Critical (And Growing) IT Security Threats

All Of Our Clients Must Protect Against NOW

To Avoid Cyber-Attacks, Data Breach Lawsuits, Ransomware, Bank Fraud, Negative PR and Compliance Penalties

Brian Clark, President
CCPlus Computer Solutions

www.ccplus-usa.com

Today We're Going To Cover

- The #1 security threat to your business that antivirus, firewalls and other security protocols can't protect against.
- Why firewalls and antivirus software aren't enough anymore.
- How mobile phones and cloud applications are seriously jeopardizing your organization's security and data protection – and what you need to do to protect yourself.

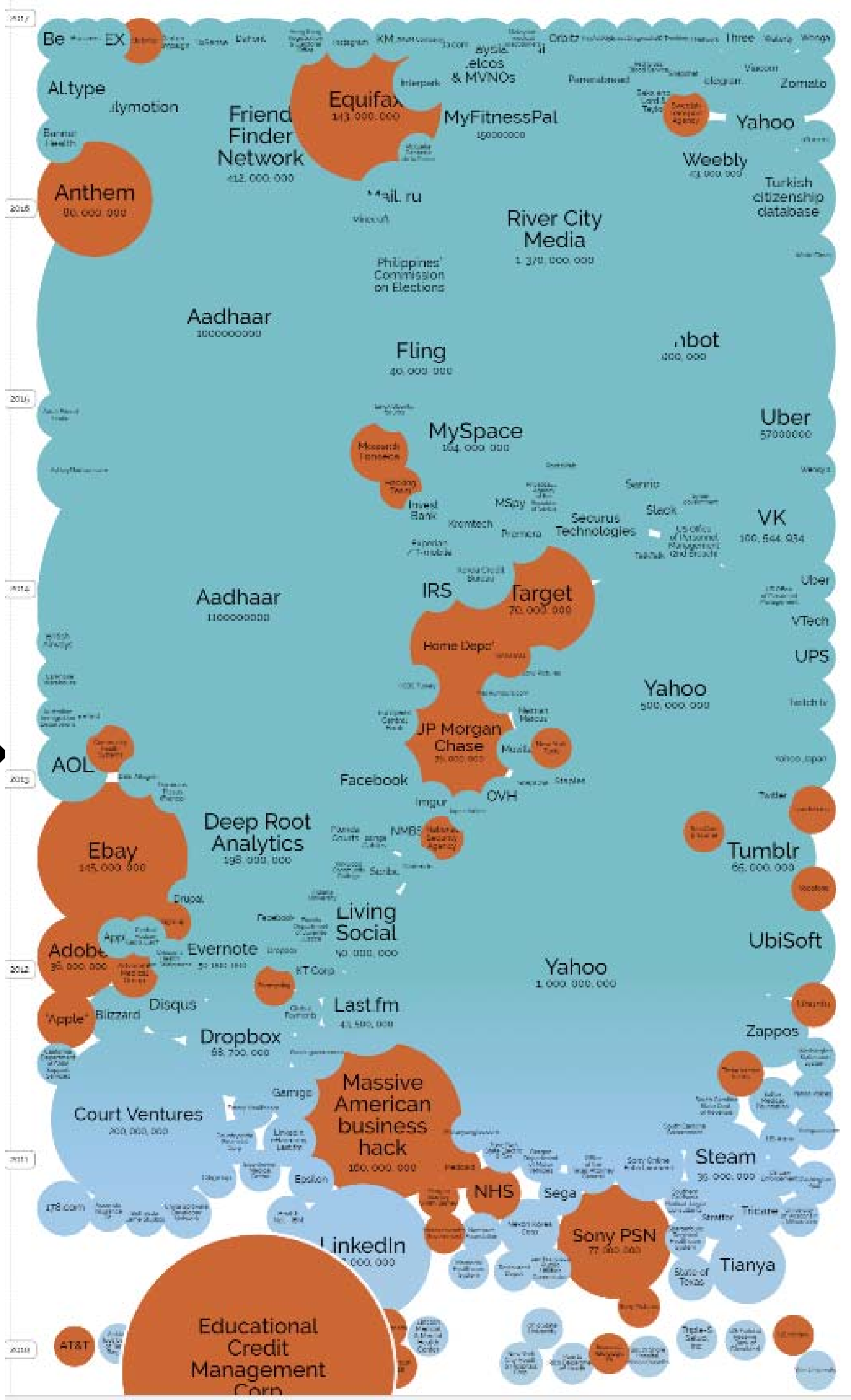
Ultimately We're Going To Cover...

How To Avoid Being A **Sitting Duck** To Cybercriminals And Protect Everything You've *Worked So Hard To Achieve*

A Quick Overview Of The Sophistication And Proliferation Of The

Cybercrime Business

The Evolution Of Crime



80 Million Households And 7 Million Small To Medium Businesses HACKED

The Criminal Digital Underground's Thriving Black Market

- Credit card details sell for: **$2 to $90**
- A Medical Record sells for over **$150**
- iTunes accounts sell for about: **$8**
- Physical credit cards sell for: **$190**
- Card cloners can be bought for: **$200-$300**
- Fake ATMs can be bought for: **$35,000**
- **THIS IS A BUSINESS**: anyone can easily buy training, tools and services for committing fraud, hacking systems, buying stolen credit cards, setting up fake websites, etc.

$141

Additional Damages And Costs NOT INCLUDED In The Above Number:

- Reputational damage
- Loss of clients
- Class action lawsuits, individual lawsuits
- Legal fees to handle a breach
- Compliance lawsuits (fines for non-compliance)
- Replacement of data
- Downtime, loss of productivity
- Time required to re-enter data and get your internal systems back up and running again

“But We’re Small… Nobody Would Bother To Hack Us, Right?”

Wrong!

- **One in five** small businesses falls victim to cybercrime each year and that number is GROWING.
  (Source: National Cyber Security Alliance)
- Small businesses **are low-hanging fruit** because they don’t believe they are a target, and therefore have very loose or no security systems and protocols in place.
- **Half of all cyber attacks** are aimed at SMBs.
  (Source: Forbes Article, “5 Ways Small Businesses Can Protect Against Cybercrime”)

Why Don't You Hear More About It?

- It's extremely embarrassing to admit you've been hacked.
- Many people ***don't even know*** they've been hacked.
- ***Horrible PR; do you REALLY want your clients (or patients!) to know their information was accessed?***
- The legal ramifications (fines, lawsuits, legal fees) can be *significant*, <u>so many incidents go unreported</u>.

