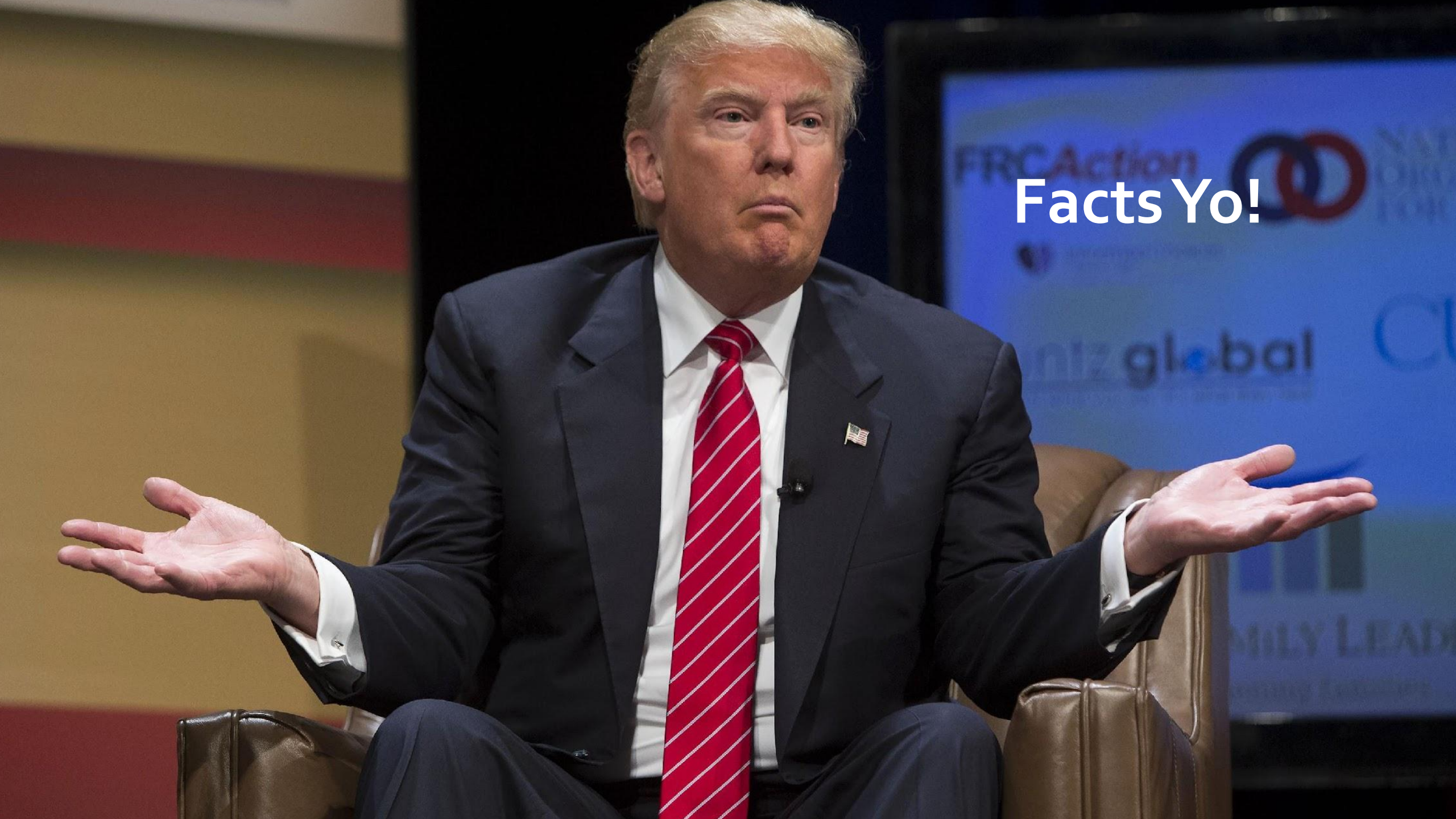
ImpactingGrowth

The Story of the Anthem Breach

CONTENTS

Contents


Facts Yo!


QUESTION:
How many data breaches were there last year
in the United States?

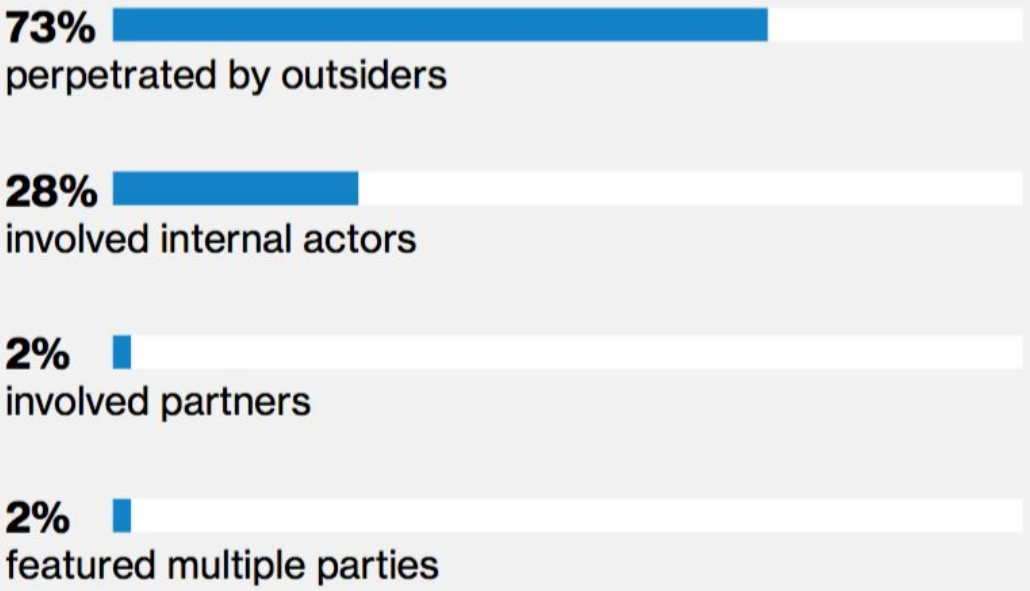
KEY TAKEAWAY

Last year, there were over **53,000 incidents** and **2,216 confirmed data breaches**.

- 2018 Verizon Data Breach Investigations Report

KEY TAKEAWAY

Who's behind the breaches?



What tactics are utilized?

KEY TAKEAWAY

Who are the victims?

24%
of breaches affected [redacted] organizations

15%
of breaches involved [redacted]

14%
were breaches of [redacted]

58%
of victims are categorized as [redacted]

What are other commonalities?

49%
of non-POS malware was installed via malicious email[1]

76%
of breaches were financially motivated

13%
of breaches were motivated by the gain of strategic advantage (espionage)

