efforts and the coverage chosen, Fenaroli said. For hospitals, premiums can be much larger—sometimes more than $100,000 or even $1 million for larger health systems, he said."

Opinion & Editorial Research Interactive Data Products Ed

Modern Healthcare

The leader in healthcare business news, research & data

My account

Search Modern Healthcare

Providers Insurance Government Finance Technology More

Home > Insurance > Private Plans

RELATED CONTENT

Hackers breach Anthem; 80M exposed

Anthem attack a wake-up call to step up cybersecurity

Chinese hackers hit Community Health Systems; others vulnerable

Anthem hack will shake up market for cyber risk insurance

By Adam Rubenfire | February 5, 2015

The cyberattack on Anthem, which affected 80 million people, likely won't do immediate financial damage to Anthem's bottom line because it had cybersecurity insurance coverage, J.P. Morgan Securities analyst Justin Lake said Thursday.

WhiteHat SECURITY

Sony Pictures Entertainment holds $60 million in Cyber insurance with Marsh, according to documents leaked by the group claiming responsibility for the attack on the movie studio.

"The documents, covered in detail by Steve Ragan at CSO, say that **after sonypictures.com was breached in 2011, Sony made a claim of $1.6 million with Hiscox,** its Cyber provider at the time. The insurer declined to quote at renewal, so **Sony Pictures turned to Lockton, which brokered a $20 million policy that included $10 million in self-insured retention**."

FILED UNDER: AGENT BROKER, COMMERCIAL BUSINESS

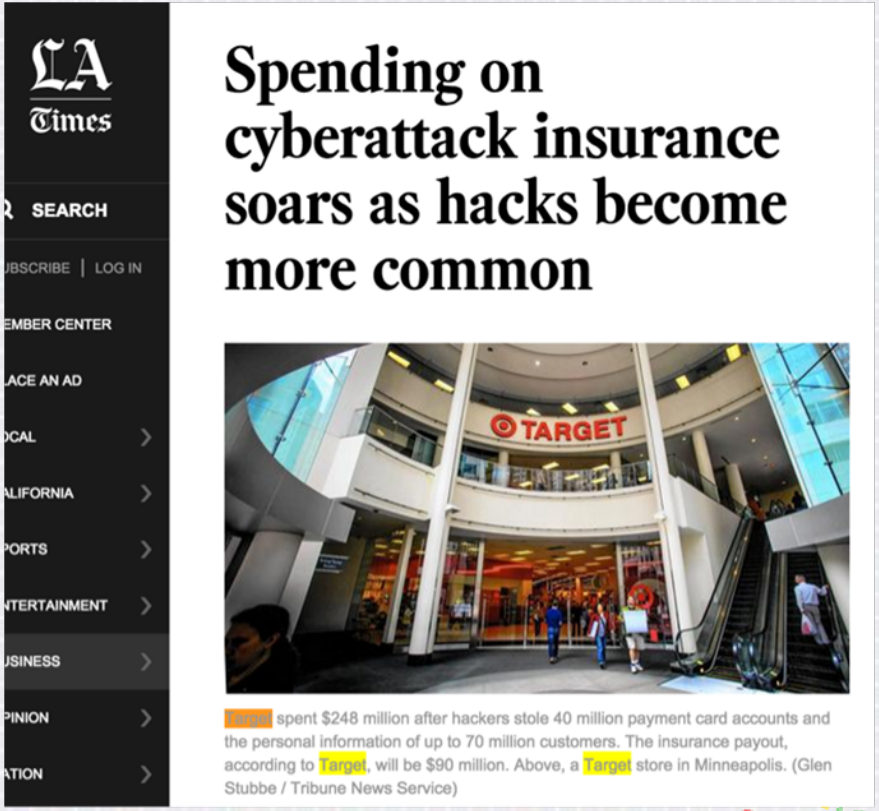
Sony Pictures holds $60 million Cyber policy with Marsh

DEC 18, 2014 | BY MELISSA HILLEBRAND

Sony Pictures Studios in Culver City, Calif.

