Internal Revenue Service Software Developers Conference

David W. Stender
CISSP CSSLP CAP
ACIO Cybersecurity

What Keeps Me Up At Night

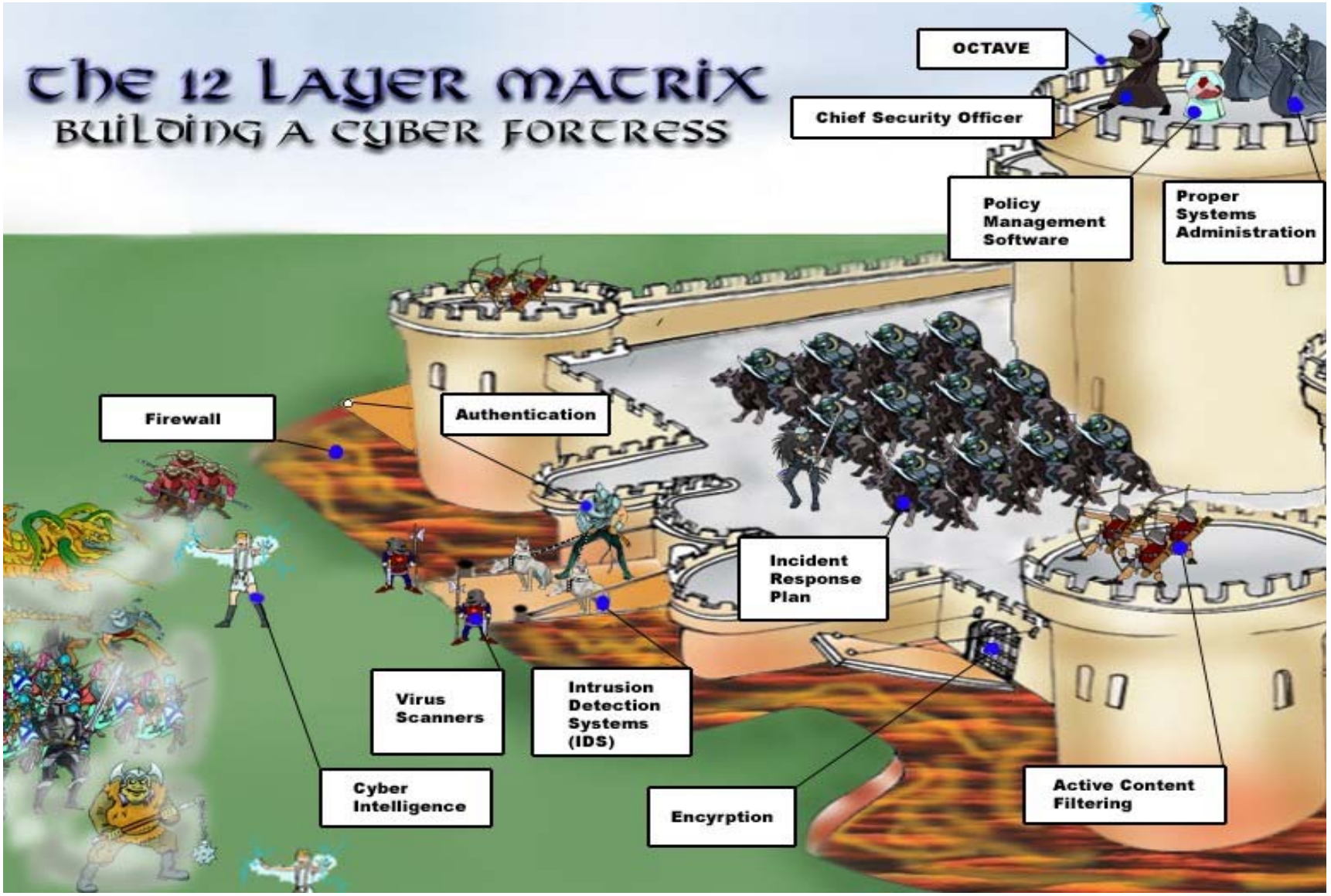
- Infrastructure
- Less than elegant coding
- Application attacks
- Insider threat
- The ever-changing perimeter
- Malicious code/redirects on websites
- Convergence vs. security
- Fraud/phishing/whaling
- Zero days

