

# Busted Myths...and Practical Tips

Steve Werby

# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips

## Risk mitigation

- Mitigate – eliminate or reduce
- Transfer – insure or outsource
- Accept
- ?

# Busted Myths...and Practical Tips

Risk mitigation – the missing link



**Denial**

This orange is in it.

# Busted Myths...and Practical Tips

## In the news

- “TJX breach could top 94 million accounts”
- “Data stolen from firm that handles student loans”
- “Data of 70 million veterans exposed”

# Busted Myths...and Practical Tips

Myth #1:

Hackers cause data breaches.



# Busted Myths...and Practical Tips

Data doesn't support this



# Busted Myths...and Practical Tips

Then what are the causes of data breaches?

- Attacks (24%)
- Glitches (36%)
- Negligence (40%)

# Busted Myths...and Practical Tips

Expensive!



# Busted Myths...and Practical Tips

## Breaches can be expensive!

- Average cost?
  - \$6.75 million per breach
  - \$204 per compromised customer record
    - Direct - \$60 (notification - \$15, post-response - \$46)
    - Indirect - \$144 (detection - \$8, lost biz - \$135)

# Busted Myths...and Practical Tips

## Cost varies by type of breach

- Attacks – \$215
- Glitches – \$166
- Negligence – \$154

# Busted Myths...and Practical Tips

## Practice makes...not quite perfect

- Glass half-empty
  - 82% of cases involved orgs with >1 1,000 record breach
- Glass half-full (sort of)
  - First timers - \$228 per record
  - Experienced organizations - \$199 per record

# Busted Myths...and Practical Tips

## Virginia's data breach notification law

- First initial + last name

and

- SSN or drivers license OR state ID

or

- Financial account info + access code

# Busted Myths...and Practical Tips

## Myth #2:

My customers are only in Virginia so I don't need to worry about other states' data breach laws.



# Busted Myths...and Practical Tips

Don't shoot the messenger



# Busted Myths...and Practical Tips

45 other states have data breach notification laws

- Most are reactive, but that's changing
- Massachusetts passed law that's **PROACTIVE**
- But, who cares...right?

# Busted Myths...and Practical Tips

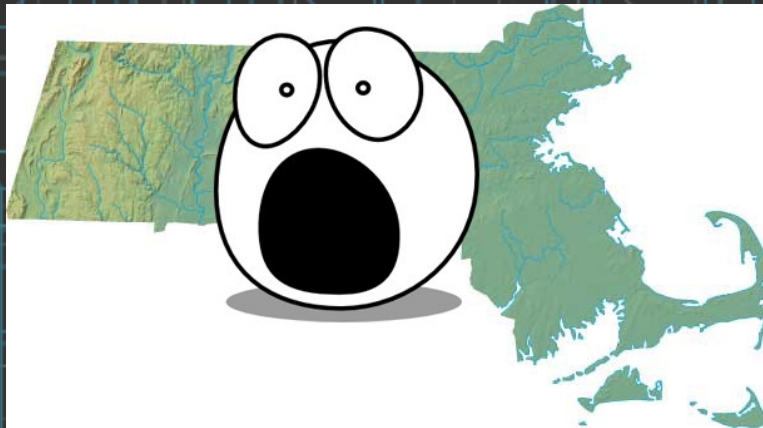
You should care...

- If you have customers who live there and have their personal information
- Must develop written information security program
  - Identify and limit risk
  - Disciplinary measures for violations
  - Restrict physical access to records
- Controls, controls...and more controls
  - Portable device encryption, transmission encryption
  - Secure authentication and access
  - Employee security awareness training

# Busted Myths...and Practical Tips

I just won't comply!

- Up to \$5,000 fine per violation
- May have to pay investigation and litigation costs
- Private civil lawsuits possible



# Busted Myths...and Practical Tips

Thank heaven for antivirus!

