Attack Progressions

First they came for bandwidth…
Now they want to make a difference

Steve Riley
Technical Director, CTO Office
steve.riley@riverbed.com

Menu

- Who are the bad guys?
- Why is software insecure?
- How bad are the threats?
- How expensive are attacks?
- What’s going on?
- What’s particularly troubling?
- Is there a pattern that can help us?
- What should we be doing?

Prelude

Short history of "hacking"

Services

Operating System Services
- Buffer overruns, XSS
- Web spoofs, worms

Application Services
- SQL injection, SQL Slammer
- Media players

Networks

Eavesdropping
- DES, AES, IPSec

Network Protocols
- Syn flood, DNS spoofing

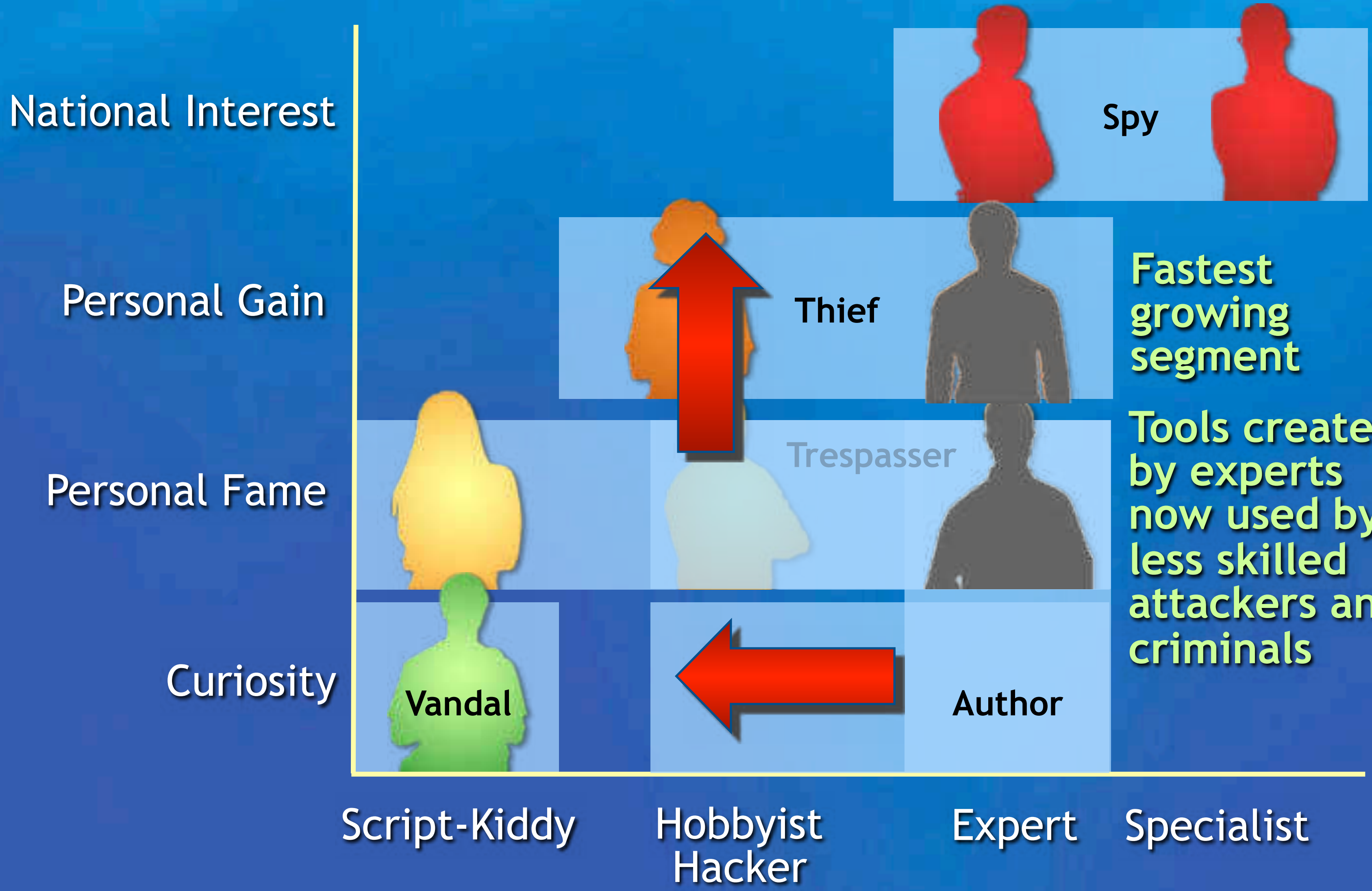
Network Stacks
- "Ping of death"

Mainframes

Emanations
- Tempest

Insiders
- TCSEC, Common Criteria

Understanding the landscape



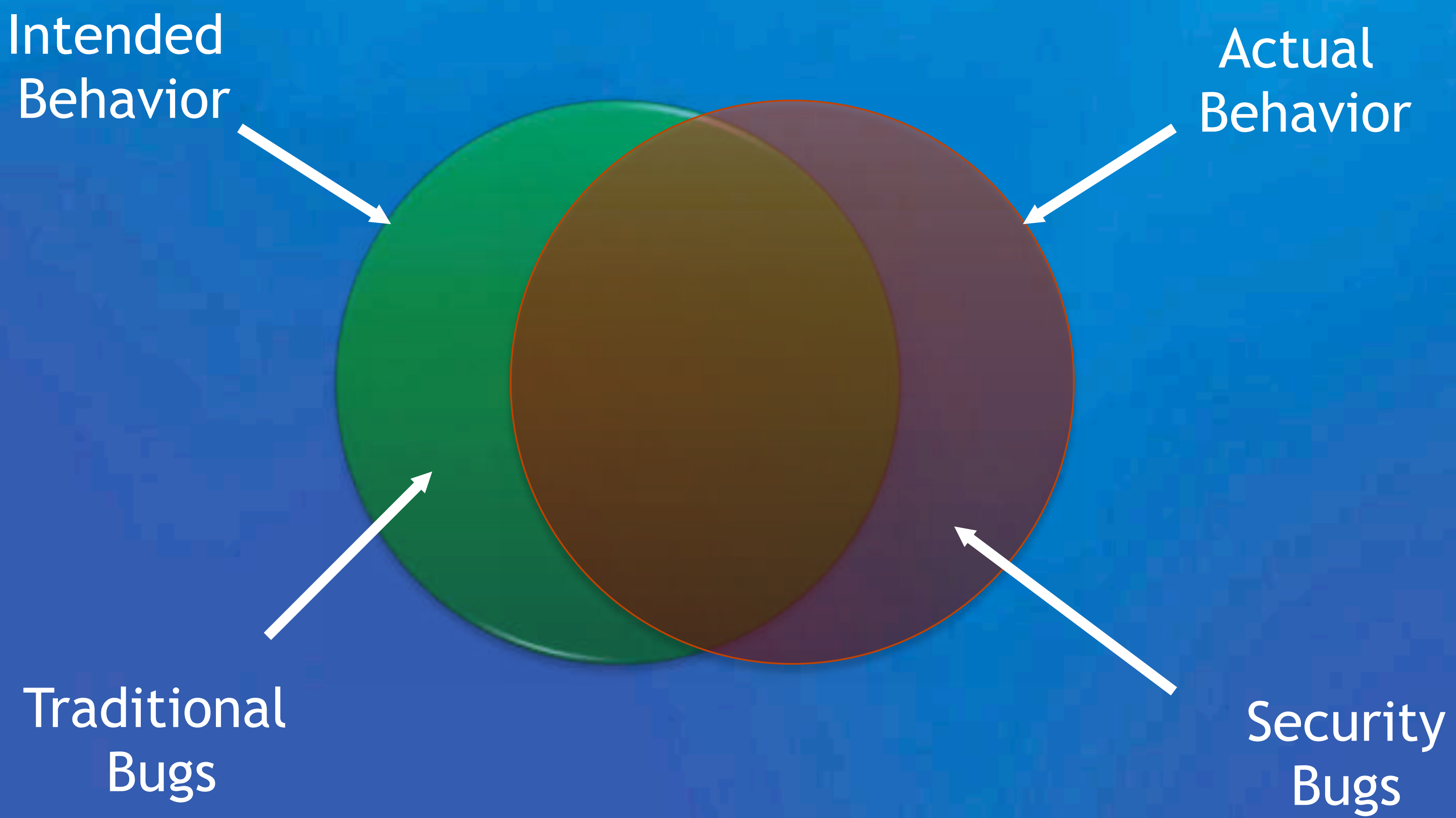
Fastest growing segment

Tools created by experts now used by less skilled attackers and criminals

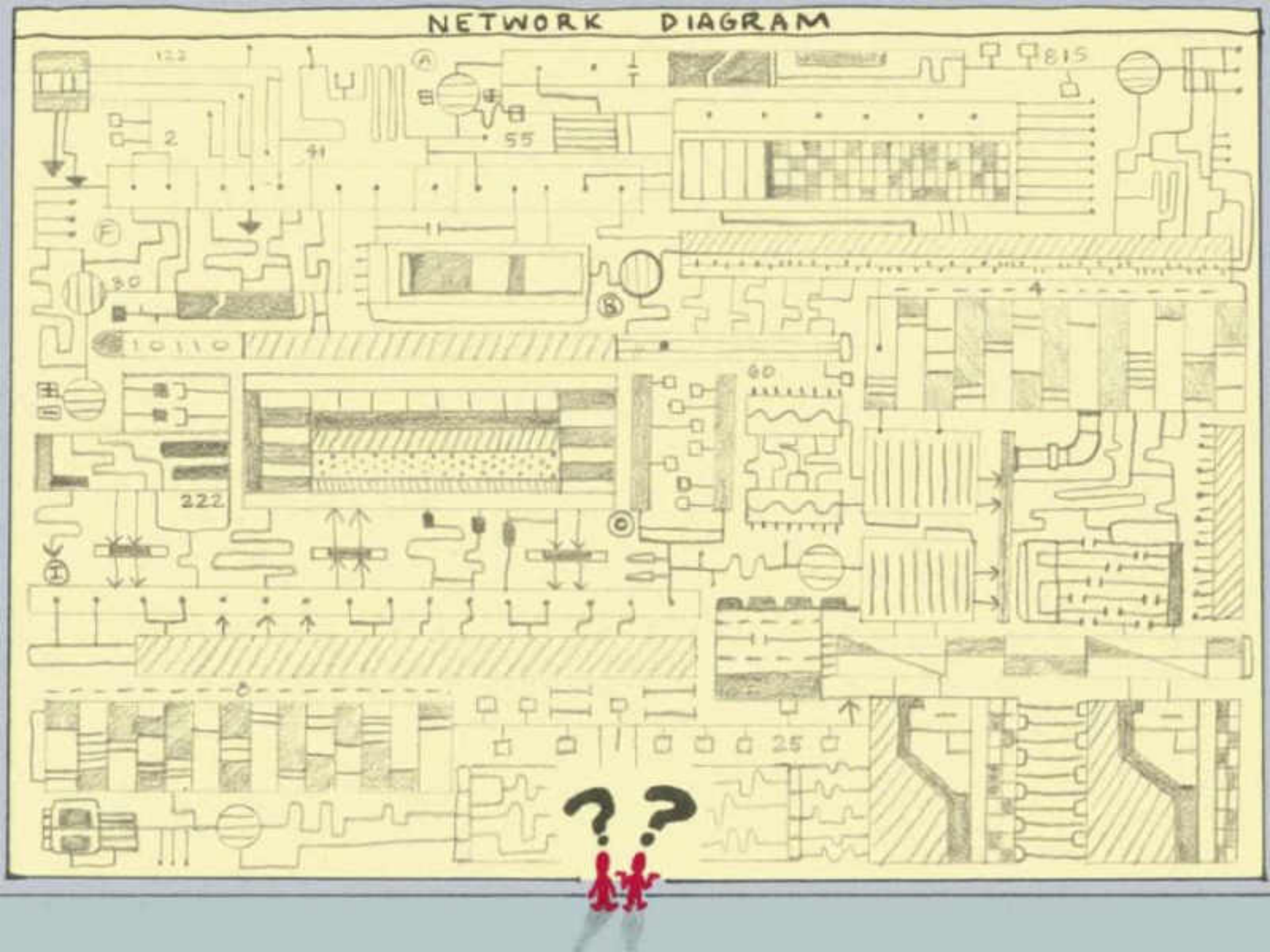
Fix all	Vulnerabilities	*Find one*
Protect all	Victims	*Attack one*
Rare	Automation	*Common*
A lot	Work to do	*Not much*
Limited	Time to do it	*Infinite*

The fundamental problem

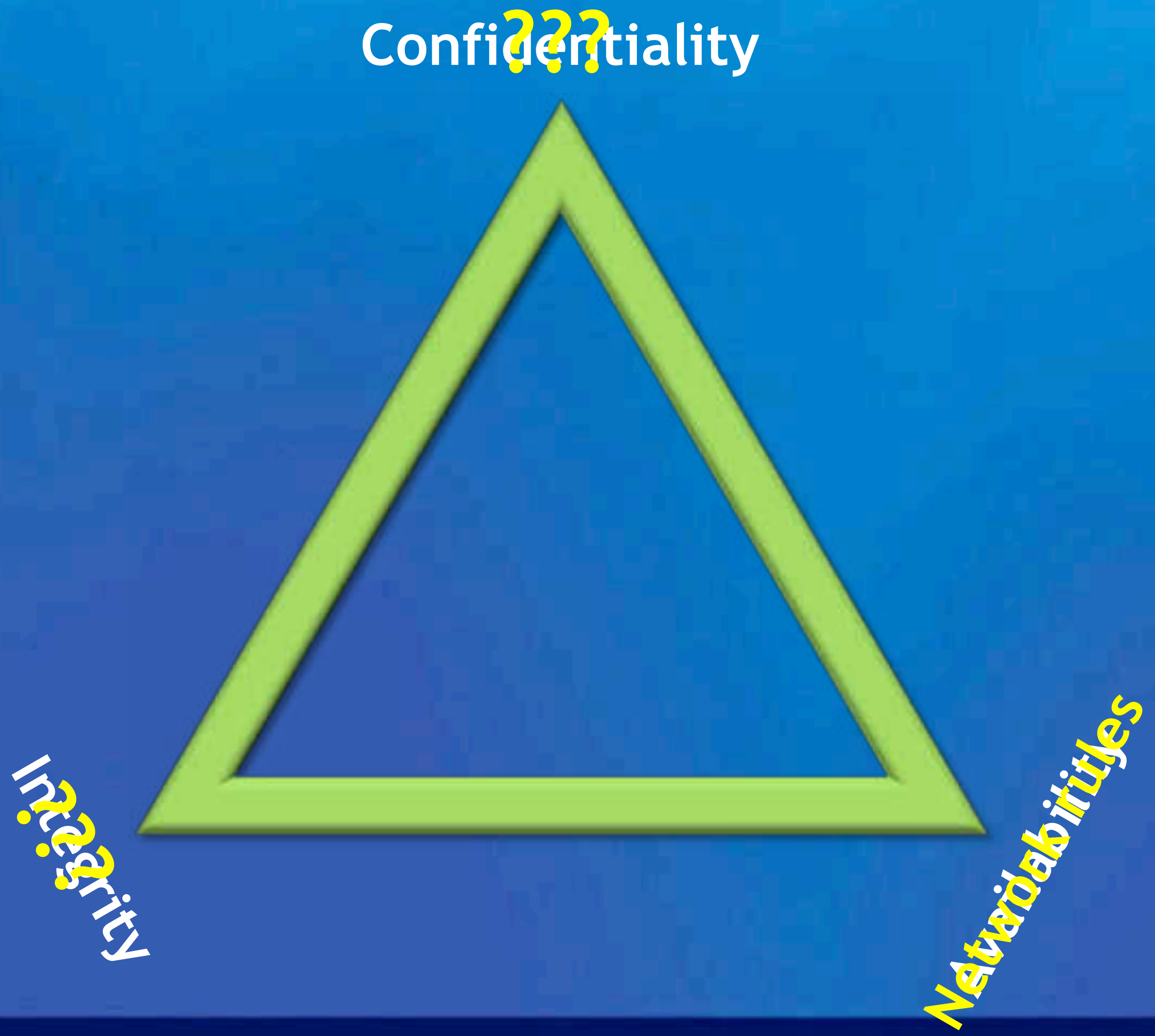
(examples later)



Traditional methods are no longer effective

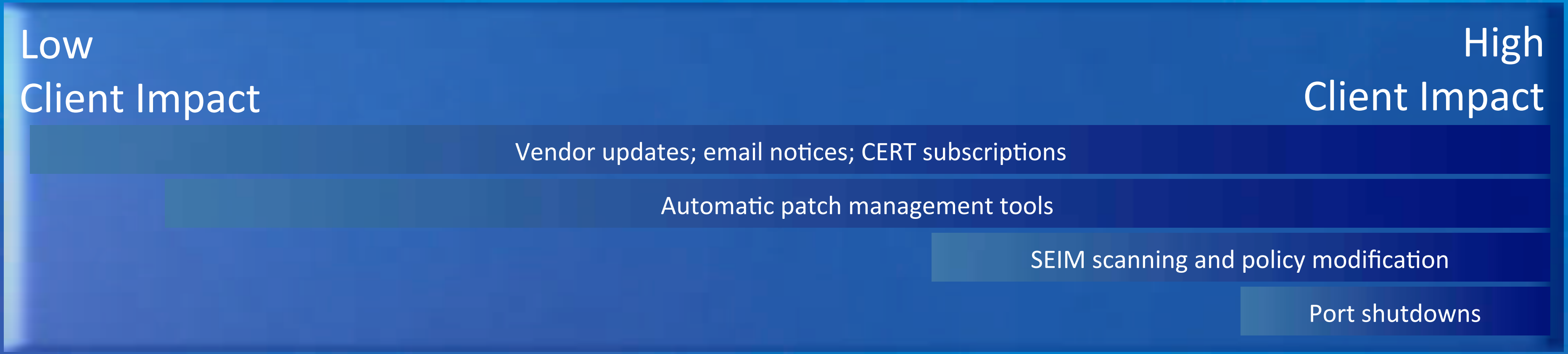

NETWORK DIAGRAM
122
A
815
2
41
55
F
90
B
10110
4
60
222
C
I
D
8
25
? ?

