

JEREMIAH GROSSMAN
CHIEF OF SECURITY STRATEGY

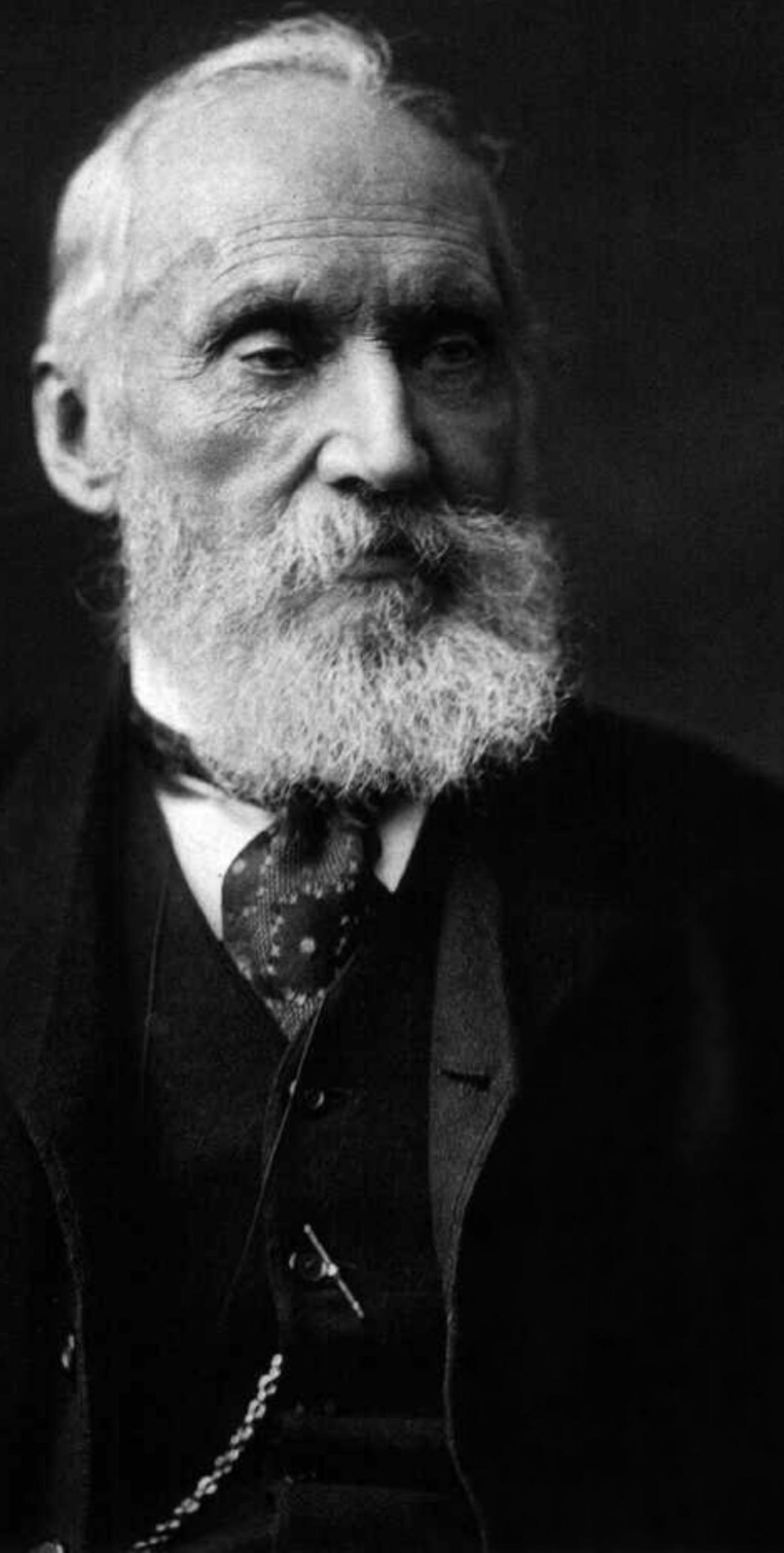
AN INSIDERS GUIDE TO CYBER-INSURANCE AND SECURITY GUARANTEES

 @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,...”