"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

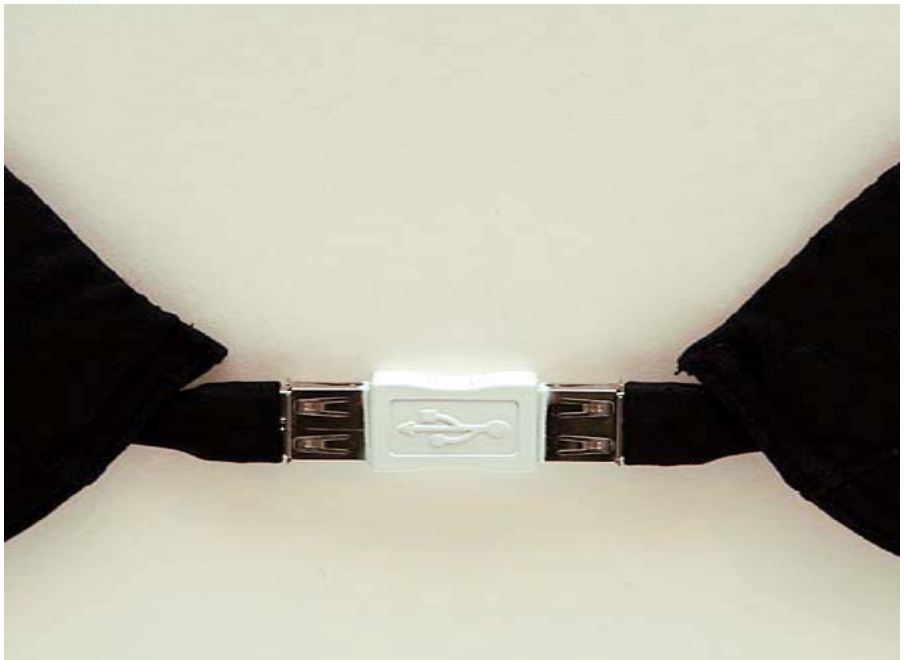
It Gets Worse

The insider threat is growing…

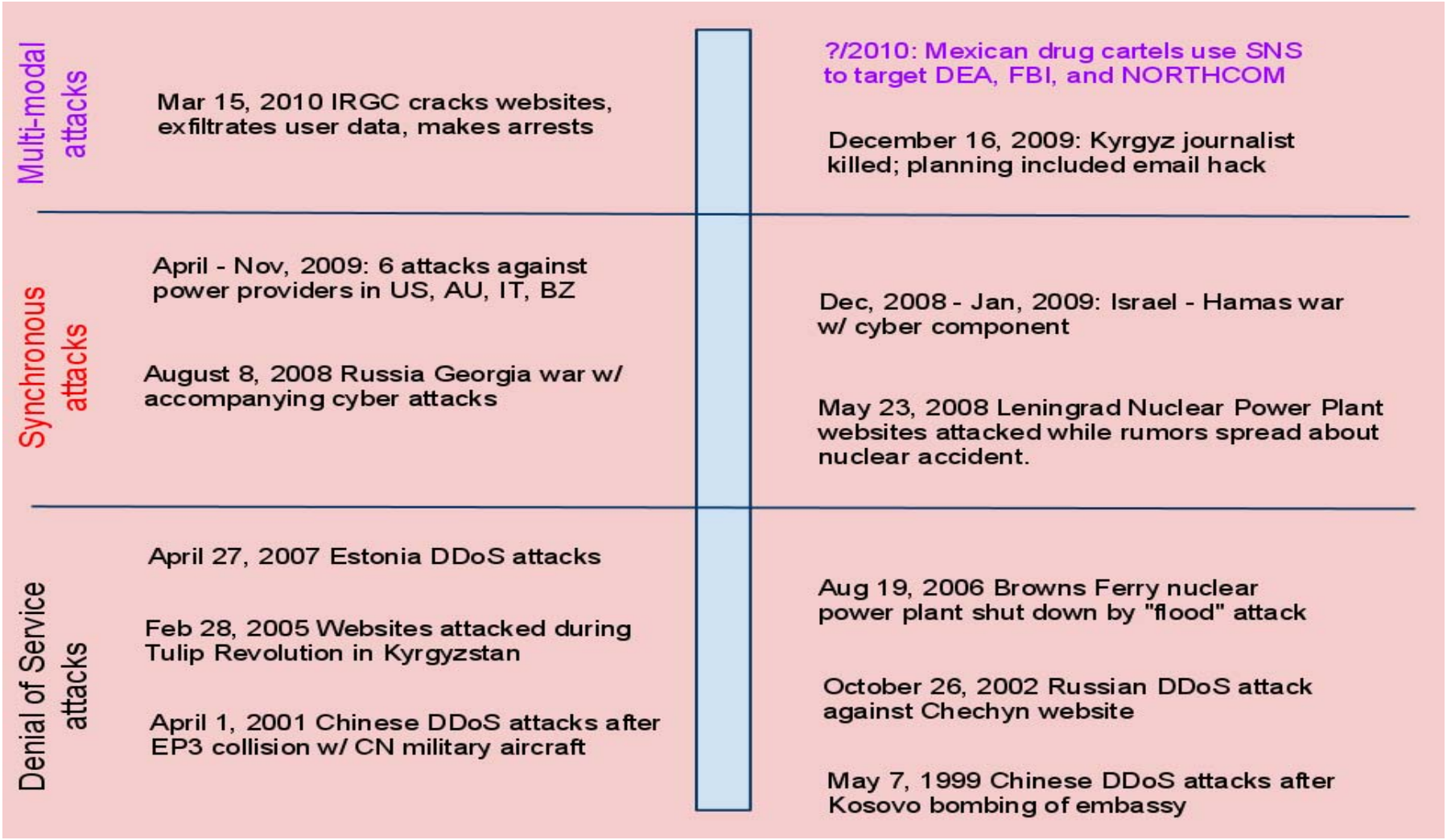
- **No pay raise, budget cuts, lack of vision, low morale contribute to the problem**
- **Every bit of information is fair game, not just national security information**
- **Are we are own worst enemy?**

Just read the latest Data Breach Investigation Report and start crying…

Yes This Is Real…..