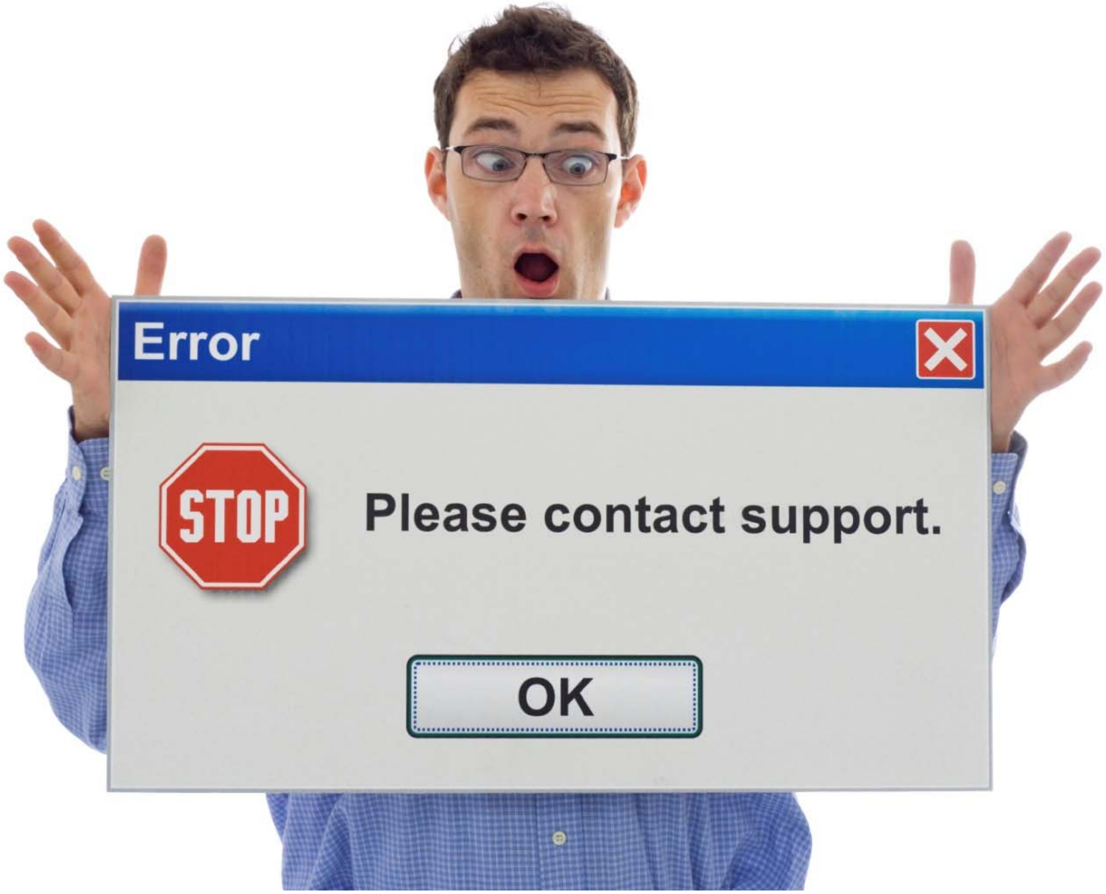
Key Point: Just because YOU aren't that worried about your information being stolen doesn't mean your **customers' information and privacy is any less valuable to *them*.** What are you doing to be a good steward of their information?

The Biggest Danger Is Your Complacency

Please **DO NOT underestimate** the importance of addressing and protecting yourself from this threat.

The 7 Biggest Threats To Your Organization Right Now

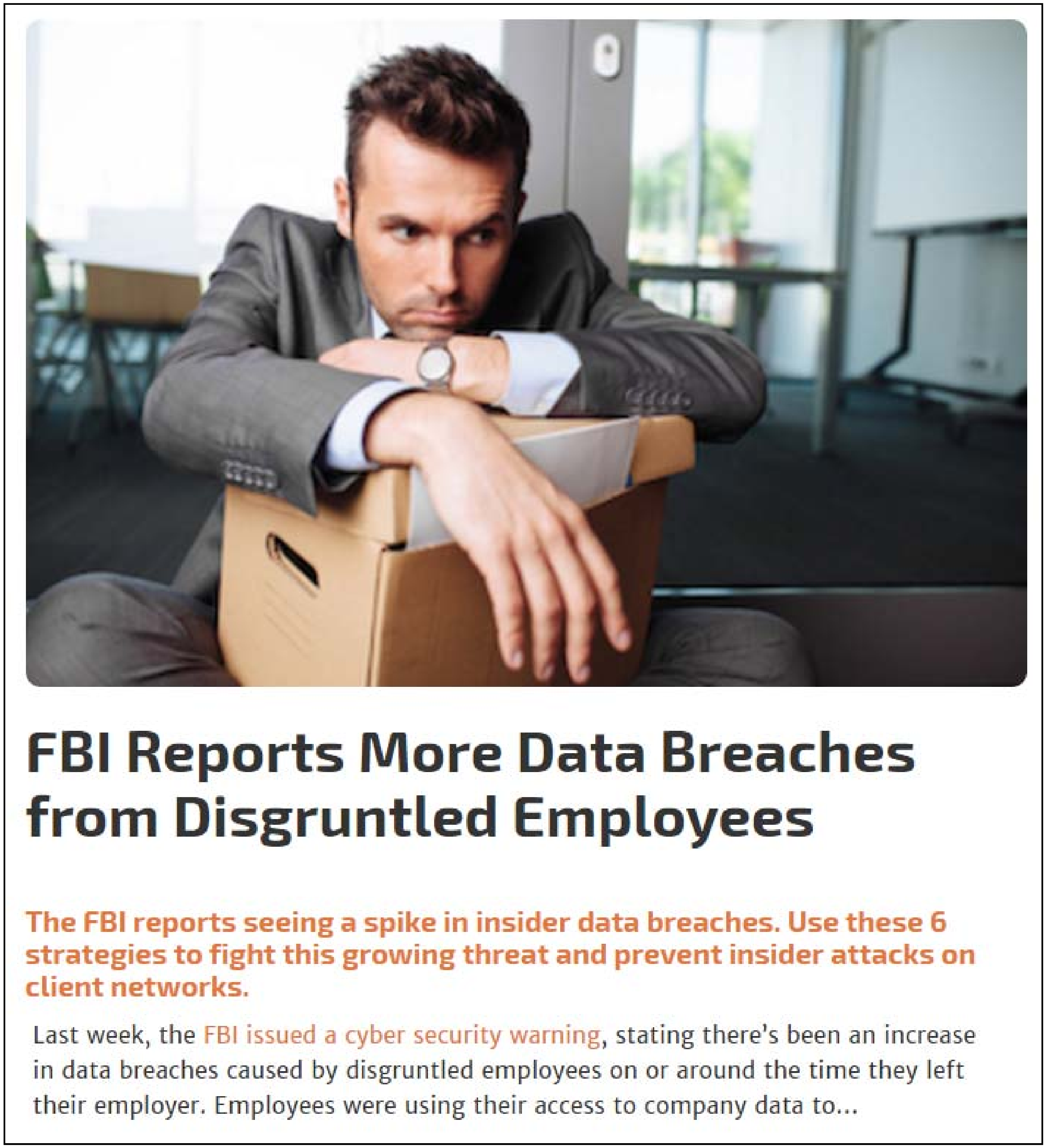
And How To Stop Them



Cyber-Thugs Aren't Your #1 Threat…

Your Employees Are!

- **Even GOOD employees make mistakes;** deleting files, clicking on phishing e-mails or innocently logging in to a compromised Facebook page.
- Employees often use free and unsecured file-sharing applications like Dropbox to share confidential information simply because they don't know better – and they don't think to tell you about it!



FBI Reports More Data Breaches from Disgruntled Employees

The FBI reports seeing a spike in insider data breaches. Use these 6 strategies to fight this growing threat and prevent insider attacks on client networks.