Attack progressions



The future isn’t what it used to be…

You don’t have time



Low
Client Impact

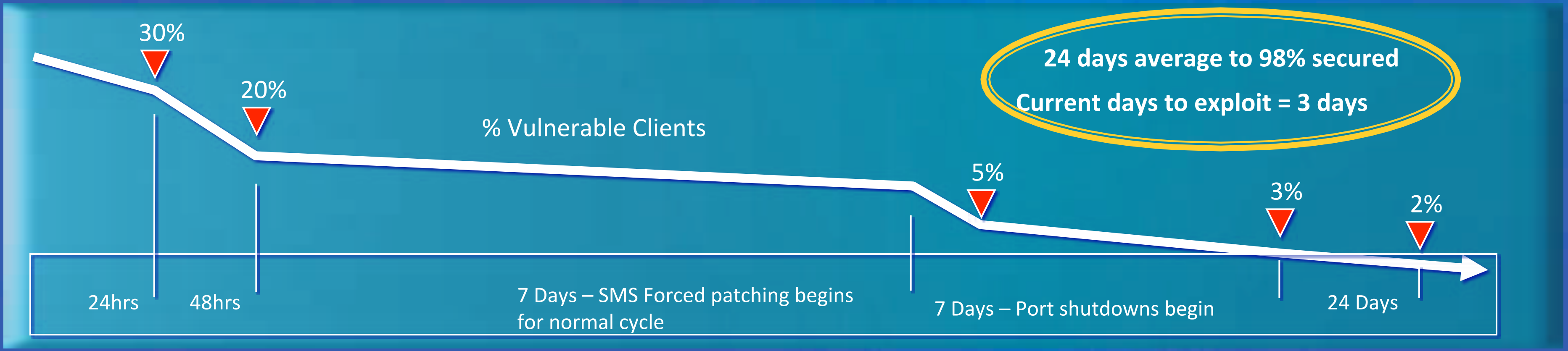
High
Client Impact

Vendor updates; email notices; CERT subscriptions

Automatic patch management tools

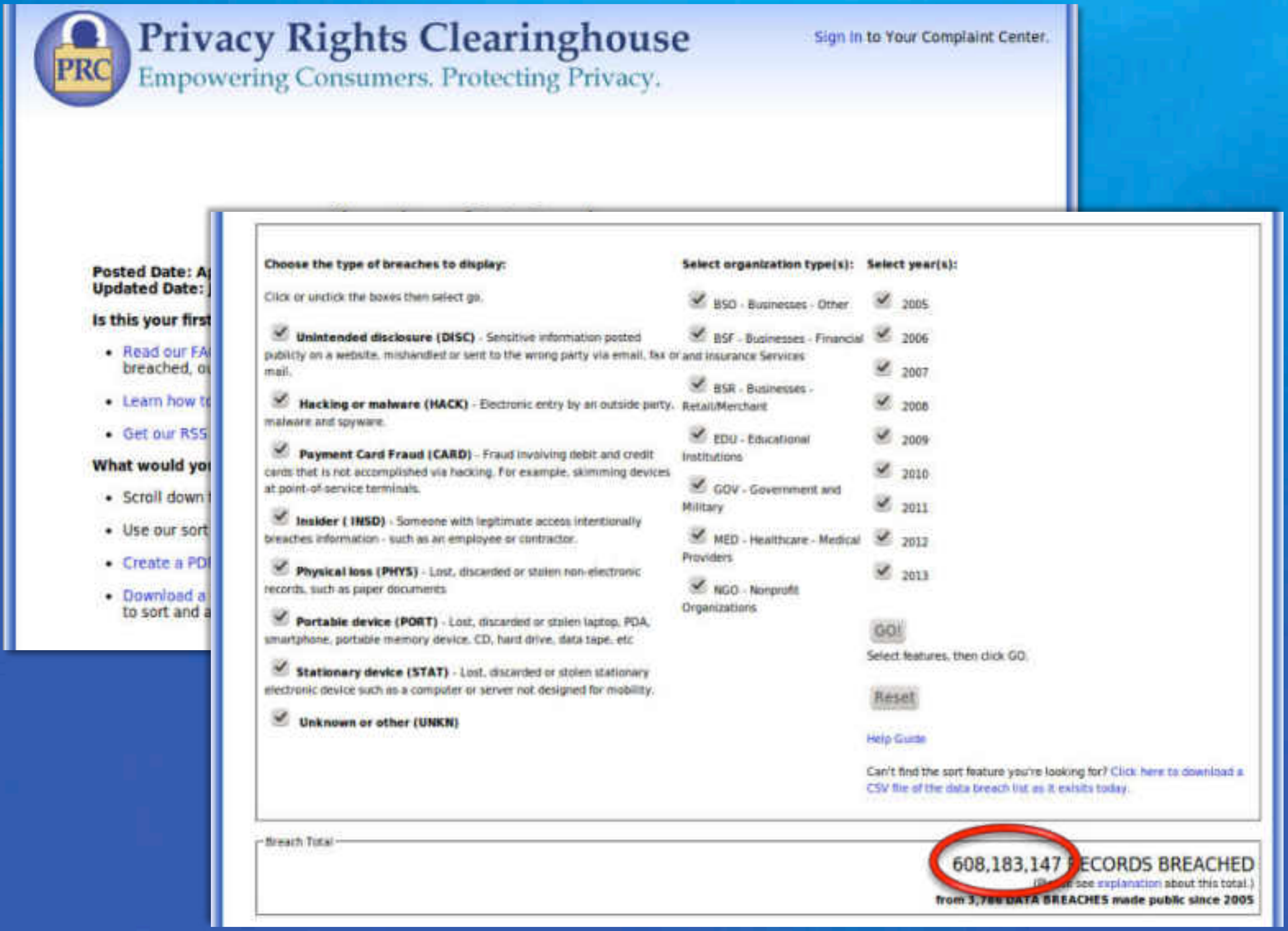
SEIM scanning and policy modification

Port shutdowns



24 days average to 98% secured

Current days to exploit = 3 days



Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

Sign In to Your Complaint Center.

Posted Date: A
Updated Date:

Is this your first

- Read our FA breached, o
- Learn how t
- Get our RSS

What would yo

- Scroll down
- Use our sort
- Create a PD
- Download a to sort and a

Choose the type of breaches to display:

Click or unclick the boxes then select go.

☑ **Unintended disclosure (DISC)** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.

☑ **Hacking or malware (HACK)** - Electronic entry by an outside party, malware and spyware.

☑ **Payment Card Fraud (CARD)** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.

☑ **Insider (INSD)** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.

☑ **Physical loss (PHYS)** - Lost, discarded or stolen non-electronic records, such as paper documents

☑ **Portable device (PORT)** - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc

☑ **Stationary device (STAT)** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.

☑ **Unknown or other (UNKN)**

Select organization type(s):

☑ BSO - Businesses - Other

☑ BSF - Businesses - Financial and Insurance Services

☑ BSR - Businesses - Retail/Merchant

☑ EDU - Educational Institutions

☑ GOV - Government and Military

☑ MED - Healthcare - Medical Providers

☑ NGO - Nonprofit Organizations

Select year(s):

☑ 2005

☑ 2006

☑ 2007

☑ 2008

☑ 2009

☑ 2010

☑ 2011

☑ 2012

☑ 2013

Select features, then click GO.

Help Guide

Can't find the sort feature you're looking for? Click here to download a CSV file of the data breach list as it exists today.

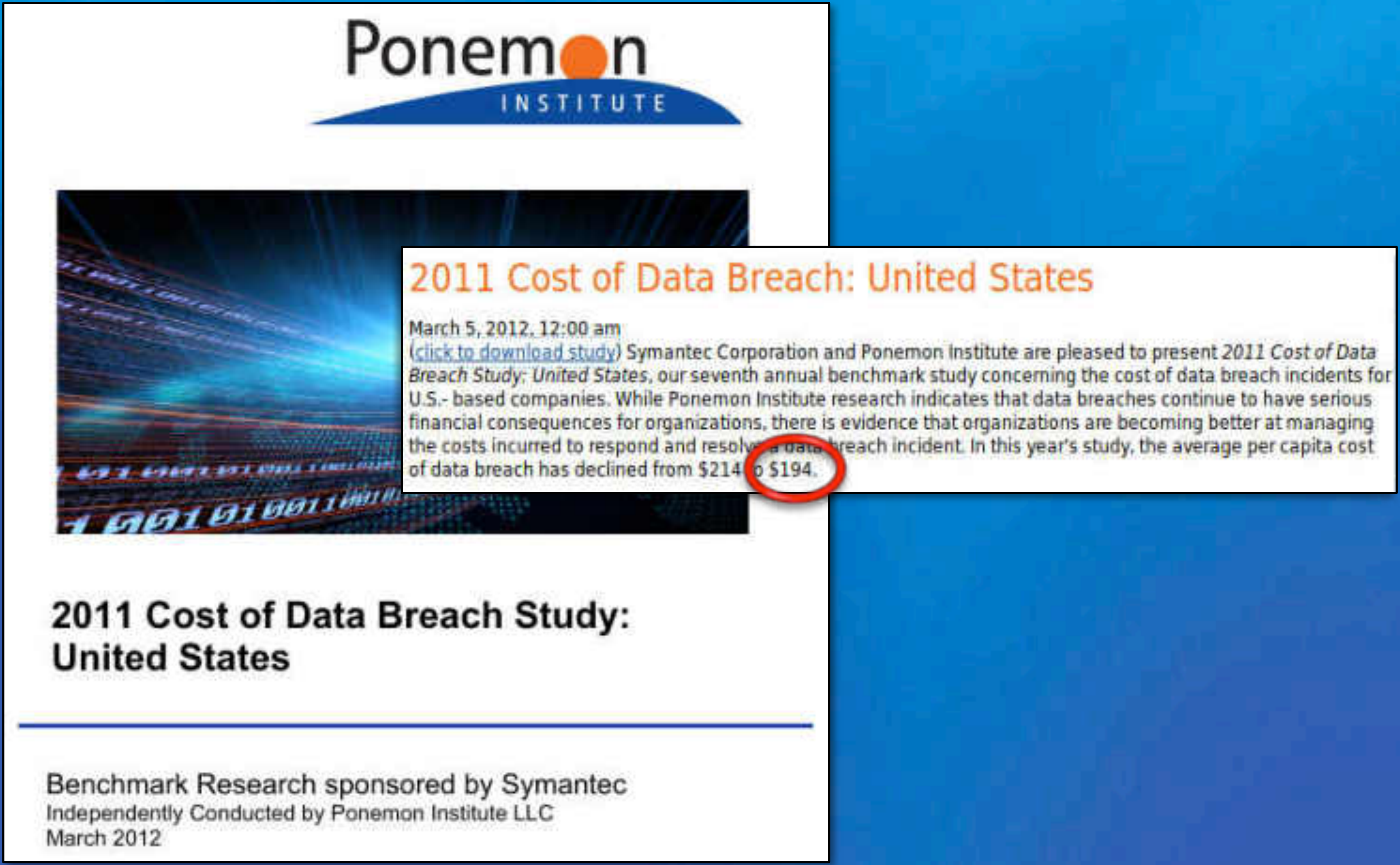
Breach Total

608,183,147 RECORDS BREACHED

(Please see explanation about this total.)

from 3,766 DATA BREACHES made public since 2005

http://www.privacyrights.org/data-breach/



Ponemon INSTITUTE

2011 Cost of Data Breach: United States

March 5, 2012, 12:00 am

(click to download study) Symantec Corporation and Ponemon Institute are pleased to present *2011 Cost of Data Breach Study: United States*, our seventh annual benchmark study concerning the cost of data breach incidents for U.S.- based companies. While Ponemon Institute research indicates that data breaches continue to have serious financial consequences for organizations, there is evidence that organizations are becoming better at managing the costs incurred to respond and resolve a data breach incident. In this year's study, the average per capita cost of data breach has declined from $214 to $194.

2011 Cost of Data Breach Study: United States

Benchmark Research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
March 2012

http://www.ponemon.org/library/2011-cost-of-data-breach-united-states

$$\begin{array}{lr} & 608{,}183{,}147 \\ \times & \$194.00 \\ \hline \multicolumn{2}{r}{\$117{,}987{,}530{,}518} \end{array}$$

$$\begin{array}{lr} & 608{,}183{,}147 \\ \times & \$194.00 \\ \hline \multicolumn{2}{r}{\$117{,}987{,}530{,}518} \end{array}$$

Can’t we do better?

1,179,875,305 barrels of oil

(at $100/bbl.)

9,111,006 four-year degrees

($12,950 for one year tuition at Univ WA, 2013)

190,641 HIVer lives saved

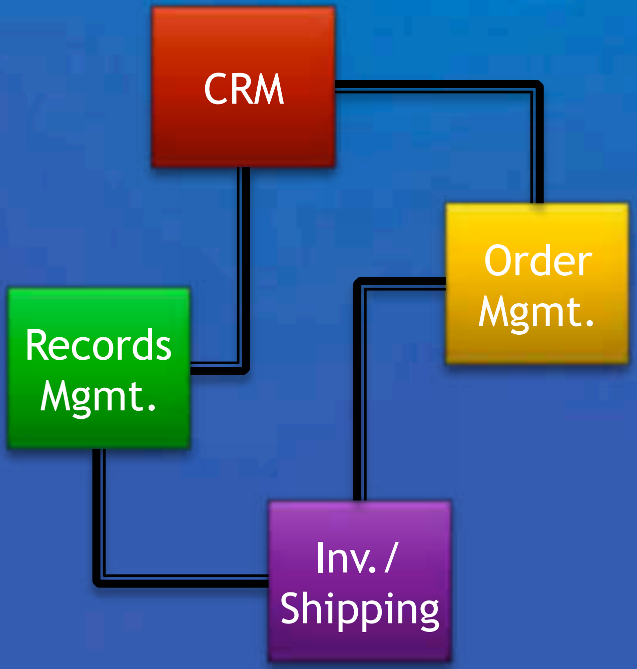
($618,900 lifetime, Nov. 2006 Medical Care)

9,493,686 families/yr fed

($239/wk for 2 adults and 2 children, USDA 2013)

Caught with pants down, again

We fiddle with



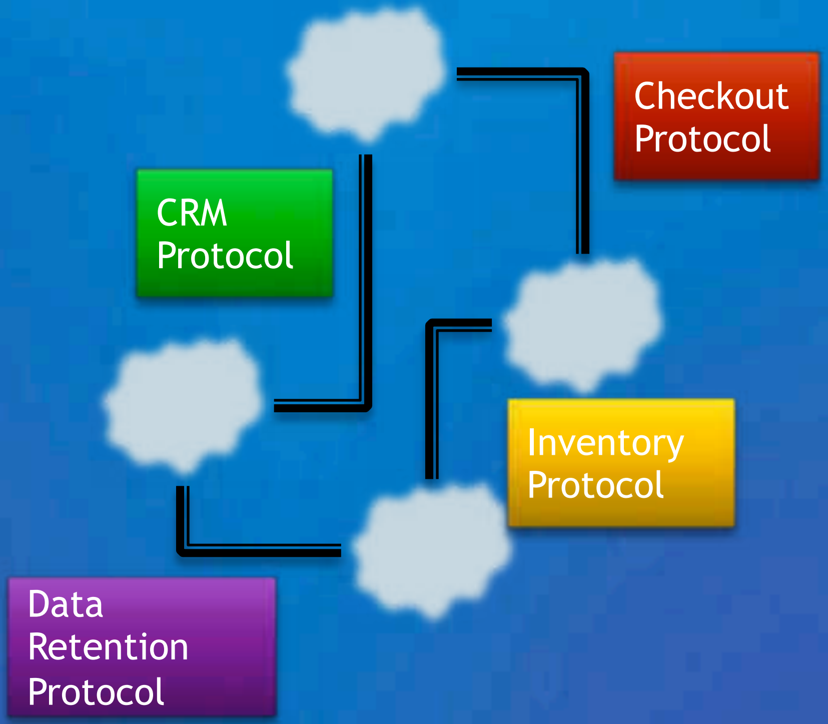
CRM

Records Mgmt.

Order Mgmt.

