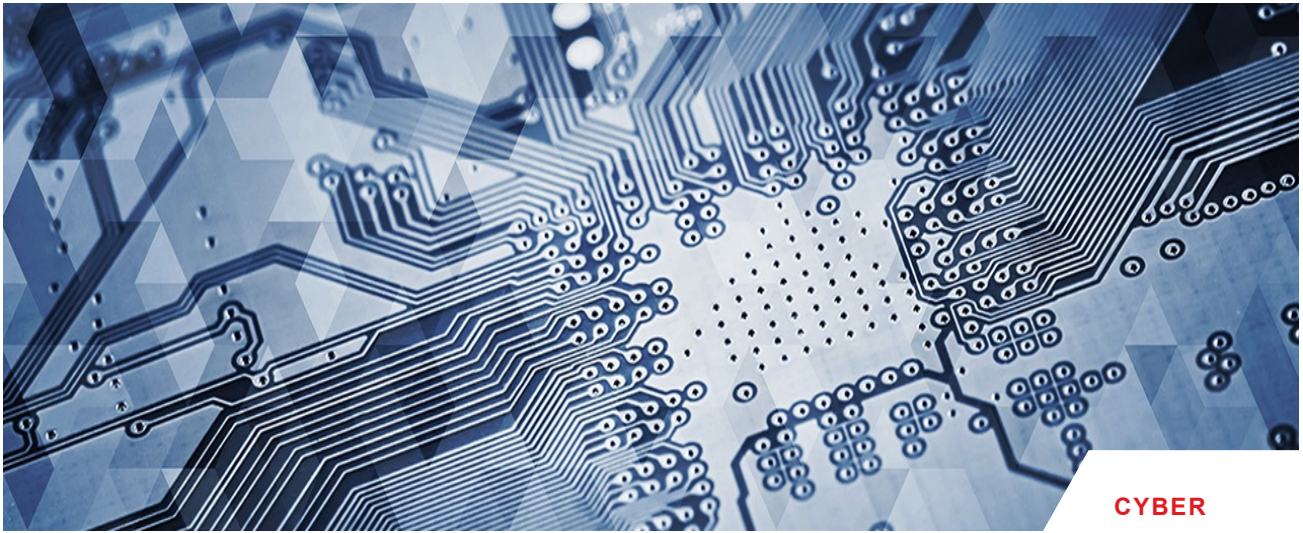


Cyber *In*security

What you Can do Now to Help Keep Your Organization Safe

John Ansbach, JD, CIPP-US
@johnansbach
jansbach@strozfriedberg.com

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

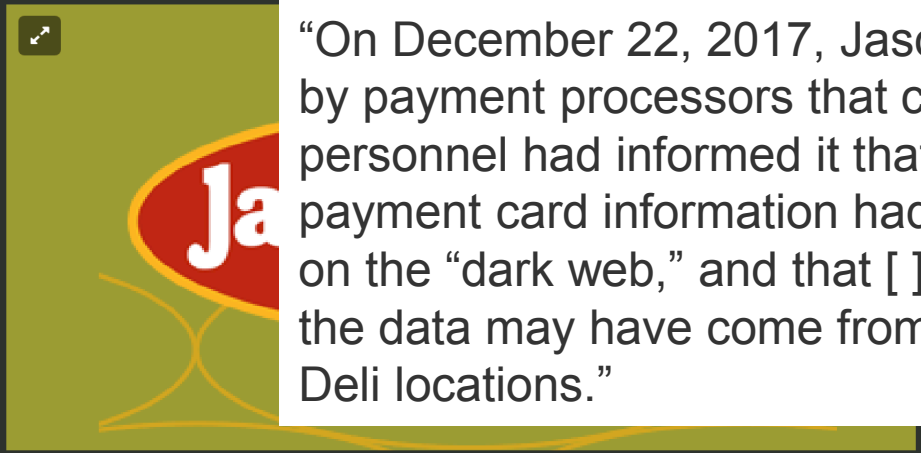

A new data leak hits Aadhaar, India's national ID database
Exclusive: The data leak affects potentially every Indian citizen subscribed to the database.
By Zack Whittaker for Zero Day | March 23, 2018 -- 20:00 GMT (13:00 PDT) | Topic: Mobility
Top 10 Breaches through July 2018 exposed roughly 1.9 billion records

TOP STORY

Jason's Deli identifies 164 locations affected by Dec. 2017 data breach

By Ronnie Marley, Digital Content Manager Jan 18, 2018 Updated Jan 18, 2018

Jan 18, 2018



(Source: Facebook)

"On December 22, 2017, Jason's Deli was notified by payment processors that credit card security personnel had informed it that a large quantity of payment card information had appeared for sale on the "dark web," and that [ ] at least a portion of the data may have come from various Jason's Deli locations."

- Woman found dead outside the courthouse in Live Oak

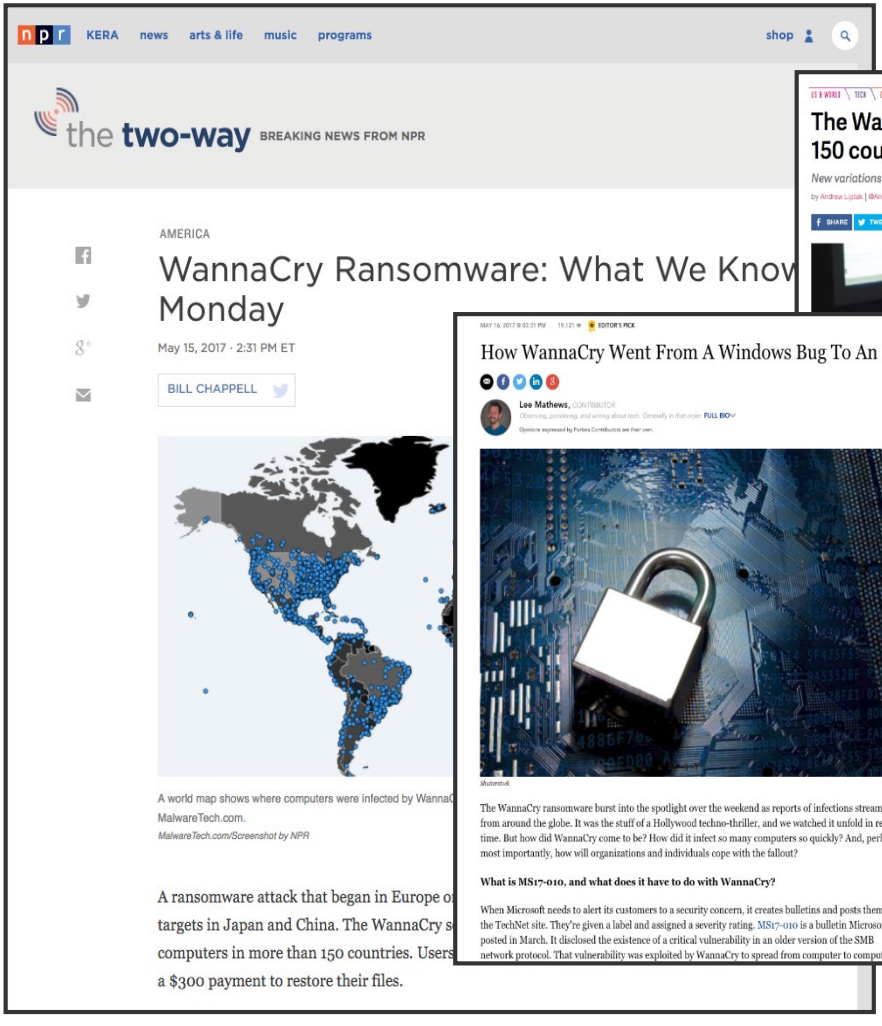
"…criminals used [ ] malware to obtain payment card information off of the POS terminals beginning on June 8, 2017… approximately ***2 million unique payment card numbers*** may have been impacted…"

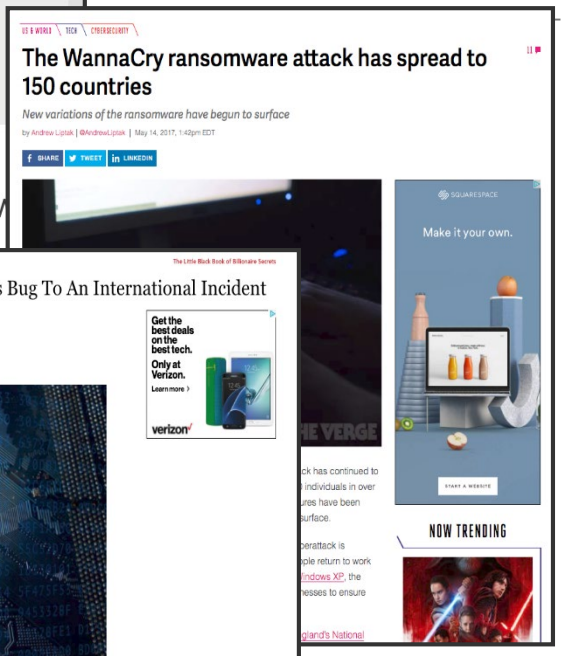
(KWES) - Jason's Deli has release
2017.