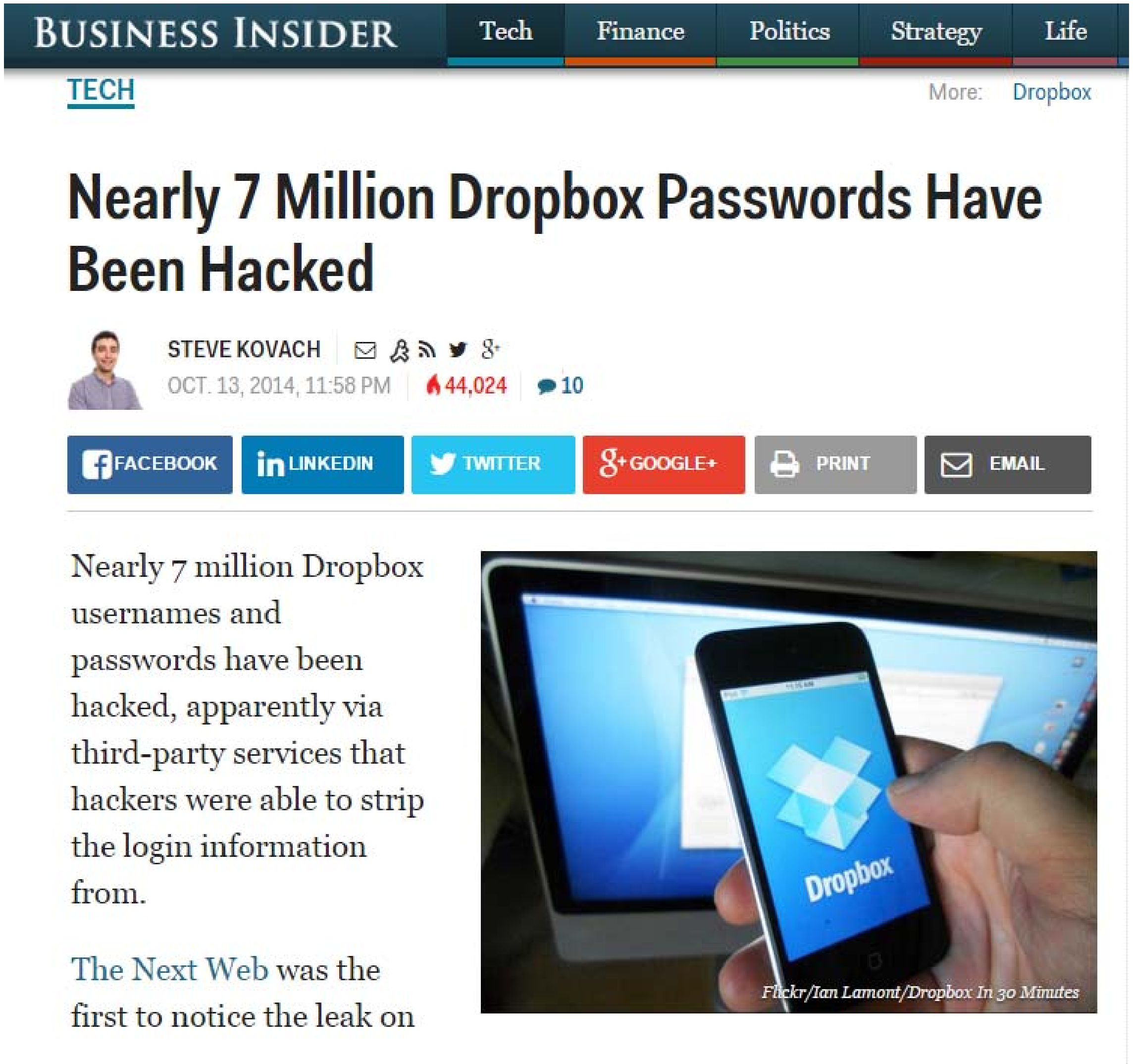
Last week, the FBI issued a cyber security warning, stating there's been an increase in data breaches caused by disgruntled employees on or around the time they left their employer. Employees were using their access to company data to...

Disgruntled employees (and vendors!) who've been fired also pose a HUGE THREAT since they often have direct access to a VAST NUMBER of cloud applications and data.

Shadow IT

How Much Of Your Company’s Data Is Out On Rogue Cloud Apps, Put There By Employees Who Are Just Trying To Do Their Job?

That’s A GOOD Question; Do You Even Know The Answer?



Nearly 7 Million Dropbox Passwords Have Been Hacked

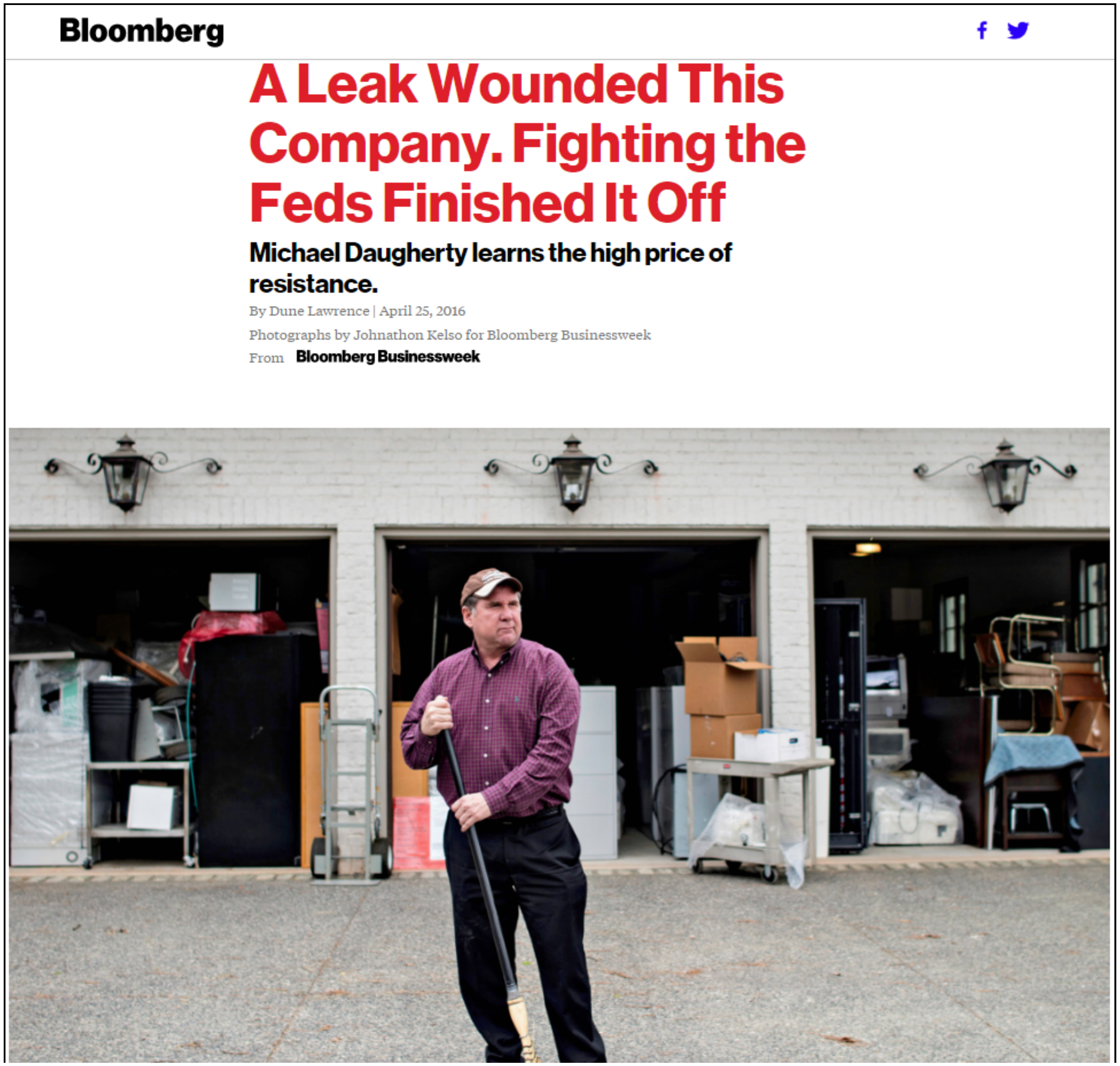
STEVE KOVACH
OCT. 13, 2014, 11:58 PM 44,024 10

Nearly 7 million Dropbox usernames and passwords have been hacked, apparently via third-party services that hackers were able to strip the login information from.

