An Introduction of the Cyber Threat Landscape

To the Kansas House Committee on Vision 2020

March 18, 2015

Center for Internet Security

Andrew Dolan, Member Services Manager

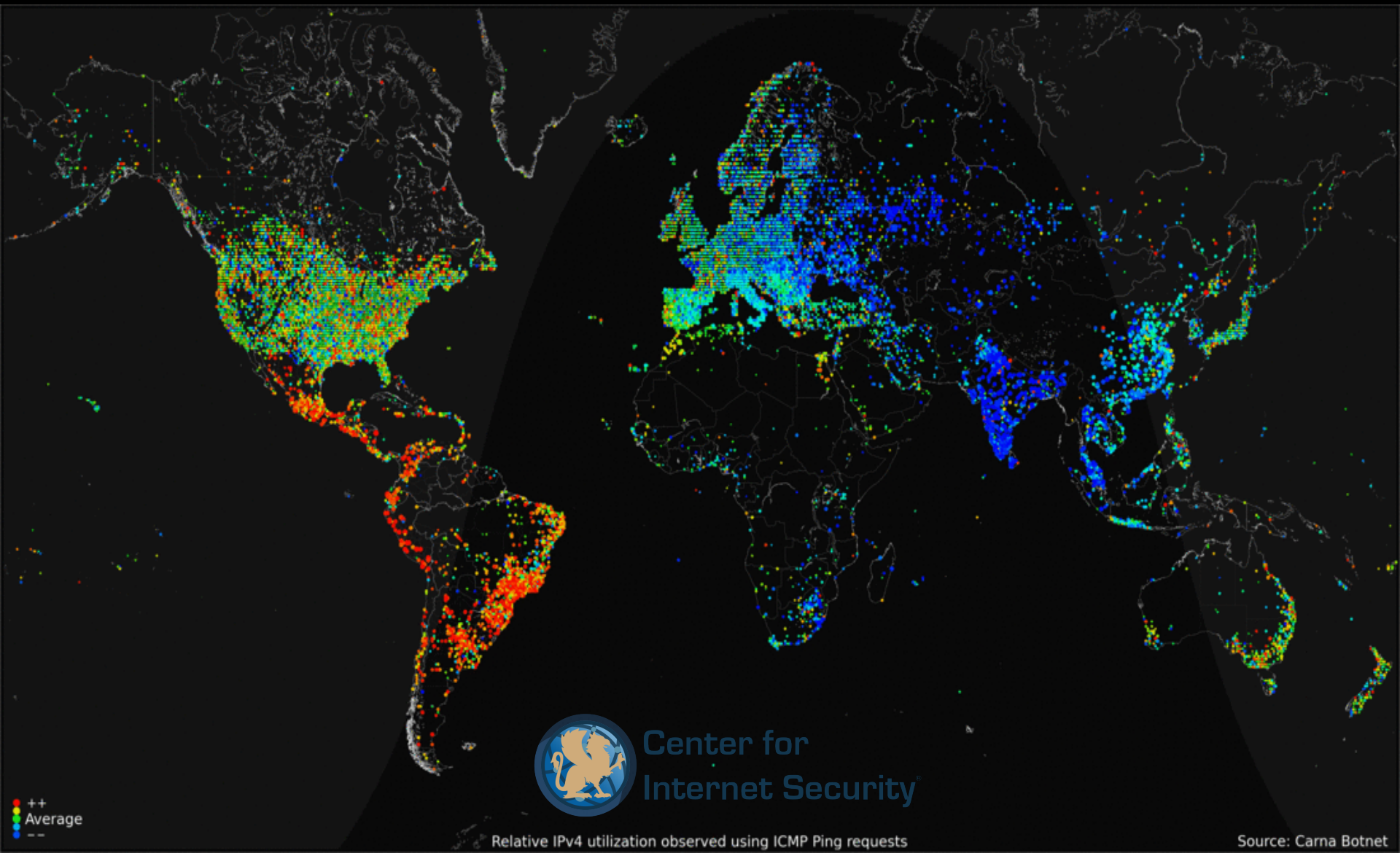
Center for Internet Security®

The Center for Internet Security is an international nonprofit organization focused on enhancing cyber security readiness and response for the public and private sectors.