The list, which is posted on their

The locations are in Alabama, Ar
Nevada, Pennsylvania, South Ca

In a statement, Jason's Deli said, "a large quantity of payment card information had appeared for sale on the


npr KERA news arts & life music programs shop
the two-way BREAKING NEWS FROM NPR
AMERICA
WannaCry Ransomware: What We Know
Monday
May 15, 2017 · 2:31 PM ET
BILL CHAPPELL
A world map shows where computers were infected by WannaC
MalwareTech.com.
MalwareTech.com/Screenshot by NPR
A ransomware attack that began in Europe o
targets in Japan and China. The WannaCry s
computers in more than 150 countries. Users
a $300 payment to restore their files.


US & WORLD TECH CYBERSECURITY
The WannaCry ransomware attack has spread to 150 countries
New variations of the ransomware have begun to surface
by Andrew Liptak | @AndrewLiptak | May 14, 2017, 1:42pm EDT
SHARE TWEET LINKEDIN
SQUARESPACE
Make it your own.
START A WEBSITE
NOW TRENDING

How WannaCry Went From A Windows Bug To An International Incident
Lee Mathews, CONTRIBUTOR
Get the best deals on the best tech.
Only at Verizon.
Learn more
verizon
Shutterstock
The WannaCry ransomware burst into the spotlight over the weekend as reports of infections streamed in from around the globe. It was the stuff of a Hollywood techno-thriller, and we watched it unfold in real time. But how did WannaCry come to be? How did it infect so many computers so quickly? And, perhaps most importantly, how will organizations and individuals cope with the fallout?
What is MS17-010, and what does it have to do with WannaCry?
When Microsoft needs to alert its customers to a security concern, it creates bulletins and posts them to the TechNet site. They're given a label and assigned a severity rating. MS17-010 is a bulletin Microsoft posted in March. It disclosed the existence of a critical vulnerability in an older version of the SMB network protocol. That vulnerability was exploited by WannaCry to spread from computer to computer.
And everything in between.
verizon


Center for American Progress

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 respo
Powell and the Democratic National Committee (DNC). SecureWorks, an ent
command and control servers and uncovered who Fancy Bear targeted and
account. They identified approximately 3,900 targeted individuals in go
companies in military and government supply chains, journalists, peo
Clinton's campaign organization like Podesta. Fancy Bear used a spe

Phishing, spear phishing and the Podesta hack

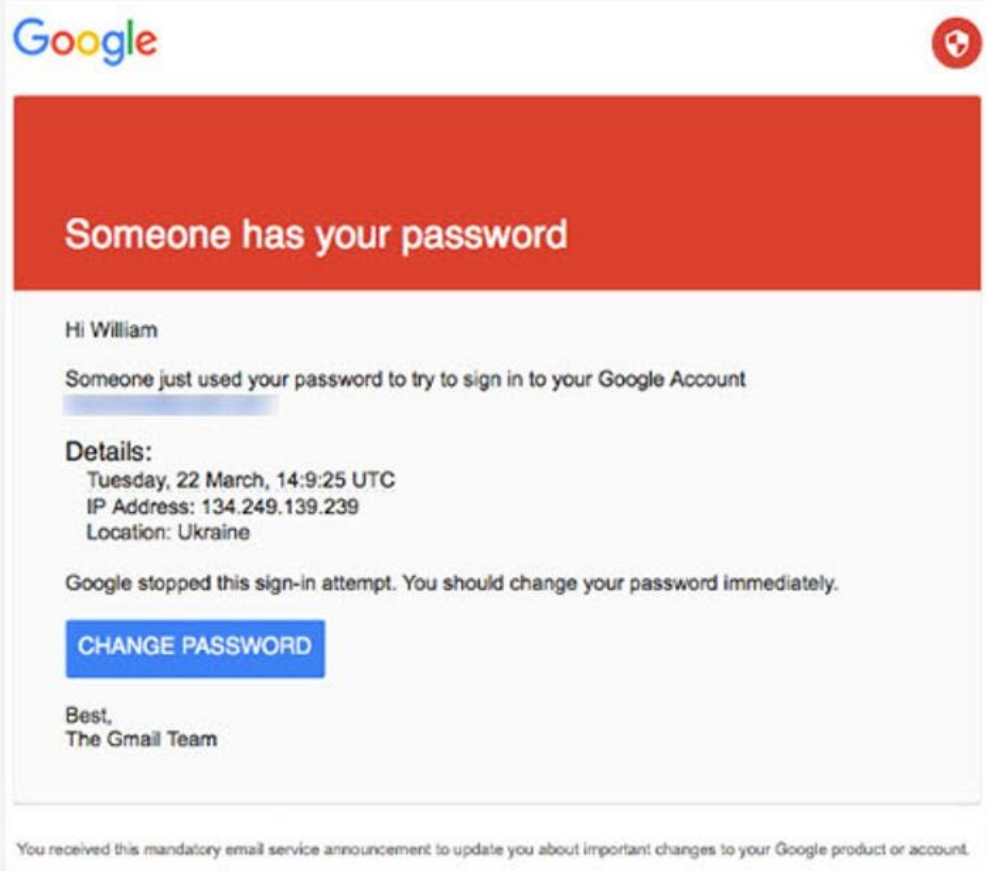
Phishing scams try to trick people into giving up information , or bank ac
emails that falsely claim to be from a "trusted" source. An example of phishing is t
which an email promised to gift you with a lot of money if you would give up your banki
someone move money out of Nigeria. Phishing attacks are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

Spear-phishing is a more sophisticated form of phishing that targets individuals using p
spear-phasing email purports to come from a friend, a company you do business with su

"…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."



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

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 Am

"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."

As reported by Motherboard, the Russian hacking group Fancy Bear
Powell and the Democratic National Committee (DNC). SecureWorks, an enterprise sec
command and control servers and uncovered who Fancy Bear targeted and how they we
account. They identified approximately 3,900 targeted individuals in government, the n
companies in military and government supply chains, journalists, people who worked fo
Clinton's campaign organization like Podesta. Fancy Bear used a spear-phishing campa

Phishing, spear phishing and the Podesta hack

Phishing scams try to trick people into giving up information like passwords, or bank account and credit card numbers through emails that falsely claim to be from a "trusted" source. An early example of phishing is the notorious Nigerian bank scam in which an email promised to gift you with a lot of money if you would give up your banking information in order to help 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

SECTIONS

Deseret News Utah

LOGIN

Utah Food Bank security breach exposes 10,000 donors' personal info

By Katie McKellar @KatieMcKellar1
Published: August 29, 2015 7:50 pm
Updated: Aug. 29, 2015 9:34 p.m.

Leave a comment

Laura Seitz, Deseret News

Bread products are given away at the Utah Food Bank in Salt Lake City on Wednesday, Dec. 5, 20

SALT LAKE CITY — A security breach in the Utah … website may have resulted in the disclosure of more than 10,000 donors' personal information.

In a letter that was sent to a donor on Tuesday and obtained by the Deseret News, Utah Food Bank officials said they recently discovered that an "unauthorized individual" may have gained access to donation information submitted through the organization's website between Oct. 8, 2013 and July 16, 2015.

Names, addresses, emails, credit or debit card numbers, security codes and expiration dates may have been exposed during that time period, the letter states.

"A security breach in the Utah Food Bank's website may have resulted in the disclosure of more than **10,000 donors' personal information**…
In a letter that was sent to a donor on Tuesday [ ], Utah Food Bank officials said they recently discovered that an "unauthorized individual" may have gained access to donation information submitted through the organization's **website…Names, addresses, emails, credit or debit card numbers, security codes and expiration dates** may have been exposed during that time period, the letter states."