"**Target spent $248 million after hackers stole 40 million payment card accounts** and the personal information of up to 70 million customers. **The insurance payout, according to Target, will be $90 million.**"

"**Home Depot reported $43 million in expenses related to its September 2014 hack**, which affected 56 million credit and debit card holders. **Insurance covered only $15 million.**"



LA Times

SEARCH

UBSCRIBE | LOG IN

EMBER CENTER

LACE AN AD

OCAL

ALIFORNIA

PORTS

NTERTAINMENT

USINESS

PINION

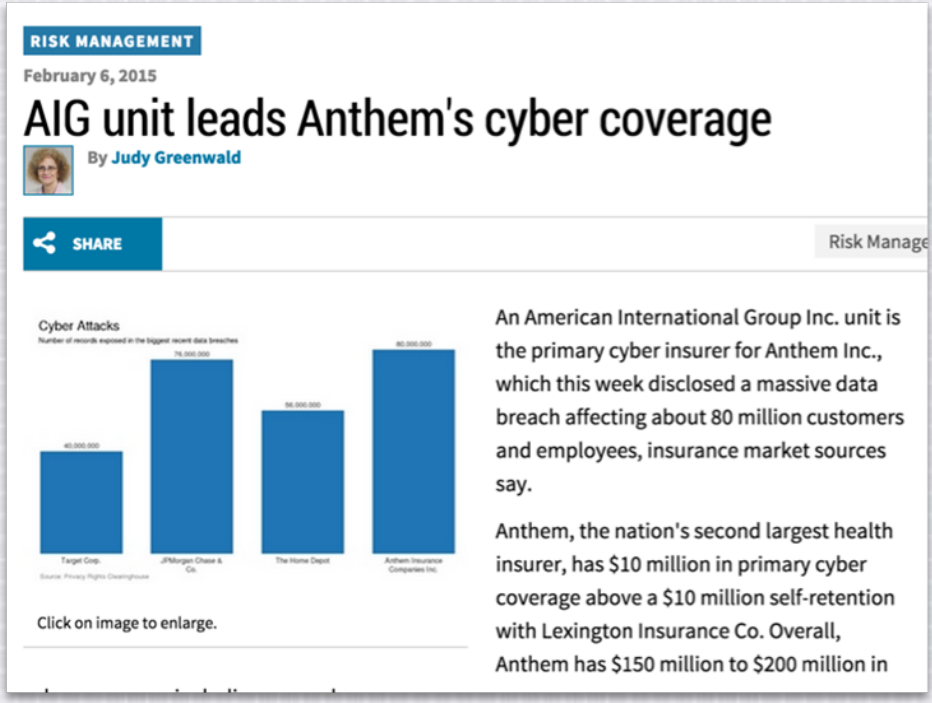
ATION

Spending on cyberattack insurance soars as hacks become more common

Target spent $248 million after hackers stole 40 million payment card accounts and the personal information of up to 70 million customers. The insurance payout, according to Target, will be $90 million. Above, a Target store in Minneapolis. (Glen Stubbe / Tribune News Service)

"**Anthem has $150 million to $200 million in cyber coverage**, including excess layers, sources say."

Insurers providing excess layers of cyber coverage include: Lloyd's of London syndicates; operating units of Liberty Mutual Holding Co.; Zurich Insurance Group; and CNA Financial Corp., sources say.



RISK MANAGEMENT

February 6, 2015

AIG unit leads Anthem's cyber coverage

By Judy Greenwald

SHARE

Risk Manage

Cyber Attacks

Number of records exposed in the biggest recent data breaches

Target Corp. | JPMorgan Chase & Co. | The Home Depot | Anthem Insurance Companies Inc.