- AVG, BitDefender, F-Secure, Kaspersky, McAfee, Norton, Panda, Sophos, Trend Micro, etc.
- Do you...
  - Have antivirus installed?
  - Run it in real-time?
  - Have heuristic protection enabled?

# Busted Myths...and Practical Tips

## Myth #3:

My computer is protected against malware because I run antivirus software.



# Busted Myths...and Practical Tips

That would be nice!



# Busted Myths...and Practical Tips

## The dirty little secret about antivirus software

- How long is a strain used by criminals?
  - Spread for 24 hours (52%)
  - Spread for 48 hours (19%)
  - Spread for 72 hours (9%)
  - Longer (20%)
- And this is a problem because...

# Busted Myths...and Practical Tips

## The dirty little secret about antivirus software

- The lifecycle of an antivirus signature
  1. Malware author creates malware strain
  2. Malware author uses it and/or sells it
  3. Antivirus vendor receives sample...maybe...eventually
  4. Antivirus vendor develops signature...
  5. Signature made available to customers
  6. User's computer checks for new signatures
  7. Customers protected against the strain
- And this is a problem because...

# Busted Myths...and Practical Tips

## The dirty little secret about antivirus software

- Signature typically not available until 24-48 hours after antivirus vendor receives copy of strain
- Could be in use for hours or days before antivirus vendor receives a copy
- Your computer may not check for new signatures regularly
- Plenty of exceptions
  - Often takes days or weeks
  - May never receive strain or create signature

# Busted Myths...and Practical Tips

## Save me from malware!

- Why!?
  - Criminals generate malware faster than AV vendors can keep up
  - Criminals test their strains against AV products
- Heuristics is the new sheriff in town
  - Checks for malicious behavior, not signatures
  - Detects 75-90% of malware not caught via signature
- But that's not enough

# Busted Myths...and Practical Tips

## Antivirus software isn't enough

- Some malware will still slip through the cracks
- Users still can be tricked into disabling security software and installing seemingly legit software
  - Rogue antivirus software
    - 35 million new infections per month, \$34 million per month
- Other attacks involve exploiting vulnerabilities in the
  - Personal firewall
  - Patch, patch, patch

# Busted Myths...and Practical Tips

## Patch it all...and patch it fast

- Why!?
  - Criminals generate malware faster than AV vendors can keep up
  - Criminals test their strains against AV products
- Heuristics is the new sheriff in town
  - Checks for malicious behavior, not signatures
  - Detects 75-90% of malware not caught via signature
- But that's not enough (more later)

# Busted Myths...and Practical Tips

Myth #4:

My software isn't vulnerable because I run Windows Update.



# Busted Myths...and Practical Tips

Ignores the most-exploited vulnerable software



# Busted Myths...and Practical Tips

## But I run Windows Update!

- It only patches the OS and components like IE
- Is it configured to install updates automatically?
- Microsoft Update is a better alternative
  - Adds updating for Microsoft Office and other Microsoft applications
- But what about other applications?
  - Vast majority of attacks are against apps, not the OS
  - Some notify user when update available, some don't
  - 60% of 0-day vulnerabilities in non-Microsoft software

# Busted Myths...and Practical Tips

Are apps really a problem?

- 50% of users run 66+ apps from 22+ vendors
- 50% of users affected by 75+ security advisories PER YEAR!
- These advisories represent 297 vulnerabilities
- User has to deal with 22 different updating mechanisms
- 75 times per year = once every 4.8 days