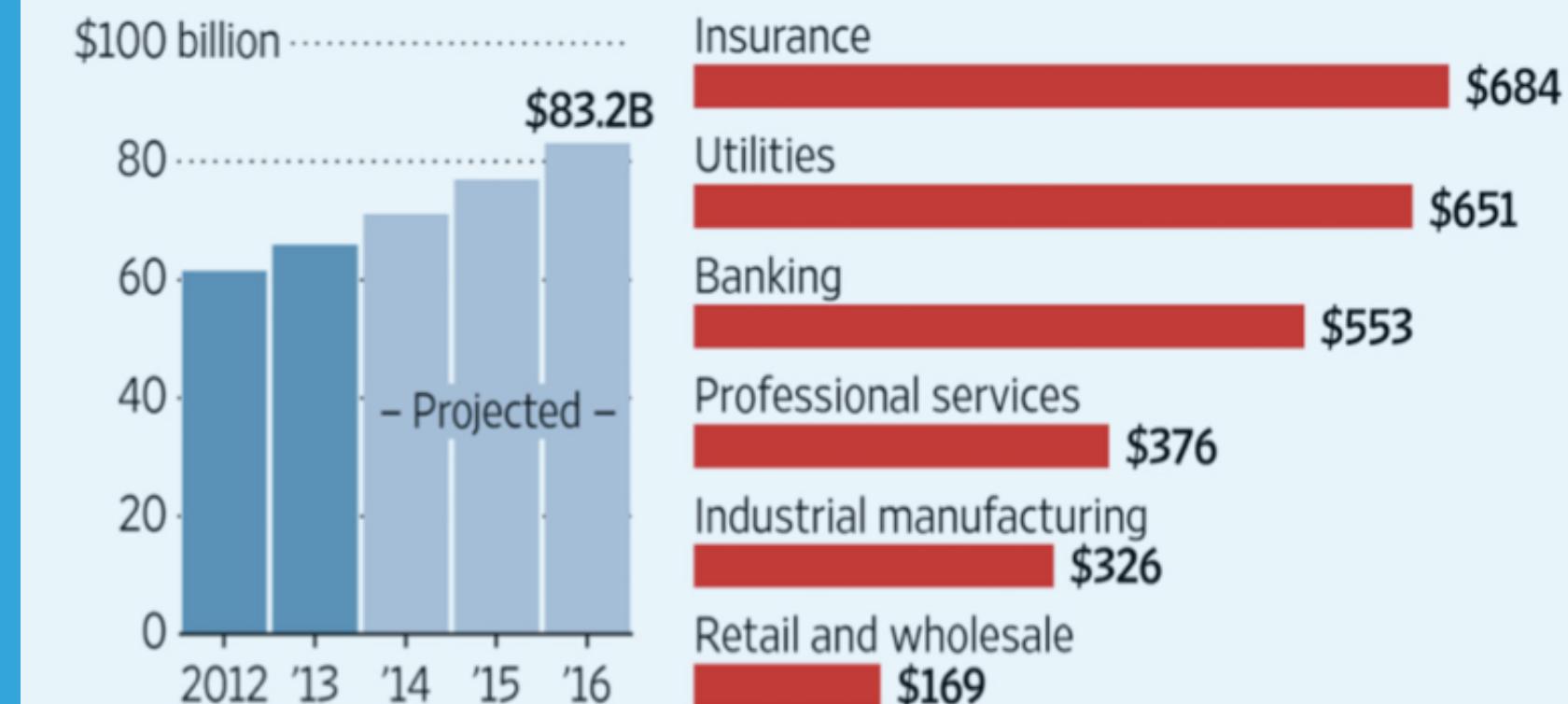
Cyber Spike

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

World-wide security spending



World-wide 2013 information security spending per employee by industry



Source: Gartner

The Wall Street Journal



HACKTIVISTS



ORGANIZED CRIME



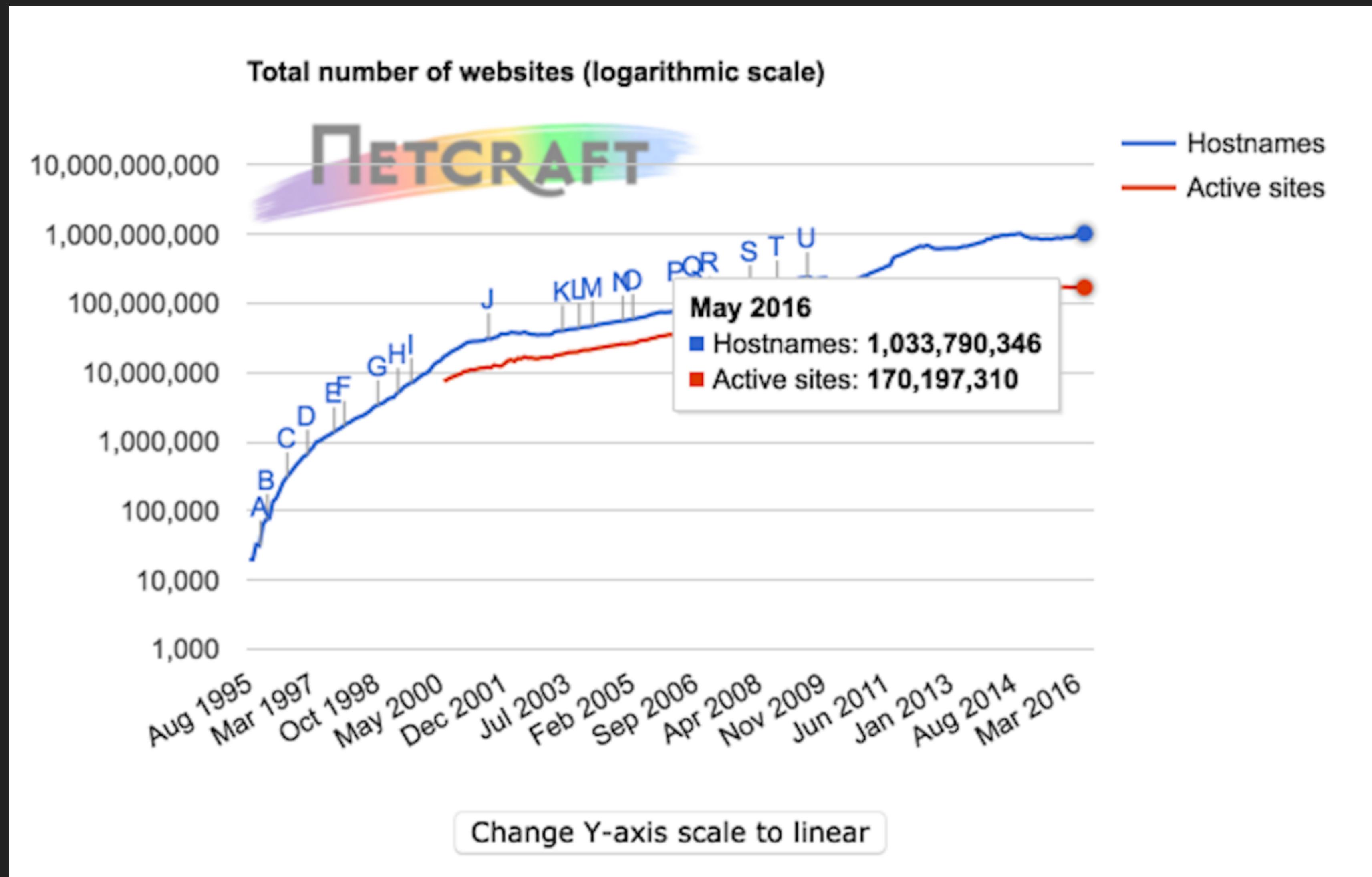
NATION-STATE



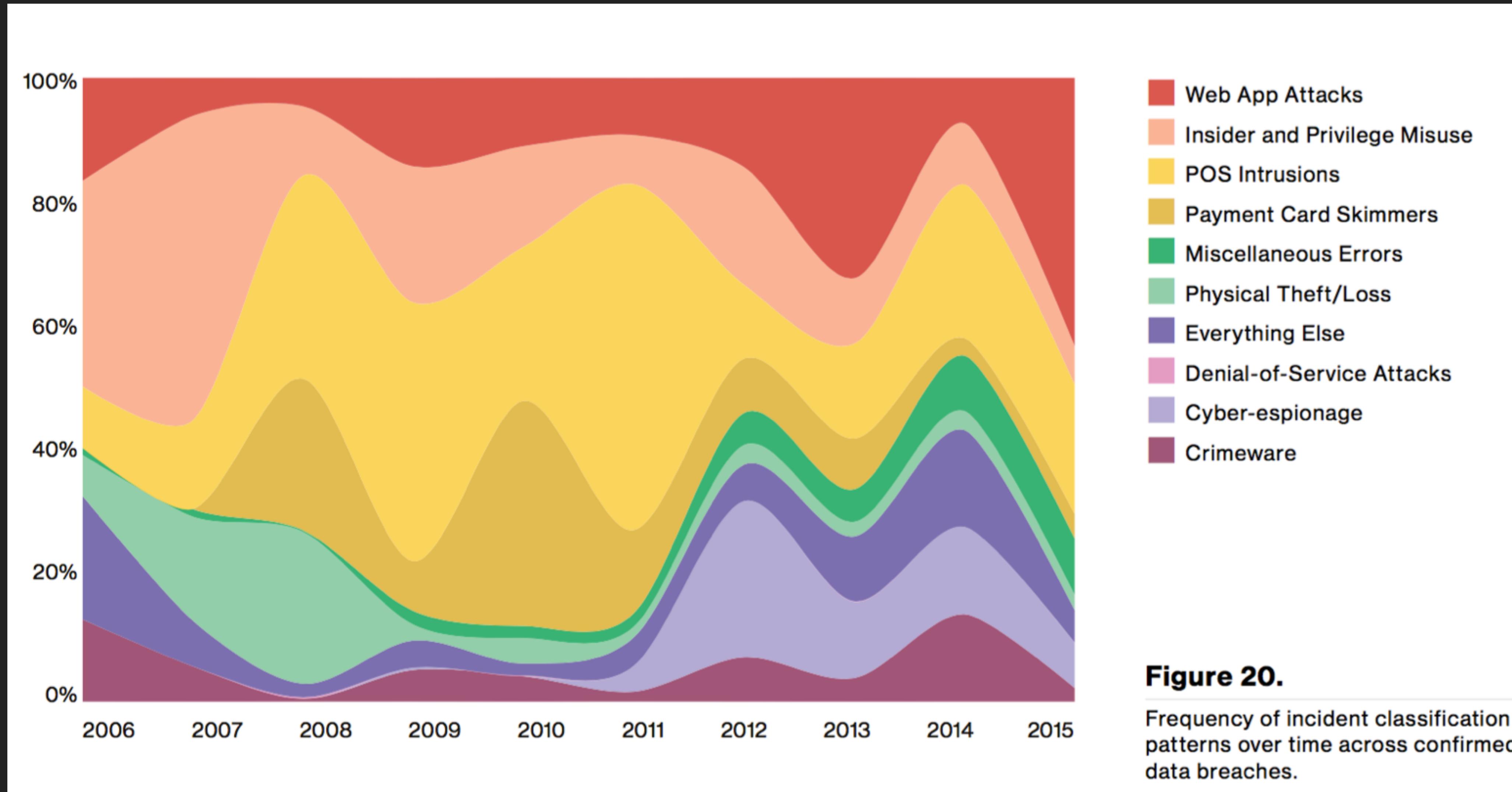
TERRORISM?

1,073,777,722

NETCRAFT: JULY 2016 WEB SERVER SURVEY



NO WAY REGULATIONS CAN KEEP UP.