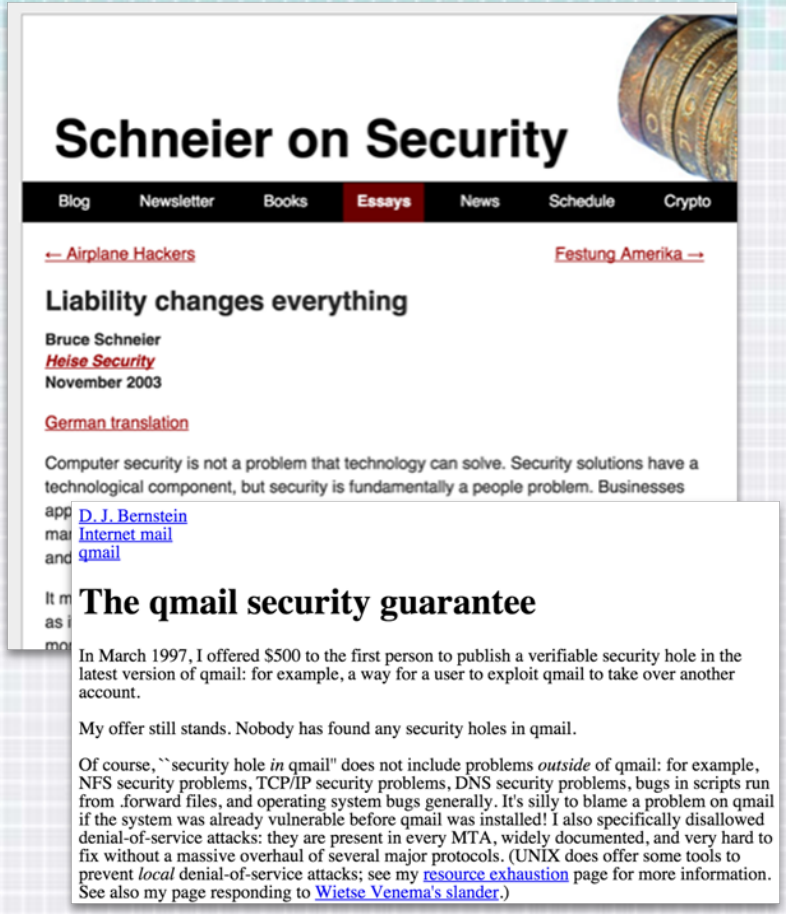
Source: Privacy Rights Clearinghouse

Click on image to enlarge.

An American International Group Inc. unit is the primary cyber insurer for Anthem Inc., which this week disclosed a massive data breach affecting about 80 million customers and employees, insurance market sources say.

Anthem, the nation's second largest health insurer, has $10 million in primary cyber coverage above a $10 million self-retention with Lexington Insurance Co. Overall, Anthem has $150 million to $200 million in

WhiteHat SECURITY



Schneier on Security

Blog Newsletter Books Essays News Schedule Crypto

← Airplane Hackers Festung Amerika →

Liability changes everything

Bruce Schneier
Heise Security
November 2003

German translation

Computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem. Businesses

D. J. Bernstein
Internet mail
qmail

The qmail security guarantee

In March 1997, I offered $500 to the first person to publish a verifiable security hole in the latest version of qmail: for example, a way for a user to exploit qmail to take over another account.

My offer still stands. Nobody has found any security holes in qmail.

Of course, ``security hole *in* qmail'' does not include problems *outside* of qmail: for example, NFS security problems, TCP/IP security problems, DNS security problems, bugs in scripts run from .forward files, and operating system bugs generally. It's silly to blame a problem on qmail if the system was already vulnerable before qmail was installed! I also specifically disallowed denial-of-service attacks: they are present in every MTA, widely documented, and very hard to fix without a massive overhaul of several major protocols. (UNIX does offer some tools to prevent *local* denial-of-service attacks; see my resource exhaustion page for more information. See also my page responding to Wietse Venema's slander.)

"Liability enforcement is essential. Remember that I said **the costs of bad security are not borne by the software vendors that produce the bad security.** In economics this is known as an externality: a cost of a decision that is borne by people other than those making the decision.

However it happens, liability changes everything. Currently, there is no reason for a software company not to offer more features, more complexity, more versions. Liability forces software companies to think twice before changing something. **Liability forces companies to protect the data they're entrusted with."**

WhiteHat SECURITY

Objections to Security Guarantees

"You're not entitled to take a view, unless and until you can argue better against that view than the smartest guy who holds that opposite view. If you can argue better than the smartest person who holds the opposite view, that is when you are entitled to hold a certain view."