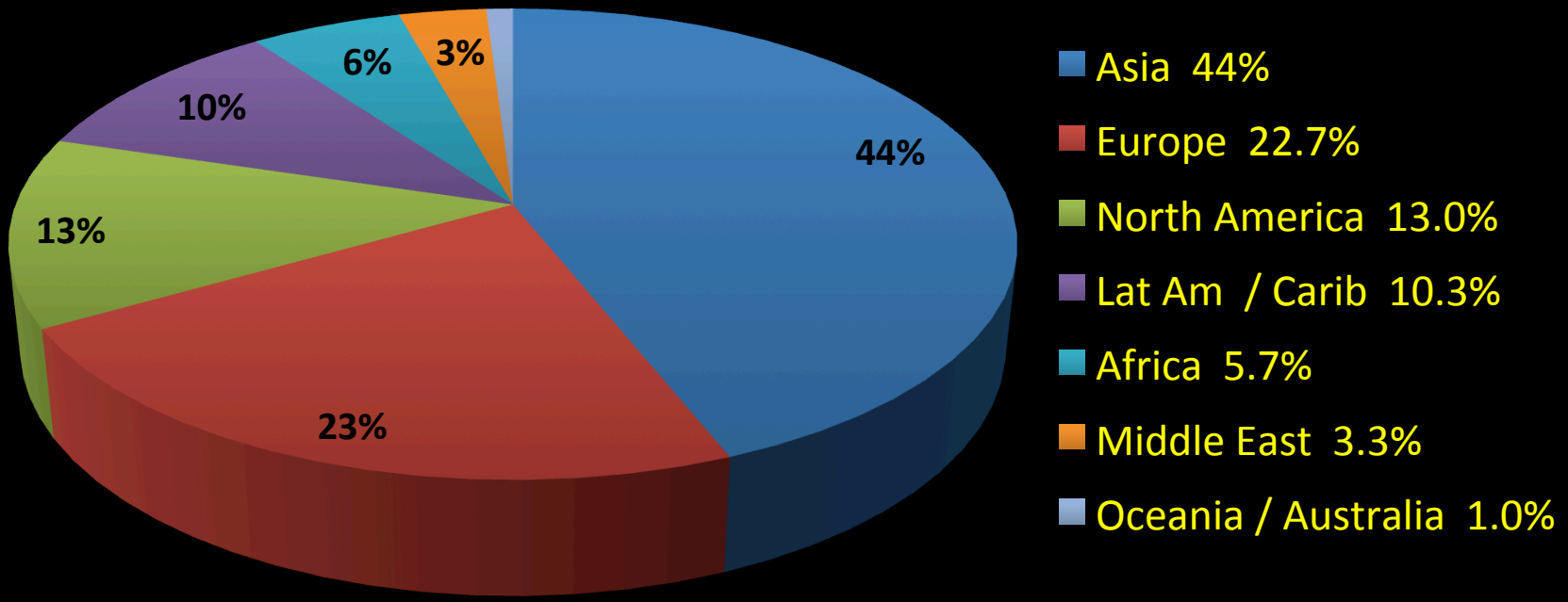
Jane Lute
CEO

William Pelgrin
CEO

The Internet



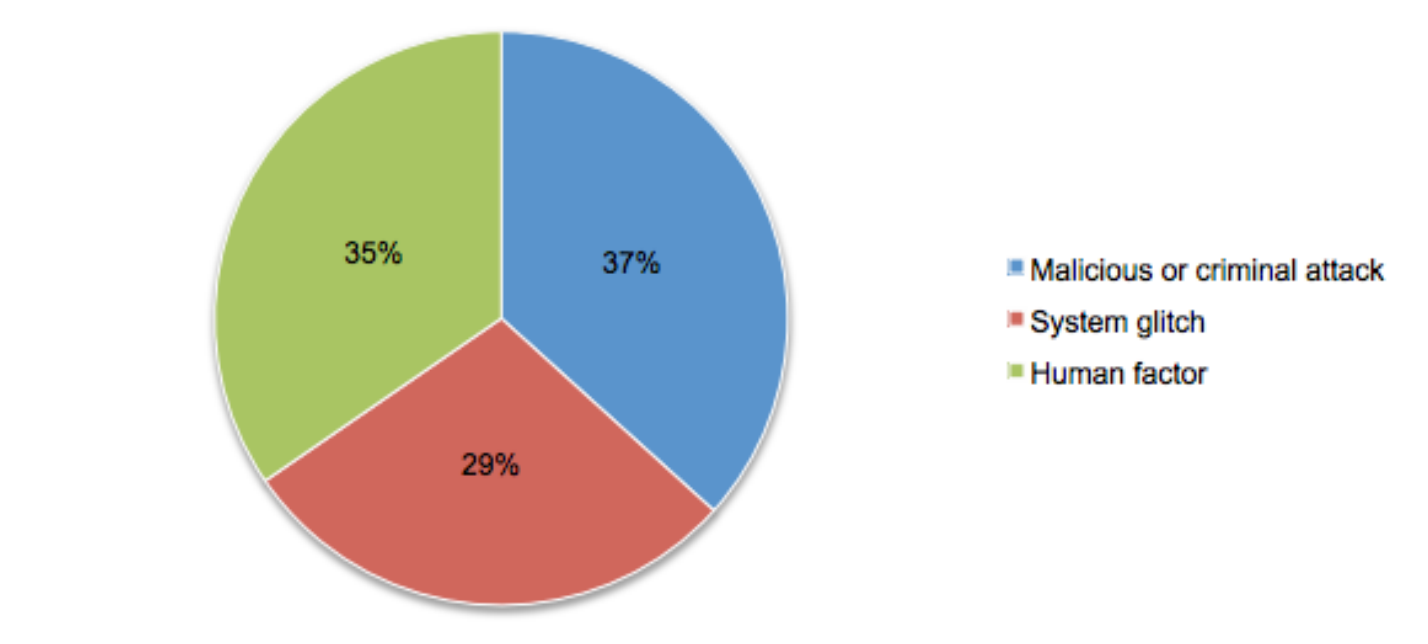
2.6 Billion Internet Users



Center for Internet Security®

What are the causes of data breaches?

According to the Ponemon Institute, data breaches have three main causes:



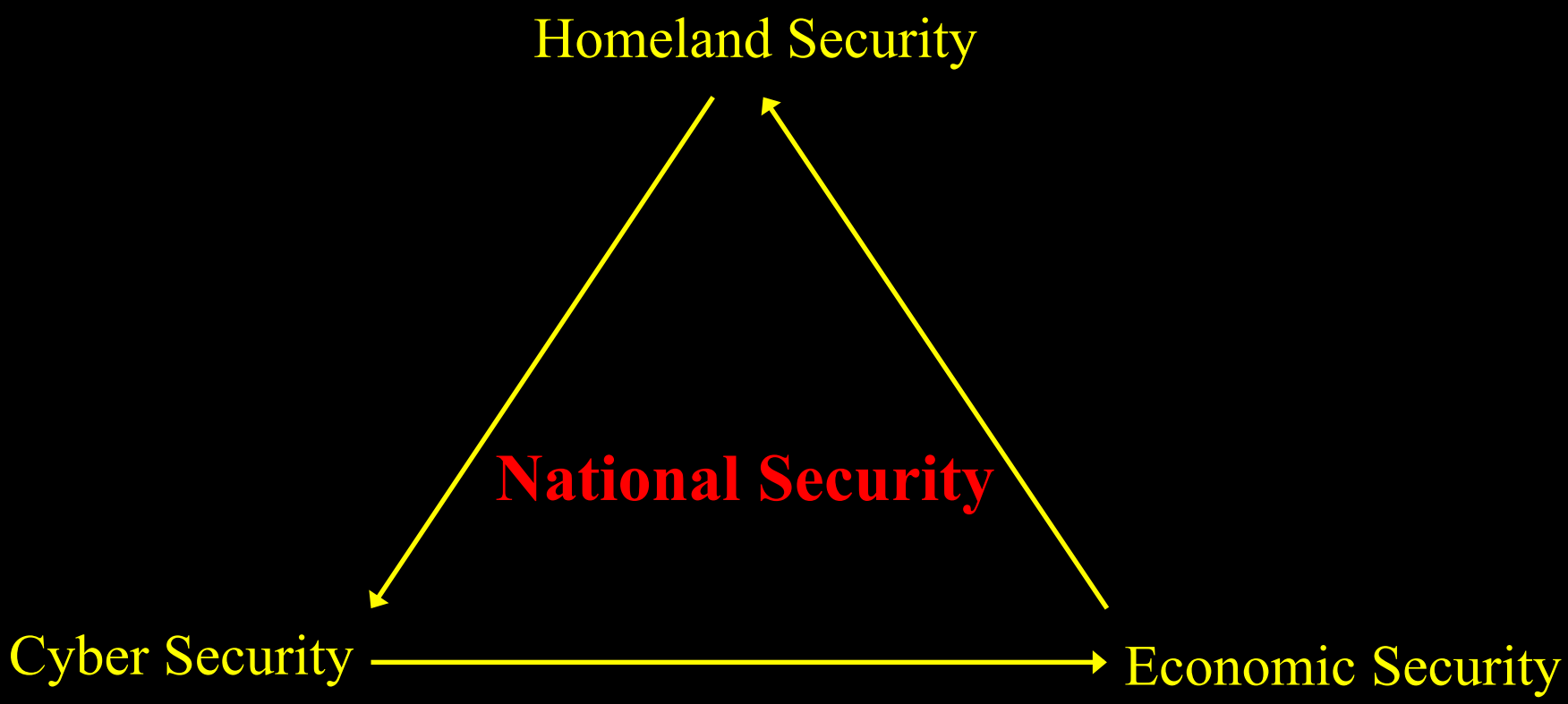
Center for Internet Security®

FBI Director
James Comey

"The cyber threat – both cyber espionage, cyber crime, and cyber terrorism is an enormous and an exponentially growing threat, and so will certainly be a key part of the next 10 years."

Center for Internet Security®

Our Security Posture Has Changed



Center for Internet Security®

Presidential Executive Orders
Critical Infrastructure Protection

- Directs federal authorities to improve information sharing on cyber threats with companies that provide support to CI
- Participation is voluntary
- New program to ease the delivery of classified information to eligible companies
- Expedited security clearances

Center for Internet Security®

Who Is Behind The Threats?

Cyber Criminals

Insider Threat

Hacktivists

Nation States

Center for Internet Security®

Center for
Internet Security®

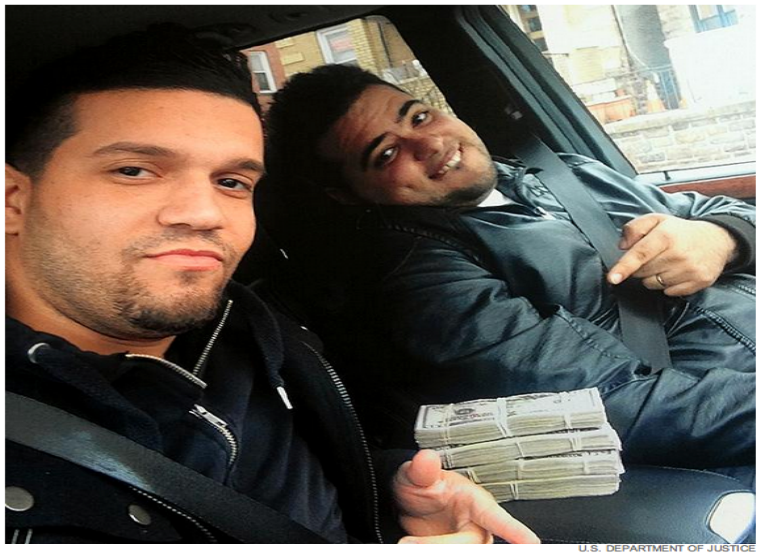
Global cyber, ATM heist nets thieves $45 million from 26 counties

Eight people have been arrested in New York for participating in a global scheme that stole ATM PINs and siphoned millions from banks and other financial institutions around the world.

Comments (46)

BY JOHN MARZULLI / NEW YORK DAILY NEWS

PUBLISHED: THURSDAY, MAY 9, 2013, 8:21 AM
UPDATED: FRIDAY, MAY 10, 2013, 5:31 AM



U.S. DEPARTMENT OF JUSTICE

Evidence photo showing defendants Elvis Rafael Rodriguez (left) and Emir Yasser Yeje with stacks of cash. Eight members of New York cybercrime cell were indicted in $45 million operation.

FOX NEWS

Search

U.S. Home | Crime | Terrorism | Economy | Immigration | Disasters | Military | Education | Environment | Persona

CRIME & COURTS

Anonymous linked to hack of Albuquerque police amid shooting protests

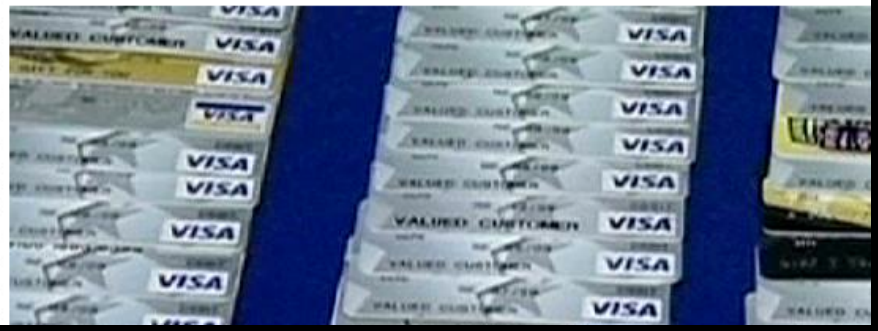
By Joseph J. Kolb · Published April 02, 2014 · FoxNews.com 148 0 0

While hundreds of demonstrators battled tear gas during a downtown demonstration against an alleged pattern of lethal force by the Albuquerque Police Department, the hacker activists known as Anonymous were apparently registering their protest with a cyber attack on the department's website.