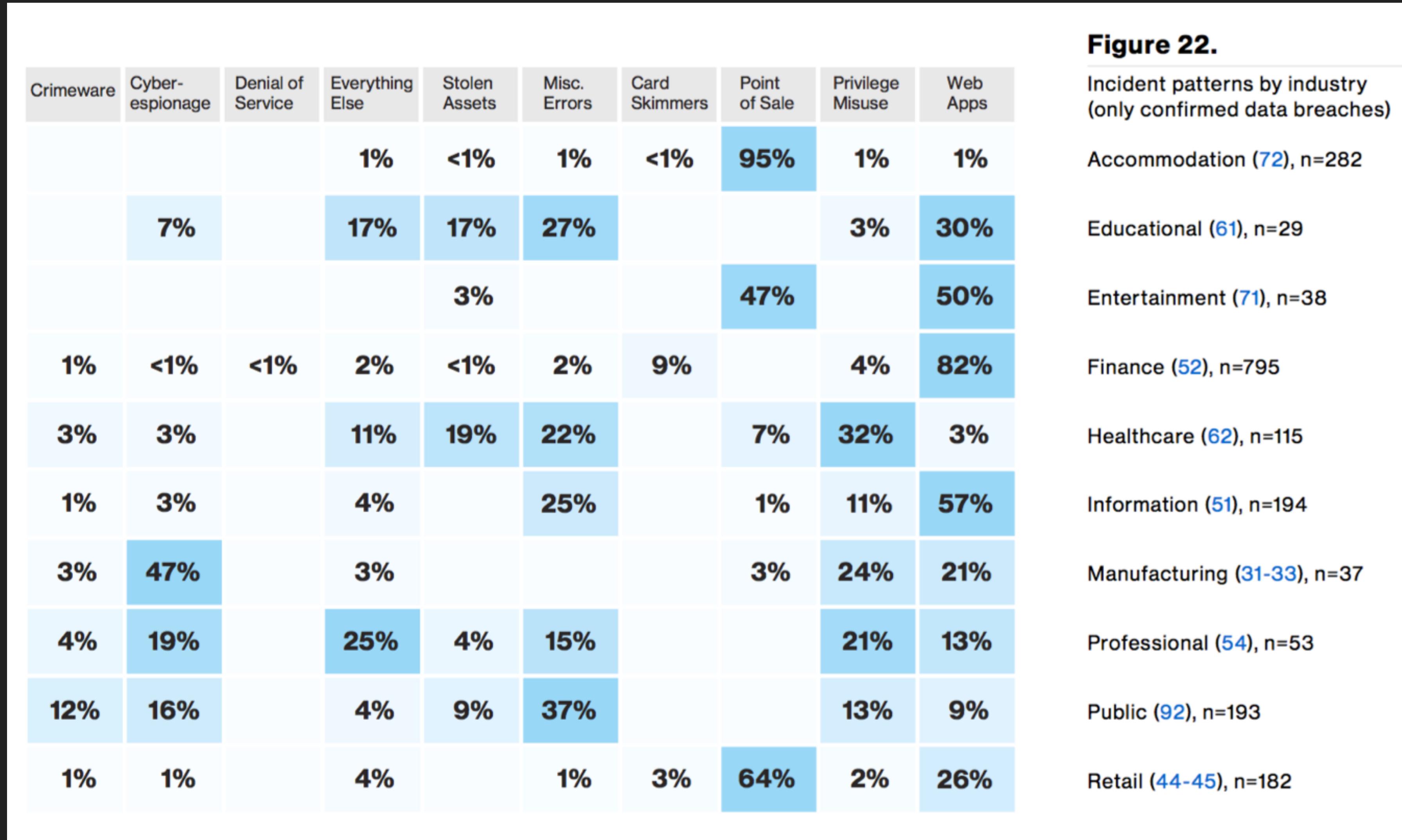


FREQUENCY OF INCIDENT CLASSIFICATION PATTERNS OVER TIME ACROSS CONFIRMED DATA BREACHES.

VERIZON DATA BREACH INVESTIGATIONS REPORT (2016)

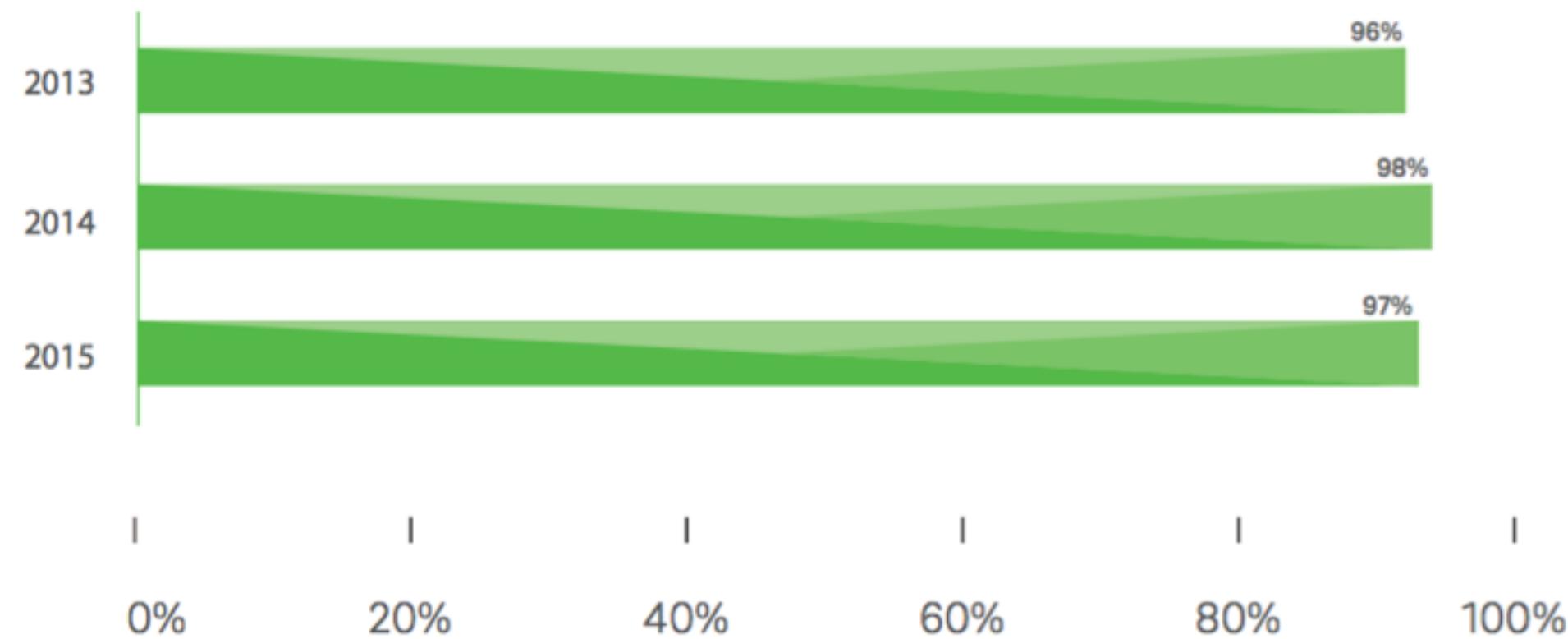
“APPSEC IS EATING SECURITY”

