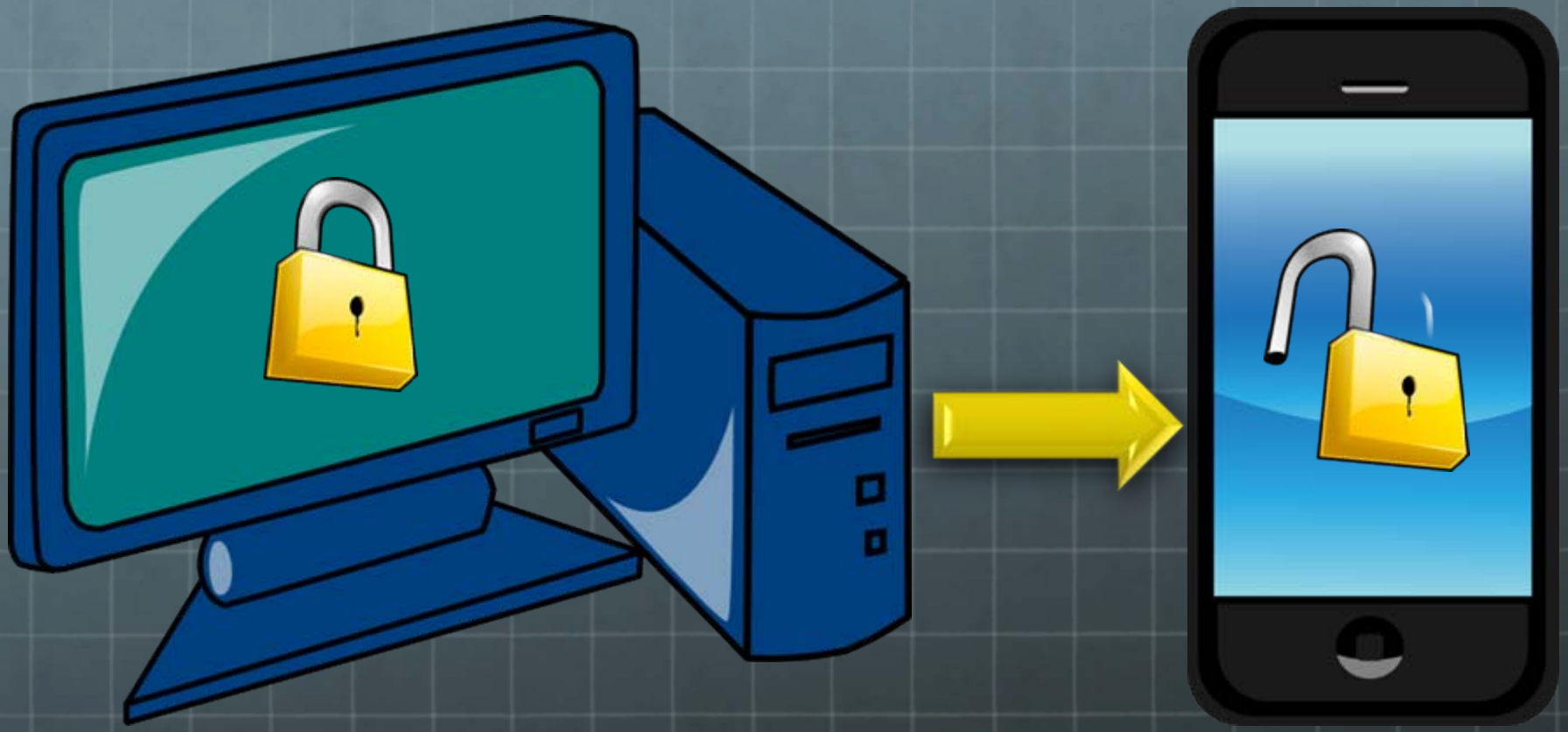


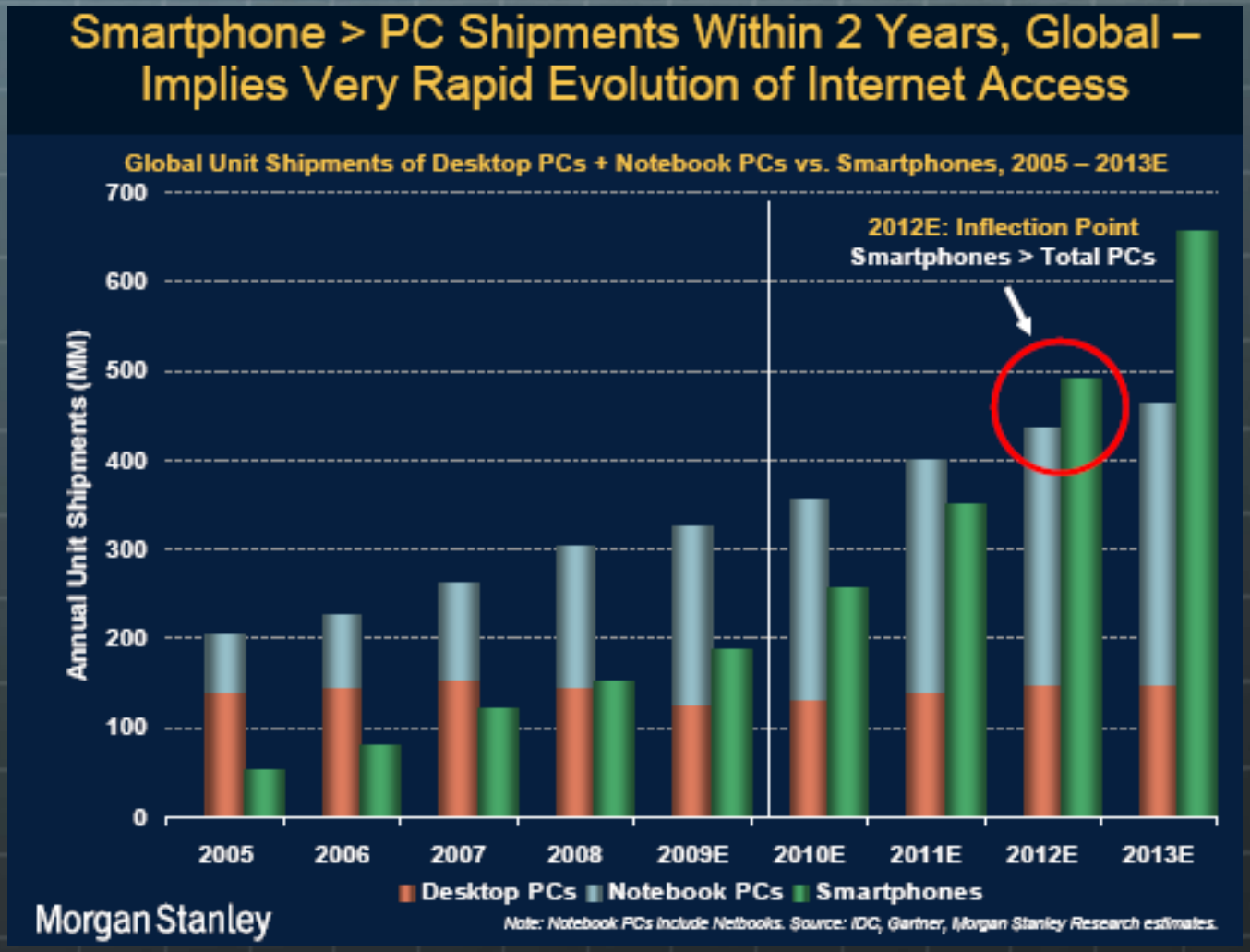
Mobile Device Security

Exploring and Understanding the Challenges in the Shift From the Desktop To the Personal Area Network

