Interested in learning more about security?

SANS Institute InfoSec Reading Room

Legal Issues within Corporate "Bring Your Own Device" Programs

As our work becomes less and less dependent on a physical brick and mortar corporate office tethered to an Ethernet cable, the tools with which we access our workspace and corporate data are also evolving rapidly. Devices that workers use at home are now being demanded as workspace tools as well due to the convenience and rapid ascension of products such as iPads, iPhones, and Android devices. While technology has provided for this paradigm shift, it has also brought to the forefront a host of legal issues. Corporate d...

Legal Issues within Corporate "Bring Your Own Device" Programs

GIAC (GLEG) Gold Certification

Author: Robert J. Mavretich, bmav@rocketmail.com

Advisor: Rob VandenBrink

Accepted: May 15th, 2012

Abstract

As our work becomes less and less dependent on a physical brick and mortar corporate office tethered to an Ethernet cable, the tools with which we access our workspace and corporate data are also evolving rapidly. Devices that workers use at home are now being demanded as workspace tools as well due to the convenience and rapid ascension of products such as iPads, iPhones, and Android devices. While technology has provided for this paradigm shift, it has also brought to the forefront a host of legal issues. Corporate data is now available on very personal devices. Considerations such as maintaining and storing corporate data, secure destruction of that data, as well as breach notification and legal hold need guidelines on how to proceed. How do you account for an evolving legal environment that assumes export of your data (corporate AND customer) outside the corporate network borders and protection? We will examine potential ways in which a company can provide what workers demand in “Bring Your Own Device” programs (BYOD) to increase productivity, as well as mitigating the inherent legal risks that these programs introduce.

1. Introduction

As corporate finance departments look for ways to decrease costs, their eyes and pencils invariably wander to the Information Technology department. Information Technology has long been considered an overhead expense – a cost of doing business rather than a true revenue generator. The financial crisis of 2008 forced a major re-consideration of the role of Information Technology as a revenue generator. As social media has risen in the public space, the corporate arena has taken notice and seemingly overnight opened its previously guarded network borders to monetize the Facebook and Twitter phenomenon. “Gen Y is constantly pushing for companies to implement new technologies in the workplace, such as online training or benefits enrollment, to make their jobs more efficient. They are even getting their supervisors, who were initially hesitant to adopt these new tools, to see their practical use and everyday value. A widespread adoption in the workplace is important, especially to companies that wish to attract tech-savvy employees” (Townsend, 2011). As such, the personal device has taken the pole position even inside the corporate network borders as the gateway to a continuing and profitable relationship with your customers.

The legacy access model can be defined as follows: Employees use corporate assets (desktop/laptop/Blackberry) for business purposes. Employees were *potentially* allowed (but not encouraged) to use non-corporate assets (webmail is a common tool that is exposed to non-corporate employee assets such as home PCs) to access business and/or customer information. The current bleeding edge access model seeks to *explicitly* utilize personal assets (desktop, laptop, iPad/iPhone/Android) to access business and/or customer information such as customer records, financial projections, marketing material, and a multitude of other non-public, potentially confidential/restricted information. Gartner predicted that by 2012, 30% of knowledge workers in the United States and Europe will access corporate data from a personal mobile device at least one time per week (Hiner, 2008). That prediction has come true, and the unofficial numbers keep trending even higher.

While the pool of legal precedence is relatively shallow, it is also fast evolving. There have been cases of note that encapsulate this phenomenon and provided rulings within this rapidly changing space. Cases such as Quon vs. Arch, and the Microsoft anti-

trust cases of the early 90's involving historical e-mail trails (Wright, 2010) can show how companies can utilize good policy and standards, historical record keeping, and technology vendors, in order to show good faith efforts that will help defend the organization in a legal proceeding regarding the protection of data that the company is entrusted with safeguarding.

In this paper we will review a number of legal concerns within corporate Bring Your Own Device (BYOD) programs, and tools a company can use to mitigate the risk. Utilizing current technology and good policy to reduce the risk scope (and therefore the potential legal implications) will allow you to decide whether or not to allow your user population to leverage their own assets for the benefit of the company based on the residual risk.

2. BYOD Demand – How We Got Here

While to the common user, it may seem that Bring Your Own Device (BYOD) is a relatively new technology trend, Information Technology professionals didn’t have a hard time seeing this paradigm shift coming. What IT professionals have a hard time with is figuring out how to secure the barrage of new devices and do it within corporate budgets. “The N-gen is entering a world of highly customized products and services which will be shaped by them, not just as a market but as individuals. This is causing changes in learning and the relationship between working, learning and daily life as a consumer. Daily life for N-Geners will increasingly include diffusing their knowledge and personal information into products-everything from bread to in-line skates” (Tapscott, 1998). When is the last time you bothered trying to remember a new phone number? It’s likely been quite a while, mainly because you have access to a productivity suite such as Lotus Notes, Outlook, Gmail, Yahoo Mail, all of which will be happy to add users and track information about them including phone numbers, birthdays, and much more.

