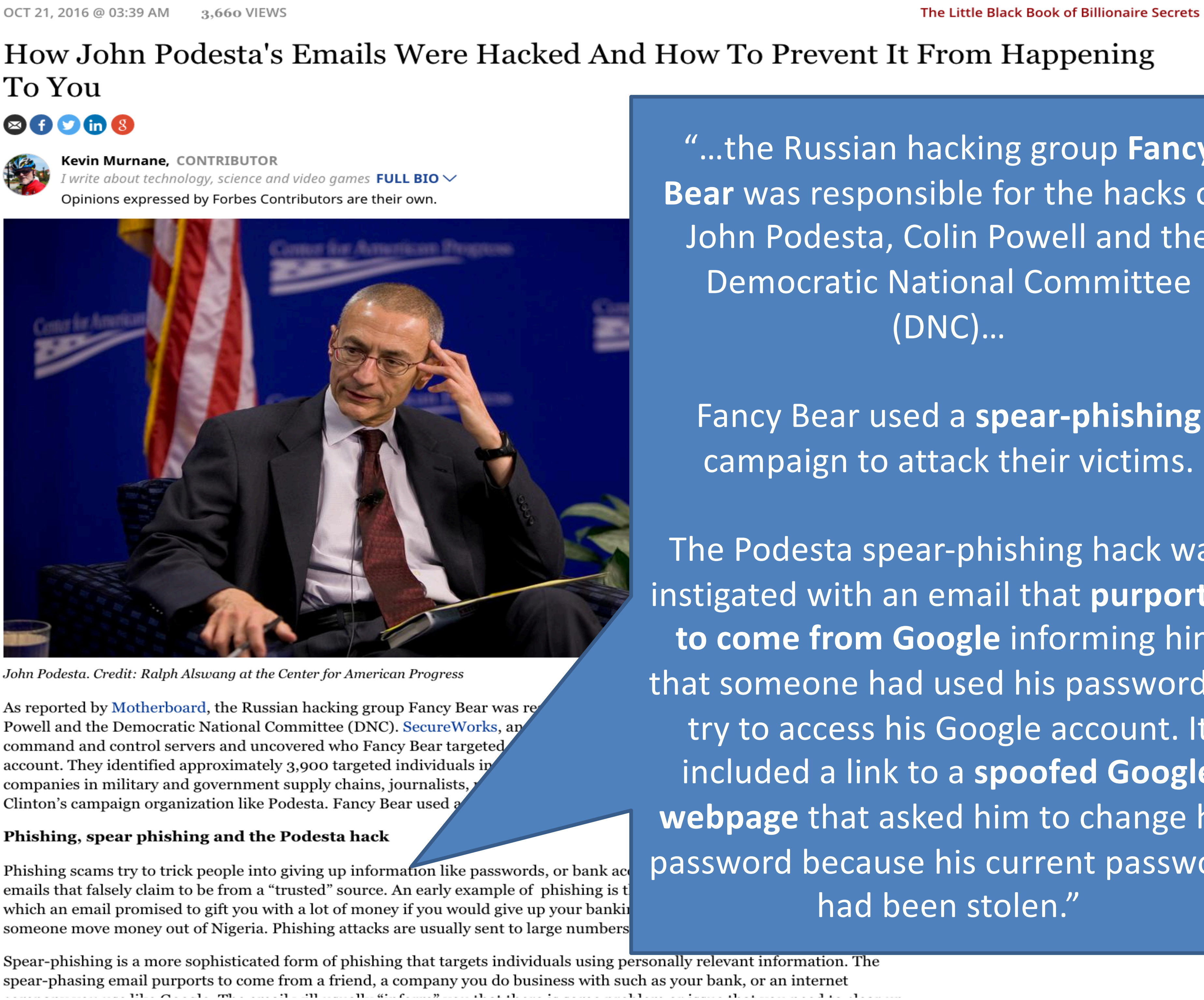
Philanthropy southwest

The World Wide Web: Facing the Cyber Threat

John Ansbach, CIPP/US
General Counsel
General Datatech, L.P.

#2016PSWAC
@johnansbach

Center for American Progress
Center for American
Center for American



OCT 21, 2016 @ 03:39 AM 3,660 VIEWS

The Little Black Book of Billionaire Secrets

How John Podesta's Emails Were Hacked And How To Prevent It From Happening To You

Kevin Murnane, CONTRIBUTOR

I write about technology, science and video games FULL BIO

Opinions expressed by Forbes Contributors are their own.

John Podesta. Credit: Ralph Alswang at the Center for American Progress

As reported by Motherboard, the Russian hacking group Fancy Bear was re
Powell and the Democratic National Committee (DNC). SecureWorks, an
command and control servers and uncovered who Fancy Bear targeted
account. They identified approximately 3,900 targeted individuals in
companies in military and government supply chains, journalists,
Clinton's campaign organization like Podesta. Fancy Bear used a

Phishing, spear phishing and the Podesta hack

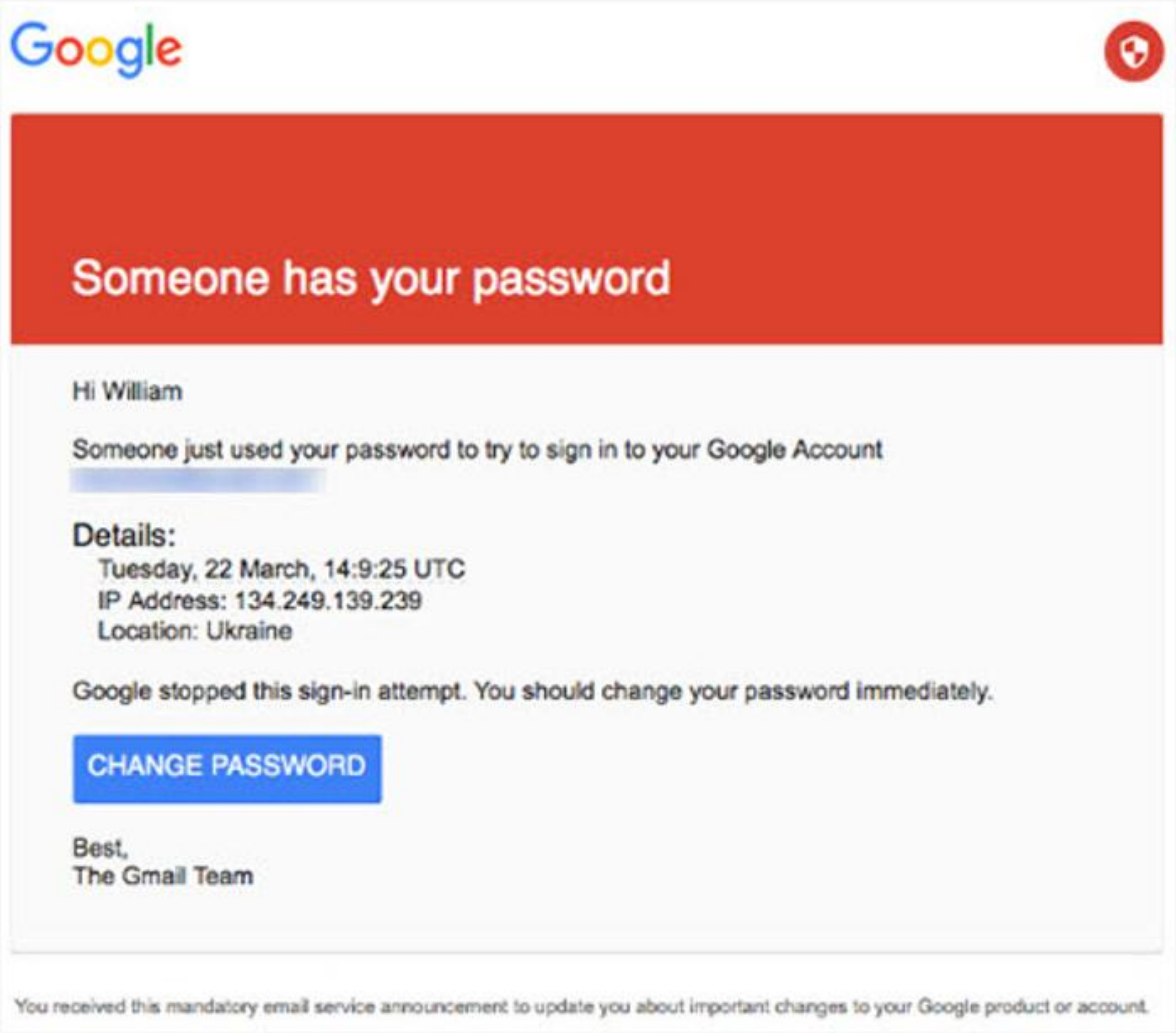
Phishing scams try to trick people into giving up information like passwords, or bank acc
emails that falsely claim to be from a "trusted" source. An early example of phishing is t
which an email promised to gift you with a lot of money if you would give up your bankin
someone move money out of Nigeria. Phishing attacks are usually sent to large numbers

Spear-phishing is a more sophisticated form of phishing that targets individuals using personally relevant information. The spear-phasing email purports to come from a friend, a company you do business with such as your bank, or an internet

"…the Russian hacking group **Fancy Bear** was responsible for the hacks on John Podesta, Colin Powell and the Democratic National Committee (DNC)…

Fancy Bear used a **spear-phishing** campaign to attack their victims.

The Podesta spear-phishing hack was instigated with an email that **purported to come from Google** informing him that someone had used his password to try to access his Google account. It included a link to a **spoofed Google webpage** that asked him to change his password because his current password had been stolen."



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]

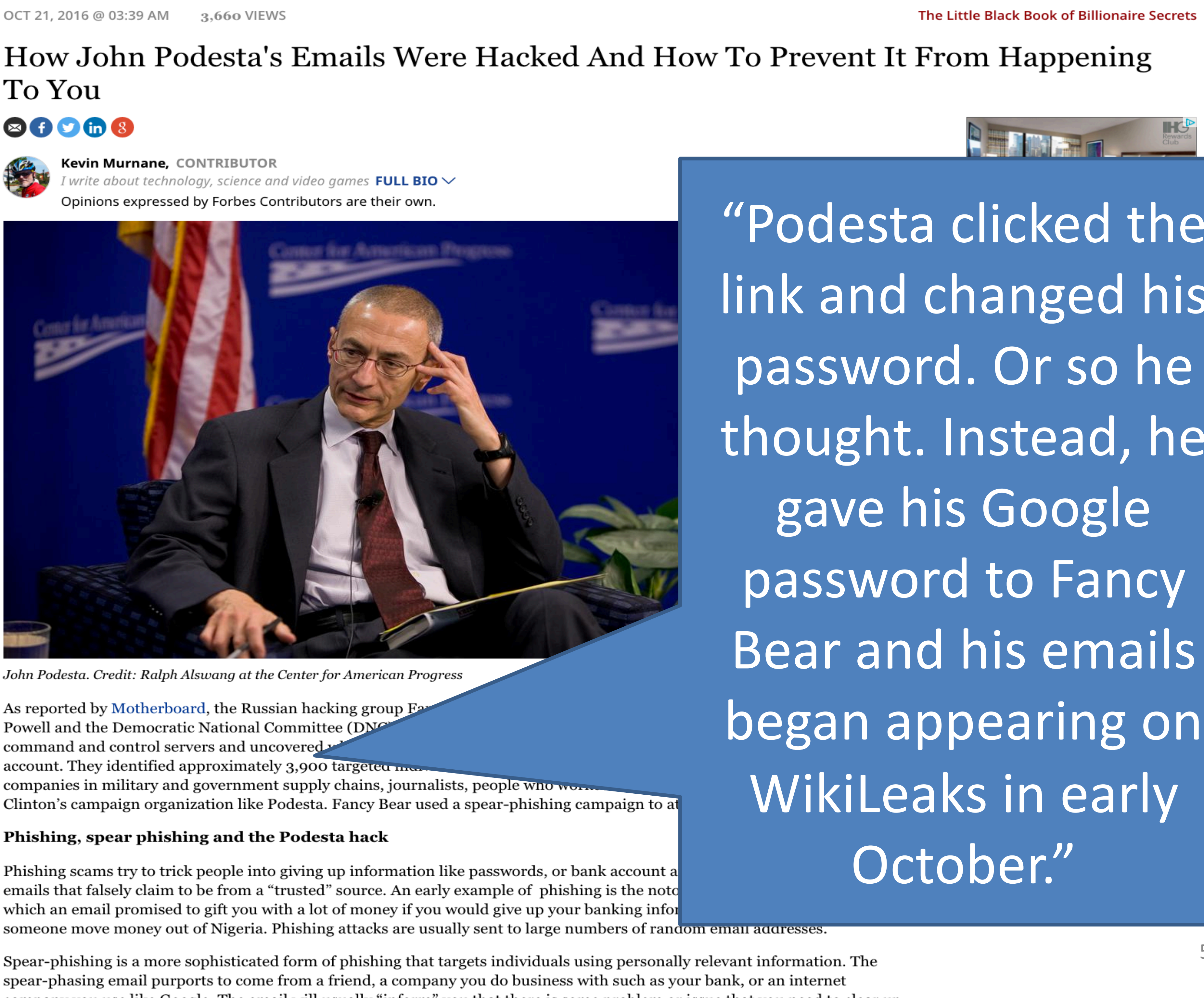
Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

A screenshot of the phishing email received by Rinehart. (Image: The Smoking Gun)



OCT 21, 2016 @ 03:39 AM 3,660 VIEWS

The Little Black Book of Billionaire Secrets

How John Podesta's Emails Were Hacked And How To Prevent It From Happening To You

Kevin Murnane, CONTRIBUTOR

I write about technology, science and video games FULL BIO

Opinions expressed by Forbes Contributors are their own.

John Podesta. Credit: Ralph Alswang at the Center for American Progress

As reported by Motherboard, the Russian hacking group Fa
Powell and the Democratic National Committee (DNC
command and control servers and uncovered w
account. They identified approximately 3,900 targeted ind
companies in military and government supply chains, journalists, people who work
Clinton's campaign organization like Podesta. Fancy Bear used a spear-phishing campaign to at

Phishing, spear phishing and the Podesta hack

Phishing scams try to trick people into giving up information like passwords, or bank account a
emails that falsely claim to be from a "trusted" source. An early example of phishing is the noto
which an email promised to gift you with a lot of money if you would give up your banking infor
someone move money out of Nigeria. Phishing attacks are usually sent to large numbers of random email addresses.

Spear-phishing is a more sophisticated form of phishing that targets individuals using personally relevant information. The spear-phasing email purports to come from a friend, a company you do business with such as your bank, or an internet company you use like Google. The email will usually "inform" you that there is some problem or issue that you need to clear up

"Podesta clicked the link and changed his password. Or so he thought. Instead, he gave his Google password to Fancy Bear and his emails began appearing on WikiLeaks in early October."

SECTIONS SEARCH

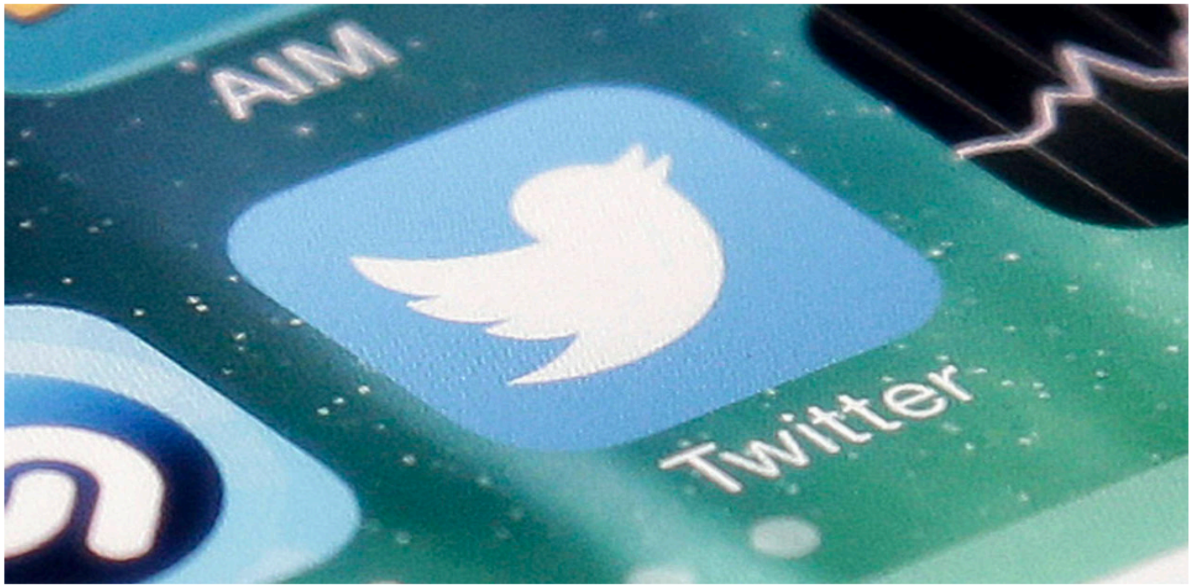
Los Angeles Times

SUBSCRIBE Sale: 49¢/week LOG IN

WEDNESDAY OCT. 26, 2016 MOST POPULAR LOCAL SPORTS ENTERTAINMENT POLITICS ORANGE COUNTY OPINION PLACE AN AD ☼ 68°

BUSINESS

A massive cyberattack blocked your favorite websites; FBI and Homeland Security are investigating



Twitter is among the websites affected by a cyberattack. Above, the icon for the firm's smartphone app in 2013. (Marcio Jose Sanchez / Associated Press)

ALL-NEW
WOLVERINE
DURASHOCKS
ABSORBS SHOCK. RETURNS ENERGY.
FREE EXPRESS SHIPPING ▶ SHOP NOW

By Samantha Masunaga • Contact Reporter

OCTOBER 21, 2016, 3:40 PM

The Department of Homeland Security and the FBI are investigating a massive cyberattack that stopped or slowed access to Twitter, Spotify, Amazon and other sites Friday by targeting a firm responsible for routing Internet traffic their way.

In Case You Missed It

An aide says he once arranged for $50 million in payments for Bill Clinton

3:05 PM

'El Chapo' says he's depressed by prison life, complains of 'psychological torture'

2:05 PM

Someone took a sledgehammer to Donald Trump's Walk of Fame star

1:15 PM

These 2 recent incidents alone…

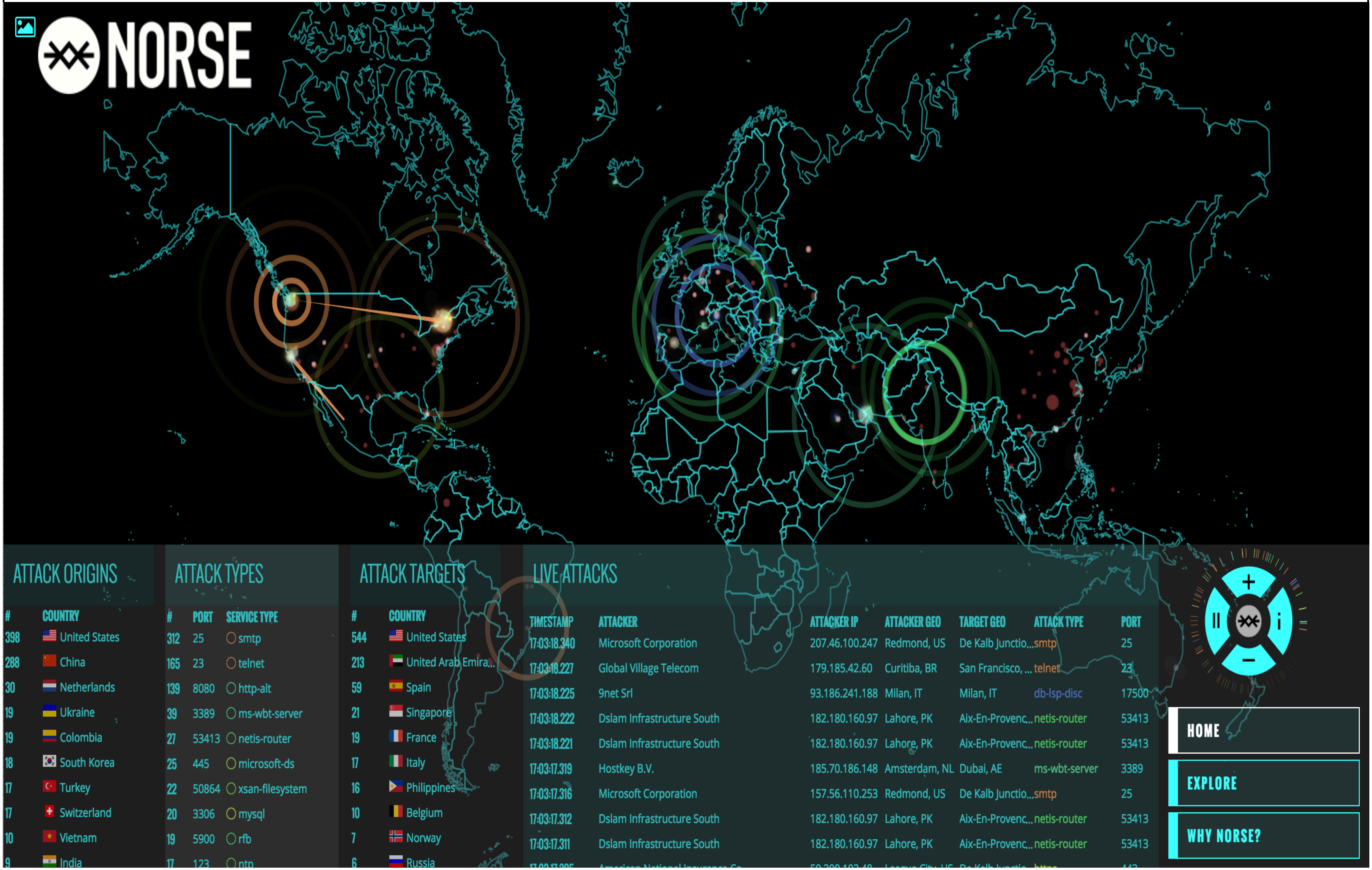
- Embarrassment to principal
- Embarrassment to principal's clients, friends, colleagues, partners, etc.
- Compromise of principal's data, as well as principal's client data, potentially including personal information (email addresses, etc.)
- Business disruption, inability to operate

Imagine what could be done to you and your organization in similar attacks…?

