ISSA CHATTANOOGA

I bet your enterprise data is not near as secure as even you think it is…

Do you want to bet your bottom line on it?

Who is here today?

- *C- level personnel*
- *IA-IS personnel*
- *CISSP's*
- *Legal staff*
- *Sales (Vendors)*
- *Program Developers*
- *Marketing Staff*

BYOD

- *How many have a true BYOD policy?*
- *How many are happy with your BYOD?*
- *How many have MDM for your BYOD?*
- *How many have legal teams where you have BYOD?*
- *How many have Malware protection running on all BYO-Devices?*
- *How many have your MDM managed in the cloud?*

Still Confident?

- *By 2020 there will be 20 billion endpoints on the internet.*
- *By 2050 there will be 1 trillion.*
- *Soon your car will automatically take you to Mapco on the way home because your refrigerator told your car it needs milk.*
- *Currently there are over 3800 versions of just Android in use…is your MDM up to that?*
- *17 million mobile devices are lost in taxi’s alone in any one year.*

Not so sure now?

- *How long does it take to remove a SIM card?*
- *How long to remove an SD memory card?*
- *If you have only looked away from your mobile device for even three minutes…is it still secure?*
- *How about Sidetracking?*
- *Has your SIM been in your possession constantly? Are you sure?*
- *Is your Bluetooth on? Examples…1, 2, 3*
- *Has your data been captured while you had legitimate use of it?*
- *Has someone from your company decommissioned an old BYOD without clearing data properly?*

Can you be sure…

- *Users of your data have not:*
  - *Printed your data*
  - *Forwarded your data, email, drop box*
  - *Posted your data, Facebook, twitter*
  - *Made screen shots of your data*
  - *Saved it to a SD card, USB drive*
  - *Allowed someone else to remove it on a SIM or SD*
  - *Synced their Mobile device to their home computer*
- *So have you lost control???   YES*

53% of employees bring their own technology to work

Source: Forrester's Forrsights Workforce Employee Survey, Q4 2011

60% of organizations have employees who move confidential data to Dropbox without permission, either “frequently” or “very frequently”

Source: 2012 Confidential Documents at Risk Study, Ponemon Institute, July 2012

MDM

- *Provides a platform for you to manage all mobile devices attaching to your network.*
- *Our goal is to manage data not devices*
- *To manage data we have to be device agnostic*
- *To maintain control you have to consider every device as dirty … every time.*
- *Vendors offer the ability to see every item on every device. Files, contacts, pictures, media. Really??*

More on MDM

- *Most are proud of their ability to manage from the cloud.*
- *Is that dynamic or static?*
- *You pay more for static.*
- *What if the cloud loses data?*
- *Is there the potential to force a breach?*
- *What if another company forces a breach of your data?*

Reality Check

You must maintain complete control of your data from creation to destruction. DoJ

You can delegate tasks and duties but never responsibility. DoD

No responsible party has ever reported any problems with any cyber attack, all they need is time and money. Gartner

Anything on the end of an IP address is vulnerable. Lockheed

Legal Issues

- Can you produce all your data in discovery?
- Will your operations violate hold orders?
- Can you be sure where your data is stored?
- Is it compliant? Location, encryption, controlled
- How much data is mobile adding to your Data store? Backup, production, control
- How much more does your legal staff now need to defend? Company and personal data
- None of this has yet been tested in a court room. hmmmmm

Legal Cont.

- ***EU legal system is “Civil Law”***
- ***US Legal System is “Common Law”***
- ***OPT- In, not OPT-Out.***
- ***Initial statue morphs over time and decisions.***
- ***Compliance law morphs as well.***
- ***Decisions can change previous decisions all the way until the US Supreme court rules…***
- ***Lets review some terms from federal courts.***

United States v. Long *05-5002/MC*

- *This is an example for us all.*
- *Long was convicted on drug charges*
- *Based on emails from her account found in a targeted search, of her mailbox.*
- *While searching the mailbox they stumbled on what became the only evidence of a crime.*
- *She appealed under expectation of privacy.*
- *What can we learn from the ruling in this case?*

US v. Long background

- Long was an active duty Marine
- Company was the US government.
- Marines relied on a splash screen disclaimer
- The management went looking for problems.
- Stumbled on private unrelated emails they used for evidence.
- Claimed a right to monitor
- Prosecuted on basis of email evidence.

US Federal Appeals Court Decision

- *Defendant DID have a reasonable expectation of privacy:*
- *Despite the logon banner which said otherwise.*
- *Because the email sits behind a password only she knows.*
- *Regardless of what was in the emails, or on the PC.*
- *Court gave the HS Locker example*
- *"EOP depends on the facts and circumstances at the time" *****
- *"EOP is equal to that which "<u>society is willing to accept as reasonable" ****</u>*

Court Findings

- *The process used for email discovery was not an appropriate, hands off, keyword discovery.*
- *Entered the mailbox and looked through it all, just like looking through snail mail.*
- *Was not the normal maintenance process. Policy by Practice*
- *Maintenance did not review individual email items.*
- *These emails were garnered for Law-enforcement without warrant. This made the office staff deputized agents.*
- *Remember this is the government – not private business.*
- *Emails used for prosecution were obtained improperly.*
- *This left the case now with constitutionally inadmissible evidence.*
- *Because of the bad evidence, the drug conviction was also overturned*

So where are we?