INCIDENT PATTERNS BY INDUSTRY



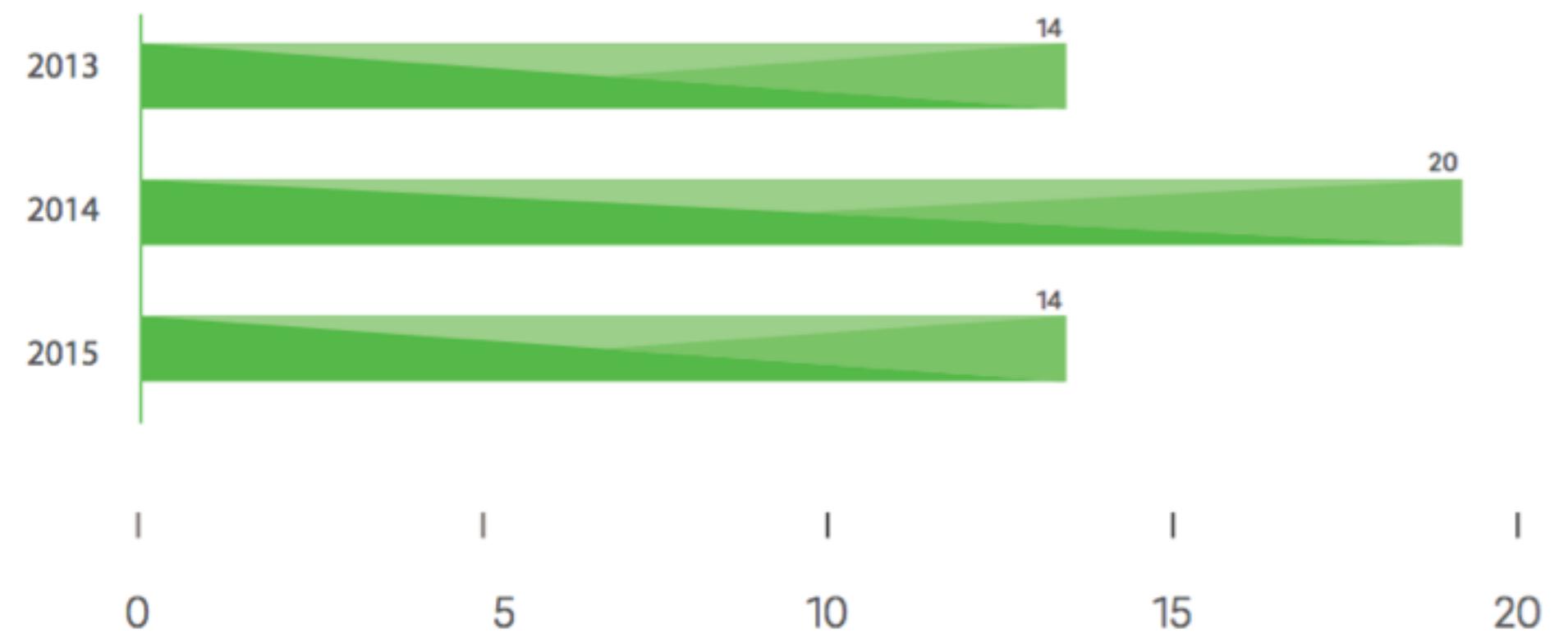
APPLICATION SECURITY

VULNERABLE APPLICATIONS

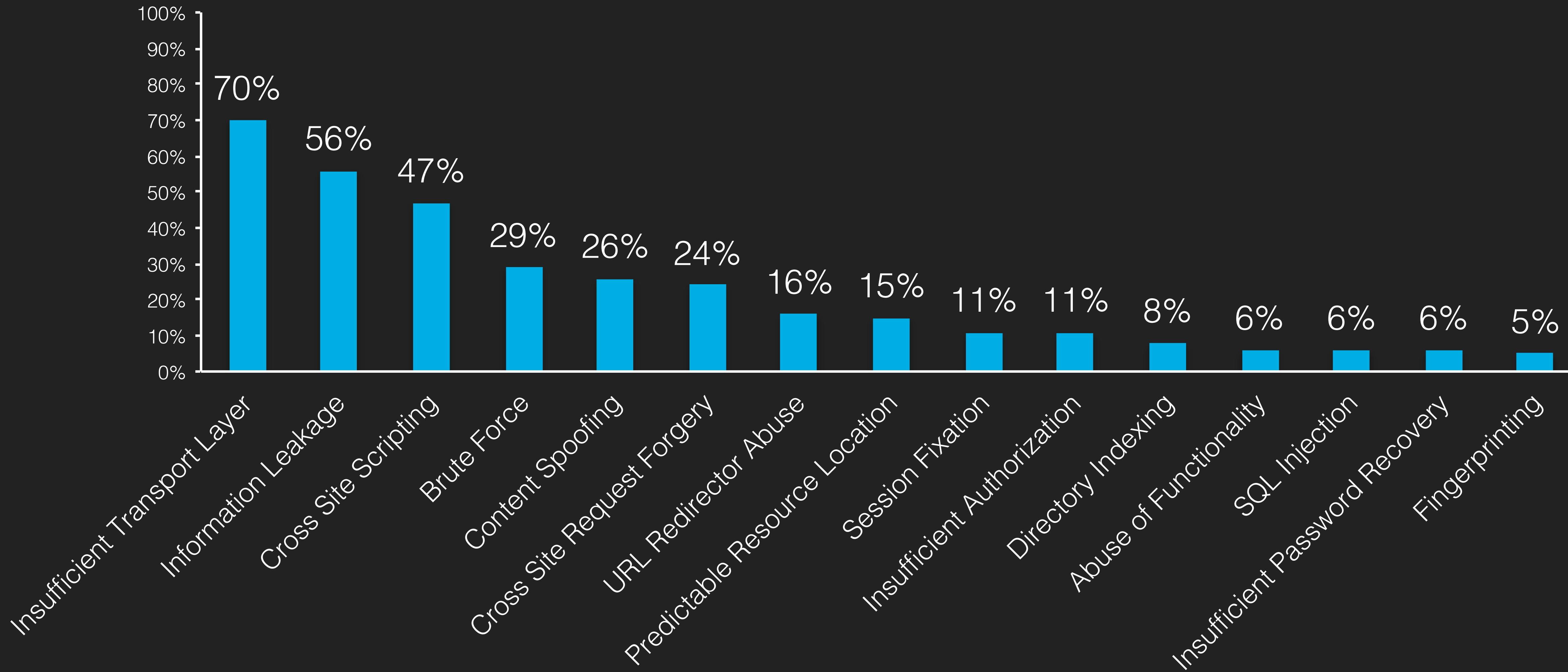


The median number of vulnerabilities per application decreased 30 percent in 2015 compared to the prior year, from 20 to 14. The maximum number of vulnerabilities we found in a single application was 667.

MEDIAN VULNERABILITIES PER APPLICATION



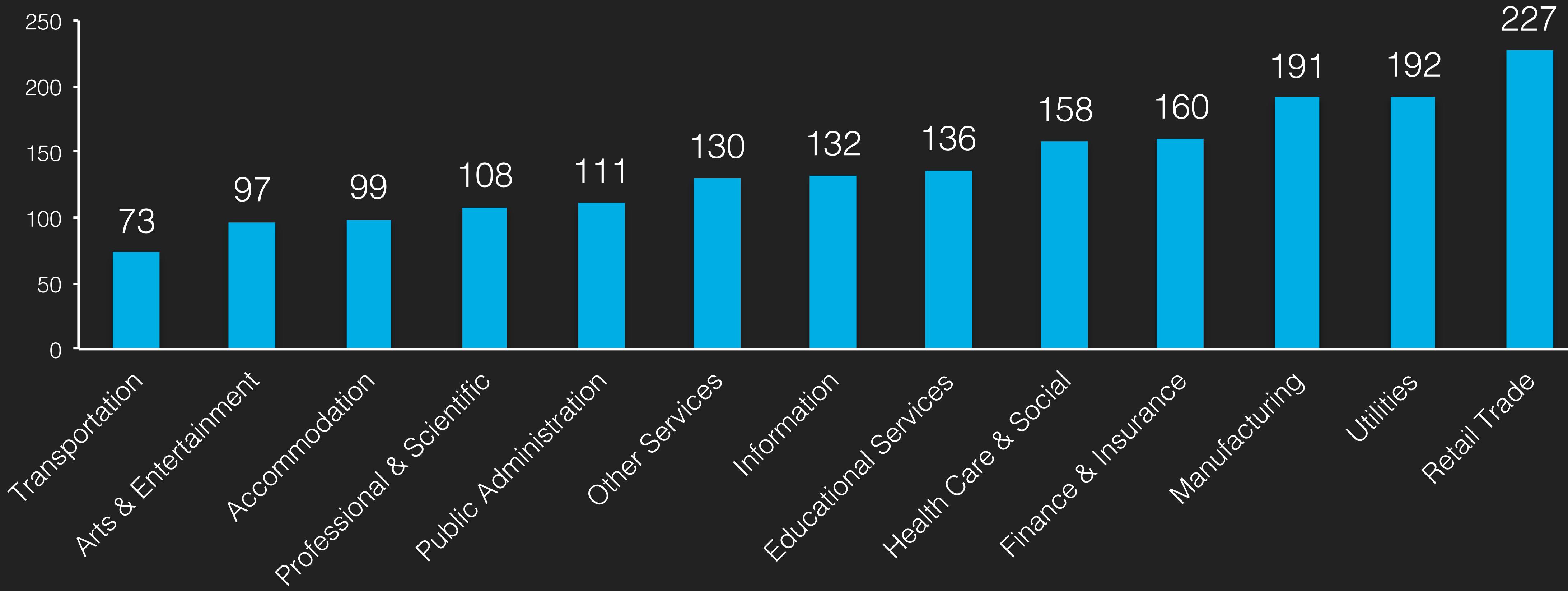
VULNERABILITY LIKELIHOOD (1 OR MORE)