Inv. / Shipping

Bad guys target



Checkout Protocol

CRM Protocol

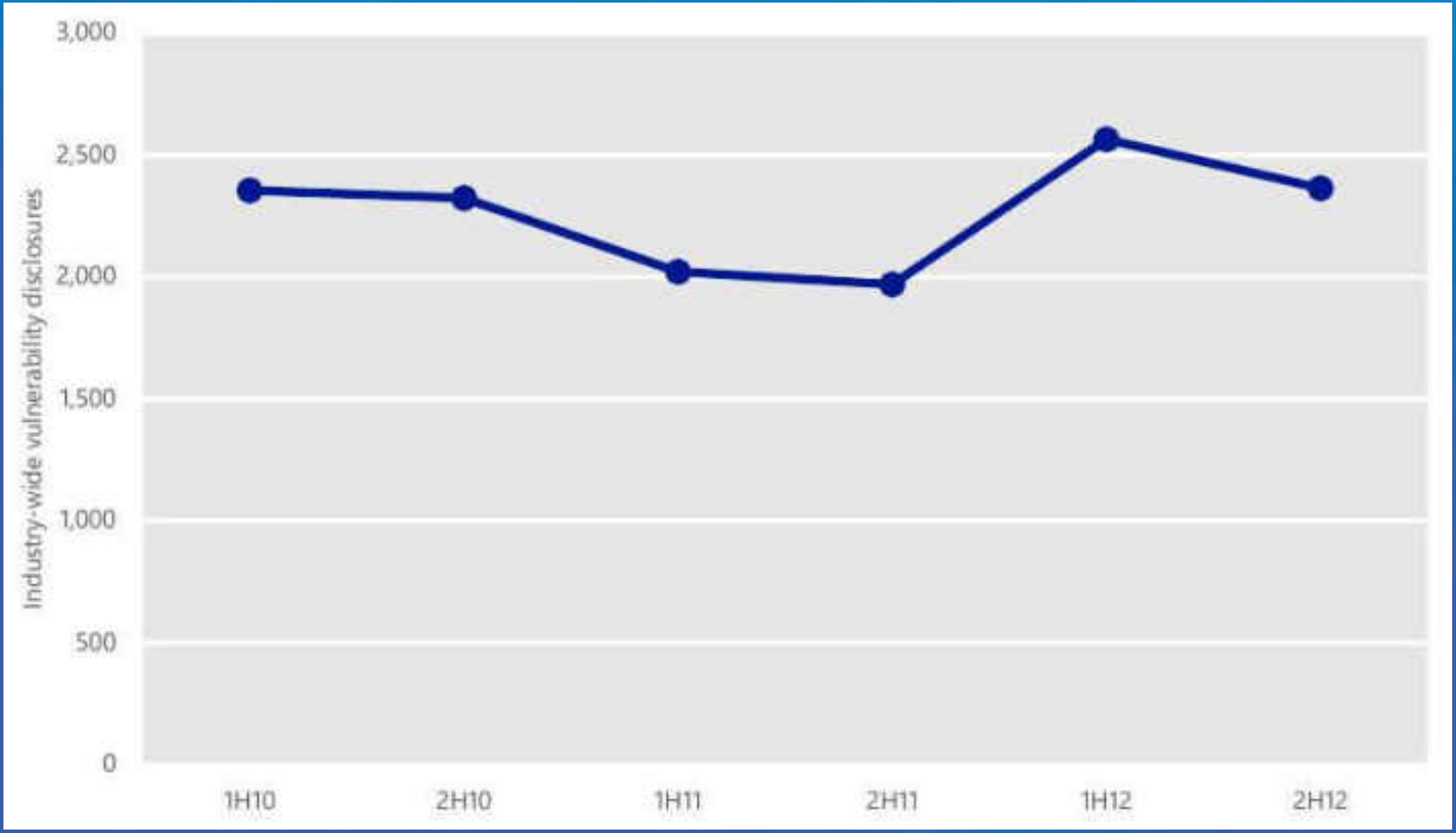
Inventory Protocol

Data Retention Protocol

Some data

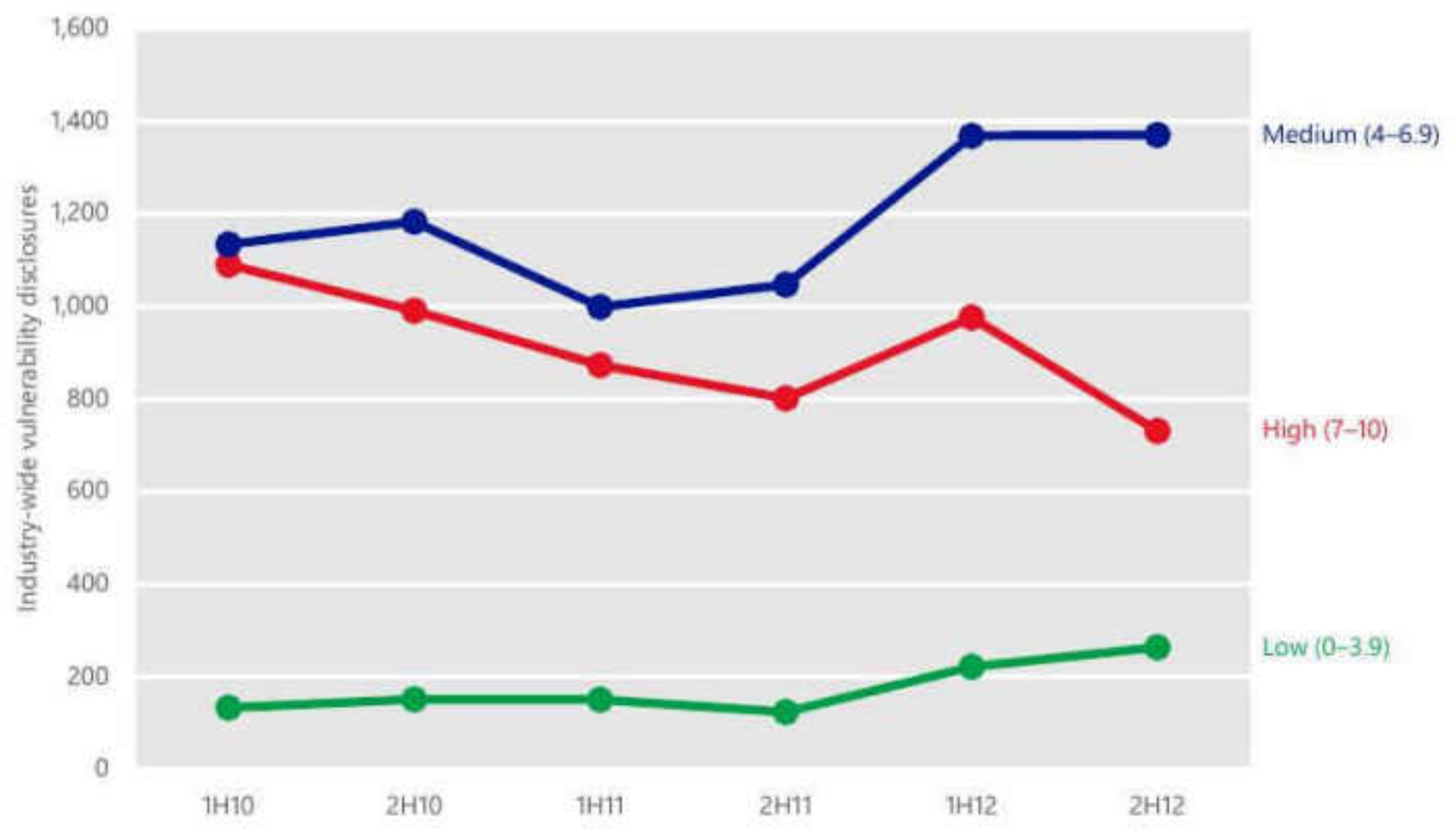
Industry-wide vuln disclosures

- Cf. 2009, avg 3,500 per H



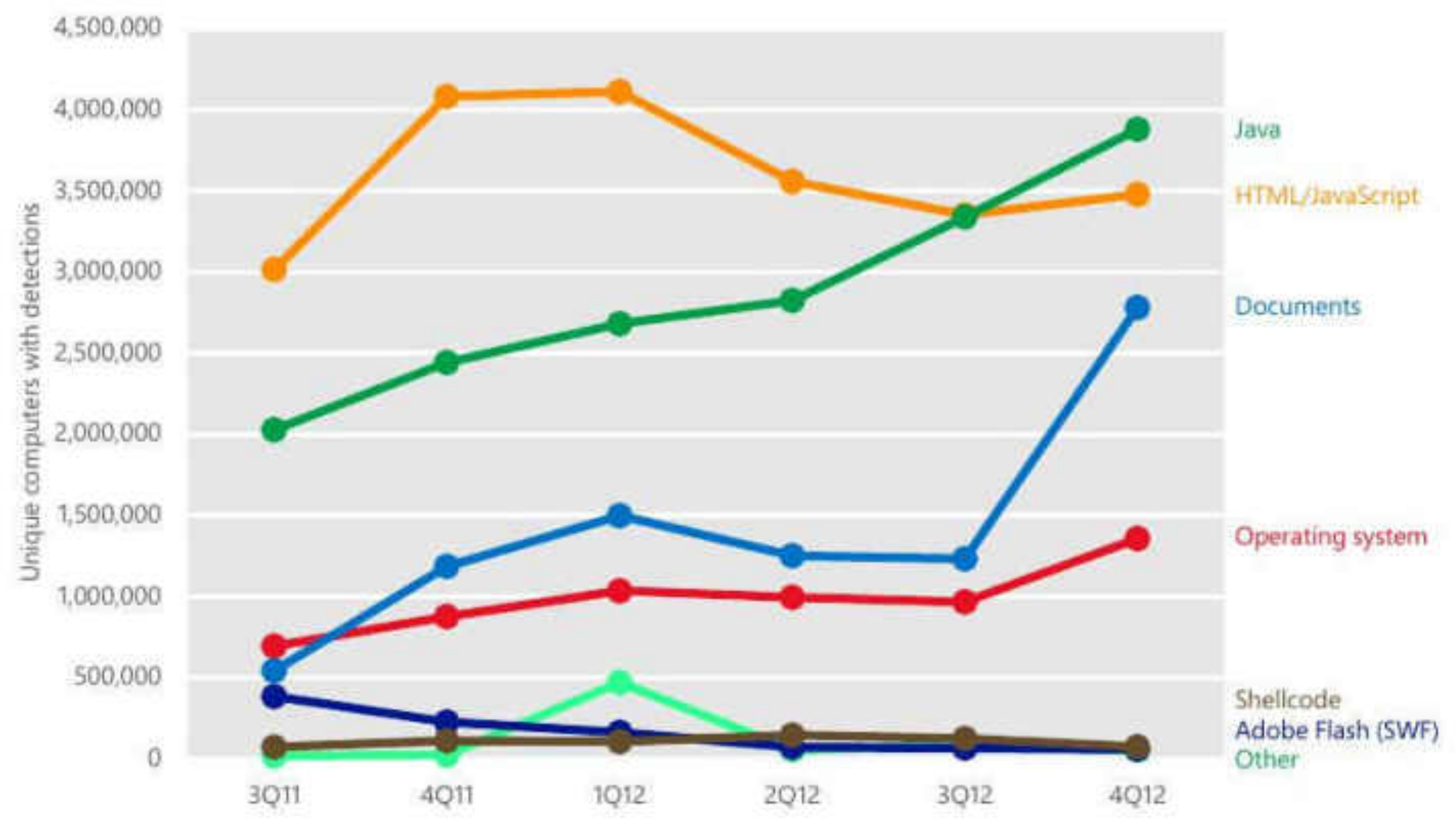
Vulnerability severity

- Based on CVSS scores



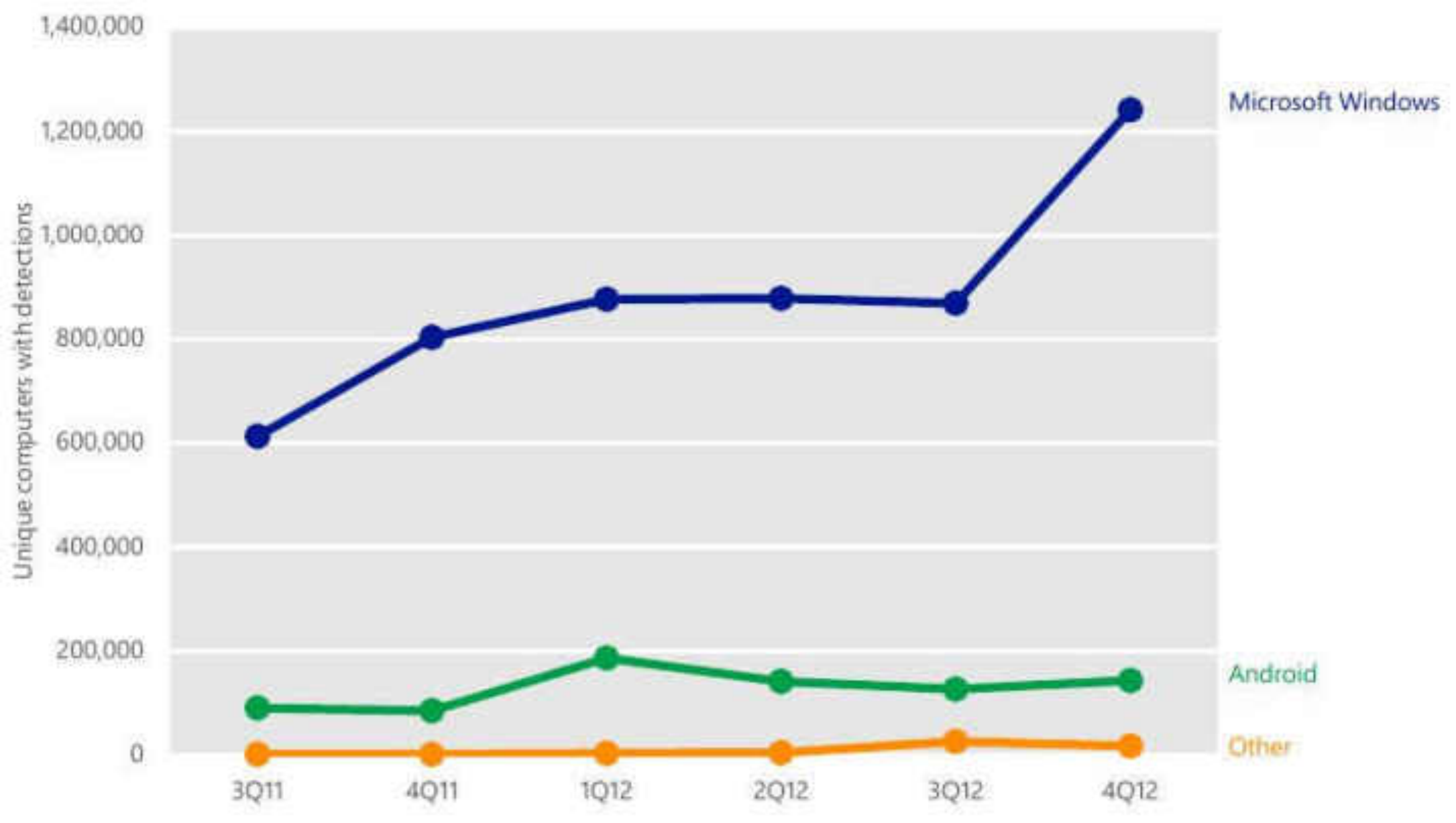
Exploit types

- No auto-update = very, very bad



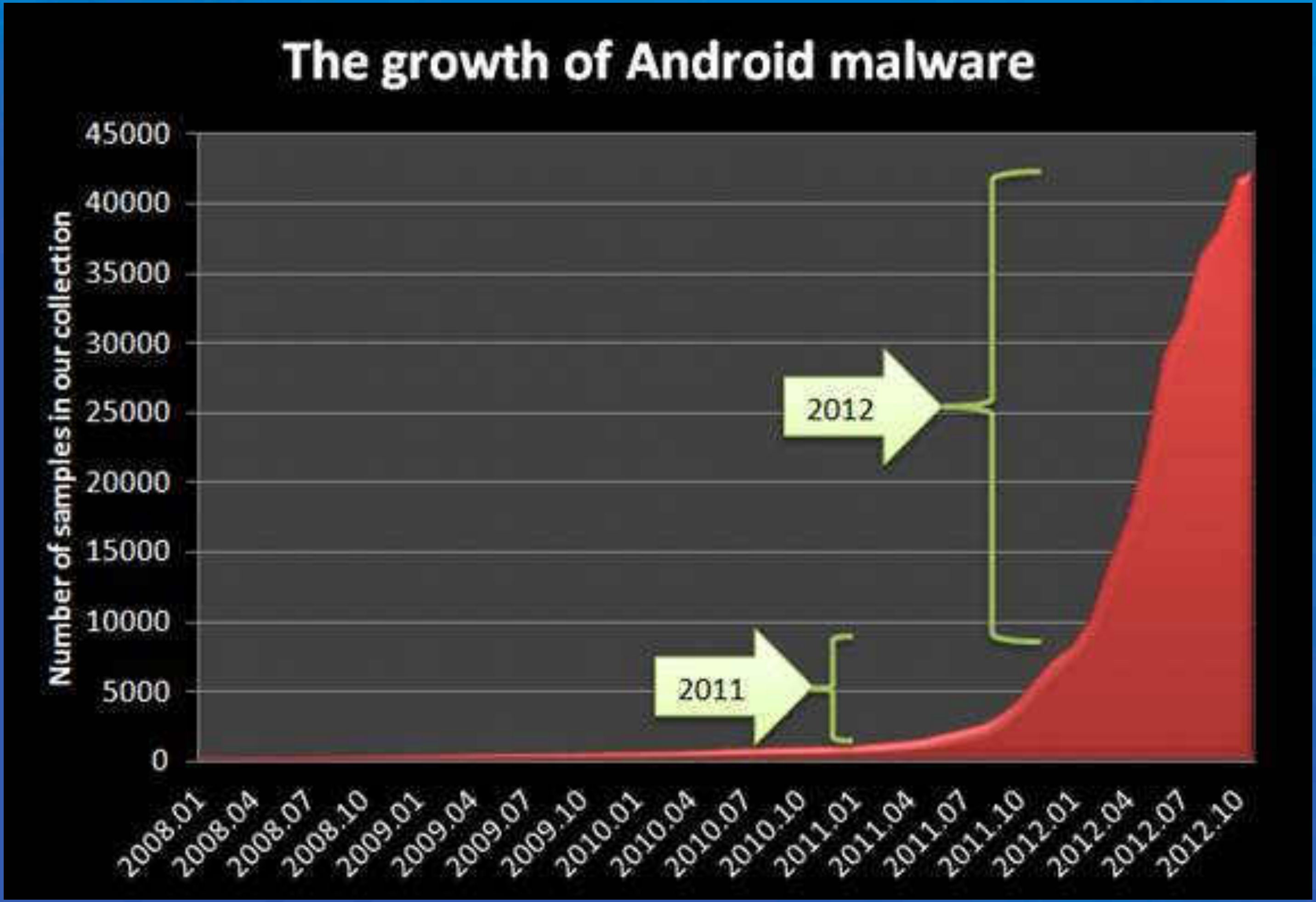
Windows vs. Android

- Won't always be this way

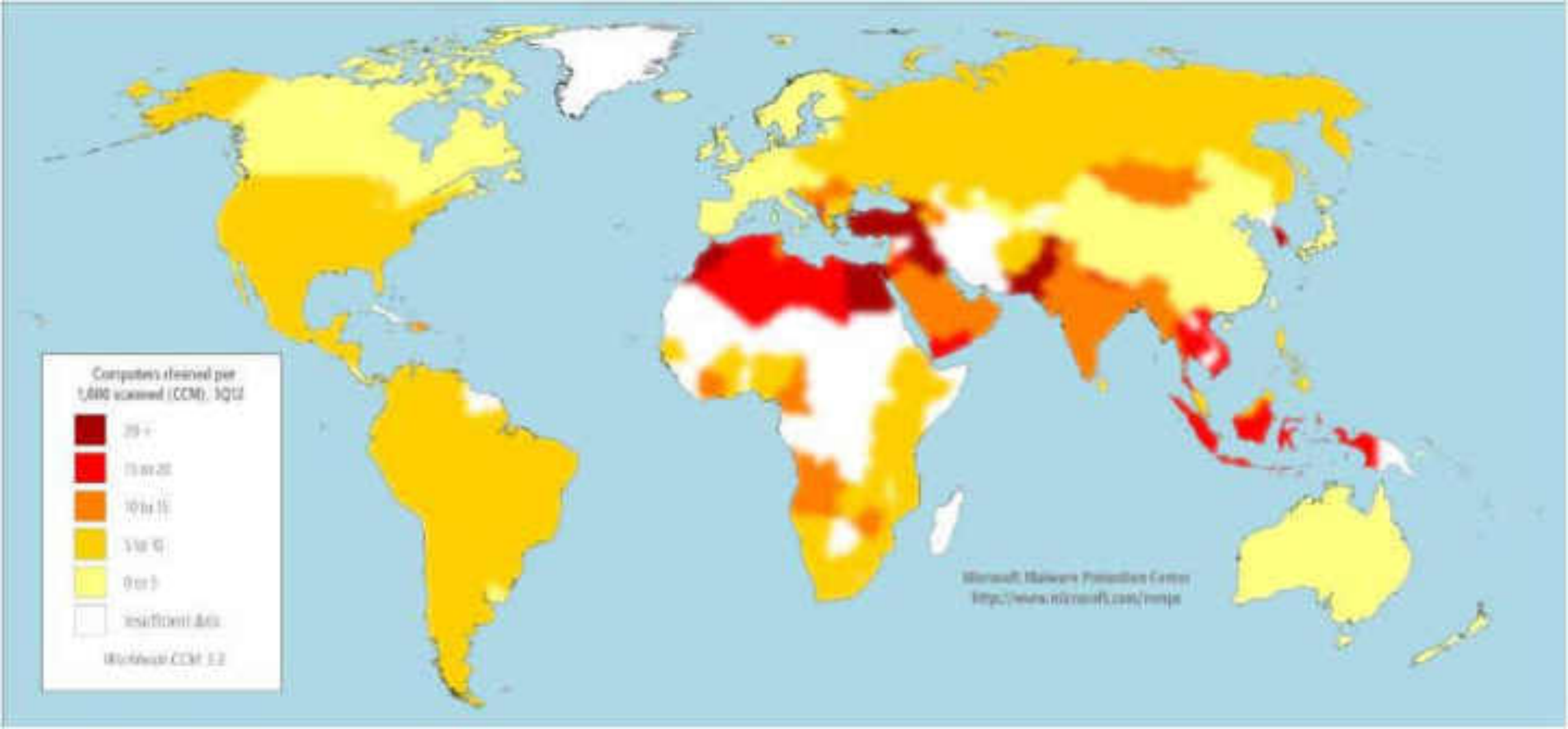


Android malware growth

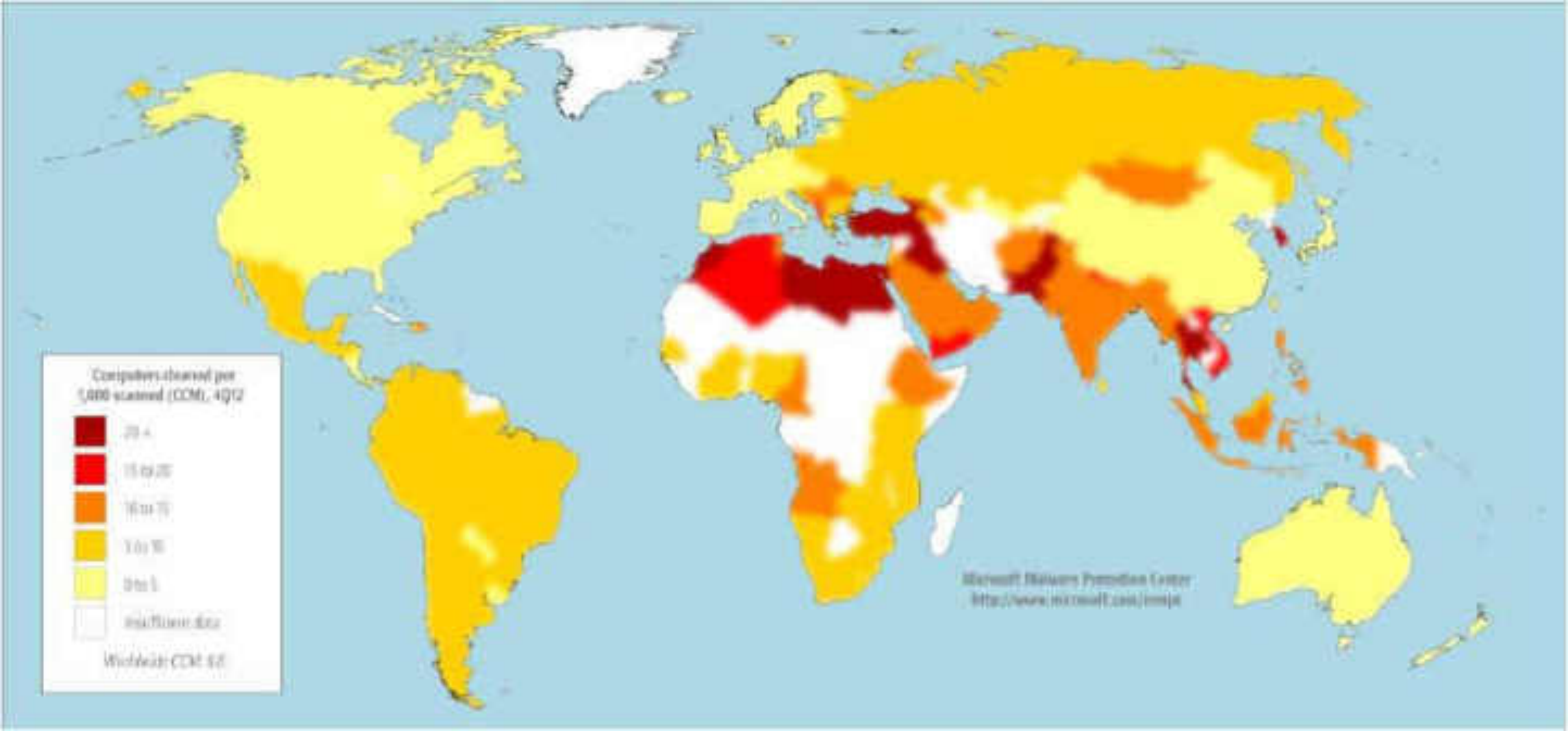