It's also true that those who would give up privacy for security are likely to end up with neither.

There is no security without privacy.

And liberty requires both security and privacy.

Ben Franklin

Privacy??

- ~~*Video Clips – Thought Process Scenarios*~~
- *Quick Examples:*
- *Equipment used for unintended purposes*
- *Search warrant already in progress?*
- *You have no control on data stored on you even if wrong.*
- *What we do now will determine IF we have ANY privacy in our futures* *Big Brother Big Business CNBC 2006*

One of the fundamental issues is that security is tangible; privacy a little tougher to define. "Privacy isn't articulated well," Dennedy says. "I think some people focus on the traditional definitions of the right to be left alone, or they look at it as the Europeans do, as a human right." *McAfee CPO Michelle Dennedy 12/5/12*

Hacktivists recently launched DDoS attacks that caused online outages at several major U.S. banks. Each institution was warned in advance; none were able to prevent disruptions.

healthcareinfosecurity.com 12.5.12

Call it a hacking-as-a-service (HaaS): a group renting network server access for a variety of Fortune 500 companies, including Cisco Systems, is taking advantage of weak passwords to offer logins for cheap. Despite its discovery three weeks ago, the service still appears to be going strong, at last count renting access to nearly 17,000 computers worldwide.

- *InfoSecurity 11/15/12*

As the holiday shopping season rolls around, online privacy and protection face fresh challenges as US consumers plan to use their work-related devices to shop online – a lot. On average, consumers expect to spend nine to 12 hours doing so, opening up a big security hole for companies.

- InfoSecurity ***11/14/12***

Whether it's accessing a SaaS application from your desktop, or a consumer cloud storage provider from your smartphone, the goal, and the challenge, is the same: get my users access to the data they need, and keep everyone else out. Everything else is window dressing.

We can't afford to make the mistake of focusing on one element at the cost of the others. Devices, services, mobility – are simply the details; the real challenge is keeping data available and secure.

- Geoff Web 11/16/12

88% of users believe their mobile devices are at least relatively secure; but 77% of IT managers see the risk of malware spreading to the corporate network from mobile devices as moderate to very high. The result, caught in the cross-fire of desire from the users, and fear of security for the business, is often a policy that is both insecure and inefficient

- InfoSecurity 11/13/12

Our security experts at SophosLabs have seen Android malware grow by more than 4,000% in the past year. It's a fact—smartphones are no longer safe from threats. *11/30/12*

- ***Review Recent Articles by Title***

TAKE NOTE

"The line between what is unethical and what is illegal is sometimes blurry and unpredictable. If a company seeks to scrape by doing the minimum the law requires, the odds are fairly high that it will fail in this goal. Those who aim for the bottom tend to miss their low target and eventually break the law." *(Murphy, Joseph E., Joshua H. Leet, and Joseph E. Murphy. Building a Career in Compliance and Ethics)*

How Do We Survive

- Privacy rule…how would you react if someone imposed your rules on you?
- Are we trying to legislate morality?
- Are we regulating & restricting productivity?
- Are we ready for the legal ramifications?
- Are our staff fully trained to be investigators?
- Do we want to manage and defend more than we have too?

Court - Lessons

- *Improper searching for discoverable data could put you in court to defend your processes.*
- *Don’t let Law enforcement convince you to act on their behalf without the protection of being a deputized agent.*
- *Know the law…all of it.*
- *Make sure your policies are defendable.*
- *Make sure your policy is written … not practice.*
- *Focus on your need to protect your data, not devices.*

Reviewing Needs…

- *So if our data is:*
- *Accessible by any device*
- *On the end of an IP address*
- *Stored where any site is hack-able*
- *Held to a zero error security standard*
- *Accessed by devices we don’t control*
- *To be under our constant control…*
- *Then…*

Securing the Future?

- *Education will need to lead in developing new technology for the following issues:*
  - *A new secure protocol that will leave a users logical DNA on every transaction. (no TCP/IP)*
  - *Michael Caloyannides, DNA wont free anyone now.*
  - *FLETC training agent how not to destroy evidence.*
  - *Protect privacy and internet as securely as we currently protect snail mail and wiretapping.*
  - *Prosecute on the logical DNA*
  - *What about those cases lost in the system forever?*
  - *GPS for data compliance*

Securing the data

- *Treat all devices as dirty…everytime.*
- *Allow view only access to our data from outside our internal network*
- *Overwrite all memory used when connection dropped*
- *Do not manage devices – control data.*
- *Ensure no loss of control on any access option.*

Securing the bottom line

- *No data left on mobile devices*
- *No critical data on the end of an IP address*
- *NEW protocols needed for secure internet.*
- *Digital DNA*
- *Aggressive prosecution*
- *Insist on non – repudiation*
- *Be over protective when needed.*
- *Once data is out there it will not come back!*

Work Groups anyone??

Anyone??

Gordon Merrill, MSIA, CISSP

Merrill.IA@gmail.com

423-280-2892

For more on this subject refer to my articles @

http://resources.infosecskills.com/perception/are-you-in-control-of-your-data-or-is-your-bring-your-own-device-byod-policy-controlling-you/