Agenda

- Landscape
- Threats
- Defenses (technical and non-technical)
- Tips & Takeaways

Landscape



ATTACK ORIGINS

#	COUNTRY
398	United States
288	China
30	Netherlands
19	Ukraine
19	Colombia
18	South Korea
17	Turkey
17	Switzerland
10	Vietnam
9	India

ATTACK TYPES

#	PORT	SERVICE TYPE
312	25	○ smtp
165	23	○ telnet
139	8080	○ http-alt
39	3389	○ ms-wbt-server
27	53413	○ netis-router
25	445	○ microsoft-ds
22	50864	○ xsan-filesystem
20	3306	○ mysql
19	5900	○ rfb
17	123	○ ntp

ATTACK TARGETS

#	COUNTRY
544	United States
213	United Arab Emira...
59	Spain
21	Singapore
19	France
17	Italy
16	Philippines
10	Belgium
7	Norway
6	Russia

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
17:03:18.340	Microsoft Corporation	207.46.100.247	Redmond, US	De Kalb Junctio...	smtp	25
17:03:18.227	Global Village Telecom	179.185.42.60	Curitiba, BR	San Francisco, ...	telnet	23
17:03:18.225	9net Srl	93.186.241.188	Milan, IT	Milan, IT	db-lsp-disc	17500
17:03:18.222	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
17:03:18.221	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
17:03:17.319	Hostkey B.V.	185.70.186.148	Amsterdam, NL	Dubai, AE	ms-wbt-server	3389
17:03:17.316	Microsoft Corporation	157.56.110.253	Redmond, US	De Kalb Junctio...	smtp	25
17:03:17.312	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
17:03:17.311	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
17:03:17.295	American National Insurance Co.	50.200.103.48	League City, US	De Kalb Junctio...	https	443

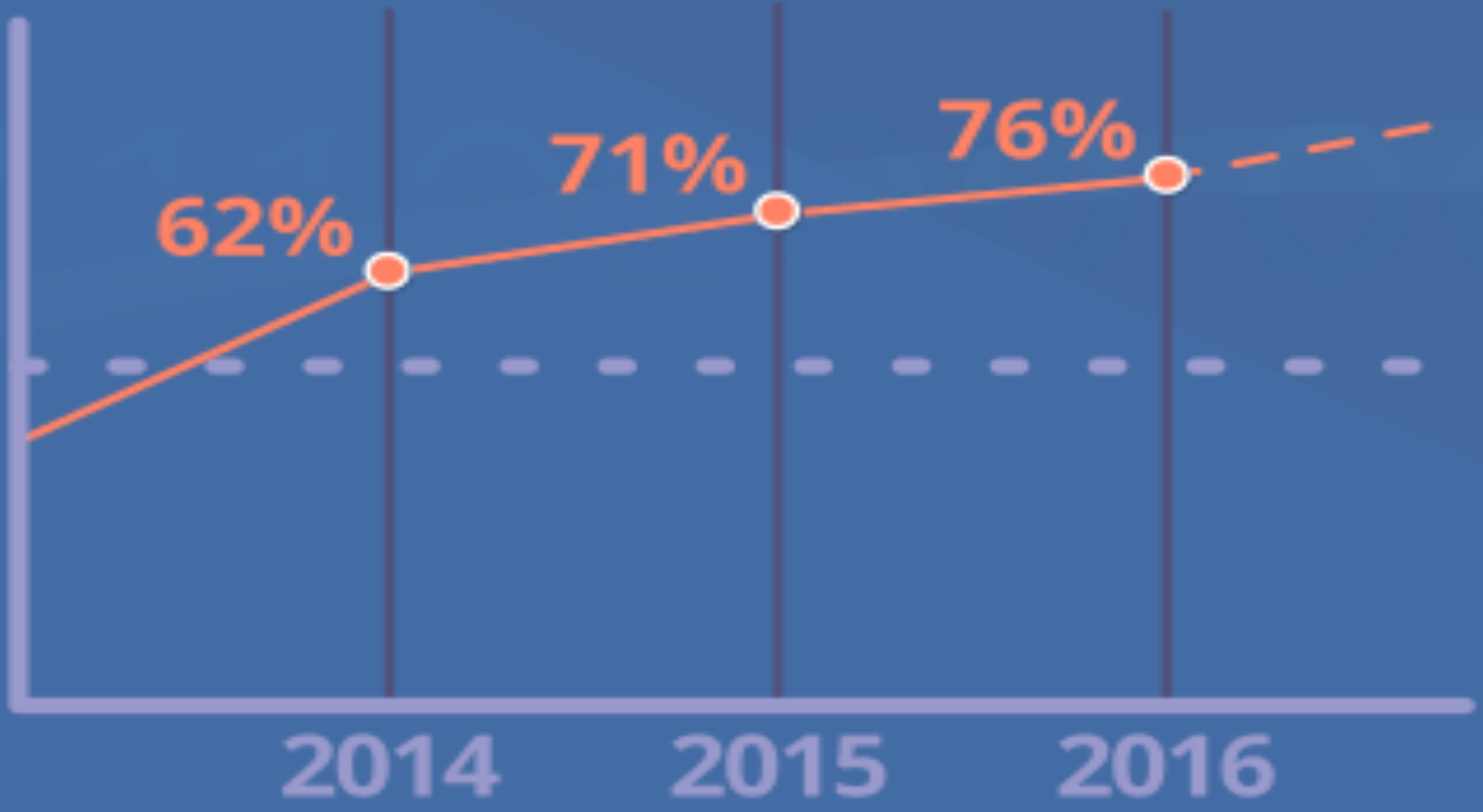
OVER

70%

of organizations report having been compromised by a **successful cyberattack** in the past 12 months.

RISING CYBERATTACKS

The percentage of respondents affected by successful attacks is rising each year.



Source: CyberEdge Group 2016

Annual number of data breaches and exposed records in the United States from 2005 to 2014 (in millions)

The statistic presents the development of cyber attacks over time. It presents the recorded number of data breaches and records exposed in the United States between 2005 and 2014. In 2014, the number of data breaches in the United States amounted to 783 with more than 85.61 million records exposed.

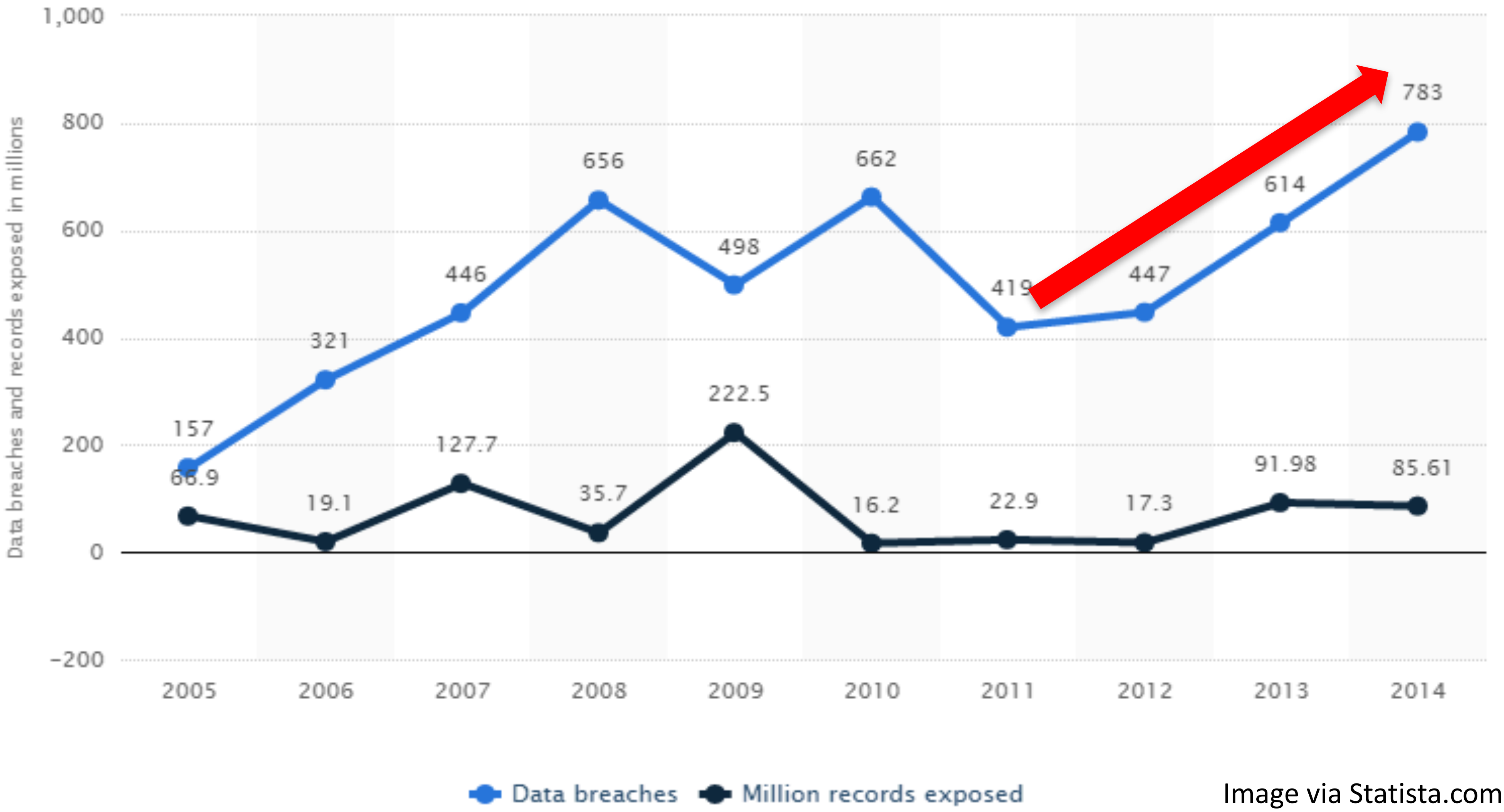
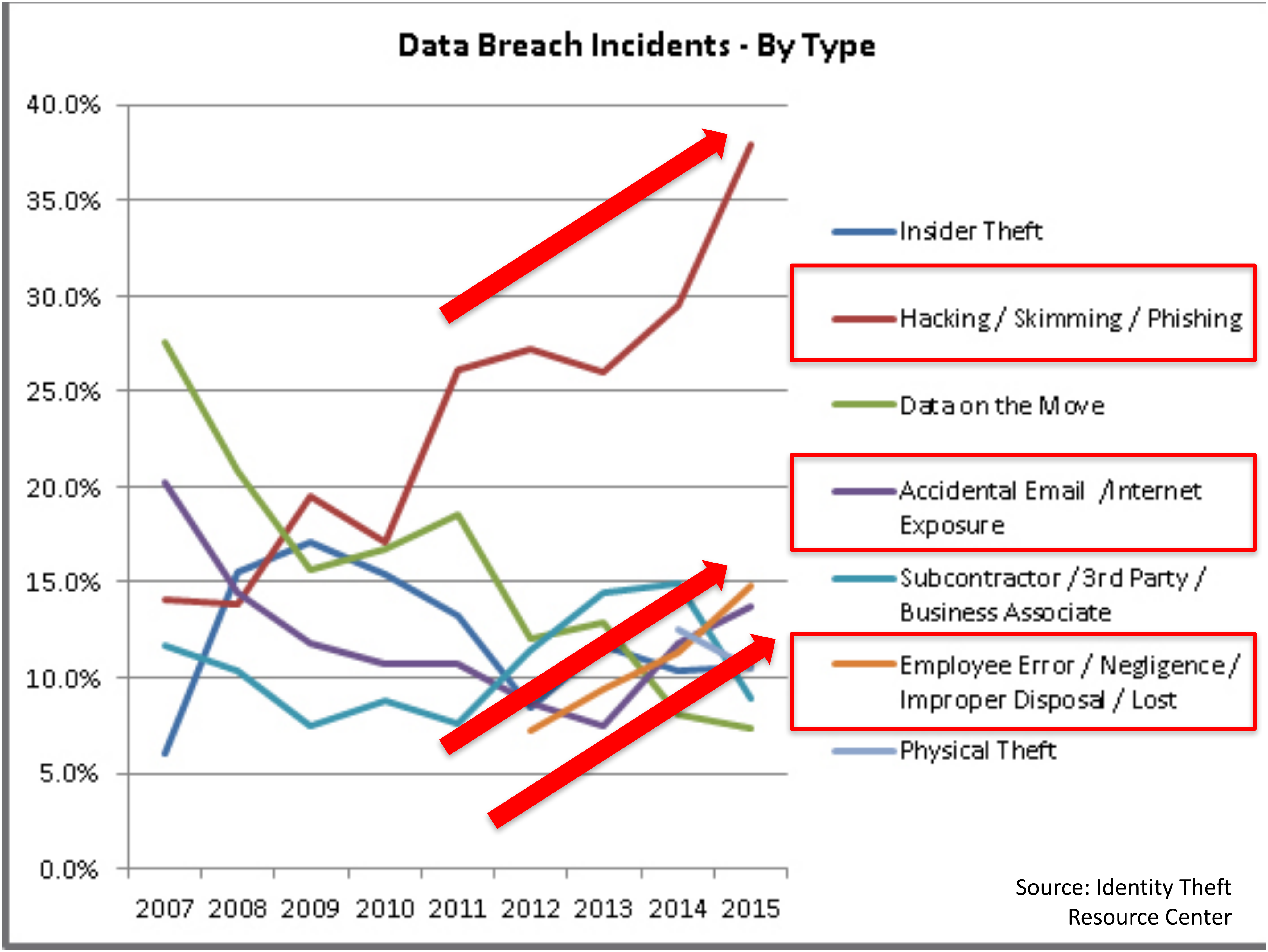


Image via Statista.com.



Source: Identity Theft Resource Center

World's Biggest Data Breaches

Selected losses greater than 30,000 records

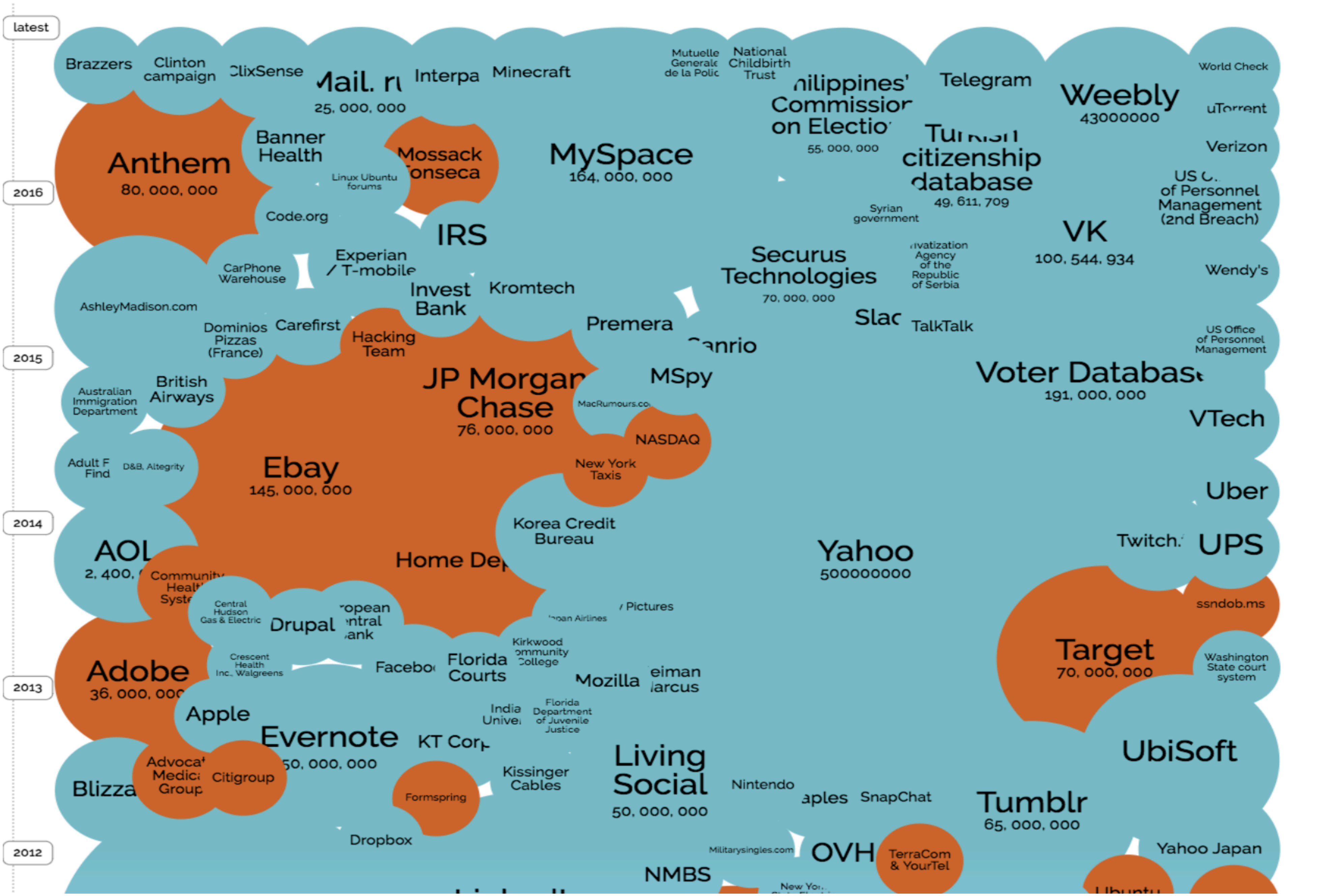
(updated 15th Oct 2016)

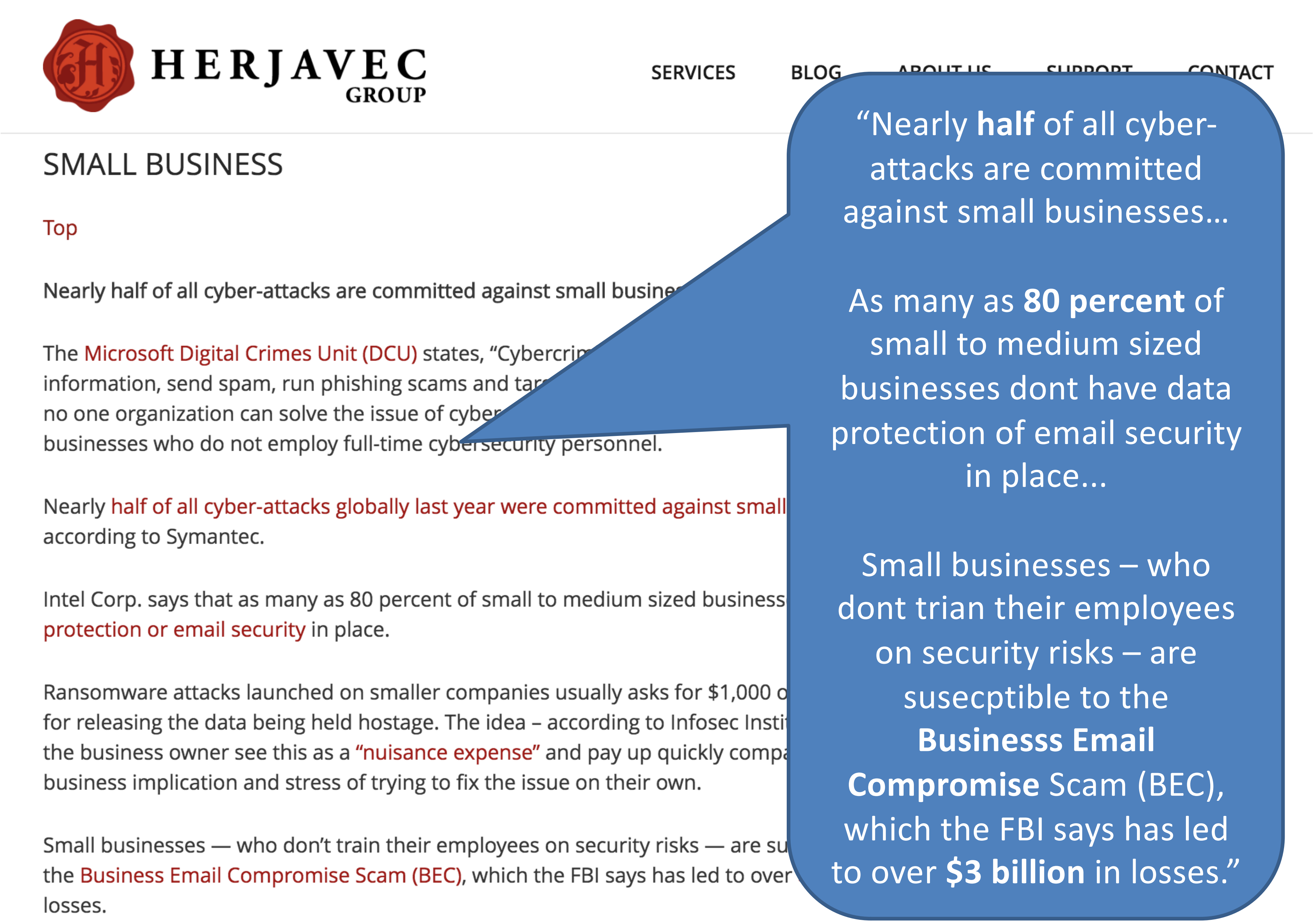
● interesting story

YEAR

BUBBLE COLOUR YEAR | METHOD OF LEAK *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY

□ SHOW FILTER





SMALL BUSINESS

Top

Nearly half of all cyber-attacks are committed against small busine

The Microsoft Digital Crimes Unit (DCU) states, "Cybercri information, send spam, run phishing scams and tar no one organization can solve the issue of cyber businesses who do not employ full-time cybersecurity personnel.

Nearly half of all cyber-attacks globally last year were committed against small according to Symantec.

Intel Corp. says that as many as 80 percent of small to medium sized business protection or email security in place.

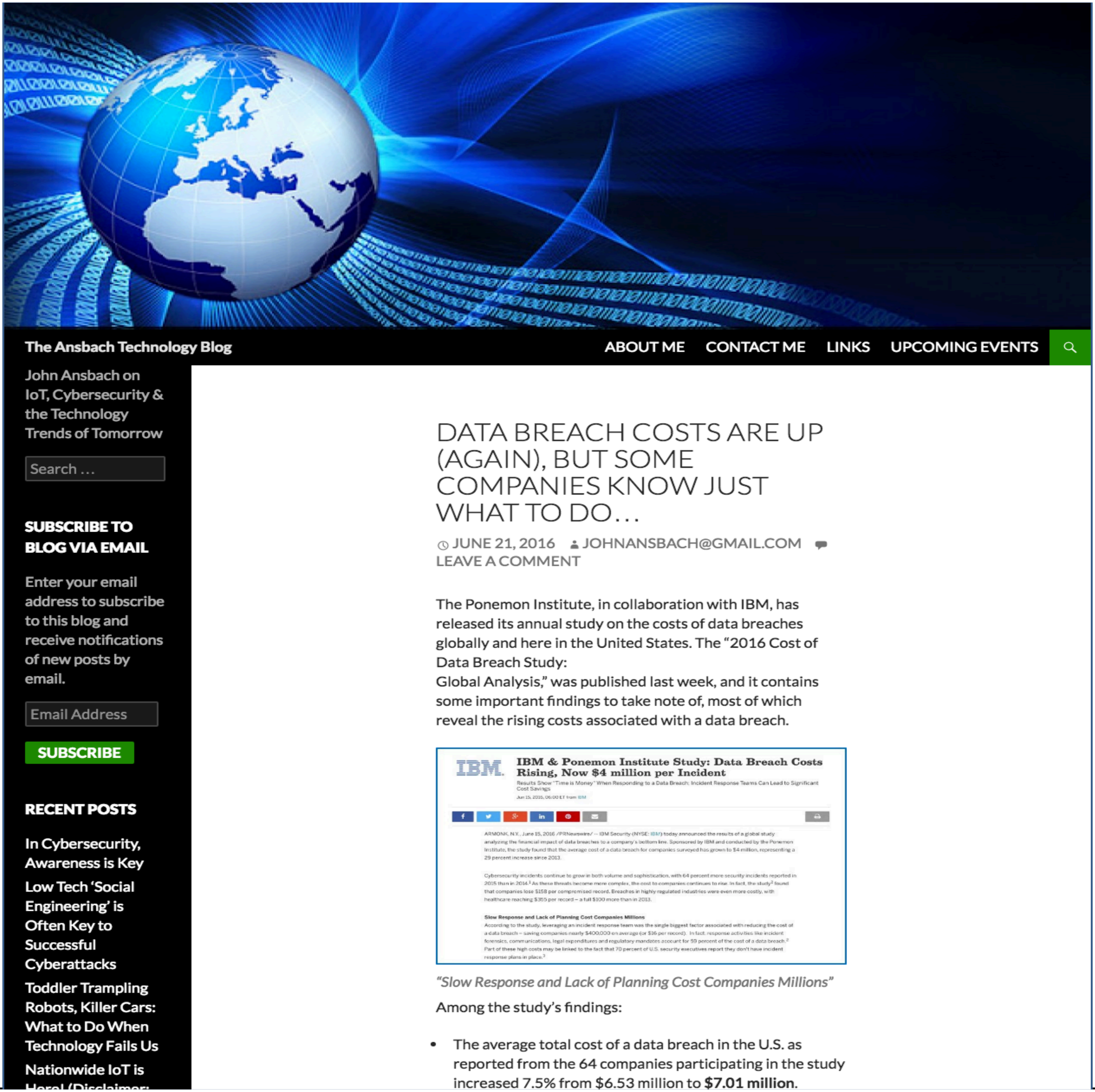
Ransomware attacks launched on smaller companies usually asks for $1,000 o for releasing the data being held hostage. The idea – according to Infosec Insti the business owner see this as a "nuisance expense" and pay up quickly compa business implication and stress of trying to fix the issue on their own.

Small businesses — who don't train their employees on security risks — are su the Business Email Compromise Scam (BEC), which the FBI says has led to over losses.