- Kaspersky predicts even more



Infection by country, 3Q12

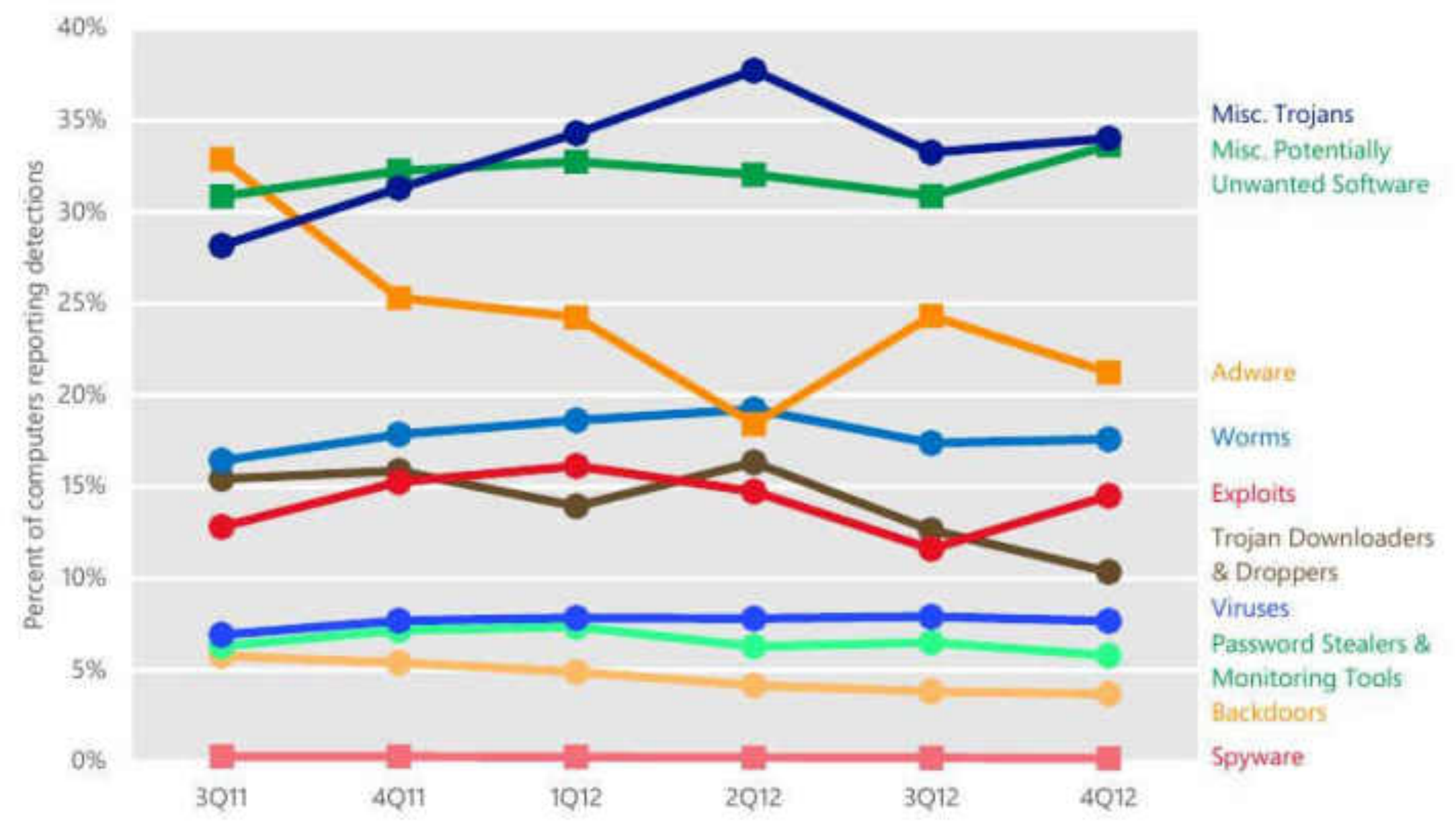

Computers cleaned per 1,000 scanned (CCM), 3Q12
20 +
15 to 20
10 to 15
5 to 10
0 to 5
Insufficient data
Worldwide CCM: [illegible]
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Infection by country, 4Q12

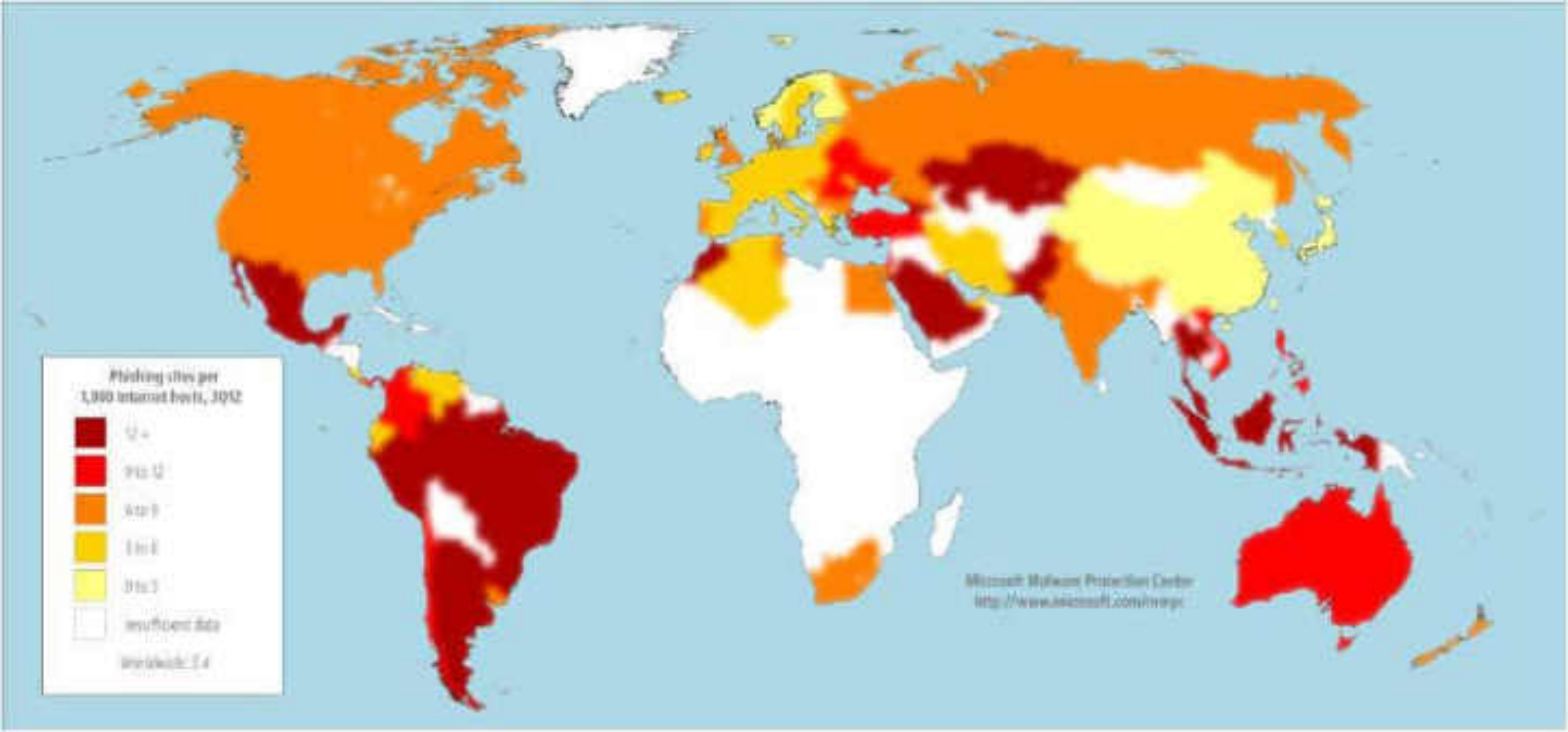

Computers cleaned per
1,000 scanned (CCM), 4Q12
20 +
15 to 20
10 to 15
5 to 10
0 to 5
Insufficient data
Worldwide CCM: 6.0
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Threat categories

- Autorun—shut it off, please
- Whatever happened to spyware?