The Next Web was the first to notice the leak on

Flickr/Ian Lamont/Dropbox In 30 Minutes

How A GOOD Employee’s Mistake, A Disgruntled Vendor And The FBI Destroyed This Man’s Business



Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From **Bloomberg Businessweek**

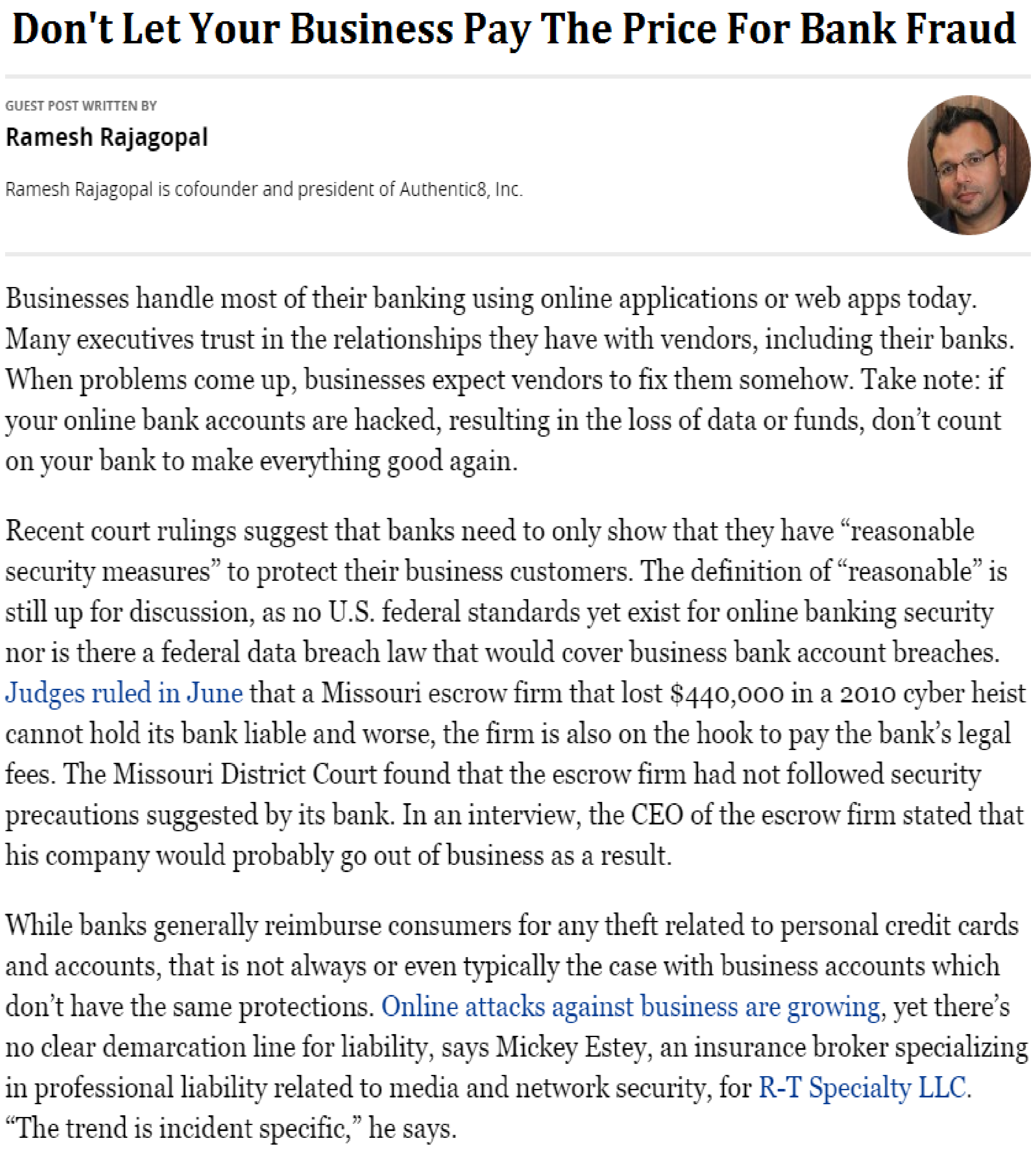
#2: Malware

250,000

NEW Malware Threats Are Being Released *Per Day*

#3: Bank Fraud

FDIC Does NOT Protect You From Bank Fraud, And The Bank Is NOT Responsible For Getting Your Money Back!!!



Don't Let Your Business Pay The Price For Bank Fraud

GUEST POST WRITTEN BY

Ramesh Rajagopal

Ramesh Rajagopal is cofounder and president of Authentic8, Inc.

Businesses handle most of their banking using online applications or web apps today. Many executives trust in the relationships they have with vendors, including their banks. When problems come up, businesses expect vendors to fix them somehow. Take note: if your online bank accounts are hacked, resulting in the loss of data or funds, don't count on your bank to make everything good again.

Recent court rulings suggest that banks need to only show that they have "reasonable security measures" to protect their business customers. The definition of "reasonable" is still up for discussion, as no U.S. federal standards yet exist for online banking security nor is there a federal data breach law that would cover business bank account breaches. Judges ruled in June that a Missouri escrow firm that lost $440,000 in a 2010 cyber heist cannot hold its bank liable and worse, the firm is also on the hook to pay the bank's legal fees. The Missouri District Court found that the escrow firm had not followed security precautions suggested by its bank. In an interview, the CEO of the escrow firm stated that his company would probably go out of business as a result.

While banks generally reimburse consumers for any theft related to personal credit cards and accounts, that is not always or even typically the case with business accounts which don't have the same protections. Online attacks against business are growing, yet there's no clear demarcation line for liability, says Mickey Estey, an insurance broker specializing in professional liability related to media and network security, for R-T Specialty LLC. "The trend is incident specific," he says.

Banks Are Prevailing In Cybercrime Cases; PLUS You Might Have To Pay The Bank's Legal Fees If You Sue Them!