68%
of breaches took months or longer to discover

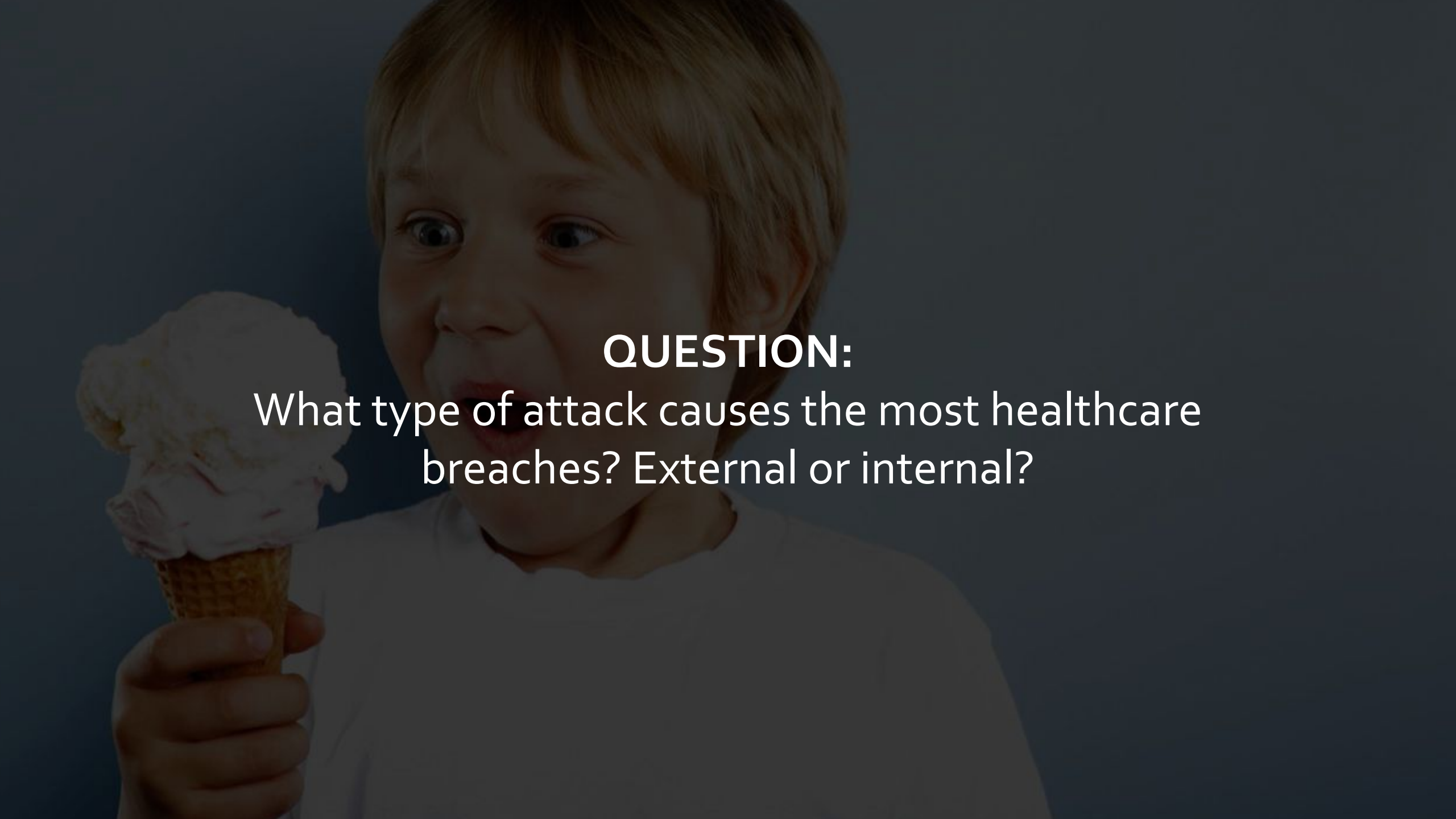

Healthcare
Drilldown

KEY TAKEAWAY

Breaches by Entity

State	Indicator	Quantity
Business Associate		317
Health Plan		274
Clearinghouse		4
Healthcare Providers		1506

- Office of Civil Rights, Breach Report



QUESTION:

What type of attack causes the most healthcare breaches? External or internal?

KEY TAKEAWAY

Healthcare is the ONLY industry vertical that has **more internal actors behind breaches than external.**

- 2018 Verizon Data Breach Investigations Report

66% of internal and external threat actors are **abusing privileged access credentials to access databases** and steal proprietary information

KEY TAKEAWAY

Frequency	750 incidents, 536 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Crimeware and Privilege Misuse represent 63% of incidents within Healthcare
Threat actors	43% External, 56% Internal, 4% Partner and 2% Multiple parties (breaches)
Actor motives	75% Financial, 13% Fun, 5% Convenience, 5% Espionage (all incidents)
Data compromised	Medical (79%), Personal (37%), Payment (4%)

KEY TAKEAWAY

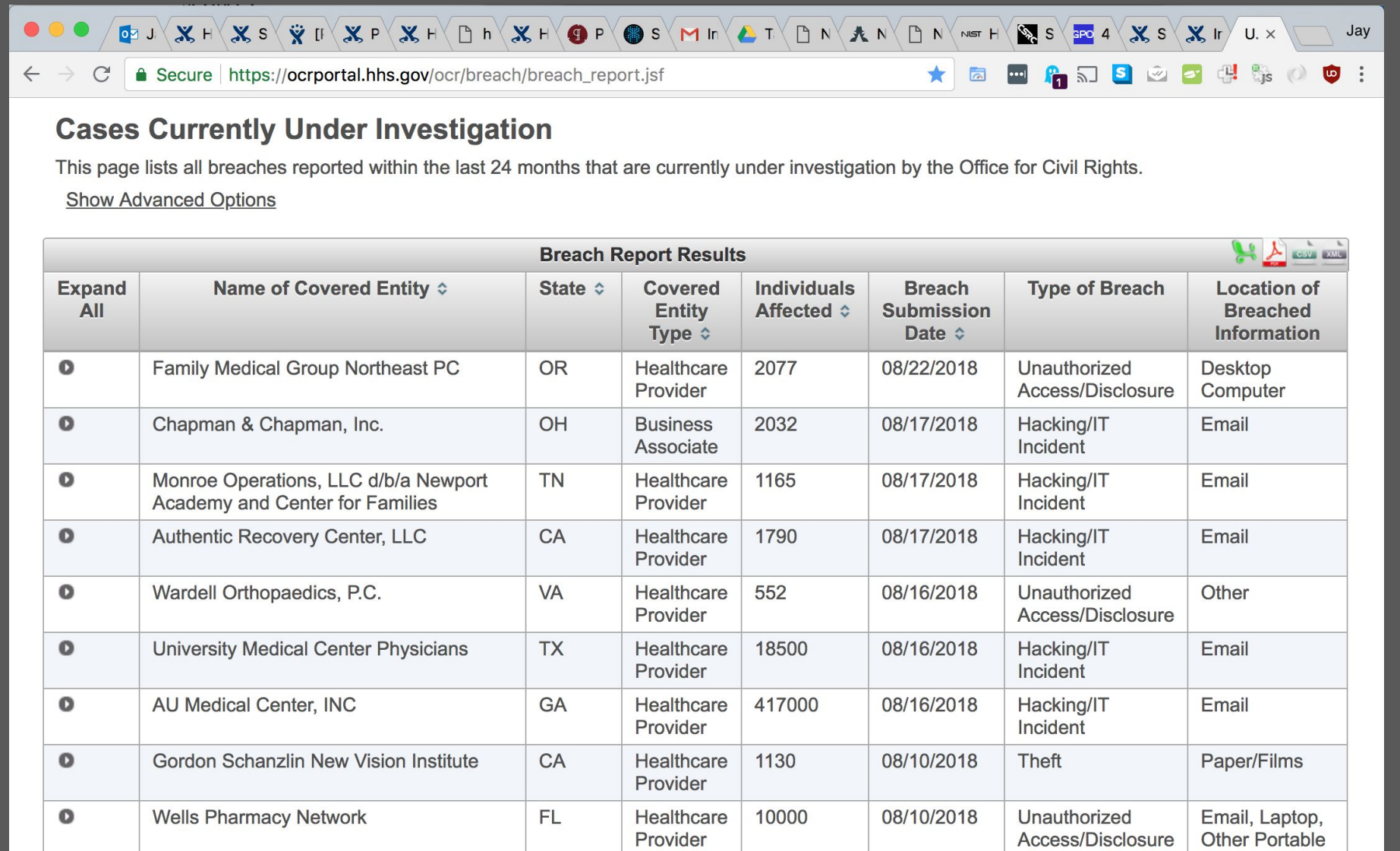
Breaches by Type

Type	Count
Theft	802
Unauthorized Access/Disclosure	561
Hacking/IT Incident	363
Loss	141
Improper Disposal	62

- Office of Civil Rights, Breach Report

Recent Incidents

KEY TAKEAWAY



Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Family Medical Group Northeast PC	OR	Healthcare Provider	2077	08/22/2018	Unauthorized Access/Disclosure	Desktop Computer
	Chapman & Chapman, Inc.	OH	Business Associate	2032	08/17/2018	Hacking/IT Incident	Email
	Monroe Operations, LLC d/b/a Newport Academy and Center for Families	TN	Healthcare Provider	1165	08/17/2018	Hacking/IT Incident	Email
	Authentic Recovery Center, LLC	CA	Healthcare Provider	1790	08/17/2018	Hacking/IT Incident	Email
	Wardell Orthopaedics, P.C.	VA	Healthcare Provider	552	08/16/2018	Unauthorized Access/Disclosure	Other
	University Medical Center Physicians	TX	Healthcare Provider	18500	08/16/2018	Hacking/IT Incident	Email
	AU Medical Center, INC	GA	Healthcare Provider	417000	08/16/2018	Hacking/IT Incident	Email
	Gordon Schanzlin New Vision Institute	CA	Healthcare Provider	1130	08/10/2018	Theft	Paper/Films
	Wells Pharmacy Network	FL	Healthcare Provider	10000	08/10/2018	Unauthorized Access/Disclosure	Email, Laptop, Other Portable