US Video

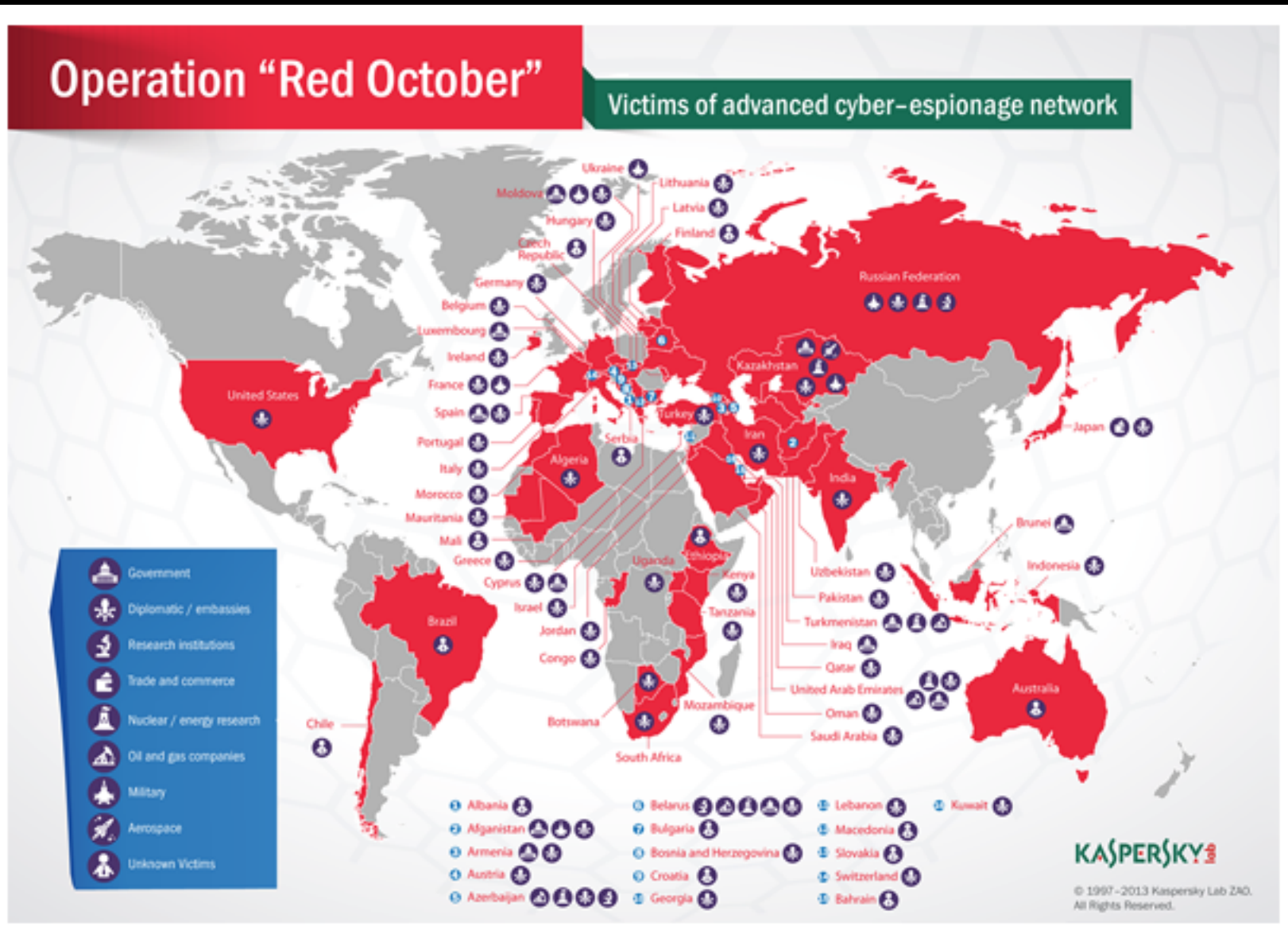
US names hackers in country's 'biggest cyber fraud case in history'

26/07 12:05 CET



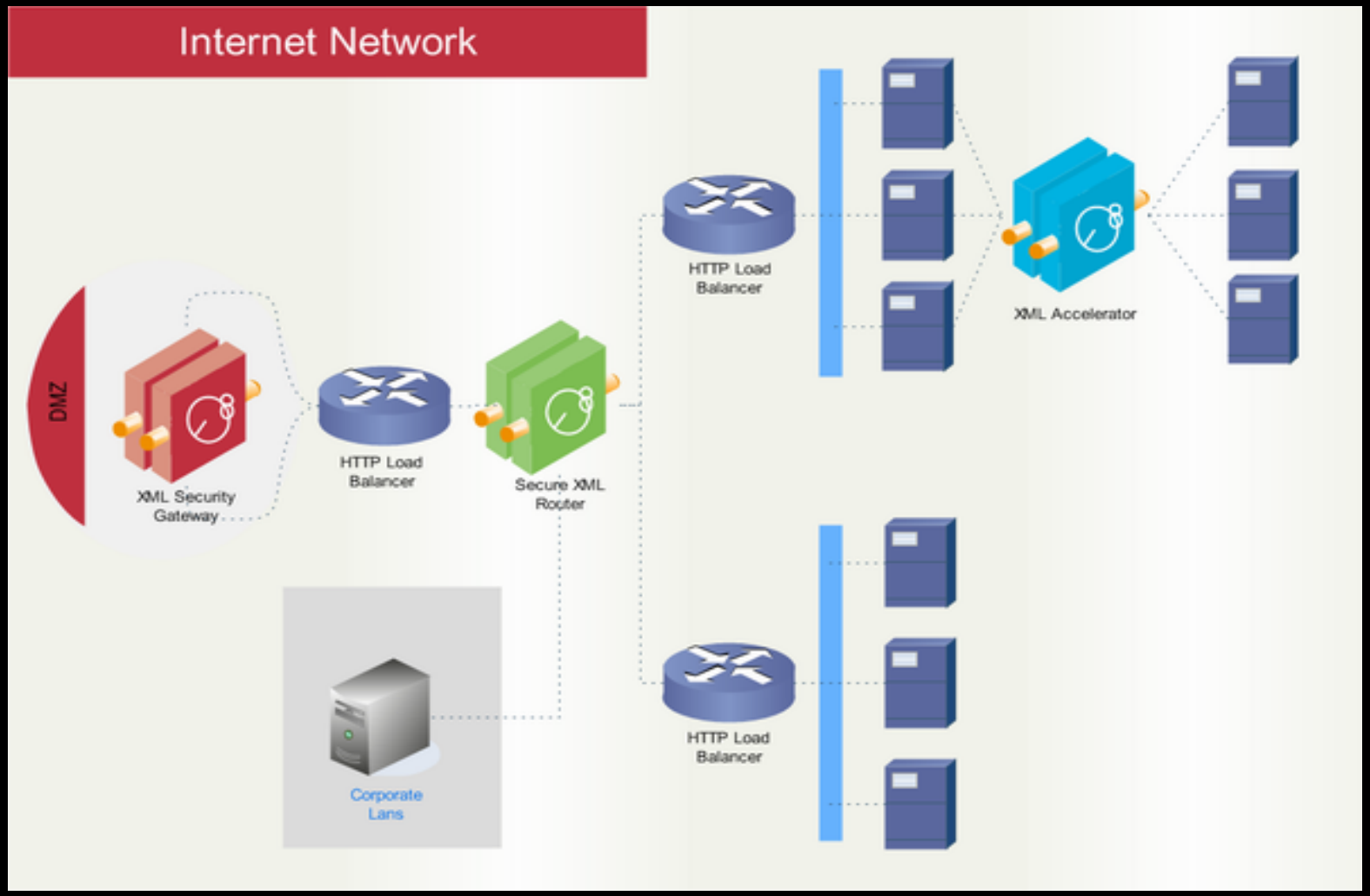
South Carolina Taxpayer Server Hacked, 3.6 Million Social Security Numbers Breached In Cyber Attack