AON Empower Results®

There may be no greater risk to foundations, charitable giving groups or for-profit enterprise than cyber *in*security.

The question is, what should those organizations - and those that lead and manage them- be doing *right now* to prepare?

Agenda

- Landscape
- Threats
- Defenses
- Tips & Takeaways

Landscape

Landscape

Over 2,300 Data Breaches Disclosed So Far In 2018, Exposing Over 2.6 Billion Records

AUGUST 15, 2018 BY RBS

Risk Based Security today announced the release of its **Mid-Year 2018 Data Breach QuickView report**, showing there have been 2,308 publicly disclosed data compromise events through June 30th. After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more "normal" pace. At the mid-year point, 2018 closely mirrors 2016's breach experience but still trails the high water mark set in 2017.

Key Findings for Mid Year 2018

- 2,308 breaches have been reported through June 30, exposing approximately 2.6 billion records.
- Compared to the midway point in 2017, the number of reported breaches is down from 2,439 breaches and the number of exposed records is down from 6 billion.
- The number of disclosed instances targeting employee W-2 forms remained low, with 42 such breaches reported through Q2 2018 compared to 239 for the same time period 2017.
- The Business sector accounted for 40% of reported breaches, followed by Medical (8.3%), Government (8.2%) and Education (4.5%). Nearly 40% of breached organizations could not be definitively classified.

2,308 publicly disclosed data compromise events through June 30th.

~13 per day

"After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more "normal" pace."

Source: CyberEdge Group 2017

RISING CYBERATTACKS

The percentage of respondents affected by successful attacks has risen the last three years with no end in sight.

Annual number of data breaches and records exposed (in millions) in the United States 2005 - 2016

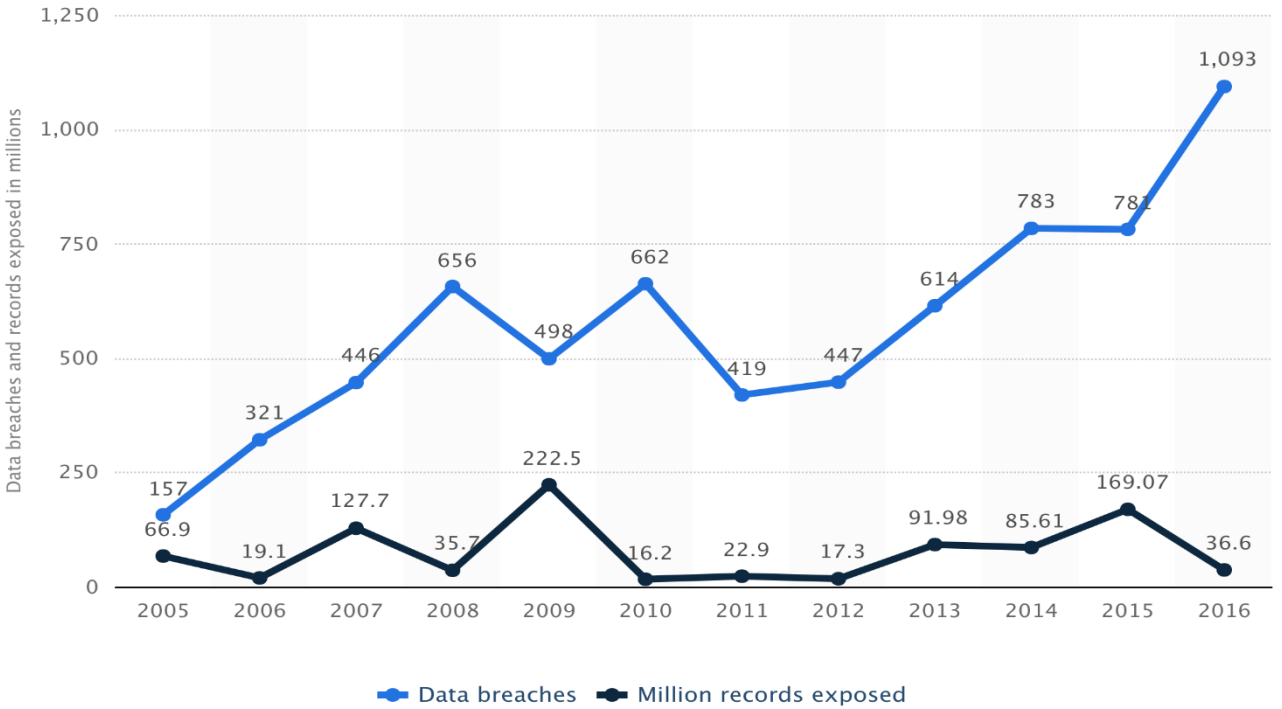
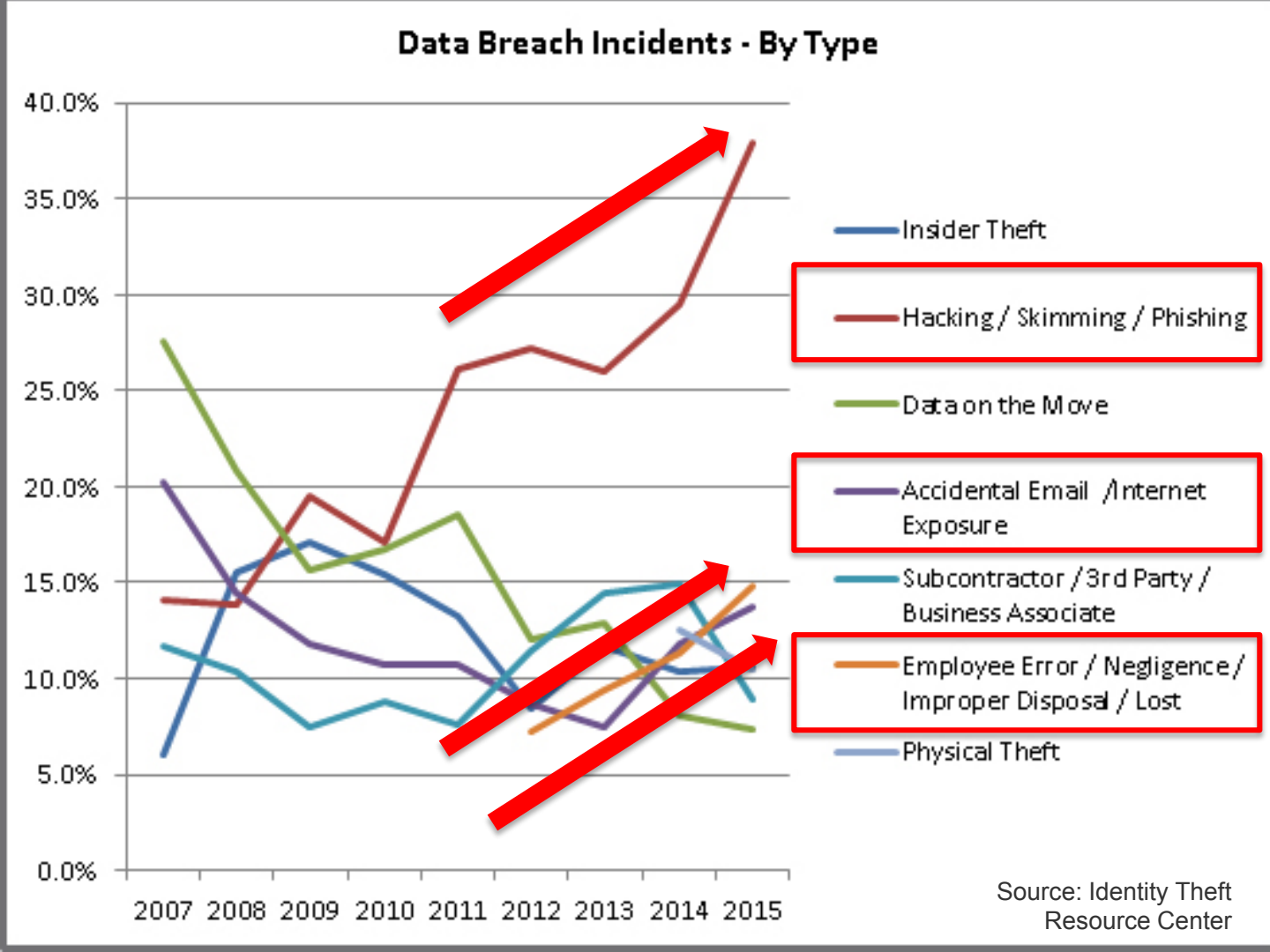
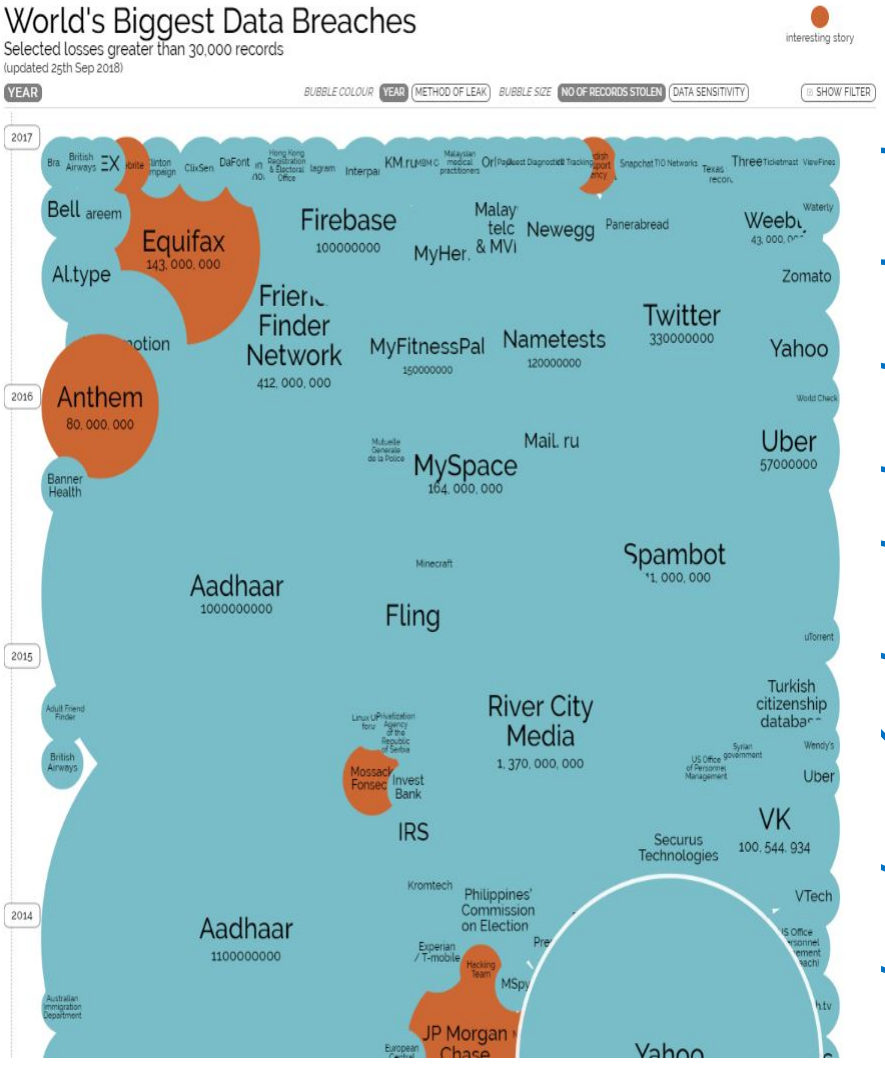


