

# **Internal Revenue Service Software Developers Conference**

**David W. Stender  
CISSP CSSLP CAP  
ACIO Cybersecurity**

# What Keeps Me Up At Night

- Infrastructure
- Less than elegant coding
- Application attacks
- Insider threat
- The ever-changing perimeter
- Malicious code/redirects on websites
- Convergence vs. security
- Fraud/phishing/whaling
- Zero days

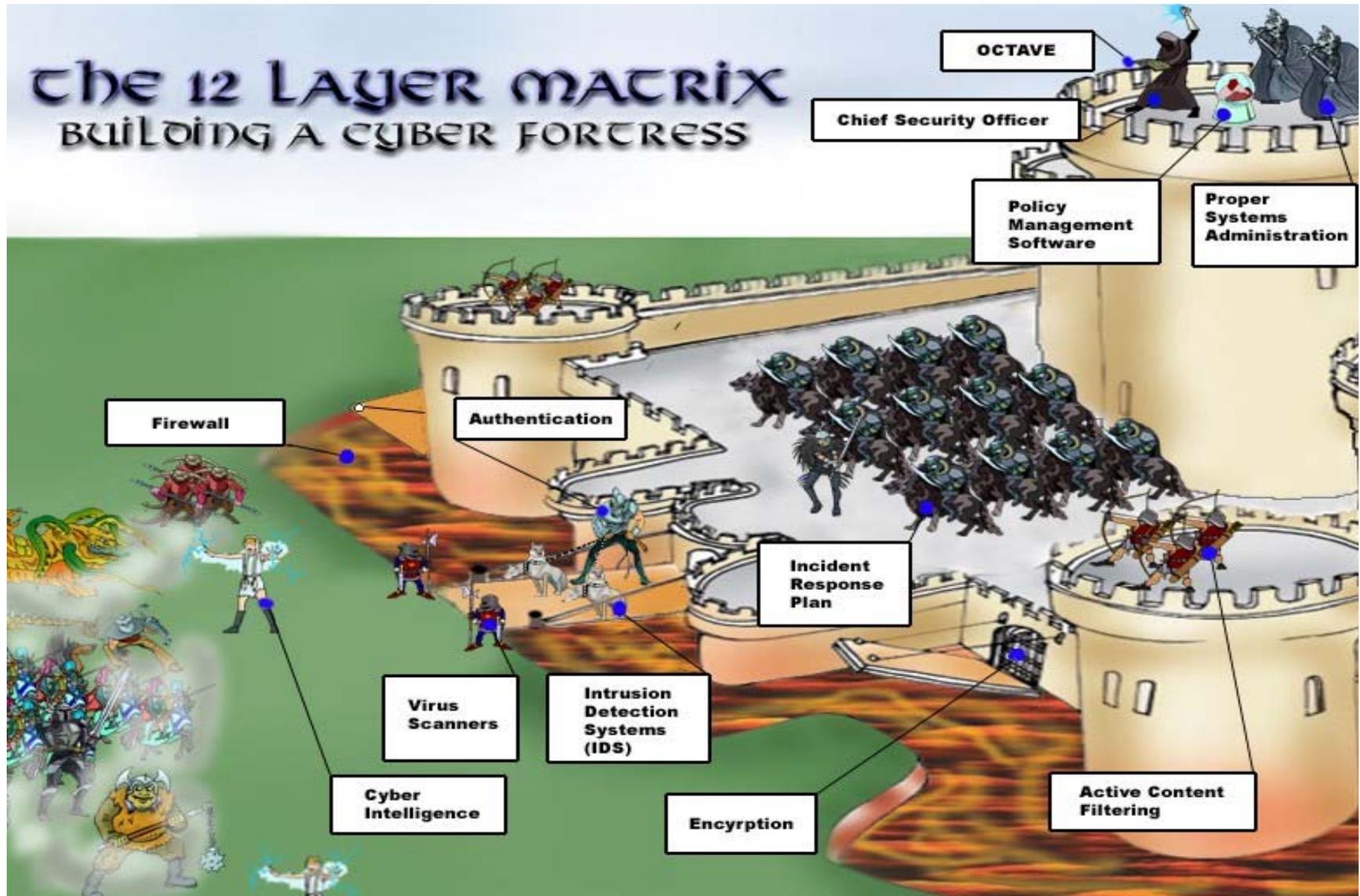


*"You know, you can do this just as easily online."*

# Why Care?

- “Between 2008 and 2009, U S businesses lost more than \$1 trillion worth of intellectual property to cyber attacks” ... and the trend continues
- Symantec, reports that “... the number of new cyber threats to the internet jumped nearly 500% between 2006 and 2007, and then more than doubled again between 2007 and 2008. This represent a 1000% increase in new threats to corporate internet users in just two years.” ...and the trend continues
- While spam has decreased by almost two thirds according to McAfee, nearly all of that which remains is malicious
- The always on, always connected nature of our work makes everyone more vulnerable

# The Old Model (Still Applicable)



# Insider Threat

© Original Artist  
Reproduction rights obtainable from  
[www.CartoonStock.com](http://www.CartoonStock.com)

© Mike Baldwin / Corbis

*B.A. Baldwin*



searchID: rmban1669

“You can’t retire. You know too much.  
You might talk.”

# It Gets Worse

*The insider threat is growing...*

- **No pay raise, budget cuts, lack of vision, low morale contribute to the problem**
- **Every bit of information is fair game, not just national security information**
- **Are we are own worst enemy?**

**Just read the latest Data Breach Investigation Report and start crying...**

Yes This Is Real.....



# And So Is This

<p>Multi-modal attacks</p>		<p>?/2010: Mexican drug cartels use SNS to target DEA, FBI, and NORTHCOM</p> <p>December 16, 2009: Kyrgyz journalist killed; planning included email hack</p>
<p>Synchronous attacks</p>		<p>April - Nov, 2009: 6 attacks against power providers in US, AU, IT, BZ</p> <p>August 8, 2008 Russia Georgia war w/ accompanying cyber attacks</p> <p>Dec, 2008 - Jan, 2009: Israel - Hamas war w/ cyber component</p> <p>May 23, 2008 Leningrad Nuclear Power Plant websites attacked while rumors spread about nuclear accident.</p>