DON'T DO THIS

Memorial Healthcare System

$5,500,000 -$5.5 million HIPAA settlement shines light on the importance of audit controls

THE UNIVERSITY OF TEXAS
MD Anderson Cancer Center

$4,348,000 – Despite encryption policies and high risk findings, MD Anderson did not adopt an enterprise-wide solution to implement encryption of ePHI

Source: https://compliancy-group.com/hipaa-fines-directory-year/

DON'T DO THIS

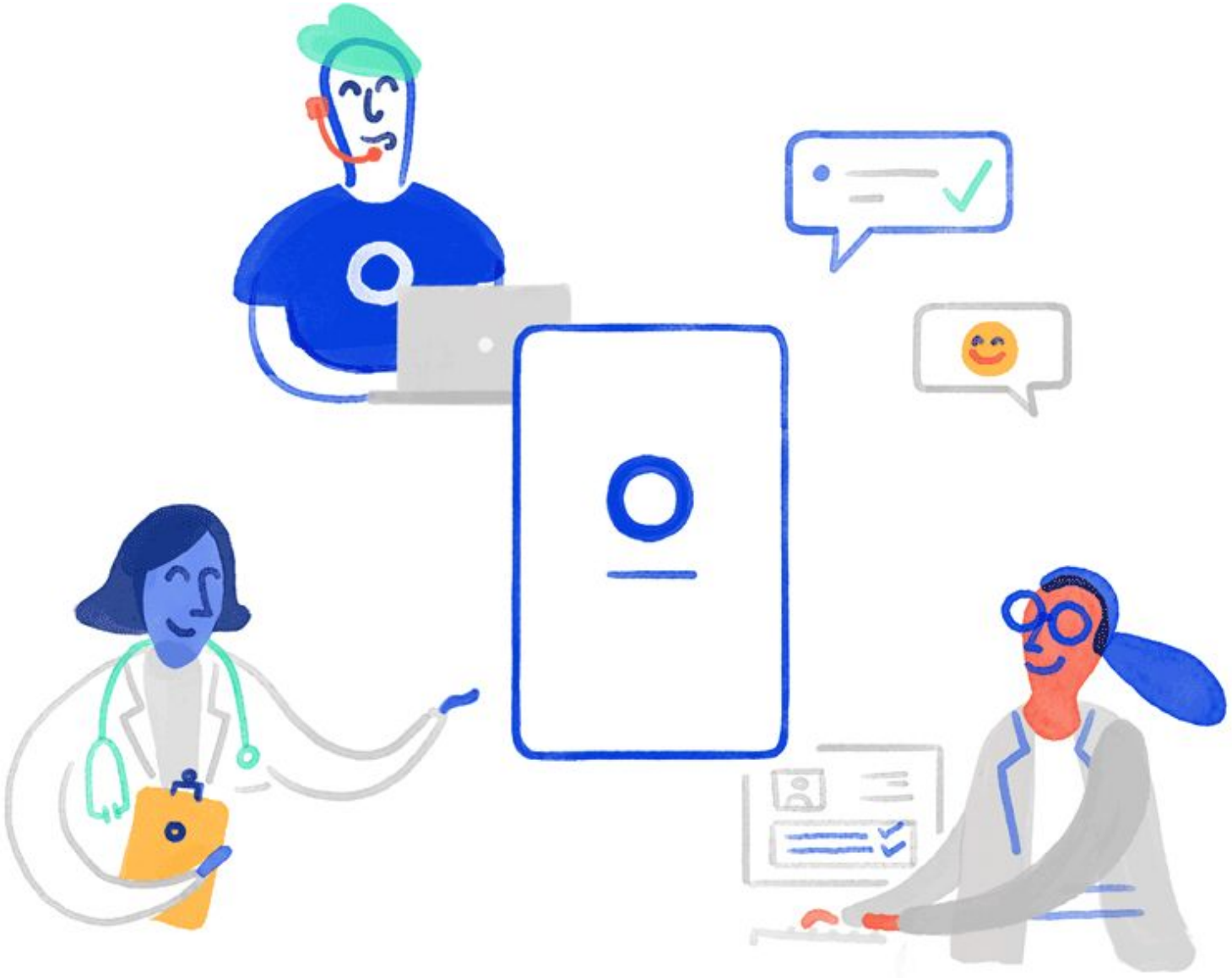
FRESENIUS MEDICAL CARE

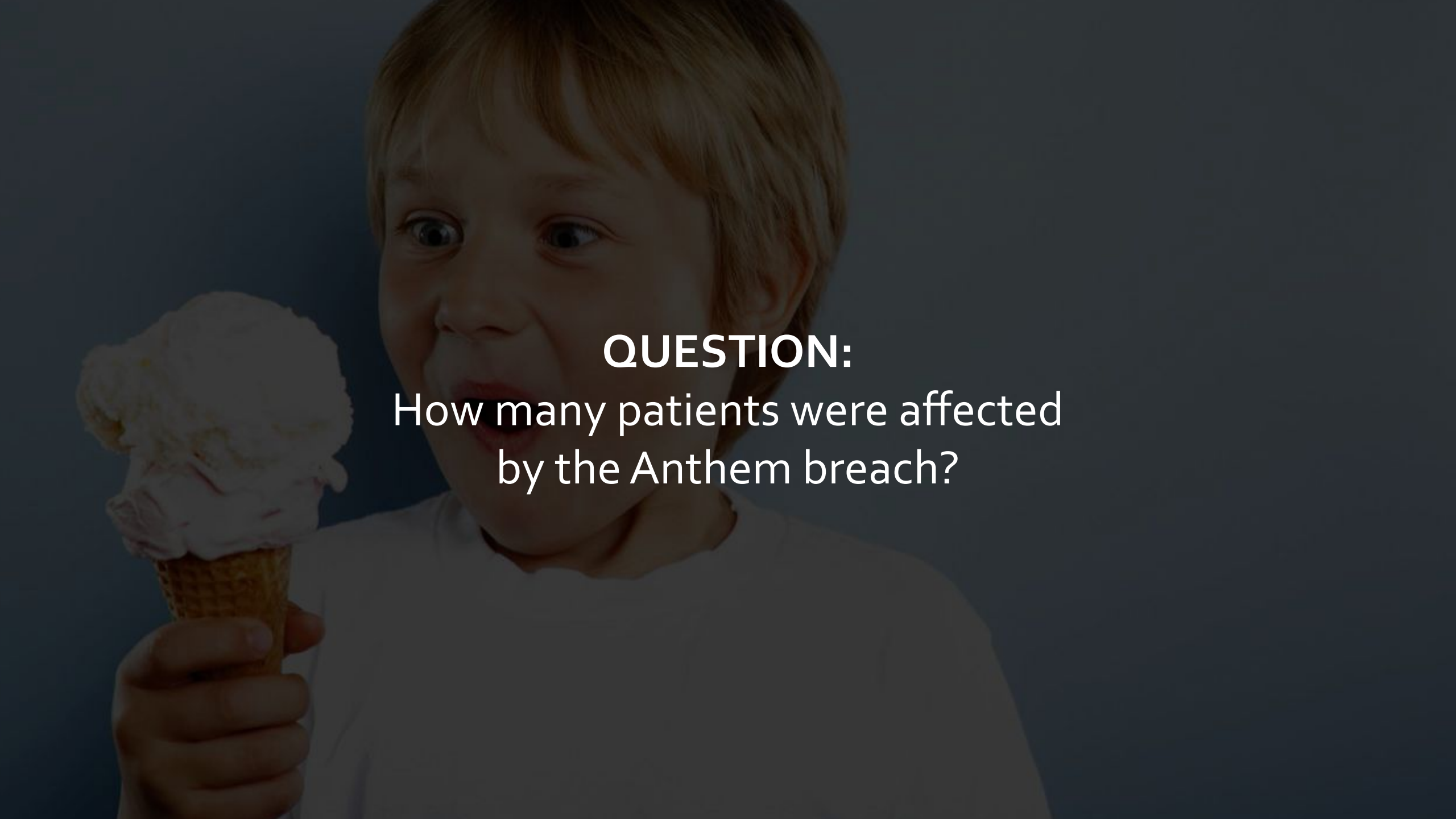
$3,500,000 - Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules

MAPFRE

$2,200,000 - HIPAA settlement demonstrates failure to conduct risk analysis, implement risk management plans, and deploy encryption

The Anthem Breach

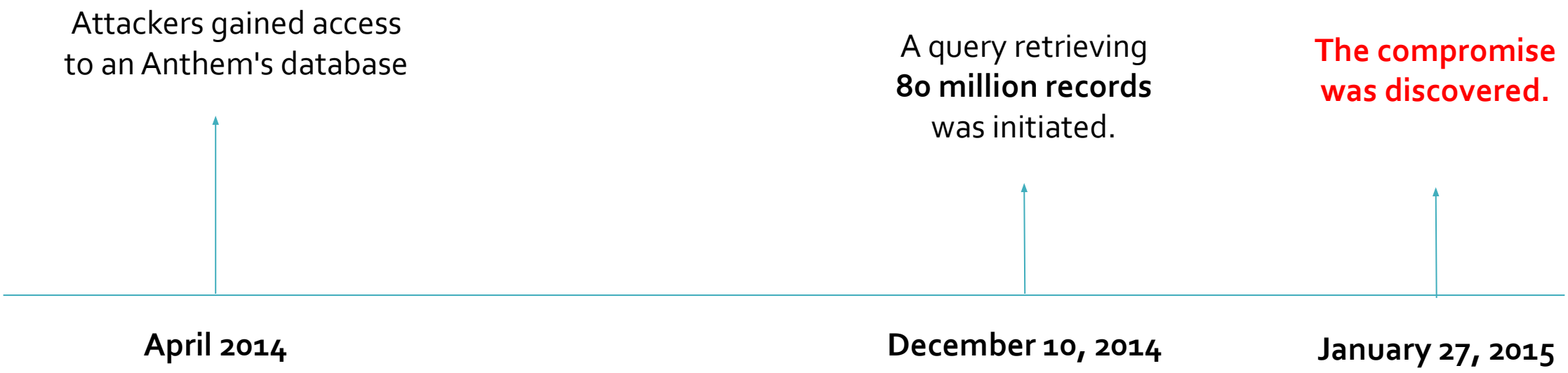



QUESTION:
How many patients were affected
by the Anthem breach?

DON'T DO THIS

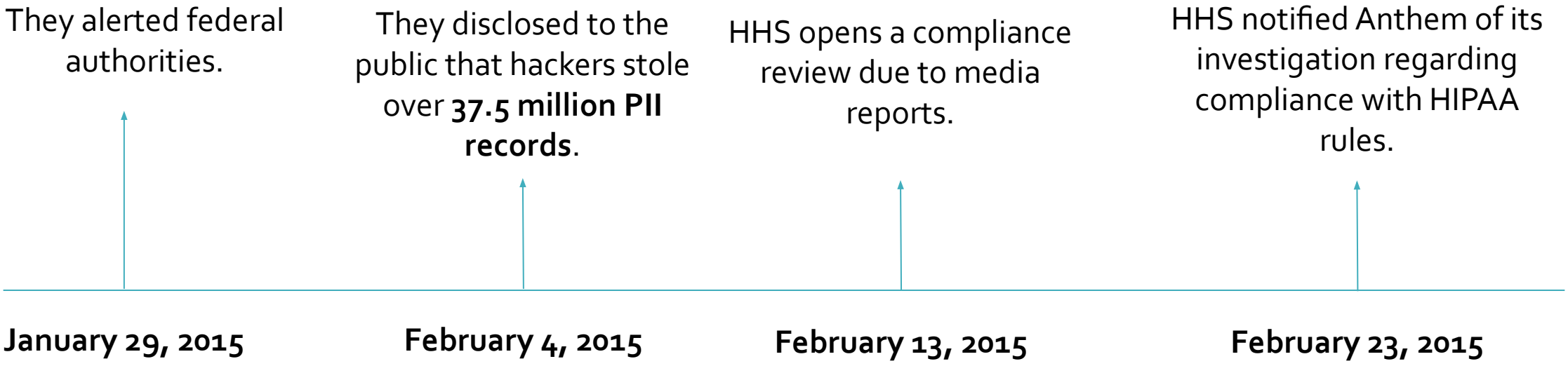
Anthem®

TIMELINE



DON'T DO THIS

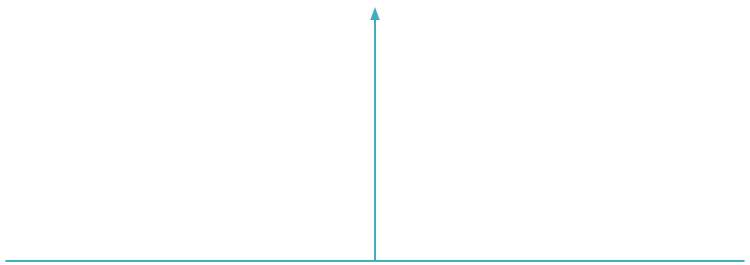
Anthem®



DON'T DO THIS

Anthem®

Anthem reports back to HHS that the number of affected persons is 78.8 million.



March 13, 2015


QUESTION:
How many patient records do you have at your company?

DON'T DO THIS

Anthem®

COMPANY INFO

Company Info:

- Fortune #29
- Publicly traded
- Health insurance company

- Annual revenue of $90 billion with earnings in 2017 of $3.8 billion

Did You Know?:

- largest for-profit managed health care company in the Blue Cross and Blue Shield Association

- Plans include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, and UniCare.