Charlie Munger
Vice-Chairman Berkshire Hathaway

Objection:
100% security is impossible.

Rebuttal: Nothing is ever 100% secure, just like no every-day product is 100% reliable. With product performance data, even if unable to provide 100% protection, offering security guarantees is possible.

Objection:
Guarantees can't keep up.

Rebuttal: It's contractually possible to specify exactly what a security guarantee covers and disclaim excessively risky events and unknowns. Insurance companies do this routinely.

Objection:
Vendors don't have the data.

Rebuttal: Today we're in the era of the cloud, managed services, and products routinely phoning home for updates, all providing real-time access to an ample supply of performance data.

Objection:

Pinpointing product failure is difficult.

Rebuttal: For organizations capable of performing effective forensic investigations, identifying the gap in the defense or the product that failed, is entirely possible.

Objection:
Soft costs are hard to quantify.

Rebuttal: Security guarantees and cyber-security insurance typically cover only hard costs associated with downtime, legal feels, incident response, credit monitoring, fines, and so on.

Objection: Security vendors don't want the liability.

Rebuttal: Security guarantees represent a unique opportunity for vendors to differentiate from competitors and an opportunity for customers to demand more effective products.

Objection:

Improper product use is often the cause.

Rebuttal: Like many other products we buy, guarantees only covers intended use. Security vendors can specify how their product is meant to be used for its effectiveness to be guaranteed.

2014 - 2015 Annual Spending Increase

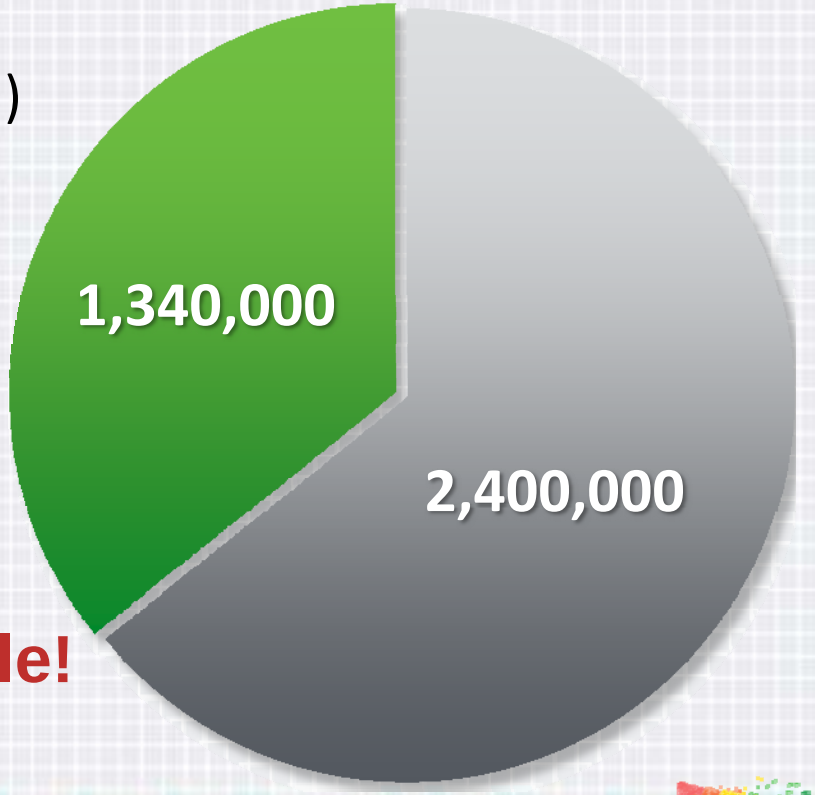
Information Security Spending (N. America)

~$2.4 billion in new spending (+7.8%)

Forecast Overview: Information Security, Worldwide, 2014 Update
(Gartner Published: 25 June 2014)

Cyber-Security Insurance

~$1.34 Billion in new spending (+67%)



1/3 of the budget left on the table!