In the latter part of the last century companies released a flood of cash thrown in the direction of client-side technology. The paradigm shifted as the internet was birthed as a consumer platform. Instead of corporate mainframes having all the computing power and information centralized, the computing power (for a start) was de-centralized due to the constant evolution foreseen within Moore’s law (The price of the hardware dropped, expanding consumer access to it). Gordon Moore was the visionary Intel co-founder and engineer who shaped the face of one of the more dominant companies of the 20th century. Moore’s Law states “that the number of transistors on a chip will double approximately every two years. Intel, which has maintained this pace for decades, uses this golden rule as both a guiding principle and a springboard for technological advancement, driving the expansion of functions on a chip at a lower cost per function and lower power per transistor by introducting and using new materials and transistor structures” (Unknown, 2012).

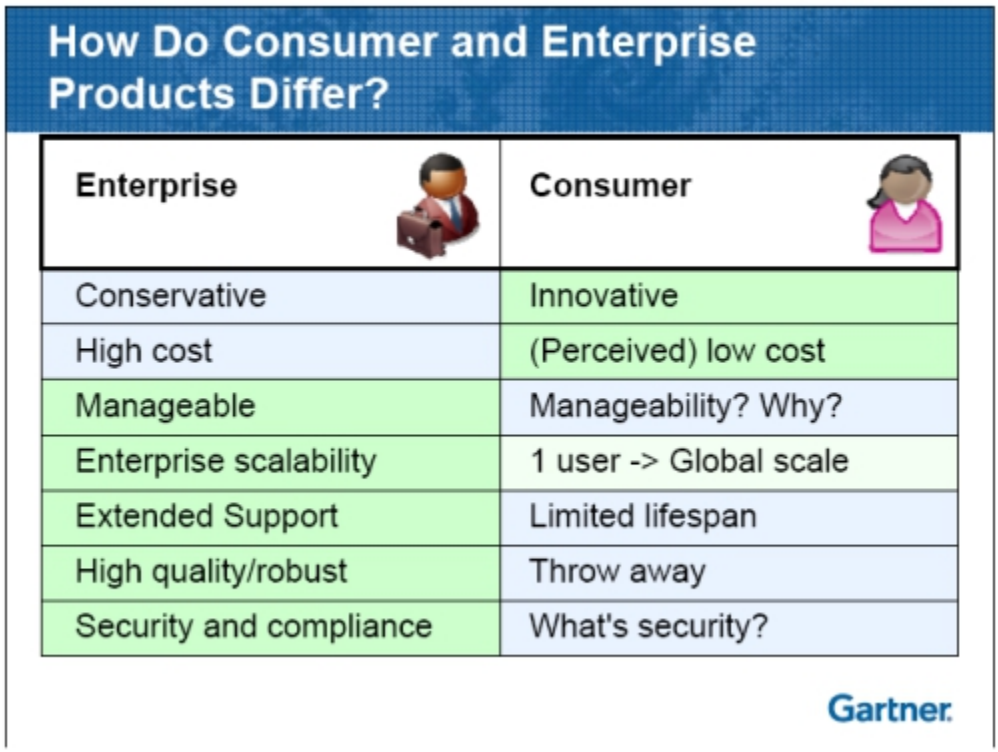
While not too many people have heard (or still haven’t heard, especially if you’re not in Information Technology) Mr. Moore’s bold prediction and watched as it came true over the past four decades, they are no doubt carrying out the mandate in their own

personal way on a daily basis. They are continuing to consume information and realize efficiency gains in their lives through devices that run on semi-conductors produced by Intel and its ilk. The service-based economy that America has become after years of outsourcing industries such as manufacturing and back-end processing, was (in theory) freeing us up to effectively do more with less. “The evidence of Moore’s Law is everywhere, embedded in devices millions of people use every day, such as personal computers and laptops, mobile phones, and common household appliances and consumer electronics—as well as inspiring, important technological innovations in automobiles, life-saving medical devices, and spacecrafts” (Unknown, 2012). Of note as well, is that “advances in process technology and reductions in cost make computing devices accessible to an ever-increasing number of people worldwide, empowering innovations across the computing continuum—from the smallest handheld devices to the largest cloud-based servers” (Unknown, 2012).

