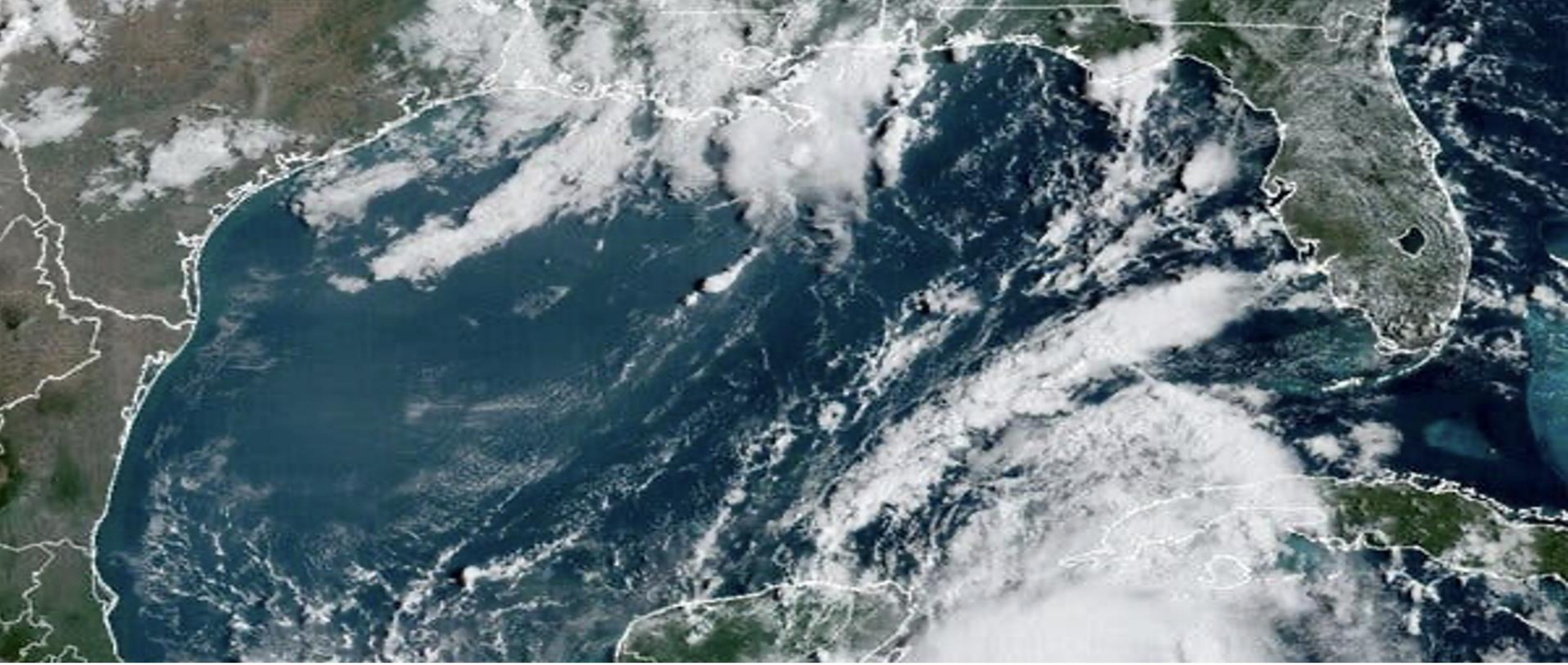
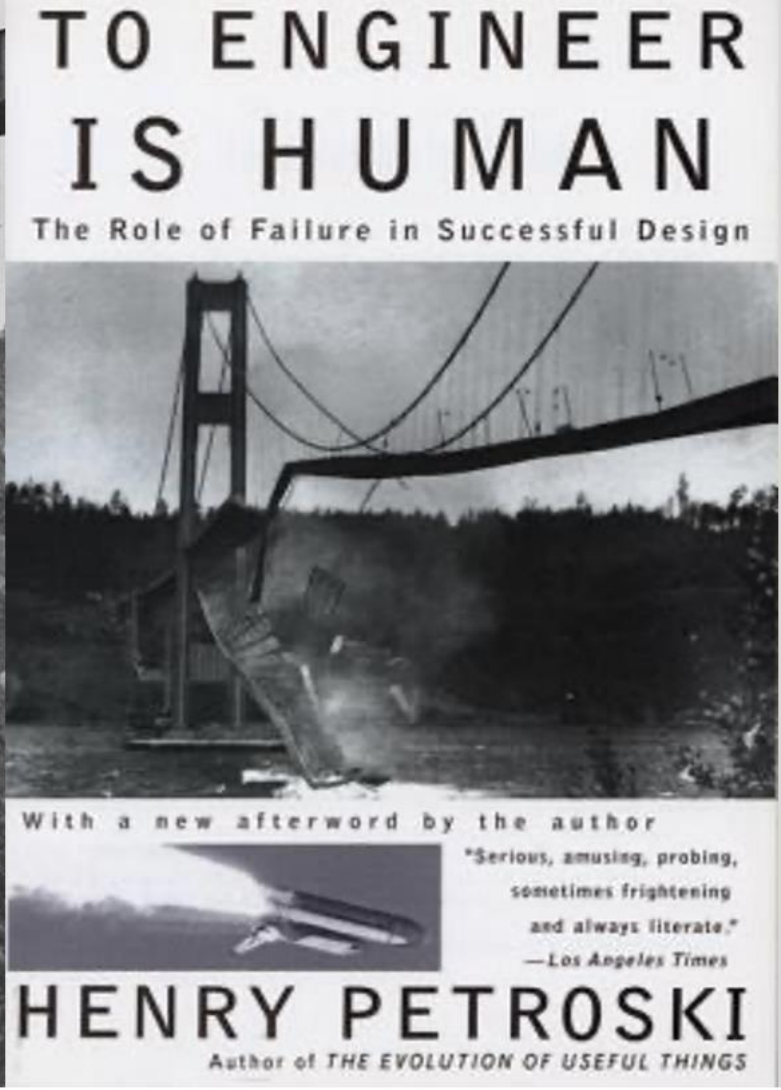
What Can We Learn from Major Cyber Catastrophes?



Hurricanes: Partially Controllable by Humans



Bridge Collapses: Mostly Controllable by Humans

Space Exploration Risk: Mostly Controllable by Humans

Cybersecurity Incidents: Fully Controllable by Humans

Numerator:
"Visit Mars"

Denominator:
"Space Deaths"

Observation: You can measure the success of an industry by dividing its achievements by its failures.

Numerator

Value Equation for Cyber

Success of Cybersecurity: Technologies That Enable Innovation, Automation, and Progress

---

Failure of Cybersecurity: Malicious Hacking, Break-Ins, Breaches, Disruptions and other Incidents

Let's spend time reviewing the denominator of this equation

Denominator

What Can We Learn from Major Cyber Incidents?

40 Million Credit Cards Stolen from Target

- Hacked third-party vendor access unnoticed from 12/2/13 to 1/16/14
- CEO and CIO of Target apologized and resigned
- Remediation/legal costs: $162M (Target) and $200M (Banks)

40 Million Credit Cards Stolen from Target

- Hacked third-party vendor access unnoticed from 12/2/13 to 1/16/14
- CEO and CIO of Target apologized and resigned
- Remediation/legal costs: $162M (Target) and $200M (Banks)

145 Million eBay Users Hacked

- Compromised name, encrypted password, email, home address, etc.
- Companywide password reset function was used in the attack.
- “The focus is on recovery,” CEO John Donahoe.

145 Million eBay Users Hacked

- Compromised name, encrypted password, email, home address, etc.
- Companywide password reset function was used in the attack.
- “The focus is on recovery,” CEO John Donahoe.

Five Month Undetected Attack at Home Depot

- Compromised 56 million customer payment cards – Five-month **Dwell Time**
- CEO apologized publicly after the cyber attack
- Famous security budget retort from ex-employee: “We sell hammers.”

Five Month Undetected Attack at Home Depot

- Compromised 56 million customer payment cards – Five-month **Dwell Time**
- CEO apologized publicly after the cyber attack
- Famous security budget retort from ex-employee: “We sell hammers.”

76 Million Households Hit by JPMC Breach

- Customer contact information – name, email, address, and phone
- 2014 attack blamed on Russian hackers by FBI
- CEO Jamie Dimon claims increasing JPMC Cyber Security budget by $250M

76 Million Households Hit by JPMC Breach

- Customer contact information – name, email, address, and phone
- 2014 attack blamed on Russian hackers by FBI
- CEO Jamie Dimon claims increasing JPMC Cyber Security budget by $250M