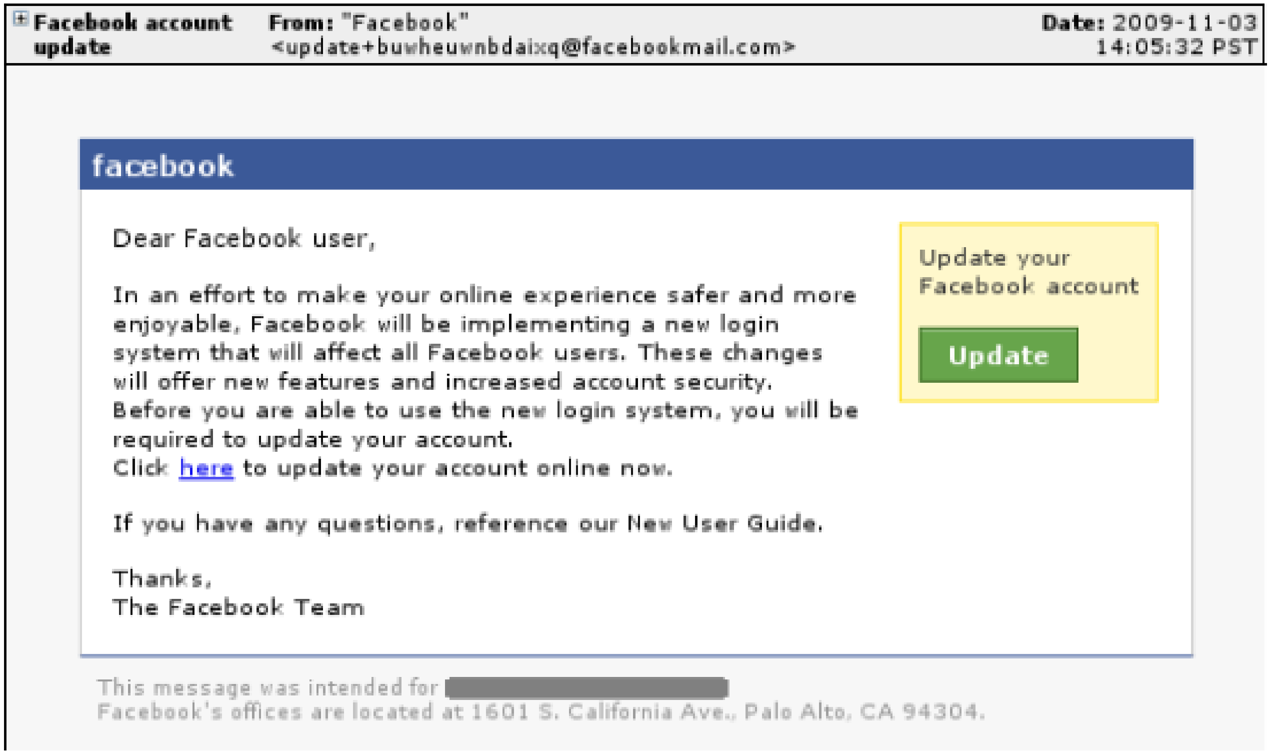
Tips For Protecting Yourself:

- Cancel your debit cards; they are the #1 way bank accounts get compromised.
- Have a dedicated Google Chromebook or iPad Pro for online banking and DON'T use that PC for accessing any other websites, e-mail access, social media sites or for downloading files and applications.
- Sign up for e-mail alerts from your bank whenever a withdrawal over $100 happens.
- Require YOUR signature for any wire transfers and turn on dual factor authentication to log into your bank account.
- Have your money spread out in multiple accounts to minimize the risk.
- Carry CRIME insurance.

#4: Social Media

Threat #1: Security

600,000 Facebook Accounts Are Hacked
<u>Every Single DAY</u>.



Facebook account update **From:** "Facebook" <update+buwheuwnbdaixq@facebookmail.com> **Date:** 2009-11-03 14:05:32 PST

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your Facebook account

This message was intended for [redacted]
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Social Media

Threat #2: Significant Loss Of Productivity

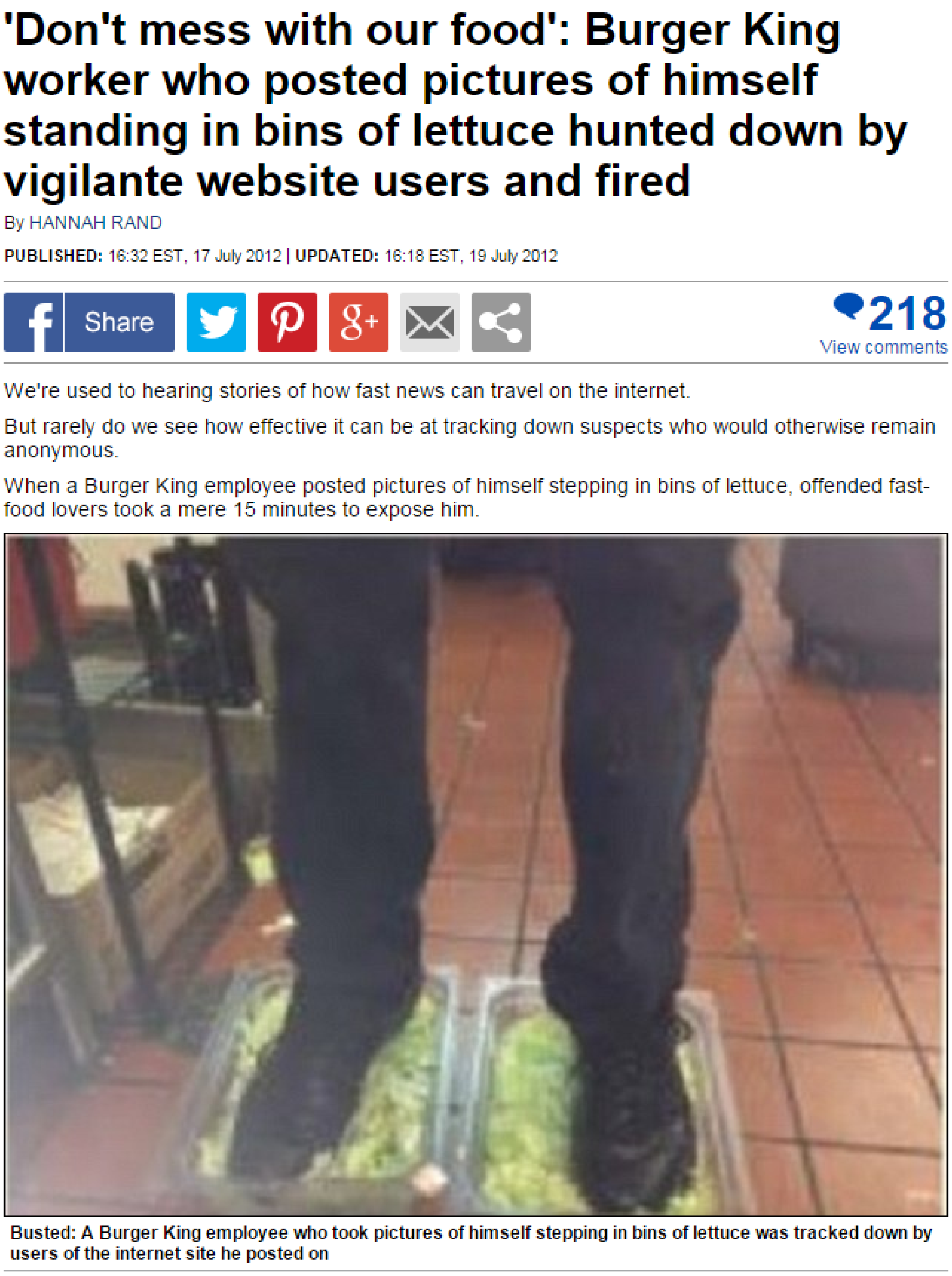
Time Wasted	Pct of Employees
<1 hour	39%
1-2 hours	29%
2-5 hours	21%
6-10 hours	8%
10+ hours	3%

Contributing to these percentages are social media networks. The winners for the time-loss warp are Tumblr (57%), Facebook (52%), Twitter (17%), Instagram (11%) and SnapChat (4%).