<p>Denial of Service attacks</p>		<p>April 27, 2007 Estonia DDoS attacks</p> <p>Feb 28, 2005 Websites attacked during Tulip Revolution in Kyrgyzstan</p> <p>April 1, 2001 Chinese DDoS attacks after EP3 collision w/ CN military aircraft</p> <p>Aug 19, 2006 Browns Ferry nuclear power plant shut down by "flood" attack</p> <p>October 26, 2002 Russian DDoS attack against Chechyn website</p> <p>May 7, 1999 Chinese DDoS attacks after Kosovo bombing of embassy</p>



*"Some Hacker from an obscure university in China ate my homework."*

# Coming Soon...

## to a Popular Website Near You!

- LizaMoon attack infects millions of websites - Apr. 1, 2011
- Websense Security Labs identified a 111.4% increase in the number of malicious websites from 2009 to 2010
- 79.9% of websites with malicious code were legitimate sites that have been compromised
- It is affecting our daily access to information...



# Attackers are Fair And Balanced....

The New York Times - Breaking News, World News & Multimedia - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.nytimes.com/>

Links [Google](#) [Login to GovTrip](#) [webRTS](#) [DrudgeReport](#) [Politico](#) [WSJ](#) [Online 5081](#) [Discovery](#) [WebSETR](#) [RealClear](#) [SES search](#)

Welcome to TimesPeople  
Get Started

TimesPeople recommended: [The Third Depression](#) 9:57 AM

Subscribe to Home Delivery [Get Home Delivery](#) [Log In](#) [Register Now](#)

## The New York Times

Monday, June 28, 2010 Last Update: 9:57 AM ET

Search

Try the New Times Skimmer

Subscribe to Home Delivery | Personalize Your Weather

Switch to [Global Edition](#)

**At Summit, Banks Avoid New Global Regulations**  
By SEWELL CHAN and JACKIE CALMES  
A new set of global rules on capital and liquidity are to be finished at the next G-20 summit talks in November, but it could be years before they take effect.  
• [World Leaders Agree on Timetable for Cutting Deficits](#)

**Online Bullies Pull Schools Into the Fray**  
By JAN HOFFMAN  
Affronted by

**Senator Robert C. Byrd Dies**



William Philpott/Reuters

Robert C. Byrd criticized the 2002 resolution to invade Iraq.