Sony Destructively Hacked by North Korea

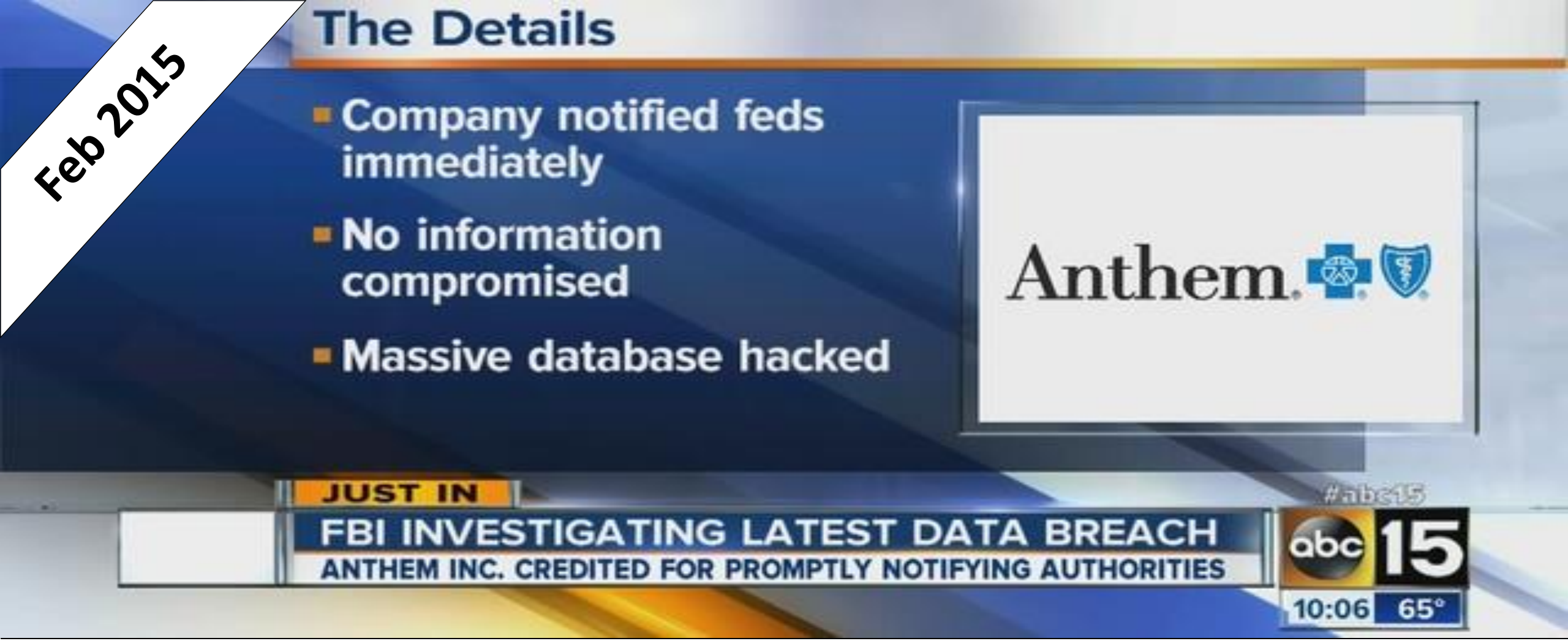
- Destructive malware attack ruined Sony compute infrastructure
- Revealed corporate emails including racist remarks about Pres. Obama
- “It was an attack on our freedom of expression.” DHS Secretary Johnson

Nov 2014

Destructive Attack

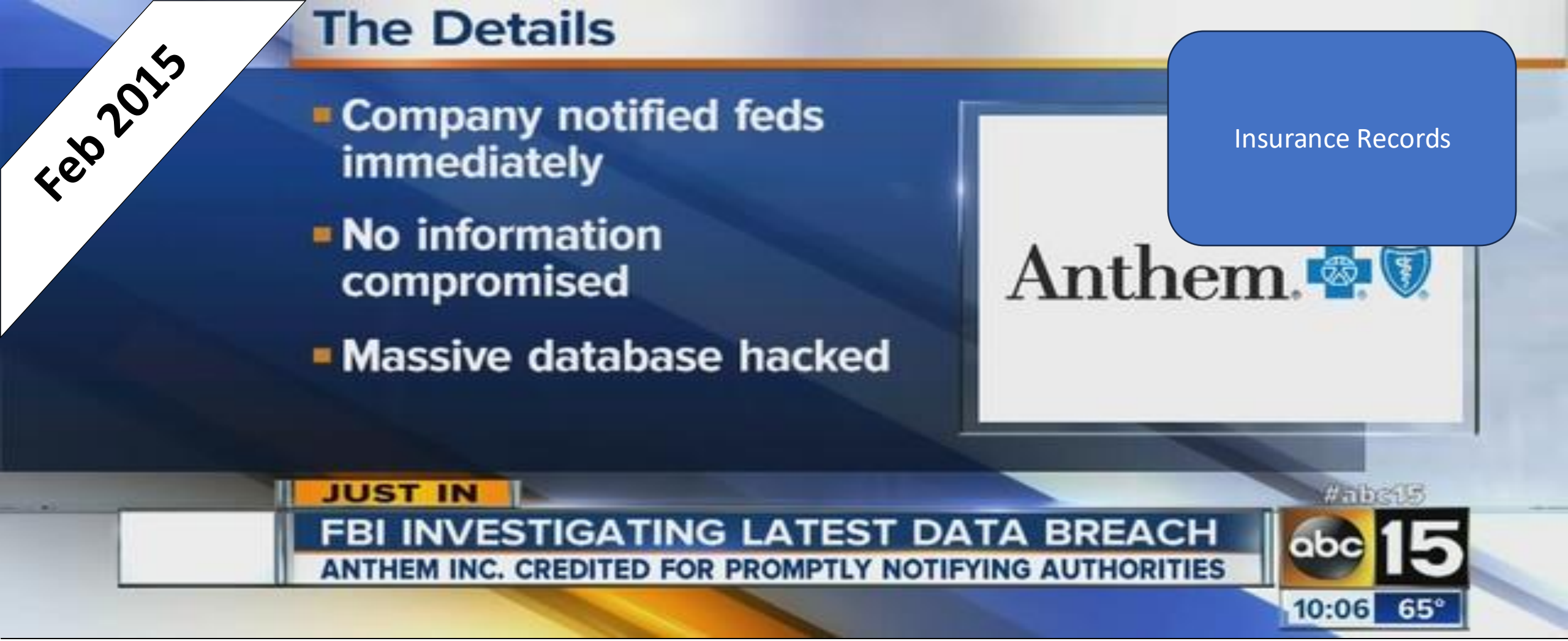
Sony Destructively Hacked by North Korea

- Destructive malware attack ruined Sony compute infrastructure
- Revealed corporate emails including racist remarks about Pres. Obama
- “It was an attack on our freedom of expression.” DHS Secretary Johnson



80 Million Medical Records Stolen from Anthem

- Two-month process to notify astonished customers
- Abnormal system behavior went unnoticed for several months
- “I want to personally apologize to each of you.” *Joseph Swedish, CEO*



80 Million Medical Records Stolen from Anthem

- Two-month process to notify astonished customers
- Abnormal system behavior went unnoticed for several months
- “I want to personally apologize to each of you.” *Joseph Swedish, CEO*

11 Million Premera Customer Insurance Records

- Thirty-eight class action lawsuits based on 2015 attack
- Name, birthdate, SSN, address, bank account info, claim info, etc.
- “Privacy of our members’ personal information remains a priority.”

11 Million Premera Customer Insurance Records

- Thirty-eight class action lawsuits based on 2015 attack
- Name, birthdate, SSN, address, bank account info, claim info, etc.
- “Privacy of our members’ personal information remains a priority.”

Hackers Nab Data on 18,000 Penn State Students

- Started in September 2012, continued through mid-2014
- University claims attack carried out by Chinese threat actor
- CISO being recruited ($300K- $700K) – Avg. Public College Pres. ($428K)

Hackers Nab Data on 18,000 Penn State Students

- Started in September 2012, continued through mid-2014
- University claims attack carried out by Chinese threat actor
- CISO being recruited ($300K- $700K) – Avg. Public College Pres. ($428K)

Sixteen Month Undetected OPM Breach

- Background and thumbprints for 15% of the US workforce
- Director Katherine Archuleta resigned 7/15
- Military group from PRC most likely malicious actor

Sixteen Month Undetected OPM Breach

- Background and thumbprints for 15% of the US workforce
- Director Katherine Archuleta resigned 7/15
- Military group from PRC most likely malicious actor

Hackers Breach Harvard University Credentials

- Involved eight colleges (Arts & Sciences, Divinity, Radcliffe, etc.)
- University has no clear understanding of what happened or how
- FAQ suggests that everyone change their passwords

Hackers Breach Harvard University Credentials

- Involved eight colleges (Arts & Sciences, Divinity, Radcliffe, etc.)
- University has no clear understanding of what happened or how
- FAQ suggests that everyone change their passwords

Oct 2015

...etter to Consumers

T-Mobile CEO on Experian's Data Breach

I've always said that part of being the Un-carrier means telling it like it is. Whether it's good news or bad, I'm going to be direct, transparent and honest.

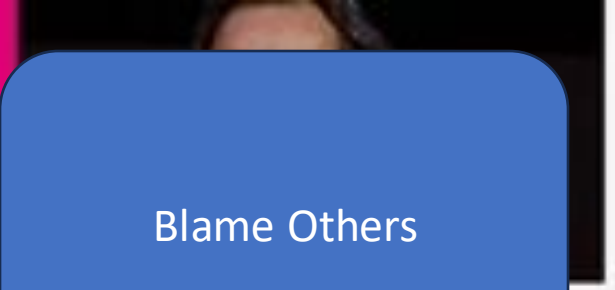
We have been notified by Experian, a vendor that processes our credit applications, that they have experienced a data breach. The investigation is ongoing, but what we know right now is that the hacker acquired the records of approximately 15 million people, including new applicants requiring a credit check for service or device financing from **September 1, 2013**

15 Million T-Mobile Records via Experian Breach

- Experian providing third-party marketing services to T-Mobile
- Name, address, SSN, birth date, passport/driver's license, etc.
- "T-Mobile's Legere 'Incredibly Angry' about Breach" – News Reports

Oct 2015

Letter to Consumers



Blame Others

T-Mobile CEO on Experian's Data Breach

I've always said that part of being the Un-carrier means telling it like it is. Whether it's good news or bad, I'm going to be direct, transparent and honest.

