## Government Information Security Blogs

# The Public Eye with Eric Chabrow

Keeping tabs on federal government efforts to protect citizens' privacy.

## Thoughts on 9/11 and Cyberthreats

**Thinking of the Unthinkable**

September 9, 2011 - Eric Chabrow

**Comments (0) Read All Posts (365)**

*What follows are some random thoughts about the Sept. 11, 2001, terror attacks and their impact on how the federal government approaches cybersecurity.*

Fears of a cyber 9/11 focus, not on a terrorist organization, but on a nation-state seeking to disrupt our key information networks, banking systems or electric grids. Little evidence has surfaced in the past decade that terrorists have the interest or wherewithal to stage a massive cyberattack. Groups such as al-Qaida focus on physical and human assaults; for instance, the threat surfacing of potential terrorist attack in New York and Washington over the weekend marking the 10th anniversary of the Sept. 11 are not aimed at IT networks, but at property and people (see ***Feds Confirm 9/11 Terrorist Threat***).

> **“The unthinkable was suddenly thinkable and the known risks weren't only known to us, but could be easily exploited by the terrorists unless we took real fast action.”**

Yet, physical assaults could disrupt IT networks. So, the main concern of IT security managers should be disaster recovery and business continuity planning. Being ever vigilant is the main lessons of 9/11. "Have your plans always up to date and ready to execute at a moment's notice," says Karen Evans, a former federal CIO (see ***9/11 Remembered: What We've Learned***).

Some IT security experts believe cyberterrorism cannot exist. One skeptic is Jim Harper, coauthor of last year's *Terrorizing Ourselves*, a book that contends politicians use fear for political purposes and spend vast sums of money on dubious security measures. In an interview I had with Harper when he was writing the book (see ***Are D.C. Insiders Stoking Cyber Fears?***), the director of information policy at the libertarian Cato Institute said: "I think there is no such thing as cyberterrorism because cyberattacks can't cause terror. They don't scare us and that is an essential element of terrorism as the name implies."

Harper may have a point. IT security professionals don't fret too much about terrorists threatening their systems. A Symantec survey of global IT security managers earlier this summer listed terrorism as dead last among seven risks that could threaten their businesses.

Still, just because Harper dismisses and I doubt the potential of a terrorist cyberattack, that doesn't mean it couldn't happen. After all, how many people 10 years ago imagined terrorists hijacking several jetliners in a single day and crashing them into the World Trade Center and Pentagon? Sept. 11 teaches us to be prepared for the unexpected. "Think the unthinkable," says Patrick Howard, chief information security officer at the Nuclear Regulatory Agency. "When we

**Latest Tweets & Mentions**

idtsoa Congress Gets Health Breach Update - http://t.co/uncD6WX - ^SA

ApexTechJobs RT @clearancejobs: Why are IT security #careers still so hot? Because there's still so much to do http://t.co/2bI0ps1

ClearanceJobs Why are IT security careers still so hot? Because there's still so much to do http://t.co/rcPBWvJ

wcleghorn US lawmaker hopes to get tough on phishing scammers who

twitter Join the conversation

1 Thoughts on 9/11 and Cyberthreats...
2 Research Projects Raise Privacy Issues...
3 Who Do You Trust? Part 2...
4 Anon Defector: 14 Ways to Secure IT...
5 Giving Gov't Workers Their Due Respect...
6 VA's CIO Moves From Laptop to iPad...
7 RSA Breach Evidence Uncovered...
8 Android's Popularity Has Its Costs...
9 16 Ways to Stay Safe on Facebook...
10 7 Controls for Mobile Devices Accessing...

More Posts

**Posts By Category**

**ACH Fraud**

**Advanced Persistent Threat**

**Agencies**

consider the threat, concentration on the worst-case scenarios is not only viable, but essential," he says.

## Wakeup Call

The 9/11 attack served as a wakeup call to a wide variety of threats the nation faced.