"Nearly **half** of all cyber-attacks are committed against small businesses…

As many as **80 percent** of small to medium sized businesses dont have data protection of email security in place...

Small businesses – who dont trian their employees on security risks – are susecptible to the **Businesss Email Compromise** Scam (BEC), which the FBI says has led to over **$3 billion** in losses."



John Ansbach on IoT, Cybersecurity & the Technology Trends of Tomorrow

SUBSCRIBE TO BLOG VIA EMAIL

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

RECENT POSTS

- In Cybersecurity, Awareness is Key
- Low Tech 'Social Engineering' is Often Key to Successful Cyberattacks
- Toddler Trampling Robots, Killer Cars: What to Do When Technology Fails Us
- Nationwide IoT is Here! (Disclaimer:

DATA BREACH COSTS ARE UP (AGAIN), BUT SOME COMPANIES KNOW JUST WHAT TO DO…

JUNE 21, 2016 JOHNANSBACH@GMAIL.COM LEAVE A COMMENT

The Ponemon Institute, in collaboration with IBM, has released its annual study on the costs of data breaches globally and here in the United States. The "2016 Cost of Data Breach Study:
Global Analysis," was published last week, and it contains some important findings to take note of, most of which reveal the rising costs associated with a data breach.

IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident

Results Show "Time is Money" When Responding to a Data Breach: Incident Response Teams Can Lead to Significant Cost Savings

Jun 15, 2016, 06:00 ET from IBM

ARMONK, N.Y., June 15, 2016 /PRNewswire/ -- IBM Security (NYSE: IBM) today announced the results of a global study analyzing the financial impact of data breaches to a company's bottom line. Sponsored by IBM and conducted by the Ponemon Institute, the study found that the average cost of a data breach for companies surveyed has grown to $4 million, representing a 29 percent increase since 2013.

Cybersecurity incidents continue to grow in both volume and sophistication, with 64 percent more security incidents reported in 2015 than in 2014.[1] As these threats become more complex, the cost to companies continues to rise. In fact, the study[2] found that companies lose $158 per compromised record. Breaches in highly regulated industries were even more costly, with healthcare reaching $355 per record – a full $100 more than in 2013.

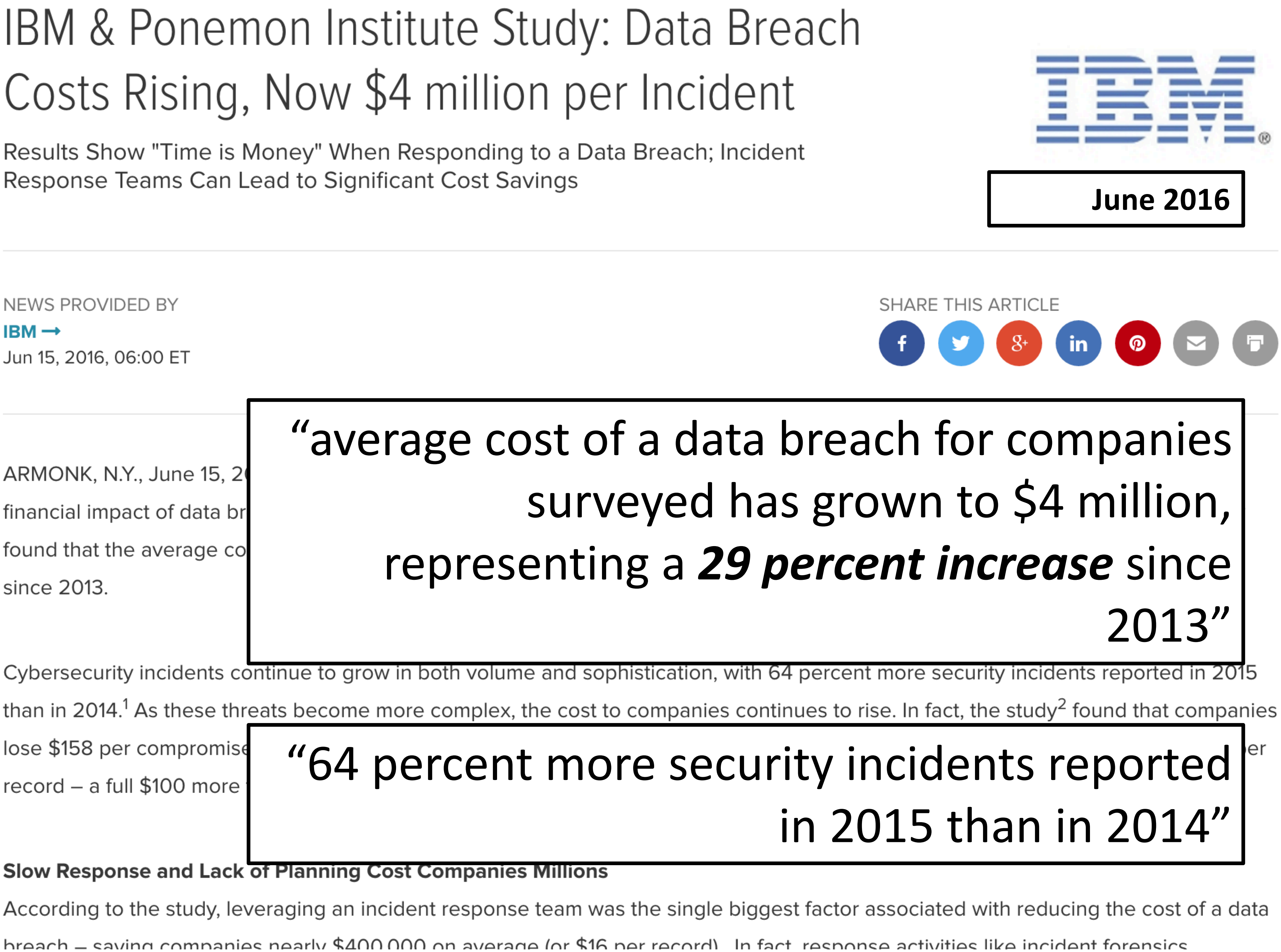
Slow Response and Lack of Planning Cost Companies Millions

According to the study, leveraging an incident response team was the single biggest factor associated with reducing the cost of a data breach – saving companies nearly $400,000 on average (or $16 per record). In fact, response activities like incident forensics, communications, legal expenditures and regulatory mandates account for 59 percent of the cost of a data breach.[2] Part of these high costs may be linked to the fact that 70 percent of U.S. security executives report they don't have incident response plans in place.[3]

"Slow Response and Lack of Planning Cost Companies Millions"

Among the study's findings:

- The average total cost of a data breach in the U.S. as reported from the 64 companies participating in the study increased 7.5% from $6.53 million to **$7.01 million.**



IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident

Results Show "Time is Money" When Responding to a Data Breach; Incident Response Teams Can Lead to Significant Cost Savings

June 2016

NEWS PROVIDED BY
IBM →
Jun 15, 2016, 06:00 ET

SHARE THIS ARTICLE

ARMONK, N.Y., June 15, 2
financial impact of data br
found that the average co
since 2013.

“average cost of a data breach for companies surveyed has grown to $4 million, representing a ***29 percent increase*** since 2013”

Cybersecurity incidents continue to grow in both volume and sophistication, with 64 percent more security incidents reported in 2015 than in 2014.[1] As these threats become more complex, the cost to companies continues to rise. In fact, the study[2] found that companies lose $158 per compromise ... er record – a full $100 more

“64 percent more security incidents reported in 2015 than in 2014”

Slow Response and Lack of Planning Cost Companies Millions

According to the study, leveraging an incident response team was the single biggest factor associated with reducing the cost of a data breach – saving companies nearly $400,000 on average (or $16 per record). In fact, response activities like incident forensics

Breach Costs

U.S. average cost of a data breach	**$6.5 mm** ($5.8mm)
World average cost of a data breach	**$3.8 mm** ($3.5 mm)
World cost per Record	**$154** ($145)
Cost per Record in the U.S.	**$217** (highest)

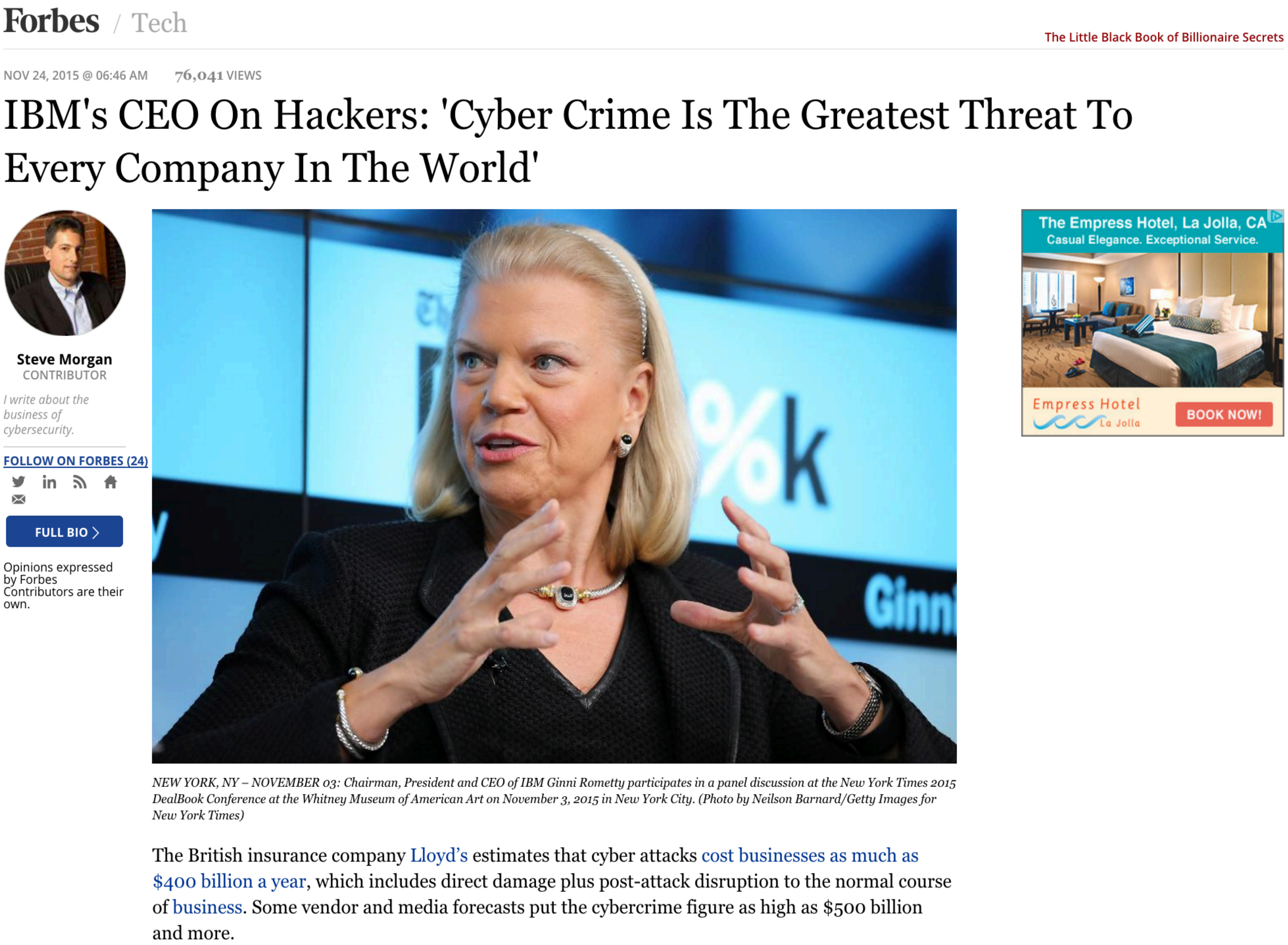
Source: 2015 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC

Landscape

- More attacks
- Against a broader swath of organizations of differing size
- With increasing sophistication
- Resulting in higher costs

There is more risk today for more organizations and their clients, partners and friends

The image part with relationship ID rId18 was not found in the file.



Forbes / Tech

NOV 24, 2015 @ 06:46 AM 76,041 VIEWS

IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'

Steve Morgan
CONTRIBUTOR

I write about the business of cybersecurity.

FOLLOW ON FORBES (24)

FULL BIO ›

Opinions expressed by Forbes Contributors are their own.

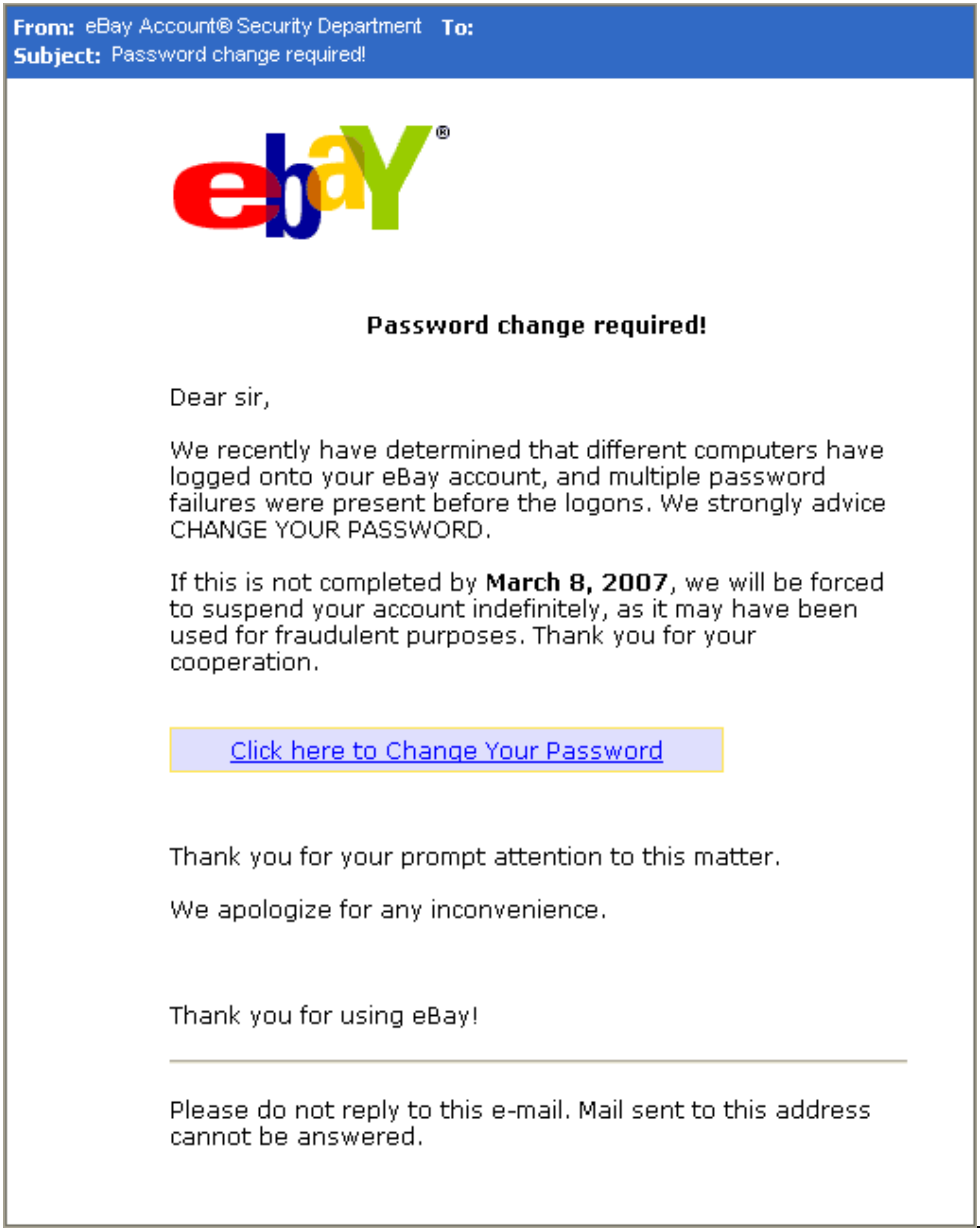
NEW YORK, NY – NOVEMBER 03: Chairman, President and CEO of IBM Ginni Rometty participates in a panel discussion at the New York Times 2015 DealBook Conference at the Whitney Museum of American Art on November 3, 2015 in New York City. (Photo by Neilson Barnard/Getty Images for New York Times)

The British insurance company Lloyd's estimates that cyber attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts put the cybercrime figure as high as $500 billion and more.

Threats

DEFINED
TOPOLOGY
CODE
WAY
MALICIOUS
SECURITY
HACKERS
DOCUMENT
VICTIM
TRAFFICKING
VARIETY
GROUPS
RESOURCES
SURROUNDING
CONSIDERED
WEBSITE
KINETIC
CYBER
ADVANCE
CRIMINAL
THEFT
INFORMATION
CITATION
ORGANIZED
DOCUMENTED
FACILITATED
GOVERNMENT
USE
INTERNATIONAL
HATE
TRADES
ELECTRONIC
TRAFFICKERS
DIRECTLY
BOTNET
TECHNOLOGY
HARM
WARFARE
COMPUTER
JURISDICTIONS
BETWEEN
CONTENT
COMMUNICATIONS
TERRORISM
MILLION
SCAMS
PROFILE
ENTERING
HARASSMENT
HACKING
CRIME
RACE
PACKAGES
AREA
ATTACK
PORNOGRAPHY
SYSTEMS
GOING
PURPOSES
DEPARTMENT
NETWORKS
FACE
WELL
REFERS
GROUP
INCREASINGLY
INCLUDE
FORM
SPAM
DEVICES
USED
SPECIFIC
ALTERING
FRAUD
OBSCENE
SYSTEM
UNSOLICITED
DURING
SEVERAL
COUNTS
PEOPLE
CHILD
CYBERSPACE
SERVICES
ILLEGAL
DRUG
UNAUTHORIZED
CAUSE
INTERNET
MAN
ACTIVITIES
TARGET
OFFENSIVE
ALLEGEDLY
UNIVERSITY
INVESTIGATORS
INDIVIDUALS
COPYRIGHT
PROBLEMS
DATA
SERVER
FEDERAL
CASES
HIGH
NETWORK
INCLUDED
CONCERN
NATION
USING
SERVICE
SENDING
MAIL
IDENTITY
CRIMES
INCLUDING
WEBSITES
RING
ROOMS
MAJOR
NEEDED
STORED
CYBERTERRORISM
DISTRIBUTED
DETECT
FUTURE
TECHNICAL
COMBATTING
ENCRYPTED
DEROGATORY
ACCESS
COMMITTED
DEFENSE
UNLAWFUL
INDIVIDUAL
FINANCIAL
PHYSICAL
ALLOW
STALKING
COMPANIES
OFFICIALS
TIME
LIMITS
INFECTED

Phishing (and Spearphishing, SMiShing, Vishing…)



From: eBay Account® Security Department **To:**
Subject: Password change required!

Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD.

If this is not completed by **March 8, 2007**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

Click here to Change Your Password

Thank you for your prompt attention to this matter.

We apologize for any inconvenience.

Thank you for using eBay!

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

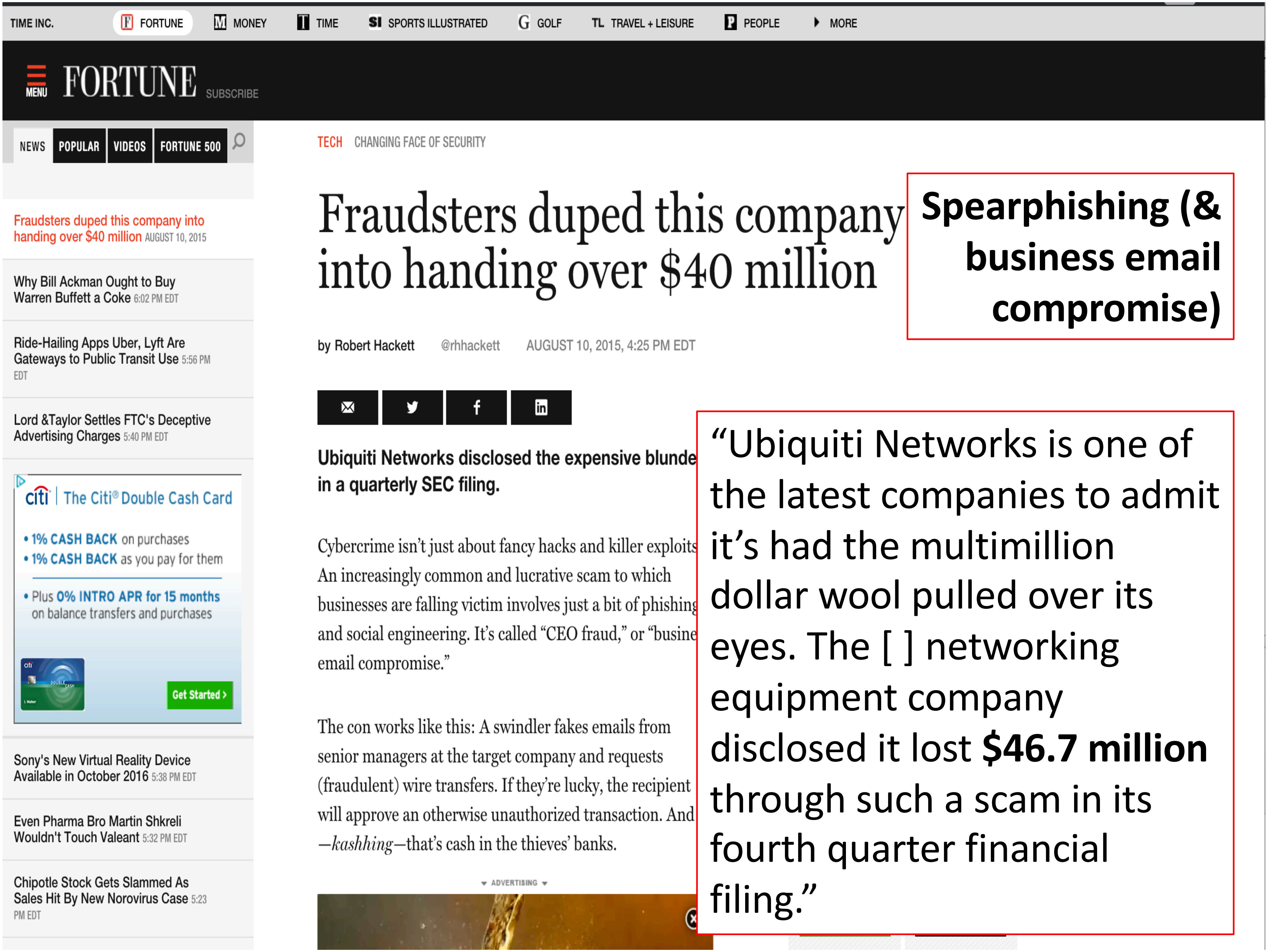
Phishing scam

Generic email sent to a high number of recipients

Not tailored, not engineered to appear valid

Likely uses actual company logos

Uses a sense of urgency to motivate the intended action



Fraudsters duped this company into handing over $40 million AUGUST 10, 2015

Why Bill Ackman Ought to Buy Warren Buffett a Coke 6:02 PM EDT

Ride-Hailing Apps Uber, Lyft Are Gateways to Public Transit Use 5:56 PM EDT

Lord &Taylor Settles FTC's Deceptive Advertising Charges 5:40 PM EDT

Sony's New Virtual Reality Device Available in October 2016 5:38 PM EDT

Even Pharma Bro Martin Shkreli Wouldn't Touch Valeant 5:32 PM EDT

Chipotle Stock Gets Slammed As Sales Hit By New Norovirus Case 5:23 PM EDT

TECH CHANGING FACE OF SECURITY

Fraudsters duped this company into handing over $40 million

by Robert Hackett @rhhackett AUGUST 10, 2015, 4:25 PM EDT

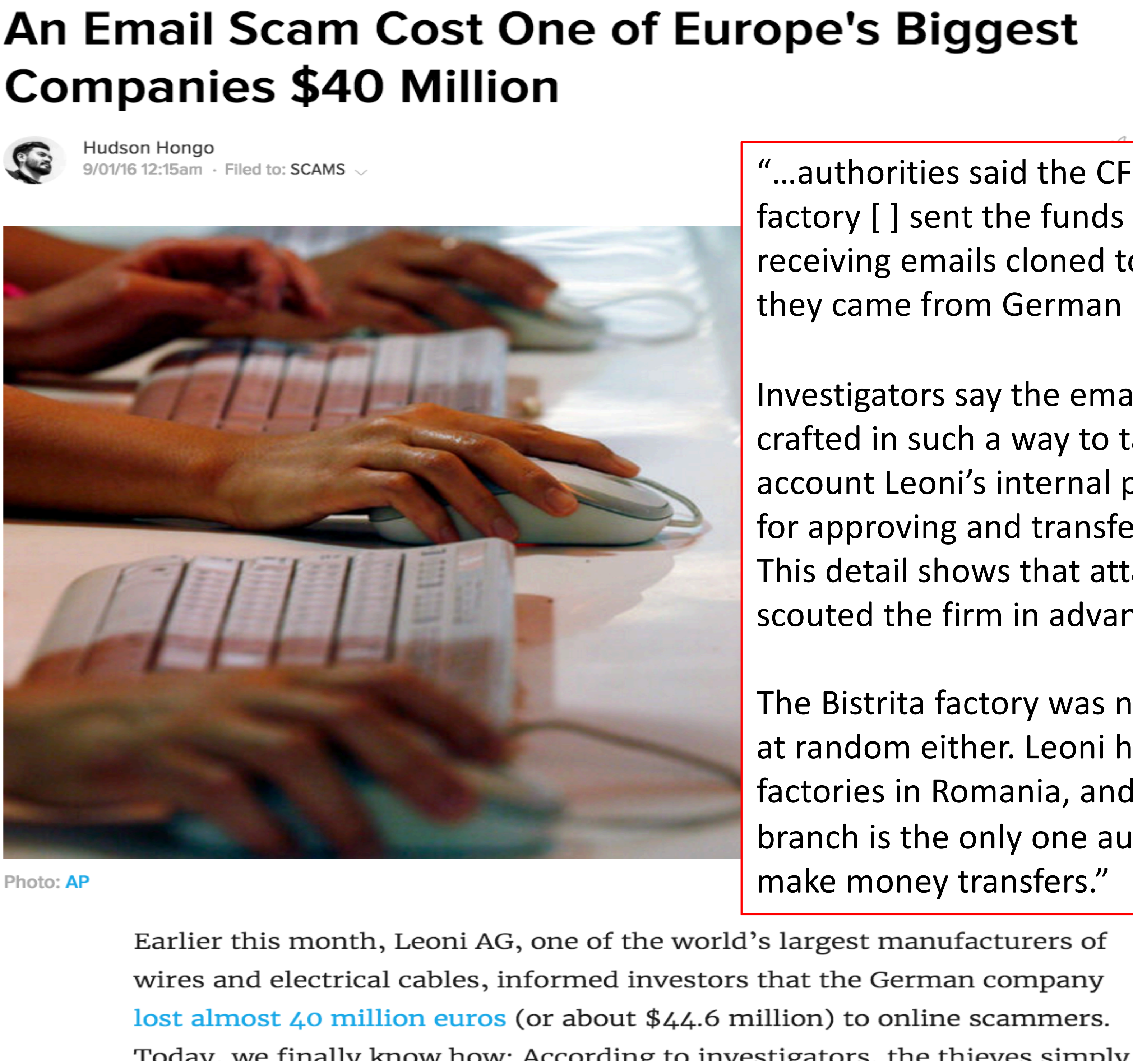
Ubiquiti Networks disclosed the expensive blunde in a quarterly SEC filing.