Social Media

Threat #3:

Bad PR; You Don't Think A Disgruntled Employee Will Do Damage?



'Don't mess with our food': Burger King worker who posted pictures of himself standing in bins of lettuce hunted down by vigilante website users and fired

By HANNAH RAND

PUBLISHED: 16:32 EST, 17 July 2012 | **UPDATED:** 16:18 EST, 19 July 2012

We're used to hearing stories of how fast news can travel on the internet.

But rarely do we see how effective it can be at tracking down suspects who would otherwise remain anonymous.

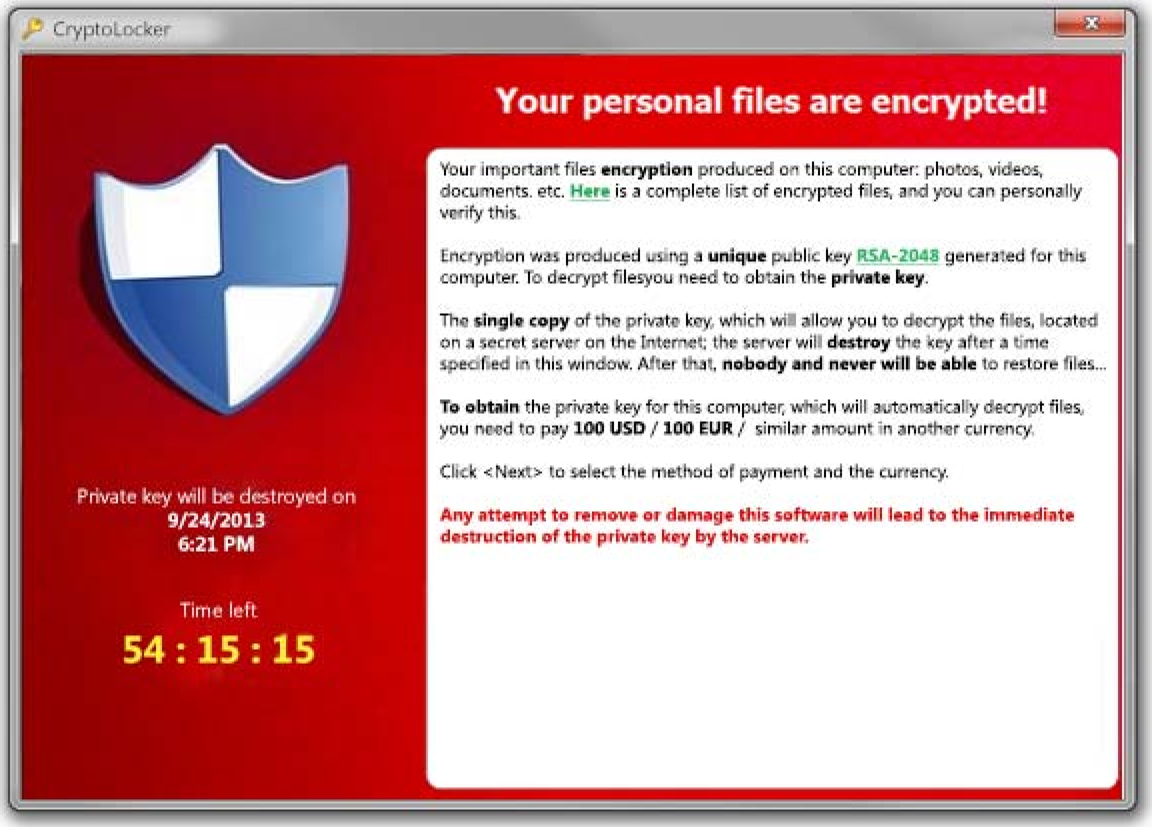
When a Burger King employee posted pictures of himself stepping in bins of lettuce, offended fast-food lovers took a mere 15 minutes to expose him.

Busted: A Burger King employee who took pictures of himself stepping in bins of lettuce was tracked down by users of the internet site he posted on

#5: Ransomware

A writer once asked a literary agent, **“What kind of writing pays the most?”** Her answer was simple: **“Ransom notes.”**

That’s sort of what’s happening in the cybercrime world — sensitive data in the wrong hands is used to extort money.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

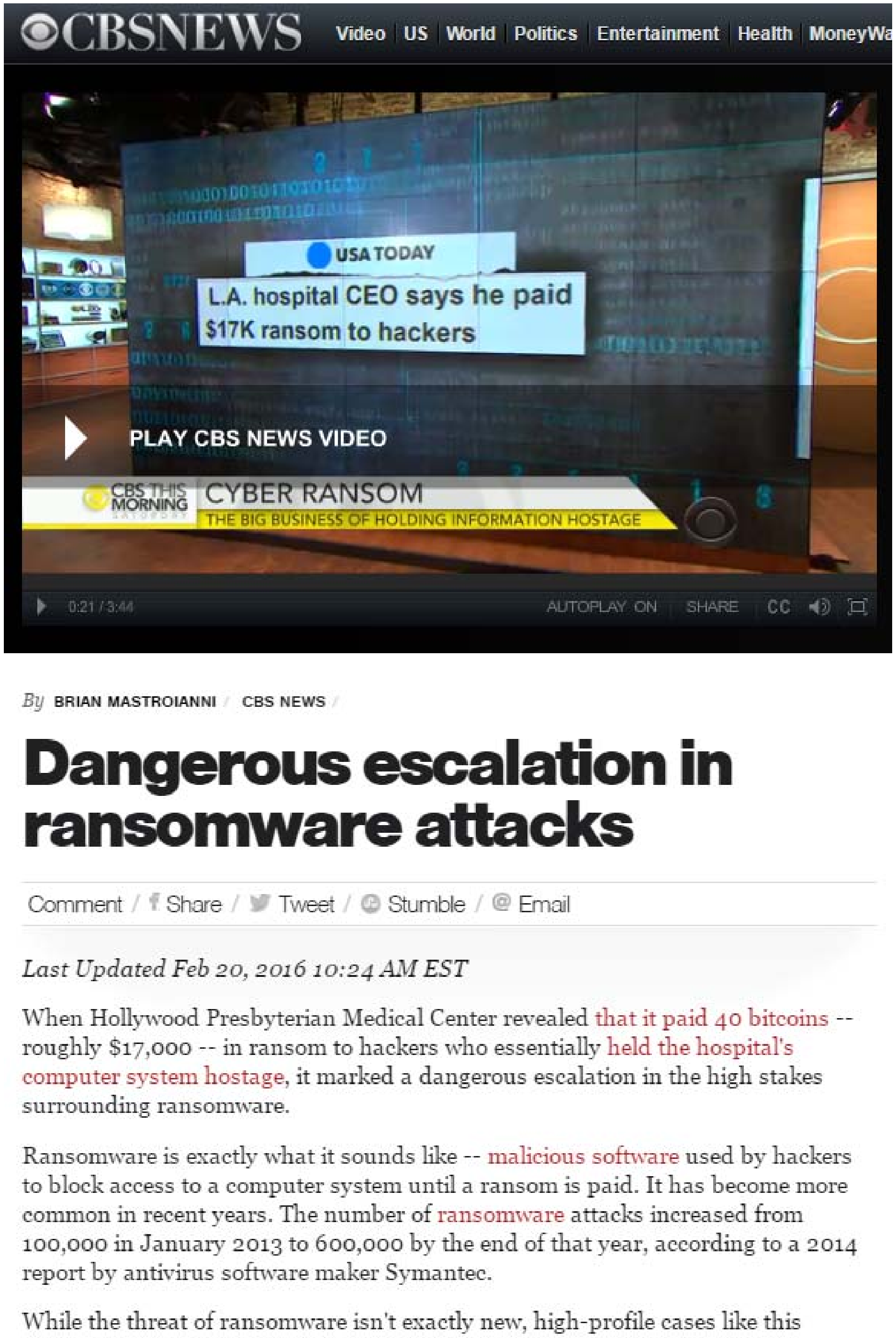
Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Ransomware Is Proliferating