"The day after 9/11, everybody realized that these (IT security) weaknesses had to get shored up very quickly," says Mark Forman, the federal CIO on the day of the terrorist attacks (see *Shifting Course on Infosec Post-9/11*). "The unthinkable was suddenly thinkable and the known risks weren't only known to us, but could be easily exploited by the terrorists unless we took real fast action."

A decade later, Forman says he feels IT systems are much more secure than they were in 2001.

## DHS as a Cybersecurity Leader

The biggest impact on government IT security from the Sept. 11 attack was the creation of the Department of Homeland Security. The impetus of DHS was to thwart future attacks such as those that occurred in New York, Virginia and Pennsylvania. But over time, more of the federal government's efforts to secure government and civilian information security shifted in DHS, especially since President Obama took office in 2009. Indeed, Obama in May proposed legislation to give more cybersecurity authority in dealing with threats to executive branch systems to DHS (*White House Unveils Cybersecurity Legislative Agenda*).

Forman thinks the administration's plan presents new challenges in governing IT security in the federal government. The E-Government Act of 2002 gave much of IT security authority to the White House Office of Management and Budget and the administrator for e-government and IT (the federal CIO). "That's really hard for one federal agency to oversee another federal agency," Forman says. "It will be very interesting to see bureaucratically, how successful that becomes."

## 9/11 Legacy

The 9/11 attacks had a major impact on those charged with keeping government IT operational.

Before the aforementioned Karen Evans became the top IT official in George Bush's White House, she served as a senior manager at the Office of Justice Programs in the Justice Department, a job she held on Sept. 11, 2001. In an interview I had with Evans (see *3 Questions for Karen Evans*), I asked her what was her most memorable moment in her career?

> "That's really easy for me to talk about is because of the work that I did after Sept. 11 and that was when I was at the Office of Justice Programs and I was given the opportunity to work directly with the fire department up in New York City, the police department and the Port Authority and there were benefit programs that OJP had available. They were under the Public Safety Officers Benefits Program and so we had the opportunity to work directly with them.
>
> "And in an aftermath of that, it's really very interesting because they weren't letting a whole lot of people help them. They wanted to take care of themselves. You can imagine how fire departments, police departments and things like that, and they were very open to our programs. I'm still friends today with several of the people who I worked with that had to administer those benefit programs for the fire department. It really was a very moving, emotional experience. It was something that really helped me to be able to explain to my family what I do for a living because it was very real, because every day I would be late and tell them I'm working on something and he could see direct impact because they were talking about it on TV about how the federal government was helping the city of New York recover."

Digg digg del.icio.us reddit Share 2 retweet Print

## Post a Comment

**Please login or register to post a comment**

Login Register Need Help?

**Username:**

**Password:** Login

Remember Username?

Anti-Fraud
Anti-Malware
Anti-Money Laundering
Application Security
ARRA/HITECH
ATM Fraud
Audits Investigations Reports
Authentication
Awareness & Training
Bank Secrecy Act
Banking Today
Biometrics
Budgeting & Funding
Business Continuity & Disaster Recovery
Certifications
Check Fraud
CIO Council
Cloud Computing
Collaboration & Interagency
Committees and Testimonies
Compliance
Confidence In Banking
Congress
Cybersecurity
Data Loss
Debit, Credit, Prepaid Cards
Defense Department
Device Identification
E-Government Act
Electronic Health Records
Emerging Technology
Encryption
Endpoint Security
Federal Deposit Insurance Corp
Federal Reserve Board
Federal Trade Commission
FFIEC
FFIEC Handbook
FISCAM
FISMA
For Employers
For Job Seekers
Fraud
GAO
Governance & Standards
Governance, Risk & Compliance
Government Accountability Office
Gramm-Leach-Bliley Act
GRC
Guidance
Health and Human Services
Health Information Exchanges
HIPAA
Homeland Security Department
HR

Topics of Interest

## Homeland Security Department

- Understanding Technologies for Creating High-Security ID Cards
- Sensible DoD Asset Management and Tracking

## Incident Response

- Shifting Course on Infosec Post-9/11
- 9/11: The Global Perspective

## Agencies

- Protect Your Agency Against Dangerous & Costly Fraudulent Activities
- Managing IT Costs to Align with Agencies' Budgets