Cybercrime isn't just about fancy hacks and killer exploits An increasingly common and lucrative scam to which businesses are falling victim involves just a bit of phishing and social engineering. It's called "CEO fraud," or "busine email compromise."

The con works like this: A swindler fakes emails from senior managers at the target company and requests (fraudulent) wire transfers. If they're lucky, the recipient will approve an otherwise unauthorized transaction. And —*kashhing*—that's cash in the thieves' banks.

Spearphishing (& business email compromise)

"Ubiquiti Networks is one of the latest companies to admit it's had the multimillion dollar wool pulled over its eyes. The [ ] networking equipment company disclosed it lost **$46.7 million** through such a scam in its fourth quarter financial filing."



An Email Scam Cost One of Europe's Biggest Companies $40 Million

Hudson Hongo
9/01/16 12:15am · Filed to: SCAMS

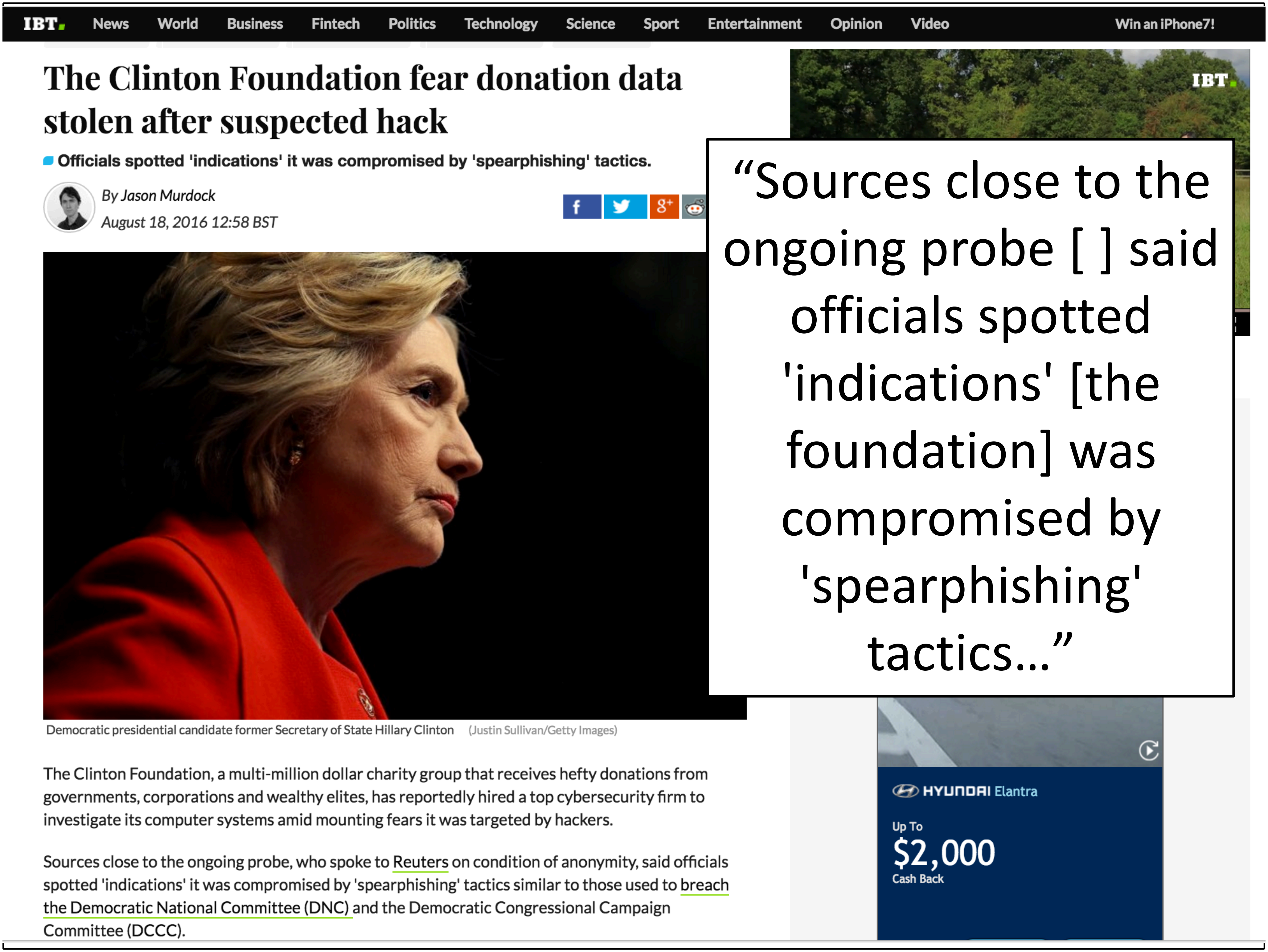
Photo: AP

Earlier this month, Leoni AG, one of the world's largest manufacturers of wires and electrical cables, informed investors that the German company lost almost 40 million euros (or about $44.6 million) to online scammers. Today, we finally know how: According to investigators, the thieves simply

"…authorities said the CFO of a Leoni factory [ ] sent the funds after receiving emails cloned to look like they came from German executives…

Investigators say the email was crafted in such a way to take into account Leoni's internal procedures for approving and transferring funds. This detail shows that attackers scouted the firm in advance…

The Bistrita factory was not chosen at random either. Leoni has four factories in Romania, and the Bistrita branch is the only one authorized to make money transfers."



The Clinton Foundation fear donation data stolen after suspected hack

Officials spotted 'indications' it was compromised by 'spearphishing' tactics.

By Jason Murdock
August 18, 2016 12:58 BST

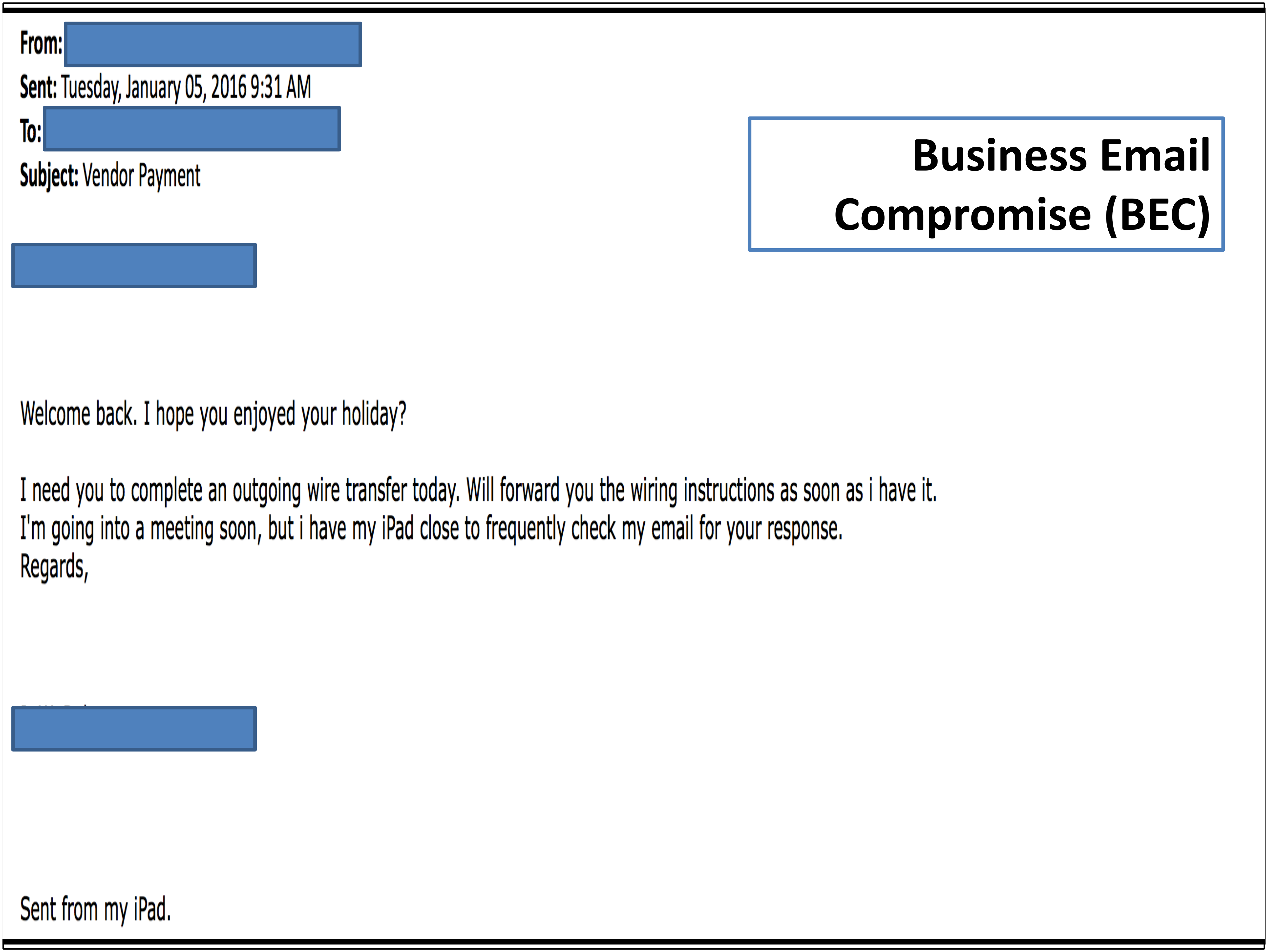
Democratic presidential candidate former Secretary of State Hillary Clinton (Justin Sullivan/Getty Images)

The Clinton Foundation, a multi-million dollar charity group that receives hefty donations from governments, corporations and wealthy elites, has reportedly hired a top cybersecurity firm to investigate its computer systems amid mounting fears it was targeted by hackers.

Sources close to the ongoing probe, who spoke to Reuters on condition of anonymity, said officials spotted 'indications' it was compromised by 'spearphishing' tactics similar to those used to breach the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC).

"Sources close to the ongoing probe [ ] said officials spotted 'indications' [the foundation] was compromised by 'spearphishing' tactics…"

Business Email Compromise (BEC)



From: [redacted]
Sent: Tuesday, January 05, 2016 9:31 AM
To: [redacted]
Subject: Vendor Payment

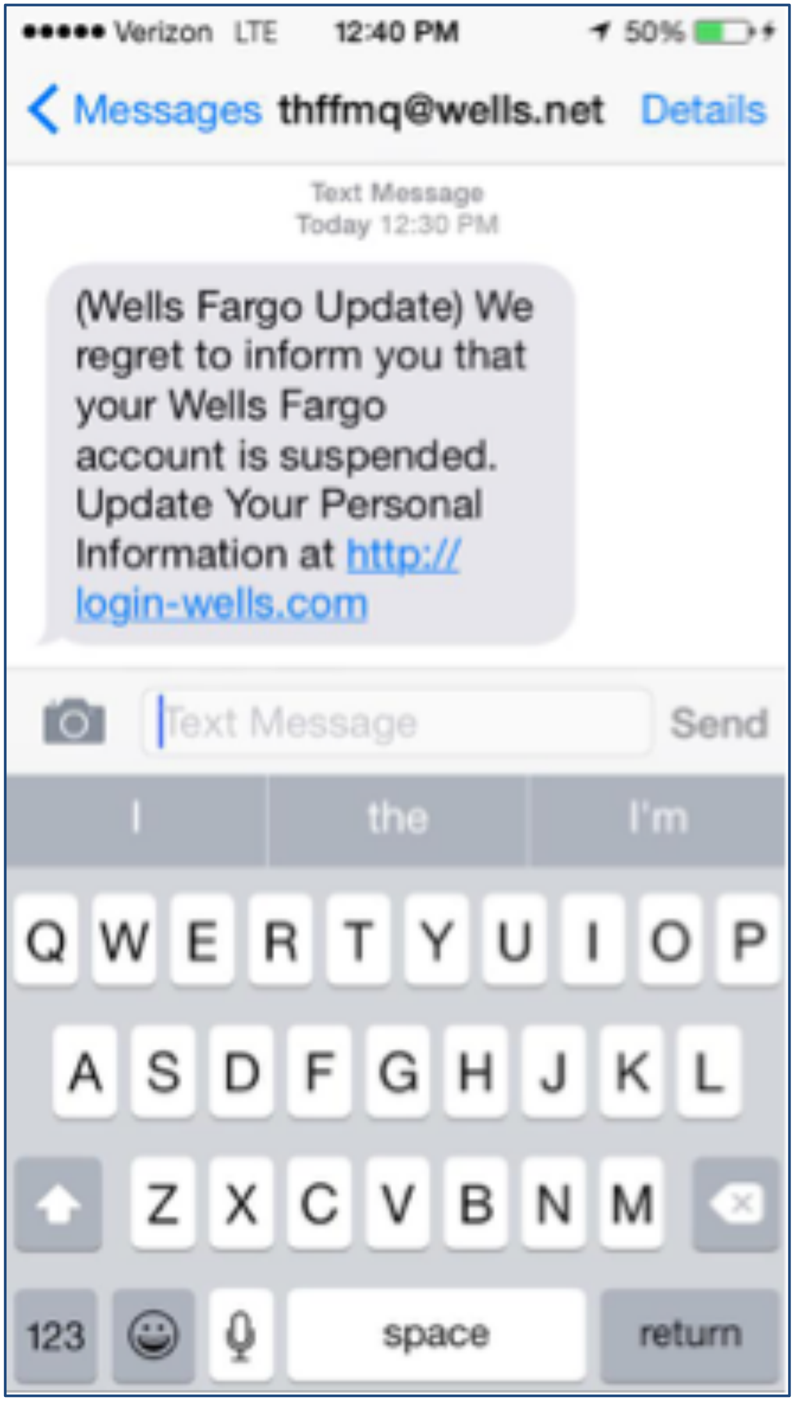
[redacted]

Welcome back. I hope you enjoyed your holiday?

I need you to complete an outgoing wire transfer today. Will forward you the wiring instructions as soon as i have it.
I'm going into a meeting soon, but i have my iPad close to frequently check my email for your response.
Regards,

[redacted]

Sent from my iPad.



(Wells Fargo Update) We regret to inform you that your Wells Fargo account is suspended. Update Your Personal Information at http://login-wells.com

SMiShing scam

SMS is short message service, a/k/a texting

Same scam, sent by text message

Requests user to click a link

Also uses a sense of urgency to motivate the intended action

VISHING

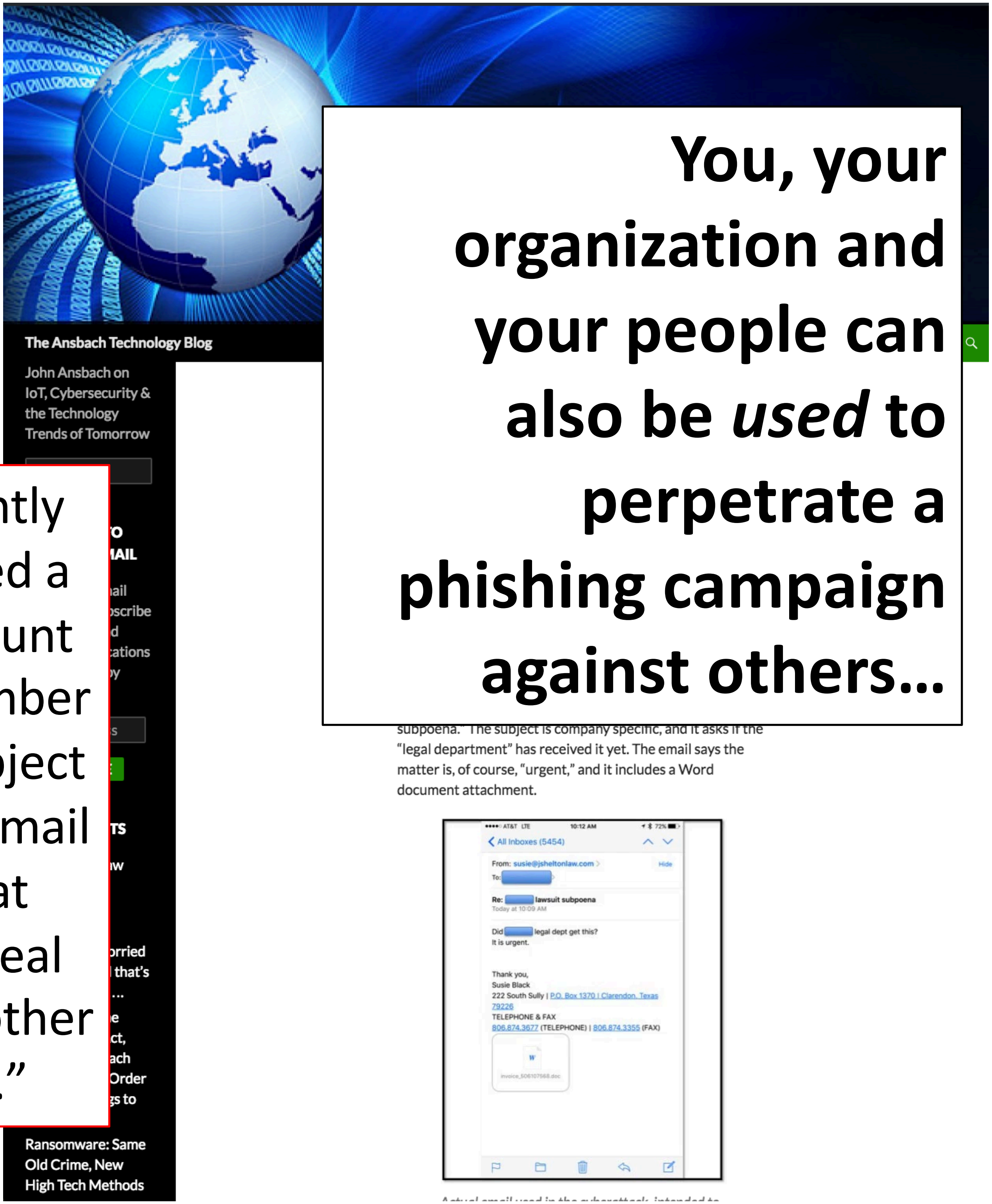
Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "Voice" and phishing. Vishing exploits the public's trust in landline telephone services.

Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Small Texas Law Firm Used in International Cyberattack

You, your organization and your people can also be *used* to perpetrate a phishing campaign against others…

"Cybercriminals apparently gained access to and used a valid law firm email account to email an unknown number of recipients with the subject 'lawsuit subpoena.' The email contained malware that attackers could use to steal banking credentials and other personal information…"



The Ansbach Technology Blog

John Ansbach on IoT, Cybersecurity & the Technology Trends of Tomorrow

o
AIL
ail
scribe
d
ations
y
s
TS
w
orried
that's
…
e
ct,
ach
Order
gs to

Ransomware: Same Old Crime, New High Tech Methods

subpoena." The subject is company specific, and it asks if the "legal department" has received it yet. The email says the matter is, of course, "urgent," and it includes a Word document attachment.