By BRUCE SMITH 10/26/12 06:44 PM ET EDT AP



Center for Internet Security®

Traditional IT Infrastructure



Center for Internet Security®

ITS

Intelligent Transportation Systems

Critical Infrastructure

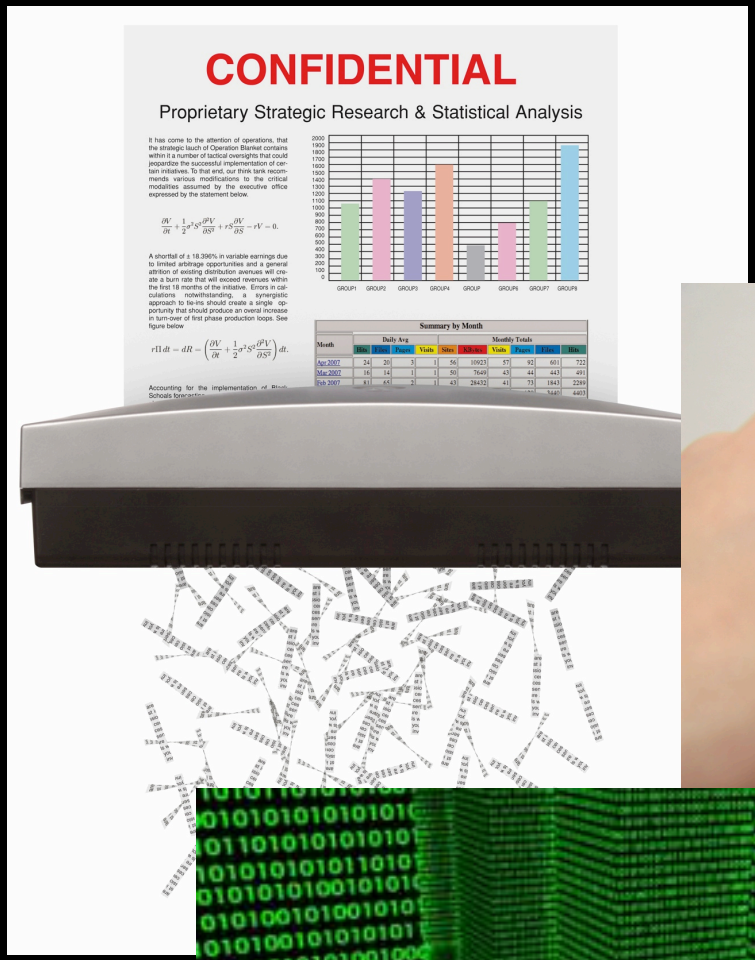
facebook

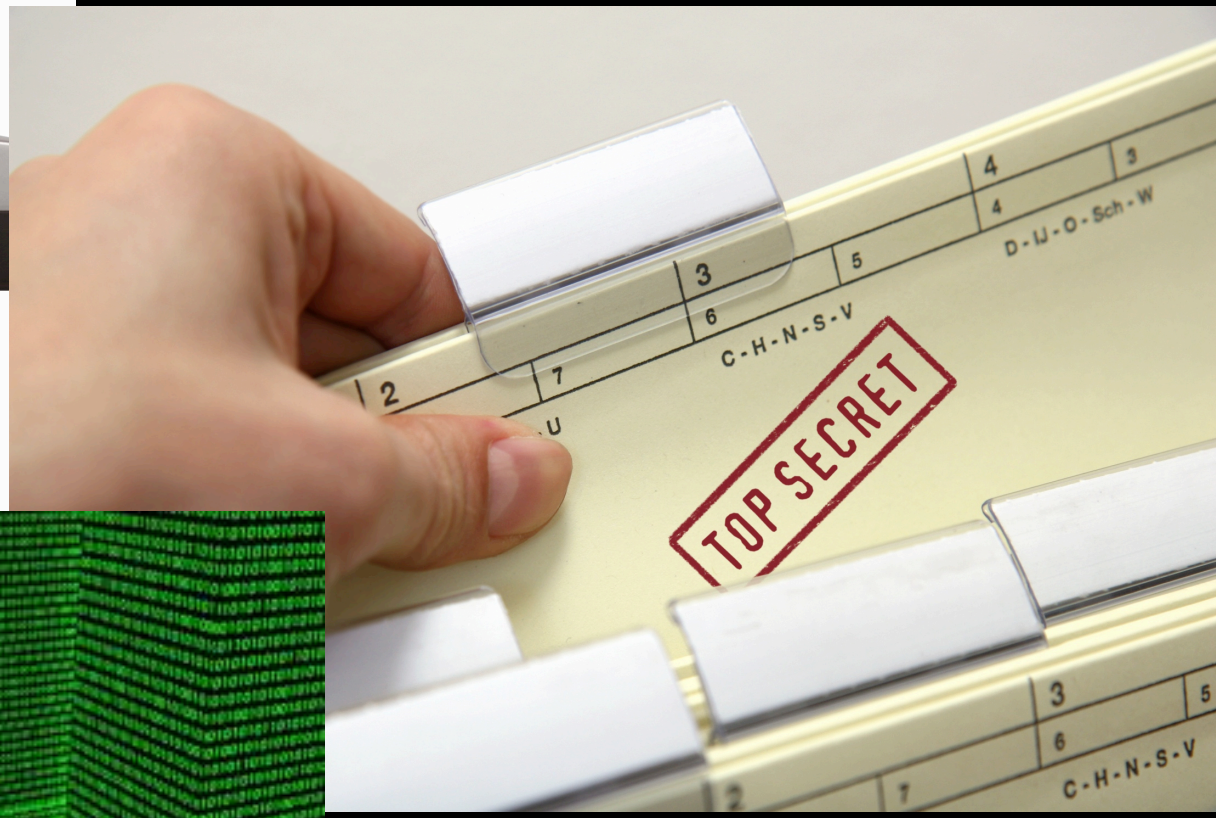
Register Now

The Internet is a tremendous tool for governments

Center for Internet Security

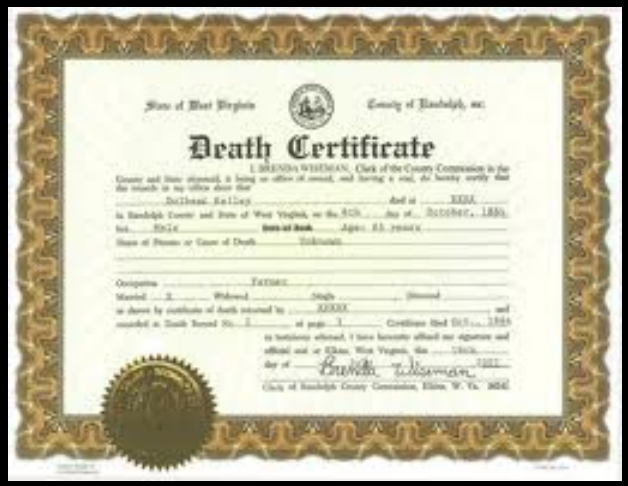
Criminals look for data…





Center for Internet Security®

And State & Local Governments have a lot of it!