DON'T DO THIS

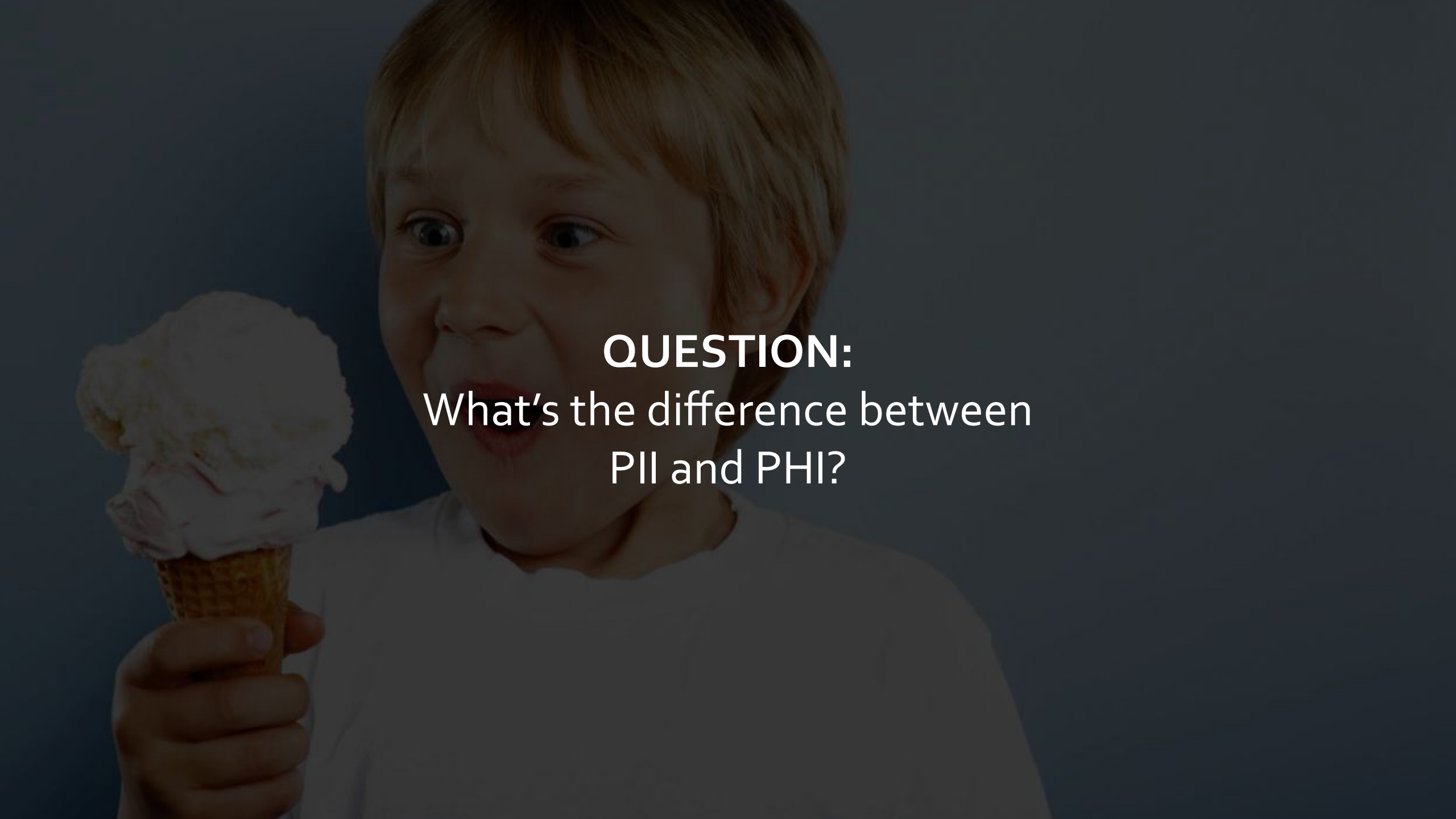
Anthem®

WHAT WAS STOLEN

Did You Know?:

- Names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data

- The stolen data was not encrypted


QUESTION:
What's the difference between
PII and PHI?

DON'T DO THIS

HOW DID THE BREACH HAPPEN?

we11point.com

DON'T DO THIS

2. The victim clicks on the link to we11point.com from the email

3. Installs several malware on victim's system

Attacker

1. Sends an email with link to we11point.com (impersonating as Wellpoint)

Victim

5b. Sends the credentials and access to the victim's system

5a. Accesses the Anthem database using credentials

6. Query resulting in 80 million rows as output

DON'T DO THIS

"**The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse** - a system that stores a large amount of consumer personally identifiable information," the report notes.

"Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records."

DON'T DO THIS

1	Domain Name: WE11POINT.COM	1	Domain Name: WE11POINT.COM
2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN	2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2014-04-21 03:13:19	5	Update Date: 2014-04-21 03:21:23
6	Creation Date: 2014-04-21 03:13:19	6	Creation Date: 2014-04-21 03:13:19
7	Registrar Registration Expiration Date: 2015-04-21 03:13:19	7	Registrar Registration Expiration Date: 2015-04-21 03:13:19
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.480-624-2505	11	Registrar Abuse Contact Phone: +1.480-624-2505
12	Domain Status: clientTransferProhibited	12	Domain Status: clientTransferProhibited
13	Domain Status: clientUpdateProhibited	13	Domain Status: clientUpdateProhibited
14	Domain Status: clientRenewProhibited	14	Domain Status: clientRenewProhibited
15	Domain Status: clientDeleteProhibited	15	Domain Status: clientDeleteProhibited
16	Registry Registrant ID:	16	Registry Registrant ID:
17	Registrant Name: wen ben zhou	17	Registrant Name: ad fire
18	Registrant Organization:	18	Registrant Organization:
19	Registrant Street: wen ren zheng fei ren chun 120hao	19	Registrant Street: fdsbcacfdt43
20	Registrant City: xiamen	20	Registrant City: new
21	Registrant State/Province: fu jian	21	Registrant State/Province:
22	Registrant Postal Code: 366115	22	Registrant Postal Code: 366512
23	Registrant Country: China	23	Registrant Country: Cayman Islands
24	Registrant Phone: +86.5925035801	24	Registrant Phone: +65.561235001


QUESTION:
Who do you think did it?

DON'T DO THIS

25	Registrant Email: li2384826402@yahoo.com
26	Registry Admin ID:
27	Admin Name: li ning
28	Admin Organization:
29	Admin Street: guangdongsheng
30	Admin City: guangzhoushi
31	Admin State/Province: Alabama
32	Admin Postal Code: 54152
33	Admin Country: United States
34	Admin Phone: +1.4805428751
35	Admin Phone Ext:
36	Admin Fax:
37	Admin Fax Ext:
38	Admin Email: li2384826402@yahoo.com
39	Registry Tech ID:
40	Tech Name: li ning
41	Tech Organization:
42	Tech Street: guangdongsheng
43	Tech City: guangzhoushi
44	Tech State/Province: Alabama
45	Tech Postal Code: 54152
46	Tech Country: United States
47	Tech Phone: +1.4805428751

28	Registrant Email: TopSec_2014@163.com
29	Registry Admin ID:
30	Admin Name: Top Sec
31	Admin Organization: TopSec
32	Admin Street: china
33	Admin City: china
34	Admin State/Province: china
35	Admin Postal Code: 100000
36	Admin Country: China
37	Admin Phone: +1.82776666
38	Admin Phone Ext:
39	Admin Fax:
40	Admin Fax Ext:
41	Admin Email: TopSec_2014@163.com
42	Registry Tech ID:
43	Tech Name: Top Sec
44	Tech Organization: TopSec
45	Tech Street: china
46	Tech City: china
47	Tech State/Province: china
48	Tech Postal Code: 100000
49	Tech Country: China
50	Tech Phone: +1.82776666

DON'T DO THIS

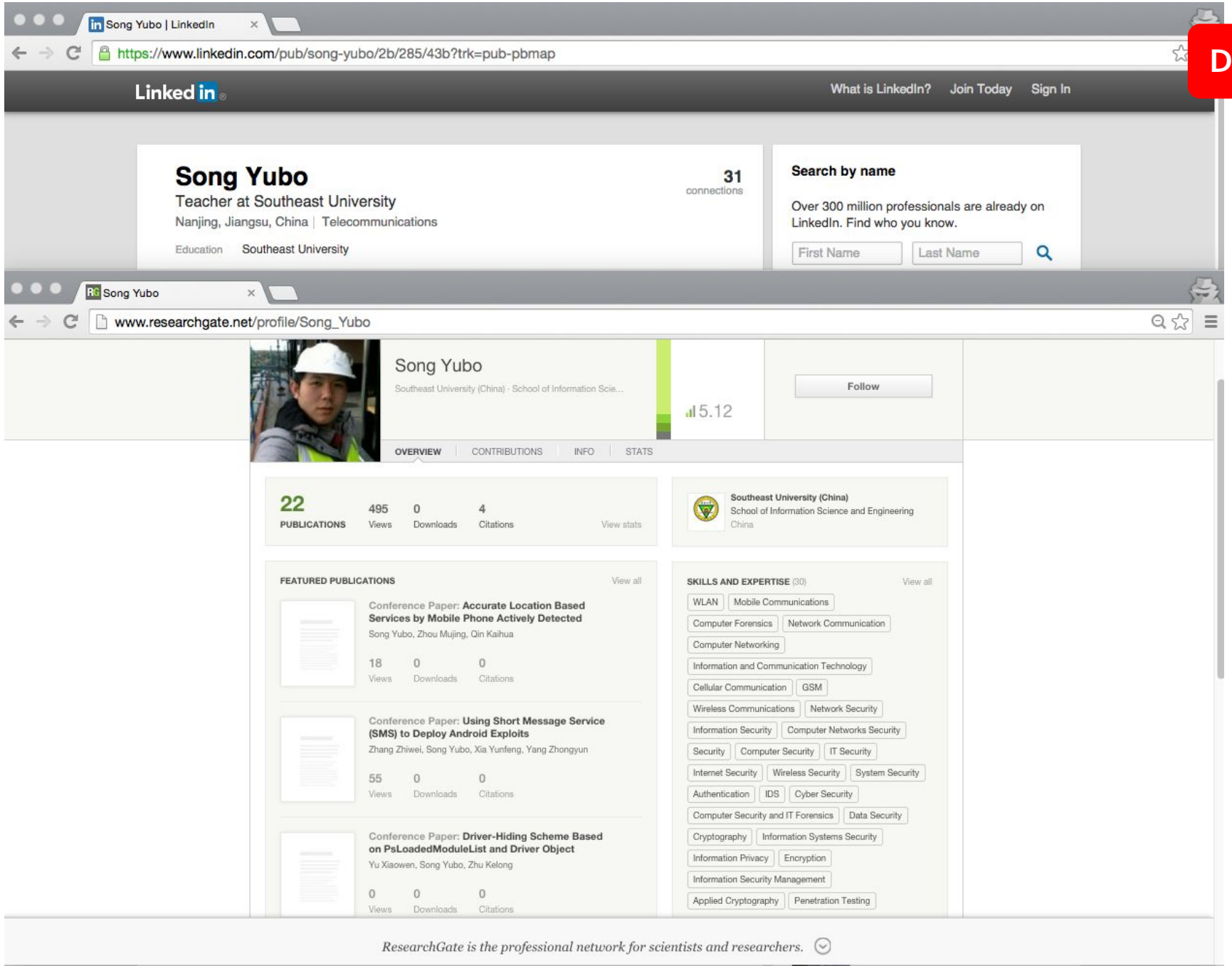
Anthem®

WHO DID IT

Did You Know?:

- The domain name belongs to Professor Song Yubo, a professor with the Information Security Research Center at Southeast University in Nanjing

- He has published numerous academic papers on computer network exploitation on various e-journal publication sites that can be found via Google Scholar

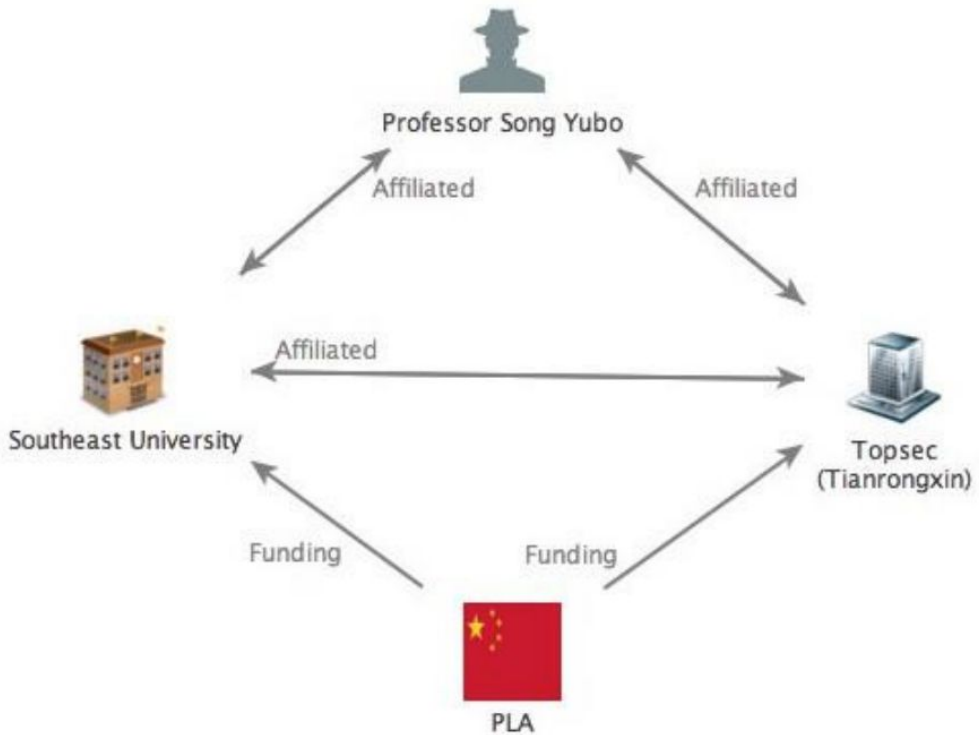

Song Yubo | LinkedIn
https://www.linkedin.com/pub/song-yubo/2b/285/43b?trk=pub-pbmap
Linked in
What is LinkedIn?
Join Today
Sign In
Song Yubo
Teacher at Southeast University
Nanjing, Jiangsu, China | Telecommunications
Education Southeast University
31
connections
Search by name
Over 300 million professionals are already on LinkedIn. Find who you know.
First Name
Last Name
Song Yubo
www.researchgate.net/profile/Song_Yubo
Song Yubo
Southeast University (China) · School of Information Scie...
5.12
Follow
OVERVIEW
CONTRIBUTIONS
INFO
STATS
22
PUBLICATIONS
495
Views
0
Downloads
4
Citations
View stats
Southeast University (China)
School of Information Science and Engineering
China
FEATURED PUBLICATIONS
View all
Conference Paper: Accurate Location Based Services by Mobile Phone Actively Detected
Song Yubo, Zhou Mujing, Qin Kaihua
18 Views 0 Downloads 0 Citations
Conference Paper: Using Short Message Service (SMS) to Deploy Android Exploits
Zhang Zhiwei, Song Yubo, Xia Yunfeng, Yang Zhongyun
55 Views 0 Downloads 0 Citations
Conference Paper: Driver-Hiding Scheme Based on PsLoadedModuleList and Driver Object
Yu Xiaowen, Song Yubo, Zhu Kelong
0 Views 0 Downloads 0 Citations
SKILLS AND EXPERTISE (30)
View all
WLAN
Mobile Communications
Computer Forensics
Network Communication
Computer Networking
Information and Communication Technology
Cellular Communication
GSM
Wireless Communications
Network Security
Information Security
Computer Networks Security
Security
Computer Security
IT Security
Internet Security
Wireless Security
System Security
Authentication
IDS
Cyber Security
Computer Security and IT Forensics
Data Security
Cryptography
Information Systems Security
Information Privacy
Encryption
Information Security Management
Applied Cryptography
Penetration Testing
ResearchGate is the professional network for scientists and researchers.