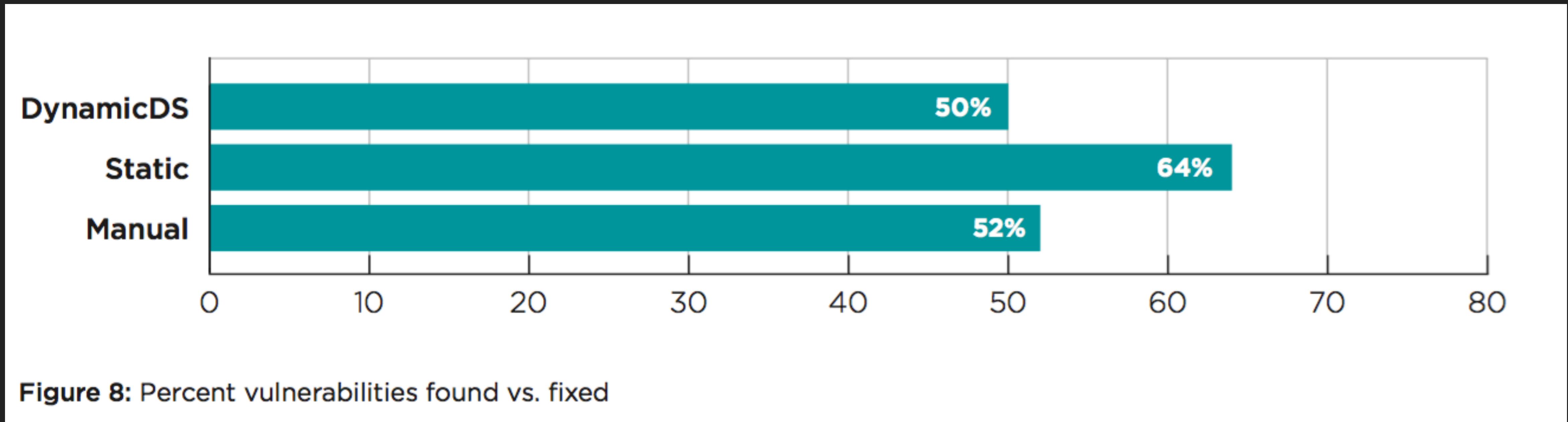
TOP 10 VULNERABILITY CATEGORIES BY PROGRAMMING LANGUAGE

| 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% |

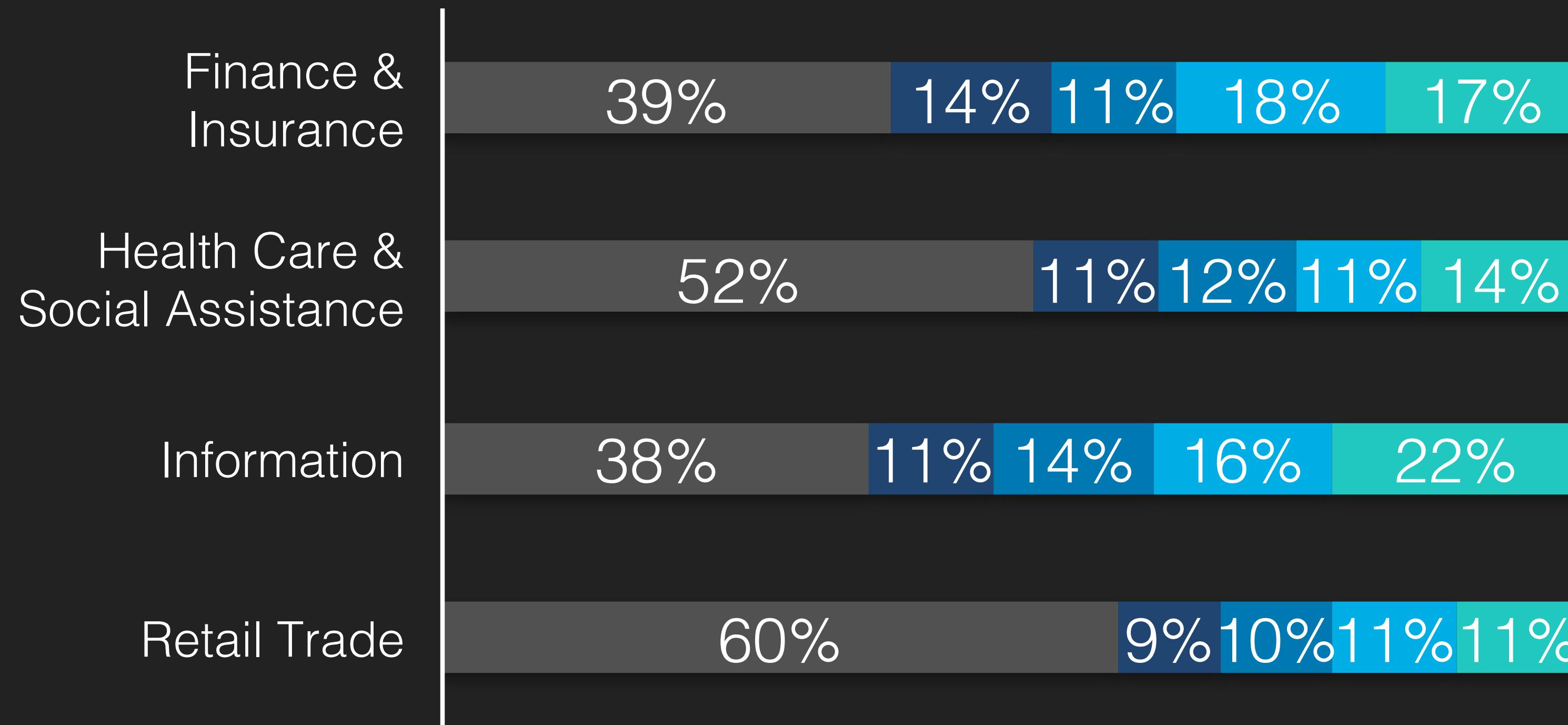
AVERAGE TIME-TO-FIX (DAYS)



PERCENT VULNERABILITIES FOUND VS. FIXED



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?

2016 2015

I have no doubt that we will have to respond to a major incident in the next 12 months

15%

13%

It's highly likely

25%

24%

It's somewhat likely

32%

36%

It's somewhat unlikely

15%

13%

It's highly unlikely

7%

6%

Don't know/not sure

6%

8%

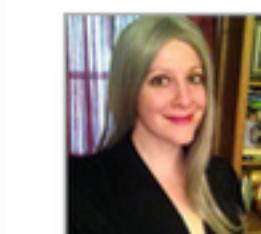
Base: 250 respondents in 2016 and 460 respondents in 2015