"We also asked about the importance of being offered a 'security guarantee' by cloud service providers. **Three-quarters of respondents (74%) say it's 'Very Important' that cloud providers offer a guarantee**, and another 22% say 'Somewhat Important.' Companies not using cloud place a greater importance on security guarantees than current users. As such, **security guarantees give cloud service providers an opportunity to attract new customers.**"

ChangeWave

Subsidiary of 451 Research

Survey of 1,097 respondents involved in their company's IT buying decisions (Jul, 2014). 445 currently uses public cloud.

WhiteHat SECURITY

Customer challenges…

- Difficult telling security vendors apart.

  Security guarantees help customers differentiate truly effective security products from those that are…less effective.

- Justifying the business value of security products to management.

  Security guarantees help quantify the value of security products in dollars and cents for the business.

- Trusting security vendors since their interests are misaligned.

  Security guarantees hold vendors accountable for the performance of their products and therefore more credible.

How WhiteHat Approaches Security Guarantees

WhiteHat Sentinel: Tests tens of thousands of websites 24x7x365

Incident Data: Data sharing relationships incident responders

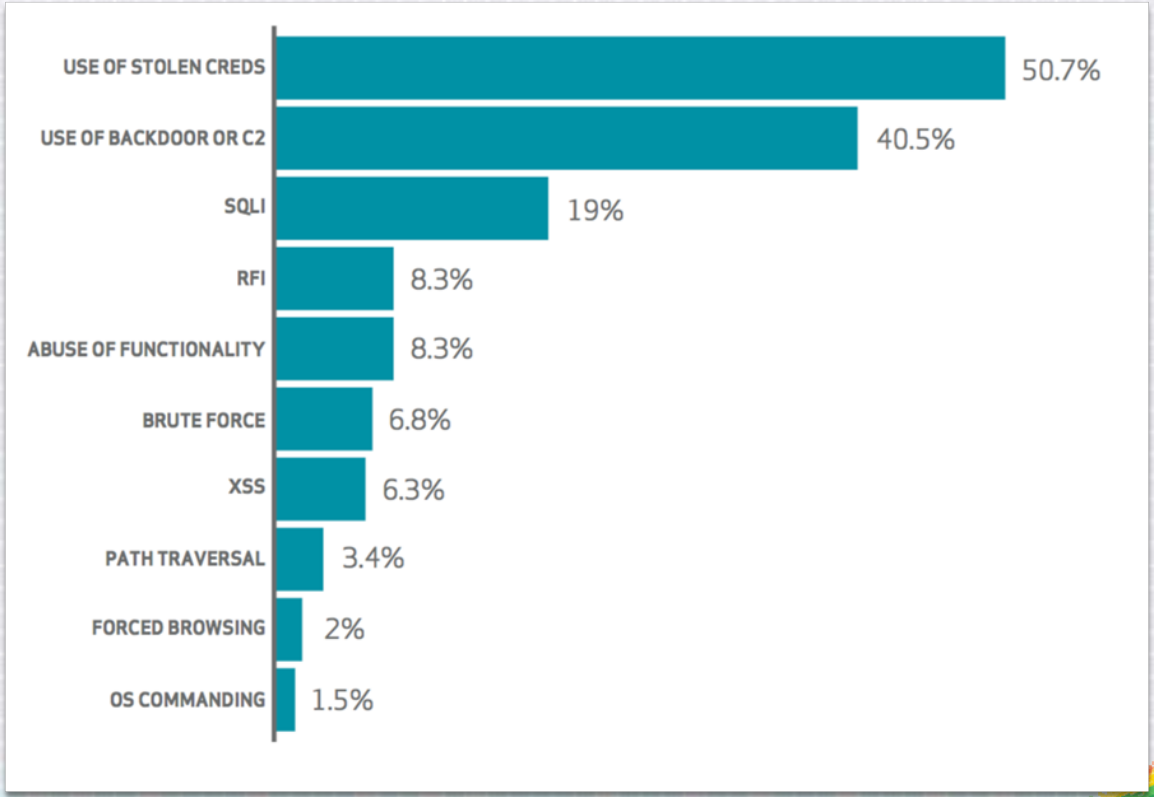
Customer Relationships: 'Missed' vulns leading to breaches

Our success rate is over 99%.

What WebApp Attacks At Adversaries Using?