CBSNEWS
Video
US
World
Politics
Entertainment
Health
MoneyWa
USA TODAY
L.A. hospital CEO says he paid $17K ransom to hackers
PLAY CBS NEWS VIDEO
CBS THIS MORNING SATURDAY
CYBER RANSOM
THE BIG BUSINESS OF HOLDING INFORMATION HOSTAGE
0:21 / 3:44
AUTOPLAY ON
SHARE
CC
Comment / Share / Tweet / Stumble / Email

By BRIAN MASTROIANNI / CBS NEWS /

Dangerous escalation in ransomware attacks

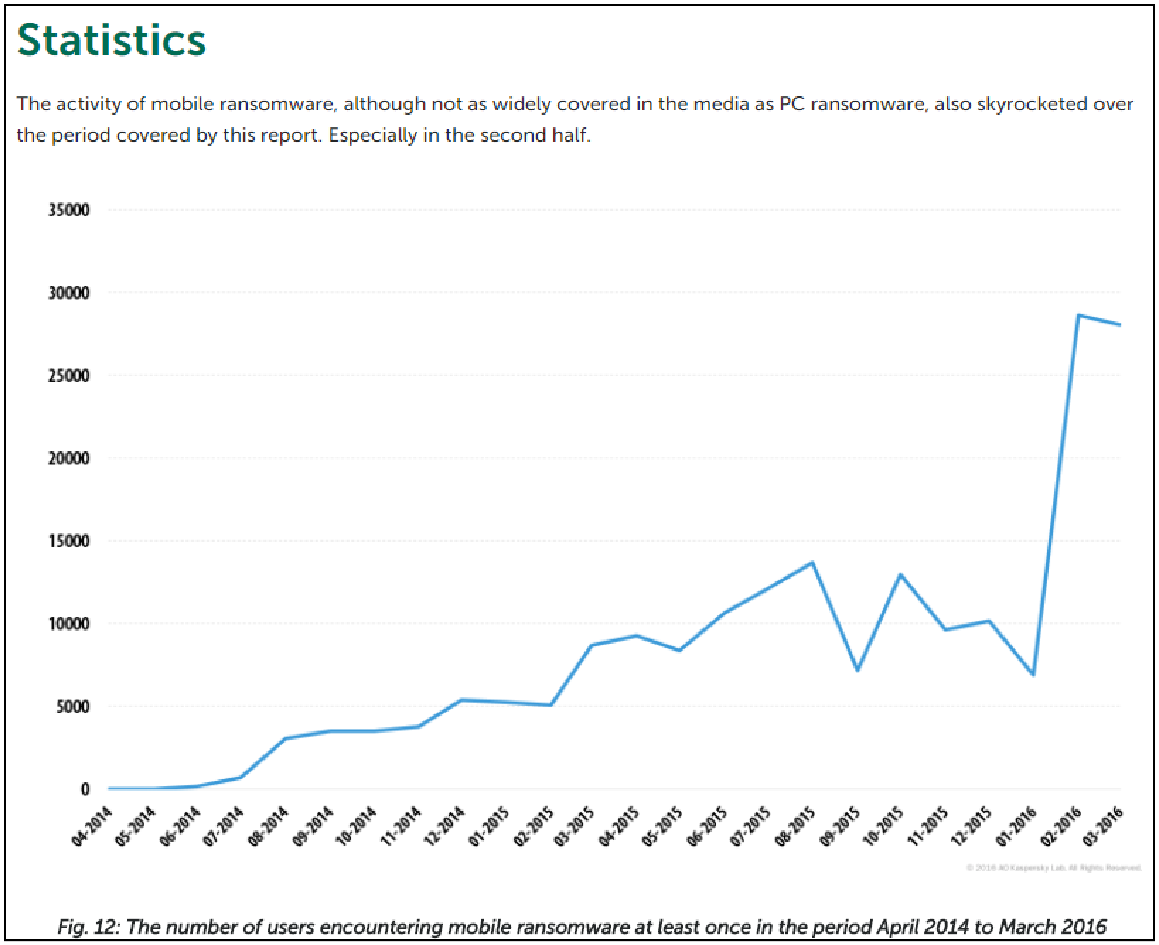
Last Updated Feb 20, 2016 10:24 AM EST

When Hollywood Presbyterian Medical Center revealed that it paid 40 bitcoins -- roughly $17,000 -- in ransom to hackers who essentially held the hospital's computer system hostage, it marked a dangerous escalation in the high stakes surrounding ransomware.

Ransomware is exactly what it sounds like -- malicious software used by hackers to block access to a computer system until a ransom is paid. It has become more common in recent years. The number of ransomware attacks increased from 100,000 in January 2013 to 600,000 by the end of that year, according to a 2014 report by antivirus software maker Symantec.

