Are We Insane?

David Barton
Managing Director,
UHY LLP
Objectives

• Current State
• Where we came from
• What we have done
• What we continue to do
• Paradigm Shift
• Conclusion
Current State

Swiped
Credit-card fraud, $bn

<table>
<thead>
<tr>
<th>Year</th>
<th>Total</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2004</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2005</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2006</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2007</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2008</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>2009</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>2010</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>2011</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>2012</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

Source: The Nilson Report

in 2013 alone there were 199 breaches affecting over 7 million patient records

Ice Miller
LEGAL COUNSEL
Current State

**Large-Scale Data Breaches Affect Millions of Users**
Number of compromised data records in selected data breaches

- **Adobe** 2013: 152m
- **eBay** 2014: 145m
- **Heartland** 2009: 130m
- **T.J. Maxx** 2007: 94m
- **AOL** 2005: 92m
- **Sony PSN** 2011: 77m
- **US Military** 2009: 76m
- **Target** 2014: 70m
- **Evernote** 2013: 50m
- **LivingSocial** 2014: 50m

Source: Media reports
Current State

Fraud Incidence by Data Breach Victims, Non-Data-Breach Victims, and All Fraud Victims

Q2. In the past 12 months, have you been notified by a business or other institution that your personal or financial information has been lost, stolen, or compromised in a data breach?

October 2010 - 2012, n = varies 337 - 5,249
Base: All consumers, data breach victims, non data breach victims.
© 2013 Javelin Strategy & Research
Current State

Annual Global Fraud Losses (in Billions)

- Year: 2000, Losses: $2 billion
- Year: 2001, Losses: $2.2 billion
- Year: 2002, Losses: $2.5 billion
- Year: 2003, Losses: $2.8 billion
- Year: 2004, Losses: $3.1 billion
- Year: 2005, Losses: $3.5 billion
- Year: 2006, Losses: $3.9 billion
- Year: 2007, Losses: $4.3 billion
- Year: 2008, Losses: $4.7 billion
- Year: 2009, Losses: $5.1 billion
- Year: 2010, Losses: $5.6 billion
- Year: 2011, Losses: $6.1 billion
- Year: 2012, Losses: $6.6 billion

CardHub
Current State
Current State

TARGET

$148 Million
A little History......
Where we came from... 1970s
Where we came from.... 1990s
What we’ve done

• Physical connectivity
• Passwords
• Firewalls
• IDS/IPS
• 2 factor authentication
• VPN
• Encryption
What we’ve done

• What does all this have in common?
What we’ve done

Firewalls were designed and implemented to separate internal resources from the outside world.
“History has shown us that perimeter defenses, whether they are stone walls or firewalls, will be breached.”

– Prakash Panjwani
President & Chief Executive Officer

safenet-inc.com/data-protection
Insight

November 2011 – CSA Congress - Orlando

• My first time as an attendee
• Lots of discussion of Cloud Security challenges
• Phrase I heard consistently was:

“Collapse the perimeter”
"In recent years, traditional “perimeter-based” security models have been rendered less effective by two evolving forces: the increasing sophistication, frequency, and scale of cybercrime and the rapid adoption of new, disruptive IT technologies such as social, mobile and cloud."

Nicholas Evans - Computerworld
Insight

“The perimeter has been eroded by the forces of globalization, ubiquitous connectivity, mobility, teleworking, virtualization, and cloud computing. The concept of a ‘perimeter’ becomes difficult to define when the concepts of inside and outside change rapidly and fluidly.”

Andreas Antonopoulos – Nemertes Research
Insight

“The line between the public internet and the internal network is fading. Remote workers, virtualization, BYOD and outsourcing have combined to cloud the boundaries of an enterprise’s network.”

Avishai Wool – TechNews World
What should we conclude?

THERE IS NO PERIMETER
What to Do???

• More of the same?
  – What is your organization’s budget for network security hardware?
  – How many new internal network layers will you add this year?
  – What new types of authentication will you implement?
“The definition of insanity is doing the same thing over and over again and expecting different results.”

Albert Einstein
THE FIRST STEP IN RECOVERY

IS ADMITTING YOU HAVE A PROBLEM
“These strategies are 20 years old and have to change. A completely different way of thinking is required. 80 percent of security spend is going on firewalls, IDS and anti-virus solutions, despite only being effective to 30 percent of threats.”

former Websense CSO Jason Clark
Insight

Tsion Gonen, chief strategy officer with SafeNet, made this observation:

• “Until very recently, companies did not see the financial impacts of data breaches being that significant. However, following the Target breach, this has changed drastically. But unfortunately, what has not changed is how companies secure customer data. This potential breach and the many data breaches we have seen recently are a symptom of an outdated approach to data security. Companies need to have a Plan B that enables them to secure the breach after intruders penetrate the perimeter defenses.”

Gonen recommended taking steps such as attaching security directly to the data itself and using data encryption as the last line of defense. That, he said, would make the data useless to thieves.

What do you think of Gonen’s recommendations?
Insight

“...we need to find ways to protect data rather than trying to build elaborate and often difficult architectures to compensate for today's poorly written applications.”

Rafal Los - Director, Solutions Research at Accuvant
Collapse the Perimeter
The concept

A shopping mall
Getting beyond the concept
Getting beyond the concept
Getting beyond the concept
Getting beyond the concept
Which "data" will have better security?
New Techniques

• Endpoint Activity Monitoring
• Software Defined Perimeter
  – Servers only receive traffic from authenticated device, application, and location
• Zero Trust
  – Protects data and assets from the inside-out
  – Provide advanced data protection to all critical data assets at rest and in motion
• Data Loss Prevention
  – More and better systems for detecting “merchandise” leaving the “store” unauthorized
Data Classification

• Public or non-classified
• Internal use – only for use inside the organization
• Confidential – should be strongly protected against unauthorized use and disclosure
• Secret – very limited access with very strong protection
Train your People

• People are the weakest link
  – Everyone is different
  – Goals and objectives don’t always align

• “Why” is important
  – Not enough to know what the policy is
  – Also need to know why it is in place
  – Lots of examples help reinforce

• Train often
  – People forget so they have to be reminded
  – New threats everyday
David Barton,
Managing Director
UHY LLP
Six Concourse Parkway
Suite 1700
Atlanta, GA 30328
678-602-4400

Twitter: @itcontrolsfreak
Blog: itcontrolsfreak.wordpress.com