Center for Internet Security®

Recent Attack Trends

Center for Internet Security®

Bash Bug

What is Bash?

- Bash is a common piece of software used to “tell your computer what to do.”

What does the Bash Bug do?

- It allows outsiders to take control of the affected device and run commands or install programs.

What is affected by the bug?

- Mac computers, Android phones, IPhones, servers, routers, medical devices, SCADA systems, and anything else using UNIX!

Center for Internet Security®

Content Management Systems

CIS/MS-ISAC recently uncovered an APT campaign that exploited CMS vulnerabilities to compromise networks. Attackers identified sites running vulnerable Ektron CMS.

- Vulnerability was only couple months old and allowed arbitrary file upload
- By uploading a webshell, attackers took control of the webserver
- Installed mimikatz/gsecdump to gain access to the cached credentials on the server
- Used the newly acquired credentials to pivot into the internal network of an organization
- Gained access to and exfiltrated significant amount of sensitive data

Center for Internet Security®

Attackers

- Use search tools to identify vulnerable systems
- Write scripts to attacks systems
- Then they own the system
  - Use your bandwidth to DDoS other systems
  - Compromise data
  - Compromise visitors/customers/citizens

Center for
Internet Security®

Content Management Systems Mitigation

Patch Your Systems!!!!!!

Center for Internet Security®

Recent Attack Trends
CryptoWall / CryptoLocker

Center for
Internet Security®

Cryptolocker

- Spreads through phishing emails
  - Attached zip file or straight executable
- Also installed after a Zeus infection
- After infection
  - Connects to C2 server (DGA) for 2048bit encryption key
  - If successful, encrypts all personal files on local hard drive and file shares focusing on office documents
- Demands $200-$600 for the decryption key
  - Payment must be made within 72hrs-100hrs otherwise the decryption key is destroyed

Center for Internet Security®

Cryptolocker Mitigation

- User awareness and training is the first line of defense
- Make sure you have backups
- DGA is broken so blocking the IP addresses for the C2 server is effectively preventing the encryption process to start
- Subset of files may be recovered from the restore points and volume shadow copies
- Pushing out a domain policy that prevents an executable to run from “Document&Settings” folder may be effective but this may also break other programs

Center for Internet Security®

And as always… Watch out for phish

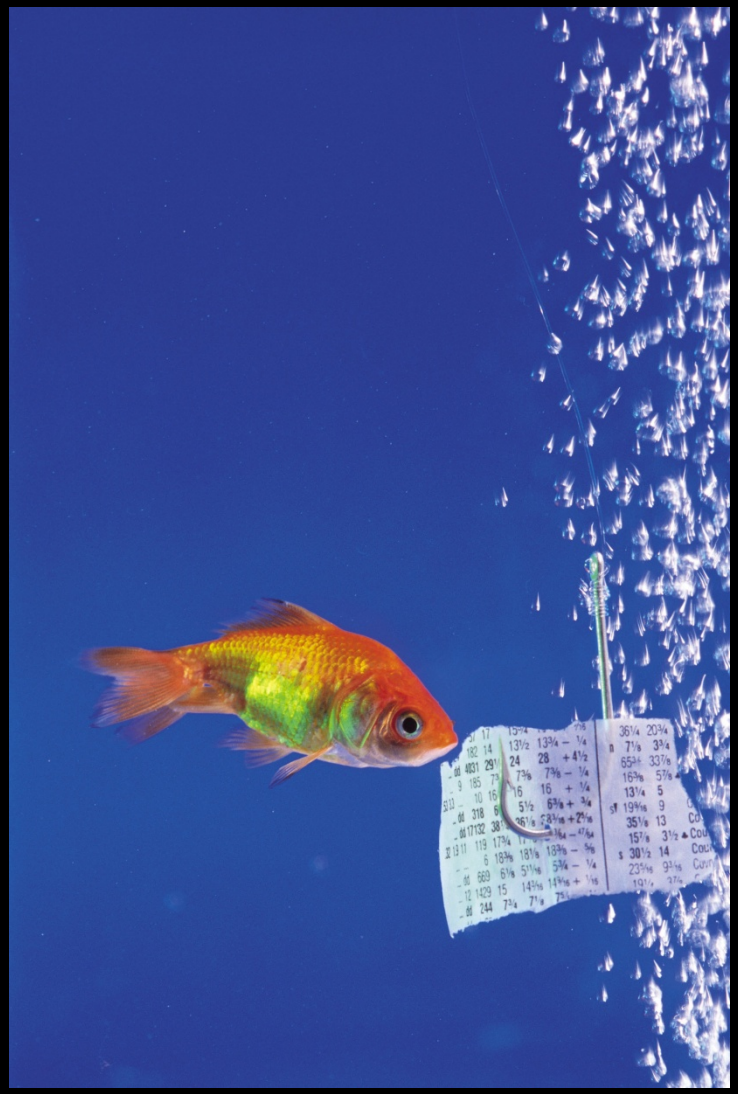
Phishing scams entice email recipients into clicking on a link or attachment which is malicious.