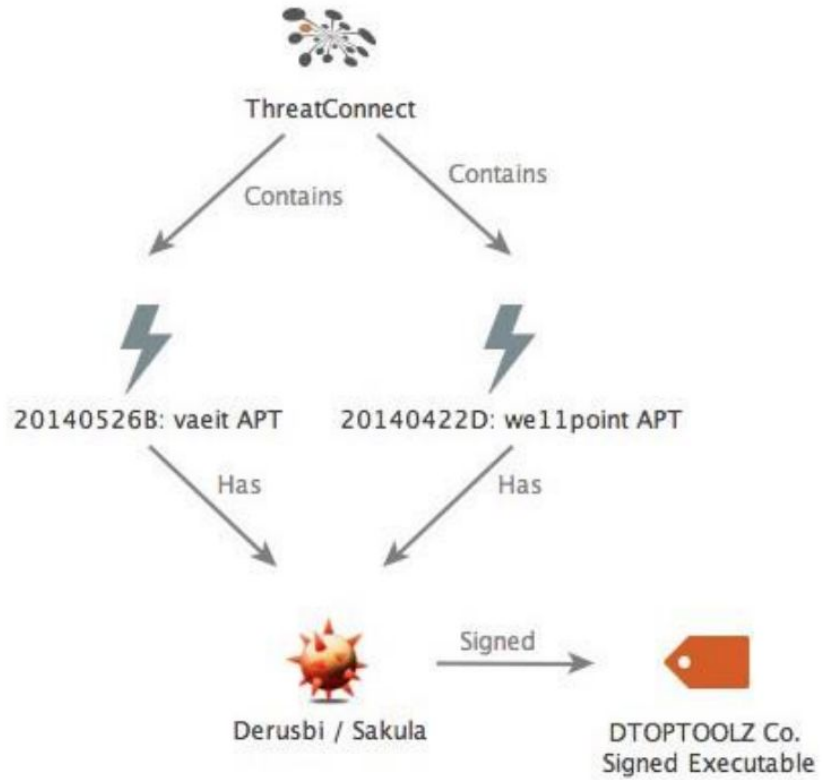
DON'T DO THIS

DON'T DO THIS

Competition Timeline	topsec2014 Infrastructure	VAE Inc. Juniper SSL Malware	Faux VAE Inc. Infrastructure
May 4 - 14 2014: Registration period	**May 6, 2014**: topsec2014[.]com registered by li2384826402@yahoo[.]com at 04:48:49; email registrant changed to TopSec_2014@163[.]com at 04:52:21. **May 8, 2014**: topsec2014[.]com resolves to 192.199.254.126. **May 10, 2014**: topsec2014[.]com does not resolve.	***	**May 17, 2014**: ssl-vaeit[.]com registered by li2384826402@yahoo[.]com at 06:51:01; changed to "Dubai Tycoon" at 06:56:27. **May 19, 2014**: wiki-vaeit[.]com registered by li2384826402@yahoo[.]com at 22:38:41; changed to "Tony Stark" at 22:40:02. **May 19, 2014**: sharepoint-vaeit[.]com registered by li2384826402@yahoo[.]com at 01:06:10; changed to "Natasha Romanov" at 01:09:48.
May 24, 2014: Preliminary remote access round	**May 22, 2014**: topsec2014[.]com resolves to 123.1.157.179. **May 24, 2014**: Changed name server from "NS11.DOMAINCONTROL.COM" to "NS1.JIASULE.NET".	**May 23, 2014**: Juniper SSL VPN ActiveX.exe compiled at 08:07:49, signed at 08:55:00; configured to call out to sharepoint-vaeit[.]com and 192.199.254.126.	***
May 31, 2014: Final round	***	***	***

DON'T DO THIS


Professor Song Yubo
Affiliated
Affiliated
Affiliated
Southeast University
Topsec
(Tianrongxin)
Funding
Funding
PLA


ThreatConnect
Contains
Contains
20140526B: vaeit APT
20140422D: we11point APT
Has
Has
Signed
Derusbi / Sakula
DTOPTOOLZ Co.
Signed Executable

DON'T DO THIS

Anthem®

WHO DID IT

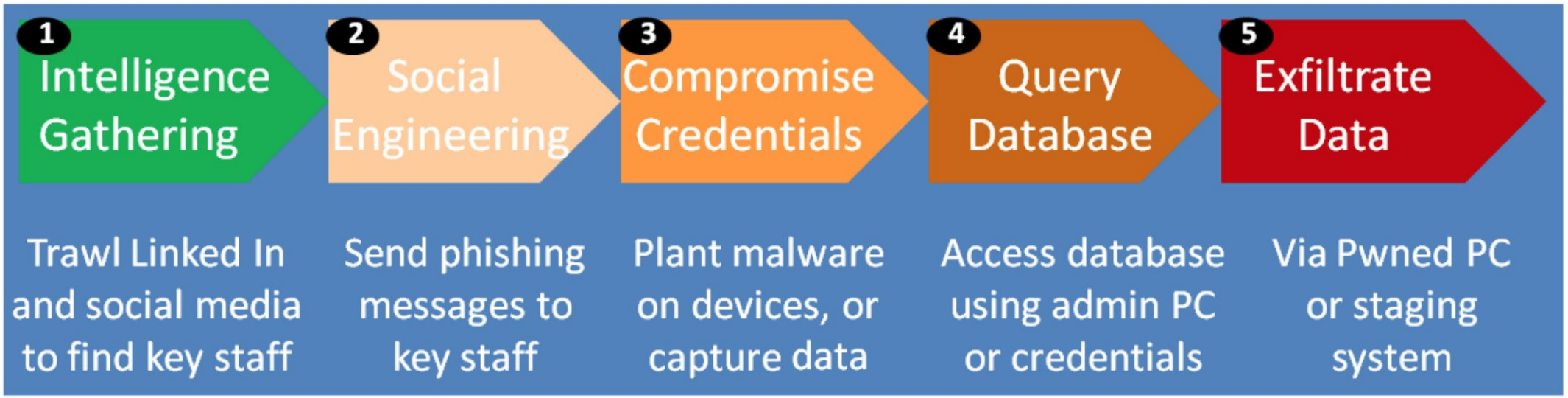
Did You Know?:

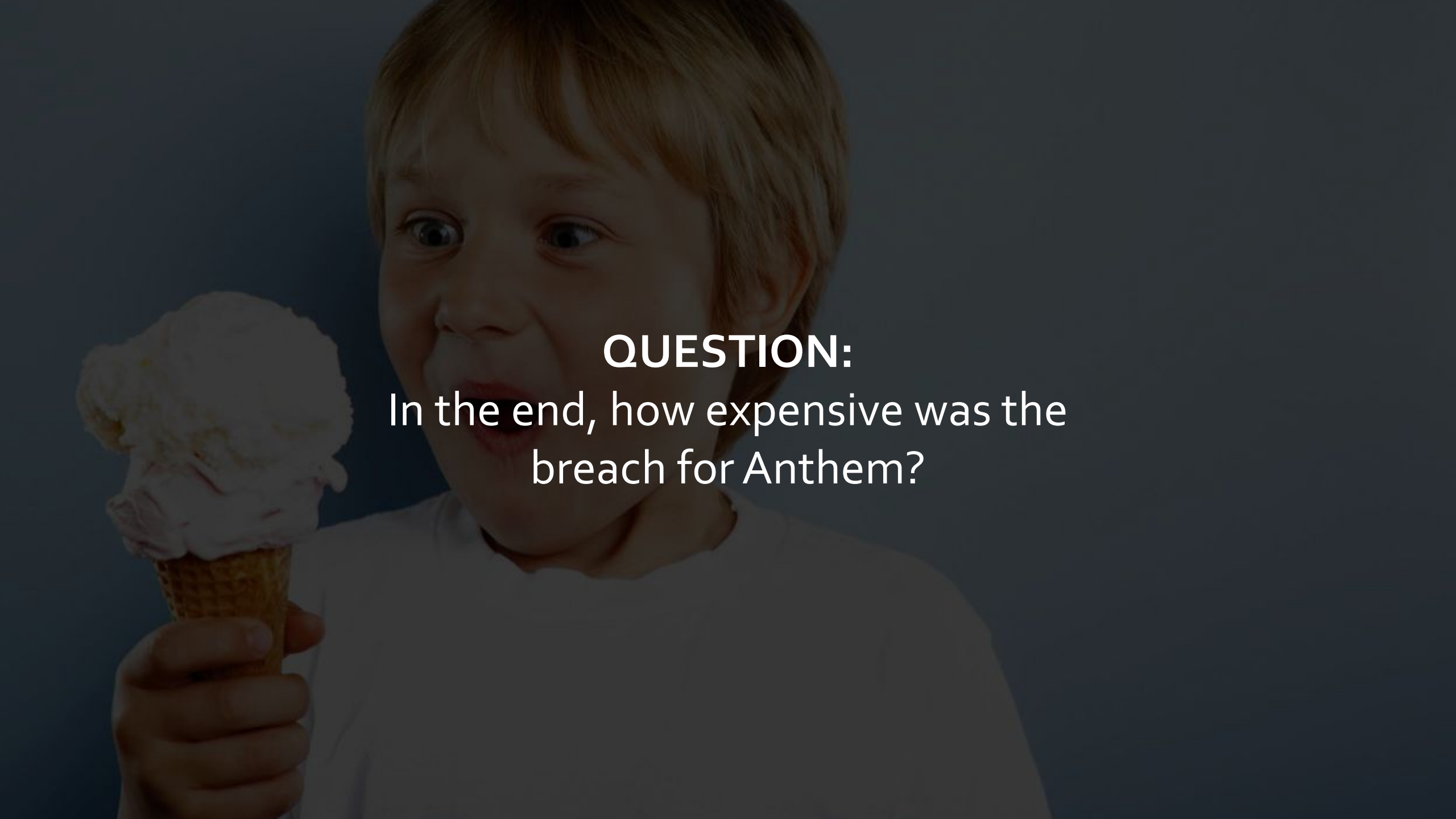
- He Weidong, the founder of Beijing Topsec has stated that Topsec actively recruits for the PLA cyber army from schools and the local independent hacker community.

- They hired notorious hacker Lin Yong, a.k.a. "Lion" in the early 2000s as a security service engineer and to conduct network training

DON'T DO THIS

RECAP




QUESTION:
In the end, how expensive was the breach for Anthem?