So we arrived at this point due to natural selection within the technology space; the best and constantly evolving tools often win. It was only a matter of time before the workers in a company said they were tired of waiting for tools from the company’s internal IT department to serve their customers effectively. “The company’s mantra is speed, with heavy reliance on electronic communication. The first thing it does is break down the hierarchy of the company so that you don’t have massive layers. It improves communications” (Tapscott, 1998). However, with the advent of products such as smart phones, tablets, Facebook and Twitter and other varied Web 2.0 frameworks that started to become communication platforms unto themselves, (crowding out basic and effective tools such as email) corporate America’s boardrooms finally stood up and took notice. You have to be where your customers are! Otherwise, you have no customers and very quickly no revenue! Sales and Marketing roared across the world’s companies at the projected revenue streams. Finance rejoiced at the cost savings in overhead for the company. Information Technology support departments became the proverbial “deer in the headlights.”

2.1. Considering the Legal Risks of BYOD programs

When you are considering whether or not to allow your employees to use their personal devices, it is helpful to understand their point of view. The graph below is very instructive as to how technology products are viewed.



How Do Consumer and Enterprise Products Differ?

Enterprise	Consumer
Conservative	Innovative
High cost	(Perceived) low cost
Manageable	Manageability? Why?
Enterprise scalability	1 user -> Global scale
Extended Support	Limited lifespan
High quality/robust	Throw away
Security and compliance	What's security?

Gartner

Credit: Gartner (Monica Basso and Nick Jones)

Robert J. Mavretich, bmav@rocketmail.com

One of the best risk mitigations you can have from a legal standpoint, promulgated by Ben Wright in his SANS GLEG 523 course, is the concept of "consent." If I tell you specific things that I would like to do with your information, and you agree to those parameters and are willing to sign a document or accept by clicking, you have agreed to allow me to do these things. If you are a corporation, how can you provide consent on behalf of your customers to deliver their information to other devices outside your corporate control? If customers have information out in the public domain (a public Facebook page for example), is that good enough as "implied consent" for you to use any information that you choose, in any way that you choose? Corporations are interested in specific information about you so that they can market products specific to your preferences, at just the right time. This does bring into focus your right to privacy as a consumer and citizen. "We need to support governments in both the E.U. and the U.S. to protect online privacy through 'do not track' legislation; force companies like Google to be more transparent with their use of our data and even enshrine, as the EU Justice Commissioner Viviane Reding is bravely championing, a 'law of forgetting' on the Internet" (Keen, 2012).

So how do we rationalize this line of privacy thinking, or "consent-based marketing" with the desire to turn a responsible profit and provide great products and services, with a productive and effective (read: happy) workforce? "According to a recent report produced by Millennial, today's younger generation will bring change to the workplace by continuing to shake up how we communicate, consume media, browse the Web and make products. To succeed, organizations will need to find new ways to empower the Gen Y employees (born mid 1970's to early 2000s) and unlock their creativity as they continue to advocate change" (Tapscott, 1998).

Similarly, "the content and curriculum in our college systems are rapidly changing, and students are learning the latest technology, which they'll apply in their future careers. This concept is especially important to technology companies, which need to stay current with new trends and applications. On the other hand, the older generation is integral to the flow of daily business projects because nothing can replace its wisdom and experience – especially the value that experience brings to mentoring younger generations in the workplace. Organizations need to successfully harness these differing thought processes so employees can collaborate and learn from each other, making the workplace more productive and successful" (Townsend, 2011).

Because of the different ways and speeds at which the up and coming generations will creatively disrupt the landscape of work and blur the lines between personal and professional, Information Technology as a whole professional has been forced into a fast

forward motion that is rarely conducive to corporate budgets, or privacy and legal concerns. While technology may move at the speed of light, business accounting and revenue collection does not. Privacy and any legal implications many times become an afterthought instead of being “baked-in” early in the conception process of a new idea. “Build it and they will come” within the Legal privacy space has been supplanted by “build it and we’ll fix it in release 2.0 unless you acknowledge that we can share your information for our financial gain.”

“Many N-Geners will also have additional mobility as they acquire knowledge and the capacity for hyper-speed lifelong learning – critical to innovation and creating wealth… There is no reason firms can’t create a new kind of contract between employers and themselves. Whether part-time, mobile, teleworking, contingent, contract, or all of the above, relationships can be forged which are based on clear expectations, mutual support and trust, commitment, and community. The ball is in management’s court on this one, and if there isn’t change there will be trouble” (Tapscott, 1998).