About The Presenter

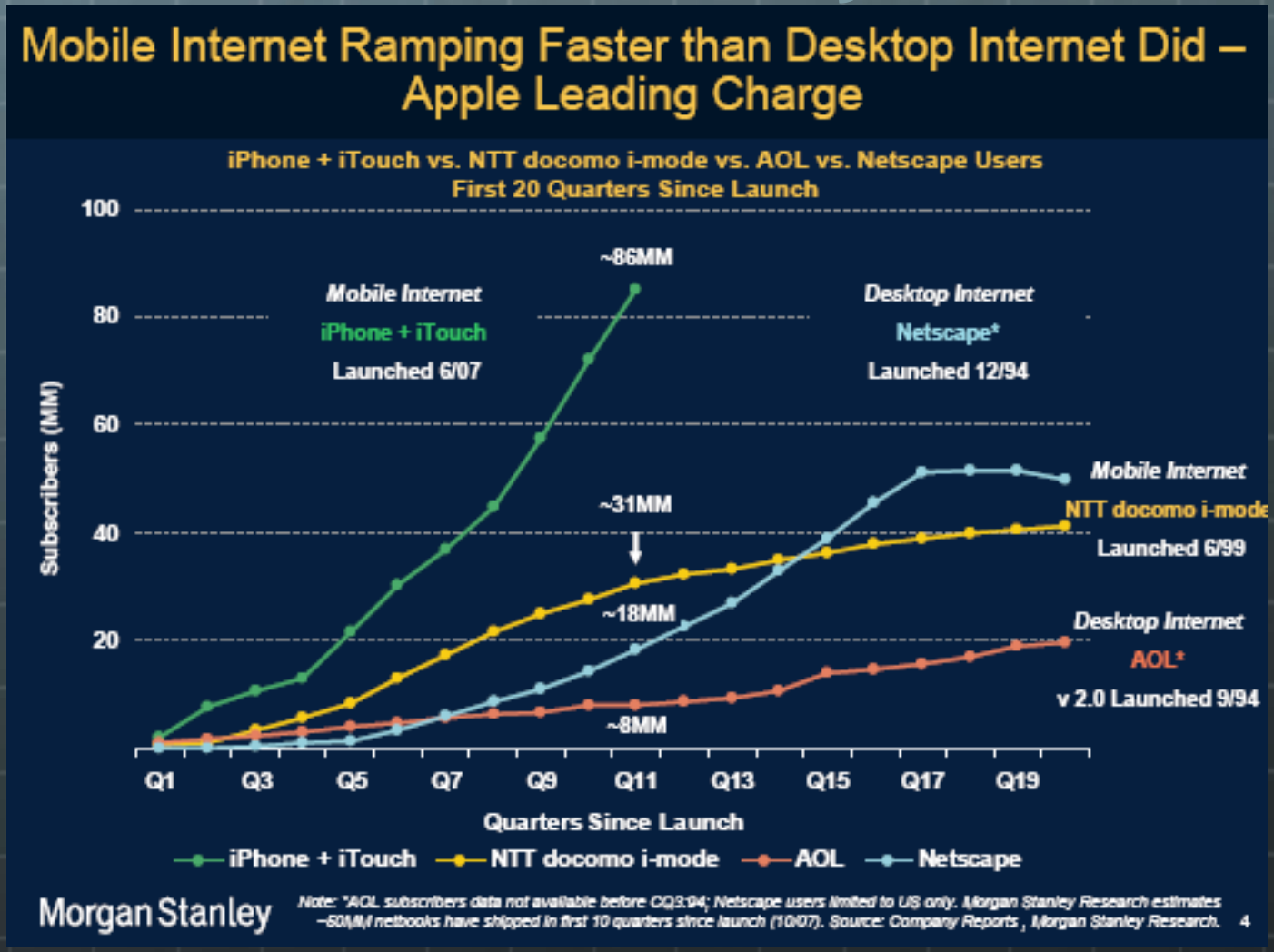
- Mike Ahmadi served as the CIO of a retail organization that implemented mobile devices for business intelligence systems over a decade ago.
- His current company develops secure mobile applications for enterprise organizations in multiple verticals, including retail, government, and health care, as well as providing security consulting services.
- Mike Ahmadi is currently serving as part of the core security team for the California Office of Health Information Integrity (CalOHII) as part of the Privacy and Security Advisory Board (PSAB)
- Mike Ahmadi is a Certified Information Systems Secruity Professional (CISSP), and is also an active member of the Smart Grid security community, where he leads a NIST Cyber Security Working Group (CSWG) task force, and is a US Expert for the International Electrotechnical Commission (IEC) TC65 working group, where he is currently focused on developing international cyber security standards.