And So Is This



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

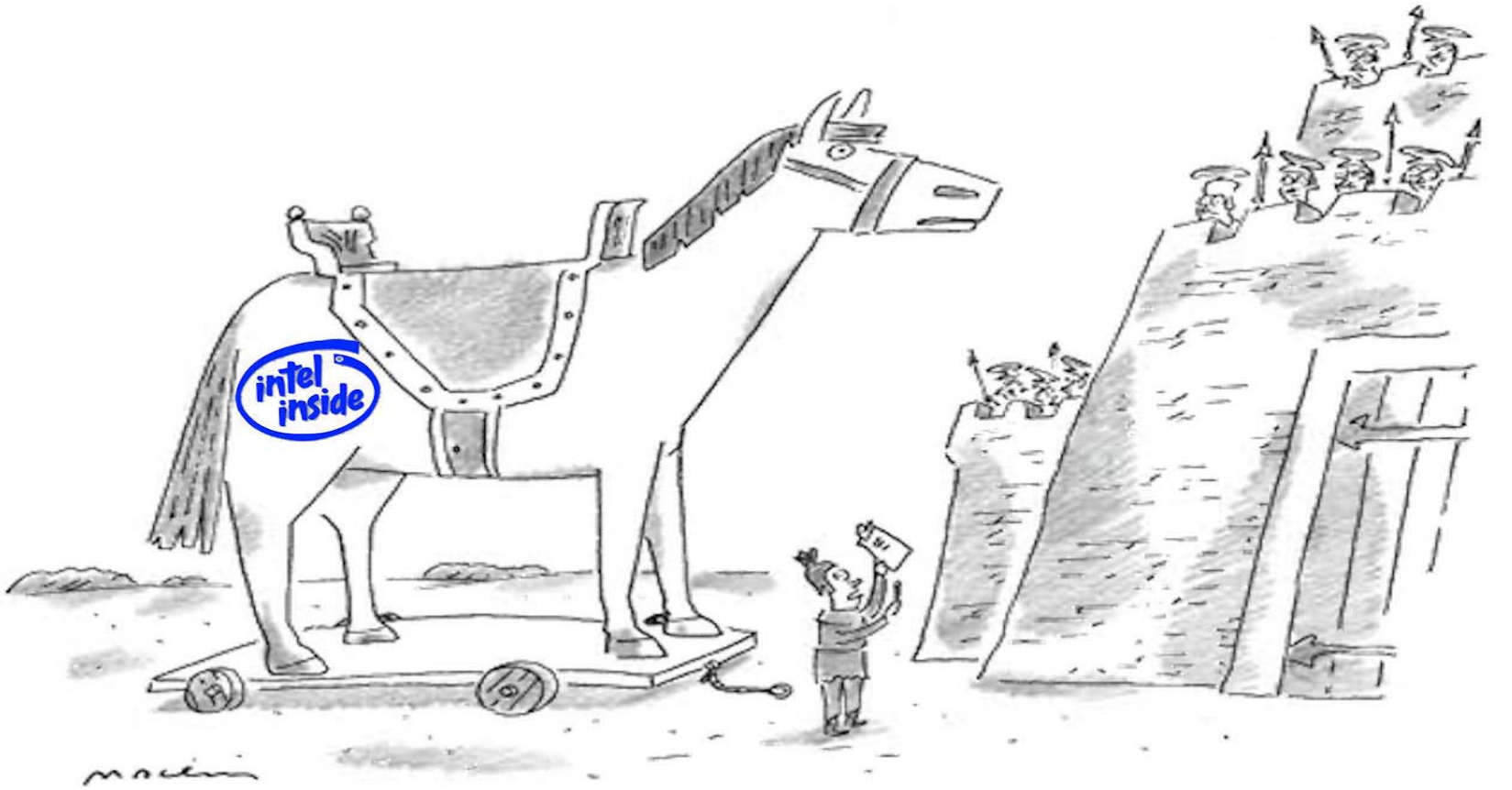
Coming Soon…
to a Popular Website Near You!

- 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…

Not Just One Target Audience…

Attackers are Fair And Balanced….

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

"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 | Hel

Internal Revenue Service
United States Department of the Treasury

Keyword/Search Terms SEARC
Advanced Search Search Tips

INDIVIDUALS | BUSINESSES | CHARITIES & NON-PROFITS | GOVERNMENT ENTITIES | TAX PROFESSIONALS | RETIREMENT PLANS COMMUNITY | TAX EXEMPT BOND COMMUNIT

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
- IRS e-file
  Fast, Easy & More Accurate.
- electronic irs
  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: XXX
Debit Card Number:
Expiry date: Month Year
CVV2:
Full Name:
City:
Zip Code:
Date of Birth: Ex: mm/dd/yy
Email:

Submit

I need to...

<Select One> GO

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 #: 5568xxxxxxxxxxx
- <A> Credit Type: MasterCard
- <A> Expires: 05/2007
- <A> CVV2: 421

The Next Attack Vector?....

$1500

$50 month

$50 month

- $499 - $799