From: susie@jsheltonlaw.com
To: [redacted]

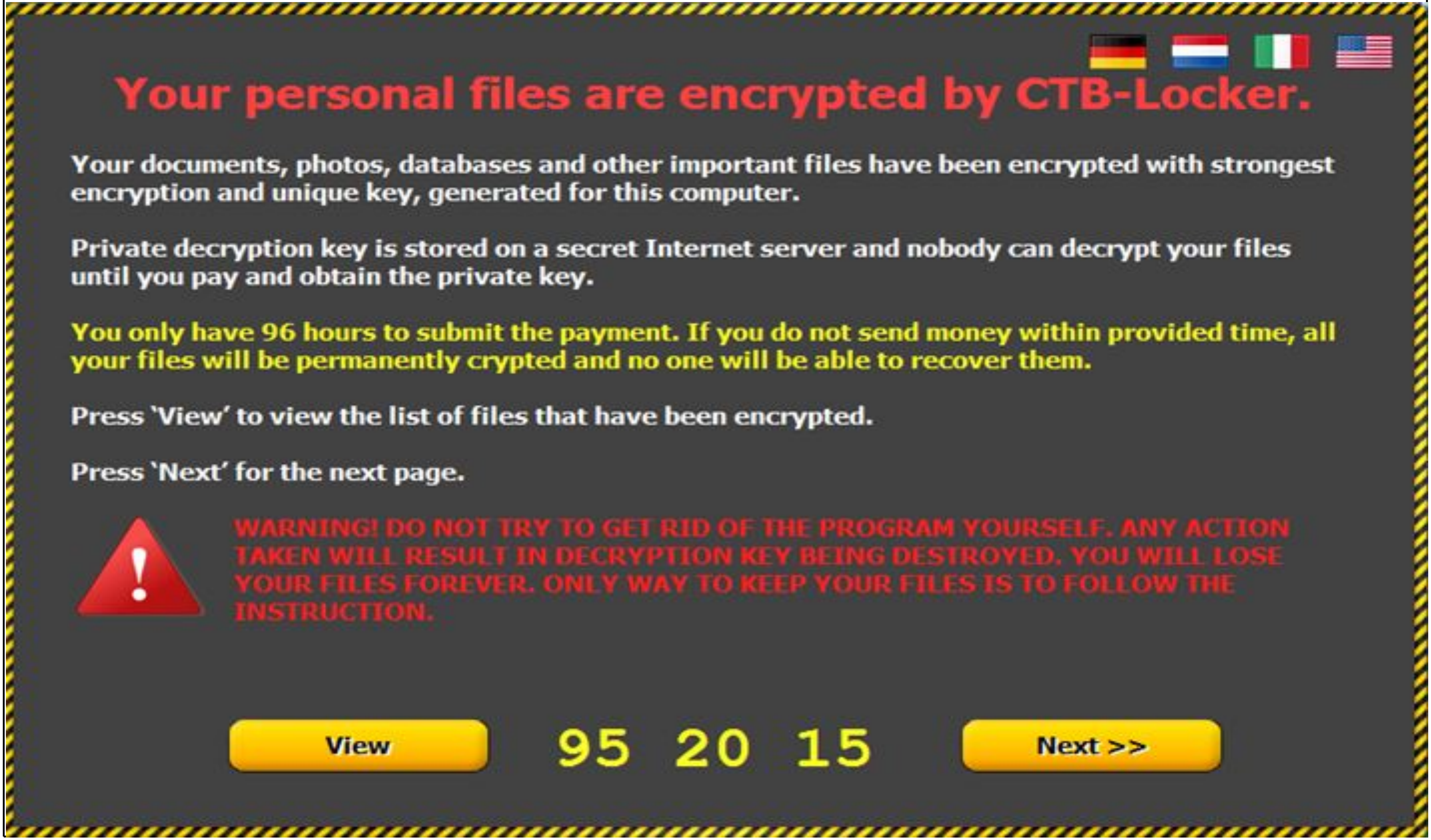
Re: [redacted] lawsuit subpoena
Today at 10:09 AM

Did [redacted] legal dept get this?
It is urgent.

Thank you,
Susie Black
222 South Sully | P.O. Box 1370 | Clarendon, Texas 79226
TELEPHONE & FAX
806.874.3677 (TELEPHONE) | 806.874.3355 (FAX)

Actual email used in the cyberattack, intended to

Ransomware



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

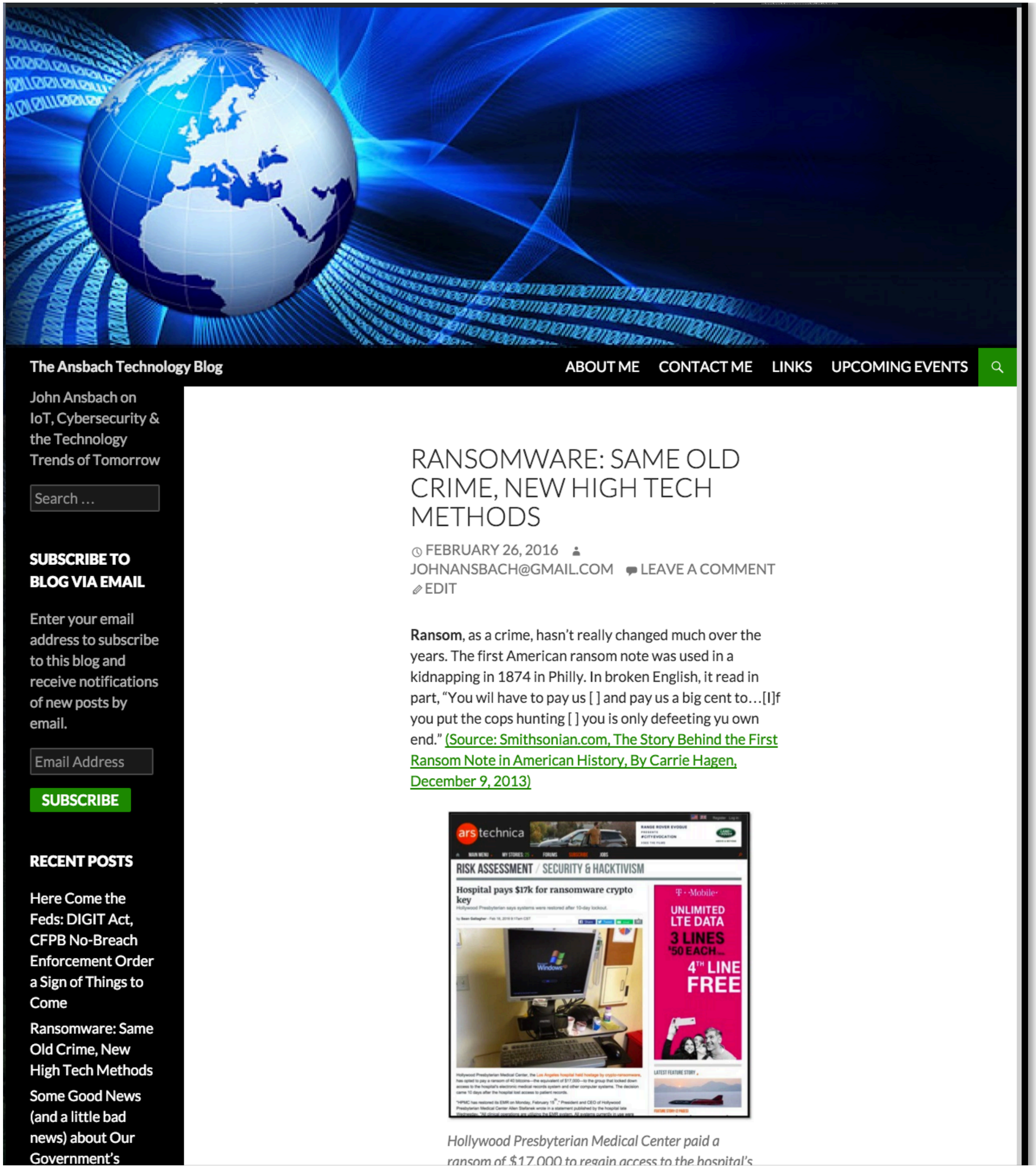
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.



The Ansbach Technology Blog

John Ansbach on IoT, Cybersecurity & the Technology Trends of Tomorrow

SUBSCRIBE TO BLOG VIA EMAIL

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

RECENT POSTS

- Here Come the Feds: DIGIT Act, CFPB No-Breach Enforcement Order a Sign of Things to Come
- Ransomware: Same Old Crime, New High Tech Methods
- Some Good News (and a little bad news) about Our Government's

RANSOMWARE: SAME OLD CRIME, NEW HIGH TECH METHODS

FEBRUARY 26, 2016 JOHNANSBACH@GMAIL.COM LEAVE A COMMENT EDIT

Ransom, as a crime, hasn't really changed much over the years. The first American ransom note was used in a kidnapping in 1874 in Philly. In broken English, it read in part, "You wil have to pay us [ ] and pay us a big cent to…[I]f you put the cops hunting [ ] you is only defeeting yu own end." (Source: Smithsonian.com, The Story Behind the First Ransom Note in American History, By Carrie Hagen, December 9, 2013)

RISK ASSESSMENT / SECURITY & HACKTIVISM

Hospital pays $17k for ransomware crypto key

Hollywood Presbyterian says systems were restored after 10-day lockout.

Hollywood Presbyterian Medical Center, the Los Angeles hospital held hostage by crypto-ransomware, has opted to pay a ransom of 40 bitcoins—the equivalent of $17,000—to the group that locked down access to the hospital's electronic medical records system and other computer systems. The decision came 10 days after the hospital lost access to patient records.

Hollywood Presbyterian Medical Center paid a ransom of $17,000 to regain access to the hospital's

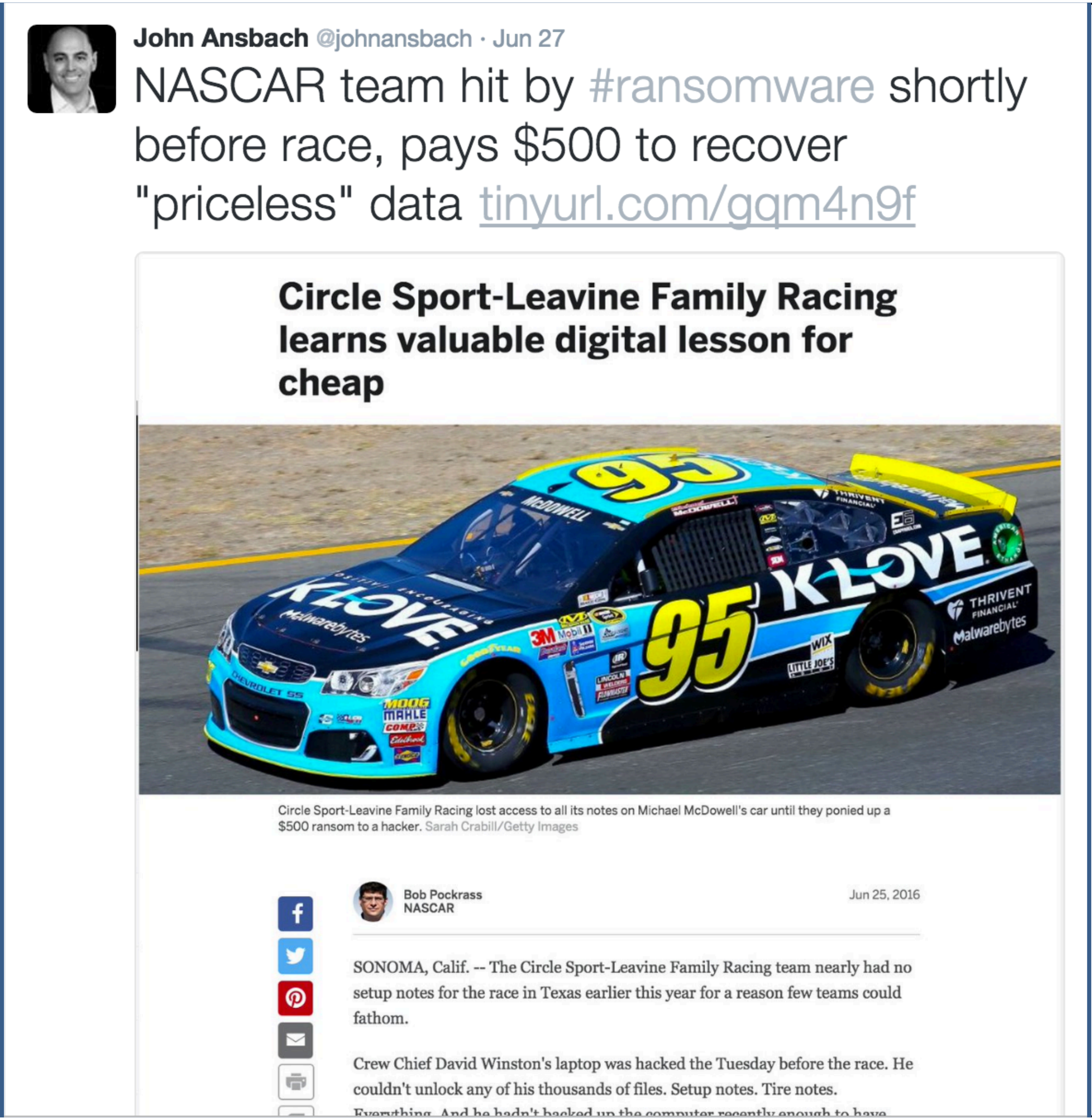
"Ransomware is the hot hacking trend of 2016"

Source: cnet, 3.10.2016

California hospital paid $17,000 to get their systems back

"Locky" loads Word documents with macros that once "enabled" deliver ransomware

Xbot is Android malware that both steals banking credentials and takes a system hostage



John Ansbach @johnansbach · Jun 27

NASCAR team hit by #ransomware shortly before race, pays $500 to recover "priceless" data tinyurl.com/gqm4n9f

Circle Sport-Leavine Family Racing learns valuable digital lesson for cheap

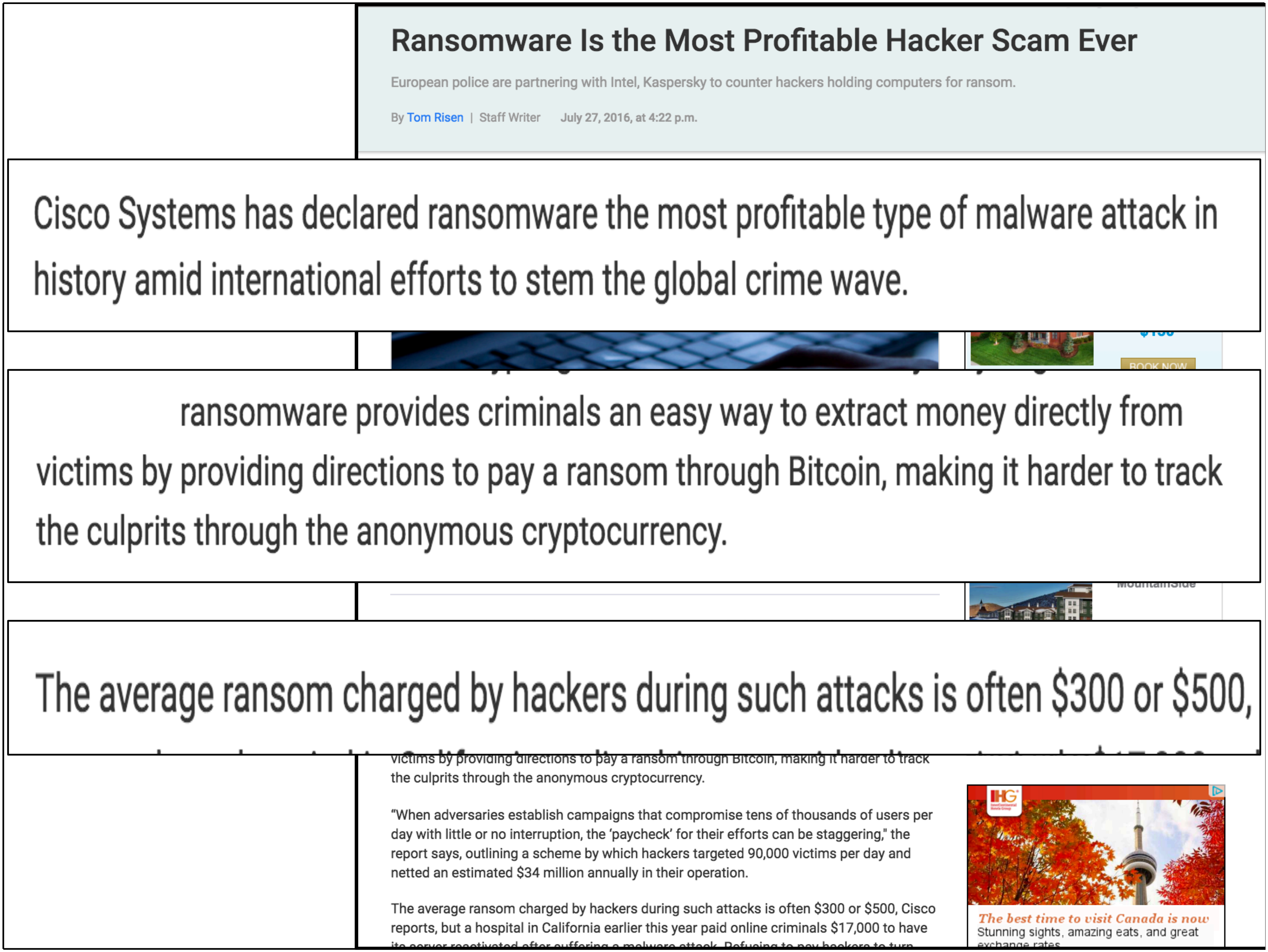
Circle Sport-Leavine Family Racing lost access to all its notes on Michael McDowell's car until they ponied up a $500 ransom to a hacker. Sarah Crabill/Getty Images

Bob Pockrass
NASCAR

Jun 25, 2016

SONOMA, Calif. -- The Circle Sport-Leavine Family Racing team nearly had no setup notes for the race in Texas earlier this year for a reason few teams could fathom.

Crew Chief David Winston's laptop was hacked the Tuesday before the race. He couldn't unlock any of his thousands of files. Setup notes. Tire notes. Everything. And he hadn't backed up the computer recently enough to have



Ransomware Is the Most Profitable Hacker Scam Ever

European police are partnering with Intel, Kaspersky to counter hackers holding computers for ransom.

By Tom Risen | Staff Writer July 27, 2016, at 4:22 p.m.

Cisco Systems has declared ransomware the most profitable type of malware attack in history amid international efforts to stem the global crime wave.

ransomware provides criminals an easy way to extract money directly from victims by providing directions to pay a ransom through Bitcoin, making it harder to track the culprits through the anonymous cryptocurrency.

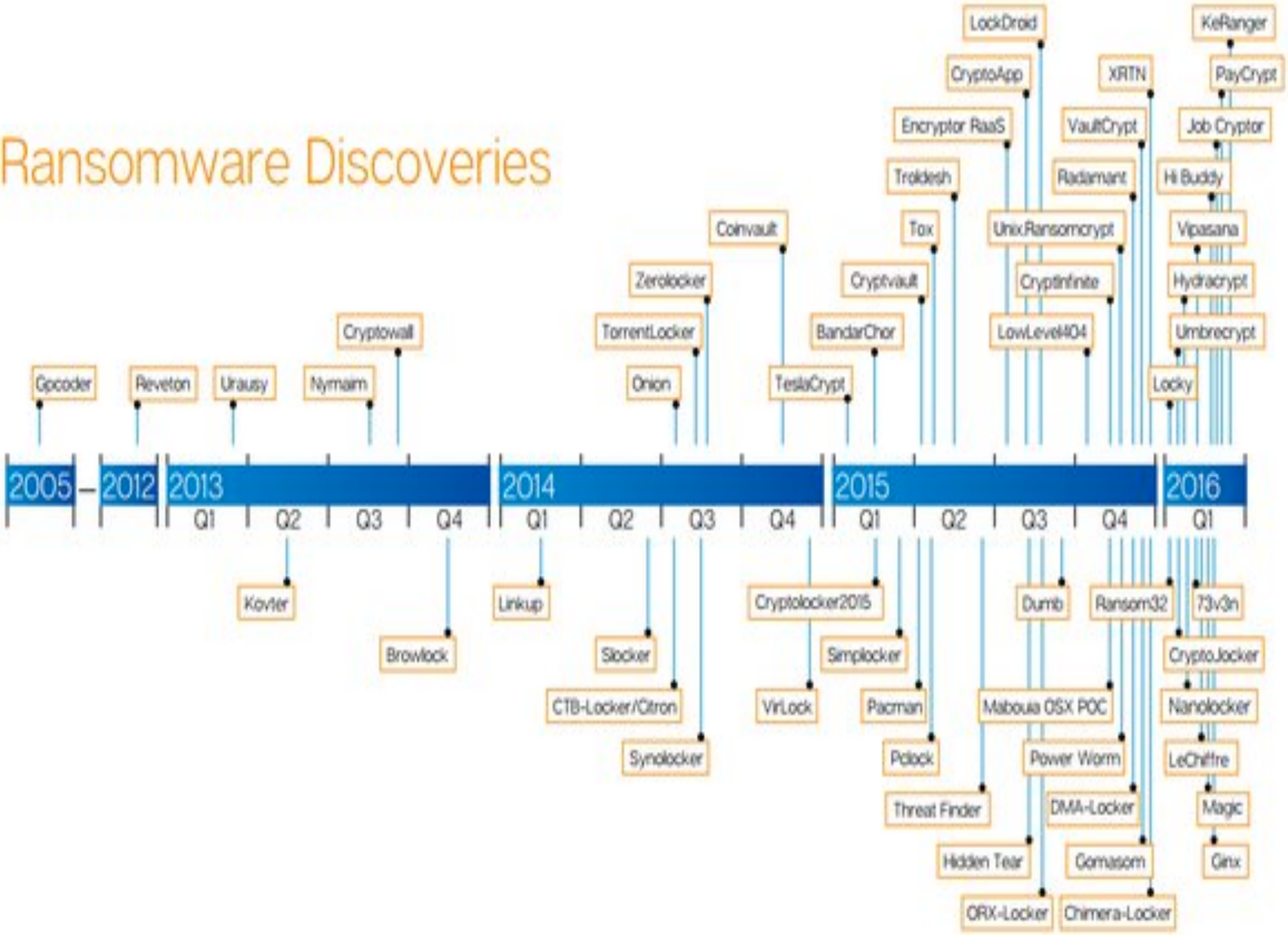
The average ransom charged by hackers during such attacks is often $300 or $500,

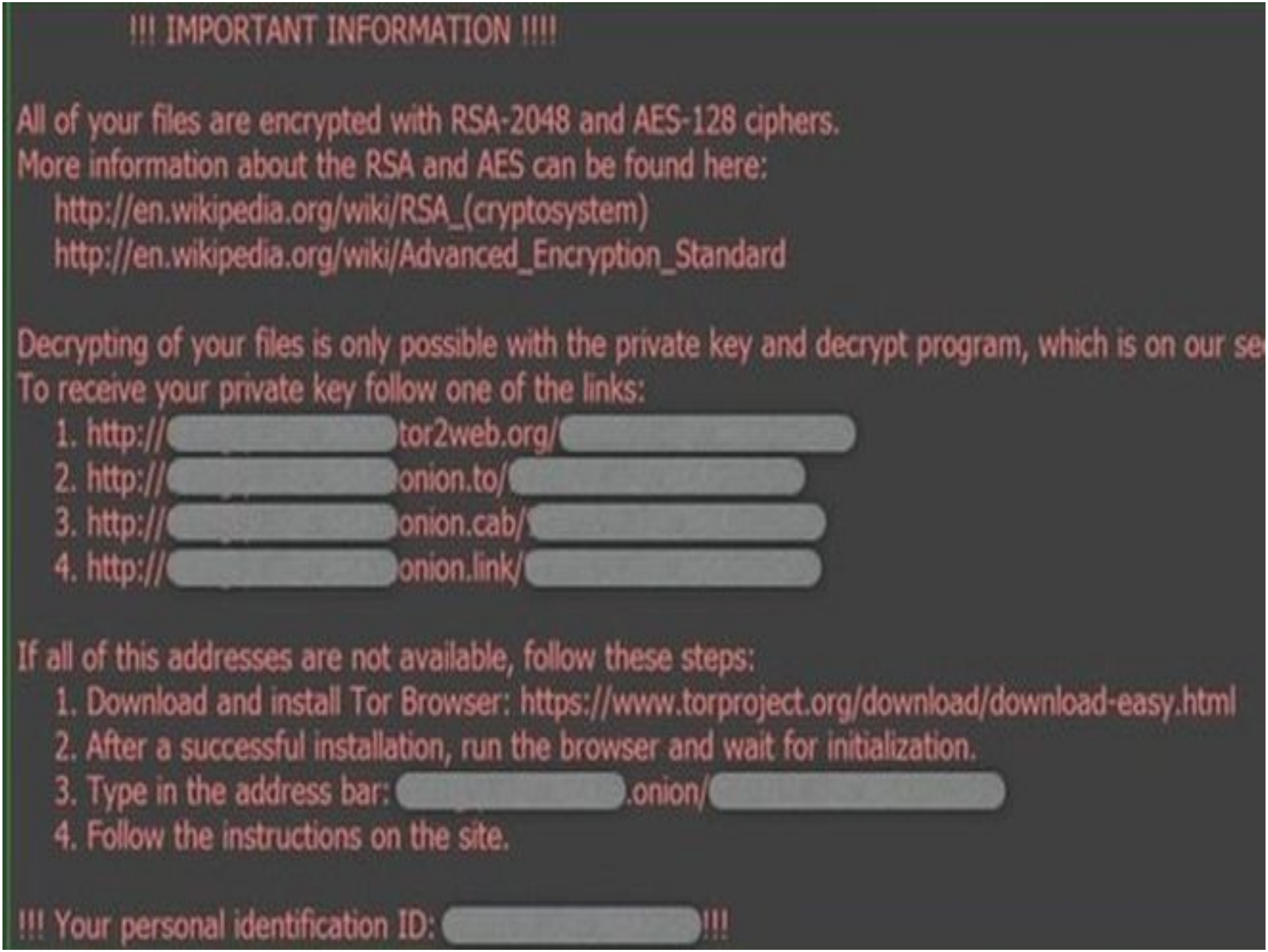
victims by providing directions to pay a ransom through Bitcoin, making it harder to track the culprits through the anonymous cryptocurrency.