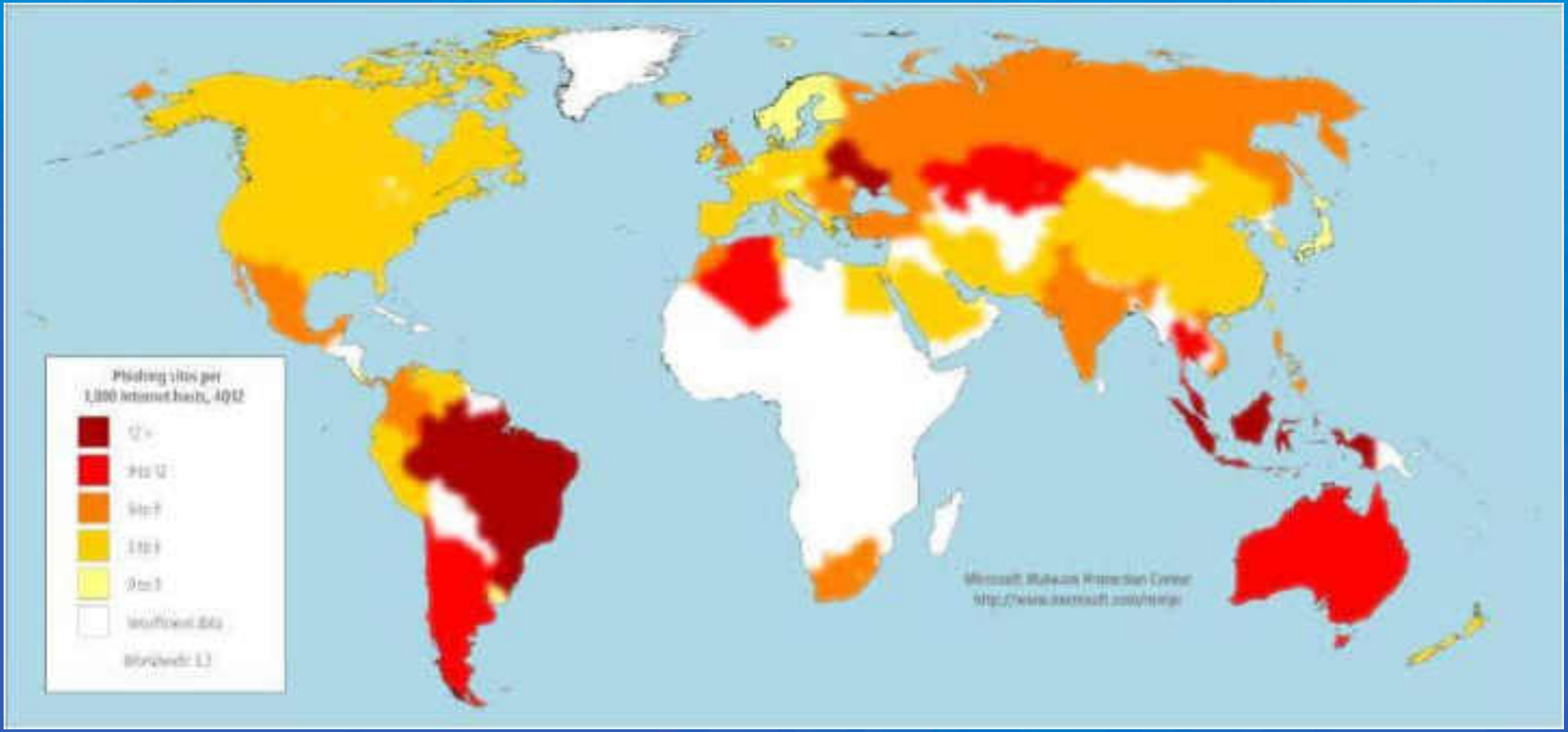


Phishing sites, 3Q12



Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

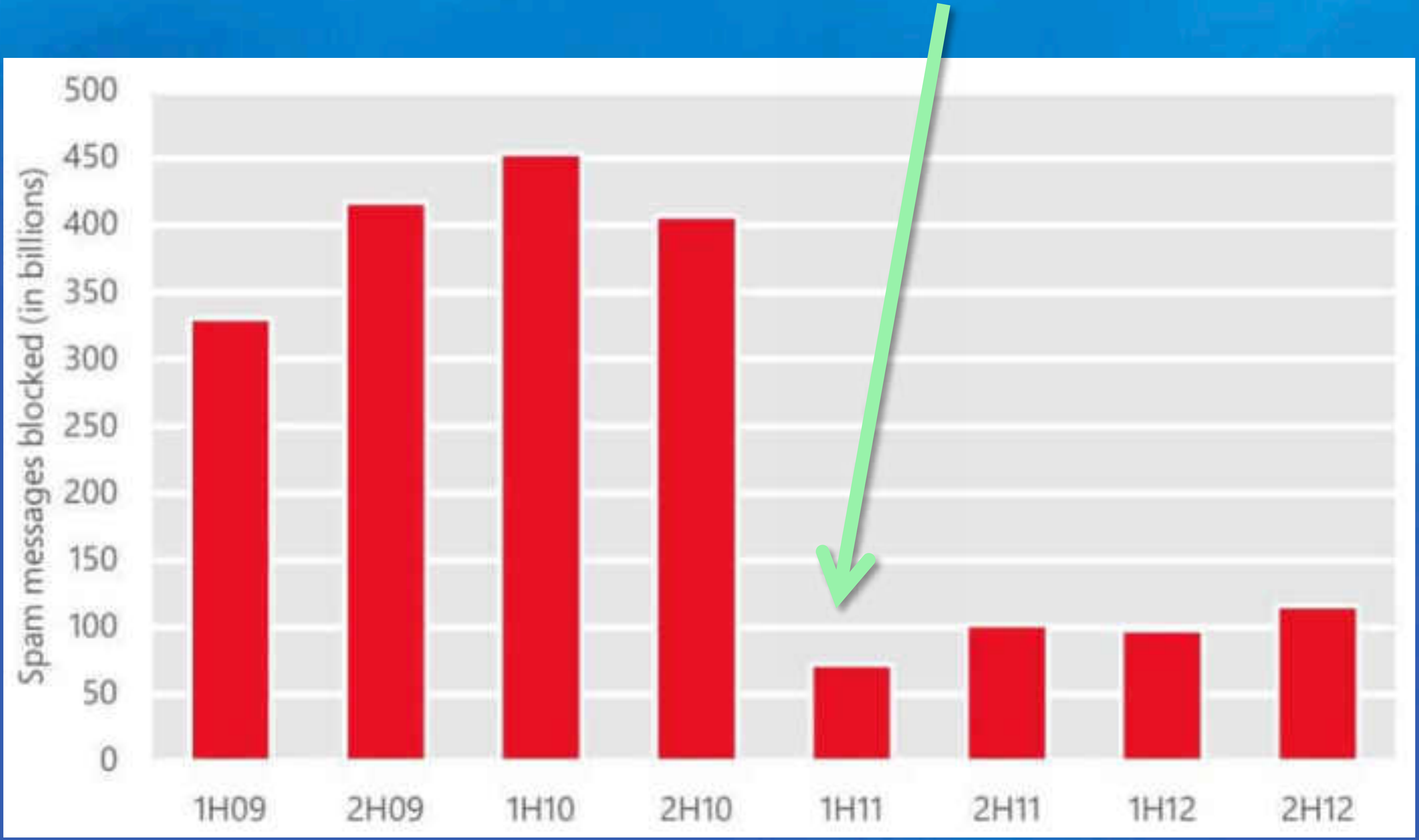
Phishing sites, 4Q12



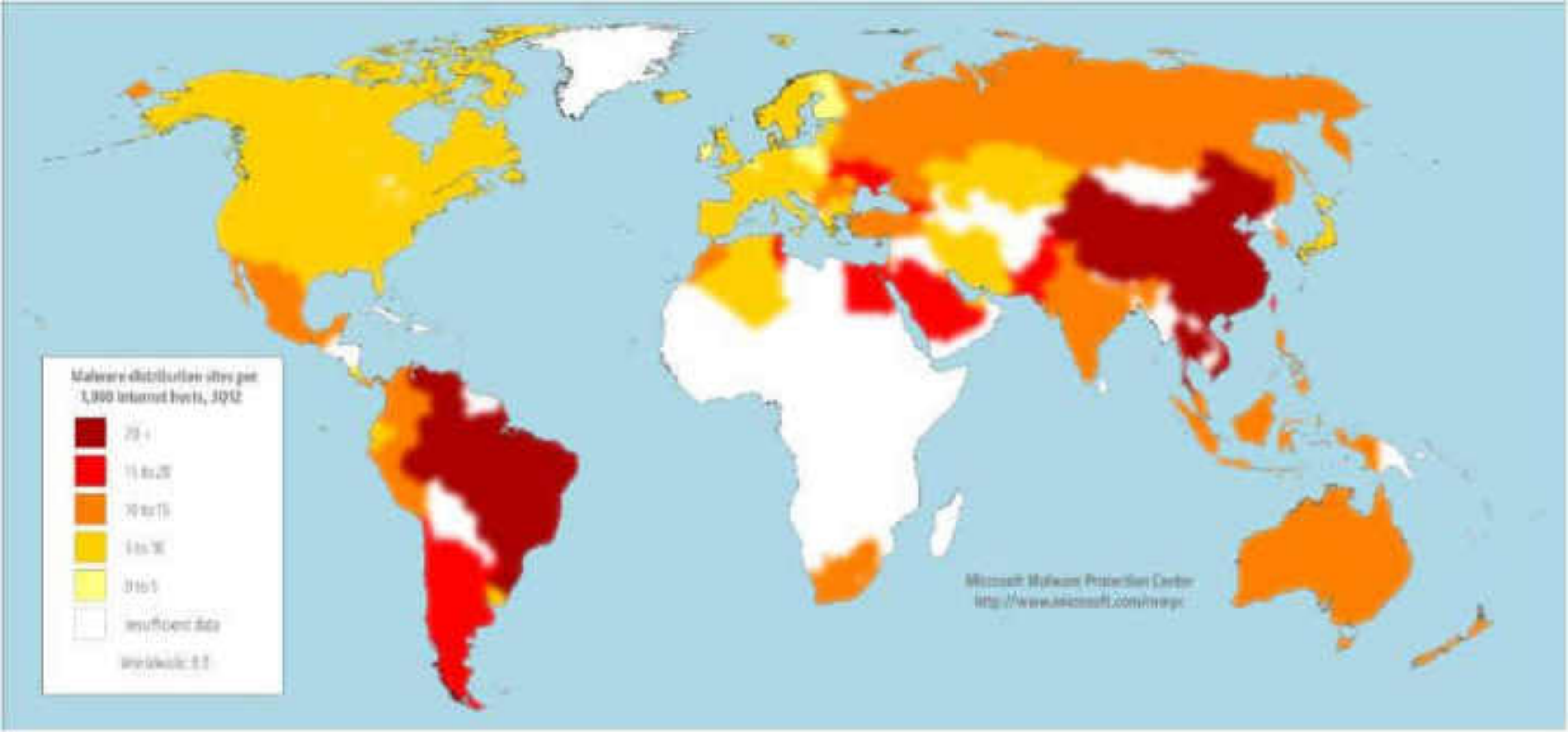
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Spam blocked, 1H09-2H12

- Cutwail and Rustock botnets taken down

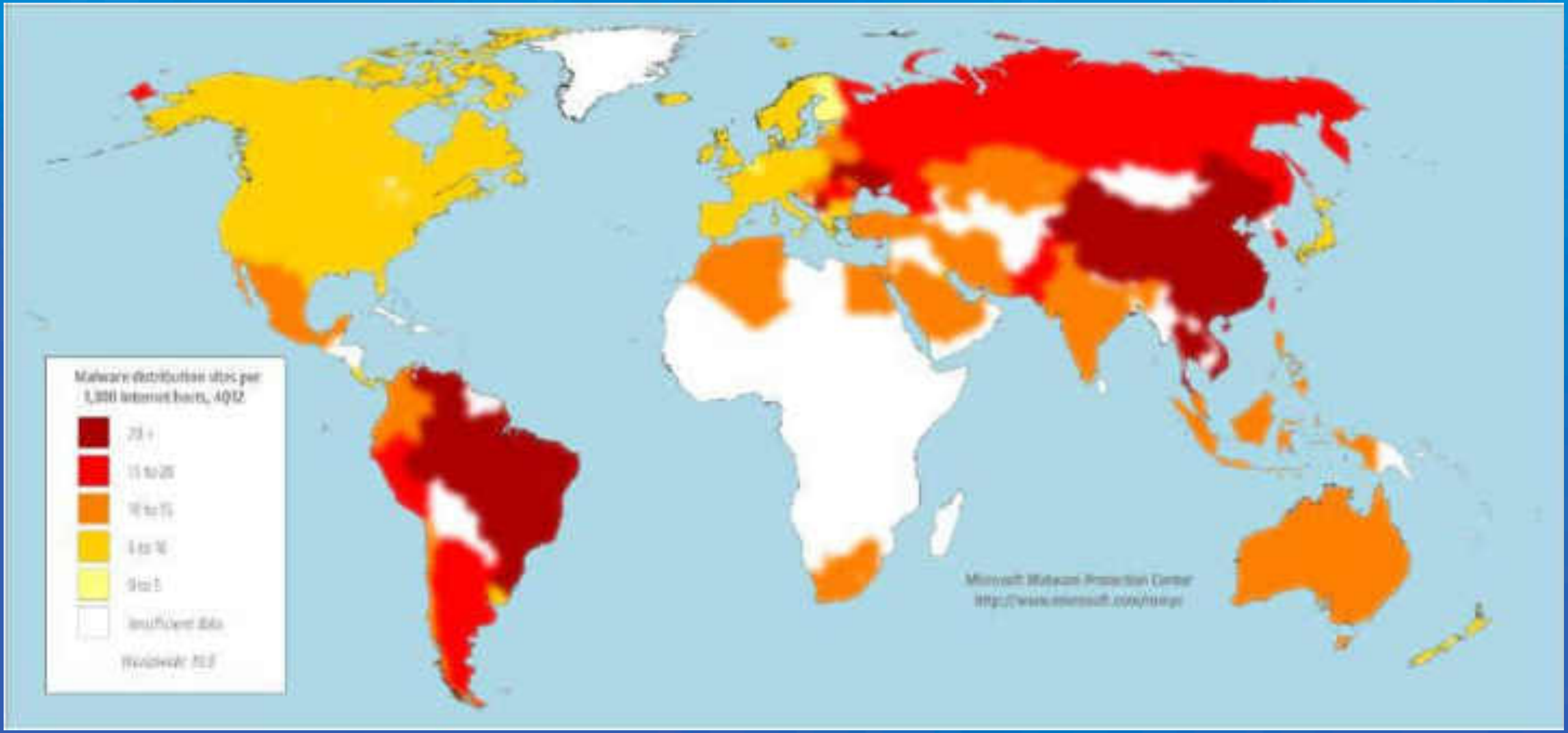


Malware distribution, 3Q12



Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Malware distribution, 4Q12


Malware distribution sites per 1,000 internet hosts, 4Q12
20 +
15 to 20
10 to 15
5 to 10
0 to 5
Insufficient data
Worldwide: [illegible]
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

What worries me

Fun with Android

- XSS in AirDroid allows DoS against host
- Send malicious SMS to premium-rate numbers to steal money
- Siphon data with Wi-Fi tether software, Shark for Root, and OpenVPN
- SIM destruction from visiting infected website

Now more popular than Windows for malware authors

(Kaspersky Labs)

BYOD

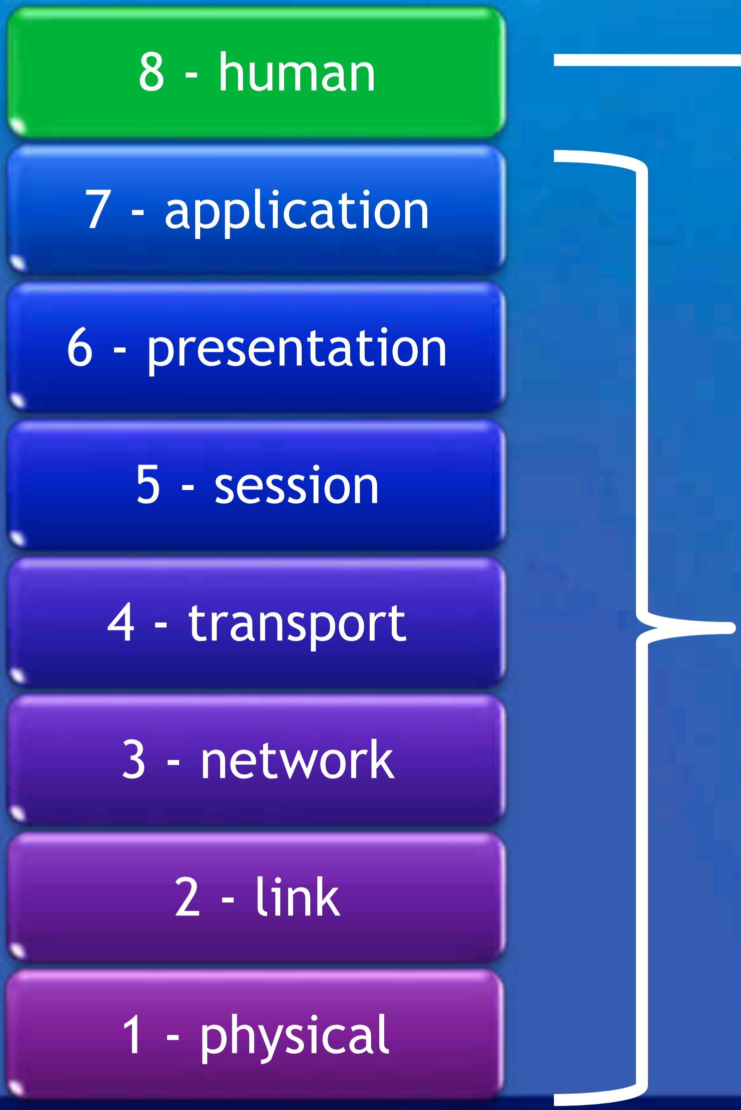
=

weak platform

+

oblivious users

People as targets



8 - human

7 - application

6 - presentation

5 - session

4 - transport

3 - network

2 - link

1 - physical

- *Figure it out on your own*
- *Minimal training exposure (few minutes a year)*
- *Quickly forgotten or ignored*
- *Unpredictable*

- Written code
- Thoroughly tested (including penetration)
- Updated regularly
- Functions only as designed

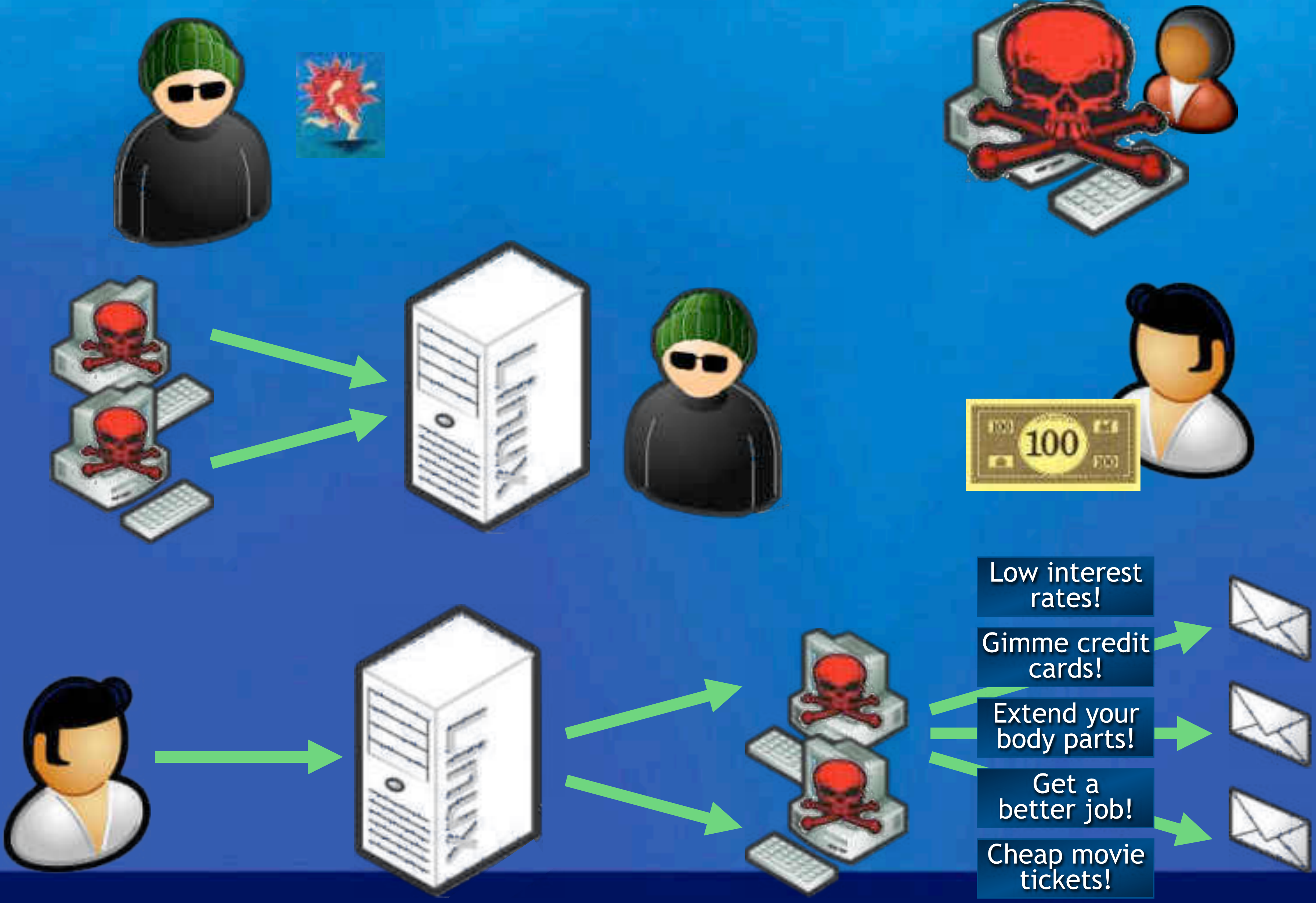
Targeted: Spear phishing

- Criminals bombard businesses with targeted spam that looks and feels like internal messaging
  - Think…how did they learn the formatting and style…?
- Usually spoofs IT and HR
- Duped people reveal credentials; attackers easily get inside
- Great for attacking small organizations

Targeted: Watering hole

- Attackers inject malware into website whose typical visitors are the target audience
- Plant multiple tools, including log harvesters
- Popular among hacktivists and those plotting espionage

Botnets: frighteningly successful



Low interest rates!