## Risk Management

- Protect Your Agency Against Dangerous & Costly Fraudulent Activities
- Managing IT Costs to Align with Agencies' Budgets

**ID & Access Management**

**ID Access & Management**

**ID Theft**

**Identity Theft Red Flags Rule**

**Incident Response**

**Information Security Compliance**

**Information Sharing**

**Insider Fraud**

**Insider Threat**

**Inspectors General**

**Intelligence**

**Law Enforcement**

**Laws, Regulations & Directives**

**Leadership & Management**

**Legislation**

**Log Analysis**

**Medical Identity Theft**

**Messaging**

**Mobile & Wireless**

**Mobile Banking**

**National Credit Union Admin.**

**National Security Agency**

**Network & Perimeter**

**Network/Perimeter**

**NIST**

**Office Comptroller of Currency**

**Office of Civil Rights**

**Office of Management & Budget**

**Office of Management and Budget**

**Office of National Coordinator**

**Office of Thrift Supervision**

**Pandemic Preparation**

**Payments Fraud**

**PCI DSS**

**Phishing**

**Physical Security**

**Privacy**

**Remote Capture**

**Risk Assessment**

**Risk Management**

**Sarbanes-Oxley Act**

**Security Leadership**

**SIM & SEM**

**SIM/SEM**

**Skimming**

**Social Media**

**Staff & Recruitment**

**Storage**

**Technology**

**Unified Threat Management**

**US-CERT**

**Vendor Management**

**Virtualization**

**Web Security**

**White House**

Wire Fraud

## Authors & Blogs

### The Field Report

There are 18,000 banking institutions in the U.S., and somebody has to blog about their breaches, concerns and security successes.

**By Tom Field**

### The Agency Insider

From the FDIC to the NCUA, banking institutions take guidance from myriad government agencies and regulations. Here's where we make sense of it all.

**By Linda McGlasson**

### Secure Marketspace

A look into how the security and privacy concerns of consumers and citizens impact institutions and government agencies.

**By Mike D'Agostino**

### Information Technology Risk Management

Not all risks are created equal. Understand, manage and transfer risks, as necessary. Ignore none.

**By Sanjay Kalra**

### Compliance Insight

A practitioner’s view from the inside out.

**By David Schneier**

### The Public Eye

Keeping tabs on federal government efforts to protect citizens' privacy

**By Eric Chabrow**

### The Expert's View

Insights from industry experts

**By Industry Experts**

### Industry Insights

Insights and opinions from the thought-leaders who represent the industry’s services and solutions providers.

**By Industry Insights**

## Career Insights

Insights from advisors, consultants and practitioners who know what it takes to be a successful security professional

**By Career Insights**

## The Security Scrutinizer

Keeping an eye on efforts to protect the privacy and security of personal healthcare information

**By Howard Anderson**

## The Fraud Blog

Tracking fraud incidents and trends wherever -- and however -- they occur.

**By Tracy Kitten**

GovInfoSecurity.com Blogs Home

## Recent Comments

"*What is being overlooked in all of this is the personal responsibility issue. If I own a business and operate online...*"
Read Post | Jump to Comments

"*The "buck" or "security" is not the sole responsibility of financial institutions. The client must be a strong...*"
Read Post | Jump to Comments

"*Making Financial Investment fraud proof or at least increasing the trust of customers and investors, banks should...*"
Read Post | Jump to Comments

Register to Post Comments

## All Posts By Date

**September, 2011**

**August, 2011**

**July, 2011**

**June, 2011**

**May, 2011**

**April, 2011**

**March, 2011**

**Older Postings**

## The ISMG Network

### Banking

BankInfoSecurity.com
US UK EU IN Asia

Interviews
Blogs
Careers

### Credit Unions

CUInfoSecurity.com

Interviews
Blogs
Careers

### Government

GovInfoSecurity.com

Interviews
Blogs
Careers

### Healthcare

HealthcareInfoSecurity.com

Interviews
Blogs
Careers

### Resource Centers

FFIEC Authentication Guidance