"When adversaries establish campaigns that compromise tens of thousands of users per day with little or no interruption, the 'paycheck' for their efforts can be staggering," the report says, outlining a scheme by which hackers targeted 90,000 victims per day and netted an estimated $34 million annually in their operation.

The average ransom charged by hackers during such attacks is often $300 or $500, Cisco reports, but a hospital in California earlier this year paid online criminals $17,000 to have its server reactivated after suffering a malware attack. Refusing to pay hackers to turn

Ransomware Discoveries





!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

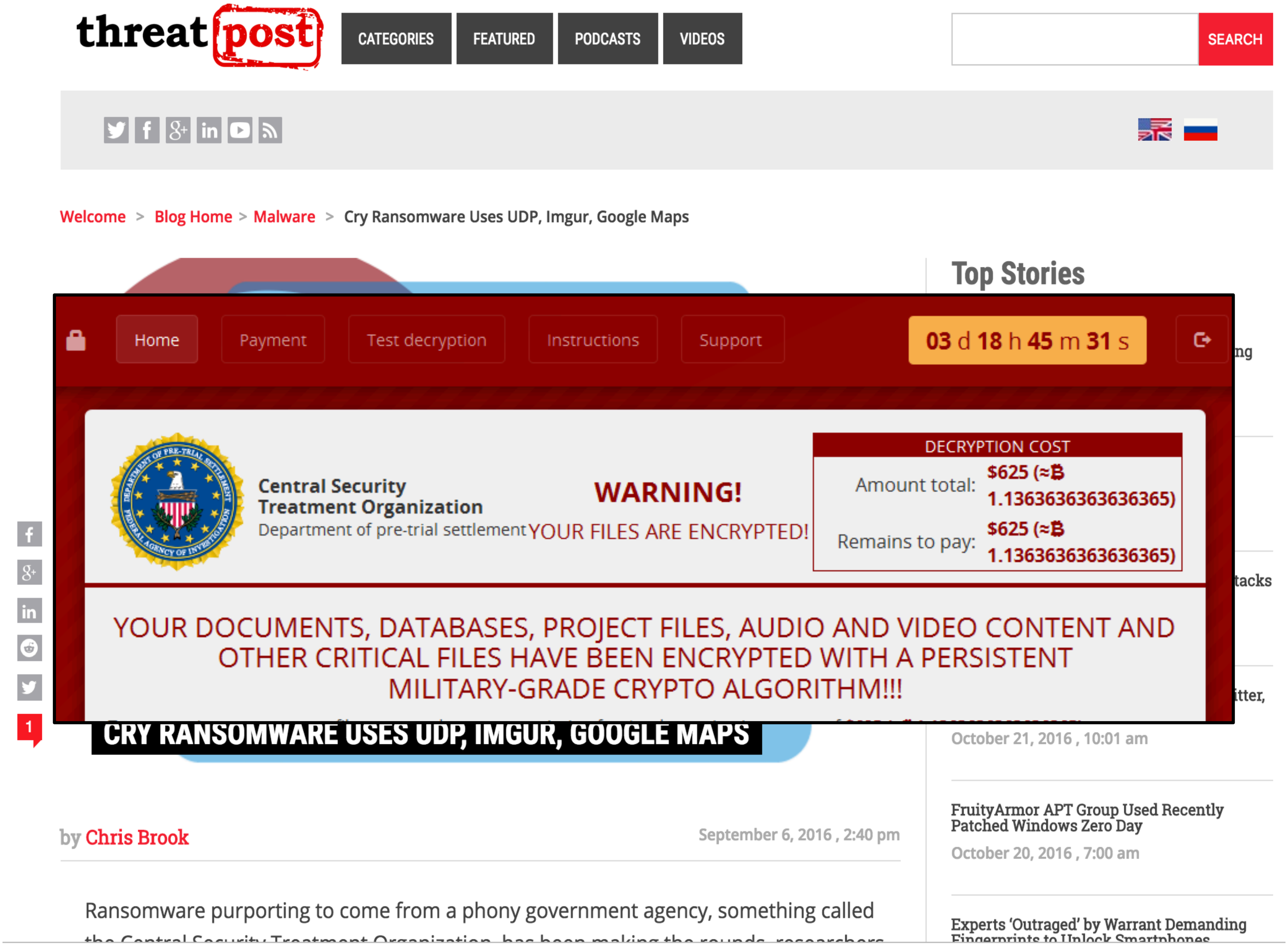
Decrypting of your files is only possible with the private key and decrypt program, which is on our se
To receive your private key follow one of the links:

1. http://[redacted]tor2web.org/[redacted]
2. http://[redacted]onion.to/[redacted]
3. http://[redacted]onion.cab/[redacted]
4. http://[redacted]onion.link/[redacted]

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted].onion/[redacted]
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]!!!



Welcome > Blog Home > Malware > Cry Ransomware Uses UDP, Imgur, Google Maps

Central Security Treatment Organization
Department of pre-trial settlement

WARNING!

YOUR FILES ARE ENCRYPTED!

DECRYPTION COST

Amount total:	$625 (≈Ƀ 1.1363636363636365)
Remains to pay:	$625 (≈Ƀ 1.1363636363636365)

YOUR DOCUMENTS, DATABASES, PROJECT FILES, AUDIO AND VIDEO CONTENT AND OTHER CRITICAL FILES HAVE BEEN ENCRYPTED WITH A PERSISTENT MILITARY-GRADE CRYPTO ALGORITHM!!!

CRY RANSOMWARE USES UDP, IMGUR, GOOGLE MAPS

by Chris Brook

September 6, 2016 , 2:40 pm

Ransomware purporting to come from a phony government agency, something called the Central Security Treatment Organization, has been making the rounds, researchers

Top Stories

ng

tacks

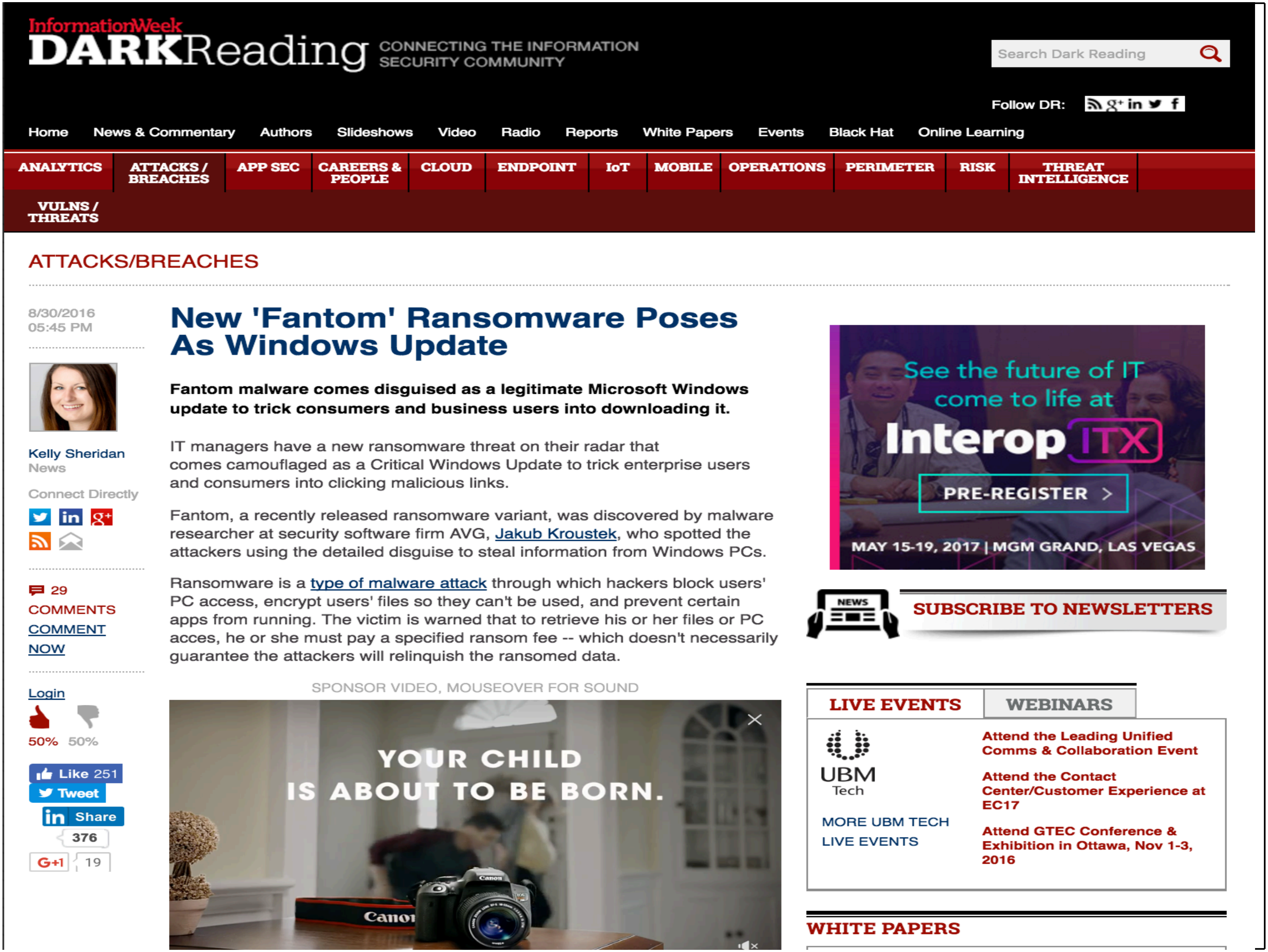
itter,

October 21, 2016 , 10:01 am

FruityArmor APT Group Used Recently Patched Windows Zero Day

October 20, 2016 , 7:00 am

Experts 'Outraged' by Warrant Demanding Fingerprints to Unlock Smartphones



InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

ATTACKS/BREACHES

8/30/2016 05:45 PM

Kelly Sheridan
News

29 COMMENTS
COMMENT NOW

New 'Fantom' Ransomware Poses As Windows Update

Fantom malware comes disguised as a legitimate Microsoft Windows update to trick consumers and business users into downloading it.

IT managers have a new ransomware threat on their radar that comes camouflaged as a Critical Windows Update to trick enterprise users and consumers into clicking malicious links.

Fantom, a recently released ransomware variant, was discovered by malware researcher at security software firm AVG, Jakub Kroustek, who spotted the attackers using the detailed disguise to steal information from Windows PCs.

Ransomware is a type of malware attack through which hackers block users' PC access, encrypt users' files so they can't be used, and prevent certain apps from running. The victim is warned that to retrieve his or her files or PC acces, he or she must pay a specified ransom fee -- which doesn't necessarily guarantee the attackers will relinquish the ransomed data.

SUBSCRIBE TO NEWSLETTERS

LIVE EVENTS | WEBINARS

UBM Tech

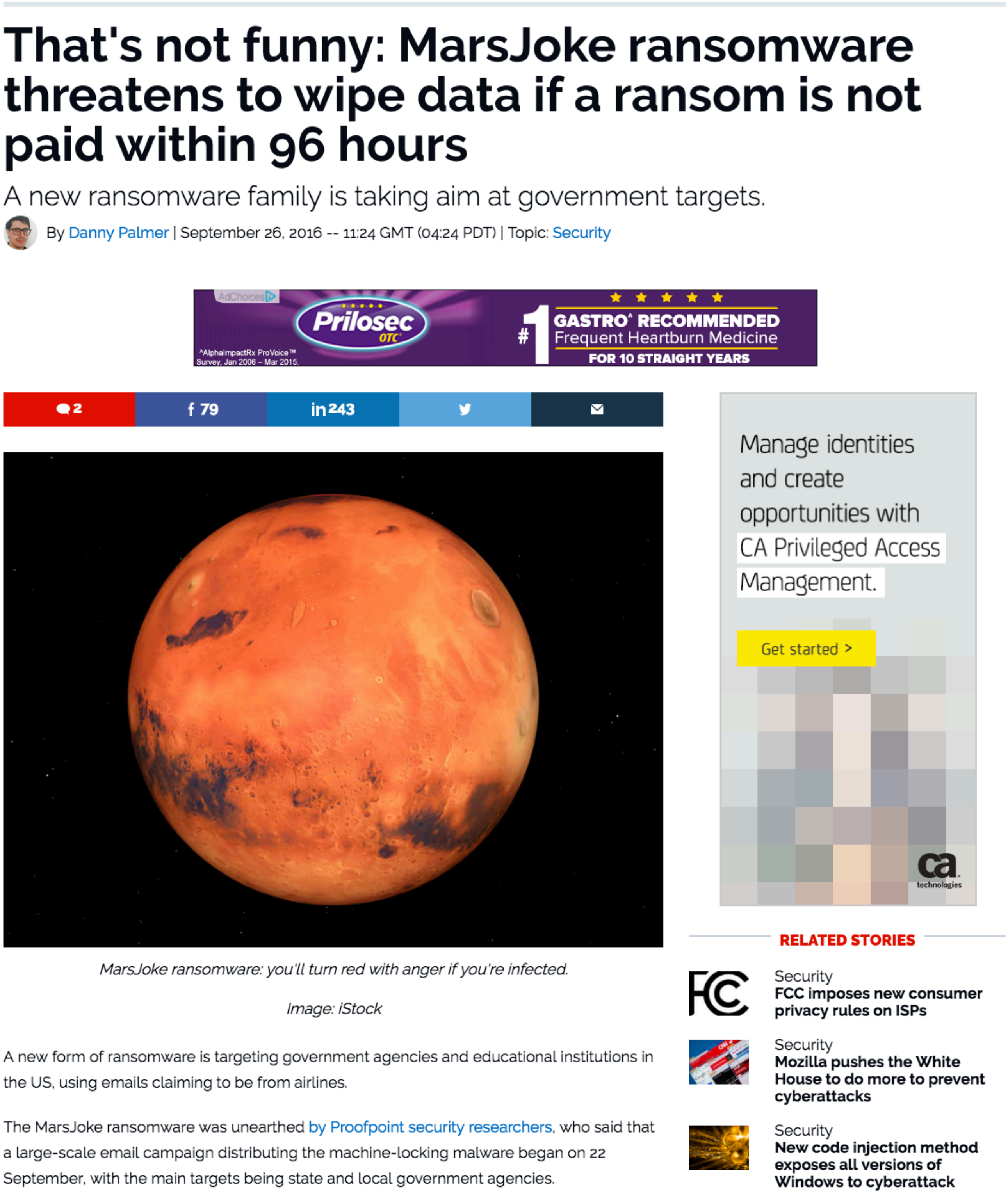
MORE UBM TECH LIVE EVENTS

Attend the Leading Unified Comms & Collaboration Event

Attend the Contact Center/Customer Experience at EC17

Attend GTEC Conference & Exhibition in Ottawa, Nov 1-3, 2016

WHITE PAPERS



That's not funny: MarsJoke ransomware threatens to wipe data if a ransom is not paid within 96 hours

A new ransomware family is taking aim at government targets.

By Danny Palmer | September 26, 2016 -- 11:24 GMT (04:24 PDT) | Topic: Security

MarsJoke ransomware: you'll turn red with anger if you're infected.

Image: iStock

A new form of ransomware is targeting government agencies and educational institutions in the US, using emails claiming to be from airlines.

The MarsJoke ransomware was unearthed by Proofpoint security researchers, who said that a large-scale email campaign distributing the machine-locking malware began on 22 September, with the main targets being state and local government agencies.

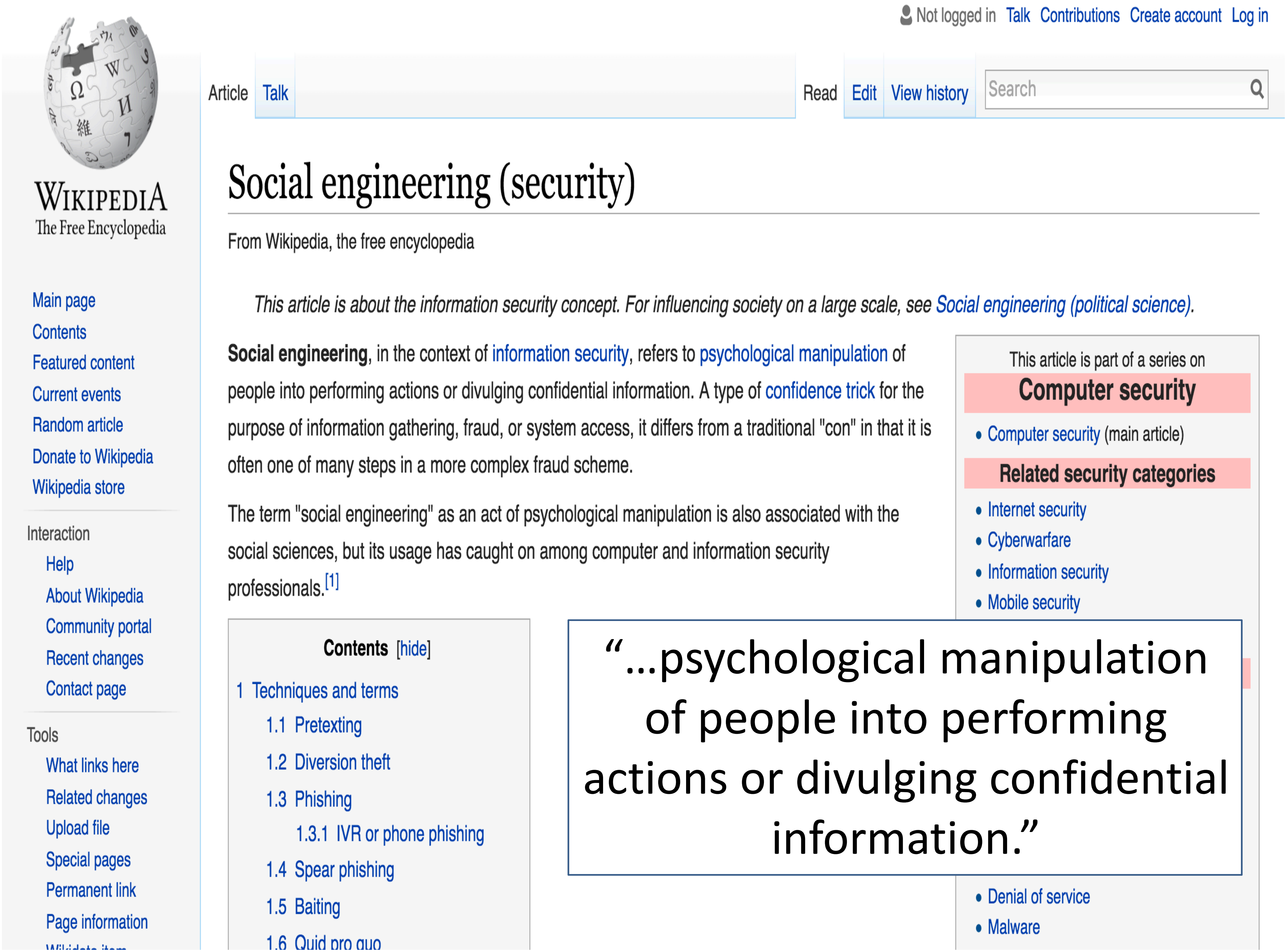
RELATED STORIES

Security
FCC imposes new consumer privacy rules on ISPs

Security
Mozilla pushes the White House to do more to prevent cyberattacks

Security
New code injection method exposes all versions of Windows to cyberattack

Social Engineering



Not logged in Talk Contributions Create account Log in

Article Talk

Read Edit View history Search

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item

Social engineering (security)

From Wikipedia, the free encyclopedia

This article is about the information security concept. For influencing society on a large scale, see Social engineering (political science).

This article is part of a series on

Computer security

- Computer security (main article)

Related security categories

- Internet security
- Cyberwarfare
- Information security
- Mobile security
- Denial of service
- Malware

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

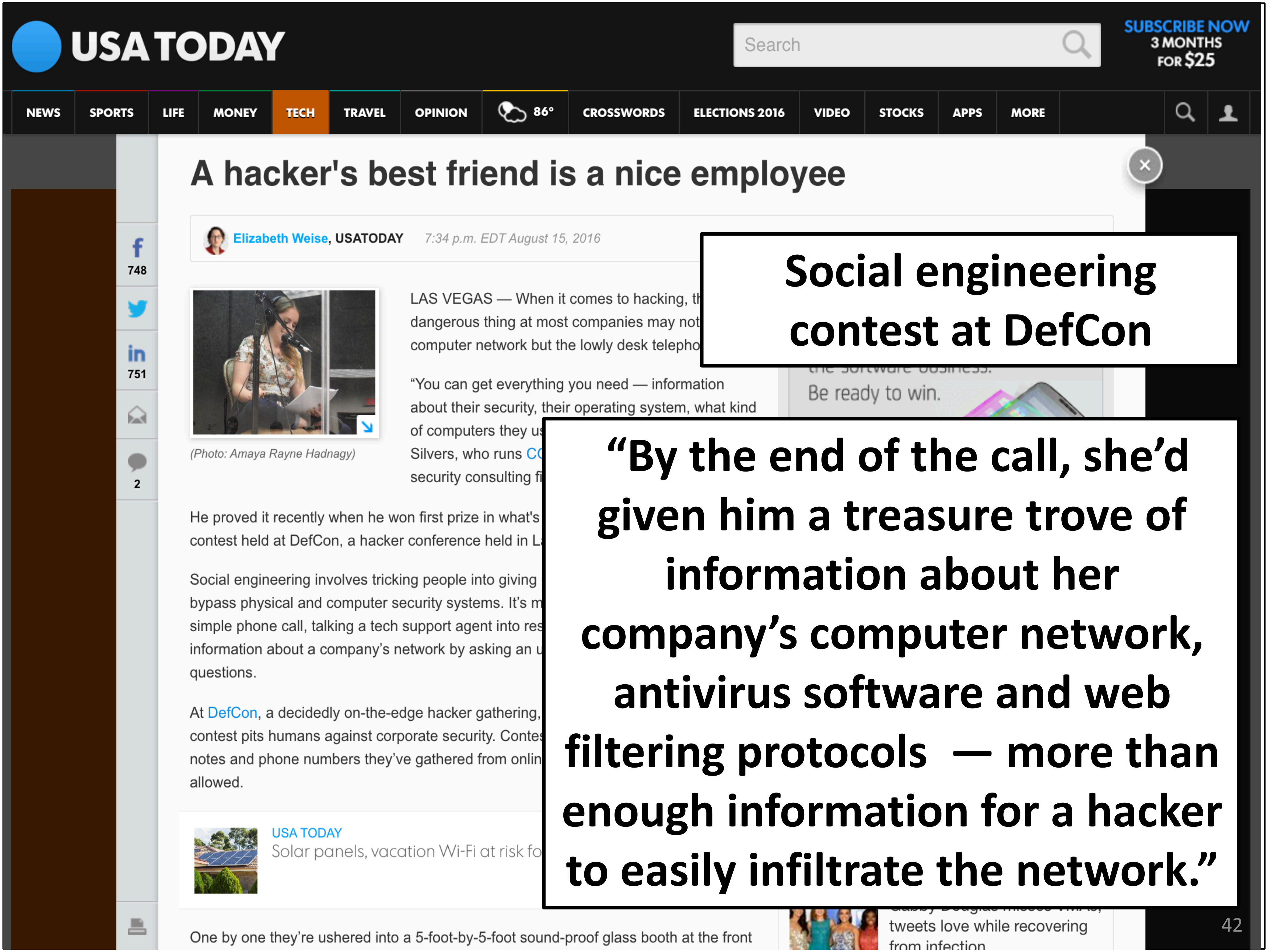
The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals.[1]

Contents [hide]

"…psychological manipulation of people into performing actions or divulging confidential information."