Image via Statista.com.


Data Breach Incidents - By Type
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
2007 2008 2009 2010 2011 2012 2013 2014 2015
Insider Theft
Hacking / Skimming / Phishing
Data on the Move
Accidental Email /Internet Exposure
Subcontractor / 3rd Party / Business Associate
Employee Error / Negligence / Improper Disposal / Lost
Physical Theft
Source: Identity Theft Resource Center



Selected losses greater than 30,000 records (updated Sept 25, 2018)

What about Smaller Organizations?

SMALL BUSINESS

Top

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

The Microsoft Digital Crimes Unit (DCU) states, "Cybercrim
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%** of small to medium sized businesses don't 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."

Small Business TRENDS

MARKETING MANAGEMENT TECHNOLOGY FIN

Trending: Google Microsoft Facebook Small Business Travel

58% of small businesses are concerned about cyberattacks, but more than half (51%) are not allocating *any budget at all* to cyber risk mitigation

CYBER SECURITY STATISTICS – Numb
Need to Know

Jan 3, 2017 by Matt Mansfield In Technology Trends 7

Only 38% regularly upgrade software solutions and only 22% encrypt databases

changed when it comes to HR software. This comprehensive e-Book will act as your guide.
Get It Now >>

60% of small companies go out of business within six months of a cyber attack

We've collected these cyber security statistics for small businesses fro

General Small Business Cyber Security Sta

- 43 percent of cyber attacks target small business.
- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.

Sometimes - depends on circumstances.

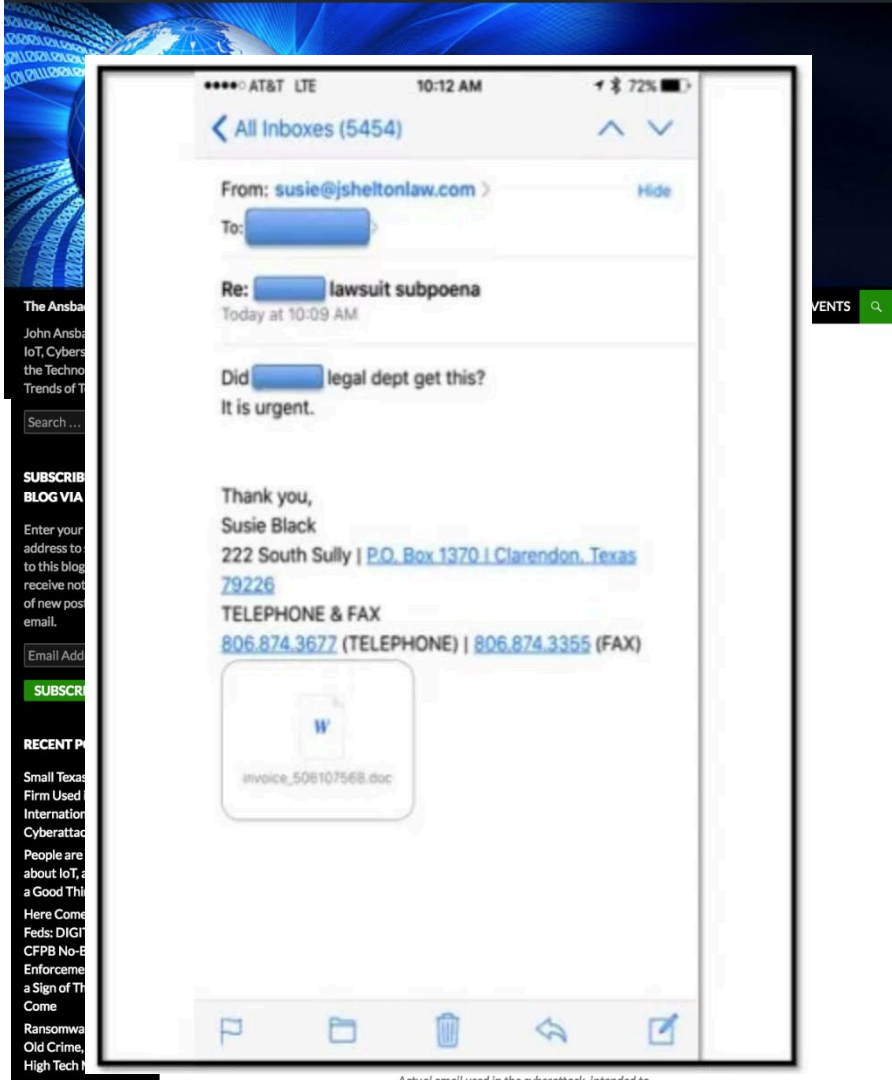
None - I use social media to connect

power Results®

Small Texas Law Firm used as Platform for Int'l Attack

Cybercriminals 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



Breach Costs

2018 IBM/Ponemon Cost a Data Breach Study

U.S. average cost of a data breach	**$7.91 M** ($7.3 M)
World average cost of a data breach	**$3.86 M** ($3.6 M)
World avg. per capit (Per capita cost is the avg. cost of a lost or stolen record compromised in a data breach)	**$148** ($141)
Per capita cost in the U.S.	**$233** (highest; was $225)

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

MUST READ MICROSOFT COMMITS TO DELIVER NEXT OFFICE CLIENT, SERVERS BY SECOND HALF 2018

NotPetya cyber attack on TNT Express cost FedEx $300m

Falling victim to global ransomware attack "posed significant operational challenges", the company says in its latest financial report.