Data: UBM survey of security professionals, June 2016



InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

7/14/2016
10:00 AM



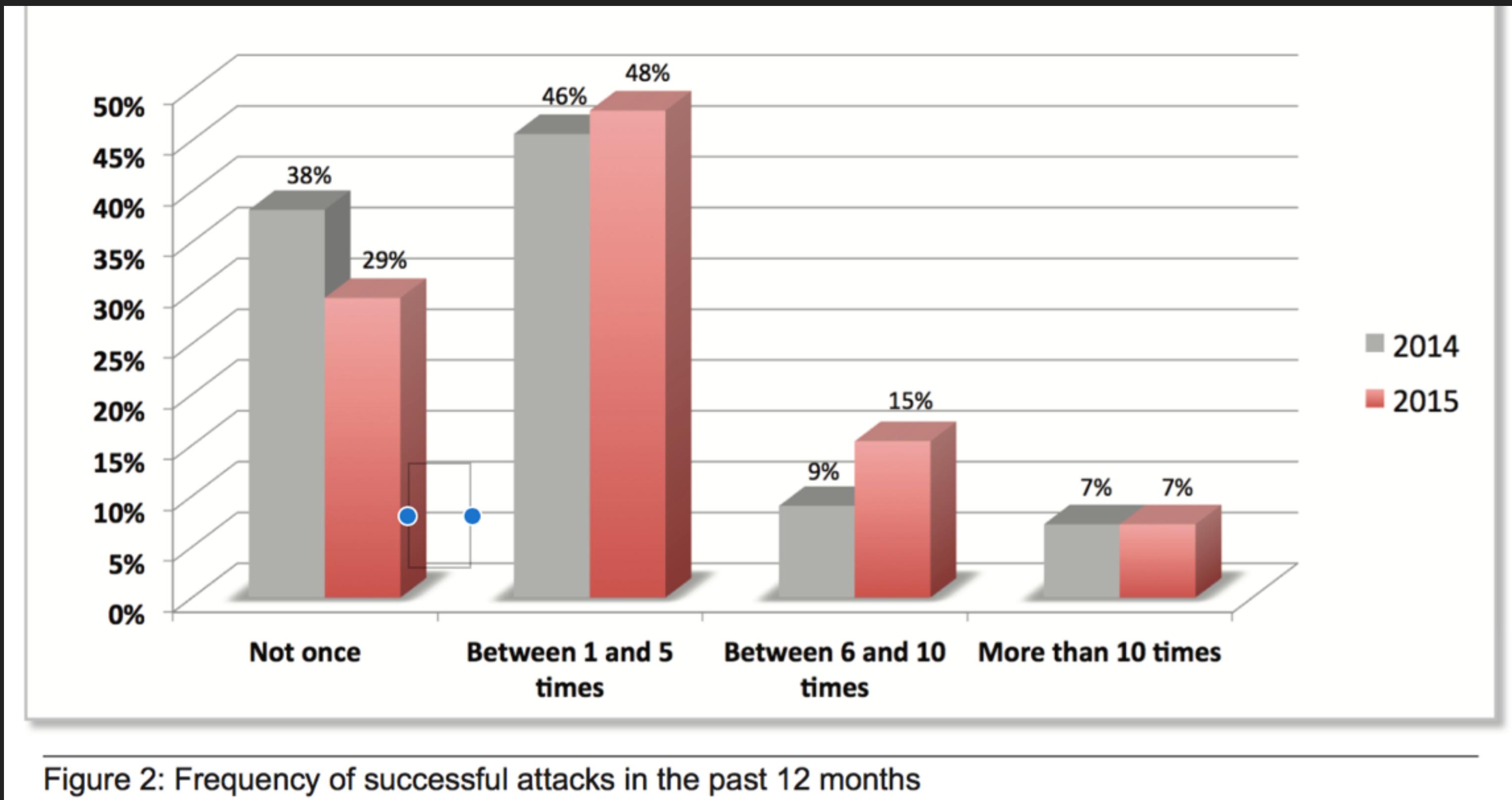
Sara Peters
Commentary
Connect Directly

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.

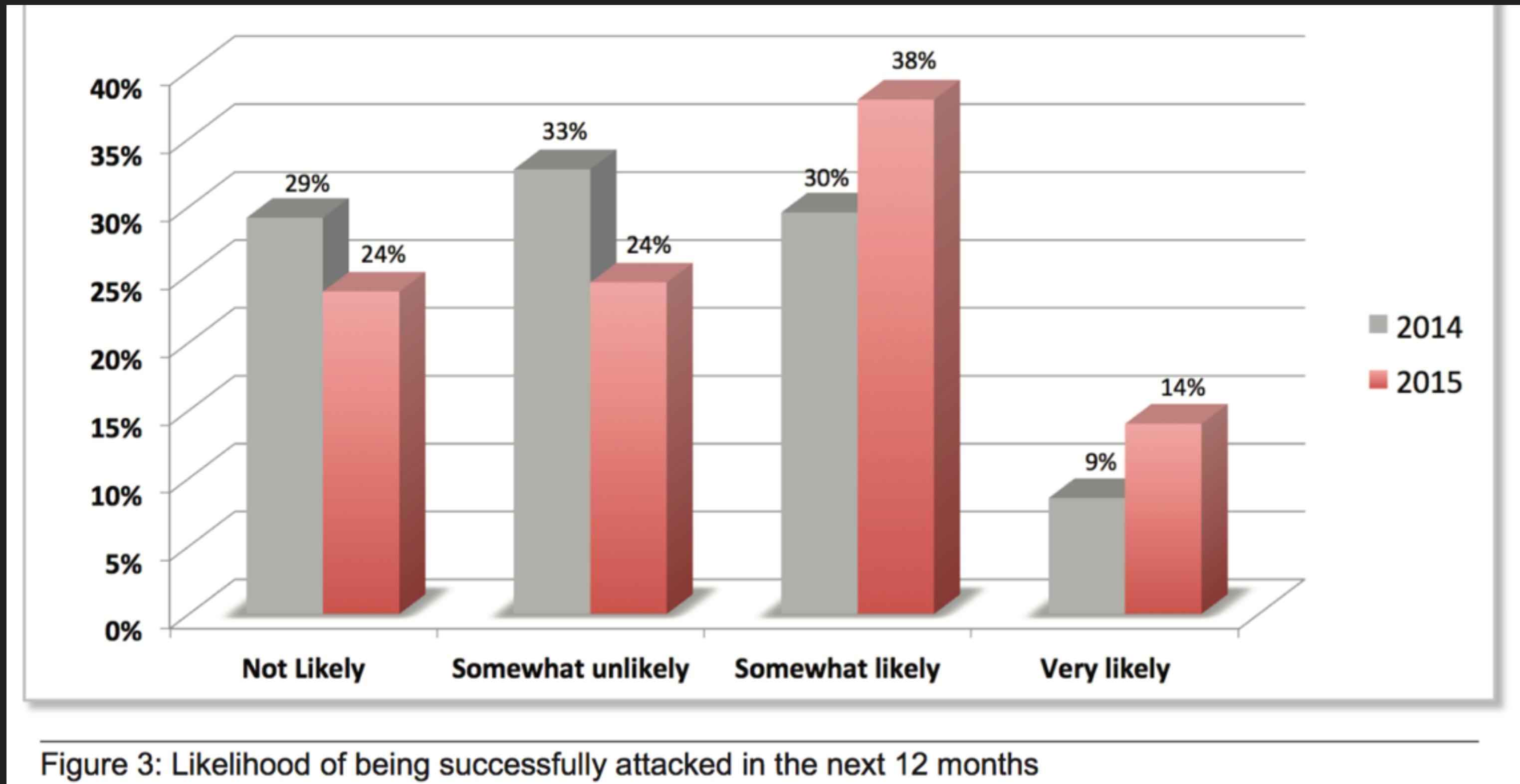
Some of the most qualified security professionals around are more confident in attackers than they are in themselves or their end users.

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



CYBER EDGE GROUP: 2015 CYBERTHREAT DEFENSE REPORT
NORTH AMERICA & EUROPE

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



CYBER EDGE GROUP: 2015 CYBERTHREAT DEFENSE REPORT
NORTH AMERICA & EUROPE

**“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% |



Trust in, and value from, information systems

2015 Global Cybersecurity Status Report

January 2015

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 |

VERIZON DATA BREACH INVESTIGATIONS REPORT (2015)

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.

The collage consists of three screenshots of news articles:

- FORTUNE** (March 31, 2015): "Lloyd's CEO: Cyber attacks cost companies \$400 billion every year" by Stephen Gandel (@stephengandel) on January 23, 2015. The article discusses the impact of cyber attacks on corporate costs.
- LA Times**: "Spending on cyberattack insurance soars as hacks become more common" by Mary Thompson (@MThompsonCNBC) on July 1, 2014. It highlights the increasing prevalence and cost of cyberattacks.
- CNBC**: "NETNET: Why cyber-insurance will be the next big thing" by Mary Thompson (@MThompsonCNBC) on July 1, 2014. It explores the future growth of the cyber-insurance market.

Each article includes a small image related to its topic: a building interior for the Fortune article, a Target store for the LA Times article, and a person in a binary code pattern for the CNBC article.

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

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home News & Commentary Authors Slideshows Video Radio Reports White Papers Events

ANALYTICS ATTACKS / BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS

ANALYTICS

1/26/2016 08:00 AM

 Ericka Chickowski News

Connect Directly   


Insurers Getting Smarter About Assessing Cyber Insurance Policy Risks

2016 shaping up to be a year of greater maturity in how insurance companies underwrite their cyber insurance policies.

Cybersecurity experts expect 2016 to be the year that insurance companies gain a greater level of maturity with how they underwrite cyber-insurance customers and assess them throughout the life of a policy. As that happens, customers could experience some pain as insurance companies get wise to the red flags of poor information security practices. But overall, this maturation could mean good things for cyber-insurance customers and the infosec world as a whole.

“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



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.