# Busted Myths...and Practical Tips

## Friend and foe – Adobe Reader/Acrobat & Flash

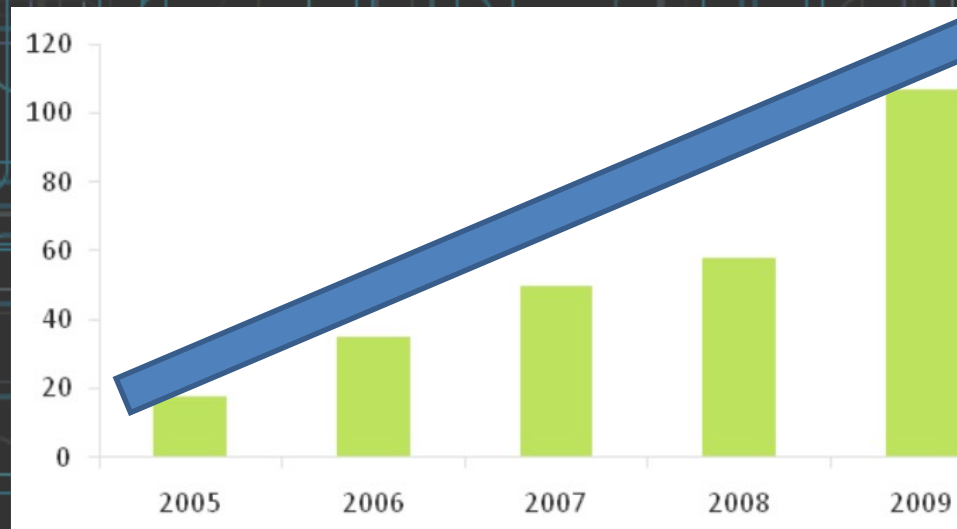
- 80% of exploits via Web target Adobe Reader
- Flash is #2, Java #3
- Office attacks - old versions, patched years prior

### Why Adobe?

- 99% penetration of Reader and Flash
- Lots of vulnerabilities
- Slow to release patches
- Some users chose not to apply patches

# Busted Myths...and Practical Tips

Documented vulnerabilities in Adobe products



# Busted Myths...and Practical Tips

## What can I do?

- Limit what users can install
  - Don't give admin access
  - Written policy, verify compliance
- Avoid software with poor vulnerability, exploit and patching records
  - Firefox instead of IE
  - Foxit Reader instead of Adobe Reader

# Busted Myths...and Practical Tips

## What else can I do?

- Implement patch management procedures
  - Run Microsoft Update, configure to install automatically
  - Define patch management requirements for IT support, preferably using centralized patch management system
  - Require users to keep their system current & provide them the tools and training to do so
    - Secunia PSI (but not for commercial use)

# Busted Myths...and Practical Tips

## What else can I do?

- Restrict admin privileges
  - Remove them
  - Create 2 user accounts and educate on use
  - Deploy software like BeyondTrust and DropMyRights which allows limited admin rights
- Removing admin privileges...
  - At least partially mitigates 64%, 100% & 100% of vulnerabilities in Windows, IE8 & Office. Older IE? 64%
  - Nearly eliminates drive-by downloads & phishing installs

# Busted Myths...and Practical Tips

There's even more!?

- Application whitelisting (solution that prevents users from installing software that hasn't been approved)
- Web filtering of malicious and infected website (blocks access to dangerous sites)

# Busted Myths...and Practical Tips

Myth #5:

I use a Mac so I don't need to worry about security!



# Busted Myths...and Practical Tips

And some say marketing doesn't work!



# Busted Myths...and Practical Tips

“Mac OS X is like living in a farmhouse in the country with no locks, and Windows is living in a house with bars on the windows in the bad part of town.”

-Charlie Miller



# Busted Myths...and Practical Tips

"Hello, I'm a Mac" campaign



# Busted Myths...and Practical Tips

## But I run a Mac!

- Not immune to attacks, **just less targeted**
  - 11% market share (7% in 2007)
- OS vulnerabilities, app vulnerabilities
  - Use Adobe Reader, Flash, Firefox, QuickTime?
  - March Mac update patched 88 vulnerabilities
- Perfect storm – rising market share, less mature security products, fewer configured controls, naïve users

# Busted Myths...and Practical Tips

Myth #6:

I'm immune to website based infections because I don't visit unsavory websites.