In response to the generational wave of continuing change, a few of the high level legal risks that will be considered in this paper are as follows: (1) Maintaining and storing corporate data on personal devices, (2) Incident Response/Breach notification (3) Secure destruction of corporate data, and (4) E-Discovery/Legal Hold.

Maintaining and Storing Data

In most situations, companies have the "keys to the kingdom" locked away in their borders. While a similar paradigm to the mainframe concept, customer expectations were that "ACME Company" had their data, and that it was required to have that data to perform a service for that customer. Now those companies are deciding to allow personal devices to access the corporate network and take that data outside, whether through an iPad or smart phone, both of which have considerable amounts of processing power and the ability to connect to public and private AP's (access points). It is very hard to maintain the confidentiality and integrity of your data if you are working on a public access point that may have nefarious folks watching or copying your data packets as they flow through the AP. Even private access points are susceptible to eavesdropping and inadequate configuration (WEP anyone?), especially a home access point that likely doesn't get firmware updates at all.

Another one of the overlooked possibilities of corporate data leakage is the storage card on some personal smart phones. These have increased exponentially in the past few years in available size and ability to hold important data in the forms of presentations, or marketing material which used to be too big for early storage disk capabilities. While some individuals take advantage of encryption capabilities that can be used to protect the contents of the storage card, most users are oblivious to its very existence, let alone the need to protect the contents.

As we have seen in the news, companies have had some bad press when a corporate laptop goes missing with Social Security numbers on the hard disk and disk encryption was not installed (or even available as an option) to appropriately safeguard what is non-public information. One painful example that the Info Security community is familiar with is the incident whereby a VA hospital employee lost a laptop with personal data records of veterans on it. In this case the employee was still working to the benefit of his employer and on a corporate device. Consideration needs to be given to the situation when an employee leaves a company after accumulating a significant amount of that company's data on a personal device. The ability of corporate data on personal devices to end up in the service of a competitor is astoundingly easy when allowing personal devices inside the corporate borders.

Potential Solutions for Maintaining and Storing Data

For accessing corporate networks, companies should require their employees to utilize a VPN client. VPN clients are available in corporate editions as well as open source. Creating a secure communication tunnel to the back end server from your device will help shield your transactions from those looking to intercept your data flow. Companies might consider packaging and distributing a VPN client to those employees requiring access on their personal devices, or take advantage of the many open source versions available. This would ensure the data is maintaining the critical components of confidentiality and integrity while in transit.

Although many companies have resisted full disk encryption in the past, it is gaining traction thanks to a number of high profile breaches, a large number of which can be found in the Verizon Breach Status report found here: http://www.verizonbusiness.com/about/events/2012dbir/. All too common in the news are the physical security incidents (laptops stolen from cars is a popular low hanging fruit data breach method). With full disk encryption enabled, you have rendered the data on the physical asset useless (unless the perpetrator has access to an impressive stable of technology and lots of free time on their hands) and virtually eliminate the need to notify customers that their personal data was stolen and at risk. Vendors such as PGP, and for personal use, GnuPG are available for this purpose. Admittedly, there are few options on the market at present to address encryption on phones and tablets in a manner as mature as laptops and desktops. This should change rapidly in the coming months as BYOD skyrockets and companies desire to protect their corporate data on employee-managed devices.

Although these are all great ways to show in a legal proceeding that you are doing what you can to protect your customer's data, none of them will be effective unless you have clear policies and procedures to require their use especially on a device that the end user is responsible for. A good example might be to direct employees that they will have to connect to the corporate network utilizing the corporately accepted VPN client to handle transactions that are classified as greater than "non-public." This would imply almost all of the time, and is a directive that shall be complied with.

From an HR perspective, there should also be a checkpoint at which the employee is asked to reset the device (or it can be done remotely by most Mobile Device Management providers) or wipe the corporate "sandbox" portion of the corporate data on the personal device. "Sandboxing is a form of software virtualization that lets programs and processes run in its isolated virtual environment. Typically, programs running within the sandbox have limited access to your files and system, and they can make no permanent changes. That means that whatever happens in the sandbox stays in the sandbox" (Geier, 2012). Companies such as GOOD Technologies provide these sandboxing technologies for corporations, and their "secure container places an unbreachable partition between personal and business data to protect email and other programs" (Unknown, 2012). This is very important to consider because if you don't have an ability to effectively have your IT department do it automatically, you are relying on a policy and procedure, which HR should enforce to protect the company. You do not want your hard won data going to a competitor because you failed to account for logical data when collecting the employee's corporately owned physical assets.