By Danny Palmer | September 20, 2017 -- 16:12 GMT (09:12 PDT) | Topic: Security

Falling victim to Petya is estimated to have cost FedEx $300m.

Image: TNT Express

FedEx has revealed the cost of falling victim to Petya to be an estimated **$300 million** in lost earnings.

While **no data breach or data loss occurred** as a result of Petya, the company previously warned that it may not be able to recover all of the systems affected by the cyber attack.


Security
SEC steps up efforts to fight cyber crime


Security
Are Jared Kushner and Ivanka Trump violating White House email rules? A guide for journalists


Security
Hackers want to crack bank ATM networks - and your nearest cash machine is probably running Windows XP

Reinsurance News

Home | News | Interviews | About | Advertising | Contact

Reinsurance News

Total WannaCry losses pegged at $4 billion

25th September 2017 - Author: Marianne Lehnis

Ransomware attacks have reached a new peak this year, with WannaCry causing estim
financial and economic losses of up to $4 billion and infecting 300,00 machines aroun
according to Trend Micro's security and threats report.

2017s WannaCry and Petya attacks show that cybercriminals are upping their game and diversifying methods to exploit the increasing inter-connectivity of global businesses.

Trend Micro estimates that by 2018, over a million industrial robots will be employed in factories around the world; tests have shown how industrial robots can be compromised through exposed industrial ro
vulnerabilities.

This year's systemic ransomware attacks have demonstrated that cyber crime has alr
same levels of catastrophic loss associated with natural catastrophes or some of the
re/insurers cover.

The capabilities of cybercrime to disrupt the value chain on all levels will continue to d
increase in the near-term future.

The Trend Micro report said; "Businesses still fall for email scams. According to the Fe
Investigation, global losses due to business email compromise (BEC) have reached $5.3 billion.

WannaCry [caused] estimated global financial and economic losses of up to **$4 billion** and infecting 300,000 machines around the world

2017's WannaCry and Petya attacks show that cybercriminals are upping their game and diversifying methods to exploit the increasing inter-connectivity of global businesses

Forbes, July 2017

Forbes CommunityVoice™ Connecting expert communities to the Forbes audience. What is this?

JUL 13, 2017 @ 10:00 AM 1,873

Free W

The True Cost Of Cybercrime For Businesses

YEC

We cover startups, founders and entrepreneur lessons. FULL BIO

Opinions expressed by Forbes Contributors are their own.

POST WRITTEN BY

Nick Eubanks

Nick is a Partner at TrafficSafetyStore.com and the Founder of I'm From The Future.

Shutterstock

It's estimated that cybercrime will cost approximately … through 2021. Tha… that is almost impossible for most people to imagi…

But more concerning than the number itself is what it means for modern businesses. Everywhere, comp… cybersecurity budgets in an attempt to lower the catastrophic costs of a potential data breach.

The average cost of a breach tallies into the millions, but the dollars lost only account for the *direct* cost … is quantifiable for businesses, but the true costs cut even deeper.

"…cybercrime will cost approximately **$6 trillion per year** on average through 2021…

…but the dollars lost only account for the *direct* cost of a breach… When investigating the **collateral effects** of a cyberattack, the outlook for businesses in the aftermath becomes bleak. Dollars and cents aside, **some businesses never fully recover** from a data breach…

Once a customer feels a company is unable to keep them and their personal and financial information safe, it's game over. **Security questions are [ ] a nonstarter for prospective customers**.

Businesses and brands can have their **reputations destroyed** and their long-term viability called into question

ANALYSIS

Cybercrime damages expected to cost the world $6 trillion by 2021

Forbes, July 2017

Massive expansion of the global cyber attack surface will fuel the cybe

Cybercrime will continue its stratospheric growth over the n
according to a recent report published by Cybersecurit
Steve Morgan is the Founder and CEO at Cyberse

While there are numerous contributors to the rise in cybercrime -- which is expected to cost the world more than $6 trillion by 2021, up from $3 trillion in 2015 -- the most obvious predictor is a massive expansion of the global attack surface which hackers target.

The cybercrime cost prediction includes **damage and destruction of data**, **stolen money**, **lost productivity**, **theft of intellectual property**, **theft of personal and financial data**, **embezzlement**, **fraud**, **post-attack disruption to the normal course of business**, **forensic investigation**, **restoration and deletion of hacked data and systems**, and **reputational harm**.

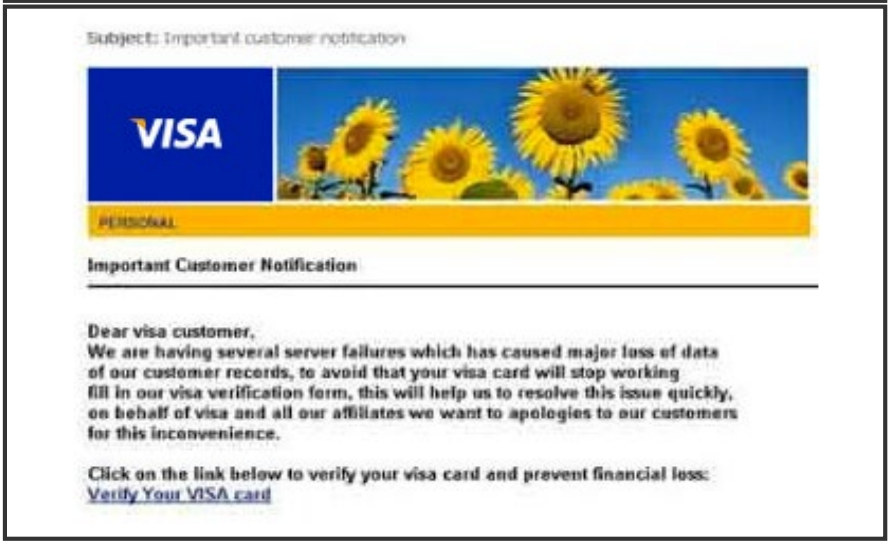
Landscape

- More attacks
- Against more organizations of differing size
- With increasing sophistication
- Resulting in higher costs and more serious damage to people, institutions & their causes

There is more risk today for organizations than ever before

Threats

Phishing and Spearphishing



Phishing scam

Generic email sent to a high number of recipients

Not tailored, but are engineered to appear valid

Likely uses actual company logos

Use 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

Spearphishing (& business email compromise)

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

Ubiquiti N
in a quart

Cybercrim
An increas
businesses
and social
email com

The con w
senior mar
(fraudulen
will approv
–kashhing

The Ubiquiti Networks networking equipment company disclosed it lost **$46.7 million** through [a BEC] scam in its fourth quarter financial filing…

The company only learned about the transfers of vast sums of money (14 over a 17 day period) after being notified by the FBI…

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

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

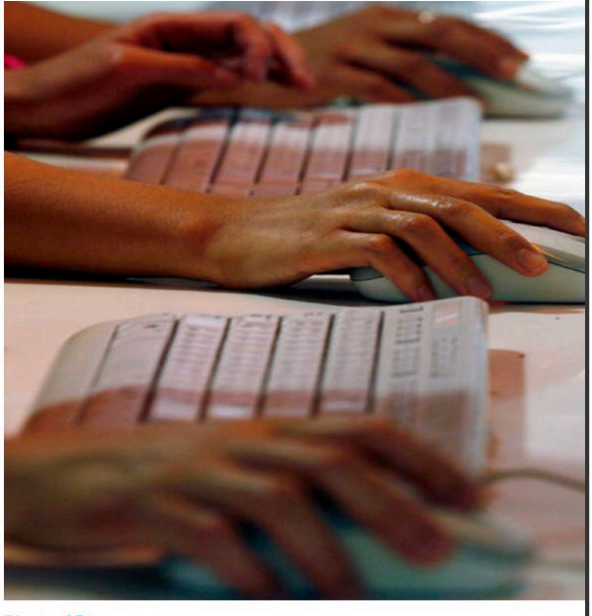


Photo: AP

"…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."