While the threat of ransomware isn't exactly new, high-profile cases like this

#6: Unsecured, Unmonitored Mobile Devices



Statistics

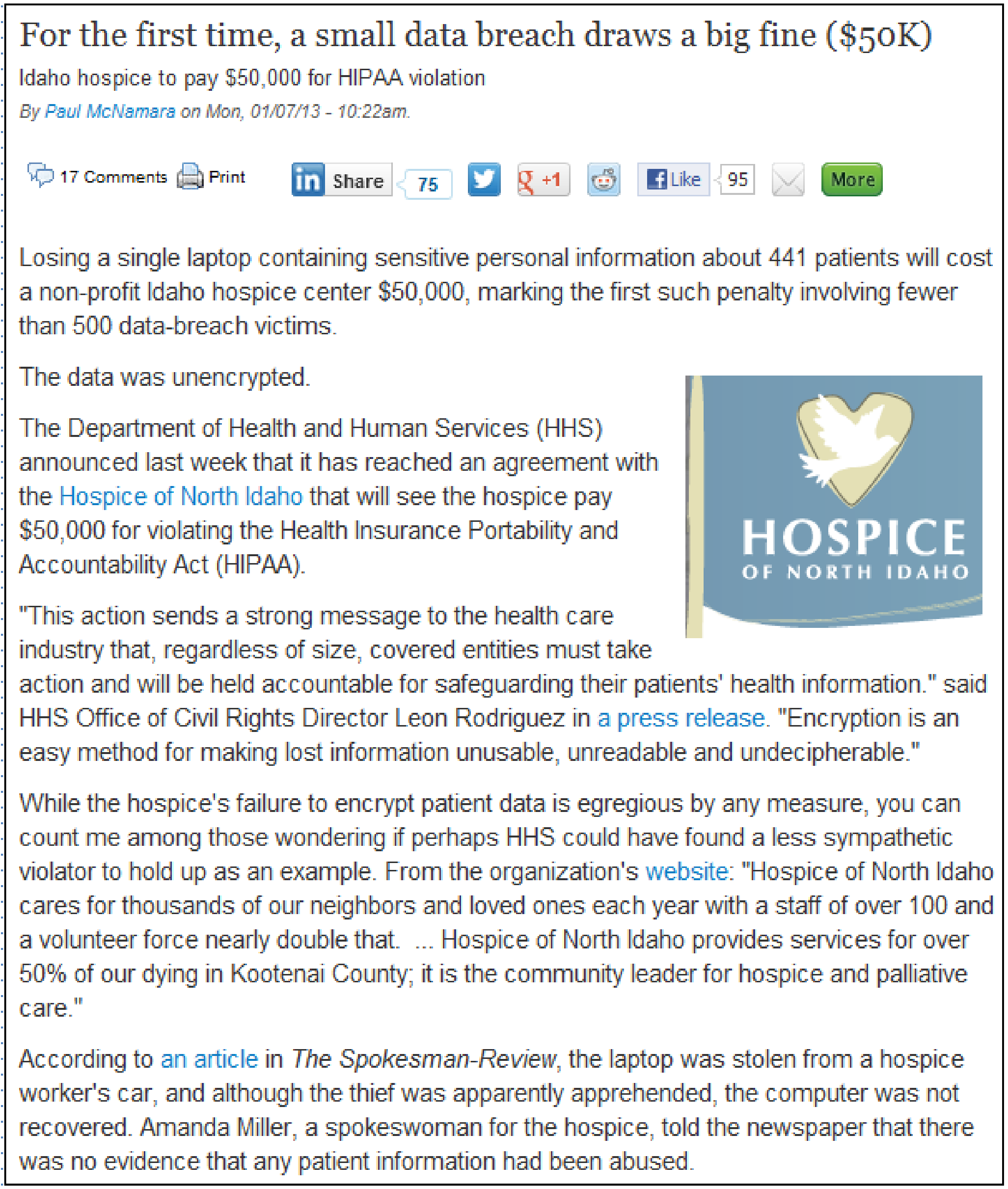
The activity of mobile ransomware, although not as widely covered in the media as PC ransomware, also skyrocketed over the period covered by this report. Especially in the second half.

Fig. 12: The number of users encountering mobile ransomware at least once in the period April 2014 to March 2016

Mobile Computing Dangers On The Rise…

If A Device Is **Lost Or Stolen,** And The Data Was NOT Encrypted, You May Have Violated A Tennessee Data Breach Law

- In Tennessee, “personal information” is considered a person’s first name or first initial and last name in combination with a driver’s license number, social security number, or any information (including logins and passwords) related to financial records (credit cards, access codes, passwords, etc.).



For the first time, a small data breach draws a big fine ($50K)

Idaho hospice to pay $50,000 for HIPAA violation

By Paul McNamara on Mon, 01/07/13 - 10:22am.

Losing a single laptop containing sensitive personal information about 441 patients will cost a non-profit Idaho hospice center $50,000, marking the first such penalty involving fewer than 500 data-breach victims.

The data was unencrypted.

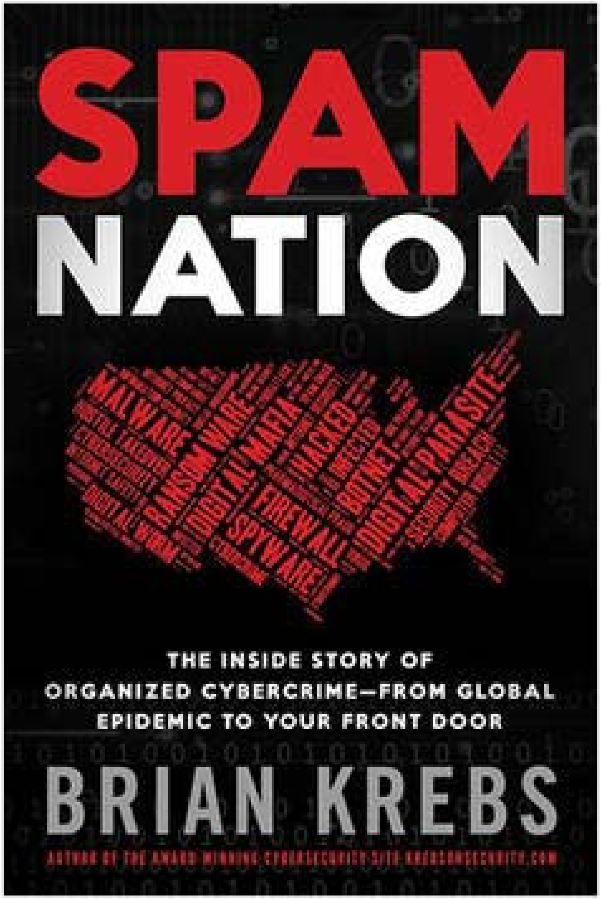
The Department of Health and Human Services (HHS) announced last week that it has reached an agreement with the Hospice of North Idaho that will see the hospice pay $50,000 for violating the Health Insurance Portability and Accountability Act (HIPAA).

"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." said HHS Office of Civil Rights Director Leon Rodriguez in a press release. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

While the hospice's failure to encrypt patient data is egregious by any measure, you can count me among those wondering if perhaps HHS could have found a less sympathetic violator to hold up as an example. From the organization's website: "Hospice of North Idaho cares for thousands of our neighbors and loved ones each year with a staff of over 100 and a volunteer force nearly double that. ... Hospice of North Idaho provides services for over 50% of our dying in Kootenai County; it is the community leader for hospice and palliative care."

According to an article in *The Spokesman-Review*, the laptop was stolen from a hospice worker's car, and although the thief was apparently apprehended, the computer was not recovered. Amanda Miller, a spokeswoman for the hospice, told the newspaper that there was no evidence that any patient information had been abused.

#7: Spam!


SPAM
NATION
THE INSIDE STORY OF
ORGANIZED CYBERCRIME—FROM GLOBAL
EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
AUTHOR OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

“Spam remains the single biggest driver of big breaches today. If we look at some of the biggest data breaches in recent memory - JPMorgan, Target, RSA Security come to mind - they all began with poisoned e-mail.”

– Brian Krebs, Spam Nation

Snapple

So How Do You Protect Yourself?

- *Advanced endpoint security, not just anti-virus*
- *Ransomware-proof backup*
- *Next Generation Firewall with monitoring, logging and reporting*
- *Spam filtering*
- *Control what web sites employees are accessing*
- *Lock down the use of 3rd-party cloud apps (Dropbox)*
- *Implement a mobile device policy and security protocols*
- *Force passwords that are difficult to hack*
- *Back up your systems properly (protects against a number of threats)*
- *Employee education and AUP*
- *Lock down the ability for employees to use home PCs and devices to access your network and cloud applications.*

Bottom Line:

You Need To Get Serious About Protecting Your Company Against Cybercrime!

But What Does That Look Like?

3 Steps To Protecting Your Organization:

- **Step 1: Threat Assessment**
  What's lacking in your security right now? How are employees using your company-owned devices? What 3rd-party cloud apps are you using? Are your systems truly backed up? Where are you exposed to risk? Whose job is it to make sure your network is protected, and how do you know if they're doing their job?
- **Step 2: Action Plan**
  Based on what's discovered, what do we need to do to ensure our systems, data and operations are secure from theft, compromise, corruption, etc.?
- **Step 3: Ongoing Maintenance**
  You definitely don't want to take a "set-it-and-forget-it" approach to security – your attackers aren't!