If you do allow your employees to bring their personal devices, you should work with Legal to craft a "Terms and Conditions" that each employee is responsible for reading and understanding, and is stored either in the employee's HR file or with a corporate records management system in a very intuitive spot for quick reference should employees need to be reminded that they agreed to those "Terms and Conditions."

"However, in high-security and highly-regulated environments, I think it's not only possible to say 'No' but highly advisable. A few examples: government jobs dealing with classified information, health care environments dealing with patient records, and financial services dealing with sensitive company information" (Hiner, 2008). If you are in these fields, there should be significant funding available for a standard corporate Blackberry device for your employees. The maintenance and storage issues are fewer when you completely control the device and legally speaking they belong to the company.

Breach Response/Notification

One of the biggest issues that companies have is accurately keeping track of their data. Offerings such as Data Loss Prevention (DLP software) have filled this space rapidly to give companies the ability to tag their data so that when it flows across an unauthorized or unrecognized channel, the end user is alerted as well as an administrator with an entry to a log file. This is difficult when the data is explicitly going outside the corporate firewall to a device that may have never accessed the corporate network before. Within a normal corporate setting once a breach is discovered, a breach response plan is put into motion. A large portion of breach response plans focus on the enterprise being directly attacked by an actor (outside or inside) with the desire to download corporate data that they are unauthorized to access. With the rise of BYOD programs, the breach response plan should consider that the data hasn’t been directly attacked and loosed into the wild, but rather “dropped” into the public domain by accident. Regardless of the employee’s unfortunate loss of the device, this should be treated the same as if your borders were compromised.

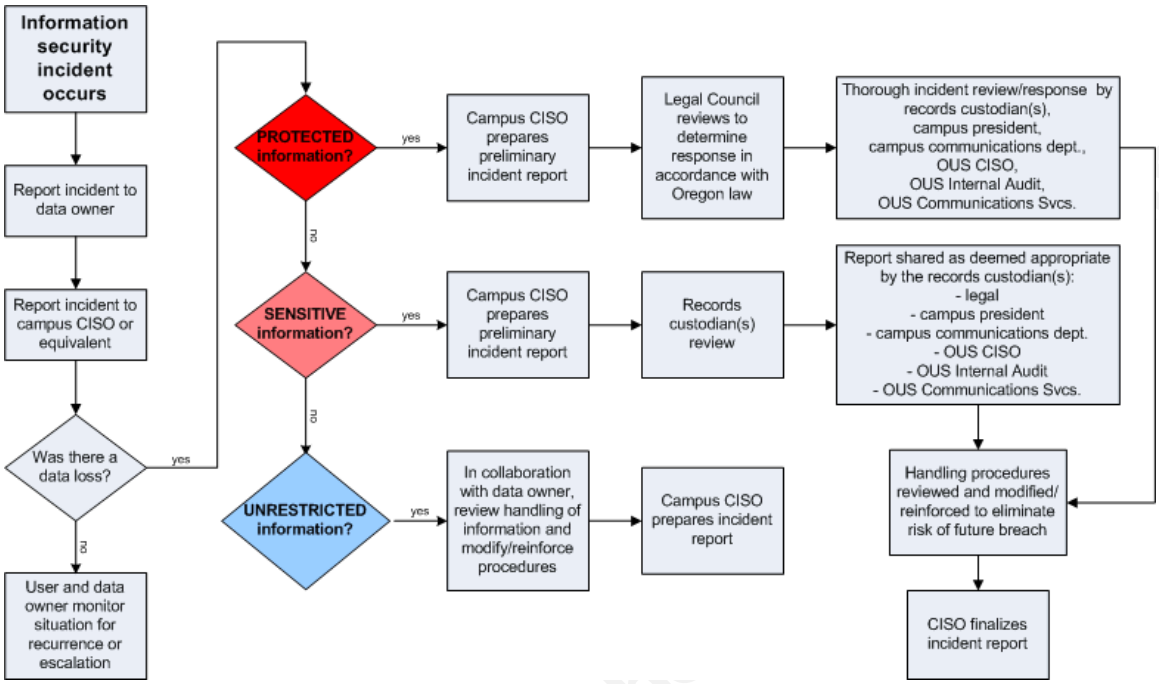
Once you do find that a breach occurs you have to determine if you are under regulatory constraints for notification. For credit card breaches for example, you are required to alert the card brand with twenty-four hours of validation of the breach, and then the affected customers. In situations where you do not have a regulatory responsibility to notify anyone regarding your breach, you have to perform a risk assessment based on what your employee can tell you what was on the device at the time and what your network logs can corroborate.