The Growth Of Mobile Computing 2010 Study



Source: http://www.onlinemarketing-trends.com/2011/06/mobile-internet-vs-desktop-internet.html

The Growth Of Mobile Computing 2010 Study



Source: http://www.onlinemarketing-trends.com/2011/06/mobile-internet-vs-desktop-internet.html

Mobile Computing Growth

- Mobile Ramping Faster than Desktop Internet Did and Will Be Bigger Than Most Think – 5 Trends Converging (3G + Social Networking + Video + VoIP + Impressive Mobile Devices)
  Source: Morgan Stanley 2010http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf

- Regarding pace of change, we believe more users will likely connect to the Internet via mobile devices than desktop PCs within 5 years
  Source: Morgan Stanley 2010http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf

- "In three years time, desktops will be irrelevant. In Japan, most research is done today on smart phones, not PCs."
  Google Europe Boss John Herlihy 2010

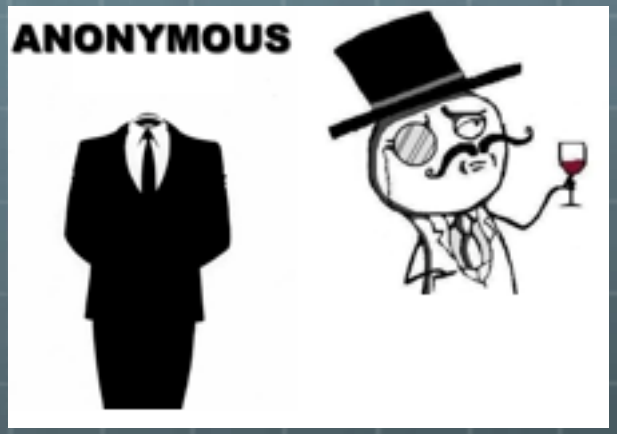
You Probably Don't Need Me To Show You Those Graphs

- How many of you carry a Smartphone today ?
- How many of you use it to check your email?
- Surf the web?
- Perform online banking?
- Access home network?
- Access home company network?
- Use it as your primary computing device?

How Many Of You…

- … password or PIN protect your device?
- … ALWAYS make sure you know EXACTLY where your device is?
- … physically secure your device?
- … understand how data on your mobile device is stored, transmitted, and secured?

The Desktop Computer



- We have completely and thoroughly figured out what it takes to secure the desktop in the last couple of decades, right?
- Mmmmm….not so much
- We are paying a bit more attention due to some unfortunate circumstances

Cybersecurity Discipline Is New and Immature

- We just celebrated 20 years of the internet, which is how most of the world entered the world of computing.
- Transition in workflow from pen and paper to digital was rapid.
- Transition in security from physical cabinets and locks to digital cabinets and locks has not kept up with the pace.
- Most of the world simply cannot wrap their heads around cybersecurity, because it is so new that even experts dare not place a “stake in the ground”

In Comes Something New and Even More Exciting

- Smartphones are ubiquitous, easy to use, and allow us to do nearly everything the desktop does, and lots of cool things our desktops could never do.
- Nearly everyone can afford one, with or without a phone plan (think iPod Touch with free VOIP and WiFi)
- Security is a buzzkill!

From Consumer Device to Enterprise Device

- The Smartphone snuck into the enterprise.
- Sure, it was there in great numbers as Blackberries and such, but those devices were controlled by the organization, with integrated security, and very few applications (comparatively)
- The iPhone and the App Store (specifically) dramatically changed the landscape
- Devices entered the corporate world as personal consumer devices, and enterprise was forced to learn to cope.

So How Is That Working Out?

- Enterprises no longer have any control of the device entering the network.
- Users can download applications to connect to the corporate network in the same way they do with their corporate managed devices (e.g. Logmein, Citrix, VNC)
- Web applications initially built for the desktop now have mobile counterparts which are just as powerful, and often considerably less secure.