Gimme credit cards!

Extend your body parts!

Get a better job!

Cheap movie tickets!

An affiliates program

“Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn't require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups.”

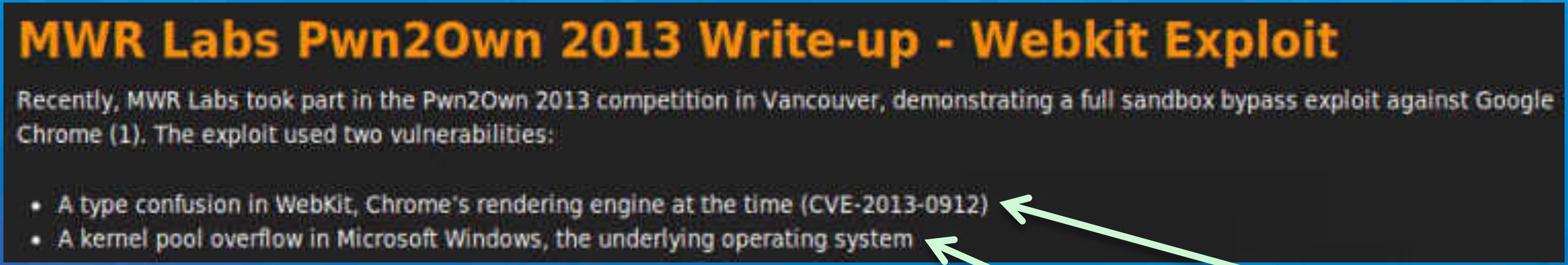
Let’s do the math

$BOTNET spams 100,000,000 mailboxes. What if…

10%	Read email and clicked link	10,000,000
1%	Signed up for a three-day trial	100,000
		$0.50
		$50,000
1%	Enrolled for 1 year	1,000
		$144
		$144,000

Would *YOU* do it???

Vulnerability chaining



MWR Labs Pwn2Own 2013 Write-up - Webkit Exploit

Recently, MWR Labs took part in the Pwn2Own 2013 competition in Vancouver, demonstrating a full sandbox bypass exploit against Google Chrome (1). The exploit used two vulnerabilities:

- A type confusion in WebKit, Chrome's rendering engine at the time (CVE-2013-0912)
- A kernel pool overflow in Microsoft Windows, the underlying operating system

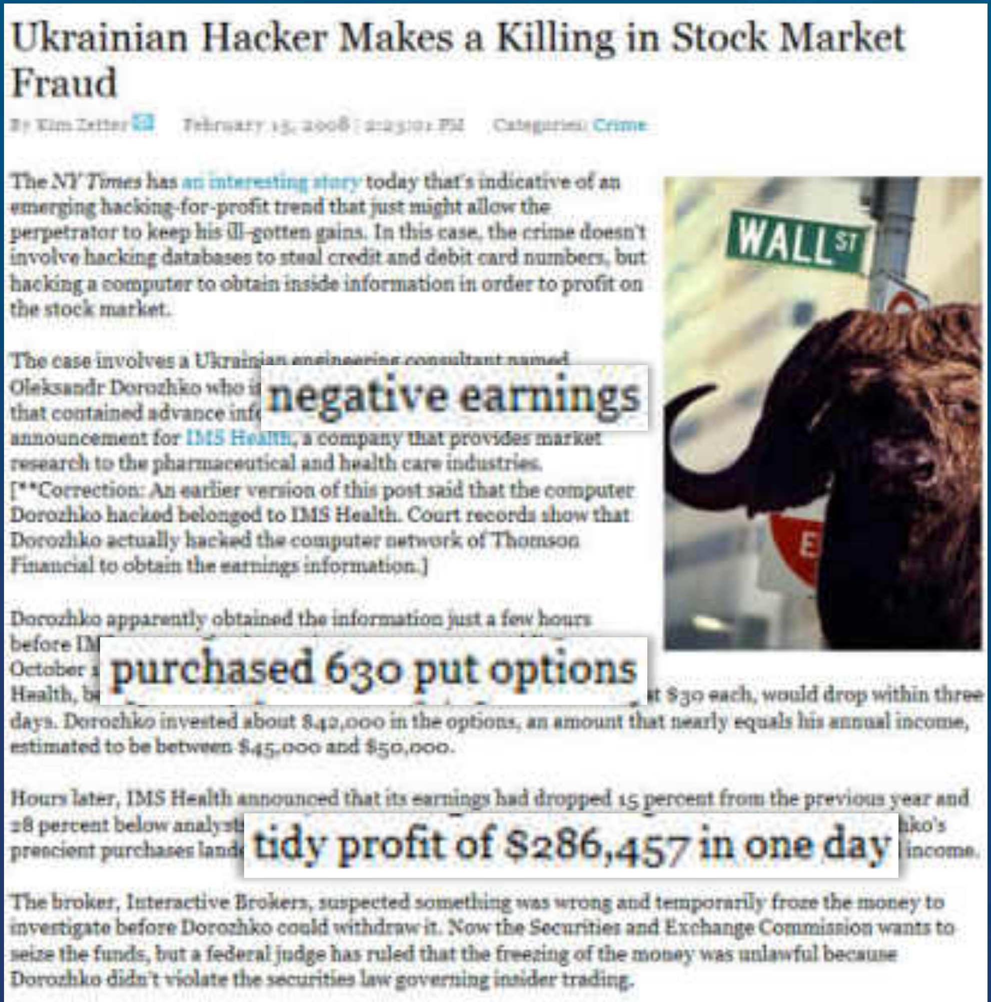
- Escaped sandboxed renderer
- Acquired elevated privileges
- Bypassed ASLR and DEP
- Executed arbitrary code

http://labs.mwrinfosecurity.com/blog/2013/04/19/mwr-labs-pwn2own-2013-write-up---webkit-exploit/

DoS attacks popular again

- THC SSL DoS
  rapid key renegotiation
- R.U.D.Y. (R U Dead Yet?)
  slow rate HTTP POST, server hangs while waiting for long form input to complete
- Slowloris
  trickle feed of HTTP headers over several simultaneous connections
- Sockstress
  overtake host with perpetually stalled connections

Attacks against integrity



Ukrainian Hacker Makes a Killing in Stock Market Fraud

By Kim Zetter ✉ February 15, 2008 | 2:23:01 PM Categories: Crime

The *NY Times* has an interesting story today that's indicative of an emerging hacking-for-profit trend that just might allow the perpetrator to keep his ill-gotten gains. In this case, the crime doesn't involve hacking databases to steal credit and debit card numbers, but hacking a computer to obtain inside information in order to profit on the stock market.

The case involves a Ukrainian engineering consultant named Oleksandr Dorozhko who i

negative earnings

that contained advance inf

announcement for IMS Health, a company that provides market research to the pharmaceutical and health care industries. [**Correction: An earlier version of this post said that the computer Dorozhko hacked belonged to IMS Health. Court records show that Dorozhko actually hacked the computer network of Thomson Financial to obtain the earnings information.]

Dorozhko apparently obtained the information just a few hours before IM

October

purchased 630 put options

Health, be

t $30 each, would drop within three days. Dorozhko invested about $42,000 in the options, an amount that nearly equals his annual income, estimated to be between $45,000 and $50,000.

Hours later, IMS Health announced that its earnings had dropped 15 percent from the previous year and 28 percent below analysts

hko's

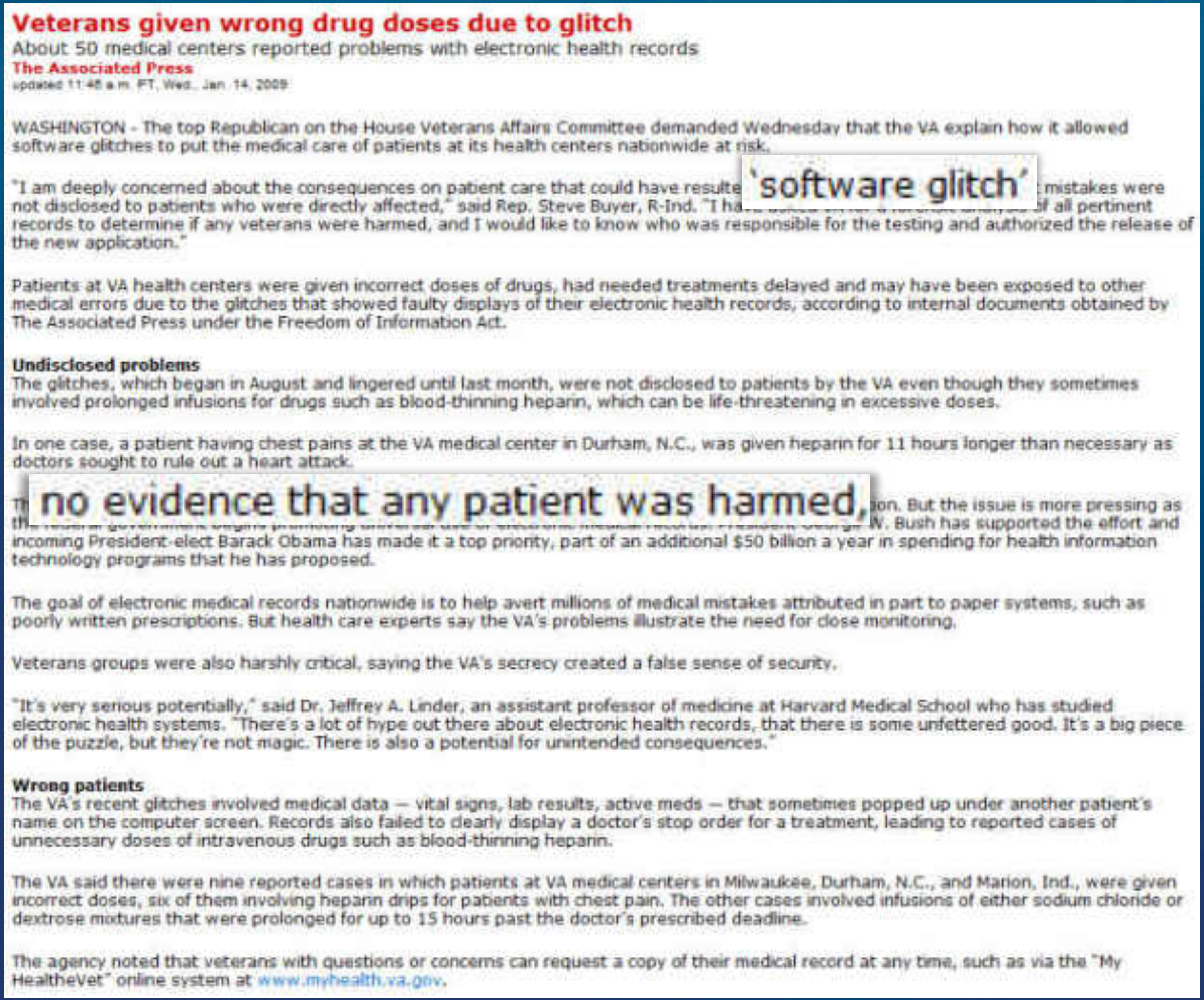
prescient purchases land

tidy profit of $286,457 in one day

income.

The broker, Interactive Brokers, suspected something was wrong and temporarily froze the money to investigate before Dorozhko could withdraw it. Now the Securities and Exchange Commission wants to seize the funds, but a federal judge has ruled that the freezing of the money was unlawful because Dorozhko didn't violate the securities law governing insider trading.

http://blog.wired.com/27bstroke6/2008/02/ukrainian-hacke.html



Veterans given wrong drug doses due to glitch

About 50 medical centers reported problems with electronic health records

The Associated Press

updated 11:48 a.m. PT, Wed., Jan. 14, 2009

WASHINGTON - The top Republican on the House Veterans Affairs Committee demanded Wednesday that the VA explain how it allowed software glitches to put the medical care of patients at its health centers nationwide at risk.

'software glitch'

"I am deeply concerned about the consequences on patient care that could have resulte mistakes were not disclosed to patients who were directly affected," said Rep. Steve Buyer, R-Ind. "I ha of all pertinent records to determine if any veterans were harmed, and I would like to know who was responsible for the testing and authorized the release of the new application."

Patients at VA health centers were given incorrect doses of drugs, had needed treatments delayed and may have been exposed to other medical errors due to the glitches that showed faulty displays of their electronic health records, according to internal documents obtained by The Associated Press under the Freedom of Information Act.

Undisclosed problems

The glitches, which began in August and lingered until last month, were not disclosed to patients by the VA even though they sometimes involved prolonged infusions for drugs such as blood-thinning heparin, which can be life-threatening in excessive doses.

In one case, a patient having chest pains at the VA medical center in Durham, N.C., was given heparin for 11 hours longer than necessary as doctors sought to rule out a heart attack.

no evidence that any patient was harmed,

Th ion. But the issue is more pressing as th W. Bush has supported the effort and incoming President-elect Barack Obama has made it a top priority, part of an additional $50 billion a year in spending for health information technology programs that he has proposed.

The goal of electronic medical records nationwide is to help avert millions of medical mistakes attributed in part to paper systems, such as poorly written prescriptions. But health care experts say the VA's problems illustrate the need for close monitoring.

Veterans groups were also harshly critical, saying the VA's secrecy created a false sense of security.

"It's very serious potentially," said Dr. Jeffrey A. Linder, an assistant professor of medicine at Harvard Medical School who has studied electronic health systems. "There's a lot of hype out there about electronic health records, that there is some unfettered good. It's a big piece of the puzzle, but they're not magic. There is also a potential for unintended consequences."

Wrong patients

The VA's recent glitches involved medical data — vital signs, lab results, active meds — that sometimes popped up under another patient's name on the computer screen. Records also failed to clearly display a doctor's stop order for a treatment, leading to reported cases of unnecessary doses of intravenous drugs such as blood-thinning heparin.

The VA said there were nine reported cases in which patients at VA medical centers in Milwaukee, Durham, N.C., and Marion, Ind., were given incorrect doses, six of them involving heparin drips for patients with chest pain. The other cases involved infusions of either sodium chloride or dextrose mixtures that were prolonged for up to 15 hours past the doctor's prescribed deadline.

The agency noted that veterans with questions or concerns can request a copy of their medical record at any time, such as via the "My HealtheVet" online system at www.myhealth.va.gov.

http://www.msnbc.msn.com/id/28655104/

Attackers follow a pattern

First they came for bandwidth by attacking availability. They executed denial of service attacks starting in the mid 1990s and monetized later with extortion.