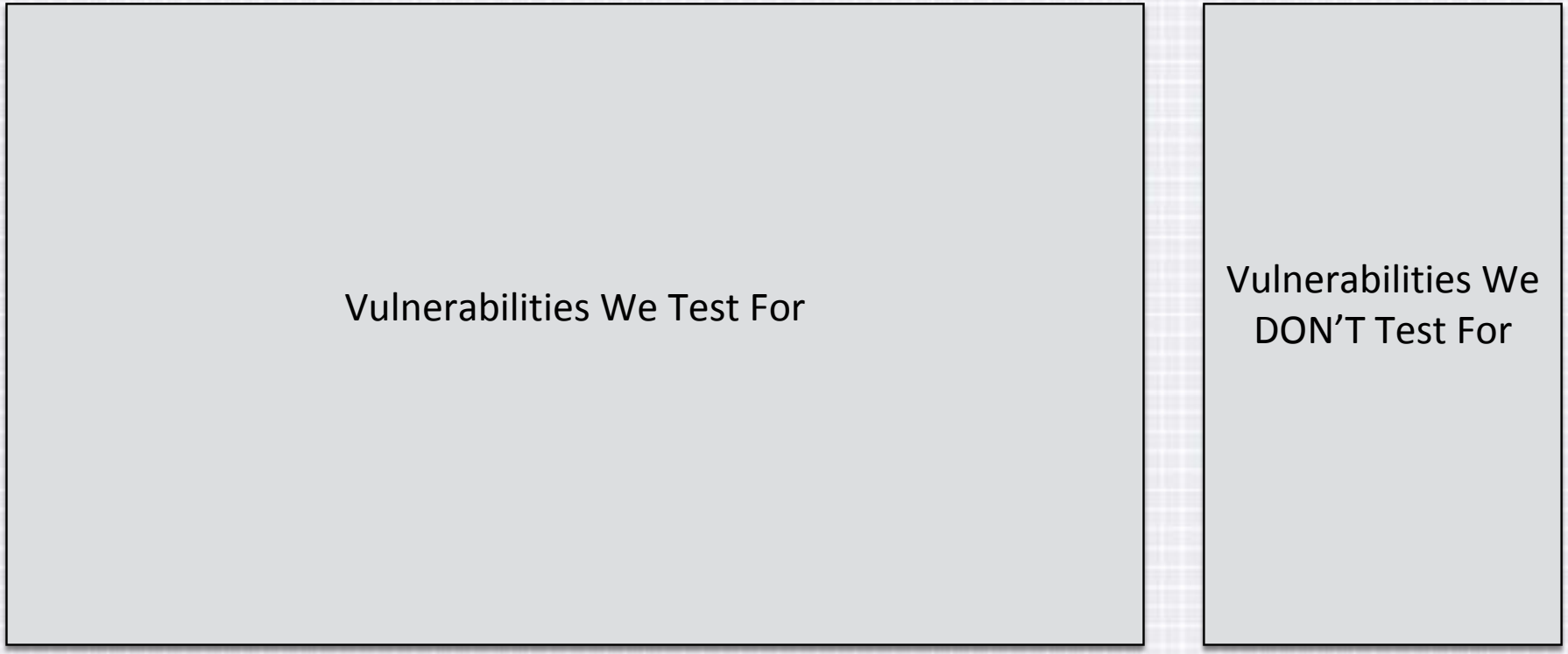
"This year, organized crime became the most frequently seen threat actor for Web App Attacks."