WELL WRITTEN

APPEARS CREDIBLE

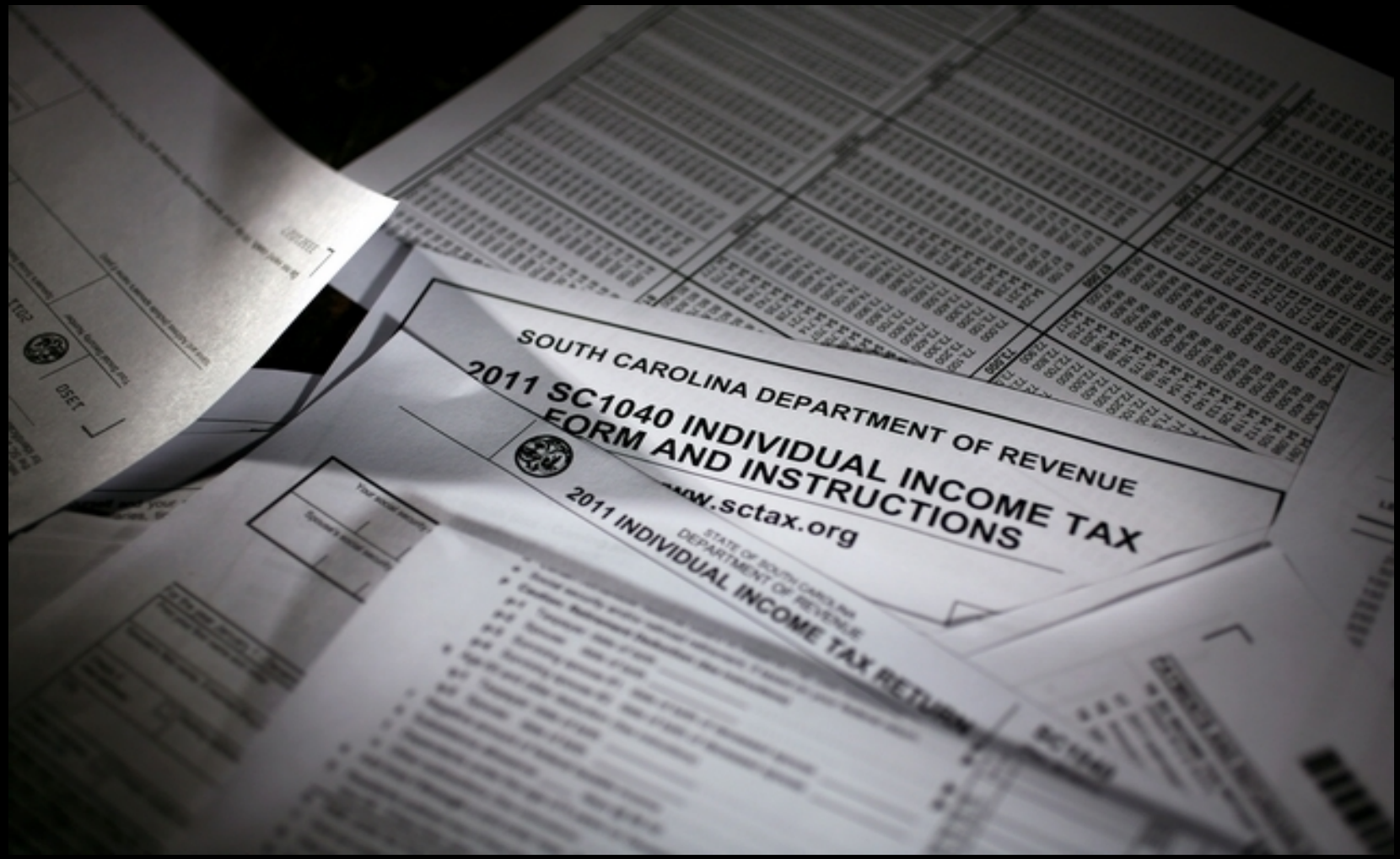
ENTICING OR SHOCKING SUBJECT

APPARENT TRUSTED SOURCE



Center for Internet Security®

South Carolina



Center for
Internet Security®

Emergency Alert Systems Compromised

'Hackers' access Emergency Alert System of local Great Falls, Montana TV station to broadcast fake warning of 'Zombie Apocalypse'

Time Newsfeed
Tue, 12 Feb 2013 14:33 CST

A Montana television station's regular programming was interrupted by news of a zombie apocalypse.

The Montana Television Network says hackers broke into the Emergency Alert System of Great Falls affiliate KRTV and its CW station Monday.

KRTV says on its website the hackers broadcast that "dead bodies are rising from their graves" in several Montana counties.

The alert claimed the bodies were "attacking the living" and warned people not to "approach or apprehend these bodies as they are extremely dangerous."

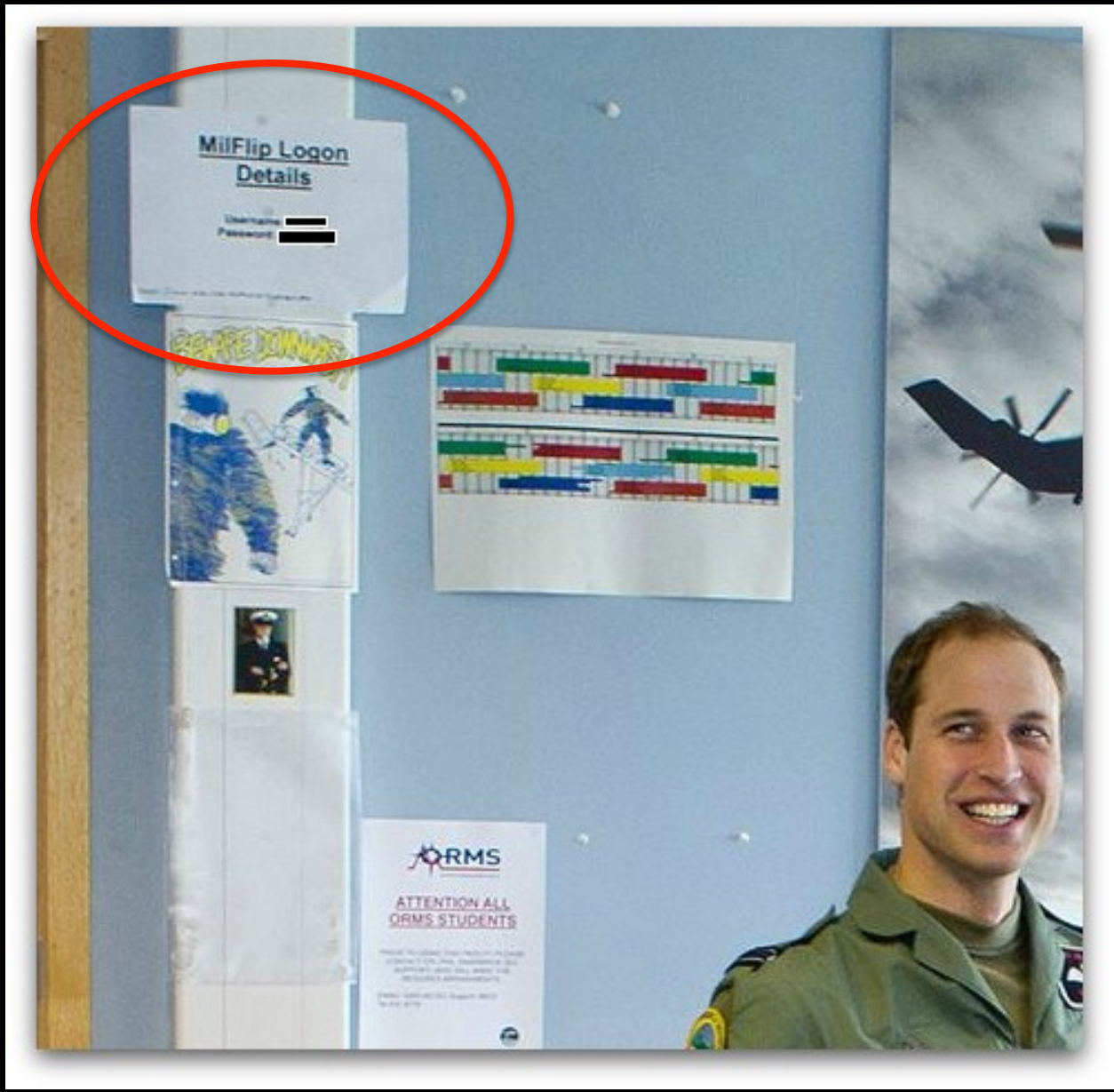
The network says there is no emergency and its engineers are investigating.