# Busted Myths...and Practical Tips

If only it was that easy!



# Busted Myths...and Practical Tips

## I can't trust ANYTHING on the web!?

- Avoiding porn, gambling and hackers sites is no longer enough
- 71% of malware that's distributed via the web is distributed via compromised, legit websites
  - Sites like NY Times, Yahoo
  - Vulnerabilities, user-generating content, 3<sup>rd</sup>-party content
- Attacks against social media up 70% in 2009
  - Users more trusting
  - Weaker controls
  - Skyrocketing use of shortened URLs

# Busted Myths...and Practical Tips

## Dangers of the Web

- Phishing
  - Exploit your fear, greed and lust
  - Content from people/orgs you trust
- Search engine poisoning using breaking news
  - 14% of searches for trending news/words yield malware
- Shortened URLs like tinyurl.com and bit.ly
  - <http://bit.ly/VaPCr> (LongURL - longurl.org)
- XSS, CSRF and clickjacking
- Drive-by downloads

# Busted Myths...and Practical Tips

## Myth #7:

My password is strong because it's 7 characters, includes uppercase letters and a number.



# Busted Myths...and Practical Tips

That makes it strong?



# Busted Myths...and Practical Tips

## Passwords

- Considered strong by traditional standards
  - R1chm0nd
  - P@\$word
  - Steve2010
- Hackers understand human behavior
  - Know common passwords and construction techniques – often doesn't take long to guess
  - People re-use passwords
  - People easily tricked into sharing passwords

# Busted Myths...and Practical Tips

## Large compromise is a wealth of data

- RockYou account compromise
  - Top 10 - 123456, 12345, 123456789, Password, iloveyou, princess, rockyou, 1234567, 12345678, abc123
  - Sport – soccer (29), color – purple (33), entertainer – eminem (75), religious figure – jesus (103), drink – cocacola (471), contains special characters – iloveyou! (984), first letter capitalized – Password (1856)
  - 32 million accounts, 11 million unique passwords
  - Top 2,000 passwords used by whopping 5 million users

# Busted Myths...and Practical Tips

## Passwords

- Password re-use
  - Same password for all websites (33%)
  - A few different passwords (48%)
  - Different passwords for all websites (19%)
- More password re-use
  - Same password for 1 financial site & 1+ non-financial?

# Busted Myths...and Practical Tips

## Passwords

- So your employee's Facebook account password could be guessed and give attacker access to your business systems
- Forgotten password functionality is convenient...
  - But challenge questions easier to guess than passwords
  - Typically send temporary password to email account so getting access to employee's email account gives keys to the kingdom

# Busted Myths...and Practical Tips

Long + unique = WIN, WIN, WIN

- Memorization techniques
  - Passphrase – RatherBeFishingOrDrinkingBeer
  - Modified Passphrase – Oscysbtdelwspwhattlg
- Or forget memorization
  - Write them down, but do so securely
    - Don't leave it laying around
    - Don't spell out site, username and password
    - Or use KeePass
- Encourage users to use unique passwords

# Busted Myths...and Practical Tips

OK, who cares? Why does this all matter?

# Busted Myths...and Practical Tips

What can happen to my business?

- Competitors can steal your data
- Hackers can encrypt and ransom your data
- Hackers can bring your network/systems down
- Hackers can use your resources
- Your systems can be used to send spam
- Your systems can be used to attack other systems
- Your systems can be used host child porn
- But perhaps **WORST OF ALL**

# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips

## Myth #8:

If I have a unique password, run antivirus & keep my system patched, my bank deposits are safe.



# Busted Myths...and Practical Tips

I wish it did. I wish it did.