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

From: [redacted]

Sent: Tuesday, January 05, 2016 9:31 AM

To: [redacted]

Subject: Vendor Payment

[redacted]

Business Email Compromise (BEC)

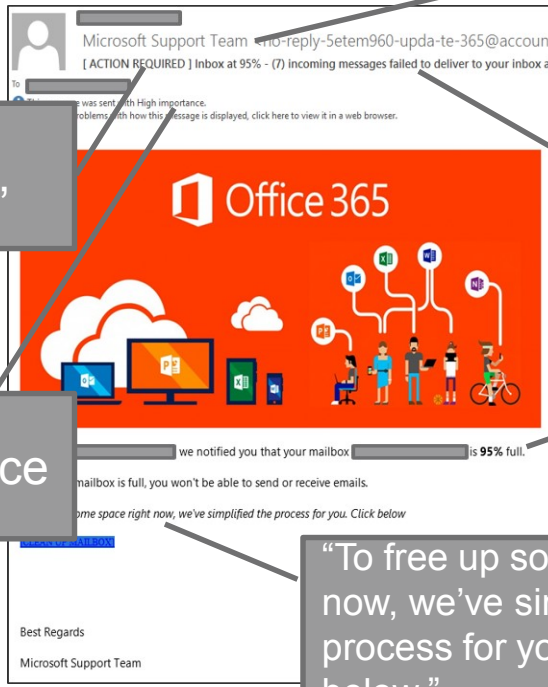
Welcome back. I hope you enjoyed your holiday?

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.

Example Case – O365 BEC



"ACTION REQUIRED"

High importance

Appears to come from Microsoft Support Team

"(7) incoming messages failed to deliver"

Inbox at 95%

"To free up some space right now, we've simplified the process for you. Click below."

Ransomware

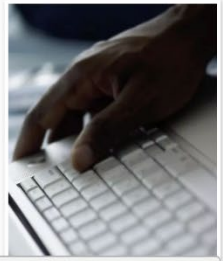

Your personal files are encrypted by CTB-Locker.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until 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.
View
95 20 15
Next >>

Hackers held patient data ransom, so Indiana hospital system paid $50,000

Jan. 17, 2018

USA TODAY NETWORK Vic Ryckaert, The Indianapolis Star Published 5:16 p.m. ET

These simple steps will help keep your computer from becoming the next ransomware target. USA TODAY



INDIANAPOLIS — An Indiana hospital system said it paid a $50,000 ransom to hackers who hijacked patient data.

The ransomware attack accessed the computers of Hancock Health in Greenfield through an outside vendor's account Thursday. It quickly infected the system by locking out data and changing the names

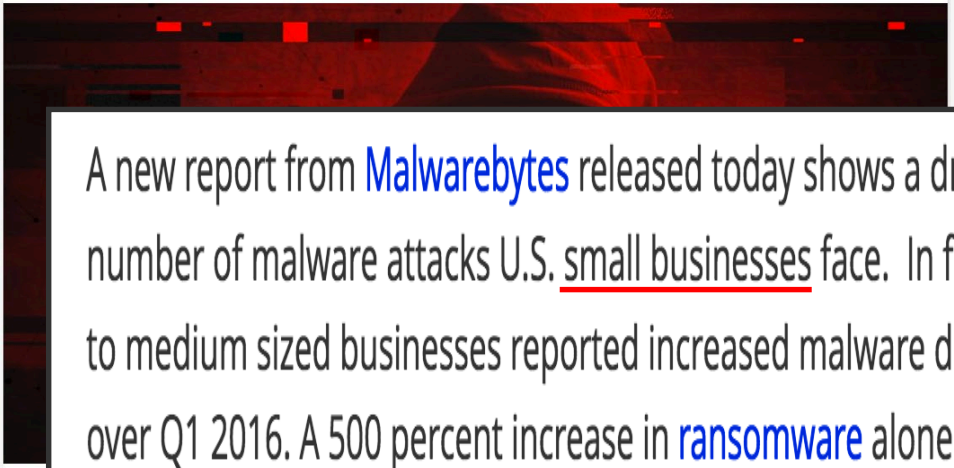
"The ransomware attack accessed the computers of Hancock Health in Greenfield ***through an outside vendor's account*** Thursday. It quickly infected the system by locking out data and changing the names of more than 1,400 files to "I'm sorry."

Small Business TRENDS

June 2017

Warning! Ransomware Attacks Against Businesses Up 500 Percent In Some States

Jun 15, 2017 by Rob Starr In Technology Trends 5



A new report from Malwarebytes released today shows a dramatic increase in the number of malware attacks U.S. small businesses face. In fact, 90 percent of small to medium sized businesses reported increased malware detection in Q1 2017 over Q1 2016. A 500 percent increase in ransomware alone was detected in March of this year in ten states.

A new report from Malwarebytes released today shows a dramatic increase in the number of malware attacks U.S. small businesses face. In fact, 90 percent of small to medium sized businesses reported increased malware detection in Q1 2017 over Q1 2016. A 500 percent increase in ransomware alone was detected in March of this year in ten states.