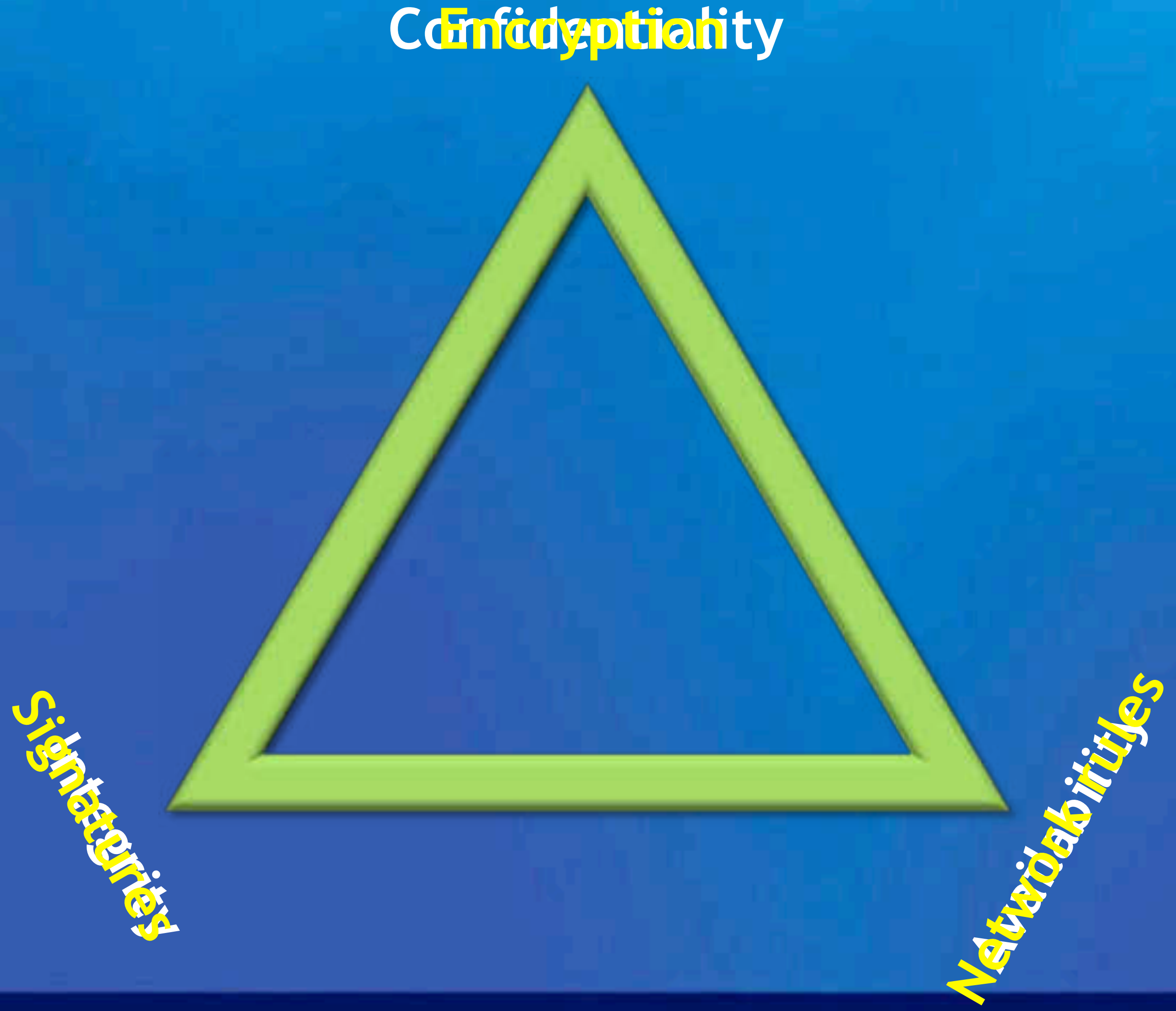
Next they came for secrets by attacking confidentiality. They disclosed sensitive data starting in the late 1990s and monetized with personally identifiable information and accounts for sale in the underground.

Now they're coming to make a difference by attacking integrity. They degraded information starting at the beginning of the 2000s. These attacks will manifest as changes to trusted data such that those alterations benefit the party making the change. This sort of attack undermines the trustworthiness of data.

*Props to **Richard Bejtlich**, http://taosecurity.blogspot.com/2008/02/first-they-came-for-bandwidth.html*

What to do

Attack progressions



Confidentiality

Encryption

Integrity

Signatures

Availability

Network rules

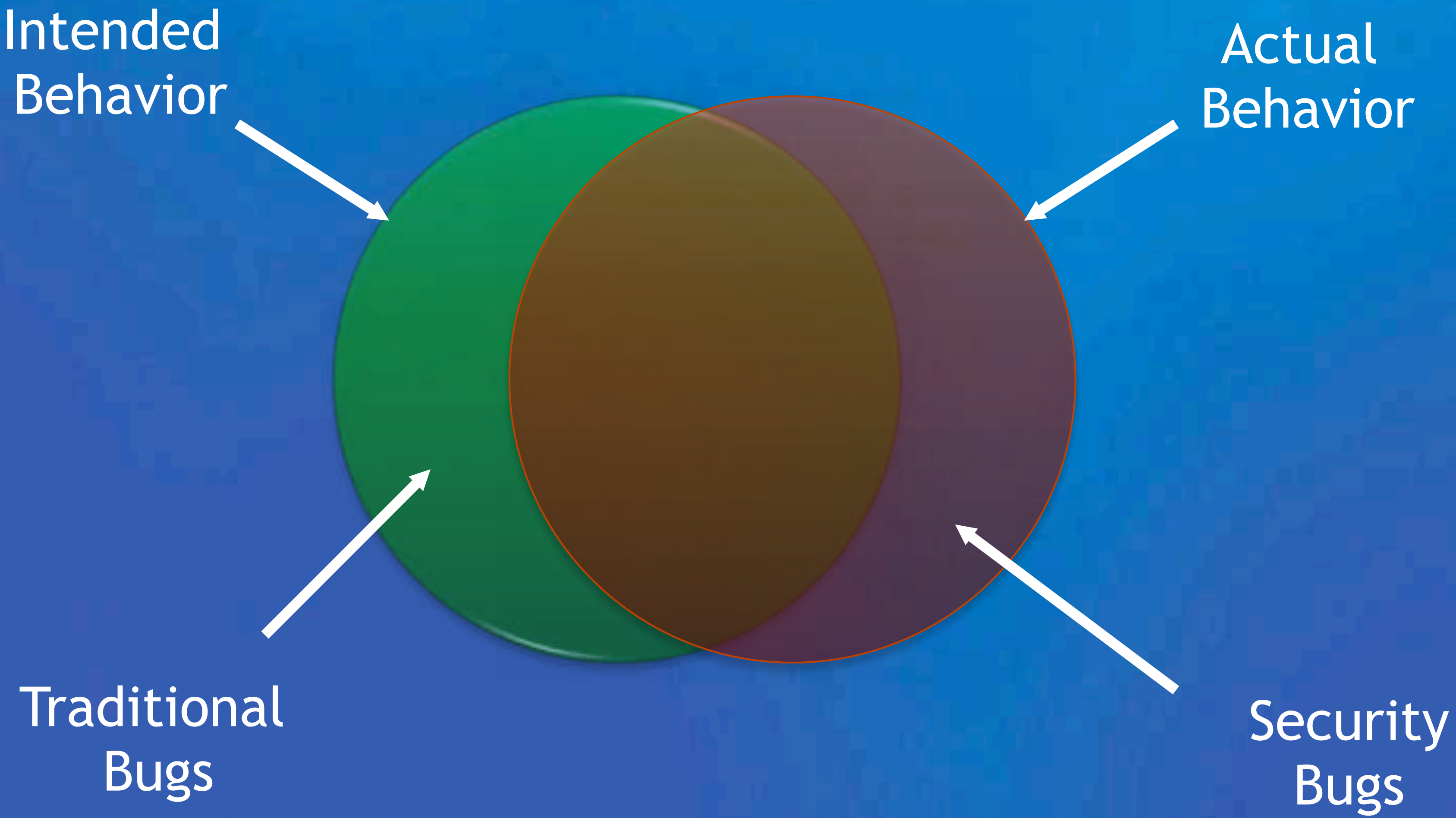
Think like a bad guy

Who would ever attack us?

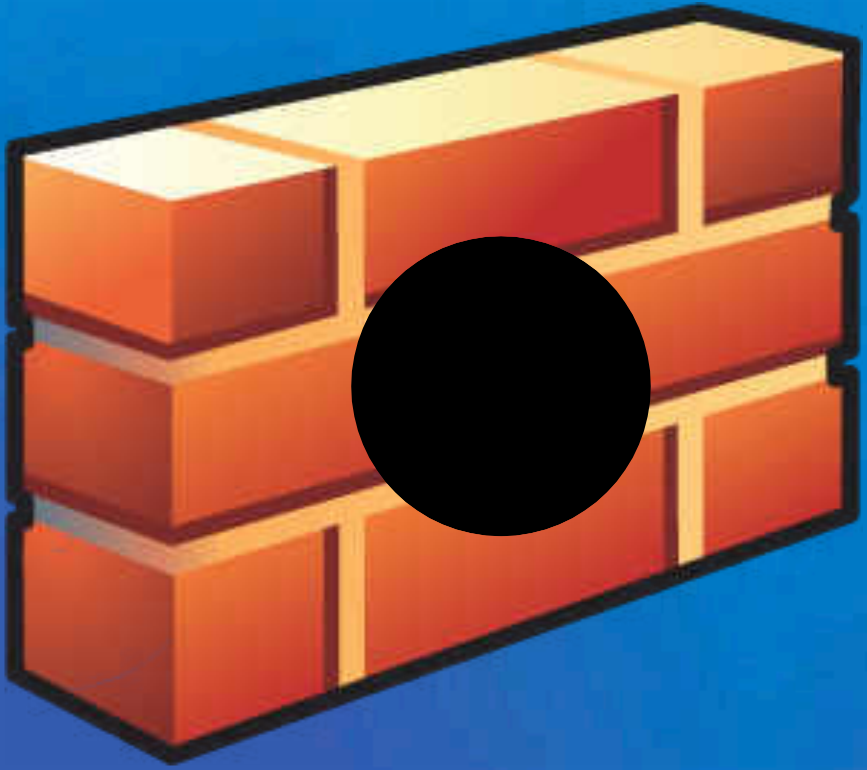
- You have **data**, you have a **net** connection
  - *Therefore, you are interesting*
- Hire some testers who are good at **breaking things** *(maybe your kids?)*
  - Think about how your code could be abused
- Build **resiliency** and **protection** into your applications

A personal example

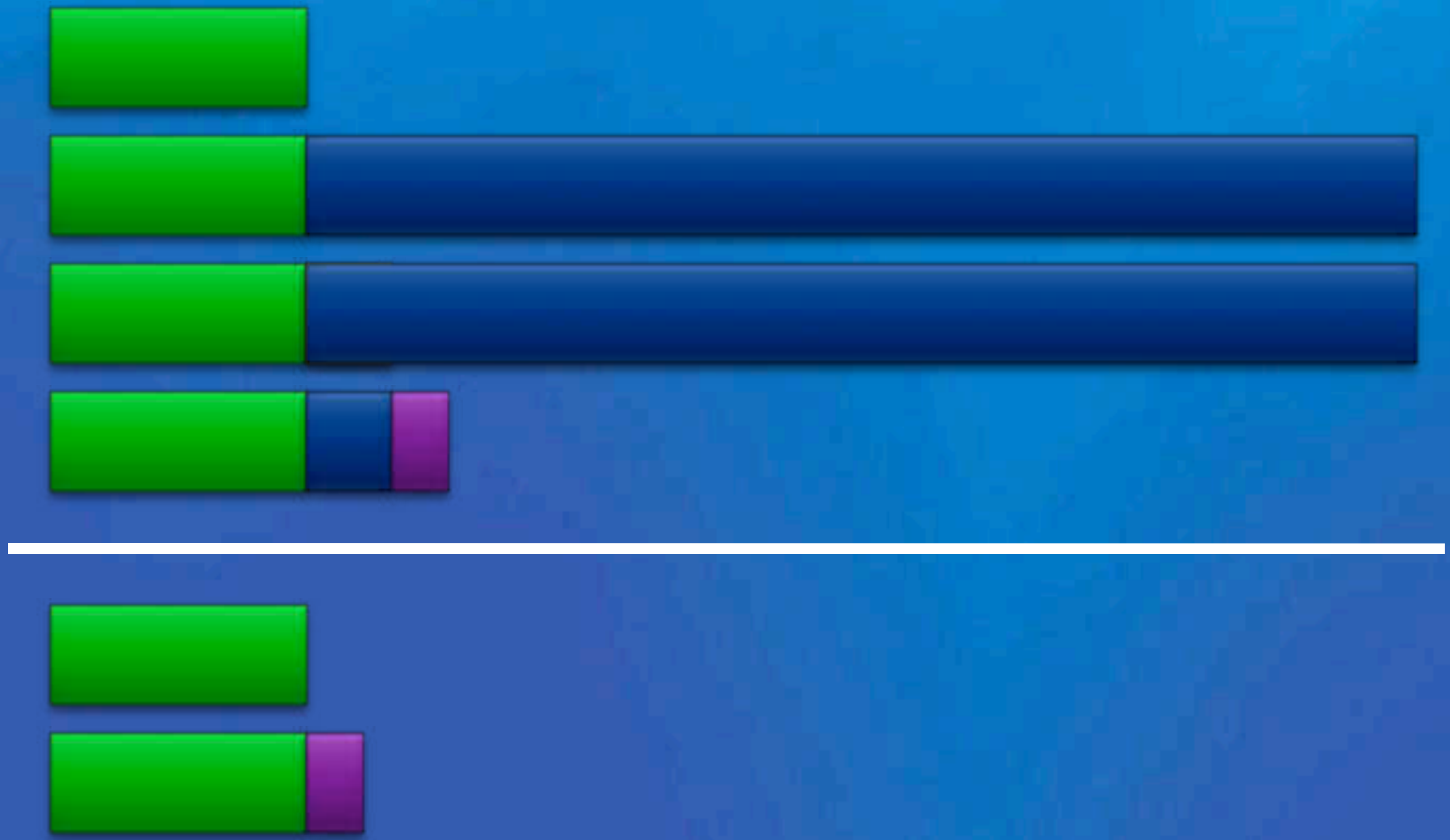
No input validation → get free stuff



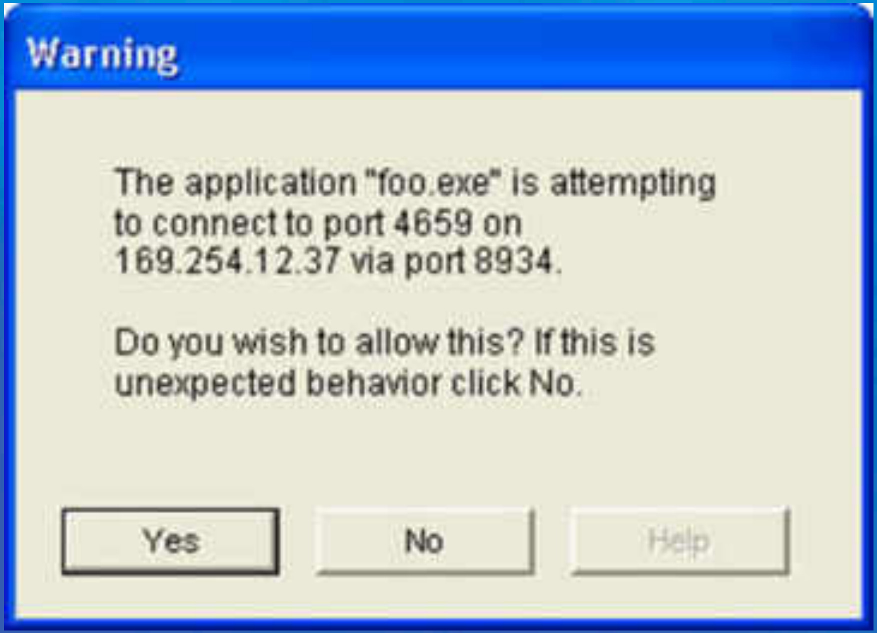
Single-layer protection



Reduce the attack surface

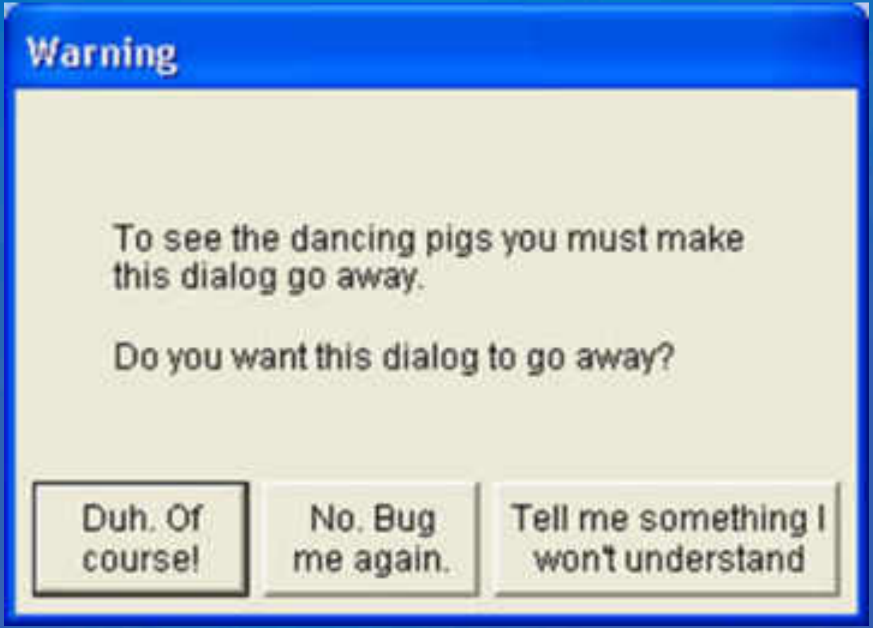


Avoid poor user decisions



The application "foo.exe" is attempting to connect to port 4659 on 169.254.12.37 via port 8934.