We have been notified by Experian, a vendor that processes our credit applications, that they have experienced a data breach. The investigation is ongoing, but what we know right now is that the hacker acquired the records of approximately 15 million people, including new applicants requiring a credit check for service or device financing from **September 1, 2013**

15 Million T-Mobile Records via Experian Breach

- Experian providing third-party marketing services to T-Mobile
- Name, address, SSN, birth date, passport/driver's license, etc.
- "T-Mobile's Legere 'Incredibly Angry' about Breach" – News Reports

200,000 Comcast Customer Records Exposed

- Company reported 200,000 customer records “exposed to hackers”
- 590,000 customer records for sale on Dark Web for $1,000.00
- Company requested that customers change their passwords

Bad Account Inventory

200,000 Comcast Customer Records Exposed

- Company reported 200,000 customer records “exposed to hackers”
- 590,000 customer records for sale on Dark Web for $1,000.00
- Company requested that customers change their passwords

Hackers Shut Power to 80,000 Ukrainian Citizens

- Hacked Power Company 1: Prykarpattyaoblenergo Electric Utility
- Hacked Power Company 2: Kyivoblenergo Electric Utility
- Affected Six More Companies with BlackEnergy Trojan Horse

Hackers Shut Power to 80,000 Ukrainian Citizens

- Hacked Power Company 1: Prykarpattyaoblenergo Electric Utility
- Hacked Power Company 2: Kyivoblenergo Electric Utility
- Affected Six More Companies with BlackEnergy Trojan Horse

191 Million US Voter Records Compromised

- NationBuilder collects information and provides as-a-service
- “We strongly believe in making voter information more accessible to political campaigns and advocacy groups,” NationBuilder's CEO Jim Gilliam

191 Million US Voter Records Compromised

- NationBuilder collects information and provides as-a-service
- “We strongly believe in making voter information more accessible to political campaigns and advocacy groups,” NationBuilder's CEO Jim Gilliam

Hackers Sell 1.5 Million Customer Records

- 1.5 million Verizon customer records stolen from the company
- Sale price: $100,000 for the entire package on the Dark Web
- Verizon blamed an exploitable flaw in their Website

Hackers Sell 1.5 Million Customer Records

- 1.5 million Verizon customer records stolen from the company
- Sale price: $100,000 for the entire package on the Dark Web
- Verizon blamed an exploitable flaw in their Website

Apr 2016

1,025 Wendy's Stores Hit by Credit Card Breach

- Blamed on unnamed third-party with access to company
- Company hit with class action lawsuit after the breach
- Initial statement under-estimated impact by the company initially

Apr 2016

Compliance Issue

1,025 Wendy's Stores Hit by Credit Card Breach

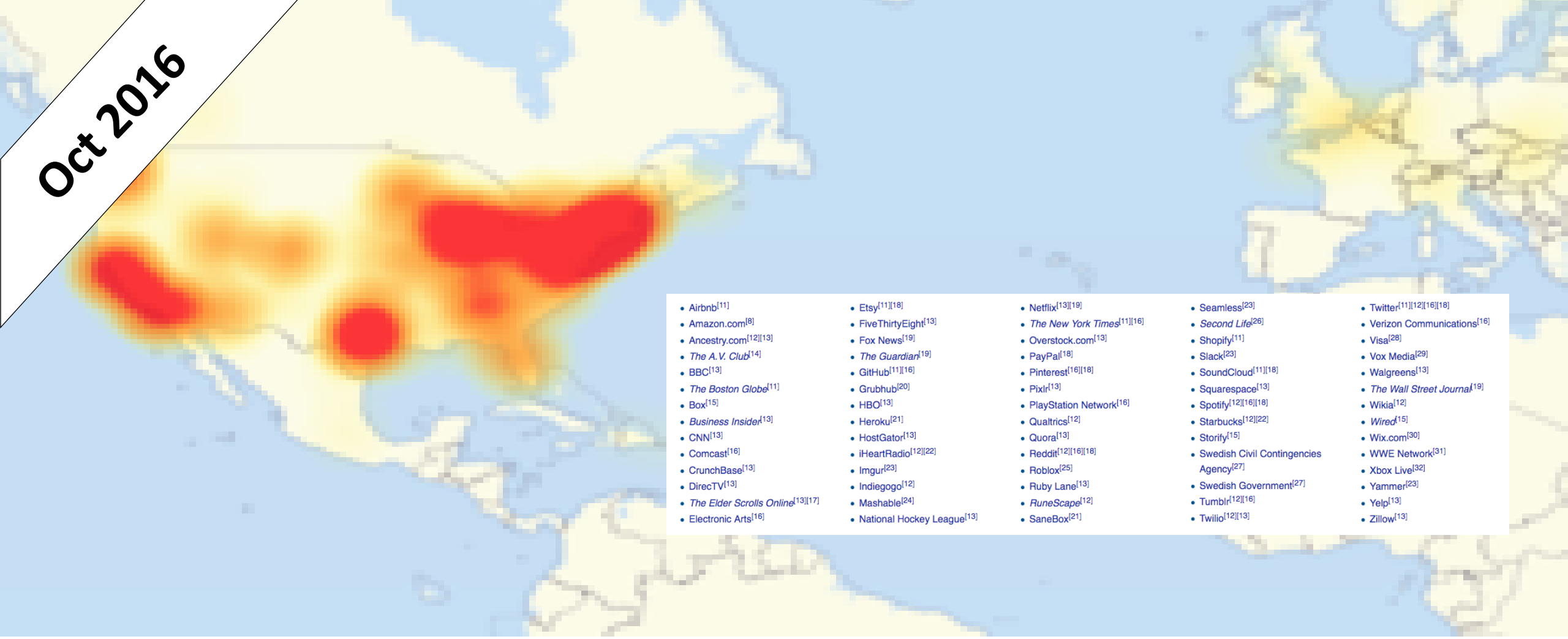
- Blamed on unnamed third-party with access to company
- Company hit with class action lawsuit after the breach
- Initial statement under-estimated impact by the company initially

427 Million Stolen MySpace Passwords

- Hacker selling batch for $2800 payment
- Hacker also claims to have data on 164M LinkedIn Accounts
- Danger: Do not reuse passwords across accounts

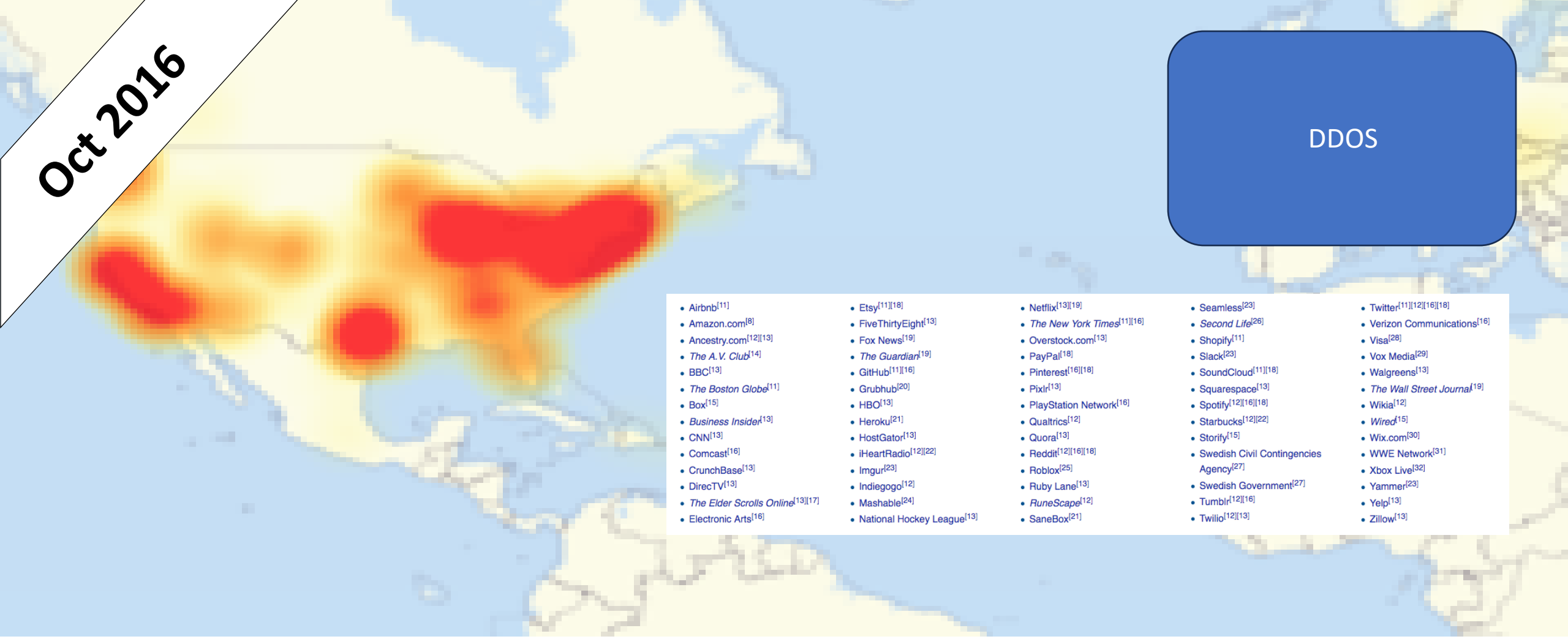
427 Million Stolen MySpace Passwords

- Hacker selling batch for $2800 payment
- Hacker also claims to have data on 164M LinkedIn Accounts
- Danger: Do not reuse passwords across accounts



DYN DDOS Attack

- Massive DDOS attack (possibly by Anonymous)
- Caused outages across major North American services
- Botnet: Cameras, gateways, baby monitor, and other IoT devices



DYN DDOS Attack

- Massive DDOS attack (possibly by Anonymous)
- Caused outages across major North American services
- Botnet: Cameras, gateways, baby monitor, and other IoT devices

Nov 2016

US Election "Information" Attacks

- Difference between "cyber superiority" and "information superiority"
- American Intelligence Community concludes Russian origin
- Social media manipulated using poorly monitored features

Nov 2016

Fake News

US Election "Information" Attacks

- Difference between "cyber superiority" and "information superiority"
- American Intelligence Community concludes Russian origin
- Social media manipulated using poorly monitored features

May 2017

WannaCry Ransomware Attack

- Hits 300,000 targets including National Institute of Health (NIH)
- Spread via worm using tools stolen from NSA
- Suggests weak disaster planning across most global business

May 2017

Ransomware

WannaCry Ransomware Attack

- Hits 300,000 targets including National Institute of Health (NIH)
- Spread via worm using tools stolen from NSA
- Suggests weak disaster planning across most global business

Equifax Breach Affects 143M US Citizens

- Vulnerabilities unpatched in Apache Struts in Equifax portal
- First vulnerability reported weeks before attack commenced
- Hackers created 39 undetected back doors into Equifax

Equifax Breach Affects 143M US Citizens

- Vulnerabilities unpatched in Apache Struts in Equifax portal
- First vulnerability reported weeks before attack commenced
- Hackers created 39 undetected back doors into Equifax

Aug 2017

Bi…ata breach! Aadhaar software hack …ses major security concerns

…software patch, which can be bought for as little as Rs 2,500 - reportedly allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers.

BusinessToday.In Last Updated: September 11, 2018 | 21:18 IST

Aadhaar Exposes 1.1B Citizens of India

- Breach exposed Aadhaar number, names, emails, and physical addresses.
- Also breached phone numbers and photos.
- Break-in to India's Unique Identification Authority (records of all citizens)

Aug 2017

International

Bi…ata breach! Aadhaar softwa…ses major security concerns

…software patch, which can be bought for as little as Rs 2,500 - reportedly allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers.