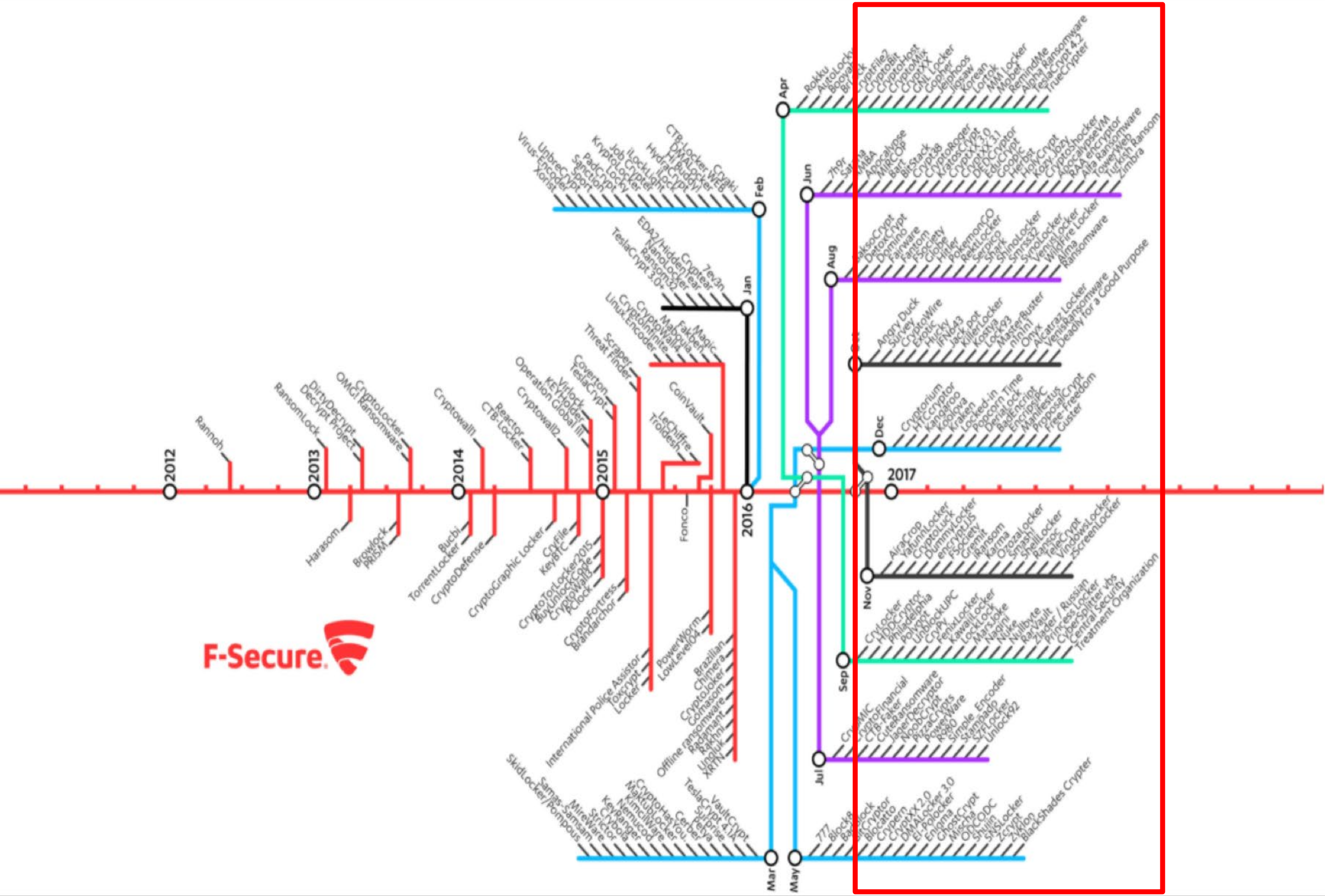
April 2017

TECHNOLOGY

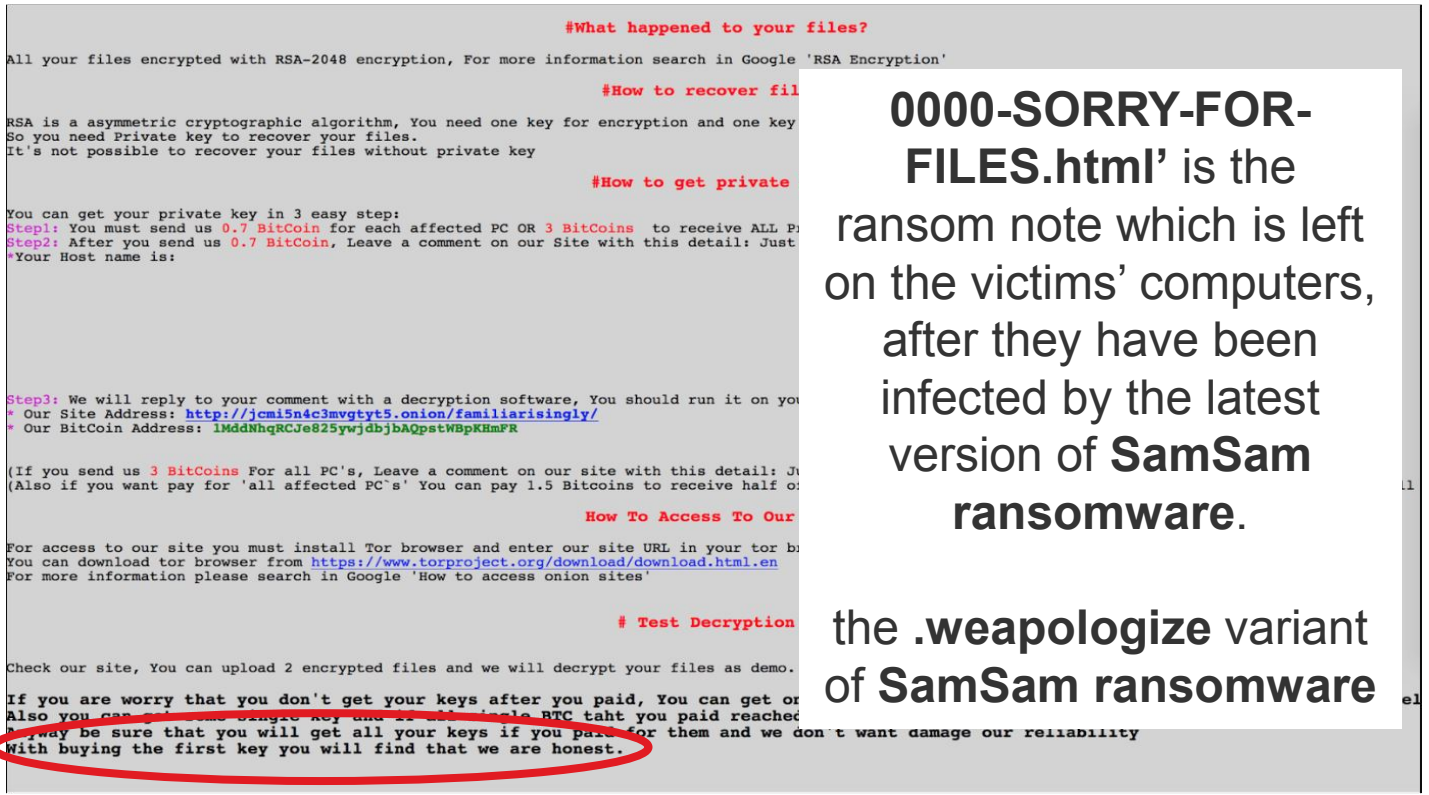
Ransomware demands now average about $1,000 because so many victims decide to pay up

The average ransomware attack yielded $1,077 last year, new research shows, representing a 266 percent spike from a year earlier.

The twist of the knife comes when only 47 percent of victims who pay the ransom actually recover any files.



2012
2013
2014
2015
2016
2017
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Nov
Dec
Rannoh
RansomLock
DirtyDecrypt
Decrypt Project
OMG! Ransomware
CryptoLocker
Harasom
Browlock
PRISM
CryptowallI
Reactor
CTB-Locker
Cryptowall2
Bucbi
TorrentLocker
CryptoDefense
CryptoGraphic Locker
CryFile
KeyBTC
Operation Global III
Virlock
Coverton
TeslaCrypt
Threat Finder
Scraper
CoinVault
LeChiffre
Troldesh
Fonco
CryptoFortress
Brandarchor
International Police Assistor
Toxcrypt
Locker
PowerWorm
LowLevel04
Brazilian
Chimera
CryptoJoker
Linux.Encoder
TeslaCrypt 3.0+
7ev3n
CTB-Locker Web
Cryaki
Rokku
AutoLocky
CryptoHost
CryptoMix
Jigsaw
Lortok
MM Locker
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
Apocalypse
Bart
CryptoRoger
Cryptoshocker
ApocalypseVM
Alfa Ransomware
Turkish Ransom
Zimbra
Domino
Fairware
Fantom
Globe
Hitler
PokemonGO
Serpico
Shark
Alma
Ransomware
Angry Duck
CryptoWire
Exotic
Jack.pot
KillerLocker
Koolova
MasterBuster
Onyx
Alcatraz Locker
Deadly for a Good Purpose
Cryptorium
Kangaroo
Kraken
Popcorn Time
Locked-In
Free-Freedom
Custer
AiraCrop
CryptoLuck
DummyLocker
Gremit
Karma
Smash!
ShellLocker
Ransoc
VenusLocker
WindowsLocker
zScreenLocker
CryLocker
Philadelphia
Polyglot
UnblockUPC
Cry
FenixLocker
KawaiiLocker
LockLock
Nuke
RarVault
Princess Locker
CyberSplitter Vbs
Central Security Treatment Organization
CryptoFinancial
CTB-Faker
CuteRansomware
PizzaCrypts
PowerWare
Simple_Encoder
Stampado
Unlock92
777
Block8
Blocatto
CryptXXX 2.0
DMALocker 3.0
Enigma
GhostCrypt
Mischa
Shujin
SNSLocker
BlackShades Crypter
SkidLocker/Pompous
Samas-Samsam
TeslaCrypt 4.1A
F-Secure



0000-SORRY-FOR-FILES.html' is the ransom note which is left on the victims' computers, after they have been infected by the latest version of **SamSam ransomware**.

the **.weapologize** variant of **SamSam ransomware**

Insiders

Harvard Business Review

SECURITY & PRIVACY

The Biggest Cybersecurity Threats Are Inside Your Company

by Marc van Zadelhoff

SEPTEMBER 19, 2016

SAVE | SHARE | COMMENT 1 | TEXT SIZE | PRINT | $8.95 BUY COPIES

When secur
about nefar
failure of te
read and eas
reality is tha
usually it's
the compan

The role tha
corporation
Security Int
were carrie
involved ma
inadvertent
health care,
three indus
intellectual
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.