Social engineering contest at DefCon

“By the end of the call, she’d given him a treasure trove of information about her company’s computer network, antivirus software and web filtering protocols — more than enough information for a hacker to easily infiltrate the network.”



A hacker's best friend is a nice employee

Elizabeth Weise, USATODAY 7:34 p.m. EDT August 15, 2016

(Photo: Amaya Rayne Hadnagy)

LAS VEGAS — When it comes to hacking, th
dangerous thing at most companies may not
computer network but the lowly desk telepho

“You can get everything you need — information
about their security, their operating system, what kind
of computers they us
Silvers, who runs CO
security consulting fi

He proved it recently when he won first prize in what's
contest held at DefCon, a hacker conference held in L

Social engineering involves tricking people into giving
bypass physical and computer security systems. It’s m
simple phone call, talking a tech support agent into res
information about a company’s network by asking an u
questions.

At DefCon, a decidedly on-the-edge hacker gathering,
contest pits humans against corporate security. Contes
notes and phone numbers they’ve gathered from onlin
allowed.

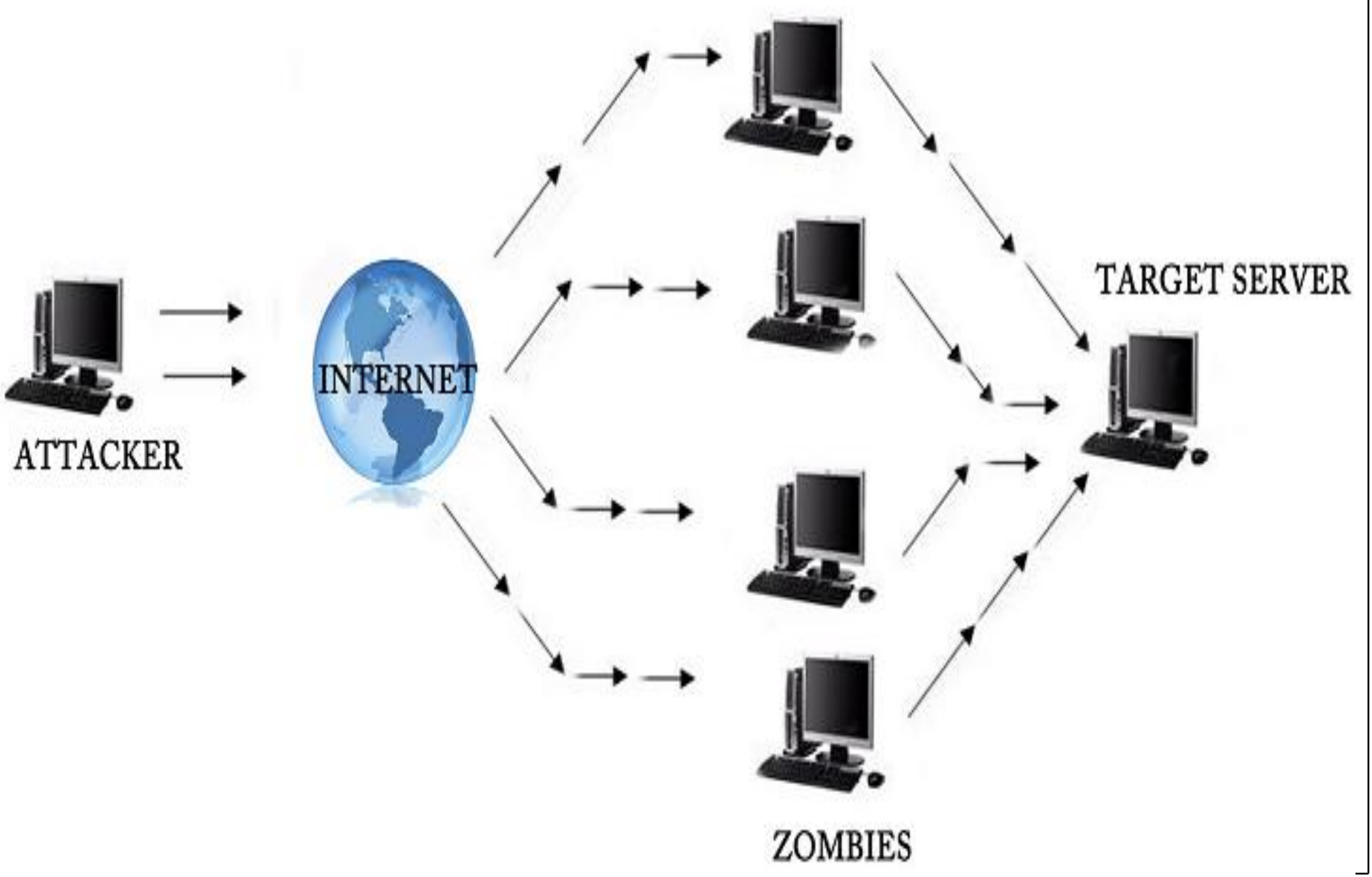
USA TODAY
Solar panels, vacation Wi-Fi at risk fo

One by one they’re ushered into a 5-foot-by-5-foot sound-proof glass booth at the front

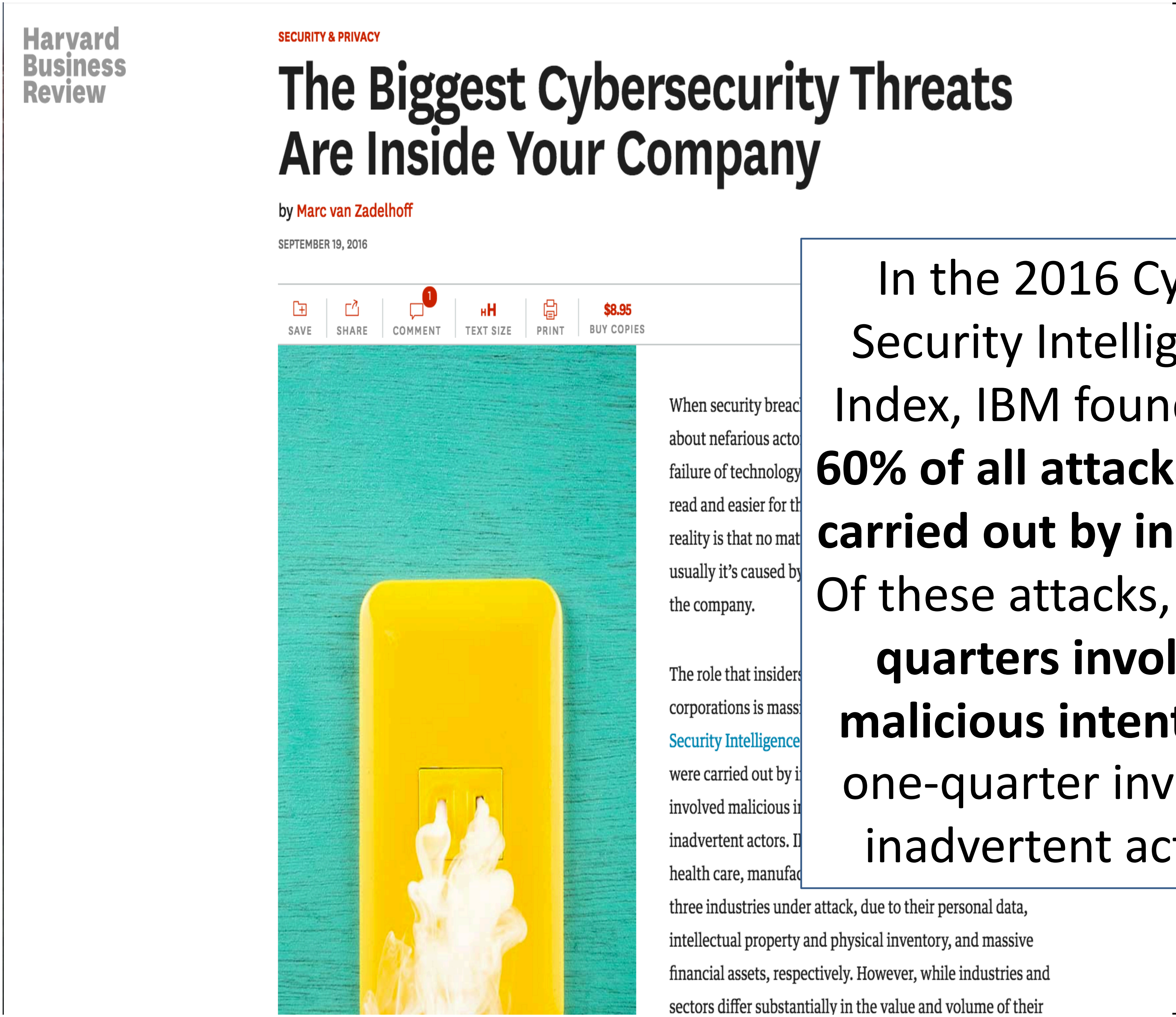
tweets love while recovering
from infection

DoS, DDoS Attacks

DENIAL OF SERVICE ATTACK



Insiders



Harvard Business Review

SECURITY & PRIVACY

The Biggest Cybersecurity Threats Are Inside Your Company

by Marc van Zadelhoff

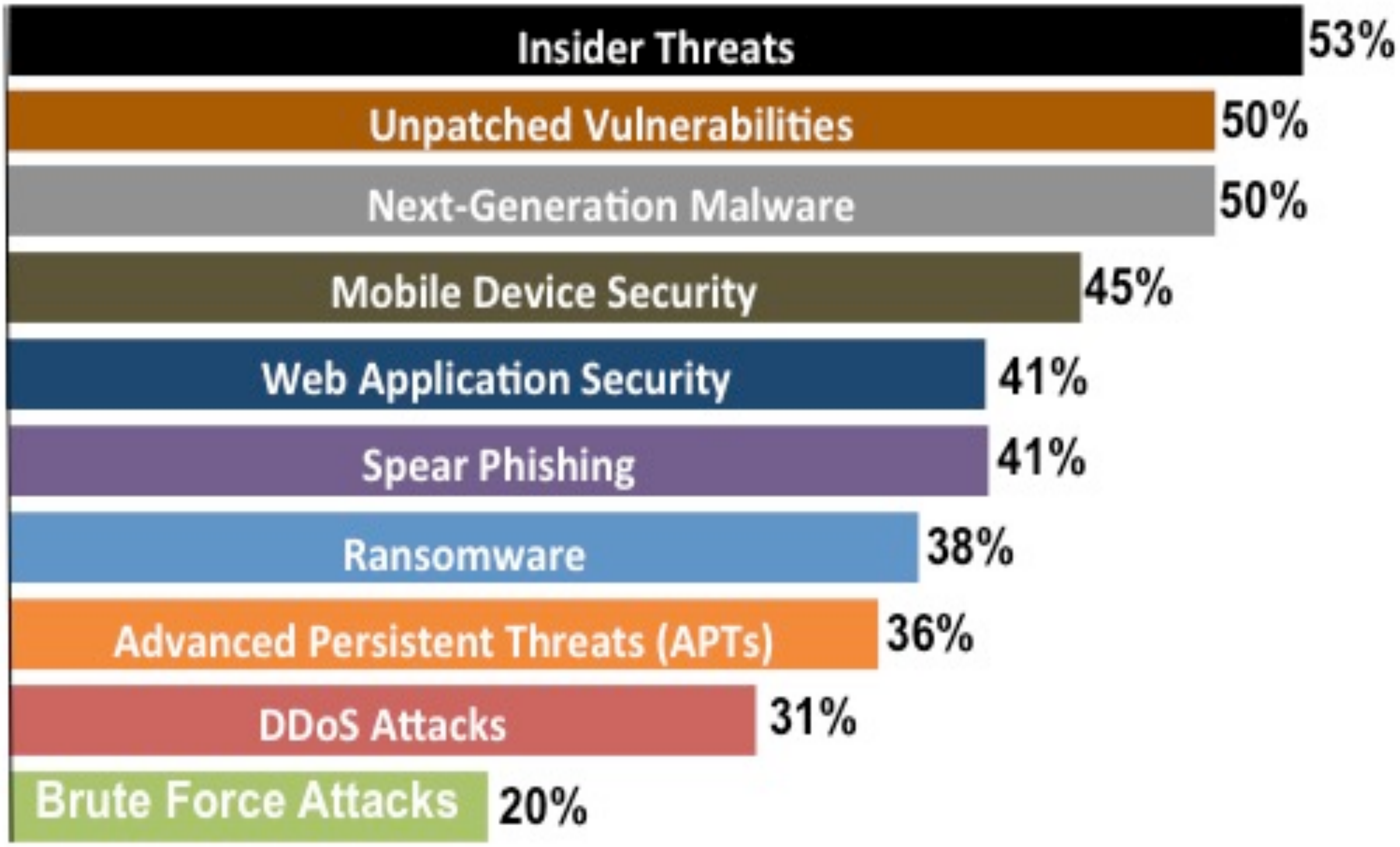
SEPTEMBER 19, 2016

When security breac
about nefarious acto
failure of technology
read and easier for th
reality is that no mat
usually it's caused by
the company.

The role that insiders
corporations is massi
Security Intelligence
were carried out by i
involved malicious i
inadvertent actors. I
health care, manufac
three industries under attack, due to their personal data, intellectual property and physical inventory, and massive financial assets, respectively. However, while industries and sectors differ substantially in the value and volume of their

In the 2016 Cyber Security Intelligence Index, IBM found that **60% of all attacks were carried out by insiders**. Of these attacks, **three-quarters involved malicious intent**, and one-quarter involved inadvertent actors.

What Will Keep IT Security Professionals Up at Night in 2016?



Source: Proficio 2016 Cybersecurity Survey

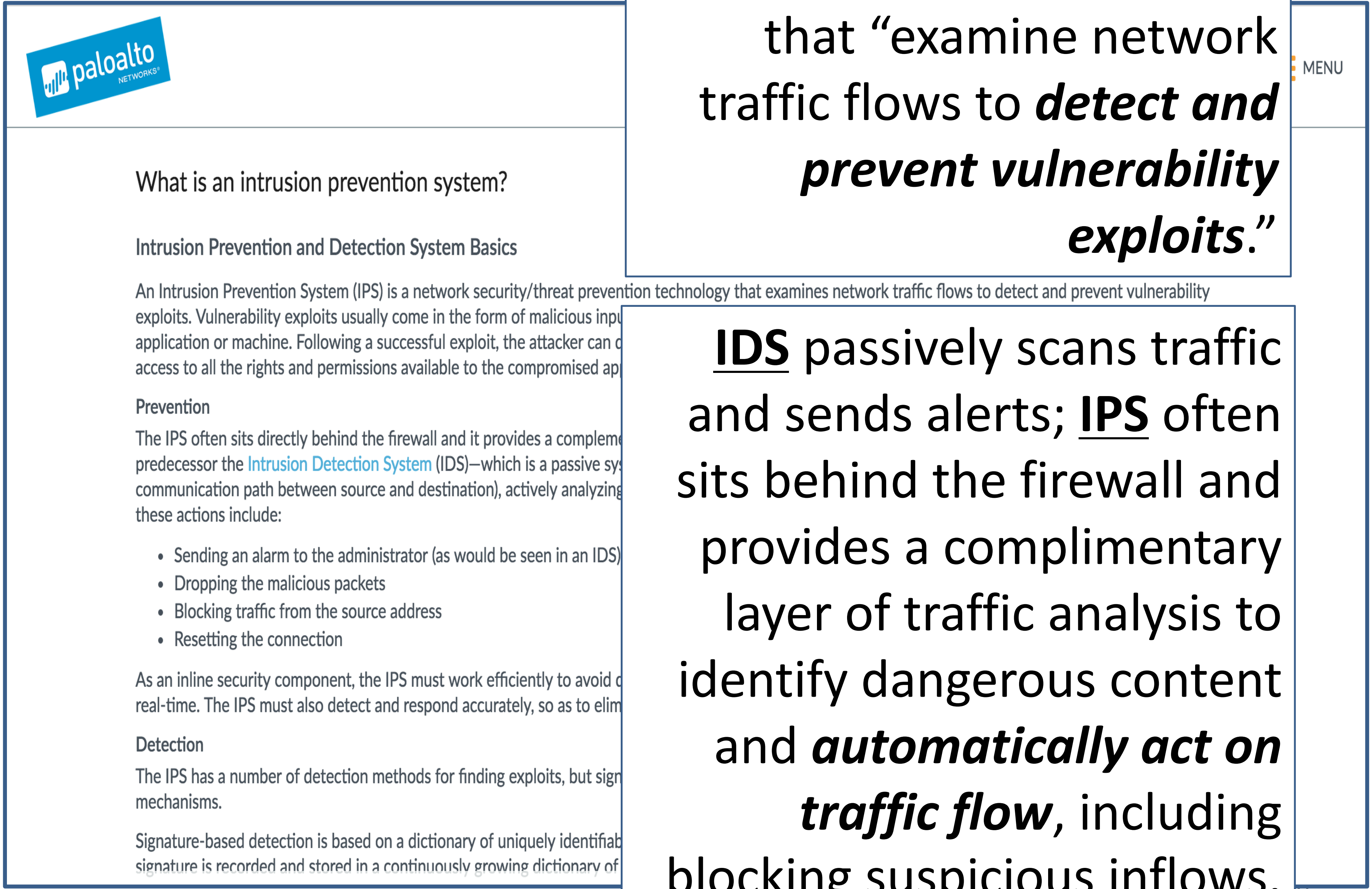
Defenses

Defenses

Technical	Non-Technical
IPS / IDS	Cultural awareness & training
Firewall	Incident / breach response, preparedness
DR / backup (DLP)	BOD / leadership engagement
Storage	Resources / Infosec Plan
Encryption	Insurance

Firewall/Encryption/IPS/IDS

IPS/IDS are technologies that "examine network traffic flows to ***detect and prevent vulnerability exploits***."



What is an intrusion prevention system?

Intrusion Prevention and Detection System Basics

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inpu
application or machine. Following a successful exploit, the attacker can d
access to all the rights and permissions available to the compromised ap

Prevention

The IPS often sits directly behind the firewall and it provides a compleme
predecessor the Intrusion Detection System (IDS)—which is a passive sys
communication path between source and destination), actively analyzing
these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

As an inline security component, the IPS must work efficiently to avoid d
real-time. The IPS must also detect and respond accurately, so as to elim

Detection

The IPS has a number of detection methods for finding exploits, but sign
mechanisms.

Signature-based detection is based on a dictionary of uniquely identifiab
signature is recorded and stored in a continuously growing dictionary of

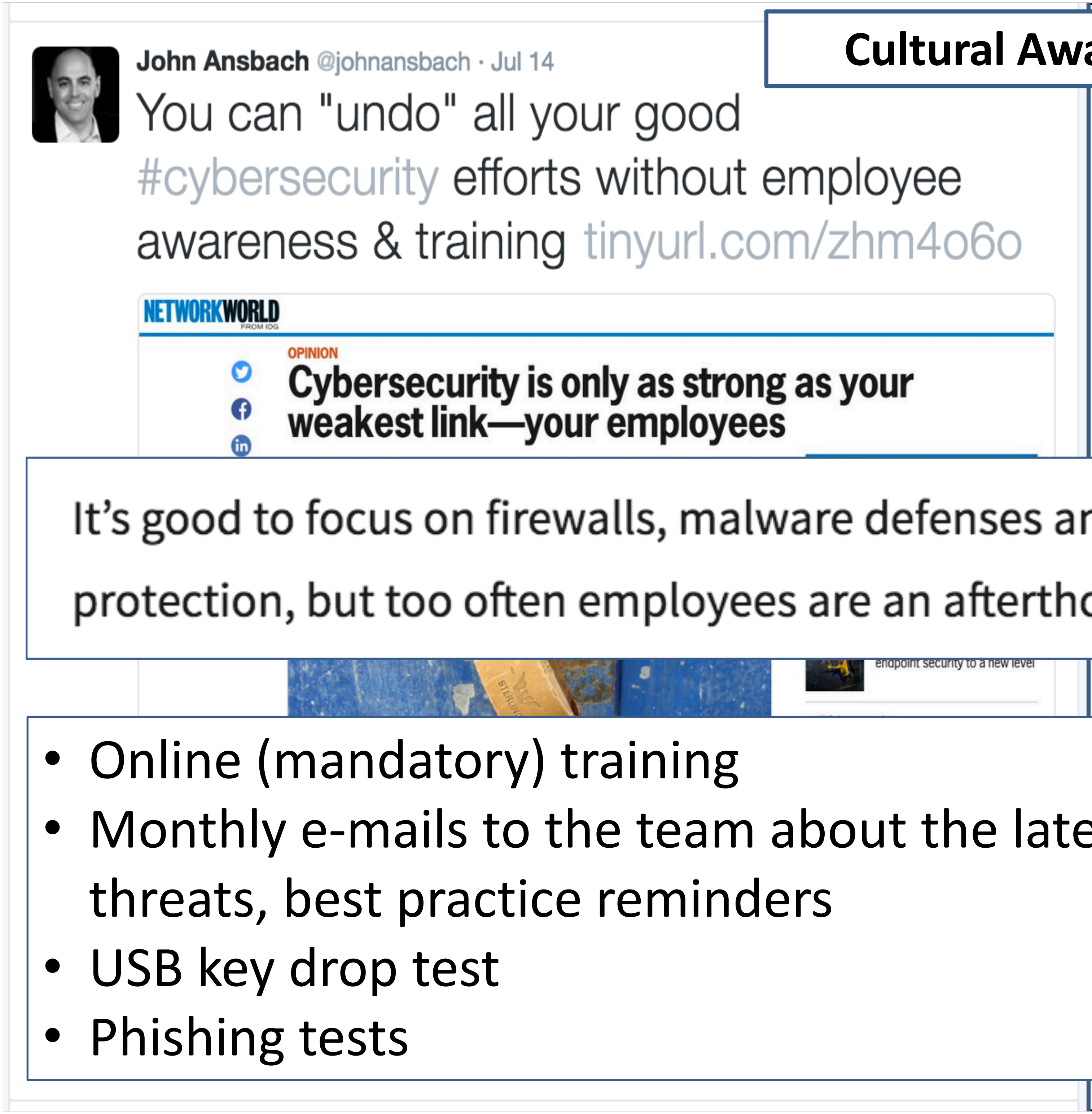
__IDS__ passively scans traffic and sends alerts; __IPS__ often sits behind the firewall and provides a complimentary layer of traffic analysis to identify dangerous content and ***automatically act on traffic flow***, including blocking suspicious inflows.

DR / storage / backup (DLP)

These are technologies designed to help an organizati the loss of data through backup and recovery efforts

- Once the attack has been detected, stopped and the intruders extricated from your systems, you'll begin assessing the damage.
- To do this, you'll need to have had plenty of **storage** to back up to prior system snapshots; you will need to have had processes that were capable of watching and **logging network traffic** to understand exactly what happened. And, in the case of a ransomware attack, you may want the ability to **completely restart your system** from scratch, in which case you will want to have had a full backup of your network and data.
- All of this requires a good conversation with IT professionals so you can explain the business goals and they can provide the HW and W recommended solutions to accomplish those goals.