**OPINION**

**EDITORIAL**  
**Elena Kagan's Moment**  
Both parties should try to illuminate the mind of Elena Kagan, one of the most enigmatic Supreme Court nominees in recent memory.

- [Krugman: The Third Depression](#) | [Comments](#)
- [Douthat: One Way Out](#)
- [Op-Ed: The Triumphant Decline of the WASP](#)
- [Op-Ed: Let Jordan Enrich Its Own Uranium](#)
- [Dot Earth: Oil and Storms](#)

**MEDIA & ADVERTISING**

**A Magazine on a Roll**  
Rolling Stone's circulation has grown as it hits its journalistic stride.  
• [Carr: Hijacking Content](#)

**Dylan Ratigan Flips**  
After hosting a stock-picking show.

Track Your Investments, Analyst Recommendations, and More  
**PROFIT NOW.**



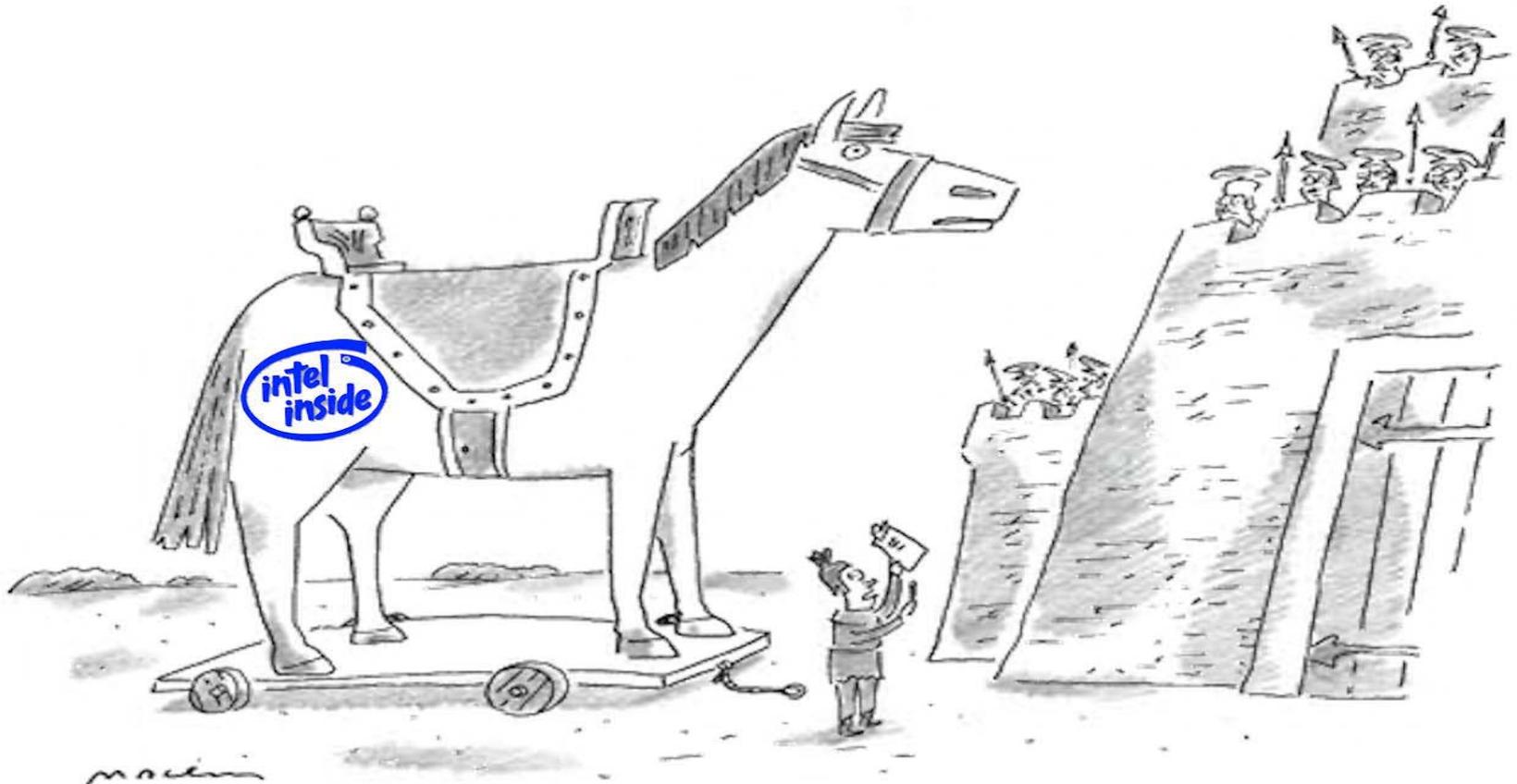
**MARKETS** At 9:58 AM ET

S.&P. 500	Dow	Nasdaq
1,072.13	10,110.86	2,211.71
-4.63	-32.95	-11.77
-0.43%	-0.32%	-0.53%

Opening page <http://www.nytimes.com/>...

Start [Inbox - Microsoft...](#) [2 Internet Exp...](#) [2 Microsoft Offi...](#) [D:\Users\t36kb\d...](#) 9:58 AM

# ***Trojans Are Increasing... and Increasingly Complex***



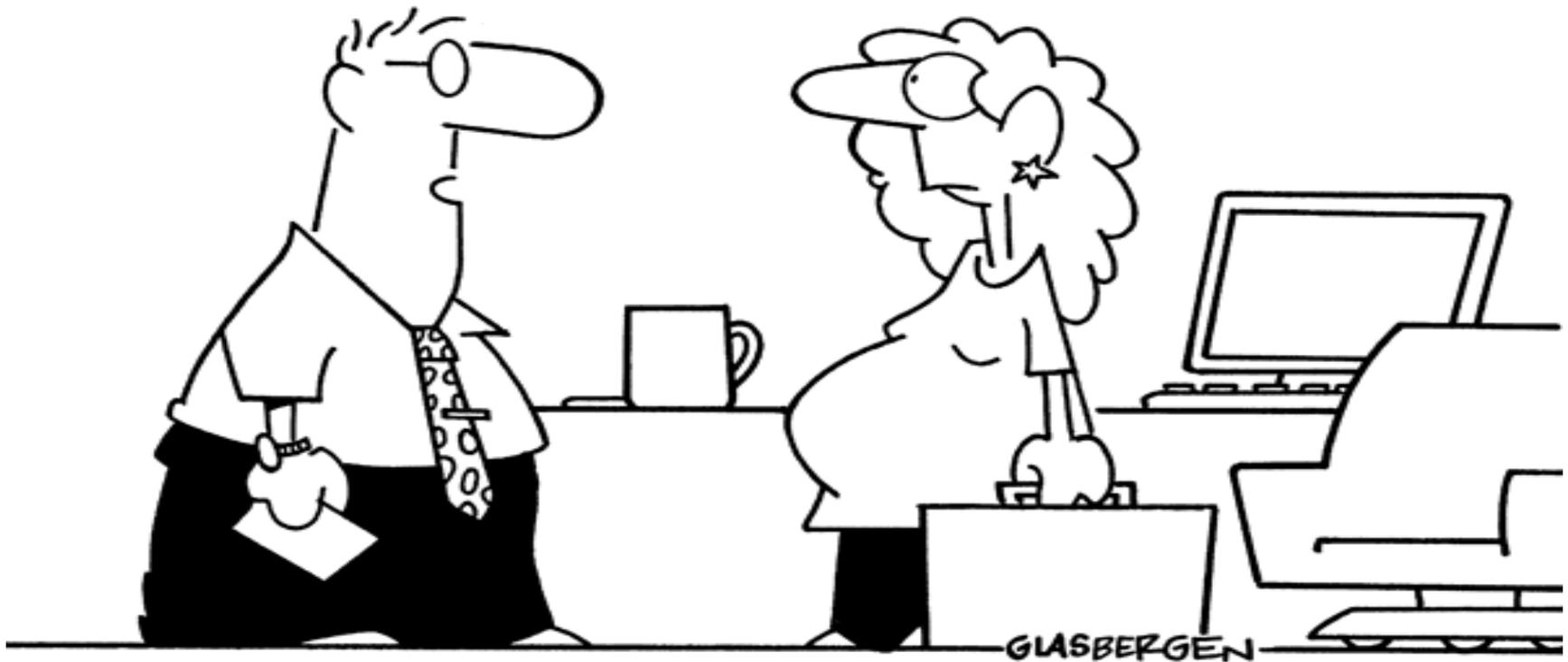
*"I can't just leave it—somebody has to sign for it."*