# Busted Myths...and Practical Tips

## Online banking fraud is big business

- FBI investigated 200 cases in 2008 and 2009, involving \$100 million in fraudulent wire transfer charges, with \$40 million unrecovered
- More than 200,000 variants of banking trojans in 2009
- Often test “micropayment” wire transfers of under \$1 to verify success
- Of 23 million computers scanned by PandaLabs in 2009Q3, 48% infected
  - Of those infected, 16% with banking trojans / password stealers

# Busted Myths...and Practical Tips

## How it works

- Primarily run by large, cybercrime syndicates
- Funnel \$ out via wire transfer and ACH transfer
- Often laundered by money mules
- Can be victimized even if take **ALL PREVIOUSLY ADVISED PRECAUTIONS**
- Steal your passwords and token codes
- Redirect you to fake bank web pages
- Rewrite bank web pages to hide transactions

# Busted Myths...and Practical Tips

## Patco Construction Company (Maine)

- 2 passwords compromised
- Lost \$588k to dozens of co-conspirators over week - \$345k unrecovered
- Consumers generally have 60 days from receipt of bill to dispute; usually reversed
- **Businesses usually have to report immediately; no guarantee transfers will be reversed or halted**
- Lawsuit that didn't do enough to prevent theft

# Busted Myths...and Practical Tips

## Experi-Metal (Michigan) and Comerica Bank

- Lost \$560k
- Bank routinely emailed customers link to update bank's digital certificate
- Password and security token stolen
- 47 wire transfers over 4 hours
  - 38 more after they notified bank
  - 2 wire transfers over 2 prior years



# Busted Myths...and Practical Tips

## Little & King LLC (New York) and TD Bank

- Lost \$164k
- Was about to be acquired, now facing bankruptcy
- Infected by ZeuS trojan, which steals passwords and allows attacker to control computer
- \$15k wire transfer to Georgia woman who was hired after phone interview for a work-at-home job as financial agent for Adams Interiors, a NY interior design firm with a stellar BBB reputation
- Money mules often end up losing too

# Busted Myths...and Practical Tips

I want to protect my bank balance

1. Don't bank online (probably not feasible)
2. Defense in depth (layered security approach described previously) and accept the risk
3. Only access the account from a live boot OS distribution (OS that boots from a DVD or flash drive, bypassing your hard drive's OS)
4. Defense in depth + dedicated computer used **ONLY** for accessing the bank website

# Busted Myths...and Practical Tips

What should I ask my bank?

1. What is my liability if my account is compromised?
2. Are there controls you can put in place for my account to reduce my risk (transfer limits, alerts, out-of-band verification, etc.)?
3. What do you do to detect fraudulent activity?

# Busted Myths...and Practical Tips

Myth #9:

Information security is hard.



# Busted Myths...and Practical Tips

Myth #10:

Information security is easy.



# Busted Myths...and Practical Tips

Information security is somewhere in between.

Don't forget – perfect is the enemy of good.

# Busted Myths...and Practical Tips



## Denial

This orange is in it.

# Busted Myths...and Practical Tips



# Busted Myths...and Practical Tips

## Stay informed

- OnGuard Online ([www.onguardonline.gov/](http://www.onguardonline.gov/))
- Twitter ([twitter.com/vcuinfosec](https://twitter.com/vcuinfosec))
- Information Security Best Practices ([bit.ly/VaPCr](http://bit.ly/VaPCr))
- Graham Cluley's Blog ([www.sophos.com/blogs/gc](http://www.sophos.com/blogs/gc))
- Krebs on Security ([krebsonsecurity.com](http://krebsonsecurity.com))
- Secunia.com Advisories ([secunia.com/advisories/historic/](http://secunia.com/advisories/historic/))
- KeePass Password Safe ([keepass.info](http://keepass.info))
- Ubuntu LiveCD ([help.ubuntu.com/community/LiveCD](http://help.ubuntu.com/community/LiveCD))
- Justifiable Paranoia Blog ([justifiableparanoia.com](http://justifiableparanoia.com))

# Busted Myths...and Practical Tips

That's all folks