A call to KRTV was referred to a Montana Television Network executive in Bozeman. Jon Saunders didn't immediately return a call for comment.

Center for Internet Security®

We all make mistakes…

The trick is to learn from them!



Center for Internet Security®

Local School District Hacked!

A bank informed a School District that $758,758.70 was to be transferred overseas

The School District cancelled the transaction

The Bank than asked about the $1,190,400 that was already sent overseas

And the 1,862,400… also already sent overseas

School District hacked, $3 million stolen

Center for Internet Security®

What can you do?

Center for Internet Security®

Be Proactive!

- Leadership
- Governance
- Responsibility (Assign)
- Compliance (Measure)

Center for
Internet Security®

There's no such thing as 100% cyber security…

- Harden systems
- Keep your systems patched
- Update cyber security policies
- Monitor compliance with the policies
- Regularly scan systems
- Backup your systems on a regular basis and store off site
- Encrypt your mobile devices
- Train your users

Center for
Internet Security®

CIS Can Help!

- Free Resources
  - Daily tips
  - Monthly newsletters
  - Webcasts
  - Guides
  - Templates for public awareness materials
  - Incident Response for governments

Center for
Internet Security®

www.cisecurity.org

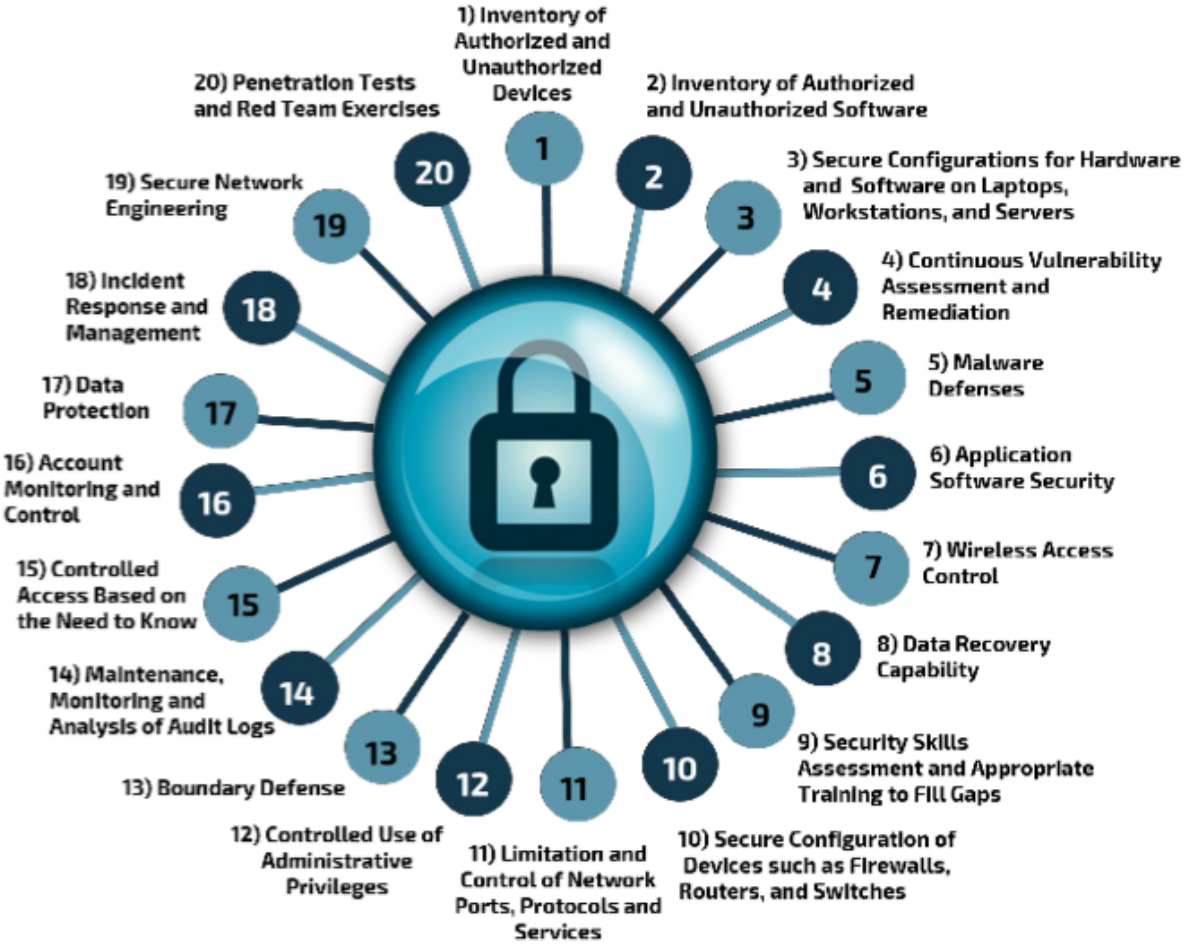
How does sharing information help protect your organization from attackers?

- Be prepared
  - Learning from others' best practices makes your organization stronger
  - Gather intel to help you be proactive
- Be willing to ask for help
  - Identify other resources to augment what you are doing
- Be a part of the solution
  - Take part in information sharing

Center for Internet Security®

Critical Security Controls

Specific and actionable ways to thwart today's most pervasive attacks



Center for Internet Security®

National Campaign for Cyber Hygiene

Count, Configure, Control, Patch, Repeat

5 Top Priorities

Count

Know what's connected to and running on your network

Configure Implement key security settings to help protect your systems

Control

Limit and manage Admin privileges and security settings

Patch

Regularly update all apps, software, and operating systems

Repeat

Regularize the Top Priorities to form a solid foundation of cybersecurity for your organization. Continue to improve!

Center for Internet Security®

Questions?

Info@msisac.org

(518) 880-0699

Center for
Internet Security®