Anthem®

IMPACT

DON'T DO THIS

$2.5 million - Security consultants (ie. security firm Mandiant)

$115 million - Security improvements

$31 million - Notification to public and affected individuals

$112 million - Free credit monitoring and identity protection services

$31 million - Class-action legal fees

$39.5 million - Multi-state settlement in 2020

$16 million - October 15, 2018 paid record HIPAA settlement with OCR

$115 million - June 23, 2018 class-action settlement

\+

$$$ - other legal costs, higher insurance premiums, etc

At least **$462 million dollars**

*Data compiled from independent incident assessments, Anthem annual reports, DOJ indictment and state insurance commissioner reports.

DON'T DO THIS

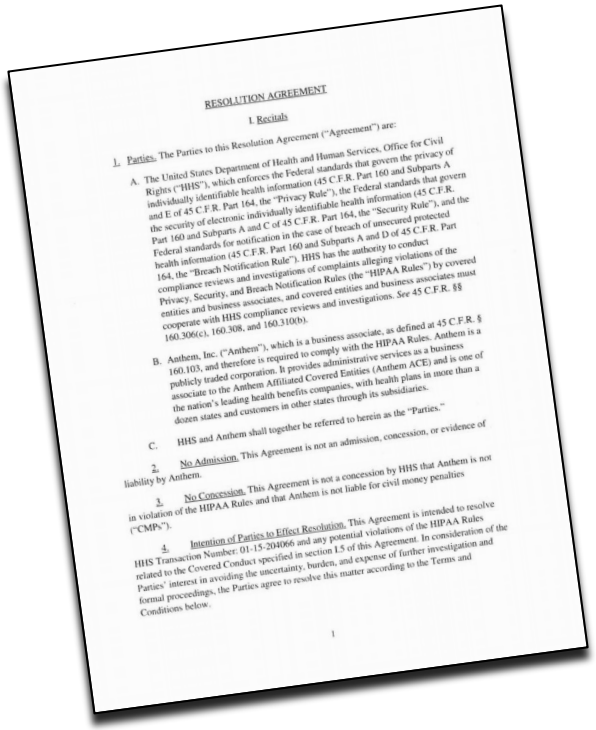
Anthem®

IMPACT

Investigation Revelations:

- **failed to conduct an enterprise-wide risk analysis**
- had insufficient procedures to regularly review information system activity
- **failed to identify and respond to suspected or known security incidents**
- failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI

Anthem®



RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are:

A. The United States Department of Health and Human Services, Office for Civil Rights ("HHS"), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164, the "Privacy Rule"), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164, the "Security Rule"), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the "Breach Notification Rule"). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the "HIPAA Rules") by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).

B. Anthem, Inc. ("Anthem"), which is a business associate, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. Anthem is a publicly traded corporation. It provides administrative services as a business associate to the Anthem Affiliated Covered Entities (Anthem ACE) and is one of the nation's leading health benefits companies, with health plans in more than a dozen states and customers in other states through its subsidiaries.

C. HHS and Anthem shall together be referred to herein as the "Parties."

2. No Admission. This Agreement is not an admission, concession, or evidence of liability by Anthem.

3. No Concession. This Agreement is not a concession by HHS that Anthem is not in violation of the HIPAA Rules and that Anthem is not liable for civil money penalties ("CMPs").

4. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 01-15-204066 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in section I.5 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden, and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

1

Corrective Action Plan

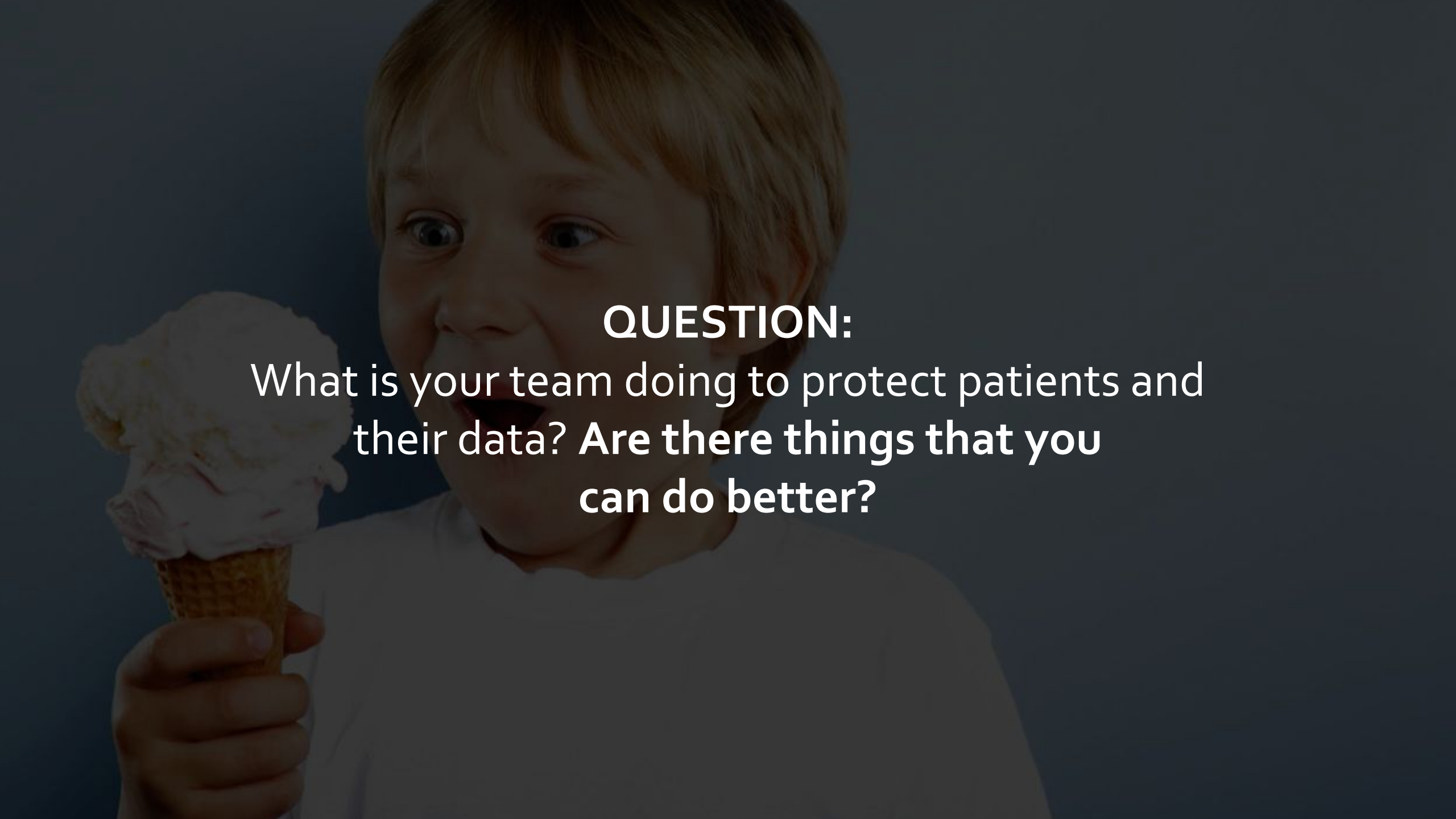
1. Conduct risk analysis **within 90 days**
2. **Within 150 days of approved risk analysis incorporate results of analysis into its security measures to reduce risks and vulnerabilities**
3. Revise and review all policies and procedures to confirm compliance with Federal standards for individually identifiable health information
4. **Submit an annual report** with the status of their compliance throughout the term
5. Retain all documents for six years

DON'T DO THIS

Anthem®

POST-BREACH CHANGES

- Implemented 2FA for all remote access tools (ie. VPN)
- Deployed a privileged account management tool
- Added enhanced logging resources to security event and incident management solutions
- Conducted a complete reset of passwords for privileged users
- Replaced all network admin ids
- Added database monitoring tech
- Created a plan for remediation of other exploitable vulnerabilities



QUESTION:

What is your team doing to protect patients and their data? **Are there things that you can do better?**

KEY TAKEAWAY

Tips

- Educate employees and clients on phishing attacks and the dangers of the Internet.
- Use principle of least privilege. Ensure that the applications asking for administration-level access are legitimate.
- Enable two factor authentication for employee and client accounts
- Transparency – If you see things that we could do better, say something to aid with prevention


Q&A

Jay Bobo
Application Security
@jaybobo