Verizon 2015 Data Breach Investigations Report



WhiteHat SECURITY

The World of Web Vulnerabilities



Vulnerabilities We Test For

Vulnerabilities Missed & Exploited

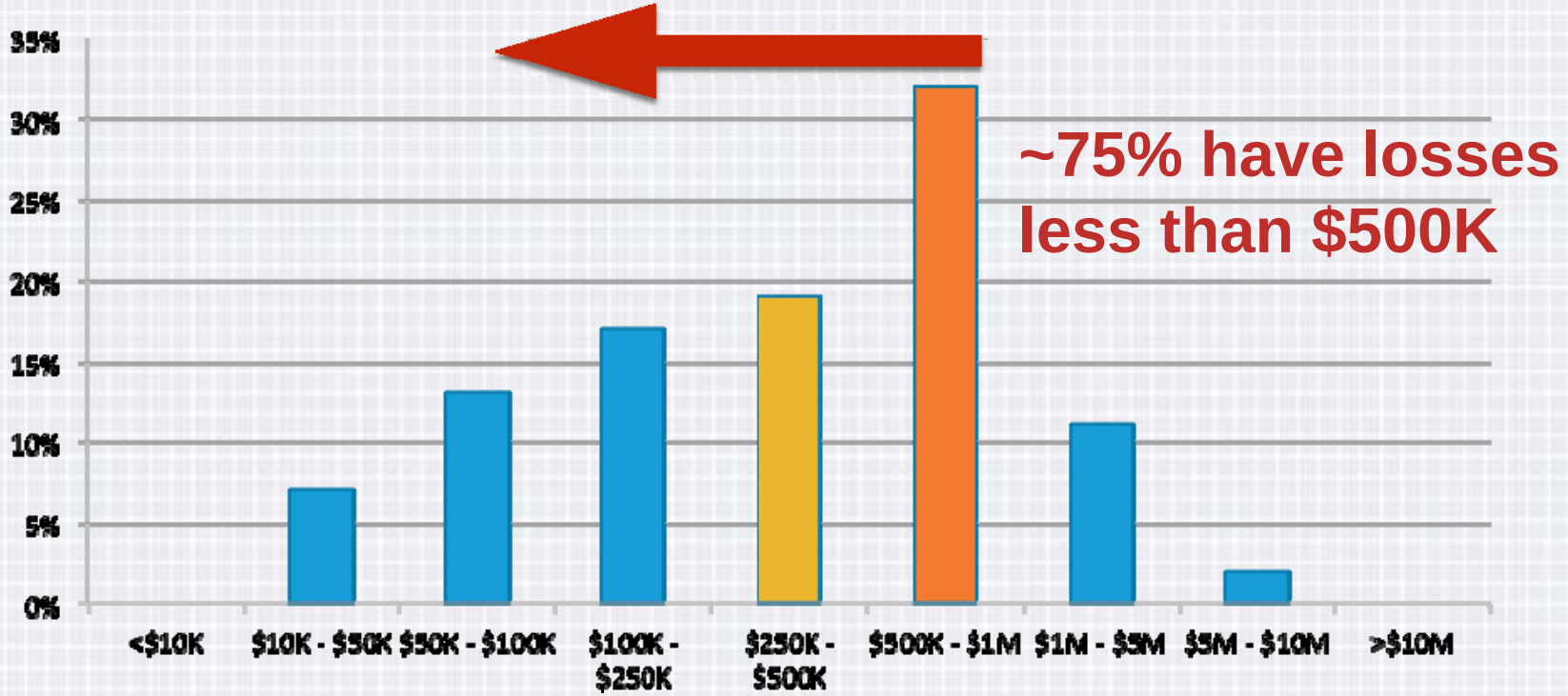
- Why was the vulnerability missed? Improve technology, training, and process.
- Other consumer products have standard performance metrics (MTB; Operating Hours – runtime of motors; Milage for drivetrain, tires, etc)

If a website covered by Sentinel Elite is hacked, using a vulnerability we missed and should have found, the customer will be refunded in full. Plus up to …

$250,000

…to help cover costs associated with the breach.

Monetary loss distribution per data breach



"The Post Breach Boom", Ponemon Institute, 2013

Ranges of expected loss by number of records

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Verizon 2015 Data Breach Investigations Report

Path for Other Security Vendors to Follow

- Obtain as much performance data as possible
- Contractually capture what your product is able to reliably guarantee and disclaim the rest.
- Back your security guarantee with an insurance provider.

“The only two products not covered by product liability are religion and software, and software shall not escape much longer.”

Dan Geer (CISO, In-Q-Tel)

RSAConference2015
San Francisco | April 20-24 | Moscone Center

Questions?

Jeremiah Grossman
Founder, WhiteHat Security

http://blog.whitehatsec.com/
Twitter: @JeremiahG