BusinessToday.In Last Updated: September 11, 2018 | 21:18 IST

Aadhaar Exposes 1.1B Citizens of India

- Breach exposed Aadhaar number, names, emails, and physical addresses.
- Also breached phone numbers and photos.
- Break-in to India's Unique Identification Authority (records of all citizens)

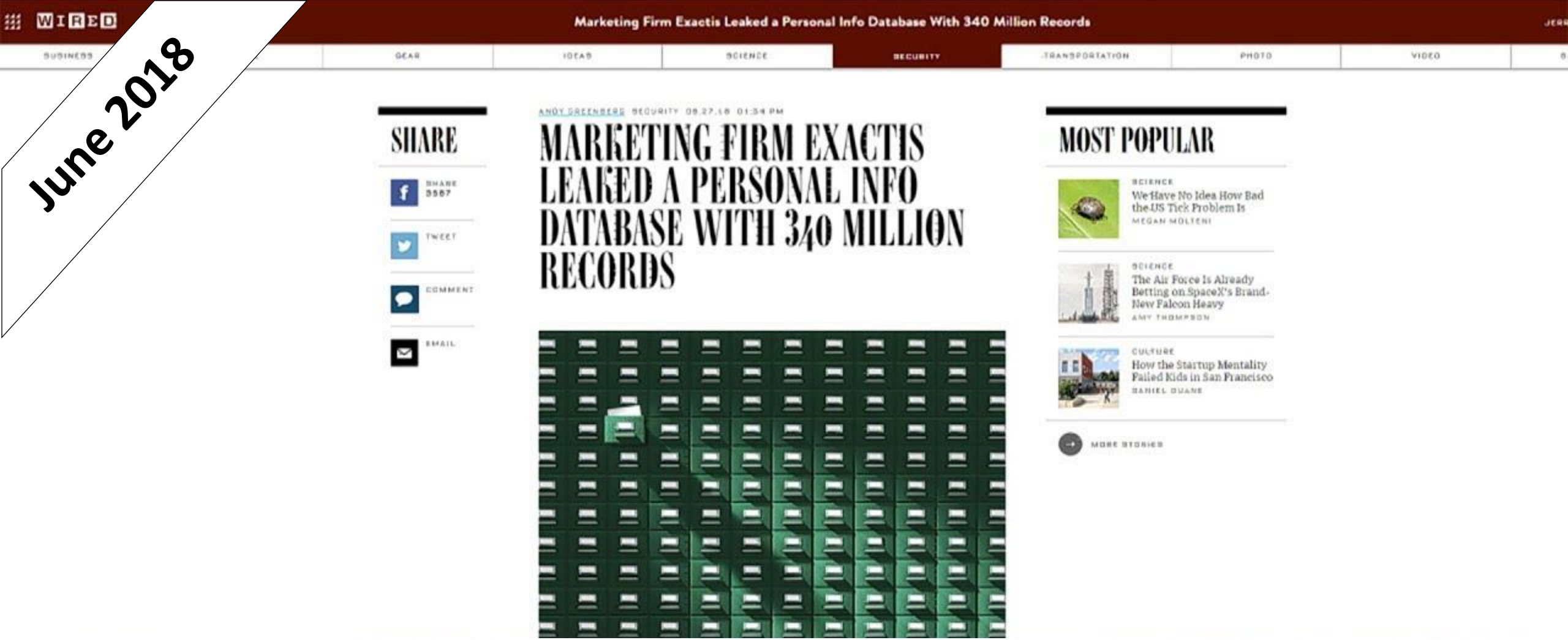
Hackers Breach Personal Data for 45M Uber Riders

- Attack occurred in 2016 (GitHub account), but reported in 2017
- Hackers demanded $100K for data and Uber paid the fee
- Cover-up causing considerable litigation on-going

Hackers Breach Personal Data for 45M Uber Riders

- Attack occurred in 2016 (GitHub account), but reported in 2017
- Hackers demanded $100K for data and Uber paid the fee
- Cover-up causing considerable litigation on-going

June 2018

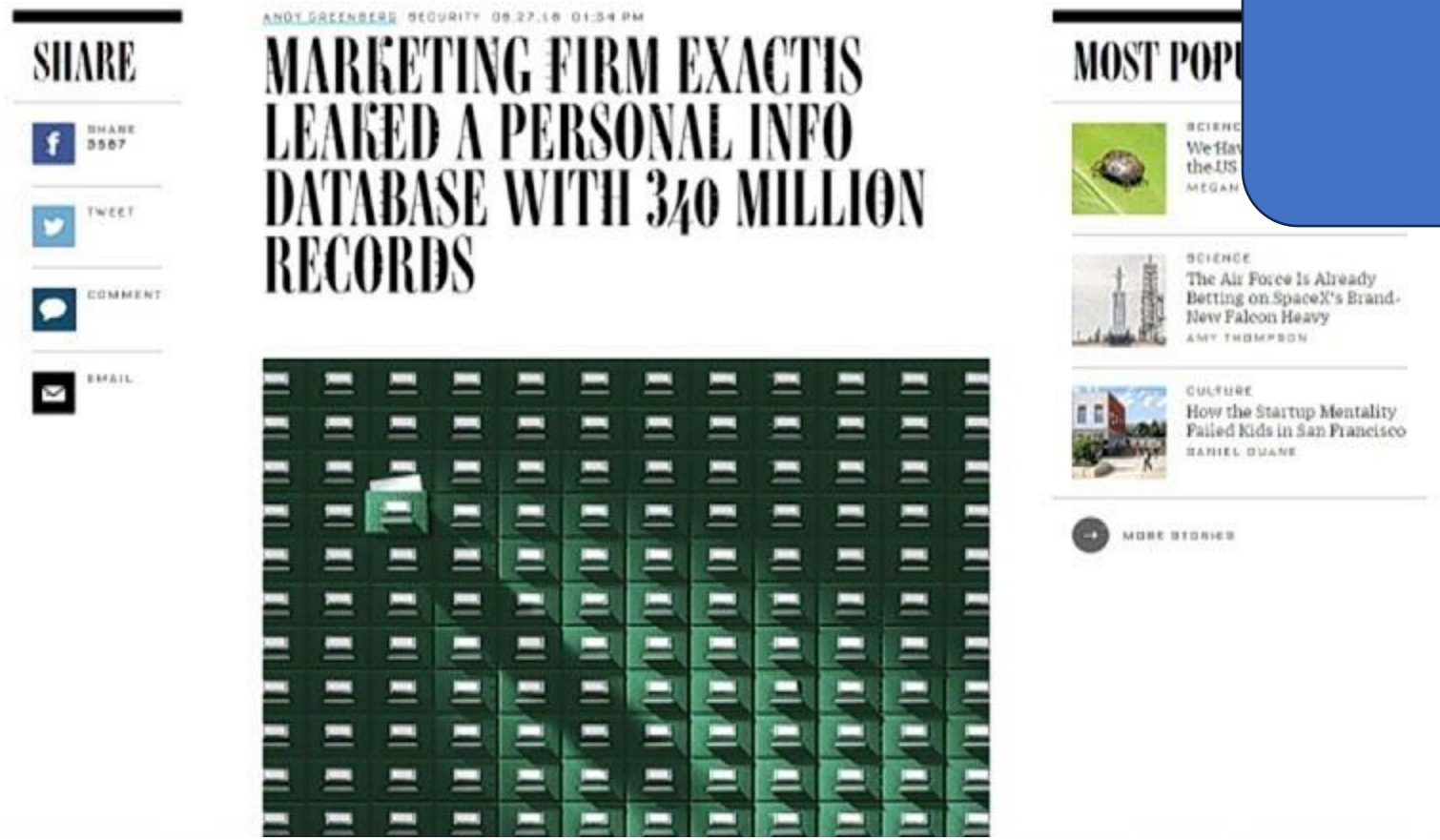


Exactis Exposes Data for 340M US Citizens

- Marketing firm had hacked data included name, address, email, etc.
- Security researcher noticed database openly accessible (via Shodan)
- Massive implications for citizen privacy

June 2018

Big Data



Exactis Exposes Data for 340M US Citizens

- Marketing firm had hacked data included name, address, email, etc.
- Security researcher noticed database openly accessible (via Shodan)
- Massive implications for citizen privacy

Starwood/Marriott Exposes Data for 500M Guests

- Breach exposed names, email addresses, and physical addresses.
- Also phone numbers, passport numbers, and account info.
- Also birth dates, gender, travel info, and accommodation info.
- Second Largest Breach Ever. (After Yahoo)

Starwood/Marriott Exposes Data for 500M Guests

- Breach exposed names, email addresses, and physical addresses.
- Also phone numbers, passport numbers, and account info.
- Also birth dates, gender, travel info, and accommodation info.
- Second Largest Breach Ever. (After Yahoo)

CapitalOne Breach Affects 100M Accounts

- Breach involved AWS misconfiguration
- Affected 100 million individuals in the US and 6 million in Canada
- Credit card and social security number information

CapitalOne Breach Affects 100M Accounts

- Breach involved AWS misconfiguration
- Affected 100 million individuals in the US and 6 million in Canada
- Credit card and social security number information

Ecuador Exposes 118% of Citizens Data

- Misconfigured Ecuadorian government database leaked 20.8 million user records
- Birth data, marital status, national ID, home addresses, children's info, phone and education recs.
- Official population is about 17.5 million

Ecuador Exposes 118% of Citizens Data

- Misconfigured Ecuadorian government database leaked 20.8 million user records
- Birth data, marital status, national ID, home addresses, children's info, phone and education recs.
- Official population is about 17.5 million

Apr 2020

Hackers Sell Half Million Zoom Accounts

- The credentials of over 500K Zoom accounts were stolen by hackers
- Found for sale on the Dark Web and hacker forums for as little as two cents per account.
- Email addresses, passwords, personal meeting URLs, and host keys stolen