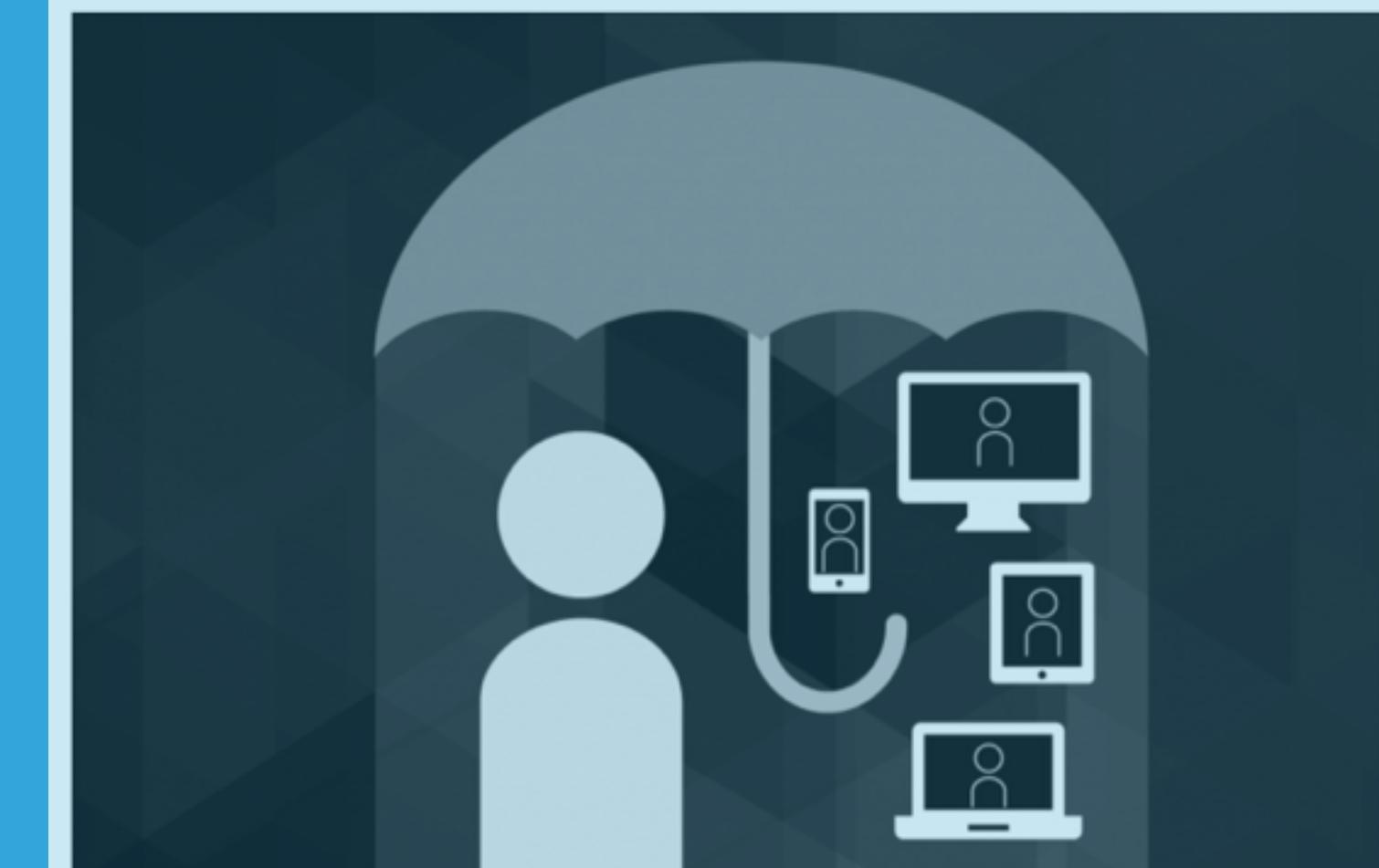
ABI Research provides technology market research and technology intelligence for industry innovators. From offices in North America, Europe and Asia, ABI Research's worldwide team of experts advises thousands of decision makers through 70+ research and advisory services. Est. 1990. For more information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

BUY WHATEVER THERE IS

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

THE PARALLAX
YOUR EYE ON SECURITY NEWS

NEWS FEATURES HOW TO OPINION/Q&A CONTACT US f t g s NEW



Businesses can buy
'cyberinsurance.' Why can't you?

The Parallax

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

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.

Risk Manag

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.”

the security ledger

INTERNET OF THINGS ▾ CONNECTED CARS THREATS ▾ THOUGHT LEADERSHIP ▾ PODCASTS VIDEO

search...

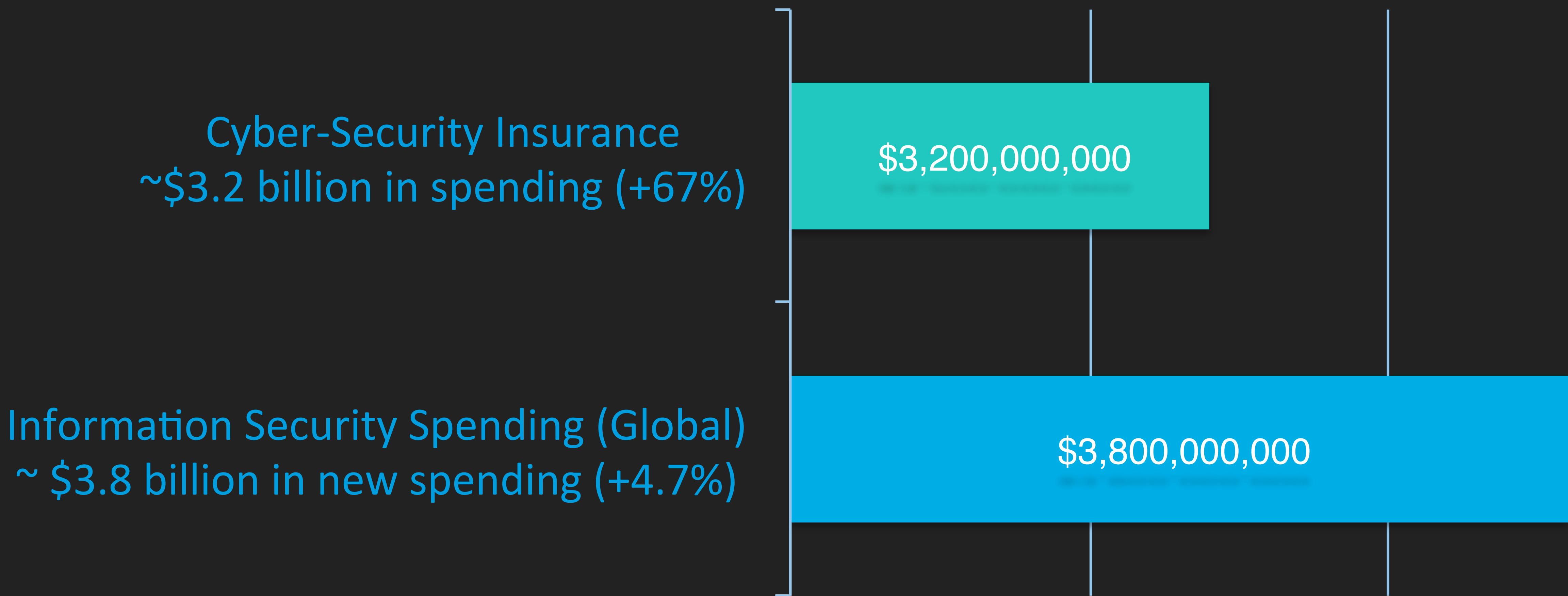
You are here: Home ▸ Companies ▸ Anthem Healthcare ▸ Report: Cyber Insurance Premiums Jump in Wake of Incidents

Report: Cyber Insurance Premiums Jump in Wake of Incidents

© POSTED BY: PAUL OCTOBER 12, 2015 18:20 COMMENTS OFF ON REPORT: CYBER INSURANCE PREMIUMS JUMP IN WAKE OF INCIDENTS



2014 – 2015 NEW SECURITY INVESTMENT VS. CYBER-INSURANCE



**ALL
SALES
FINAL**

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

NO GUARANTEES
NO WARRANTIES
NO RETURN POLICIES

A black and white photograph of a crowded exhibition hall. In the foreground, there are several booths with signs that read "CONNECTED SECURITY", "SMARTER SECURITY", and "McAfee". The floor is crowded with people walking between the booths. The background shows more booths and signs, creating a dense, busy atmosphere.

INFORMATION SECURITY

THE
\$75 BILLION
GARAGE SALE



Personal

Small Business

Commercial

Banking Loans and Credit Insurance Investing and Retirement Wealth 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 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.

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



BANKING

BORROWING

INVESTMENT & 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.



About TD | Investor Relations | Economics | Careers | Corporate Responsibility | To Our Customers

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](#)

How We Protect You > Online Security Guarantee

Your TD Online and Mobile Security Guarantee

You're protected.

In the unlikely event you experience a TD account 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 safe and secure. 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.



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](#)

▶ 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.**⁺

To receive reimbursement under this guarantee, you must:

- Sign out and close your Internet browser at the end of each Online Banking 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.