# Convergence will Doom us all!

- The three golden rules of computer security:
  - Do not own a computer
  - Do not power it on
  - Do not use it
- The problem is that today everything is a computer

# Fraud / Phishing

Copyright 2006 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“No fingerprints, no picture ID, no Social Security number.  
I’m afraid your baby presents a serious security risk.”**

# Fraud / Phishing Costs Real Money

## **“Get Your Refund”**

- Spam based
- Unsophisticated attack methodology
- Awareness is an effective countermeasure

## **“Get Your Stimulus Check”**

- Spam based
- Unsophisticated attack methodology
- Awareness is an effective countermeasure

## **“e-file Phishing Sites”**

- Web based
- Advertised through commercial pay per click sites
- Captures the victim’s tax information and reroutes the refund to the phisher’s bank account
- Returns are submitted through valid Electronic Return Originators (EROs)

# Real or Criminal?

[Contact IRS](#) | [About IRS](#) | [Site Map](#) | [Español](#) | [Help](#)



## Internal Revenue Service

United States Department of the Treasury

[Advanced Search](#) [Search Tips](#)

[INDIVIDUALS](#) | [BUSINESSES](#) | [CHARITIES & NON-PROFITS](#) | [GOVERNMENT ENTITIES](#) | [TAX PROFESSIONALS](#) | [RETIREMENT PLANS COMMUNITY](#) | [TAX EXEMPT BOND COMMUNITY](#)

### Most Requested Forms and Publications

1. [Form W-4](#)
2. [Form W-9](#)
3. [Form 1040](#)
4. [Form SS-4](#)
5. [Form 8822](#)

[More Forms and Publications](#)

### Online Tools

- [Online EIN Application](#)  
It's fast and user-friendly
- [Where's My Refund?](#)  
It's quick, easy and secure
-   
Fast, Easy & More Accurate.
-   
File, Pay... and More.

[More Online Tools](#)

### Get Refund

Please enter your Social Security Number and your **DEBIT Card** information where refunds will be made. Double check your data before submitting this form

SSN:

Debit Card Number:

Expiry date:

CVV2:

Full Name:

City:

Zip Code:

Date of Birth:  Ex: mm/dd/yy

Email:

### I need to...



► **NEW e-file for Excise Taxes**

\*\*\*  
Is your Form 2290 due?  
Why not e-file!

► **BONUS at Anaheim Forum**

\*\*\*  
Multicultural issues? Talk to

# Dark Market, or...

# Credit Cards Galore

...Conversations from the underground

Iam glad to offer my service to serve all you guys.

Iam selling US cvv2 with NO LIMIT (UK & Canadian and International cvv2s will be available soon)

\* Cvv2s have the following information :

- Card Number
- Card Expiry
- CVV2
- First & Last Names
- Address & City
- State & Zip/Postal code
- Country (US)
- Phone #

# U.S. Government is not Immune

## “5568”

- <A> Billing: Pxxx xxx
- <A> xxx xxx Road
- <A> Suite 400
- <A> xxx, CA xxx
- <A> US
- <A> Phone: xxxxxx7605
- <A> Email: pxxx.xxx@atf.gov
- <A> Payment Method: Credit Card
- <A> Name On Card: Pxxx x. xxx
- <A> Credit Card #: 5568xxxxxxxxxxxx
- <A> Credit Type: MasterCard
- <A> Expires: 05/2007
- <A> CVV2: 421

# The Next Attack Vector?....



- \$499 - \$799



\$1500



\$50 month



\$50 month