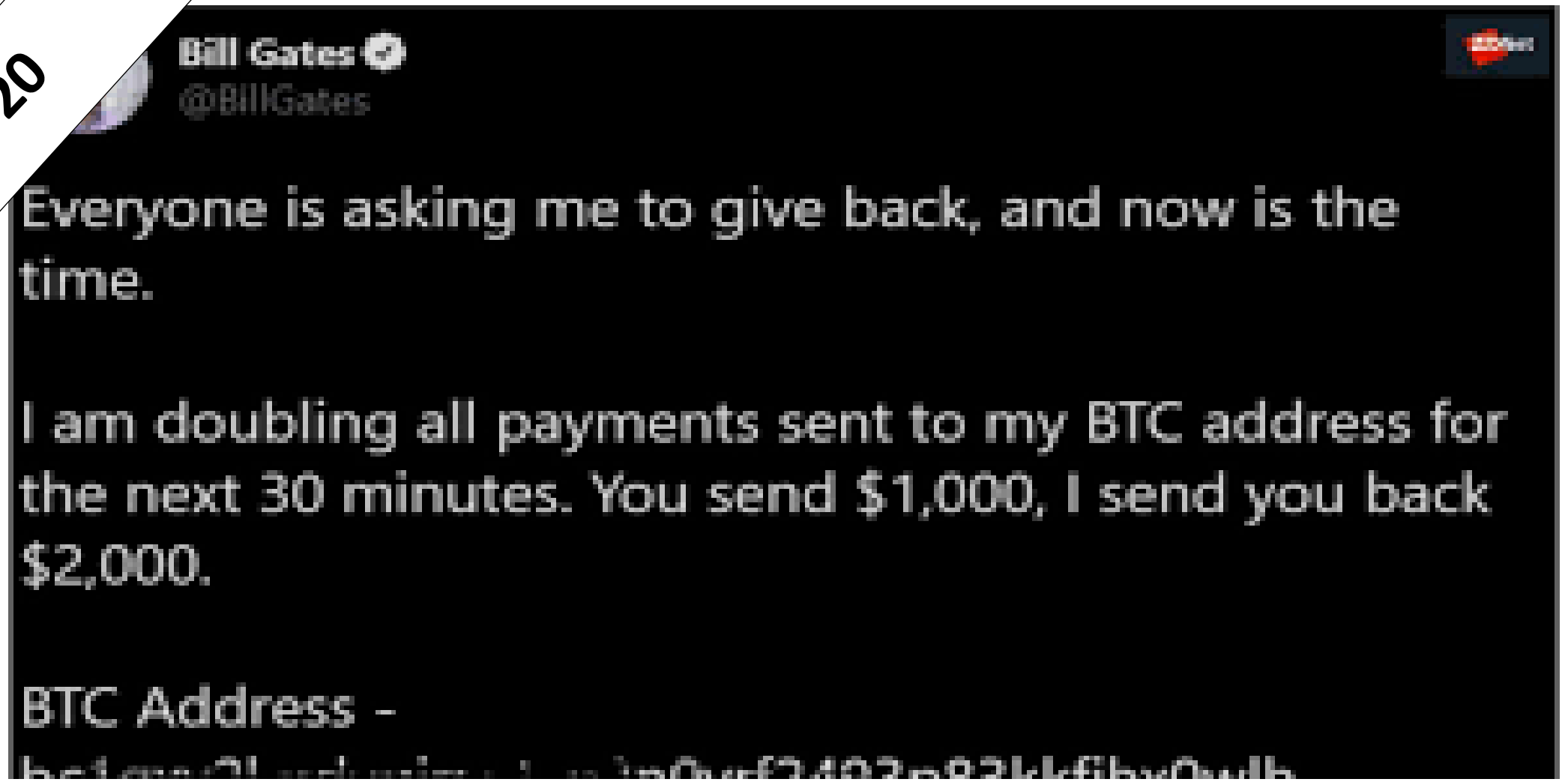
Apr 2020

Work from Home

Hackers Sell Half Million Zoom Accounts

- The credentials of over 500K Zoom accounts were stolen by hackers
- Found for sale on the Dark Web and hacker forums for as little as two cents per account.
- Email addresses, passwords, personal meeting URLs, and host keys stolen

Jul 2020

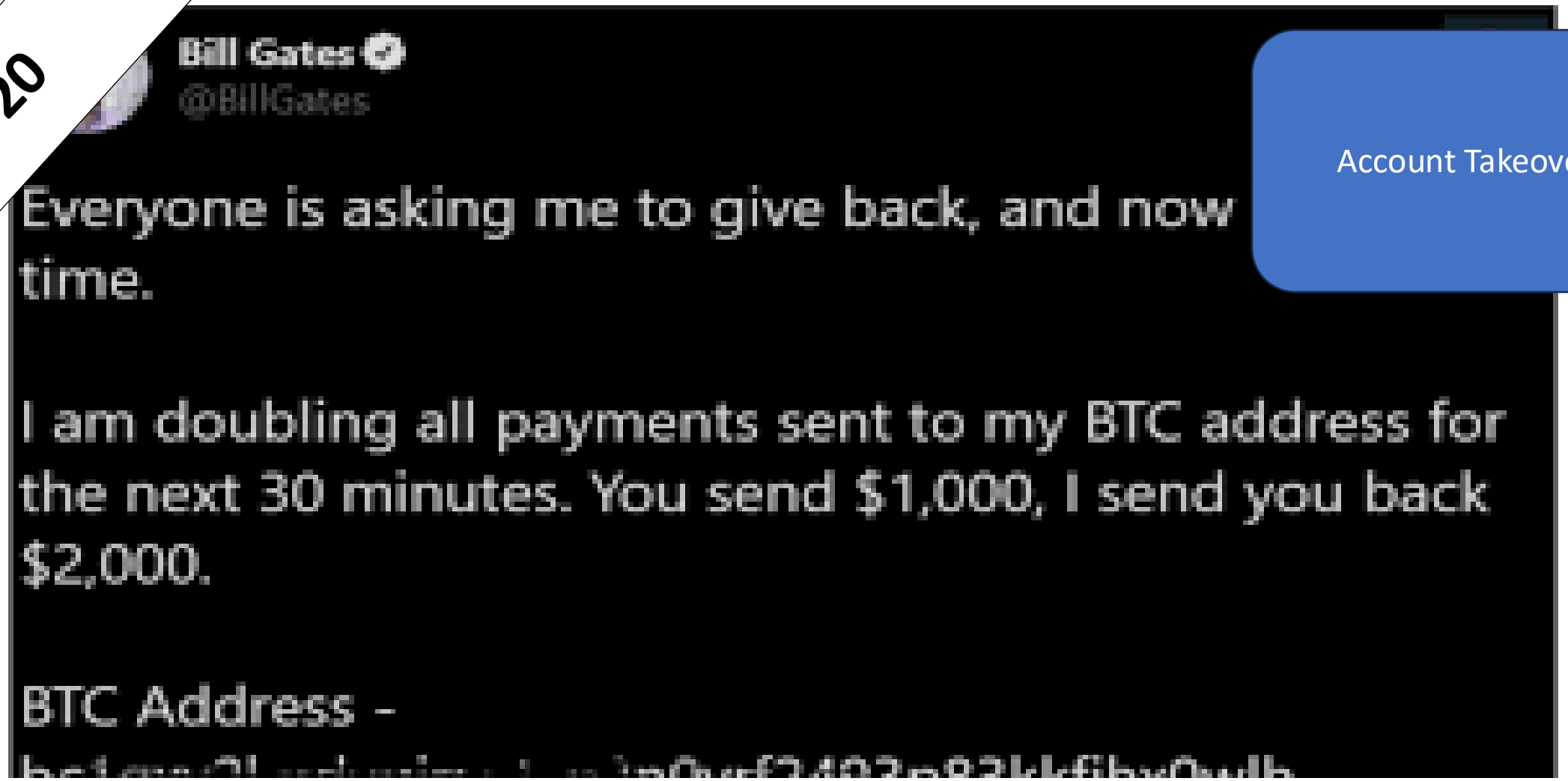


Twitter Account Takeover (ATO) Breach

- Too many team members had access to account information
- Fake Tweets sent out from prominent accounts (e.g., politicians, etc.)
- Some bitcoin sent to two twenty-somethings (Florida and Canada)

Jul 2020

Account Takeover



Twitter Account Takeover (ATO) Breach

- Too many team members had access to account information
- Fake Tweets sent out from prominent accounts (e.g., politicians, etc.)
- Some bitcoin sent to two twenty-somethings (Florida and Canada)

Jul 2020

Edward Amoroso posted this

Why I Don't Support Mudge's Decision.

Edward Amoroso on LinkedIn

August 24, 2022

You and 441 others 288 comments

118,652 impressions View analytics

SolarWinds Breach

- Nation-State (Russian) Advanced Persistent Threat (APT)
- Malicious code injection – target supply chain to users
- Massive number of victims in the US Federal Government

SolarWinds Breach

- Nation-State (Russian) Advanced Persistent Threat (APT)
- Malicious code injection – target supply chain to users
- Massive number of victims in the US Federal Government

Colonial Pipeline Attack

- Ransomware attack to Northeastern US pipeline delivery
- Nation-state involvement likely – company paid ransomware
- More serious implications if attacker had been more destructive

May 2021

OT Security

Colonial Pipeline Attack

- Ransomware attack to Northeastern US pipeline delivery
- Nation-state involvement likely – company paid ransomware
- More serious implications if attacker had been more destructive

Dec 2021

Apache Log4j 2

Apache Log4j 2 is an upgrade to Log4j that provides significant improvements over its predecessor, Log4j 1.x, and provides many of the improvements available in Logback while fixing some inherent problems in Logback's architecture.

Important: Security Vulnerability CVE-2021-44832

Summary: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration.

Details

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

Mitigation

Upgrade to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later)

Log4J Vulnerability

- 1.8 million probes against half of corporate networks launched in December 2021
- Evidence of nation-state involvements using 70 malware families
- Actual impact is unknown so far (stay tuned)

Dec 2021

Vulnerability Management

Apache Log4j 2

Apache Log4j 2 is an upgrade to Log4j that provides significant improvements over its predecessor, Log
improvements available in Logback while fixing some inherent problems in Logback's architecture.

Important: Security Vulnerability CVE-2021-44832

Summary: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration.