The screenshot shows a Microsoft Word document with a table containing various assumptions for a security guarantee program. The table has columns for Assumption Name, Description, and Value. The value column for the last row is highlighted in yellow.

| A | B | C |
|----|--|---------|
| 1 | <u>Guarantee Program Assumptions</u> | |
| 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 SentinelOne Customer | \$1,000 |
| 10 | | |
| 11 | | |
| 12 | <u>Estimated Infections Outcomes w/ SentinelOne</u> | |
| 13 | Total Annual Endpoint Infections | |
| 14 | Total Annual Endpoint Infections where Rollback Failed | |
| 15 | | |
| 16 | | |
| 17 | <u>Financial Analysis</u> | |
| 18 | Total Annual Reinsurance Premiums | |
| 19 | Total Annual Ransom Payout Loss (Max) | |
| 20 | Total Annual Reinsurance Deductable Loss | |
| 21 | | |
| 22 | SentinelOne: Total Annual Costs & Losses of the Program | |

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.

SECURITY GUARANTEE

DETAILS

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



SENTINEL ELITE
GUARANTEE YOUR SECURITY



**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.

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

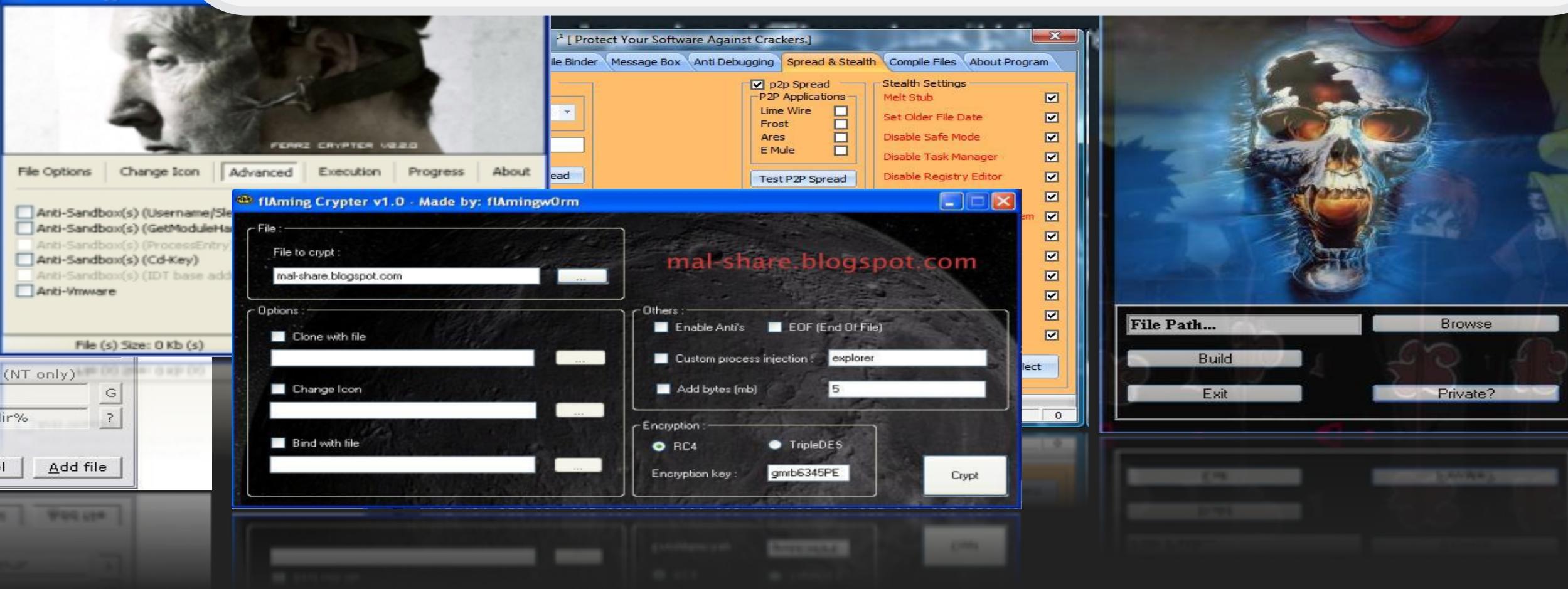
MALWARE KITS COME WITH WARRANTIES



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/ME/NT/2000/2003/XP/Vista
- Remote S...
- Webcam...
- Controlli...
- Notifies...
- Technica...

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

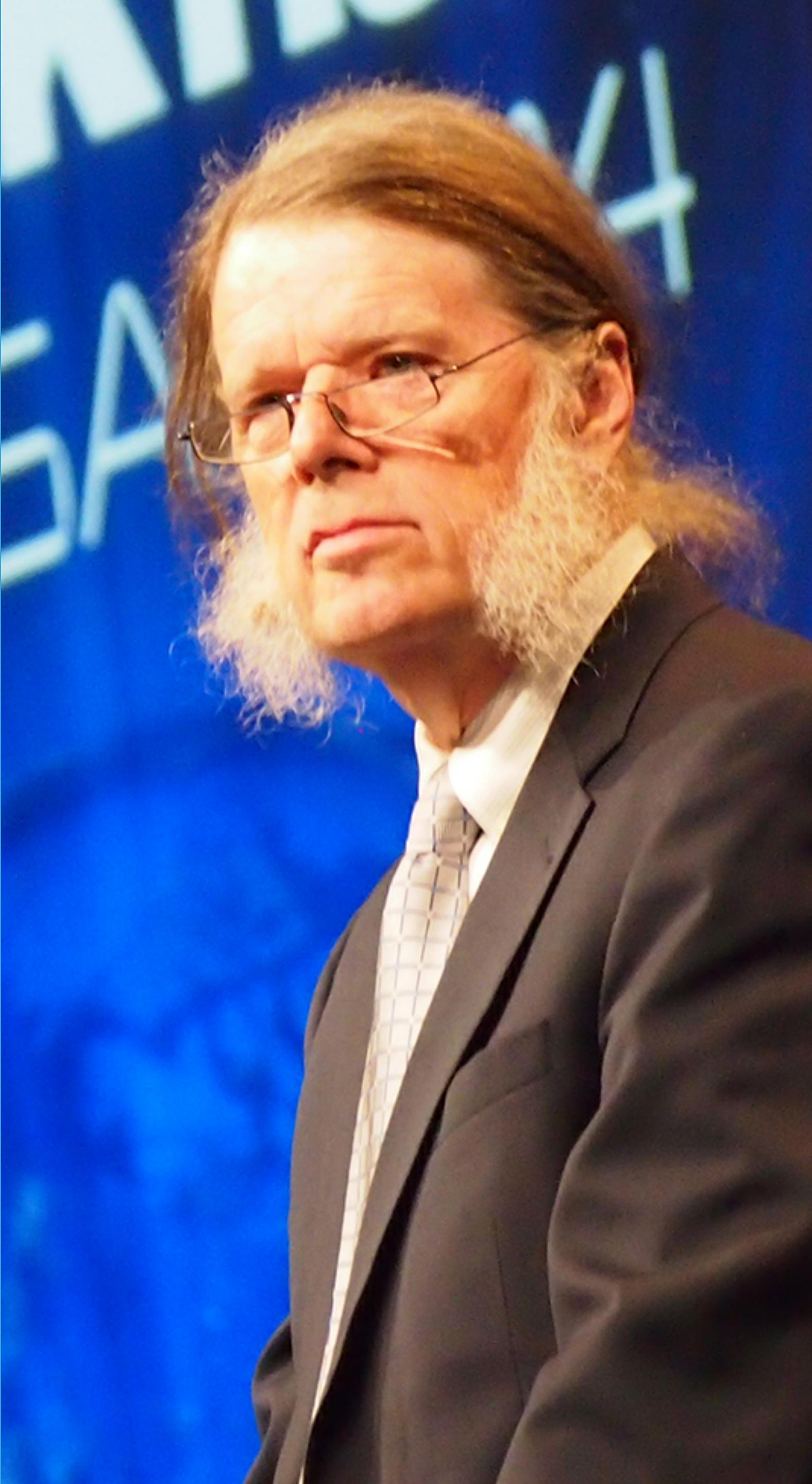
A FAMED HACKER IS GRADING THOUSANDS OF PROGRAMS — AND MAY REVOLUTIONIZE SOFTWARE IN THE PROCESS

Kim Zetter
July 29 2016, 7:00 a.m.

f t m 18



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/>