.

Potential Solutions for Breach Response/Notification

There should be a clear employee responsibility with policy and procedures to immediately contact the help desk to report the incident, and provide a copy of a police report if the loss of the device involved a crime such as theft from a vehicle. It is important that the employee understand that notification of the potential data loss allows the company to ascertain the severity of the situation, giving a bit better idea of how the situation should be responded to. If the device contained projected figures for a large project, it may be deemed "serious" but only damaging if it is discovered by a competitor, and before the end of the month RFP submission. There may be no further steps to take in this situation in the breach response plan. However, if it is a device that the CEO is using, the damage can be "potentially catastrophic" if found by anyone, due to the amount of information on that device pertaining to the financials of the company, takeover targets, and perhaps personal business of normally very private individuals. In this case, the response plan may involve meeting with Legal, Corporate Communications, and the Board of Directors. Breach Response/Notification plans should have a variety of situations that account for these scenarios, and table top exercises that can help stakeholders flesh out further examples and the appropriate responses to them. If you "follow an established process to support your desire to be transparent about what you are doing, courts should act favorable towards you" (Wright, 2010).

It is very helpful for all organizations to have a process flowchart documented that can easily be referenced for any employee to follow easily. The flowchart below offers some insights as to the identification of an incident based on the *classification* of the data; no consideration in this document is given to whether or not the data was on a *corporate* or *personal* device. This is an important point to consider – data has value no matter where it is. If it is your competitive data, you should be very careful on how you handle it and the constraints you put around the transmission of that data to personal devices.



(Credit: http://www.ous.edu/dept/cont-div/fpm/genl-56-350)

Even when you have accounted for the scenario where your data is on personal devices, a process similar to the above chart should be socialized amongst your workforce to encourage them to become advocates for the process in order to protect your data. Many employees are simply embarrassed to admit that they did something that resulted in the loss of corporate data. Some fear retribution and punishment up to and including termination, while others fail to see “what the big deal is” of losing corporate data. Within a corporate setting, you may find out about a potential breach when the employee comes asking for another corporate asset to replace the lost/stolen one. With a personal device, you are relying on them notifying you that something has gone missing. In order to be able to rely on them to do this, the process must be “user-friendly” to encourage participation. Legal may decide to go after the actor who decides to utilize that data on the open market, and shouldn’t punish your employee unless there was gross, pre-meditated misconduct involved.

Robert J. Mavretich, bmav@rocketmail.com

Secure destruction of corporate data

Once the "horse is out of the barn" so to speak, companies must do everything possible to make sure that when the time comes, the data that has made its way onto personal devices (created or stored on behalf of the company) is rendered useless. Most security professionals will debate the number of passes over a fixed disk is necessary to truly "zero" the data out, and some will tell you that short of degaussing the disk drive you are not effectively mitigating the risk of someone piecing together the data on that device's internal storage. The importance of this is cannot be understated in an environment where customers are constantly upgrading to the latest devices. The lifecycle of a consumer device can be found in the inserted graphic on page 8 from Gartner. Common treatment includes: limited lifespan and throw away.

When the newest iPhone is released and purchased by a consumer, what happens to the old device and all the accumulated data? Employees might turn it in to Apple in order to get a rebate on the newest model phone, and although there is a high probability that Apple will perform a factory reset on the phone before re-selling it at a discount, there is no guarantee. This author has witnessed first-hand in the past receiving a replacement OEM hard disk drive for a laptop still containing the image and data of another corporate customer. In the scenario above, what if the employee decides not to return the device to the original equipment manufacturer (OEM) and instead decides to sell the device on eBay? Although not intending to, your employee has just released potentially confidential information into the wild. And without necessarily knowing it, the purchaser of that device has just received information that should not be in the public domain. Relying on the ethics of that person to not use the data on the device that is now legally his or her physical property is very risky.

Possible solutions for secure destruction of corporate data

If it is agreed to allow employees to have corporate data on their personal devices such as smart phones in the above example, there should be clear expectations around the device disposal and data cleansing. Frequently, corporate mandates and processes can help spawn good behaviors even at home, which can help to reinforce a cycle of secure methods when dealing with technology assets. In this way, the employee makes no distinction between corporate and personal devices but “standardizes” their behavior across the spectrum of devices that they use when accessing any information, especially corporate information.