Empower Results®

Defenses

Defenses

+ Plans, Policies & Programs
+ Relationships
+ Test, Assess & Drill
+ Culture
+ Risk Transfer

Plans, Policies & Programs

- Develop an actionable, up-to-date **incident response (IR) plan** *before* an intrusion occurs
- Develop and adopt a formal **information security (infosec) program** and policy document
- Working with IT, develop detailed **data loss prevention** (DLP), **disaster recovery** (DR) and **business continuity plans** (BCP)

Relationships

- Identify, select and negotiate an **IR retainer agreement** with a technical provider
- Select a law firm partner
- Establish a relationship with a PR firm
- Get to know law enforcement

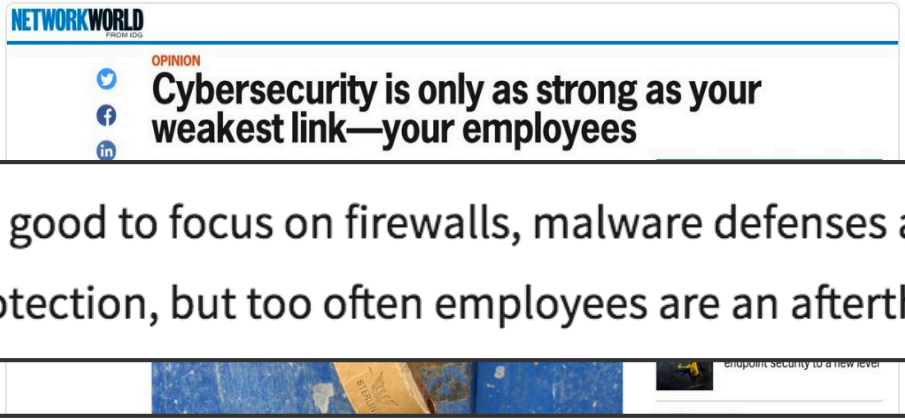
Test, Assess & Drill

- Test your IR plan with **tabletop exercises**
- Penetration testing
- Red team testing
- Vulnerability, maturity assessments
- **IR readiness assessments**
- Phishing, USB key drops

Culture

John Ansbach @johnansbach · Jul 14

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



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

- Mandatory training
- Awareness campaigns
- Monthly e-mails to the team about the latest threats, best practice reminders
- Leadership engagement…

AON Empower Results®

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

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.

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

Risk Transfer (Cyber insurance)

CIO FROM IDG

INSIDER Sign In | Register

FEATURE

What is cyber insurance and why you need it

Cyber insurance can't protect your organization from cybercrir
financial footing should a significant security event occur.

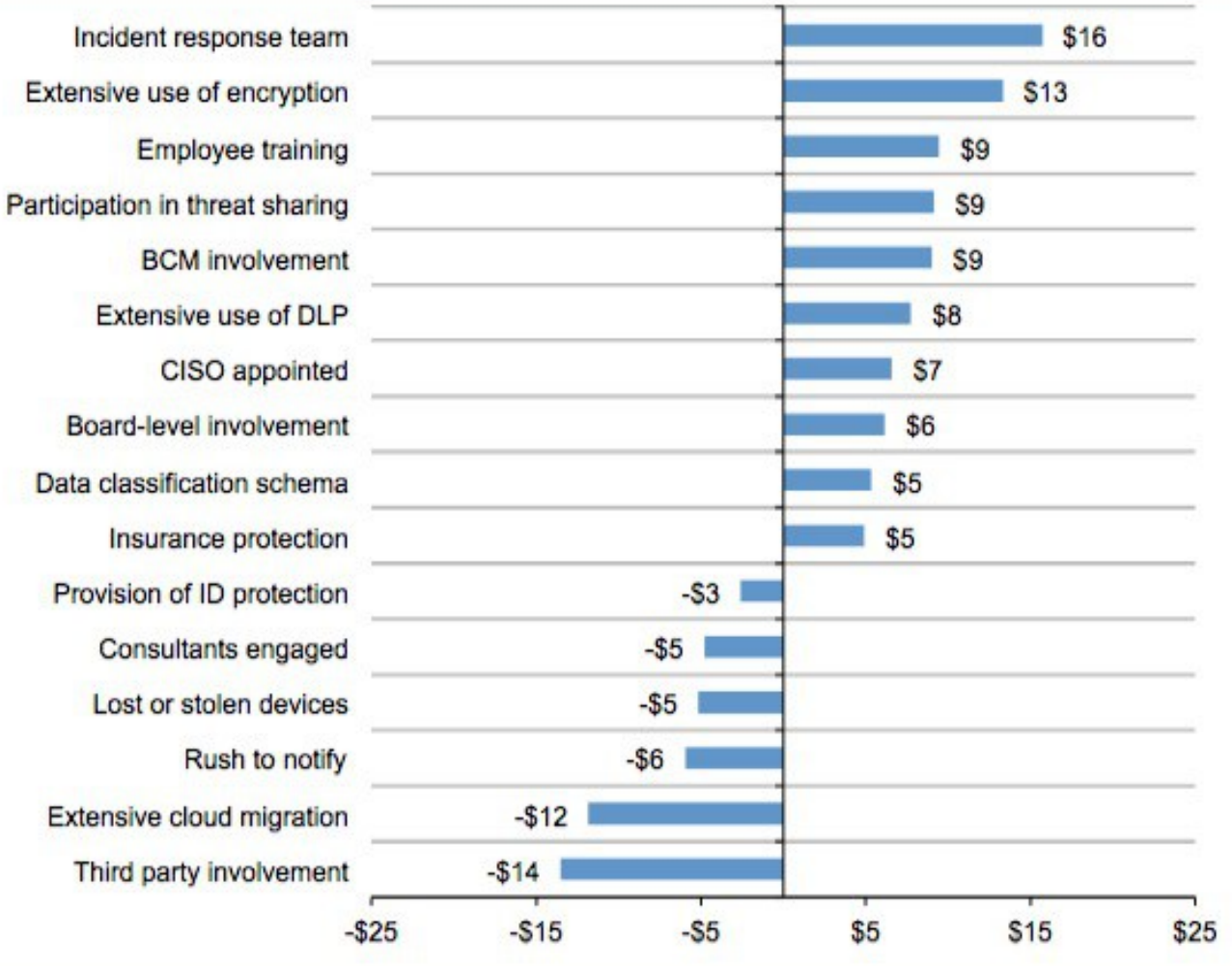
Credit: David Hilowitz, CC BY 2.0, via Flickr

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 (through risk transfer) by offsetting costs involved with recovery after a cyber-related security breach*** or similar event.


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.

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.

10. Use IPS/IDS *prevention* software

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)

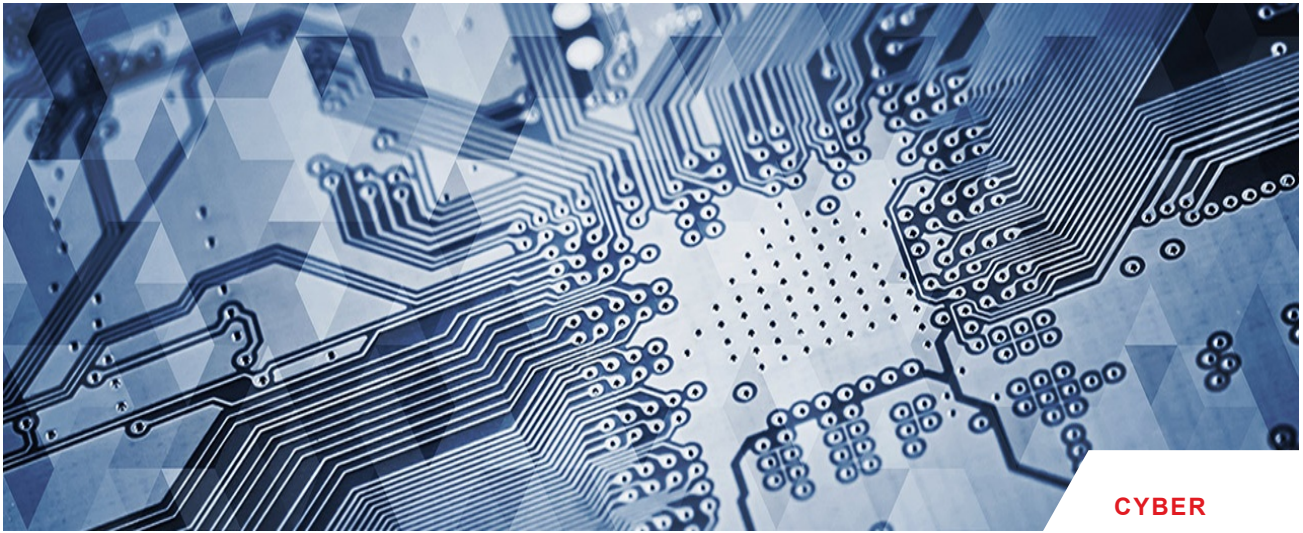
6. Train your people to be wary of phone calls seeking info – these “low tech” attacks often are advance scouting work of an impending cyberattack or spear phish.

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.

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

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



Cyber *In*security

What you Can do Now to Help Keep Your Organization Safe

John Ansbach, JD, CIPP-US
@johnansbach
jansbach@strozfriedberg.com

STROZ FRIEDBERG
an Aon company

AON
Empower Results®