Details

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

Mitigation

Upgrade to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later)

Log4J Vulnerability

- 1.8 million probes against half of corporate networks launched in December 2021
- Evidence of nation-state involvements using 70 malware families
- Actual impact is unknown so far (stay tuned)

Lapsus$ Rampage

- Teenager in the UK rampages Microsoft, Nvidia, and other major targets
- High-profile compromise of internal Microsoft DevOps account
- Ransomware demands (e.g., Nvidia make code open-source, etc.)

Lapsus$ Rampage

- Teenager in the UK rampages Microsoft, Nvidia, and other major targets
- High-profile compromise of internal Microsoft DevOps account
- Ransomware demands (e.g., Nvidia make code open-source, etc.)

Uber Breach

- Social engineering attack (fake IT call) to an Uber employee for password
- Teenager hacker gained access to entire Uber infrastructure from this access
- Follows 2016 attack (57 million accounts compromised)

Uber Breach

- Social engineering attack (fake IT call) to an Uber employee for password
- Teenager hacker gained access to entire Uber infrastructure from this access
- Follows 2016 attack (57 million accounts compromised)

Dec 2022

LastPass Loses Passwords to Hacker

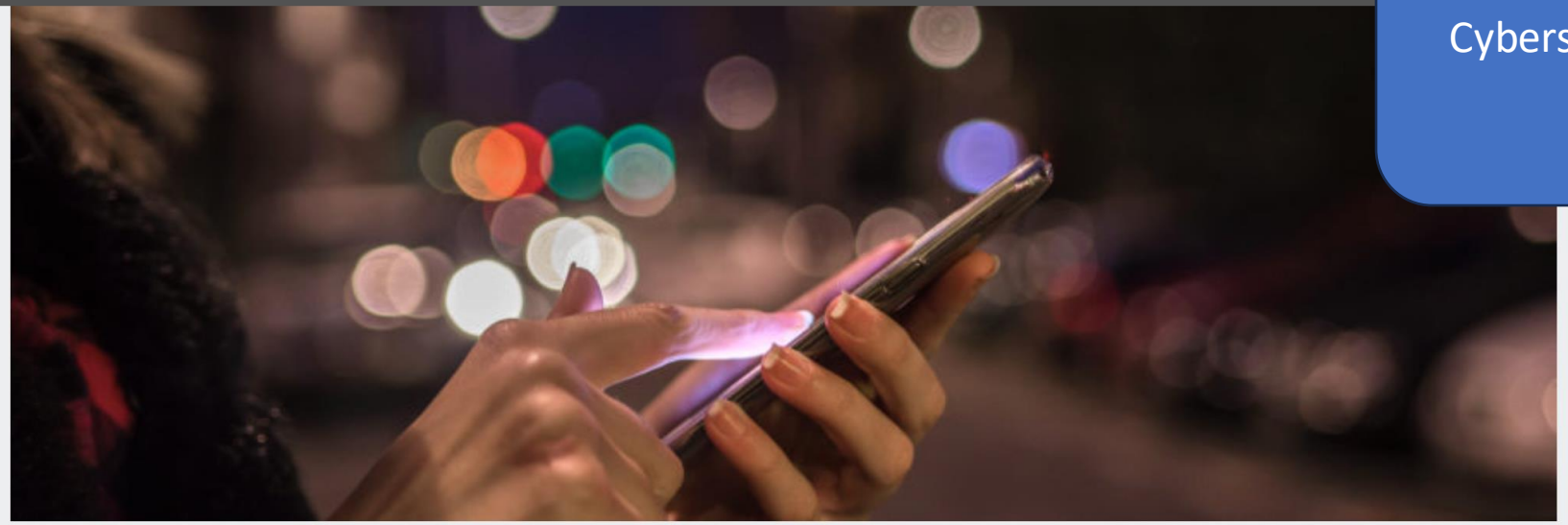
- Hacker gained access to LastPass trove of password information
- Hacker managed to decrypt and steal passwords (ugh)
- Issue calls into question safety of password managers

Dec 2022

Cybersecurity Vendor

LastPass ••• | PERSONAL BUSINESS SUPPORT ENGLISH Get LastPass Free

Blog > Product Updates > Notice of Recent Security Incident



Karim Toubba

December 22, 2022 | By Karim Toubba

Notice of Recent Security Incident

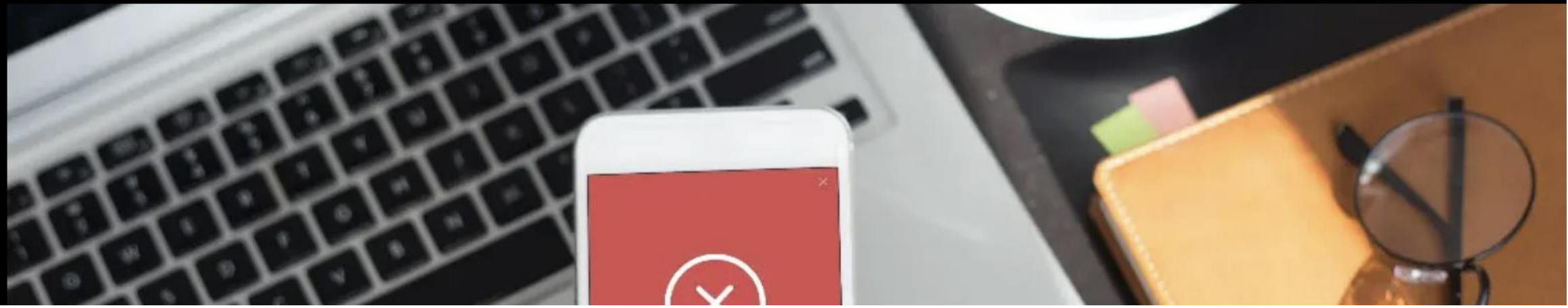
LastPass Loses Passwords to Hacker

- Hacker gained access to LastPass trove of password information
- Hacker managed to decrypt and steal passwords (ugh)
- Issue calls into question safety of password managers

May 2023

urity Intelligence

ChatGPT Confirms Data Breach, Raising Security Concerns



Initial Hack on ChatGPT

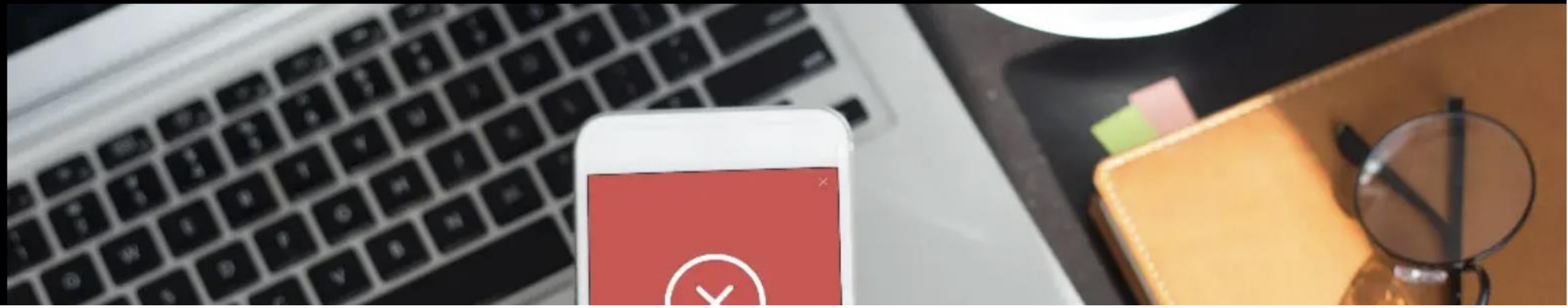
- Several initial (but seemingly minor) hacks on ChatGPT so far
- Given attention now to ChatGPT and OpenAI, should expect to see more
- Prediction: DDOS attacks on OpenAI will send many people into spasms

May 2023

urity Intelligence

ChatGPT Confirms Data B
Raising Security Concerns

AI



Initial Hack on ChatGPT

- Several initial (but seemingly minor) hacks on ChatGPT so far
- Given attention now to ChatGPT and OpenAI, should expect to see more
- Prediction: DDOS attacks on OpenAI will send many people into spasms

May 2023

Fake viral images of an explosion at the Pentagon were probably created by AI

May 22, 2023 · 6:19 PM ET

Shannon Bond

Deep Fake Image of Explosion on Twitter

- AI generated image shows fake explosion at the Pentagon
- Image begins to circulate on Twitter on Monday May 22, 2023
- Stock market takes immediately and real hit.

May 2023

Deep Fake Images

Fake viral images of an explosi
Pentagon were probably creat

May 22, 2023 · 6:19 PM ET

Shannon Bond

Deep Fake Image of Explosion on Twitter

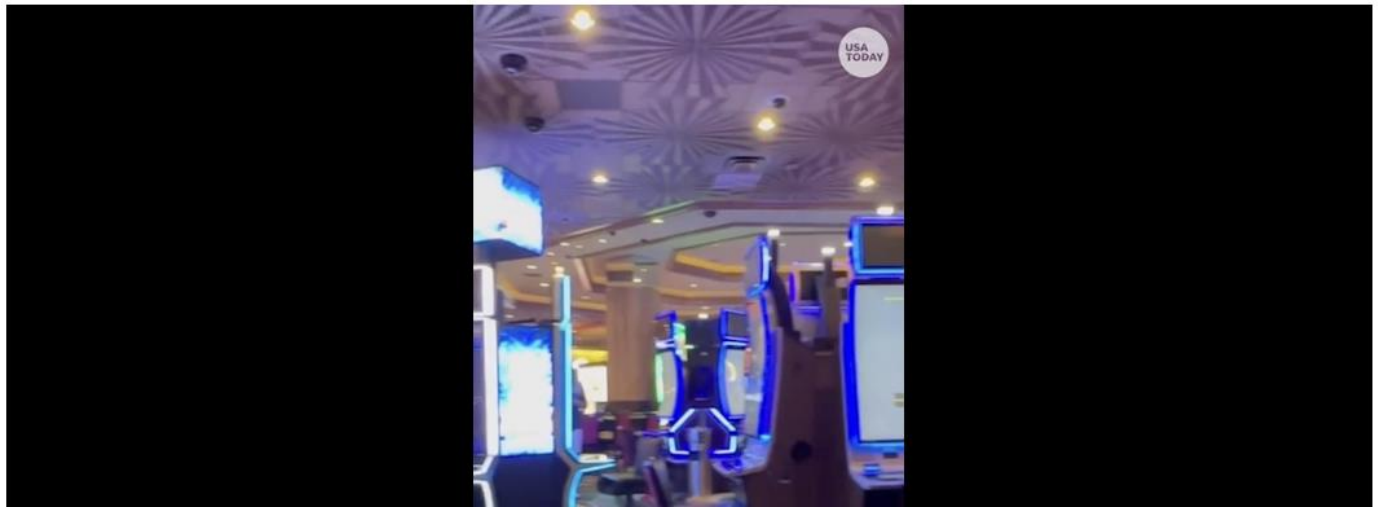
- AI generated image shows fake explosion at the Pentagon
- Image begins to circulate on Twitter on Monday May 22, 2023
- Stock market takes immediately and real hit.

Aug 2023

MGM Resorts properties in US shut down computer systems after cyber attack

Amaris Encinas USA TODAY

Published 8:02 p.m. ET Sept. 11, 2023 | **Updated 7:43 p.m. ET Sept. 13, 2023**



Cyber-Attack Degrades Operations at MGM

- Attack degrades operations at over a dozen MGM hotels and casinos
- Moody's reports that "attack appears to have material impact on MGM"
- Lateral movement implies wide attack span of control across MGM network

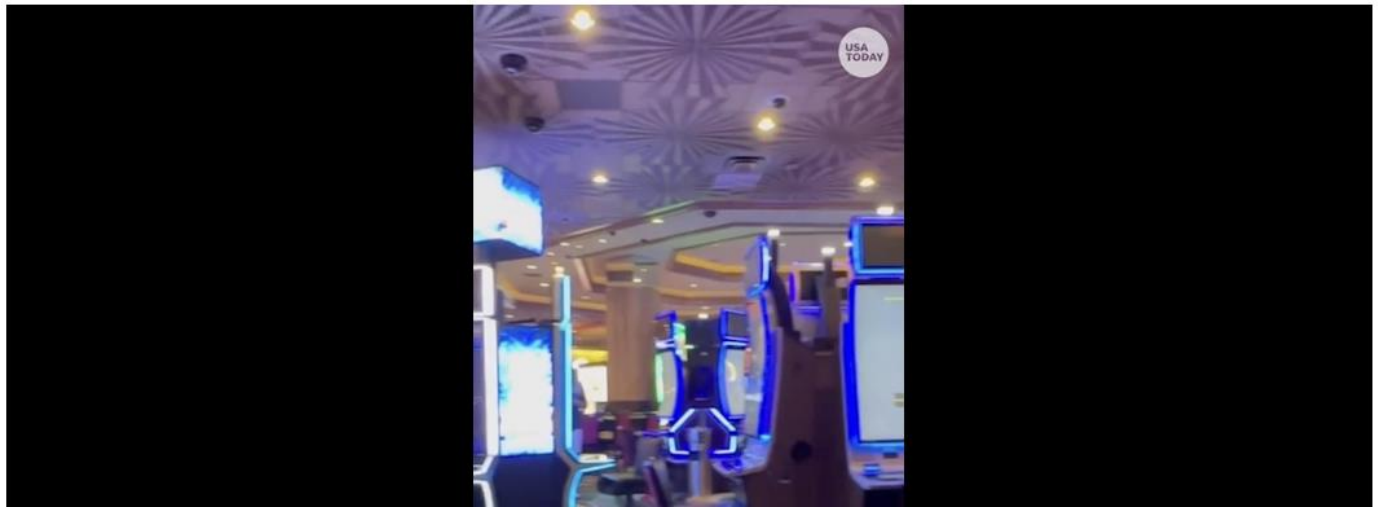
Aug 2023

Operational Shutdown

MGM Resorts properties in US shut down computer systems after cybe attack

Amaris Encinas USA TODAY

Published 8:02 p.m. ET Sept. 11, 2023 | **Updated 7:43 p.m. ET Sept. 13, 2023**



Cyber-Attack Degrades Operations at MGM

- Attack degrades operations at over a dozen MGM hotels and casinos
- Moody's reports that "attack appears to have material impact on MGM"
- Lateral movement implies wide attack span of control across MGM network

Dec 2023

Security

23andMe confirms hackers stole ancestry data on 6.9 million users

Lorenzo Franceschi-Bicchierai @lorenzofb / 12:56 PM EST • December 4, 2023 Comment

Hackers Bypass 2FA at 23andMe

- Attack *literally* steals NDA records of targets
- Highlights need for phishing-resistant multifactor authentication
- Be careful before you send your DNA to an on-line service

Dec 2023

Security

23andMe confirms hackers stole ancestry data on 6.9 million users

Lorenzo Franceschi-Bicchierai @lorenzofb / 12:56 PM EST • December 4, 2023

Comment

2FA Attack

Hackers Bypass 2FA at 23andMe

- Attack *literally* steals NDA records of targets
- Highlights need for phishing-resistant multifactor authentication
- Be careful before you send your DNA to an on-line service

Jan 2024

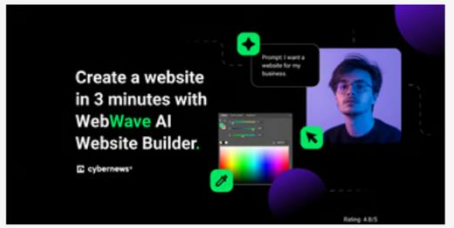
Mother of all breaches reveals 26 billion records: what we know so far

Updated on: January 29, 2024 10:07 AM 3

Vilius Petkauskas, Deputy Editor

Image by Cybernews.

Partner content



AI-powered WebWave: revolutionizing small business websites

by Cybernews Team 16 April 2024

Editor's choice

Massive Hack of Many Platforms

- Data from numerous breaches
- 12TB and 26 billion records from LinkedIn, Twitter, Weibo, Tencent
- Largest data breach ever recorded

Jan 2024

Aggregated Attack

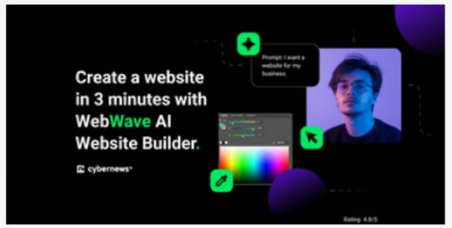
Mother of all breaches reveals 26 billion records: what we k so far

Updated on: January 29, 2024 10:07 AM 3

Vilius Petkauskas, Deputy Editor

Image by Cybernews.

Partner content



AI-powered WebWave: revolutionizing small business websites

by Cybernews Team 16 April 2024

Editor's choice

Massive Hack of Many Platforms

- Data from numerous breaches
- 12TB and 26 billion records from LinkedIn, Twitter, Weibo, Tencent
- Largest data breach ever recorded

Feb 2024

SUSTAINABILITY

Change Healthcare cyberattack

UPDATED MAY 20, 2024 • 13 MIN READ

Massive Ransomware Attack to UnitedHealth Group

- Impacts rippled through the health care insurance industry
- Company forced to shut down operations in response to attack
- Weak or non-existent MFA included as a root case

Feb 2024

MFA Weaknesses

SUSTAINABILITY

Change Healthcare cyberattack

UPDATED MAY 20, 2024 • 13 MIN READ

Massive Ransomware Attack to UnitedHealth Group

- Impacts rippled through the health care insurance industry
- Company forced to shut down operations in response to attack
- Weak or non-existent MFA included as a root case

Mar 2024

DALLAS, March 30, 2024

AT&T Addresses Recent Data Set Released on the Dark Web

AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web; source is still being assessed.

share

Download assets

Subscribe to AT&T News

Hackers Cryptanalyze AT&T Data

- Incident had previously been identified but controlled via encryption
- Evidence surfaced that data had finally been cryptanalyzed
- Illustrates the “store-now-decrypt-later” threat to data

Mar 2024

Cryptanalysis

DALLAS, March 30, 2024

AT&T Addresses Recent Data Set Released on the Dark Web

AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web; source is still being assessed.

share

Download assets

Subscribe to AT&T News

Hackers Cryptanalyze AT&T Data

- Incident had previously been identified but controlled via encryption
- Evidence surfaced that data had finally been cryptanalyzed
- Illustrates the “store-now-decrypt-later” threat to data

Aug 2024

Nation-State Targets Presidential Candidate

- Murky details on this presumed attack by a nation-state on Trump campaign
- Lack of confidence in anything reported by Trump cloud confidence here
- FBI reports that this is part of an on-going attack at both US parties

Aug 2024

Political Sabotage

NBC NEWS POLITICS U.S. NEWS WORLD BUSINESS HEALTH SPORTS SHOPPING TIPLINE CULTURE & TRENDS

SECURITY

U.S. confirms Trump campaign claim it was breached by Iranian hackers

The FBI, the Cybersecurity and Infrastructure Security Agency and the Office of the Director of National Intelligence said Iran was behind attempts this year to hack the presidential campaigns of both political parties.

Nation-State Targets Presidential Candidate

- Murky details on this presumed attack by a nation-state on Trump campaign
- Lack of confidence in anything reported by Trump cloud confidence here
- FBI reports that this is part of an on-going attack at both US parties

Dec 2024

Not too
Make a yea
Support us →
nd our journalism
Print subscriptions | Newsletters | Sign in

The Guardian
US

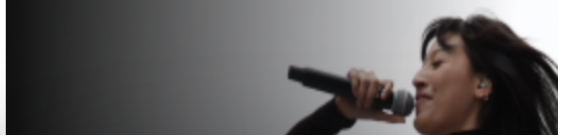
Opinion | Sport | Culture | Lifestyle

US politics | World | Climate crisis | Middle East | Ukraine | Soccer | Business | Environment | Tech | Science | Newsletters | Wellness

US news

Chinese hackers breach US treasury network, gain access to some files

Third-party cybersecurity provider was compromised after hackers obtained key to override certain systems



U.S. Treasury Compromised by BeyondTrust Hack

- Unclear what information was stolen by nation-state actor
- Root cause seems to be a third-party security company called BeyondTrust
- Tough when the security tool is the source of breach

Dec 2024

Hacked Security Tool

Not too
Make a yea
Support us
nd our journalism
Print subscriptions
Newsletters
Sign in

Opinion | Sport | Culture | Lifestyle

US politics World Climate crisis Middle East Ukraine Soccer Business Environment Tech Science Newsletters Wellness

US news

Chinese hackers breach US treasury network, gain access to some files

Third-party cybersecurity provider was compromised after hackers obtained key to override certain systems

U.S. Treasury Compromised by BeyondTrust Hack

- Unclear what information was stolen by nation-state actor
- Root cause seems to be a third-party security company called BeyondTrust
- Tough when the security tool is the source of breach

We just covered:

Third-party breach. Password Problems, Dwell Time, Security Budget, Destructive attack, Insurance Records, Class Action Lawsuits, CISO Salaries, Advanced Persistent Threats (APTs), Bad Response, Blame Others, Bad Account Inventory, Attempt to Kill, Public Data Aggregation, Selling Stolen Data, Compliance Issue, Legacy System, DDOS, Fake News, Ransomware, Open Source, International, Bug Bounty, Big Data, Massive Attack, Cloud Security, Security Metrics, Work from Home, Account Takeover, Software Supply Chain, OT Security, Vulnerability Management, Hacking Groups, Mobile Apps, Cybersecurity Vendor, AI, Deep Fake Images, Operational Shutdown, 2FA Attack, Aggregated Attack, Cryptanalysis, Political Sabotage, . . .