The ability to remotely reset a user’s device can be achieved by the Mobile Device Management toolsets commercially available. Their abilities range widely from deleting the “corporate partition” to a factory reset of the entire device. The importance of user accepted Terms and Conditions should spell this out so the employee is not surprised if through an MDM app you are required to do a complete reset of a user’s device. There are many tools that can be used to effectively zero out a device to factory settings. A large, yet incomplete list can be viewed here: (http://en.wikipedia.org/wiki/List_of_data_erasing_software) but should be considered for personal use cases such as BYOD.

Frequently, an end user will not be interested in purchasing a proprietary COTS product without the financial support (or heavy discounting) of their company. As a company you can either require the end user to utilize these products as a condition of participating in the BYOD program, or at the very least deny them access to your network unless they pass the minimum watermark to include these types of software (which incidentally include encryption options as well in some cases).

E-Discovery/Legal Hold Concerns

“For many enterprises, policy with employees regarding the ability of the

enterprise to get records must be firm and must try to avoid ambiguity. Otherwise, when controversy or investigation arises, the enterprise is exposed to delay and litigation with employees" (Wright, 2012). As Ben Wright states, it is a policy that sets the tone in employee expectations. It is very important to let those who desire to use their personal devices to the benefit of an enterprise be informed of the possibility of that device's contents becoming part of a legal proceeding. "The clause tilts toward the enterprise being transparent with employees about how the policy is being used in practice. But it aims not to give assurances that an employee could use to frustrate the enterprise's attempts to get records when they are needed" (Wright, 2012).

Many employees would be hesitant to agree to the on-demand search and seizure of their personal belongings and the resultant content (even if not germane to the situation at hand) if they even considered it. It is imperative that through the policy that you ***make them consider it.*** There have been instances whereby courts have granted access to personal devices. One example is below, and although in a Canadian jurisdiction, is instructive in showing potential paths for United States law.

"How far will the law go to get the e-mails, text message records that are relevant to a legal inquiry like a lawsuit? An eye-opening Canadian case is CIBC World Markets Inc. v. Genuity Capital Markets, [2005] O.J. No. 614 (S.C.J) (QL). CIBC sued Genuity, alleging it had stolen trade secrets from CIBC. When a lawsuit like this is filed, the parties are expected to apply a litigation hold to ensure no records are destroyed. But a litigation hold is hard to implement if a litigant is not causing copies of all business e-mails to be stored in a central archive. Furthermore, if the litigant is not storing copies of all its employees' messages, then it may be forced to canvass their home computers.

In the CIBC case, the court permitted forensics experts to go to great lengths and expense to locate e-mail. They were granted access to all PCs, BlackBerries (smart mobile phones) and similar devices under the influence of the Genuity's employees, including devices at home (like iPods, iPhones or Androids) and belonging to spouses and children! (In an investigation like this, imagine what goes through the mind of an employee who might have been involved in any kind of marital strife or infidelity.)

The lesson from the case is that enterprises are wise to keep extensive, centrally-managed archives of all business-related e-mail (including webmail, SMS, MMS [multimedia message service], text messages and instant messages) by employees and other personnel. That way they avoid the expense and hassle associated with searches of home computers and other personal gadgets.

This topic grows more important as informal electronic contracting, such as trading in OTC derivatives, attracts greater scrutiny, regulation, litigation and investigations” (Wright, 2010).

Possible Solutions for E-Discovery/Legal Hold

While the aforementioned situation describes a worst case scenario in order to re-claim records that in essence belonged to the company (and even if the employee created those records/intellectual property as an employee or independent contractor which *has* been litigated and ruled as “company property”). Ben Wright’s recommendation is that a company should “allow electronic records to expire as they become obsolete, either because the hardware on which they reside is no longer serving the company, or the format in which the record is stored is no longer supported” (Wright, 2010). It seems that records on personal devices are no longer subject to corporate records rules and processes. If the personal device is used for carrying out corporate business and then the employee leaves within the year, it is certainly not time to expire every record on the device, is it?

One very important thing to consider is that conventional record retention policies are very outdated and assumed all records could be found. “Contrary to the conventional wisdom on corporate records, the digital records within a corporation are growing at such a pace that the records cannot all be located, categorized, or managed. The old idea of classifying records so that they can later be destroyed in accordance with legally-defined destruction periods is impractical” (Wright, 2010).

Solutions such as data loss prevention software can help to determine where the most critical data is, and help to provide technology solutions in order to not allow it to be manipulated by a wide audience, but only by a small authorized subset of folks acting on corporate assets. A company could allow a larger subset of employees “view only access” to limit the amount of critical data that might be only viewed, and not taken outside the corporate borders.

However, even with DLP software, MDM management software, and a host of other technology solutions, the challenge is still going to be human behavior, which can’t reliably be standardized or implemented uniformly across your workforce. This supports the notion that personal devices with corporate content are going to be very hard to compel participation in a legal proceeding if corporations can barely keep up with the data physically residing on their own information assets.