Cultural Awareness & Training



John Ansbach @johnansbach · Jul 14

You can "undo" all your good #cybersecurity efforts without employee awareness & training tinyurl.com/zhm4o6o

NETWORKWORLD FROM IDG

OPINION

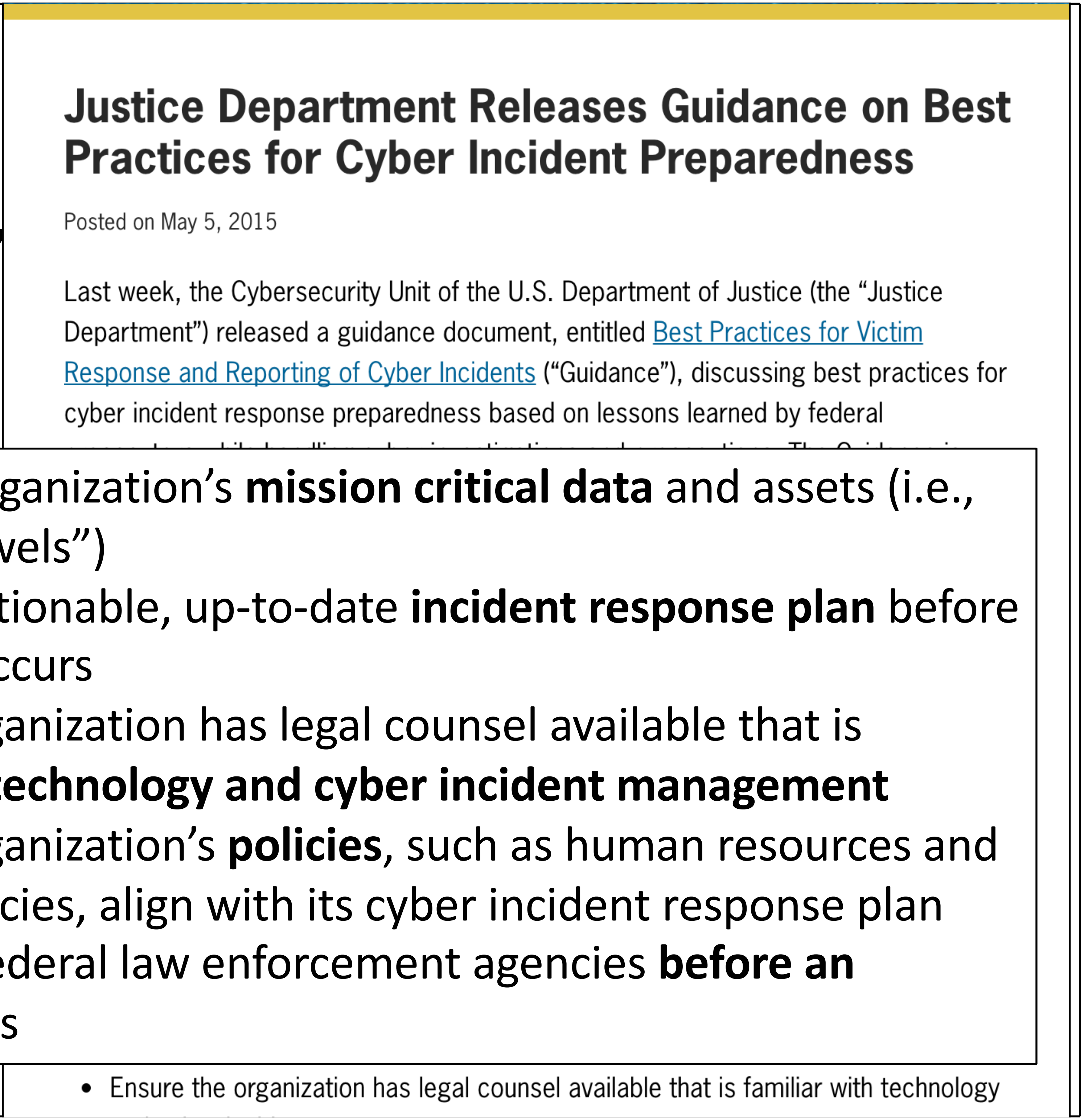
Cybersecurity is only as strong as your weakest link—your employees

endpoint security to a new level

It's good to focus on firewalls, malware defenses and data protection, but too often employees are an afterthought.

- Online (mandatory) training
- Monthly e-mails to the team about the latest threats, best practice reminders
- USB key drop test
- Phishing tests

Breach response, preparedness, training



Justice Department Releases Guidance on Best Practices for Cyber Incident Preparedness

Posted on May 5, 2015

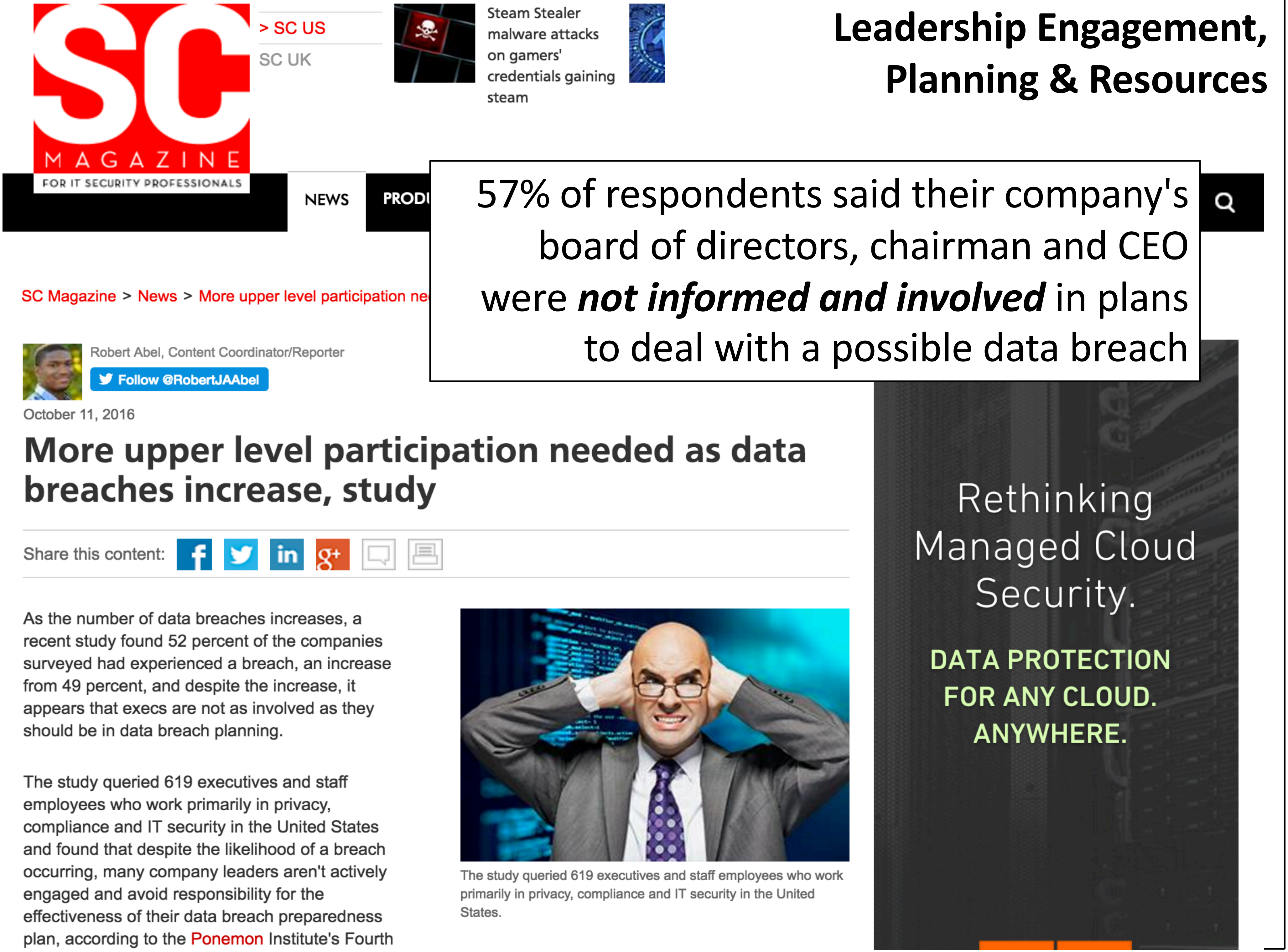
Last week, the Cybersecurity Unit of the U.S. Department of Justice (the "Justice Department") released a guidance document, entitled Best Practices for Victim Response and Reporting of Cyber Incidents ("Guidance"), discussing best practices for cyber incident response preparedness based on lessons learned by federal

- Identify the organization's **mission critical data** and assets (i.e., the "crown jewels")
- Develop an actionable, up-to-date **incident response plan** before an intrusion occurs
- Ensure the organization has legal counsel available that is **familiar with technology and cyber incident management**
- Ensure the organization's **policies**, such as human resources and personnel policies, align with its cyber incident response plan
- Engage with federal law enforcement agencies **before an incident** occurs

- Ensure the organization has legal counsel available that is familiar with technology

Leadership Engagement, Planning & Resources

57% of respondents said their company's board of directors, chairman and CEO were ***not informed and involved*** in plans to deal with a possible data breach



SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

SC Magazine > News > More upper level participation ne

Robert Abel, Content Coordinator/Reporter
Follow @RobertJAAbel

October 11, 2016

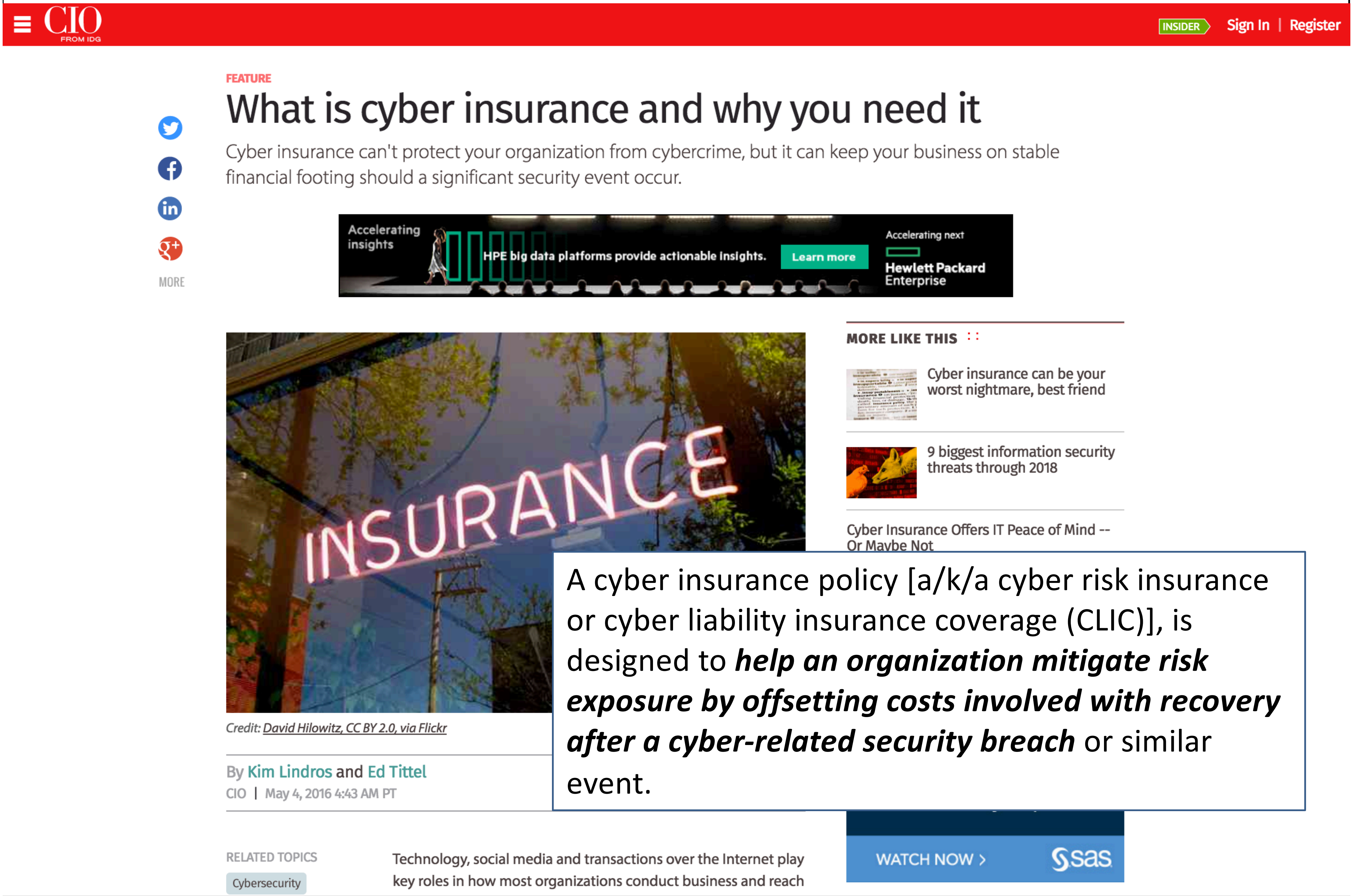
More upper level participation needed as data breaches increase, study

As the number of data breaches increases, a recent study found 52 percent of the companies surveyed had experienced a breach, an increase from 49 percent, and despite the increase, it appears that execs are not as involved as they should be in data breach planning.

The study queried 619 executives and staff employees who work primarily in privacy, compliance and IT security in the United States and found that despite the likelihood of a breach occurring, many company leaders aren't actively engaged and avoid responsibility for the effectiveness of their data breach preparedness plan, according to the Ponemon Institute's Fourth

The study queried 619 executives and staff employees who work primarily in privacy, compliance and IT security in the United States.

Cyber insurance



FEATURE

What is cyber insurance and why you need it

Cyber insurance can't protect your organization from cybercrime, but it can keep your business on stable financial footing should a significant security event occur.

MORE LIKE THIS

- Cyber insurance can be your worst nightmare, best friend
- 9 biggest information security threats through 2018
- Cyber Insurance Offers IT Peace of Mind -- Or Maybe Not

Credit: David Hilowitz, CC BY 2.0, via Flickr

By Kim Lindros and Ed Tittel

CIO | May 4, 2016 4:43 AM PT

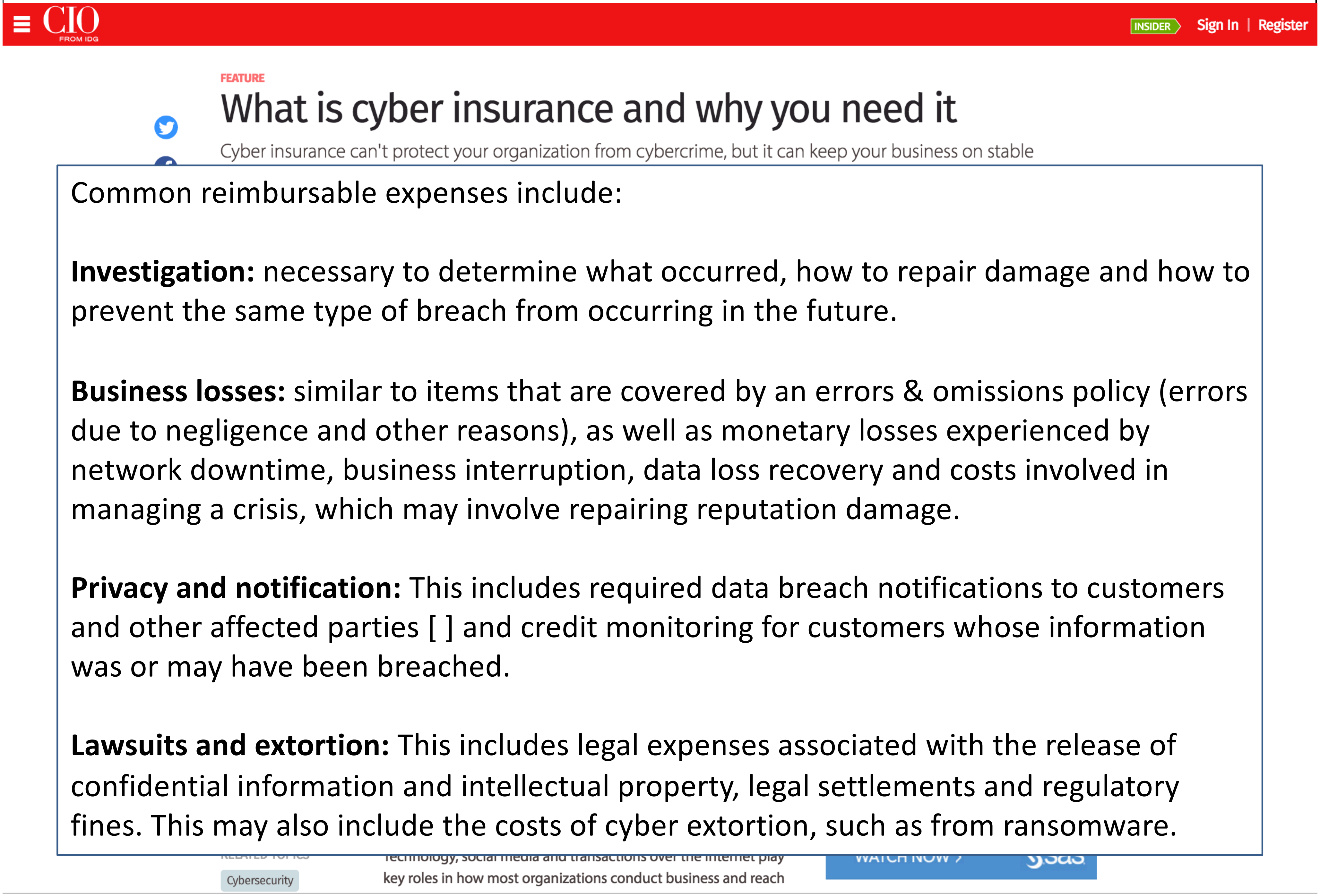
RELATED TOPICS

Cybersecurity

Technology, social media and transactions over the Internet play key roles in how most organizations conduct business and reach

A cyber insurance policy [a/k/a cyber risk insurance or cyber liability insurance coverage (CLIC)], is designed to ***help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach*** or similar event.

Cyber insurance



What is cyber insurance and why you need it

Cyber insurance can't protect your organization from cybercrime, but it can keep your business on stable

Common reimbursable expenses include:

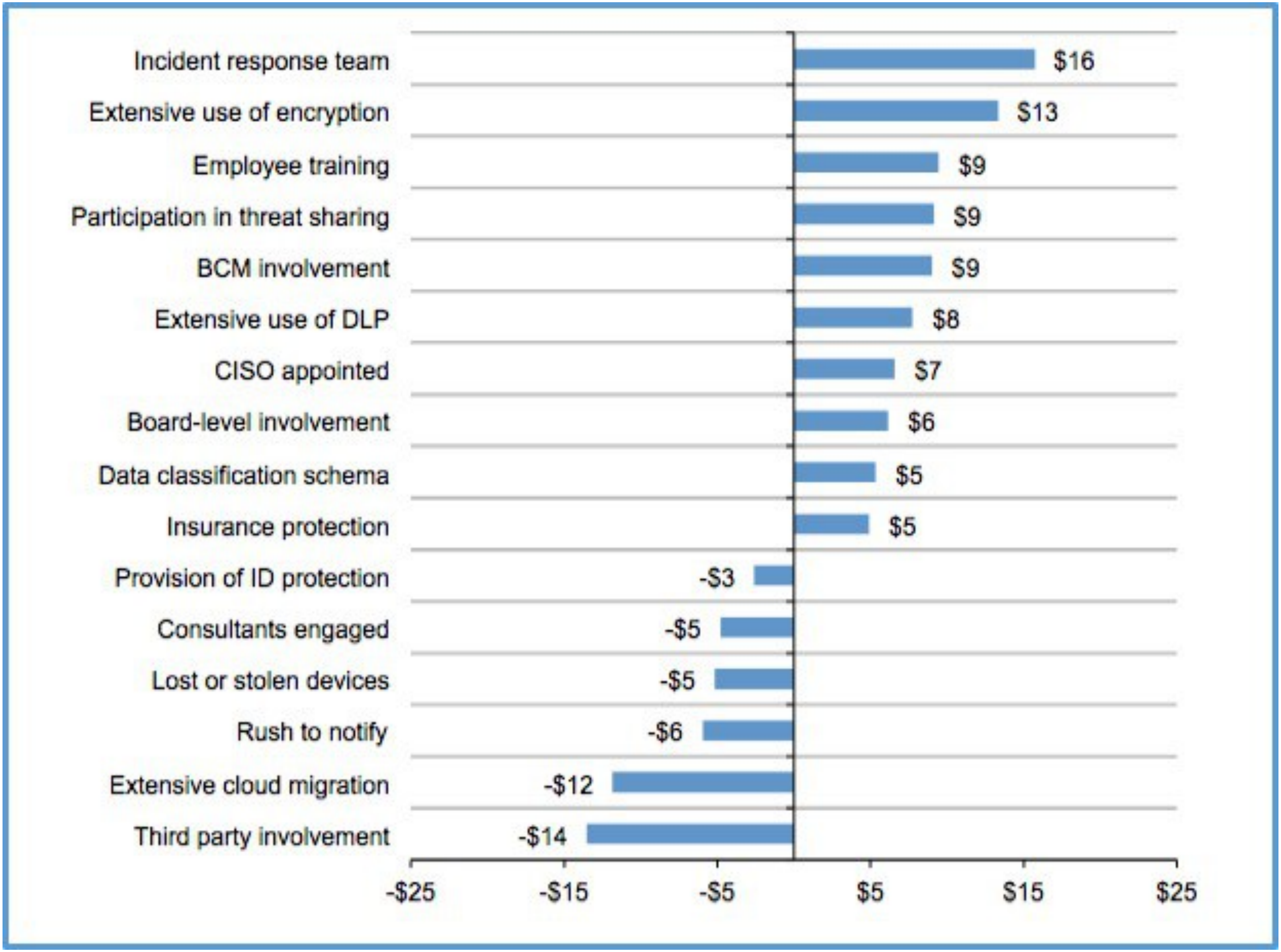
Investigation: necessary to determine what occurred, how to repair damage and how to prevent the same type of breach from occurring in the future.

Business losses: similar to items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.

Privacy and notification: This includes required data breach notifications to customers and other affected parties [ ] and credit monitoring for customers whose information was or may have been breached.

Lawsuits and extortion: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware.

Technology, social media and transactions over the internet play key roles in how most organizations conduct business and reach


Incident response team
$16
Extensive use of encryption
$13
Employee training
$9
Participation in threat sharing
$9
BCM involvement
$9
Extensive use of DLP
$8
CISO appointed
$7
Board-level involvement
$6
Data classification schema
$5
Insurance protection
$5
Provision of ID protection
-$3
Consultants engaged
-$5
Lost or stolen devices
-$5
Rush to notify
-$6
Extensive cloud migration
-$12
Third party involvement
-$14
-$25
-$15
-$5
$5
$15
$25

Tips & Takeaways

Cybersecurity Tips & Takeaways (General)

1. Change default settings, including admin account/password, as soon as you put new equipment / gadgets into service.
2. Don't use a thumb drive from an unknown source; it may contain malware!
3. Close browsers immediately after use, frequently delete website search history.
4. Think before you click / don't click a web link that is embedded in an email.
5. Confirm the email address by hovering over the sender's name, even if it is from a trusted person.

Source: Nancy Cantwell, Sr. VP, Blue Ridge Networks

Cybersecurity Tips & Takeaways (General)

6. Never assume an email is legit if the email asks you to download a file that does not make sense, asks you to send money, or send info.

7. Use phrases as passwords rather than 4-8 numbers, symbols and/or letters & change passwords frequently

8. Use security questions where the answers cannot be discovered by public records, or by looking at your LinkedIn/FB page

9. Don't give out your SSN and date of birth at the same time, even to medical practitioners.

10. Use top-rated *prevention* software like AppGuard

Source: Nancy Cantwell, Sr. VP, Blue Ridge Networks

Cybersecurity Tips & Takeaways (for the workplace)

1. Have an incident response plan
2. Train employees
3. Back up your files – if you suffer a ransomware attack, you can refuse to pay and restore your files/system to your latest backup.
4. When you walk away from your computer at work, log out!
5. Always be wary of / double check emails from a “CEO” or “President” (roughly 1/2 of all BEC scams come from a “CEO” or “President”).

Cybersecurity Tips & Takeaways (for the workplace)

6. Be wary/ train your people to be wary of phone calls seeking information – these “low tech” attacks often are advance scouting work of an impending cyberattack or spear phish.

7. Don't assume you can visit a website, not click on anything, and be “safe.” “Drive by” attacks can still install malware on your PC!

8. Use multi-factor authentication tools like LastPass or Ubikey.

9. Ask about email encryption tools that might work for you & your organization.

10. Always report suspicious emails, websites, to your IT/HR folks.

John Ansbach
General Counsel
General Datatech, L.P.
@johnansbach
jansbach@gdt.com