Example 1

- Doctor can log in to Electronic Health Record (EHR) online.
- Website requires a username (email address) and password
- Smartphone application exists to allow equivalent access (using username and password)
- Doctor leaves smartphone in car when out to dinner, and it is stolen
- Perpetrator opens application to log into health records, but does not have a password. Email address is easy to find by simply opening the email app on the smart phone.
- Perpetrator goes to desktop website and clicks on “Forgot My Password”
- Password is either emailed to Doctor, or a password reset is sent.
- Perpetrator waits for the Smartphone to “ding” when the email arrives, and resets the password, or uses the one provided.
- Perpetrator has access to records.
- Health care organization faces potential millions of dollars in fines, and patient information is exposed.

Example 2

- Doctor can log in to Electronic Health Record (EHR) online.
- Website requires a username (email address) and password
- Smartphone application exists to allow equivalent access (using username and password)
- Application caches patient information on Smartphone either unencrypted (by the way, encryption is NOT required under HIPAA HITECH laws), or in a weakly encrypted database.
- Doctor leaves smartphone in car when out to dinner, and it is stolen. Phone is not PIN protected (how many of you PIN protect your phone?)
- Perpetrator connects device to desktop and browses to database, and copies information OR
- Perpetrator simply dumps all data to desktop for later perusal.
- Perpetrator has access to records.
- Health care organization faces potential millions of dollars in fines, and patient information is exposed.

What If The Doctor Does Not Know Device Has Been Accessed?

- In the previous examples, the device is stolen. A wise doctor should know to report this immediately, and change all passwords, and close all accounts.
- Even if he does know this, will he do it, and how quickly?
- If the device is accessed long enough for the attacker to dump the information, and he can return it before the doctor knows it is missing, the attacker can mount an attack that could allow him to access data for months, and even years.

Why Is This More Likely With Mobile Devices?

- Desktop workstations are generally physically protected within a known environment, with a gauntlet to go through to get to them (ostensibly).
- Mobile devices can be anywhere and at any time, and the environment is completely unknown, and can range from risky (at best) to extremely hostile.
- Desktop computers are often password protected (at a minimum) in enterprise environments (even if personally owned). Personally owned mobile devices are rarely protected.
- Many users of mobile devices do not fully grasp the fact that their Smartphone is more powerful than the desktop computer the used less than 5 years ago.
- "The Boss" in many organizations does not want IT telling him what to do with his own device.

Enterprise Not Prepared To Address Issues

- " We are having a difficult enough time getting our health care professionals to work with the security we have to implement on workstations. Trying to force them to use their own devices securely is a challenge we are not prepared to address."
  -Security Professional in a Large Health Care Organization
- Younger generation entering workforce have grown up with mobile devices practically welded to their hands. Banning such devices is not an option, especially since many of them are not in charge.
- Desktop design and configuration change is relatively flat, and easier to address (although still a huge problem from a security perspective). Mobile devices are changing rapidly, and functionality is growing exponentially.

Other Challenges

- Regulatory environment is currently not addressing the issues adequately.
- Enterprise is not overly concerned with the security issue with mobile devices because, so far, the exploits are limited.
- Application developers focus on functionality and features. Contract work does not pay extra for security features.
- Device developers do not focus on security because it is not an interesting feature to the largest market sector, which is the consumer.
- Consumers assume that mobile devices are as secure as desktop devices (which are not that secure anyway), or simply do not care.

What Can We Do?

- End users need to understand that mobile devices are portable workstations, and subject to all security issues that would be associated with toting a workstation around everywhere they go.
- Enterprise organizations have to understand that when planning applications deployments and system configurations that mobile devices may be the preferred way for users to access them.
- Mobile application developers need to develop secure applications, and organizations that employ mobile application developers must require that they develop secure applications (and can prove it).
- Regulatory agencies have to understand that they must give this special attention, due to the explosive growth and lack of attention being given to security today. Device manufacturers and application developers must be held to security standards.
- This is all especially challenging because we still have not fully embraced the need to secure legacy environments, despite plenty of empirical evidence.

Mike Ahmadi
GraniteKey LLC

- Phone: 925-413-4365
- Email: mike.ahmadi@granitekey.com
- Twitter: @GraniteKey
- LinkedIN: http://www.linkedin.com/in/mikeahmadi