

**JEREMIAH GROSSMAN**

CHIEF OF SECURITY STRATEGY

---

# **AN INSIDERS GUIDE TO CYBER-INSURANCE AND SECURITY GUARANTEES**

 @jeremiahg

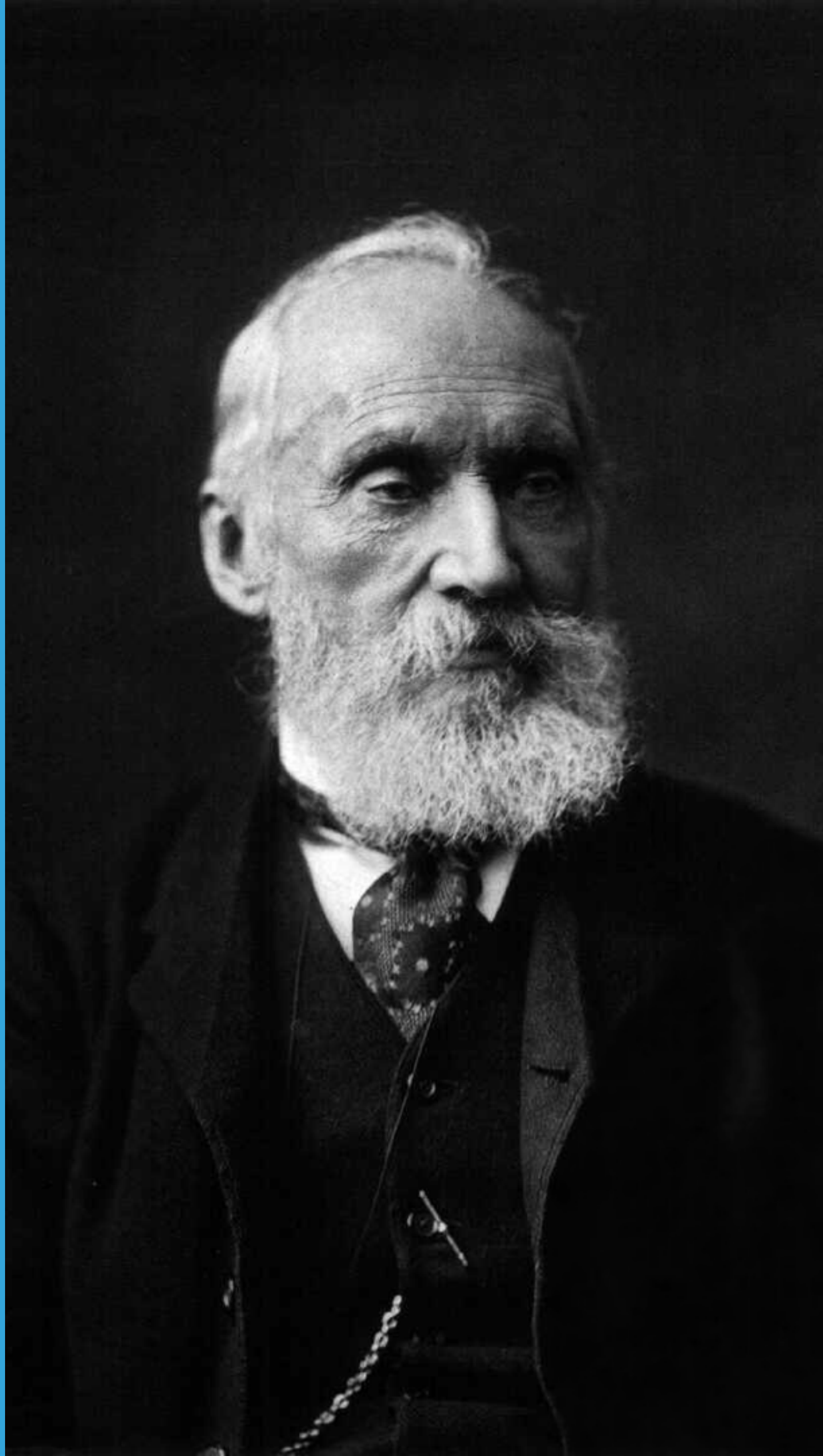
<https://www.jeremiahgrossman.com/>

<http://blog.jeremiahgrossman.com/>

## WHO I AM...

- ▶ Professional Hacker
- ▶ Person of the Year (OWASP, 2015)
- ▶ International Speaker
- ▶ Black Belt in Brazilian Jiu-Jitsu
- ▶ Founder of WhiteHat Security

- ▶ Intersection of security guarantees and cyber-insurance
- ▶ Malware / Ransomware
- ▶ Easing the burden of vulnerability remediation
- ▶ Security crowd-sourcing
- ▶ Industry skill shortage



**"I OFTEN SAY THAT WHEN YOU CAN MEASURE WHAT YOU ARE SPEAKING ABOUT, AND EXPRESS IT IN NUMBERS, YOU KNOW SOMETHING ABOUT IT;**

**BUT WHEN YOU CANNOT MEASURE IT, WHEN YOU CANNOT EXPRESS IT IN NUMBERS, YOUR KNOWLEDGE IS OF A MEAGRE AND UNSATISFACTORY KIND."**

**Lord Kelvin**

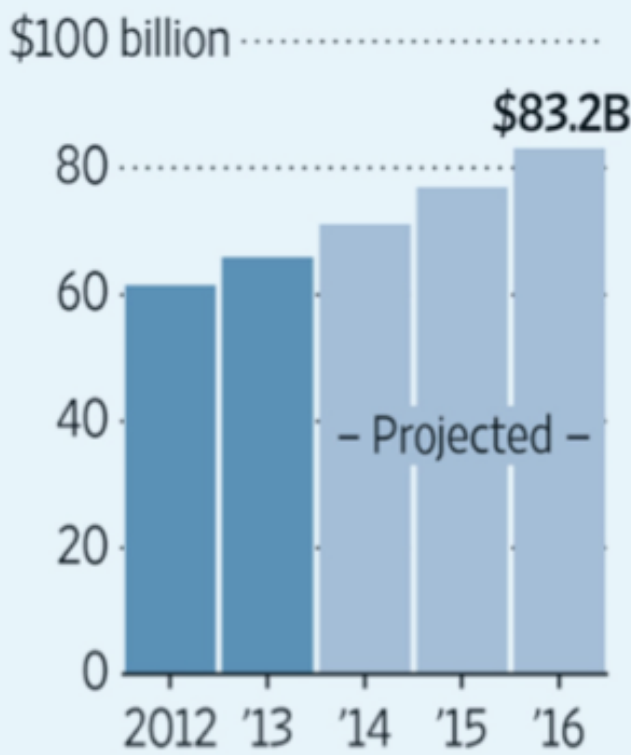


“2015 GLOBAL SPENDING ON INFORMATION SECURITY IS SET TO GROW BY CLOSE TO 5% THIS YEAR TO TOP \$75BN,....”

Cyber Spike

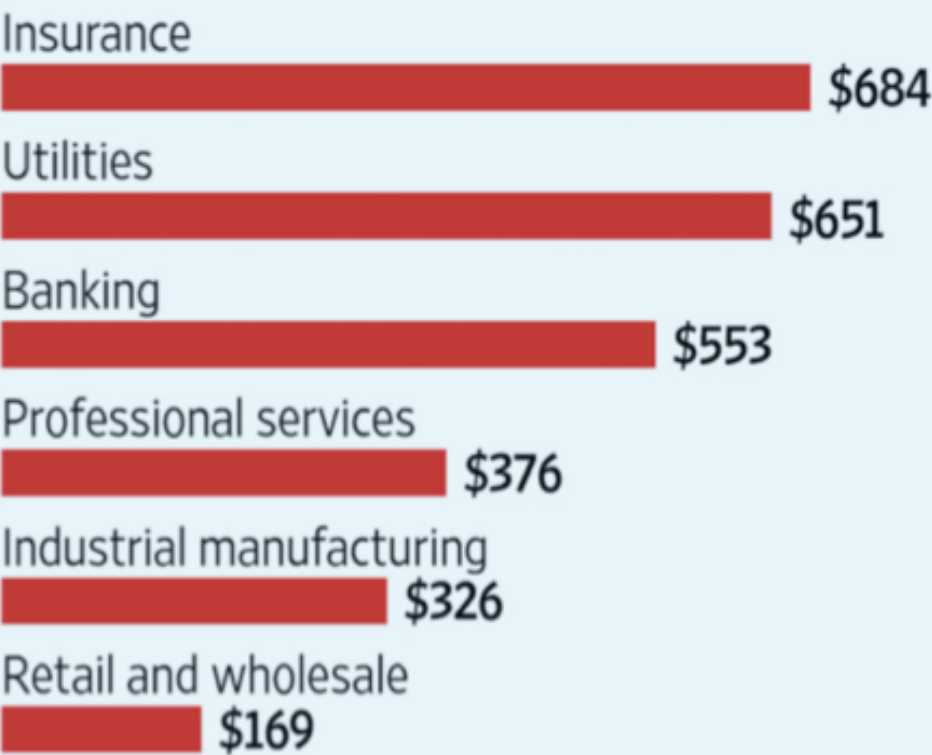
Companies are ramping up their spending to prevent cyberattacks after a string of breaches at financial firms and big retailers.

World-wide security spending



Source: Gartner

World-wide 2013 information security spending per employee by industry



The Wall Street Journal



**HACKTIVISTS**



**ORGANIZED CRIME**



**NATION-STATE**

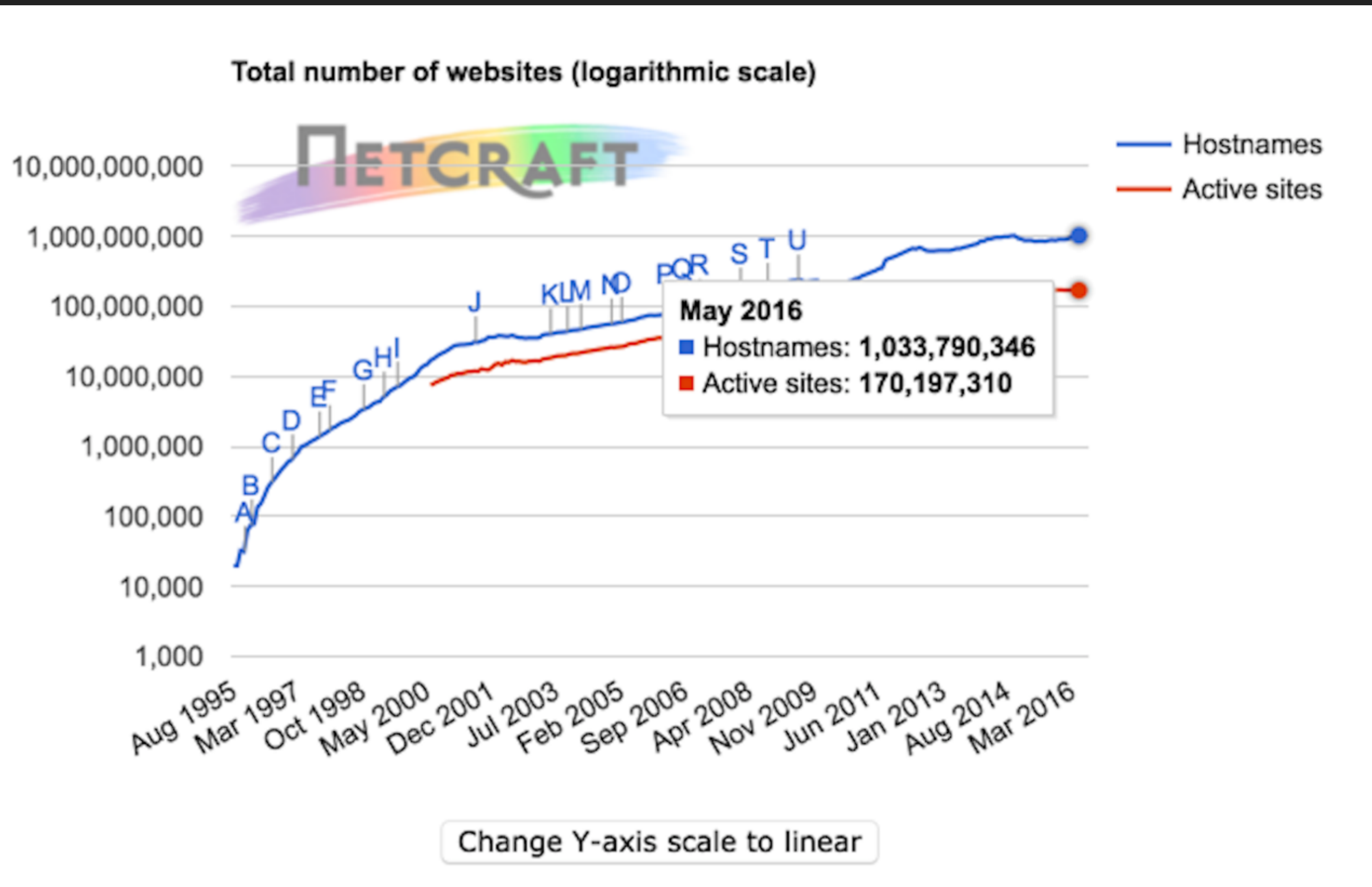


**TERRORISM?**

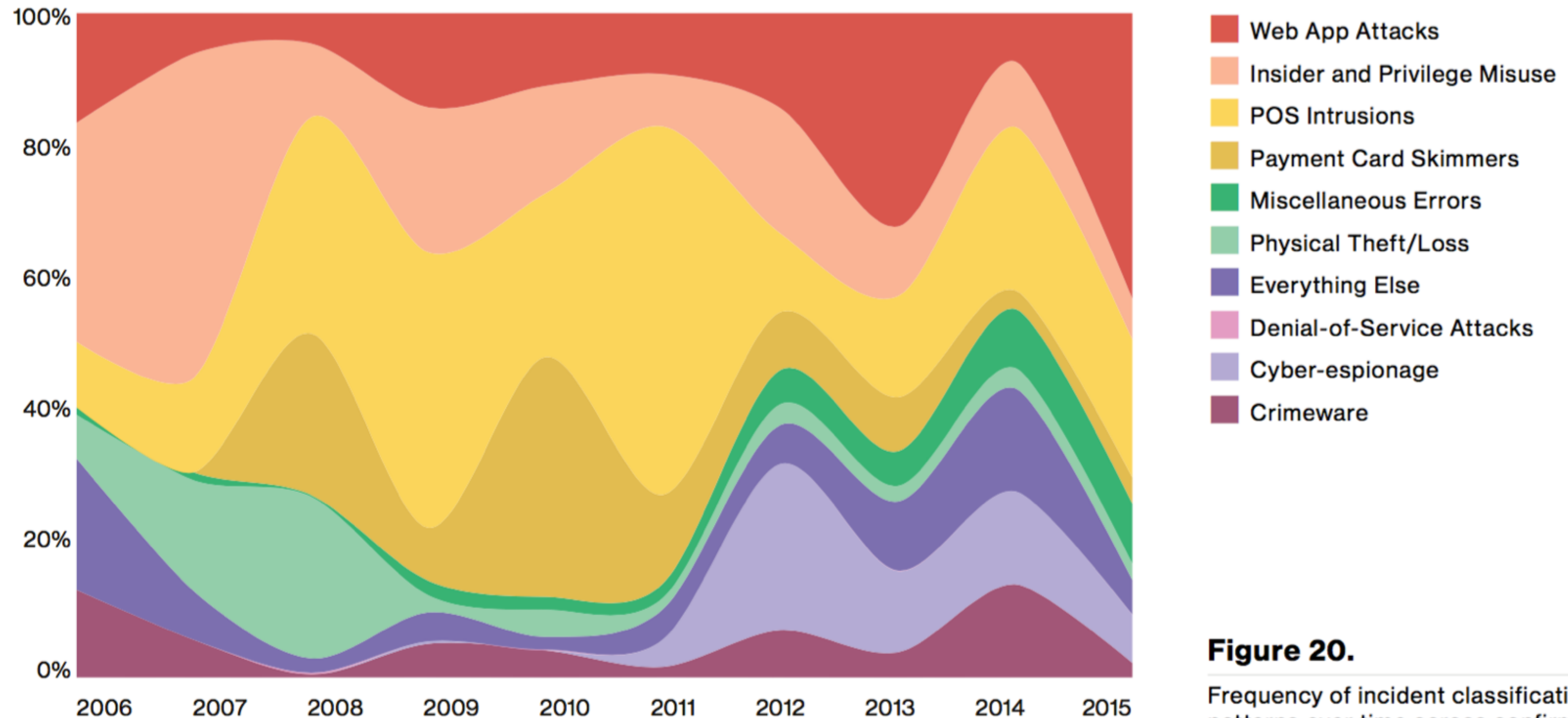


# 1,073,777,722

## NETCRAFT: JULY 2016 WEB SERVER SURVEY



# NO WAY REGULATIONS CAN KEEP UP.



**Figure 20.**

Frequency of incident classification patterns over time across confirmed data breaches.

FREQUENCY OF INCIDENT CLASSIFICATION PATTERNS OVER TIME ACROSS CONFIRMED DATA BREACHES.

VERIZON DATA BREACH INVESTIGATIONS REPORT (2016)

# "APPSEC IS EATING SECURITY"

## INCIDENT PATTERNS BY INDUSTRY

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps
			1%	<1%	1%	<1%	95%	1%	1%
	7%		17%	17%	27%			3%	30%
				3%			47%		50%
1%	<1%	<1%	2%	<1%	2%	9%		4%	82%
3%	3%		11%	19%	22%		7%	32%	3%
1%	3%		4%		25%		1%	11%	57%
3%	47%		3%				3%	24%	21%
4%	19%		25%	4%	15%			21%	13%
12%	16%		4%	9%	37%			13%	9%
1%	1%		4%		1%	3%	64%	2%	26%

**Figure 22.**

Incident patterns by industry  
(only confirmed data breaches)

Accommodation (72), n=282

Educational (61), n=29

Entertainment (71), n=38

Finance (52), n=795

Healthcare (62), n=115

Information (51), n=194

Manufacturing (31-33), n=37

Professional (54), n=53

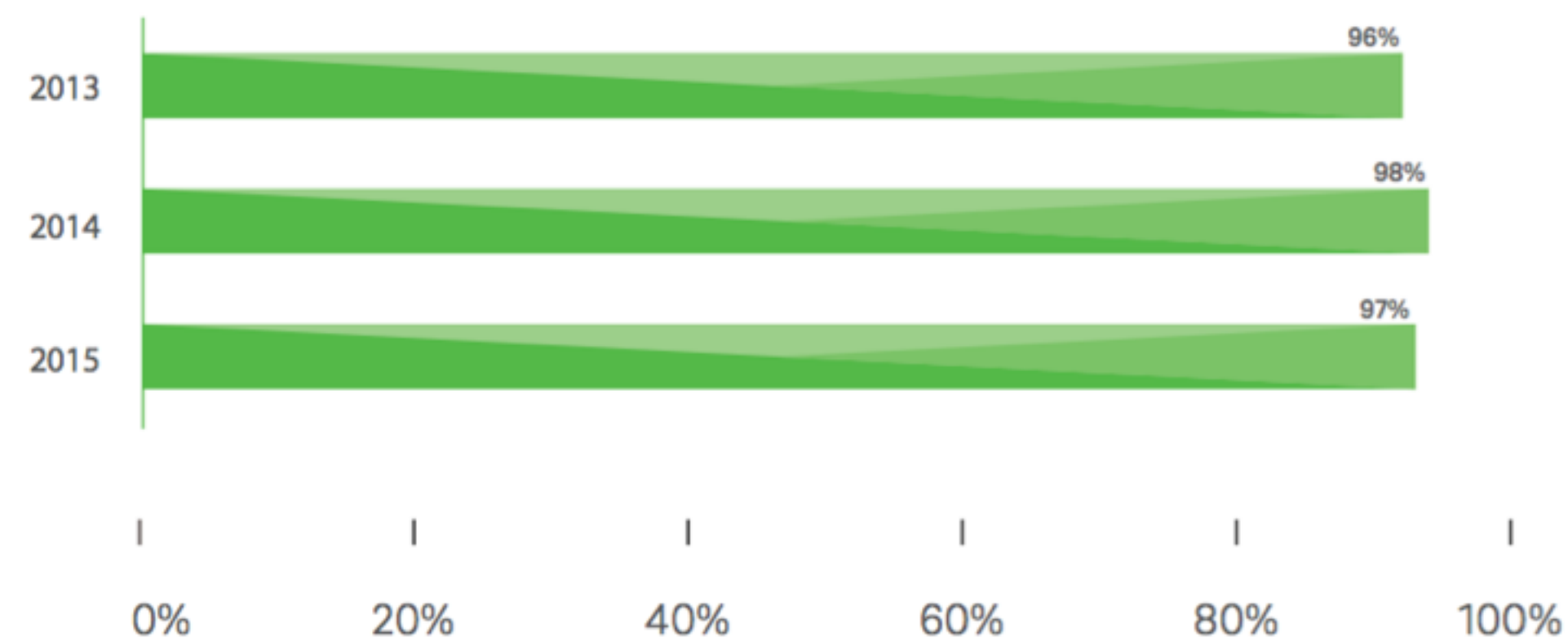
Public (92), n=193

Retail (44-45), n=182



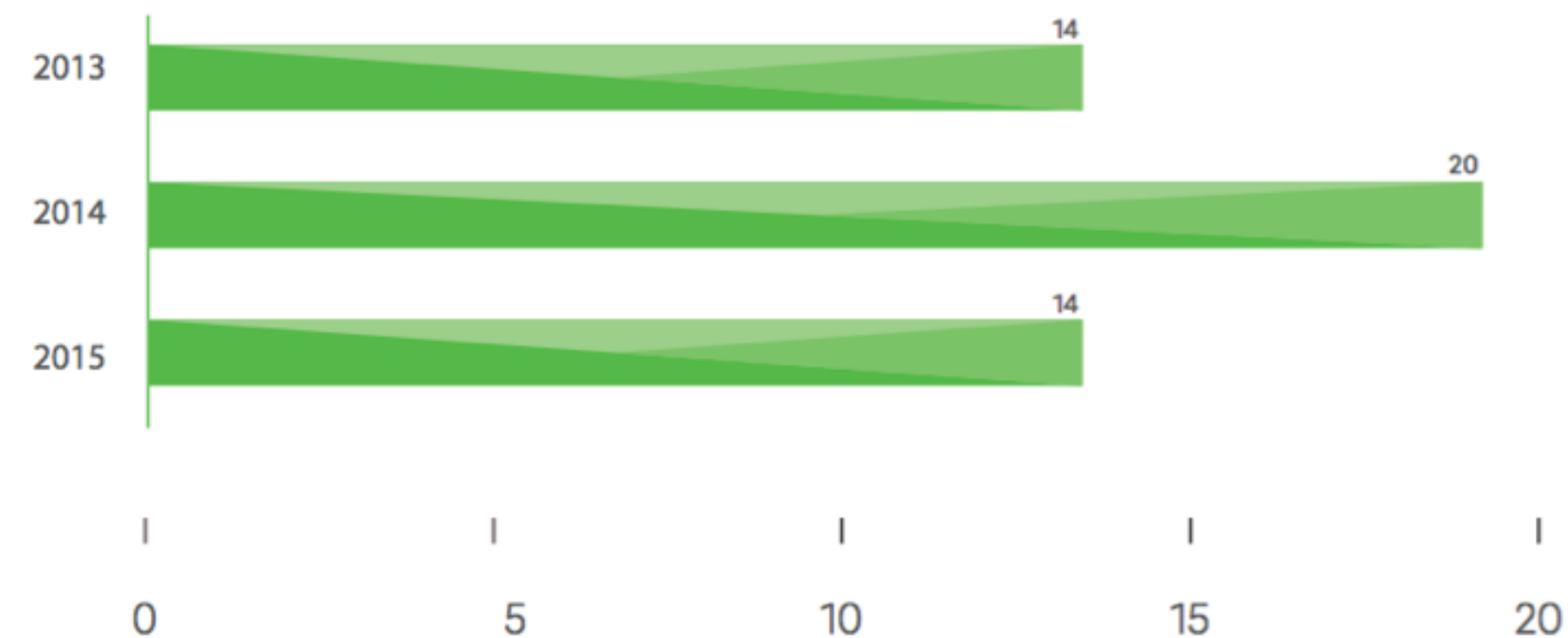
# APPLICATION SECURITY

## VULNERABLE APPLICATIONS



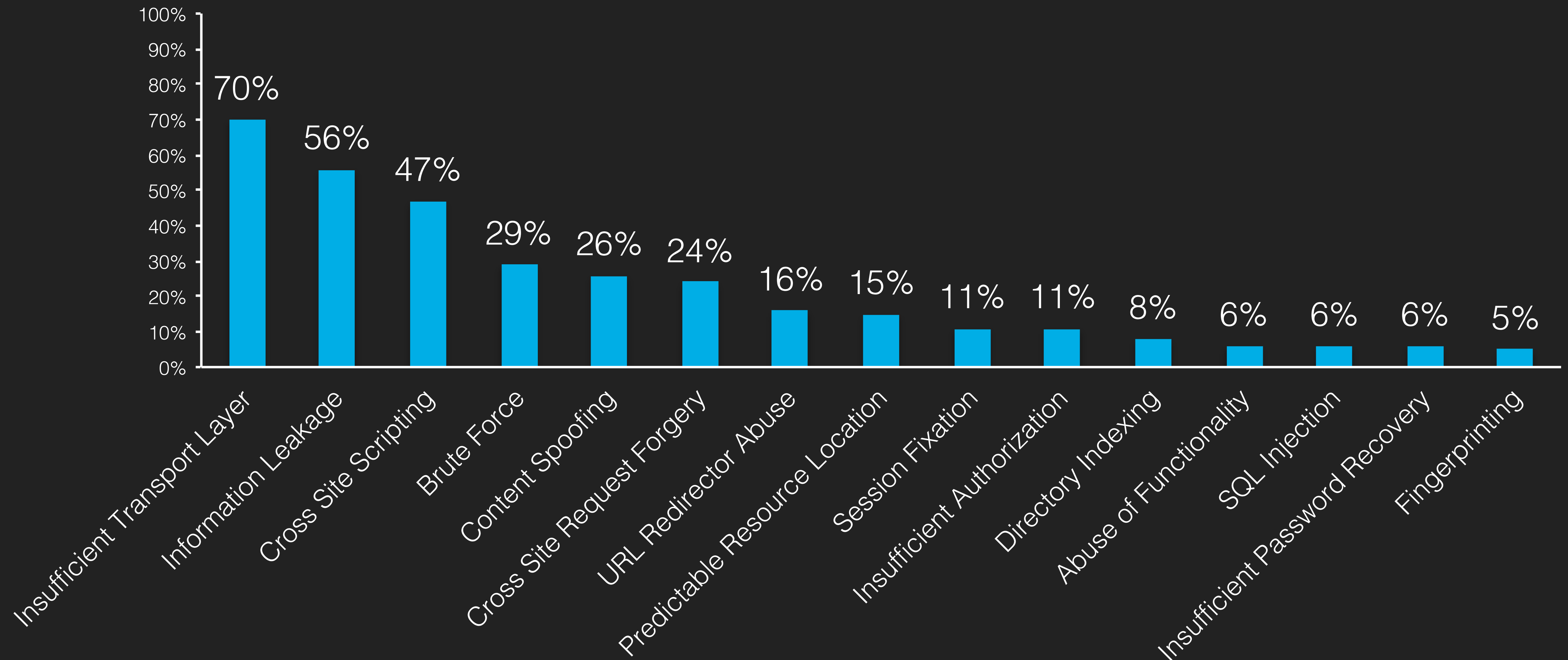
The median number of vulnerabilities per application decreased 30 percent in 2015 compared to the prior year, from 20 to 14. The maximum number of vulnerabilities we found in a single application was 667.

## MEDIAN VULNERABILITIES PER APPLICATION





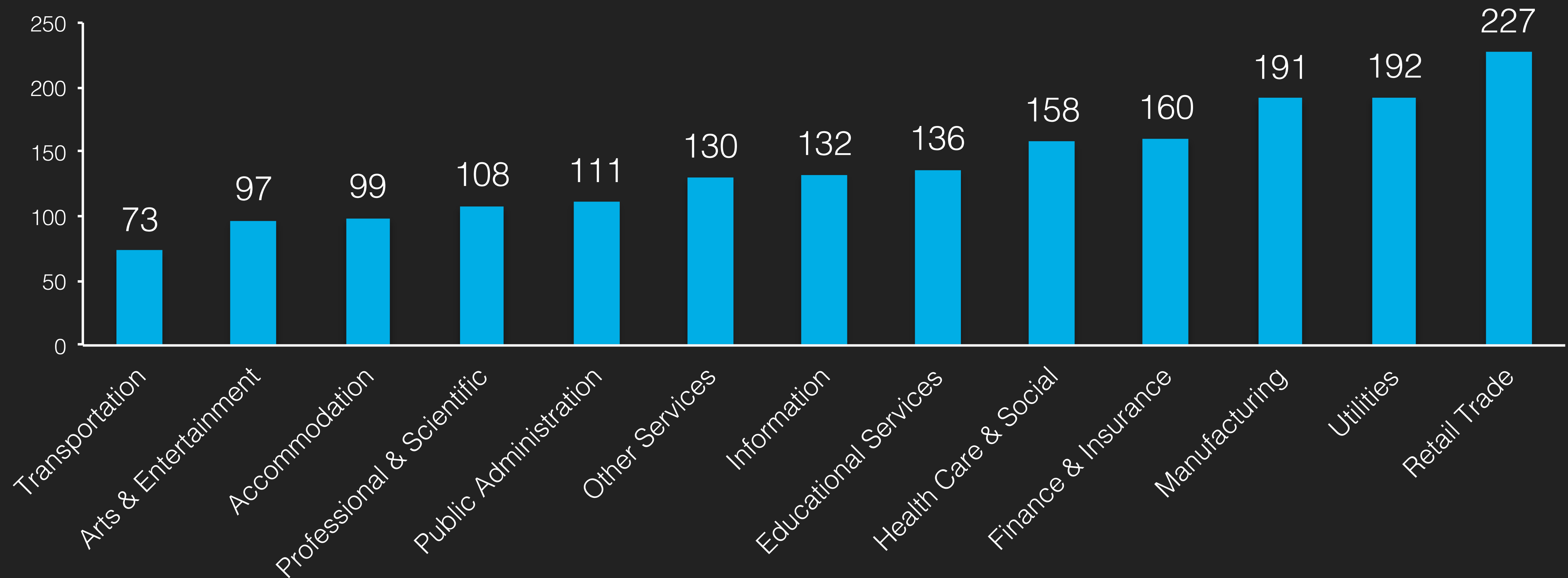
# VULNERABILITY LIKELIHOOD (1 OR MORE)



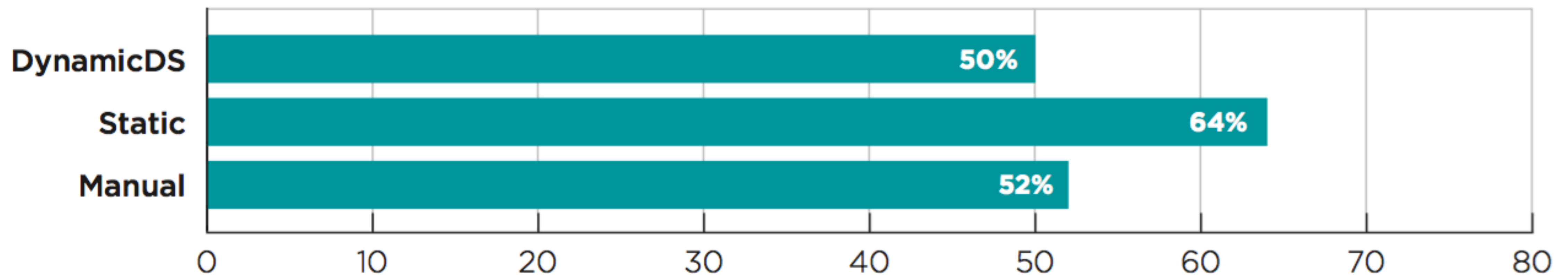
# TOP 10 VULNERABILITY CATEGORIES BY PROGRAMMING LANGUAGE

Language	CWE Category	Apps Affected
OVERALL	Code Quality	63%
	Cryptographic Issues	58%
	Information Leakage	56%
	CRLF Injection	49%
	Directory Traversal	47%
	Cross-Site Scripting (XSS)	47%
	Insufficient Input Validation	37%
	SQL Injection	29%
	Credentials Management	25%
	Time and State	23%

# AVERAGE TIME-TO-FIX (DAYS)

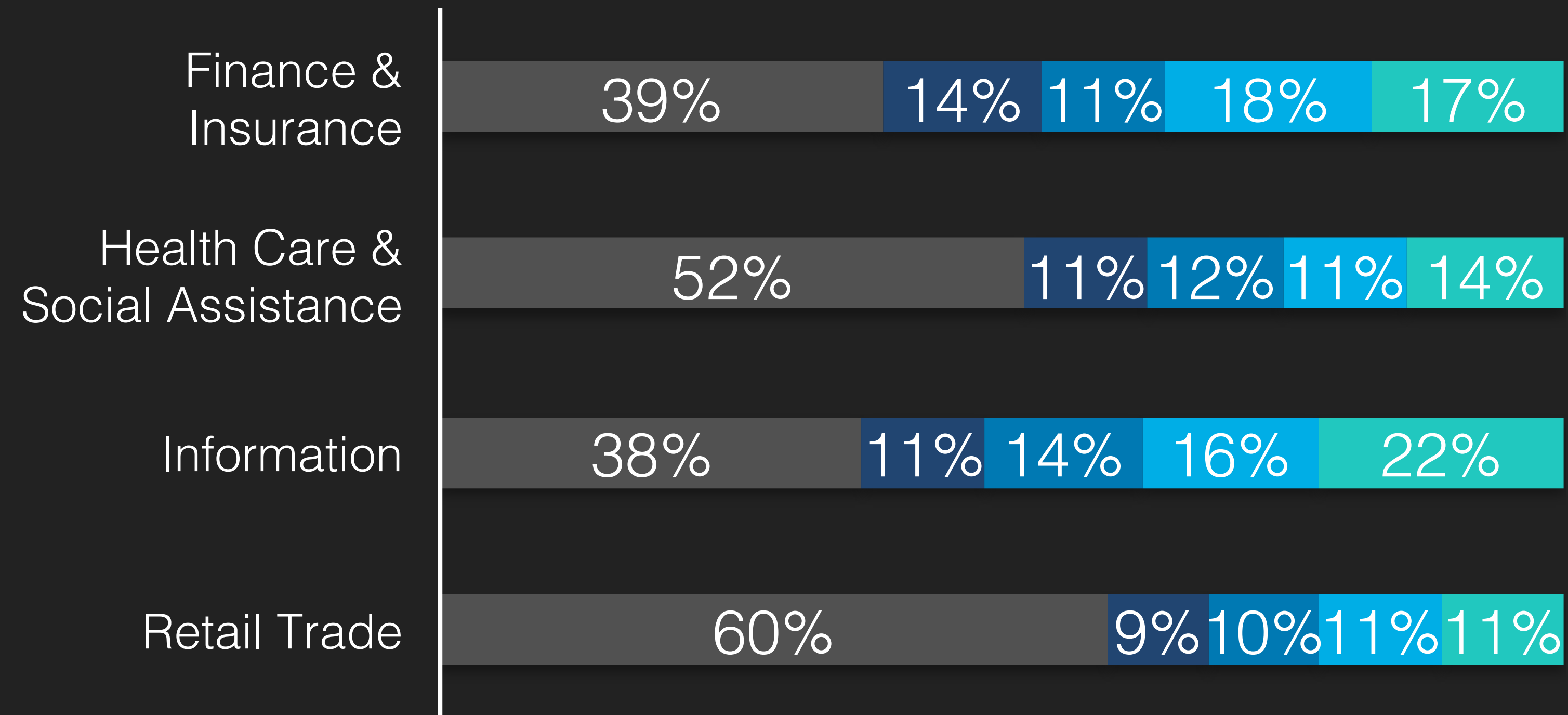


# PERCENT VULNERABILITIES FOUND VS. FIXED



**Figure 8:** Percent vulnerabilities found vs. fixed

# WINDOWS OF EXPOSURE

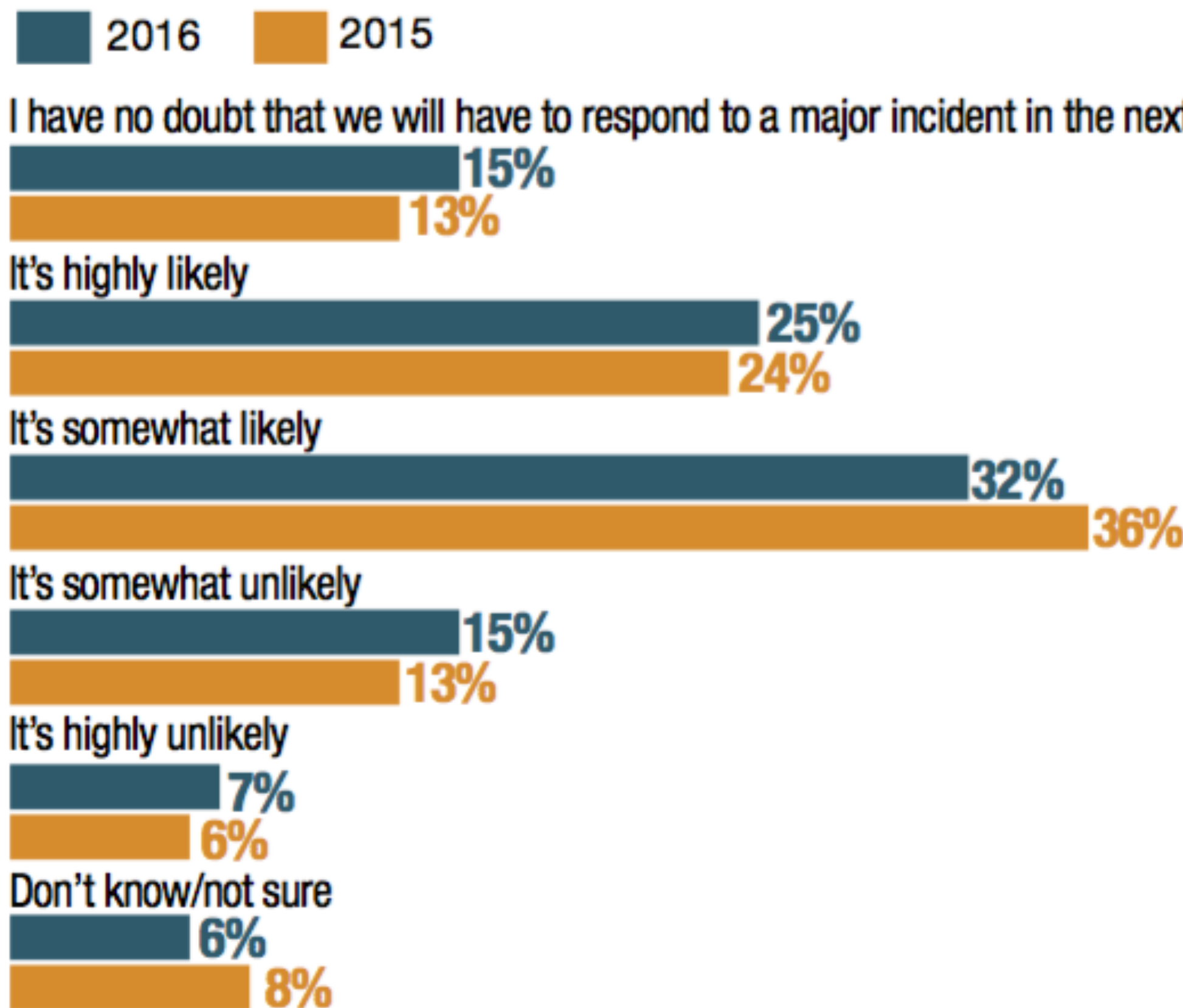


- Always Vulnerable
- Frequently Vulnerable (271-364 days a year)
- Regularly Vulnerable (151-270 days a year)
- Occasionally Vulnerable (31-150 days a year)
- Rarely Vulnerable (30 days or less a year)



Figure 1

# How likely do you think it is that your organization will have to respond to a major security breach in the next 12 months?



Base: 250 respondents in 2016 and 460 respondents in 2015  
Data: UBM survey of security professionals, June 2016



InformationWeek  
**DARK**Reading

CONNECTING THE INFORMATION SECURITY COMMUNITY

7/14/2016  
10:00 AM

Sara Peters  
Commentary

Connect Directly

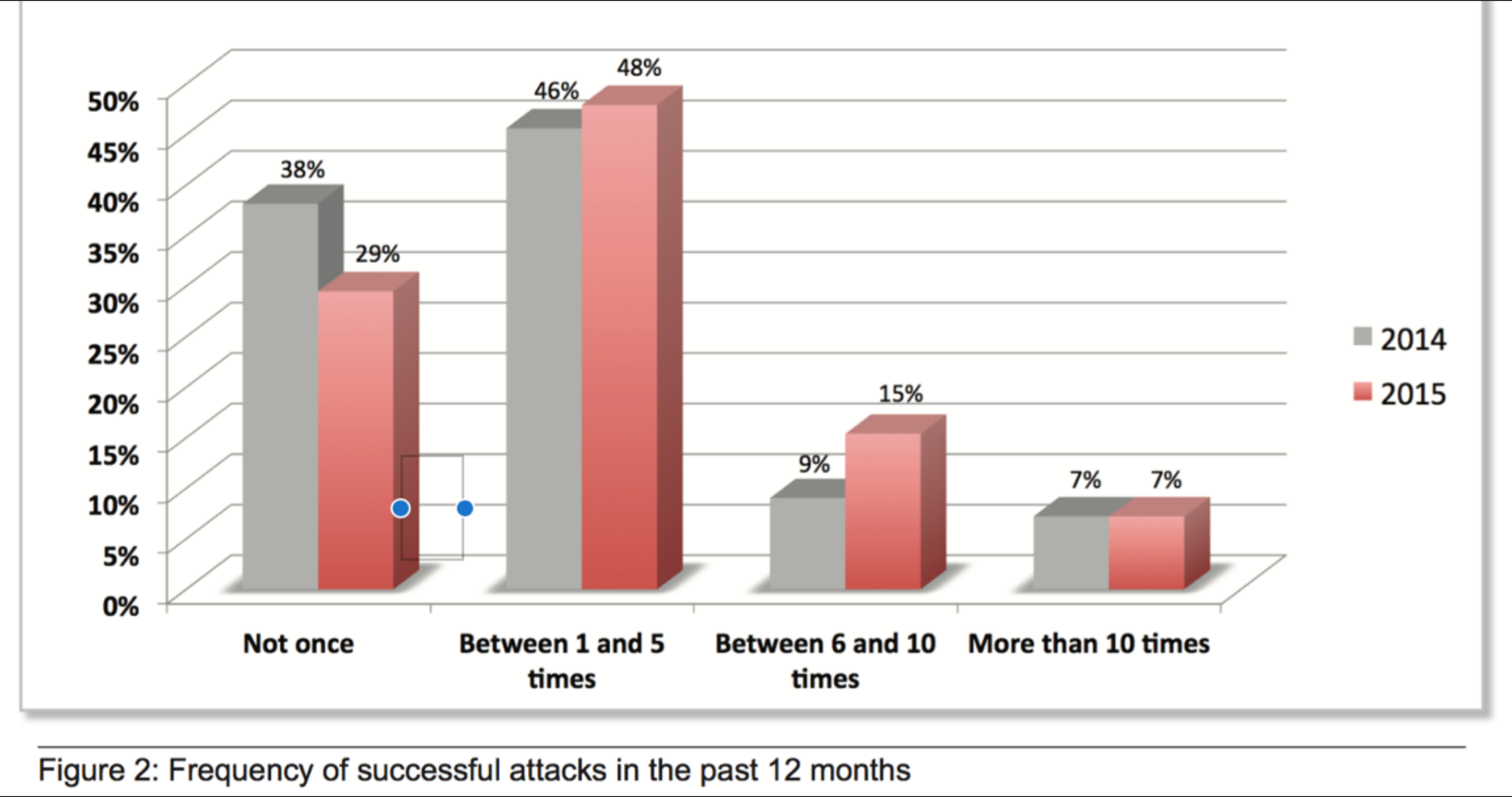
## 72% of Black Hat Attendees Expect To Be Hit By 'Major' Data Breach Within A Year

End users are the biggest weakness, and we're not doing enough to address the problem.

Some of the most qualified security professionals around are more confident in attackers than they are in themselves or their end users.



# HOW MANY TIMES DO YOU ESTIMATE THAT YOUR ORGANIZATION'S GLOBAL NETWORK HAS BEEN COMPROMISED BY A SUCCESSFUL CYBERATTACK WITHIN THE LAST 12 MONTHS?



# WHAT IS THE LIKELIHOOD THAT YOUR ORGANIZATION'S NETWORK WILL BECOME COMPROMISED BY A SUCCESSFUL CYBERATTACK IN 2015?

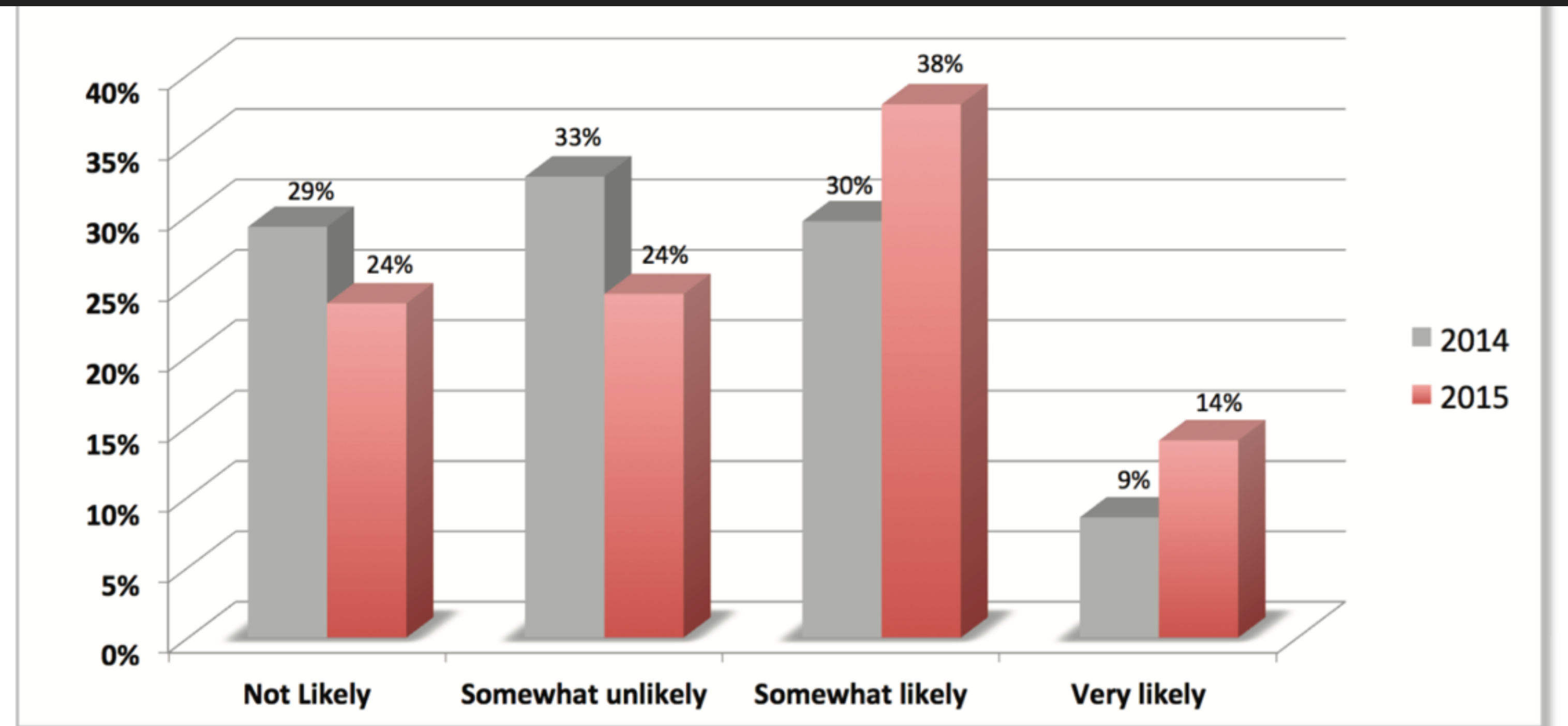


Figure 3: Likelihood of being successfully attacked in the next 12 months

**“71% WERE AFFECTED BY A  
SUCCESSFUL CYBERATTACK IN  
2014, BUT ONLY 52% EXPECT TO  
FALL VICTIM AGAIN IN 2015.”**



### **Survey Demographics**

- 814 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 7 countries in North America and Europe
- Representing 19 industries

## DO YOU EXPECT A CYBERATTACK TO STRIKE YOUR ORGANIZATION IN 2015? (N = 3,435)

A. YES	46%
B. NO	24%
C. UNSURE	30%



### 2015 Global Cybersecurity Status Report

January 2015

[www.isaca.org/cybersecurityreport](http://www.isaca.org/cybersecurityreport)

Number of respondents (n) = 3,439

Respondents are global business and IT professionals who are members of ISACA.

**APATHETIC.**

**REALISTIC.**

**BOTH?**

# RANGE OF EXPECTED LOSSES

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



# CYBER-INSURANCE

- ▶ 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.



“ACCORDING TO PWC, THE CYBER INSURANCE MARKET IS SET TO TRIPLE IN THE NEXT FEW YEARS AND WILL REACH \$7.5 BILLION BY 2020.”





“THE LARGEST BARRIER TO GROWTH IS LACK OF ACTUARIAL DATA ABOUT CYBERATTACKS, BUT THIS IS QUICKLY CHANGING WITH CONTINUED CYBER ASSAULTS.”

“ABI RESEARCH FORECASTS THE MARKET TO HIT US \$10 BILLION BY 2020.”

### Risks to Drive US\$10 Billion Cyber Insurance Market by 2020

ABIresearch®

Share: [in](#) [f](#) [t](#)

Continued and sustained cyberattacks are having a ruinous effect on enterprises and driving up the cost of incident response. With over 900 million reported records exposed in 2014, more companies are seriously starting to consider transferring risks to insurance providers. Despite growing awareness of vulnerability to breaches and risk management strategies however, less than 20% of large enterprises avail themselves of cyber insurance. For small- and medium-sized enterprises, the percentage is even lower, at less than 6%, according to ABI Research.

The largest barrier to growth is lack of actuarial data about cyberattacks, but this is quickly changing with continued cyber assaults. Currently, insurers are finding it difficult to assign the proper value to data or systems, or to determine appropriate policies since they are unable to scope the cyber risk environment of an organization.

“More information sharing, and understanding of event impact and the associated longer-term costs (through post-incident analytics, for example) can help remove some of these obstacles. In turn this will drive better policy rates and see the cyber insurance market progressively emerge from its niche, despite being around for over 30 years,” says Michela Menting, Research Director.

ABI Research forecasts the market to hit US\$10 billion by 2020. While still a fraction of the total global insurance market, the 36.6% CAGR is highly dynamic. The primary driver for this dynamism is the escalating costs associated with cyber breaches and attacks, pushing risk management strategies to increasingly transfer risks to providers.

The Cyber Risk, Liability and Insurance report looks at cyber risks and how they can be managed; the attribution of liability for cyber breaches and attacks; and the growth of a specific cyber insurance market. It is published within the [Cybersecurity Technologies and Cybersecurity Strategies for Critical Infrastructure Market Research](#). Insurance providers reviewed include ACE, AIG, AGCS, AXA Group, Liberty International Underwriters, Lloyds of London, Marsh & McLennan, Scottsdale Insurance Company, and Zurich North America.

ABI Research provides technology market research and technology intelligence for industry innovators. From offices in North America, Europe and Asia, ABI Research's worldwide team of experts advises thousands of decision makers through 70+ research and advisory services. Est. 1990. For more information visit [www.abiresearch.com](http://www.abiresearch.com), or call +1.516.624.2500.

**“ABOUT A THIRD OF U.S. COMPANIES  
ALREADY HAVE SOME FORM OF CYBER-  
INSURANCE COVERAGE, ACCORDING TO A  
REPORT PRICEWATERHOUSECOOPERS  
RELEASED LAST YEAR.”**





## BREACH CLAIMS

- ▶ 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

### Spending on cyberattack insurance soars as hacks become more common



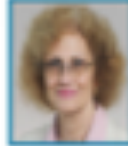
## BREACH CLAIMS


- ▶ “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

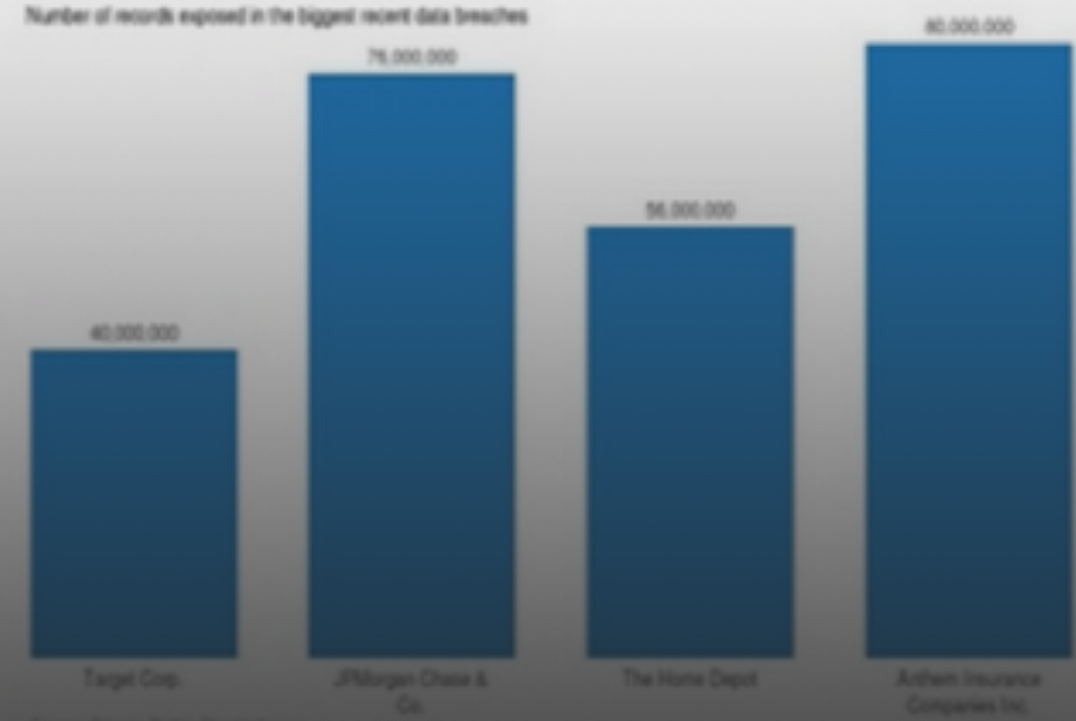
# AIG unit leads Anthem's cyber coverage

By  Judy Greenwald

 **SHARE**

Risk Manage

**Cyber Attacks**  
Number of records exposed in the biggest recent data breaches



Company	Number of records exposed
Target Corp.	40,000,000
JPMorgan Chase & Co.	76,000,000
The Home Depot	56,000,000
Anthem Insurance Companies Inc.	80,000,000

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



**“AVERAGE RATES FOR RETAILERS SURGED 32% IN THE FIRST HALF OF THIS YEAR, AFTER STAYING FLAT IN 2014, ACCORDING TO PREVIOUSLY UNREPORTED FIGURES FROM MARSH.”**

**“AND EVEN THE BIGGEST INSURERS WILL NOT WRITE POLICIES FOR MORE THAN \$100 MILLION FOR RISKY CUSTOMERS.”**



# 2014 – 2015

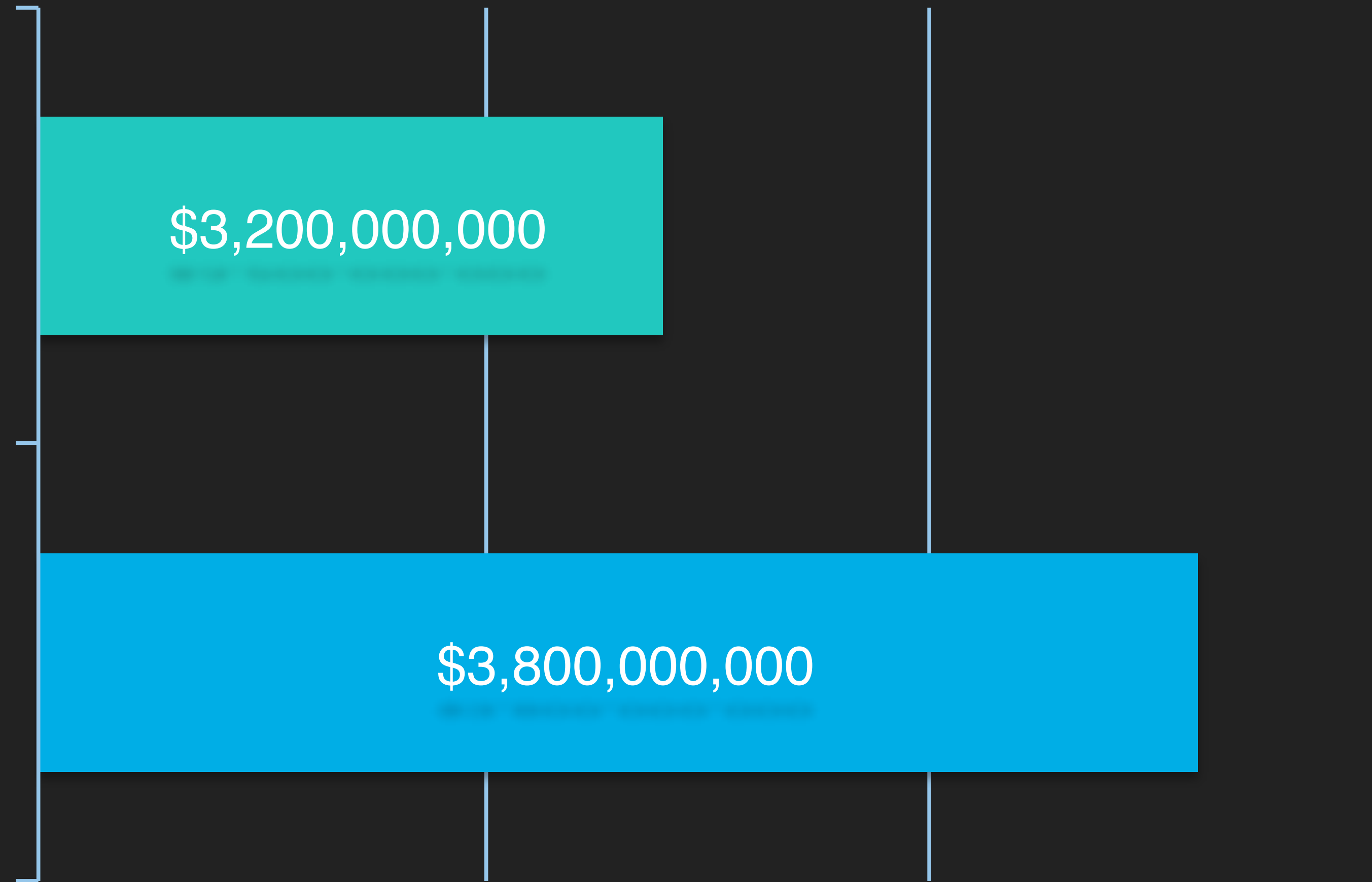
## NEW SECURITY INVESTMENT VS. CYBER-INSURANCE

Cyber-Security Insurance  
~\$3.2 billion in spending (+67%)

\$3,200,000,000

Information Security Spending (Global)  
~ \$3.8 billion in new spending (+4.7%)

\$3,800,000,000



**ALL  
SALES  
FINAL**

**EVER NOTICE HOW  
EVERYTHING IN THE  
INFORMATION SECURITY  
INDUSTRY IS SOLD “AS IS”?**

---

**NO GUARANTEES**

**NO WARRANTIES**

**NO RETURN POLICIES**



A high-angle, black and white photograph of a large, crowded exhibition hall. The hall is filled with people walking through aisles lined with various booths and displays. In the center, a large booth features a sign that reads "CONNECTED SECURITY" and "SMARTER SECURITY" with the McAfee logo. Other booths in the background have signs for "Verizon" and "Comcast". The architecture of the hall is modern, with a curved, ribbed ceiling.

**INFORMATION SECURITY**

**THE  
\$75 BILLION  
GARAGE SALE**



WELLS FARGO

PersonalSmall BusinessCommercial

BankingLoans and CreditInsuranceInvesting and RetirementWealth Management

Personal > Privacy, Security, and Legal > Online Security Guarantee

Online Security Guarantee

Our commitment

For more than 160 years, Wells Fargo has stood as a symbol of strength and security, serving as ever and use proven technology to protect your personal information.

Our guarantee

We guarantee that you will be covered for 100% of funds removed from your Wells Fargo account removes those funds through our Online Services. To qualify for this guarantee, you must follow the following steps:

Online Services means any Wells Fargo Online® or Wells Fargo Business Online® services you use for transactions (including trading losses incurred through unauthorized access and activity): (1) use your mobile device at wf.com, via text at our 93557 short code, or via one of our Wells Fargo

TD

About TDInvestor RelationsEconomicsCareersCorporate ResponsibilityTo Our Customers

How We Protect You > Online Security Guarantee

Your TD Online and Mobile Security Guarantee

How We Protect You

Online Security Guarantee

Online Security


Card Security

How You Can Protect Yourself

Our Privacy Commitments

Report Online Fraud

Options For Electronic Communications



You're protected.

In the unlikely event you experience a TD account transaction resulting from a transaction through a TD online or mobile service, that you did not authorize, you will receive 100% reimbursement of those account losses provided you have met your security responsibilities.

How we protect you

We've made a commitment to keep your online and mobile transactions secure and as safe as possible. The safeguards we've put in place to protect the security, privacy and integrity of your information during transactions include:

- Secure firewalls help prevent unauthorized access to our internal systems.

PNC

BANKINGBORROWINGINVESTMENT & RETIREMENT

Online Banking Security Pledge and Bill Pay Guarantee

With PNC Bank's Online Banking and Bill Pay service, we strive to protect your personal and financial information and to process your online transactions in a timely and accurate manner.

RBC Royal Bank

Bank AccountsCredit CardsMortgagesLoansInvestmentsAdvice

Personal Banking

Accounts & Services

Credit Cards

Mortgages

Loans & Lines of Credit

Investments

Insurance

U.S. Banking

Online Services

Business Banking

Commercial Banking

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.**<sup>+</sup>

To receive reimbursement under this guarantee, you must:

- Sign out and close your Internet browser at the end of each Online session
- Keep your password and personal verification questions (and answers) confidential
- Contact us immediately if you know or suspect that your password has become known to someone else, or if there has been suspicious activity on your account that you did not authorize

For additional details for personal clients, please see the [Electronic Agreement](#)

SECURITY GUARANTEES

---

**INFOSEC'S BIGGEST OPPORTUNITY**

## CASE STUDIES

- ▶ SentinelOne
- ▶ WhiteHat Security
- ▶ Trusona
- ▶ Others...



DETAILS

- ▶ Program Launched: July 2016.
- ▶ Setting up their guarantee with the underwriter took 3 months.
- ▶ Claims or payouts? 0.



D23		
	A	B
1		<b>Guarantee Program Assumptions</b>
2		Number of Endpoints
3		Estimated Annual Infection Rate per Endpoint (false-negatives)
4		Post-Infection Rollback Feature Success Rate
5		Ransom Payment per Endpoint (Max \$1000)
6		Reinsurance Premium per Endpoint
7		Reinsurance Deductable % per [Max] Ransom Payment
8		Reinsurance Deductable per [Max] Endpoint
9		Annual Maximum Ransom Payout per SentineOne Customer
10		
11		
12		<b>Estimated Infections Outcomes w/ SentinelOne</b>
13		Total Annual Endpoint Infections
14		Total Annual Endpoint Infections where Rollback Failed
15		
16		
17		<b>Financial Analysis</b>
18		Total Annual Reinsurance Premiums
19		Total Annual Ransom Payout Loss (Max)
20		Total Annual Reinsurance Deductable Loss
21		
22		<b>SentinelOne: Total Annual Costs &amp; Losses of the Program</b>



**SENTINELONE'S GUARANTEE OFFERS FINANCIAL SUPPORT OF \$1,000 PER ENDPOINT (UP TO \$1 MILLION PER COMPANY), SECURING AGAINST FINANCIAL IMPLICATIONS OF A RANSOMWARE INFECTION, IF SENTINELONE IS UNABLE TO BLOCK OR REMEDIATE THE EFFECTS.**

## DETAILS

- ▶ Program Launched: August 2014.
- ▶ Setting up their guarantee with the underwriter took 18 months.
- ▶ Claims or payouts? 0.



**IF A WEBSITE COVERED BY SENTINEL ELITE  
IS HACKED, EXPLOITED BY A MISSED  
VULNERABILITY, THE CUSTOMER WILL BE  
REFUNDED IN FULL AND OFFERED UP TO  
\$500,000 IN BREACH LOSS COMPENSATION.**



## DETAILS





- ▶ Program Launched: January 2016.
- ▶ Setting up their guarantee with the underwriter took 18 months.
- ▶ Stroz Friedberg ran the assessments on behalf of the underwriter to measure performance.
- ▶ Claims or payouts? 0.



### **ZERO FRAUD: 6 years & counting**

- Total number of cards issued: 4,182,875
- Total number of transactions: 119,146,069
- False acceptance rates: 0.000%
- False rejection rates\*: 0.200%

• False rejections 226,974 due to bad read on the first attempt.  
• Most were authenticated on the subsequent attempt.

<b>A+ Rated Insurance Carrier Coverage</b>	<b>\$0</b>	<b>\$1,000</b>	<b>\$25,000</b>	<b>\$1,000,000</b>
<b>Cost per User/Mo. Unlimited Trx</b>	\$1 Free <100	\$8 \$4 / no ins	\$40 \$20 / no ins	\$100 \$50 / no ins
<b>Documents</b>	DL	DL	DL & Passport	DL & ePassport
<b>ID-Proofing</b>	No	Verified	Verified	In-Person
<b>% of Users</b>	50%	45%	4%	1%
<b>User Credential</b>	TruPIN 	TruPIN/TouchID 	TruDL 	TruToken/Card 



# MALWARE KITS COME WITH WARRANTIES

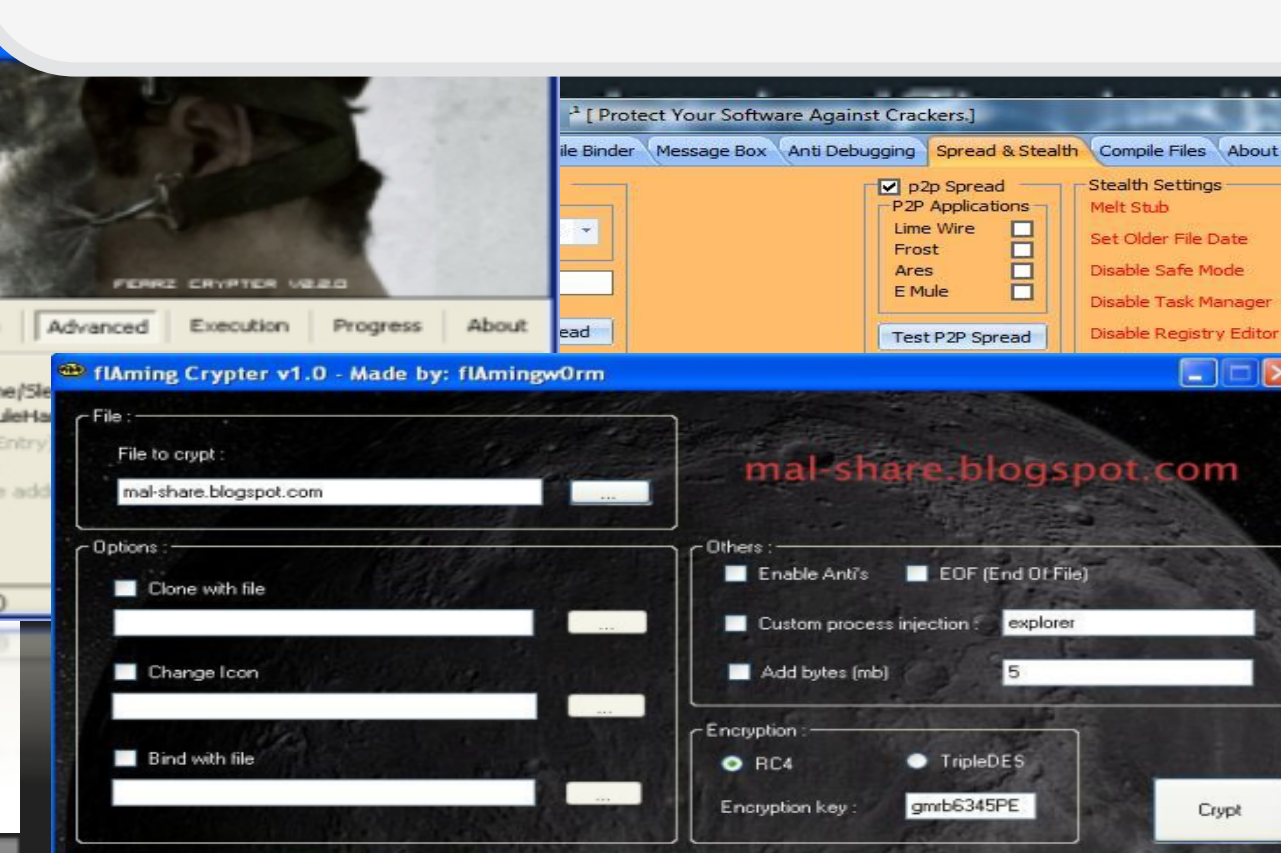
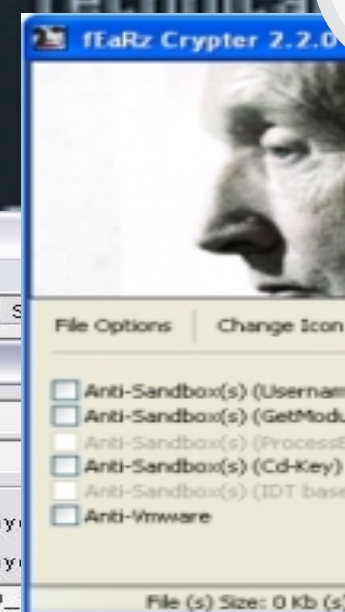
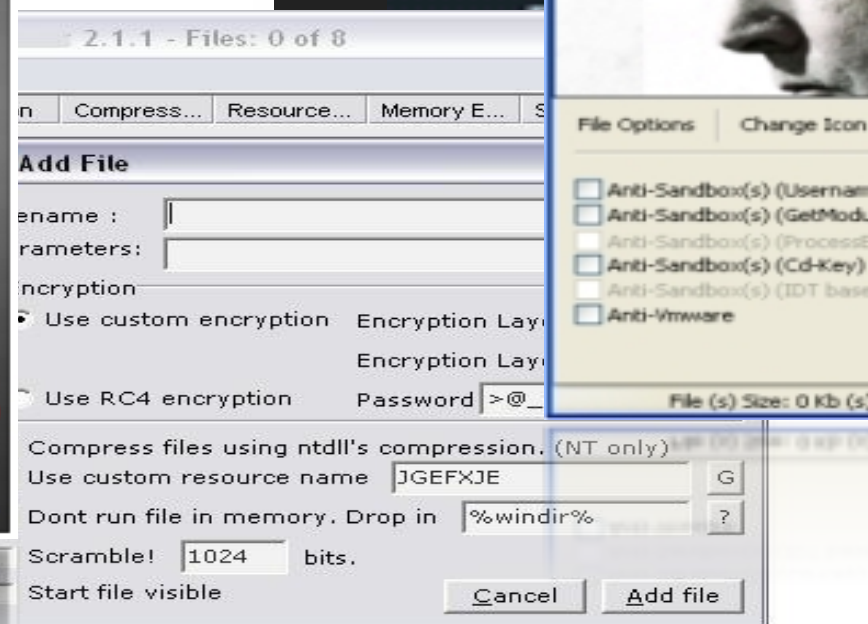


**Gold Edition**

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers

- Supports Windows 95/98/2000/2003/XP/Vista
- Remote S...
- Webcam
- Controllin...
- Notifies o...
- Technical
- 

Malware offered for **\$249** with a service level agreement (SLA) and **replacement warranty** if the creation **is detected by any antivirus** within 9 months





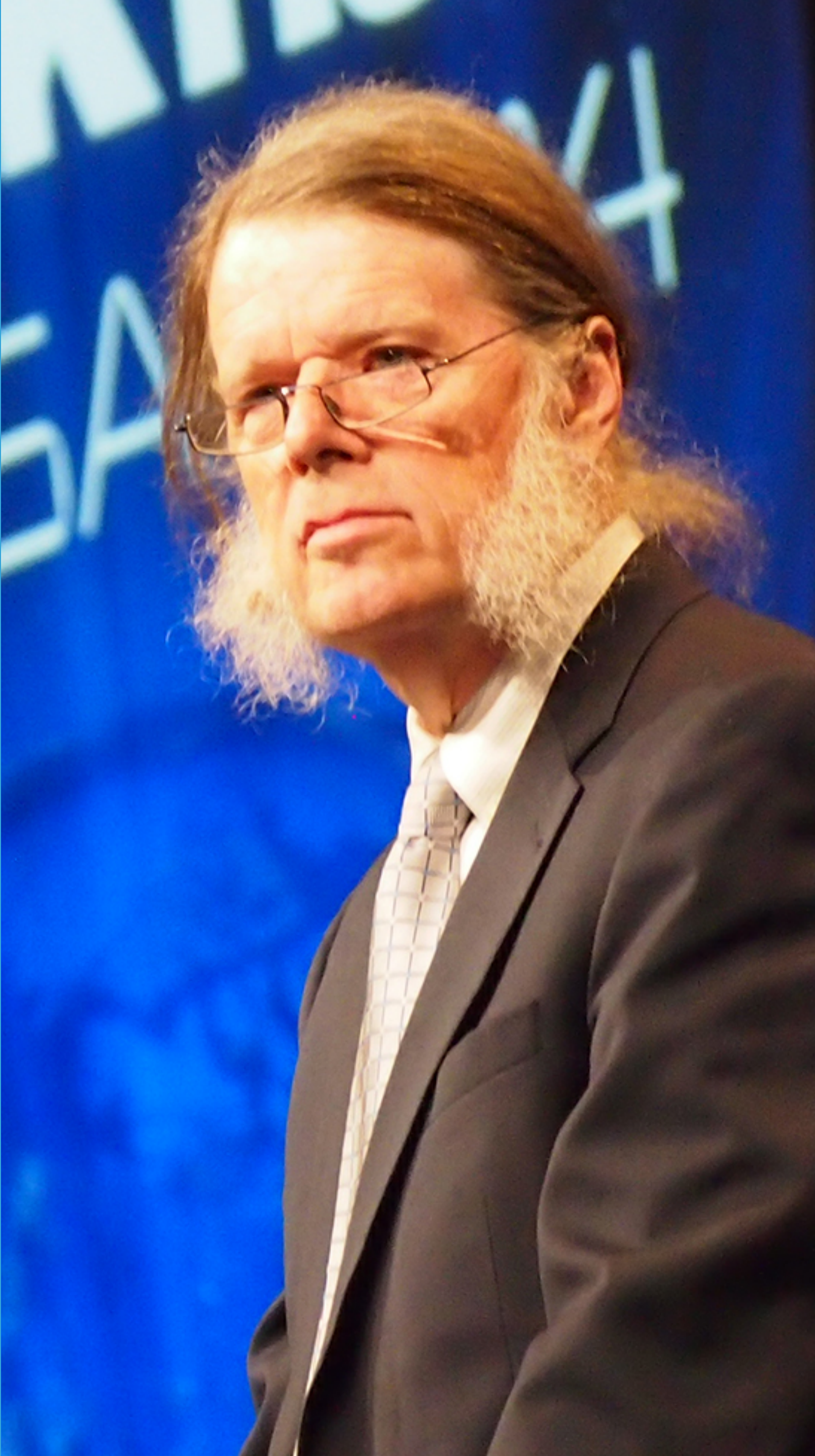
“...THE ZATKOS’ OPERATION WON’T TELL YOU IF YOUR SOFTWARE IS LITERALLY INCENDIARY, BUT IT WILL GIVE YOU A WAY TO COMPARISON-SHOP BROWSERS, APPLICATIONS, AND ANTIVIRUS PRODUCTS ACCORDING TO HOW HARDENED THEY ARE AGAINST ATTACK. IT MAY ALSO PUSH SOFTWARE MAKERS TO IMPROVE THEIR CODE TO AVOID A LOW SCORE AND REMAIN COMPETITIVE.”

No one is suggesting putting sloppy programmers to death, but holding software companies liable for defective programs, and nullifying licensing clauses that have effectively disclaimed such liability, may make sense, given the increasing prevalence of online breaches.



The Intercept





**“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**

THANK YOU

Jeremiah Grossman

 @jeremiahg



<https://www.facebook.com/jeremiahgrossman>



<https://www.linkedin.com/in/grossmanjeremiah>

<https://www.jeremiahgrossman.com/>

<http://blog.jeremiahgrossman.com/>