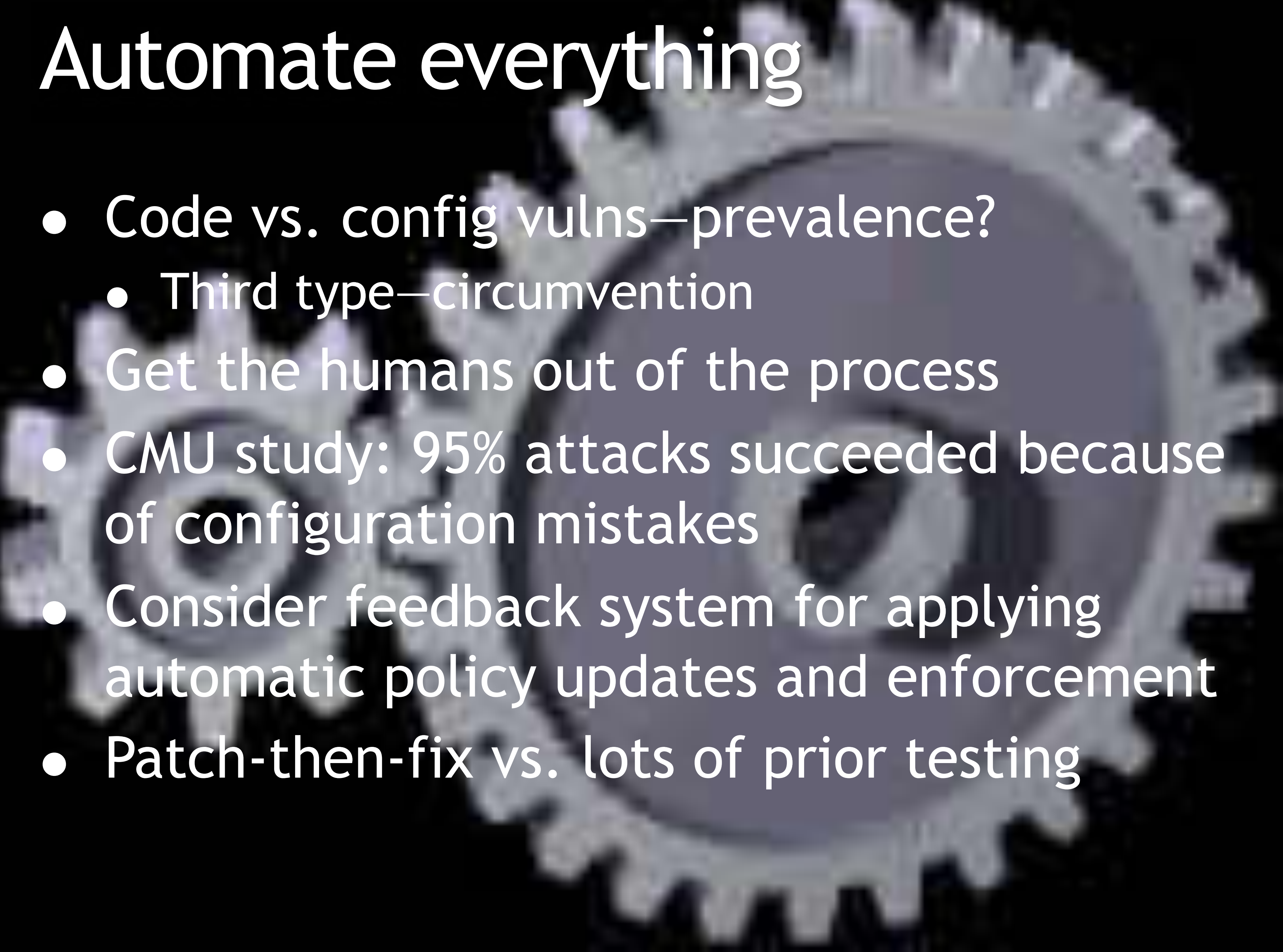
Do you wish to allow this? If this is unexpected behavior click No.



To see the dancing pigs you must make this dialog go away.

Do you want this dialog to go away?

Automate everything



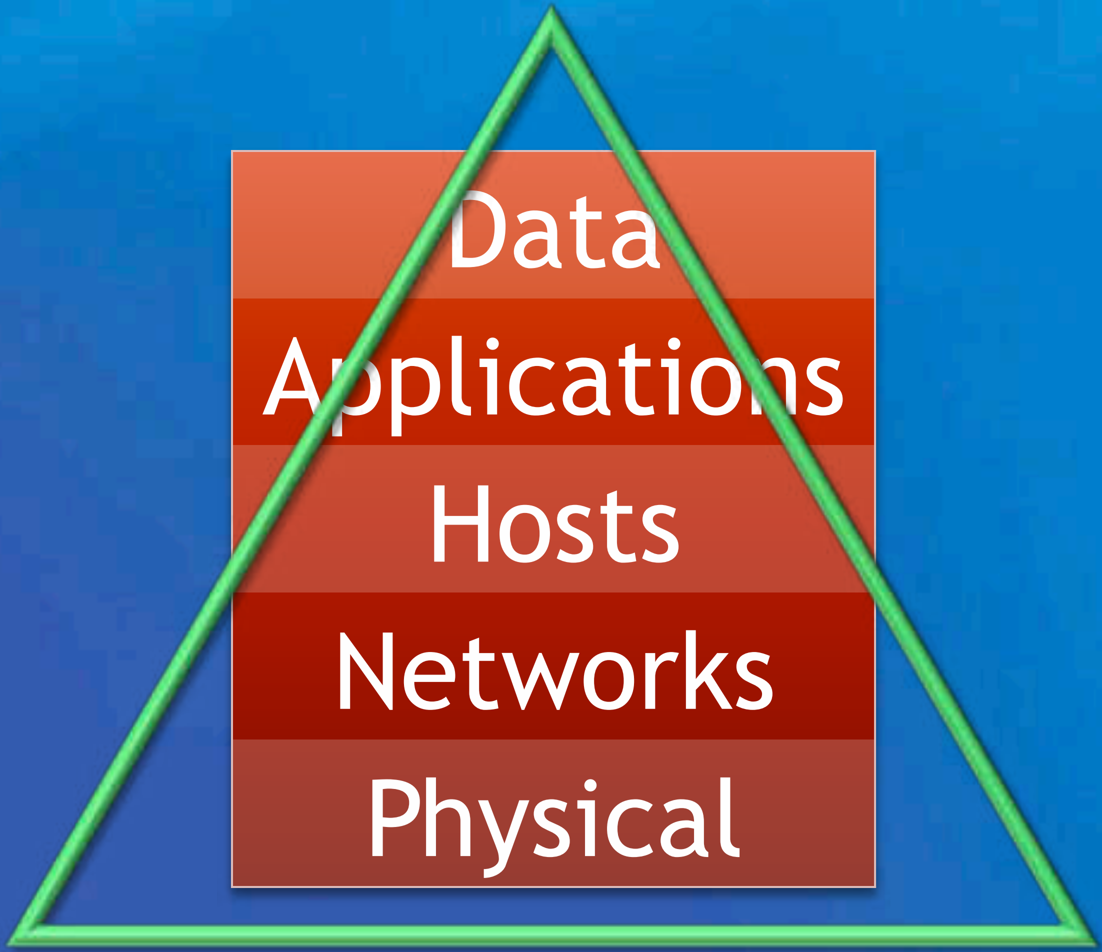
- Code vs. config vulns—prevalence?
  - Third type—circumvention
- Get the humans out of the process
- CMU study: 95% attacks succeeded because of configuration mistakes
- Consider feedback system for applying automatic policy updates and enforcement
- Patch-then-fix vs. lots of prior testing

K L M N O P Q R S
L M N O P Q R S T
Z A B C D E F G
I J K L M N O P Q
B C D E F G H I J

Encryption works—use it!

- Time/cost trade-off
  - Buy a safe (and its protection level) based on value of contents
  - Consider similar approach to encryption and digital signatures
- Watch this space
  - Predicate e.—policy-driven portion access
  - Functional e.—plaintext must satisfy some function (perhaps an identity)
  - Homomorphic e.—do work without decrypting

It's all about the data



Data

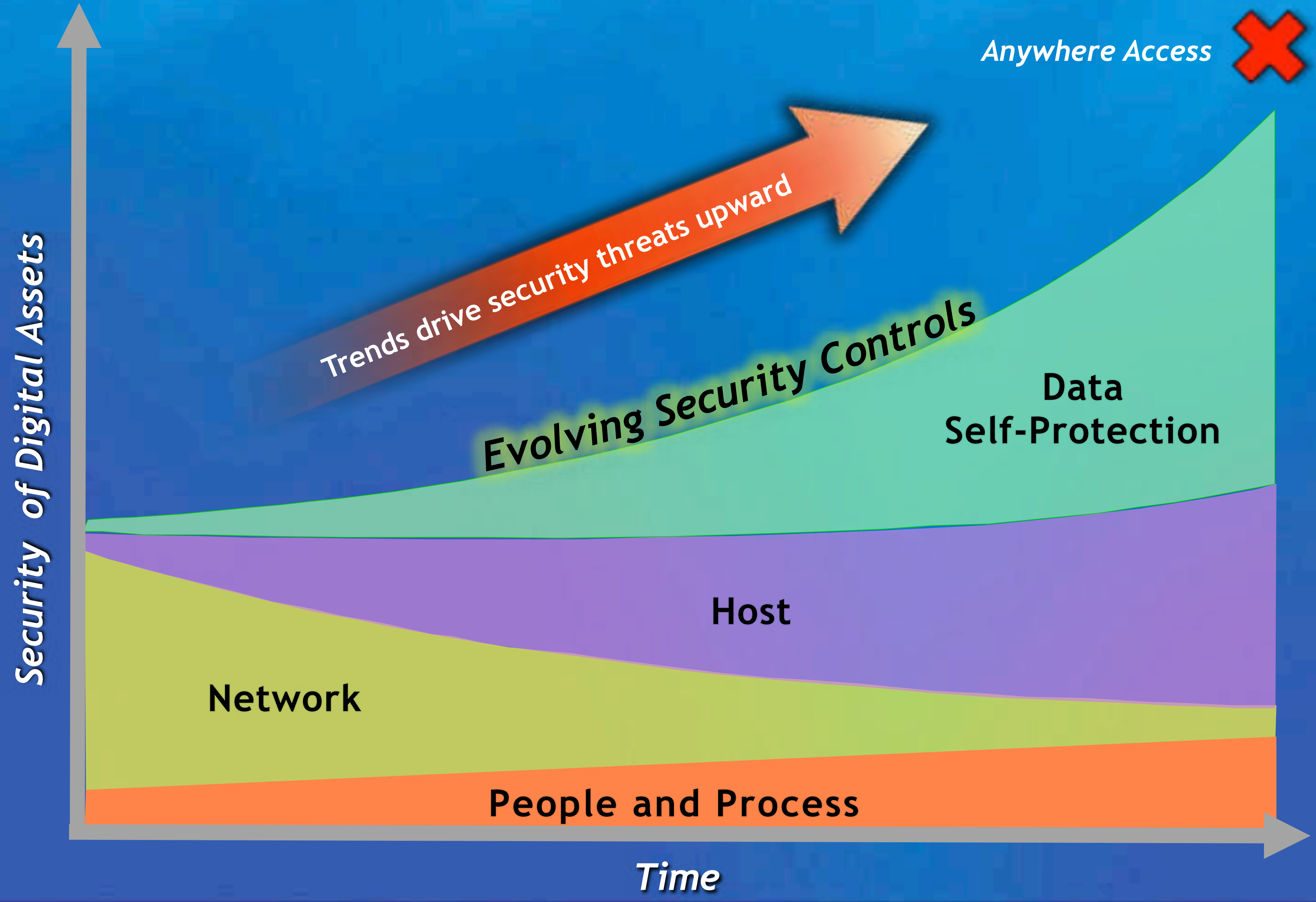
Applications

Hosts

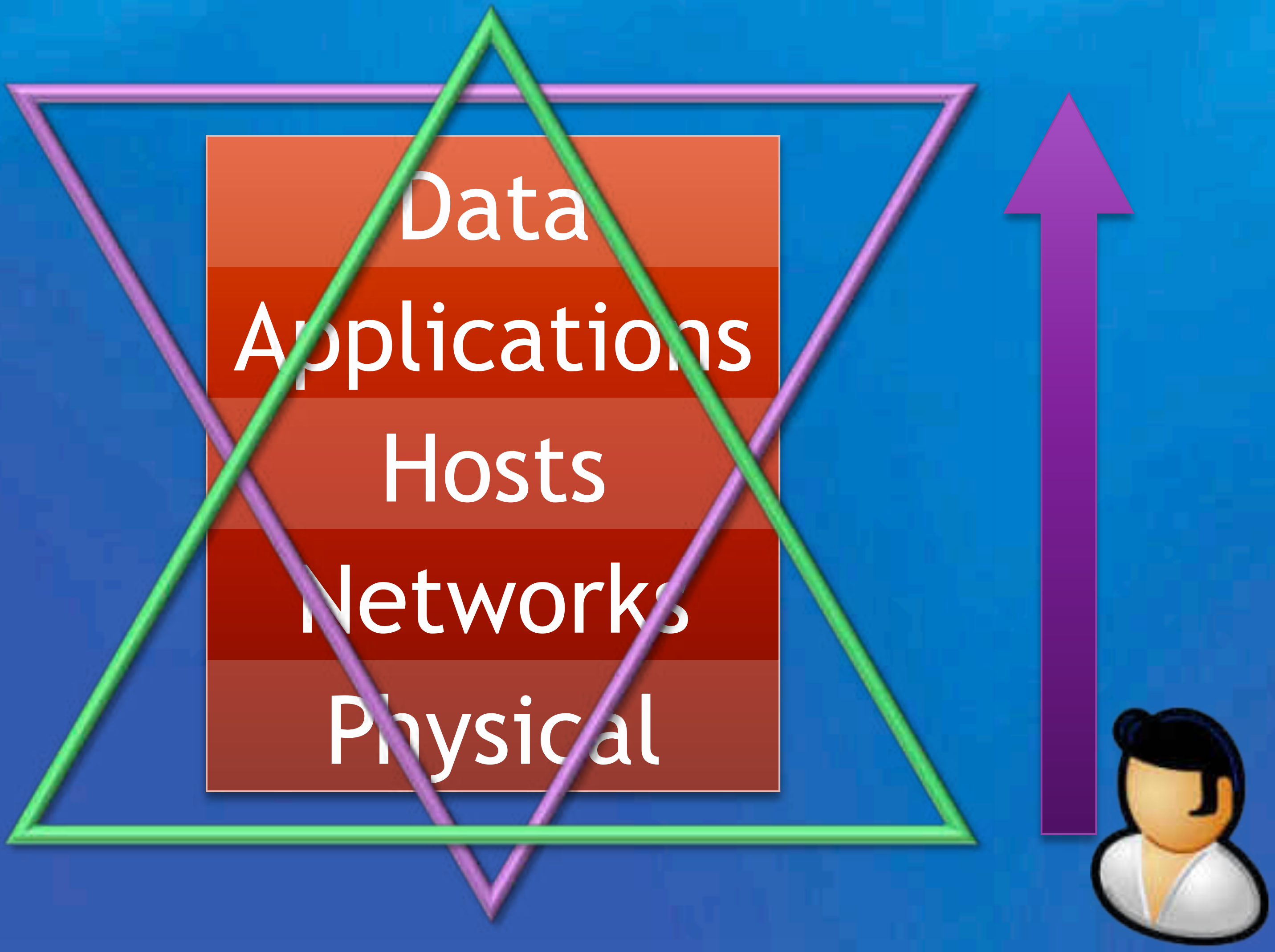
Networks

Physical

Guiding principles

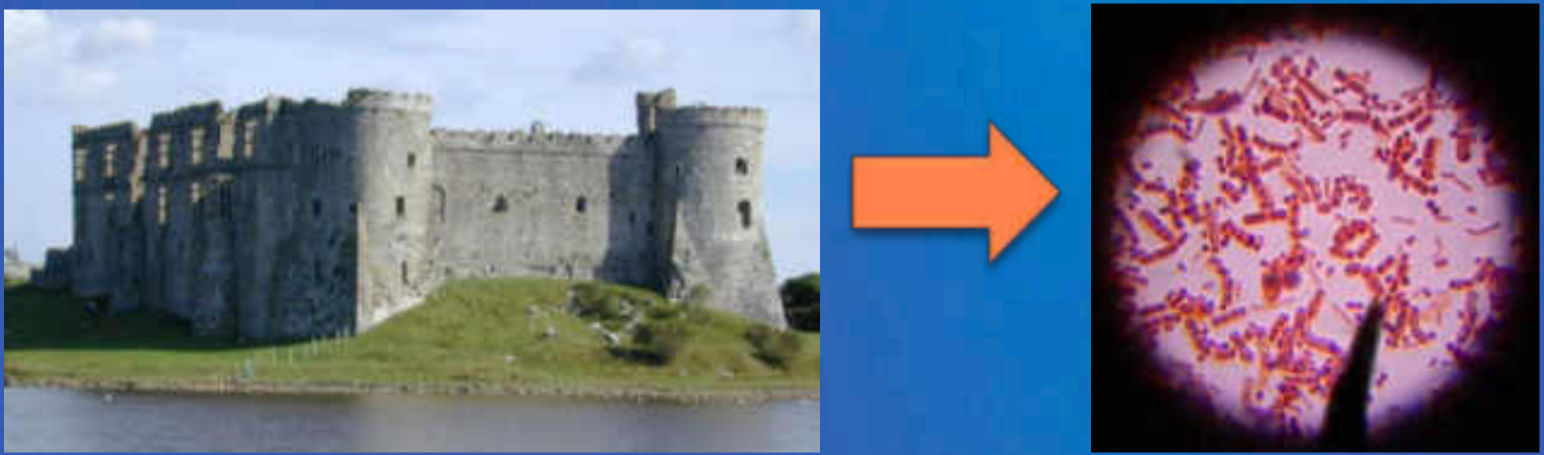


It's all about the data



Fortress vs. biology

- “Defense in depth” blah blah blah
- How many layers are enough?
- Biological systems provide “graceful degradation” with some functionality



Stuff to consider

- **Shrink** exposure
- **Consolidate** resources
- **Streamline** processes
- **Standardize** builds and configuration
- **Add redundancy** to mitigate DoS
- **Require authentication** for all access
- **Encrypt/sign data** in storage and in transit
- **Validate** transactions and procedures
- **Audit activity** for accountability and compliance

Yes, it's real work.
So start planning now.

Thank you!

Steve Riley
Technical Director, CTO Office
steve.riley@riverbed.com