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.
3. Also create a description of how each attack could have been prevented from occurring.

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.
3. Also create a description of how each attack could have been prevented from occurring.
4. Write **forty-eight** (48) PowerPoint charts showing

    (a) 24 attack scenarios and their predicted date in next two years.

    (b) 24 descriptions of how the attack could have avoided

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.
3. Also create a description of how each attack could have been prevented from occurring.
4. Write **forty-eight** (48) PowerPoint charts showing

    (a) 24 attack scenarios and their predicted date in next two years.

    (b) 24 descriptions of how the attack could have avoided
5. I will grade you on your creativity, originality and your ability to describe realistic attacks into the future.

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.
3. Also create a description of how each attack could have been prevented from occurring.
4. Write **forty-eight** (48) PowerPoint charts showing

    (a) 24 attack scenarios and their predicted date in next two years.

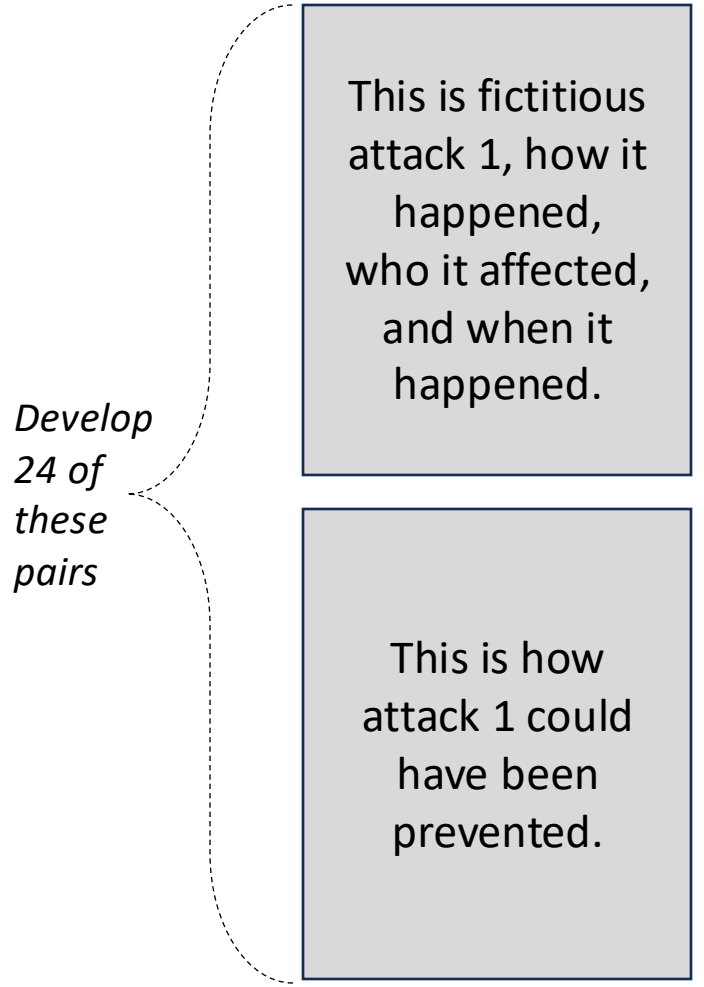
    (b) 24 descriptions of how the attack could have avoided
5. I will grade you on your creativity, originality and your ability to describe realistic attacks into the future.
6. I also know what and how ChatGPT generates output – so an obvious ChatGPT-oriented answer will receive a grade of C.

Your Midterm Examination

1. Pick **twenty-four** (24) specific companies or organizations that are reasonably well-known (make sure they are real).
2. Create a fictitious description of an attack that you predict could happen to each organization.
3. Also create a description of how each attack could have been prevented from occurring.
4. Write **forty-eight** (48) PowerPoint charts showing

   (a) 24 attack scenarios and their predicted date in next two years.

   (b) 24 descriptions of how the attack could have avoided.
5. I will grade you on your creativity, originality and your ability to describe realistic attacks into the future.
6. I also know what and how ChatGPT generates output – so an obvious ChatGPT-oriented answer will receive a grade of C.



Why Do These Hacks Continue to Happen?

For small, simple things:
I know how they work.
I don't know what they do.

It is easy to protect these
things from hacking or tampering.

For large, complex things:
I know what they do.
I don't know how they work.

It is difficult to protect these
things from hacking or tampering.

What Can Cybersecurity Learn from Bank Robberies?


R3
5437
(1931)
K5440

Foot activated hold-up station Robby

Foot activated hold-up station

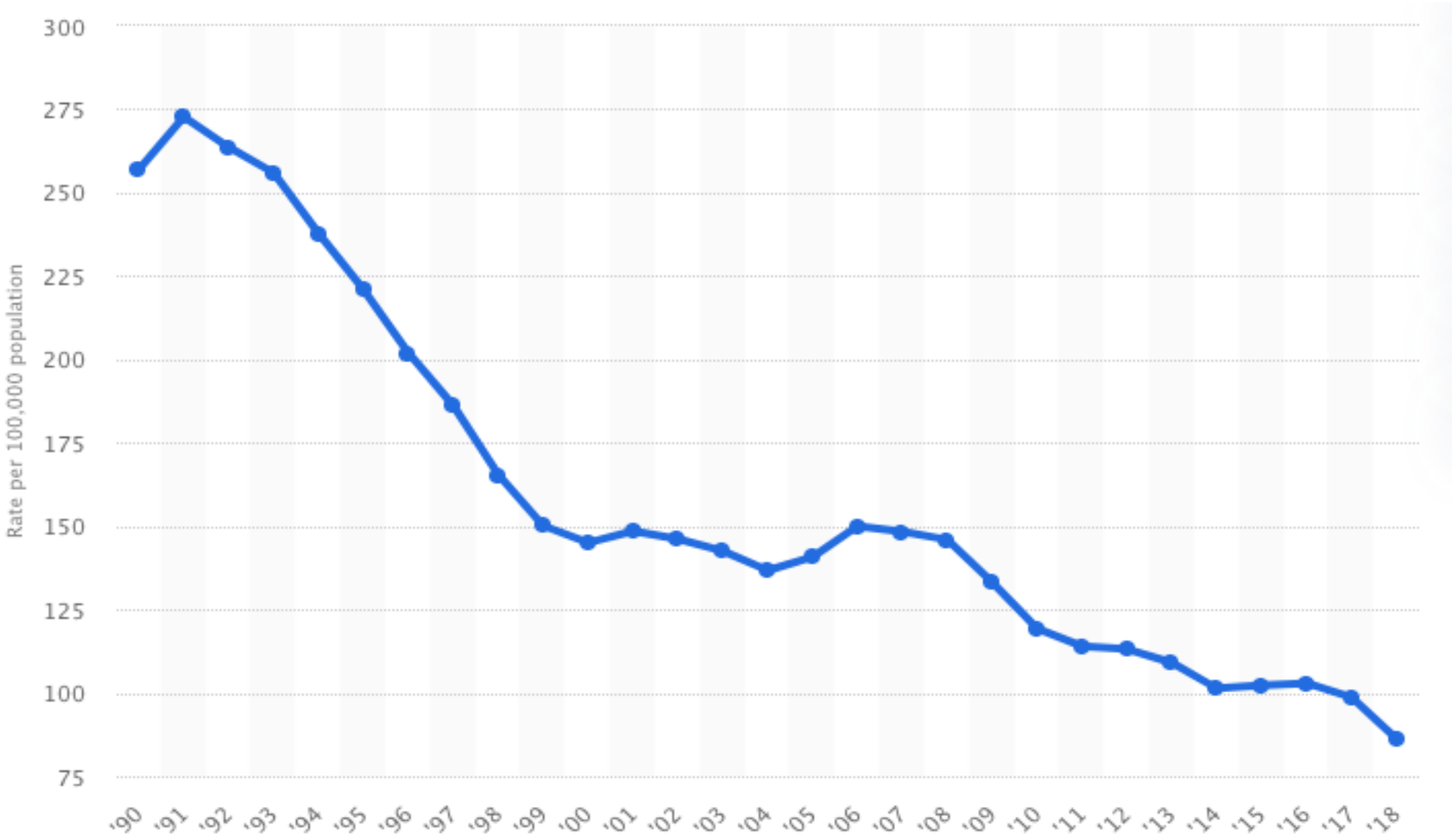
Reliable easy to operate foot activated hold-up device
Operated by lifting the foot tip
Foot activated robbery & panic station
Foot activated hod-up station with rugged metal housing
Designed to minimize the possibility of false alarms
Foot operated panic and robbery station
Designed for high-end security applications
Foot activated panic station for distress Alarm System (DAS)
Applicable for bank branches, diamonds & jewelry shops
Foot activated hold-up station used in banks and change kiosks
Send silent alarm to local or remote security center

SKU: Robby_TGL, Robby_TGO

Add to RFQ

1

Societal Goal for Hacking: Robbery Rate in the US



Long-Term Goal for Cybersecurity

To reduce the risk of cyber threats to the point where they no longer represent a significant and present danger to society (like bank robberies).