3. Conclusion

Although it is a corporate choice regarding acceptance, avoidance or mitigation of risk, toolsets such as Mobile Device Management, Data Loss Prevention, and encryption tools currently provides the highest level of assurance that corporation are looking for in the marketplace. These vendors have the ability to ensure that the end user device is current with its configuration settings, that data is classified, tagged and “aware” of its movement in and out of your network borders, and rendered useless if it falls into the wrong hands.

While these are not necessarily excuses to go right ahead and throw as much outside the corporate border as you can, it does have the ability to show in a legal setting that you are doing all you are capable of doing in a tough environment. You can show that you are trying to do the absolute best that you can to protect the information your company has entrusted its employees with by giving them clear policy and procedures (terms and conditions), and effective tools.

At the end of the day if you are perceived as doing business with utmost regard for your “honor and reputation” as Ben Wright frequently states, then you stand a better chance of surviving legal proceedings without having to shutter your business or pay excessive fines.

Robert J. Mavretich, bmav@rocketmail.com

4. References

Books

Tapscott, D. (1998). *Growing up digital*. (1st ed. ed.). New York, NY: McGraw-Hill.

Wright, B. (2010). *Fundamentals of IT Security Law and Policy*. (V2010_0220 ed., Vol. 523.1). Baltimore: The SANS Institute.

Wright, B. (2010). *E-Records, E-Discovery, and Business Law.* (V2010_0220 ed., Vol. 523.2). Baltimore: The SANS Institute.

Wright, B. (2010). *Contracting for Data Security and Other Technology*. (V2010_0220 ed., Vol. 523.3). Baltimore: The SANS Institute.

Wright, B. (2010). *The Law of IT compliance: How to conduct investigations*. (V2010_0220 ed., Vol. 523.4). Baltimore: The SANS Institute.

Wright, B. (2010). *Applying Law to Emerging Dangers: Cyber Defense*. (V2010_0220 ed., Vol. 523.5). Baltimore: The SANS Institute.

Magazines

Townsend, J. (2011, April 6). Managing generation gaps in the workplace *Baseline Magazine*, 14.

Jackson, W. (2011, March 14). “Just say yes” to new devices in the enterprise. *Federal Computer Week*, 30.

Web

Warlick, David (2004). Son of citation machine. Retrieved February 17, 2009, from Son of citation machine Web site: **http://www.citationmachine.net**

Hiner, J. (2008, March 10). *Sanity check: Should it support user owned smart phones?* . Retrieved from http://www.techrepublic.com/blog/hiner/sanity-check-should-it-support-user-owned-smartphones/600

Keen , A. (2012, May 30). *Opinion: Facebook threatens to 'zuck up' the human race*. Retrieved from http://www.cnn.com/2012/05/30/tech/keen-technology-facebook-privacy/index.html?

Wright, B. (2012, March 28). *Bring your own device policy - part 1*. Retrieved from http://hack-igations.blogspot.com/2012/03/byod-policy.html

Wright, B. (2012, March 28). *Bring your own device policy - part 2*. Retrieved from http://hack-igations.blogspot.com/2012/04/byod-policy.html

Wright, B. (2012, March 28). *Bring your own device policy - part 3*. Retrieved from http://hack-igations.blogspot.com/2012/04/corporate-policy-liability.html

Wright, B. Discovery in Business Lawsuit? Retrieved from http://legal-beagle.typepad.com/wrights_legal_beagle/litigation-hold/)

Burt, J. (2011, September 5). *BYOD trend pressures corporate networks*. Retrieved from http://www.eweek.com/c/a/Mobile-and-Wireless/BYOD-Trend-Puts-Pressure-on-Corporate-Networks-186705/

Unknown. (2012, 0717). *Moore’s law inspires intel innovation*. Retrieved from http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

Unknown, Breach Notification Flowchart diagram. Retrieved from http://www.ous.edu/dept/cont-div/fpm/genl-56-350

List of Data Wipe Software, multiple sources. Retrieved from http://en.wikipedia.org/wiki/List_of_data_erasing_software

Geier, E. How to Keep Your PC Safe With Sandboxing. Retrieved from http://www.pcworld.com/article/247416/how_to_keep_your_pc_safe_with_sandboxing.html

Unknown. Bring Your Own Device (BYOD) Boost employee productivity and satisfaction – while cutting costs. Retrieved from http://www1.good.com/mobility-management-solutions/bring-your-own-device

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced