40

RIM STRATEGIES FOR BYOD

By Sheila Taylor

Ergo Information Management Consulting www.eimc.ca

1. Introduction

Bring Your Own Device (BYOD) is a strange trend. Most new technology trends go through three general phases: a phase of early adoption in which the visionaries or evangelists seek to prove that the new technology is viable and has the potential to be beneficial. This phase is followed by a rapid adoption phase in which others ‘‘jump on the bandwagon” in order to take advantage of the technology, gain a temporary competitive advantage, and so on. Finally, the technology enters a maturity phase in which late adopters implement the technology, and the technology itself becomes more stable and mature through multiple iterations and revisions.

What has been surprising is that BYOD has not really followed the expected path. While it is not a technology *per se*, it is a trend based on several different technologies and many BYOD proponents and analysts have been expecting it to go through the same standard innovation cycle of other technologies: early adoption, growth, and maturity. In fact, many analysts still attempt to understand BYOD according to this model.

Normally a new technology only really catches on if there is a clear business case and strong drivers causing adopters to embrace it. With BYOD, the business case, while it may exist, is far less clear. At the same time the large scale adoption of BYOD seems almost inevitable, despite the lack of clear benefits and the persistence of a large number of serious disadvantages.

This situation exists primarily because the enterprise (generally represented by the Information Technology or IT department) tends not to be the only decision maker when it comes to using personal devices and technology at work. In this case the end users not only drive demand and influence investment and buying decisions for BYOD, they are often the deciding factor as well. In a normal situation, the enterprise can evaluate a new technology, evaluate the benefits and business case, assess user demand, and plan for implementation if the enterprise determines that the new technology is beneficial. There is certainly a high degree of user demand for BYOD, but this isn't what makes it inevitable. Mainly it is the fact that the enterprise isn't totally in control of whether or not the technology is available to employees. And once the BYOD box has been opened, there is often no closing it.

Many enterprises have embraced BYOD. However, many have not, often for very sound business or technical reasons. Despite the fact that many enterprises would prefer not to offer BYOD to their employees (at least not yet), employees are tending to ignore corporate policies and find ways around any restrictions that their employers have put in place.[1] This puts the enterprise in the position of either allocating resources to prevent unauthorized personal devices, or putting those same resources into investing in and implementing BYOD in a way which maximizes whatever advantages can be had while mitigating the risks and disadvantages as much as possible.

In the following sections, the implications of this strange situation will be explored, providing the background on BYOD (and its variants) in ways which records and information management (RIM) practitioners can integrate into their thinking, and also in specific terms of the RIM implications of BYOD. This information will be useful whether an organization is a champion of BYOD, is submitting to its inevitability and making the best of it, or is still trying to resist it entirely.

2. BYOD Basics

(1) *A Brief History of BYOD*

BYOD, or "Bring Your Own Device," is an IT trend which has been around for several years. It refers to the practice of allowing or encouraging employees to use their own personal phone, laptop, tablet or other device to access enterprise applications or content. The term was first coined in 2009 by Intel, but the practice had been around long before that — perhaps since the first time someone used their laptop or home PC to check their work email back in the 1990's. Intel is generally credited as the first organization to not only recognize but embrace the concept. Therefore, the term BYOD is generally used when it is supported by the enterprise as a matter of policy. It is also often meant to include only mobile devices rather than home PCs, but not all analysts keep to this exclusion.

Traditionally, there has always been a separation between enterprise and consumer (or personal) technology. Before BYOD, the common view IT managers had of consumer devices was a highly negative one. Even a decade ago, it would have been hard to fault them too much for this view. Consumer devices were less reliable, unsecured, unencrypted, hard to track, completely incompatible with back end systems, and so on. Consumer devices like early mobile phones, smartphones, pocket PCs, and laptops came with an incredible number of manufacturers, configurations, customizations, and other variations. The idea of trying to support this tangled mess of consumer devices, while keeping them working, up to date and virus free, gave IT departments nightmares (and still does, to some extent, albeit to a much lesser degree).

Even if devices were not personally owned or allowed for personal use, enterprises had their hands full because of the proliferation of many types of mobile devices which employees were demanding. Instead of the traditional PC and desktop telephone of the 1990's, IT departments were now being required to support employees who might be carrying around a laptop, palmtop, PDA, mobile phone, pager, and perhaps even more specialized devices like mobile point of sale terminals, bar code scanners, GPS trackers, and so on.

For many enterprises, the answer to this proliferation of mobile devices was standardization. The IT department would issue one or two models of PCs, smartphones, PDAs, etc. with a standardized operating system, physical configuration, set of applications, etc. Personal or consumer technology received no consideration at all: if you wanted to carry around personal devices as well you were welcome to as long as you never used them for work.

Things have changed from the streamlined and manageable days of standard issue devices. The proliferation of personal smartphones and tablets has resulted in great demand to use them at work and resulting pressure on IT departments to accommodate this demand. At the same time, consumer devices have come a long way in becoming ‘‘enterprise grade" in terms of security, reliability, and robustness.

For example, the Blackberry used to be viewed as the leading ‘‘enterprise" grade smartphone. It was robust, highly secured and encrypted, operated independently of (then unreliable) cellular networks, and was built to the specifications desired by many IT departments. The Blackberry connected to proprietary, secure back end networks. Other manufacturers, although they wanted to break into the lucrative enterprise market, were unable to break the hold Blackberry held in the business segment. Over the years, however, these enterprise specifications which only Blackberry could satisfy have either been met by consumer devices or have become irrelevant, and from an IT requirements point of view, there ceased to be much of a difference between a Blackberry and an Apple iPhone, for example. Between the pressure of user

demand on one side and the availability of enterprise features on the other, consumer smartphones started making their way into the enterprise.

Similar trends were taking place with other categories, such as laptops/ netbooks or pocket PCs. Other, newer technologies such as tablets never had the enterprise vs. consumer distinction to start with, and were acceptable to many IT departments when they were initially available. Today, there are very few enterprises or government agencies which require ‘‘hardened” devices whose requirements aren’t met adequately well by the same devices anyone can buy off the shelf.

Since the devices themselves were gaining acceptance, this opened the door for those same devices to be personally rather than corporately owned, particularly with the advancement of mobility technology and infrastructure within the enterprise. Accordingly, BYOD has gained greater traction as an IT supported policy. In general, the advantages of BYOD to the enterprise have become greater while the disadvantages have lessened or become increasingly irrelevant.

However, even though consumer devices and the enterprise mobility technology needed to support them has come a long way, they still have some distance to go and the value proposition for BYOD is still far from definitive, as will be seen in coming sections.

(2) *Advantages and Disadvantages to the Enterprise*

The following two sections will examine the main advantages and disadvantages of BYOD, first from the enterprise perspective and secondly from the employee perspective. This enterprise/employee distinction is needed because very few of the advantages or disadvantages for one group apply to the other — in fact quite the opposite, as will be seen in Section 2(4): Finding the Middle Ground:

(a) Advantages

1. *Increased mobility and freedom to work productively offsite and/or during off hours.* This is more properly viewed as an advantage of mobility technology in general, and BYOD is an extension of mobile access to enterprise resources and information which enhances this capability. It is the only result of implementing BYOD which is of clear advantage to both the enterprise and employees (but see section 3(a) Advantages for an important caveat to this).
2. *Capital savings.* Typically, in a BYOD scenario the employee bears some (or all) of the cost of the device, resulting in capital cost savings to the enterprise. Note that this cost savings will be offset by

expected increases in operations cost for support, as discussed below in section 4.

3. *Increased morale among employees.* Given the high user demand for BYOD, it is to be expected that a BYOD policy fulfilling this demand will be met with higher morale. However, it is interesting to note that while BYOD might provide a general boost to morale, it does not at this point seem to be a factor in an organization's efforts in terms of recruiting, at least among new graduates.[2]
4. *Expanded access to mobile enterprise applications.* Because people generally carry personal devices with them at times and places they wouldn't normally carry a work device, allowing access to enterprise applications from personal devices expands the ability to access them. The endgame for any mobile application is ''anytime, anywhere," so anything that enables or encourages this is an advantage.
5. *Drives investment in other mobile technologies.* According to Gartner,[3] companies are expanding investment in supporting technologies in order to support BYOD. In general, these ancillary technologies have benefits that extend beyond just BYOD but can be hard to obtain funding for on their own. For example, BYOD support may drive investment in mobile or network infrastructure, mobile device management, virtual desktop applications, or file sharing/ syncing tools. IT departments may find their efforts to fund these initiatives are buoyed by demand for BYOD.

(b) Disadvantages

1. *Security risks*. This is by far the most serious concern expressed by IT managers when it comes to BYOD. In the 2014 Gartner survey previously cited,[4] 76% of respondents reported security concerns as an issue, with 46% saying it was a large concern. Only 15% claimed security was not a problem, and one generally has to assume the nature of BYOD at those organizations must be quite limited, because any wide ranging BYOD effort creates obvious concerns that any IT manager would have to deal with. The security risks can be broken down into the following categories
    a. *Lost/Stolen Devices*: If a device is lost or stolen it creates the potential for sensitive information to fall into outside hands. Depending on the type of device, this can include confidential or proprietary documents, sensitive emails and voicemails, and other types of records. With enterprise-supplied devices there are generally safeguards in place, such as GPS tracking, high end encryption, secure or multistep authentication, and remote wipe capability. Personal devices without these features should be considered to be a high security risk.

b. *Device misuse*: Enterprise-supplied devices can be monitored for uses which contravene corporate usage policies, or are used for prohibited or illegal activity (piracy, access to banned sites, etc.). It is more controversial for the enterprise to use remote monitoring tools on personal devices, but not doing so can expose the organization to legal risks. Some IT managers also express concern that if users use their devices for non-work purposes while at work (e.g., video streaming, games, etc.), this not only decreases productivity but puts a strain on other network resources that are needed for work purposes.

c. *Malware:* Personal devices are often outside the measures taken to protect the enterprise network from malware, adware, viruses, and so on. If these devices are not as diligently protected it can lead to infections, and if users are allowed to install their own applications, there is no guarantee those applications do not have security flaws or come with their own malware/adware.

d. *Insufficient encryption*: Most devices today, consumer or otherwise, have the capability to encrypt all data stored on the device. However, it is not a given that individual users will be aware of or understand the encryption features of their device, potentially exposing the data to hacking or theft.

2. *Increased support complexity and costs:* Because of the greater potential variety of devices, applications, and configurations used by individual employees, support staff will require a great deal more training, and there may be increased need for specialists and more support tickets that have to be referred to second line support. Also, with more applications and devices comes the potential for more conflicts and interoperability issues. Support issues are a close second to security issues in terms of IT managers' concerns, with 73% reporting it as a concern, and 22% responding that it is a large issue.[5]

3. *Interoperability with back office systems*: One of the biggest challenges in any network environment is ensuring end users can connect with back office systems. These may include databases, directories, transaction systems, billing, reporting, or other specialized applications. These back office environments are in themselves usually quite complex, with a variety of potential hardware, interfaces, protocols, and management software. The additional complexity of now having to ensure these systems are compatible with a more complex end user environment is likely to be a costly and time consuming endeavour.

4. *Increased application rollout complexity and cost:* Not only do end user devices need to be compatible with existing back office systems, they also have to be compatible with new applications. Even

something as simple as an internal website has to be designed to work with devices that have varied screen sizes, memory, and processing capabilities.

5. Legal and privacy issues: Finally, having to accommodate personal devices on the network, or have personal devices which are not on the network be used for work purposes, creates a raft of potential legal issues, particularly when it comes to employee privacy and the confidentiality of personal data. Not only are employees subjecting the personal information on their devices to their employers' scrutiny, they may also be disclosing their location, internet browsing history, personal purchases, and other information that would normally be considered protected. This is not just a disadvantage to the employee, but also to the enterprise which must understand and possibly defend its legal position, risk dissatisfaction from its employees, and take additional steps to protect itself from the legal ramifications.

(3) *Advantages and Disadvantages to the Employee*

(a) Advantages

1. *Increased mobility and freedom to work productively offsite and/or during off hours.* This is the only result of BYOD which provides a clear advantage to both the employee and the enterprise. But even this is not entirely straightforward, since some employees may actually perceive an expectation or otherwise feel pressured to be available and working offsite or during off hours. For those employees this advantage may actually be perceived as a disadvantage that impinges on their work/personal life balance.
2. *Single device for work and personal use*. Although simply eliminating the need to carry around more than one device might not seem like a huge benefit, for most employees this makes the biggest difference in day to day life.
3. *Freedom to choose preferred device(s).* Generally, the latest model of phone, tablet, or other device is available in the consumer market first, meaning employees can obtain devices which are more advanced and fully featured than the devices supplied at work.
4. *Remain connected to social networks, etc. throughout the work day.* Especially for younger employees, it is hard to imagine not being connected to personal social networks throughout the day. Even though most employers would like to discourage this practice (and may even take active measures to do so) it may be difficult or impossible to prevent. For employees in a BYOD environment, easily

monitoring their social networks during work hours is an attractive thing.

(b) Disadvantages

1. *Personal privacy may be compromised.* By combining personal and work activities and information on the same device, the employee must accept the risk that the entire device (including personal information) may be subject to legal discovery or, in government organizations, freedom of information requests.
2. *Risk of personal data loss.* A standard capability which the enterprise will insist upon is the ability to wipe a device in the case of loss or theft. Although this may not adversely affect an employee since the device is no longer in his/her possession, it is possible that wiping could take place by accident or that the device is recovered later. In some cases, it may also be problematic to remove only work data when an employee leaves the organization.
3. *Limited access to applications*. Depending on other corporate policies, some applications and websites may become inaccessible on the device (e.g., Facebook, Twitter, Instagram, Spotify, iTunes, etc.)

(4) *Finding the Middle Ground: The BYOD Balancing Act*

Although it is a matter for some debate, there is a good argument to be made that the disadvantages of BYOD to the enterprise outweigh the advantages. For example, Gartner's 2014 BYOD survey[6] indicated that approximately half of respondents have experienced overall cost savings as a result of implementing BYOD, while the other half have reported exactly the opposite: their BYOD implementation has actually increased overall costs.

But even though IT departments may find BYOD objectionable from a pure business case or logical perspective, it may be that user demand for BYOD is so high that it will override IT's objections. This is particularly true if user demand is also coming strongly from the executive suite, which is often the case.

Therefore, IT may find itself in the unfortunate position of wanting to ban BYOD but being forced into adopting BYOD anyway. In creating BYOD policies, IT naturally tries to maximize advantages to both the enterprise as a whole, as well as individual users, while limiting the disadvantages. What happens, however, is that the more an enterprise advantage is maximized, the more it increases the disadvantages to the employee. Similarly, the more an employee advantage is maximized, the more disadvantageous it becomes to the enterprise.

For example, if the enterprise offers total freedom for employees to choose their preferred device (smartphones, for example), then it has a correspondingly higher number of types of devices it has to manage, all of which may have different security vulnerabilities. This increases the complexity and cost of tech support, and requires a larger knowledge base and skill set from IT support staff. This situation also increases the complexity, cost, and roll out time of introducing any new application, and guarantees more problems in attempting to get so many devices to work smoothly with back end systems and servers.

If the enterprise reacts to these highly significant problems through a compromise which still allows employees to choose their own device, but maybe limits the selection to certain devices or configurations in order to make support costs manageable, it then limits the freedom which employees were demanding in the first place. IT therefore tends to get stuck with trying to find a compromise which gives it a reasonable chance to keep costs under control while still satisfying end users. Walking this kind of tightrope means that it is very easy to create a situation where BYOD satisfies no one's needs and no one is happy. And despite this, as stated earlier, IT may still have no choice to implement and support BYOD.

Figure 1 illustrates this dilemma by listing out the primary effects expected from implementing BYOD and identifying whether it is an advantage ("A") or disadvantage ("D") to both the enterprise and the employee. If the effect on either group is negligible, this is marked as neutral ("N").

As can be seen in Figure 1, there is only one aspect of BYOD which is advantageous to both the enterprise and the employee, and even this aspect has caveats. In all other cases, what is seen as an advantage for one group is either inconsequential or disadvantageous to the other. And the more the advantage of any factor is maximized for one group, the more it tends to increase the disadvantage the other. In many respects BYOD becomes a bit of a zero sum game in which only one side can win, or there must be a compromise which may satisfy neither.

Figure 1: Summary of BYOD Advantages and Disadvantages

EXPECTED OUTCOME OF BYOD	Enterprise	Employee	Notes
Increased Productivity	**A**	**A***	Employees can work more easily and effectively outside office locations and hours. *Although this might be seen as a win-win, some employees might find it interferes with work/life balance,

EXPECTED OUTCOME OF BYOD	Enterprise	Employee	Notes
			especially in unionized environments.
Freedom to Choose Device	**D**	**A**	The greater the number of possible devices, the more complex, difficult, and expensive it is to support them.
Single Device for Personal and Work	**D**	**A**	Combining personal and work information and applications on one device, while convenient for the user, creates many challenges for the enterprise.
Cost Savings	**A or D**	**D**	Employee pays for device, but any enterprise cost savings can be offset by increased support costs.
Security Flaws	**D**	**N**	Security flaws in consumer devices are probably the greatest challenge for IT to overcome in BYOD. These flaws might include insufficient protection from loss/theft, inappropriate use, or malware/virus exposure.
Security Fixes	**A**	**D**	Measures taken by IT to remedy security flaws may be objectionable to end users or cause inconvenience. Examples might include 2-step authentication, enforced virtual private network (VPN) use, or remote wiping.
Privacy	**N**	**D**	Although both private and work information are on the same device it may not be possible to separate

EXPECTED OUTCOME OF BYOD	Enterprise	Employee	Notes
			them for purposes of legal discovery, device monitoring, location monitoring, etc., requiring the employee to give up some privacy rights.
Newer Technology	**D**	**A**	Although employees can purchase the latest model available, the enterprise will always lag behind in being able to test, integrate, and support it within the enterprise environment.
Compatibility with Enterprise Systems	**D**	**D**	Consumer devices may not integrate easily with back end systems, databases, applications, etc. or meet requirements for security, communications, etc. This lack of compatibility, while often temporary, can require significant resources on the part of IT to fix, and inconvenience the end user until any integration and customization work is complete.
Legal Issues	**D**	**D**	All mobile devices potentially contain records which may be required as evidence, including documents, database records, call logs, photos, videos, etc. This can cause issues for both the enterprise and the employee on any mobile device, but more so if the device is a personal one.

The next section will look at how this balancing act between IT and end users has affected the overall adoption of BYOD.

3. The State of BYOD in 2016

(1) *Adoption*

It is surprisingly difficult to determine accurate adoption rates for BYOD. A 2012 survey by Good Technology (a mobile technology firm) reported that 76% of respondents currently supported BYOD, with only 5% having no plans to support it in the future.[7] A 2012 Ovum survey reported that between 50%-60% of IT departments in North America supported BYOD, with percentages being slightly lower in Europe and Asia.[8]

These numbers contrast sharply with a 2014 Gartner report,[9] which show actual adoption between 14% and 19% (depending on the type of device), with projections of approximately 50% by 2017. The percentage rises to 38% if one counts organizations which encourage BYOD but still provide enterprise supplied devices. Interestingly, these numbers are actually lower than a similar survey conducted by Gartner the year before in 2013.[10]

A 2012 report from a survey conducted by Intel shows adoption by U.S. firms to be between 19%-23%, depending on the type of device.[11] Rates were somewhat higher for the other countries included in the survey (Germany, Australia, and South Korea).

Also in contrast with the Good Technology and Ovum reports, Gartner stated that 21% (2014) to 31% (2013) of companies surveyed are actively discouraging BYOD. Unfortunately, discouraging BYOD doesn't mean that it ceases to be an issue or can be ignored because of the continuing rise of ''shadow BYOD."

And finally, a 2015 survey conducted by AIIM reported approximately 30% of respondents had implemented BYOD, a further 30% had plans to implement, and 8% had policies banning BYOD.[12]

See Figure 2 for a summary of the research cited.

Clearly there is no consensus amongst analysts as to the prevalence of BYOD today. One reason for the discrepancies may be due to differences in the sample populations, in terms of geography or industry sector. Also, at least part of the problem in understanding actual adoption rates may be that BYOD covers a large range of possible implementation scenarios. For example, it might be possible that a company that allows access to a single application (like email) through an enterprise web portal or access to a shared drive via an enterprise virtual private network) (VPN) would consider itself to

have supported BYOD since employees could use their personal mobile devices or home PCs to access these resources. The lower adoption rates supported in some reports may not accept such a minor implementation and have more rigorous definitions.

Figure 2: Summary of BYOD Market Adoption Research

Report Author	Notes	Year	Currently Implement BYOD	Plan to Implement BYOD	No Plans or Ban BYOD
Good Technology[13]	40% Finance/ Insurance Sector	2012	76%	13%	5%
Ovum[14]	Commissioned by Logicalis; results are for US respondents	2012	<– 65% →		10%
Forrester[15]	Commissioned by Cisco	2012	<– 44% →		37%
Intel[16]		2012	19%-23%	N/A	N/A
Gartner[17 18]		2013	69%	22%	9%
Gartner[19]		2014	14%-19%	23%-31%	9%-21%
AIIM[20]		2015	30%	30%	8%

Clearly there is no consensus amongst analysts as to the prevalence of BYOD today. One reason for the discrepancies may be due to differences in the sample populations, in terms of geography or industry sector. Also, at least part of the problem in understanding actual adoption rates may be that BYOD covers a large range of possible implementation scenarios. For example, it might be possible that a company that allows access to a single application (like email) through an enterprise web portal or access to a shared drive via an enterprise virtual private network) (VPN) would consider itself to have supported BYOD since employees could use their personal mobile devices or home PCs to access these resources. The lower adoption rates supported in some reports may not accept such a minor implementation and have more rigorous definitions.

For the purposes of this chapter, the more rigorous definition is being applied and adoption rates can probably be considered to be in the 20%-30% range. The likely number of organizations banning BYOD is a bit more consistent at 5%-10%.

It should be noted that this figure only denotes adoption which is supported and encouraged formally by the IT department. Unsanctioned use

of personal devices to access an organization's resources is likely to be far more common. This is sometimes called "Shadow BYOD," which is discussed in the next section.

(2) Shadow BYOD

With relatively low adoption rates today (< 30%) it may be tempting to think that dealing with BYOD issues, either as a RIM or IT manager, is something that can wait. Unfortunately, this is probably not the case. Even though an organization may not have a formal policy regarding BYOD or have invested resources in adopting and managing BYOD, it is entirely likely that employees may not be waiting. In 2011, a Forrester survey of 9,000 end users worldwide reported that 43% of them bring their own devices for work purposes, regardless of their employers' BYOD policies.[21]

For example, one recent study of 20 federal government agencies in the U.S. found over 14,000 personal devices connected to government networks.[22] Approximately 50% of federal employees admitted to using personal devices for work purposes, and approximately 60% have access to work email and documents on their personal devices.

The same study reported that 40% of employees stated that IT policy regarding the personal use of devices had no impact on their behavior or intentions to continue using personal devices.

It may be that organizations which either ignore or prohibit BYOD activity are facing an inevitable outcome. Even an organization that doesn't want to implement BYOD may have no choice in the matter. Sometimes it is a matter of keeping your friends close, but your enemies closer, and the only way to avoid the downsides of BYOD will be to embrace it.

(3) CYOD and COPE

Part of the reason current adoption rates are so hard to pin down is because BYOD has a highly fluid range of definitions. As discussed previously, BYOD is a continuum rather than a black or white choice. Popular variations of the BYOD model have been emerging as compromises between allowing users total freedom of choice and banning BYOD entirely. Two of these emerging trends are CYOD (Choose Your Own Device) and COPE (Corporately Owned, Personally Enabled)

(a) CYOD (Choose Your Own Device)

CYOD (Choose Your Own Device) differs from BYOD in that the end user is permitted to pick from a set list of approved and supported devices and configurations. Usually the devices available would correspond to the most popular ones currently available in the marketplace, although typically the

choices would not immediately include the latest models, since it takes time for IT to test, configure, and debug a new device.

In a typical BYOD scenario, the end user is responsible for acquiring and paying for the device (only 2%-3% of BYOD programs in the U.S. include a full or partial stipend for the device, and only 5%-15% in other parts of the world).[23] With CYOD, the enterprise may or may not cover the cost of the device.

*(b) COPE (***Corporately Owned, Personally Enabled)**

A newer variation which is even more restrictive than CYOD is COPE (Corporately Owned, Personally Enabled). In this scenario, the end user is still able to choose from a list of approved devices. Unlike with BYOD, these devices are supplied and owned by the enterprise, much as traditional mobile devices are supplied. The difference with COPE is that the devices are configured to allow for a higher degree of personal use and customization.

For example, a COPE device would probably include partitioned storage for keeping work and personal information separate, separate accounts or applications for email and other applications, and mechanisms for isolating access to social networking or personal applications from work-related databases, directories, etc. A COPE device would also possibly include enhanced security and encryption, remote monitoring and/or wiping capability, and restricted device administration privileges (to limit the installation of new applications, for example). Many of these restrictions may also exist on BYOD devices, but they tend to be more stringent and restrictive on a COPE device. In general, think of a COPE device as an enterprise device with personalization features, whereas BYOD is a personal device that is usually hardened for the enterprise.

(4) Newer Variants and Extensions

BYOD variants like CYOD and COPE are intended as limited or restrained versions of full BYOD. At the other end of the spectrum, however, the BYOD horizon has been expanding as new technologies have become consumerized and widely adopted. Although originally limited to endpoint devices like mobile phones, smartphones, tablets, and other user devices, the potential for using personal technology has expanded into other areas such as cloud services, networking, public/consumer applications and services, and so on. The three most prominent of these emerging trends are described in the following sections.

(a) BYOA (Bring Your Own Application)

Bring Your Own Application (BYOA) is similar to BYOD, except that it concerns personal applications used for work purposes rather than devices.

These applications generally fall into several categories, as shown below, but BYOA would include any kind of personal application used for work.

Storage and Synchronization: Employees may use cloud storage or syncing applications such as Dropbox, Google Docs, OneDrive, etc. to store work documents.

Communication and Collaboration: Applications such as Skype and GoToMeeting may be used for work-related conversations and messaging. Note that even phone calls can be considered in certain cases to be records, whether it is a call detail record or a recording/transcript of the actual conversation. These records may possibly have evidentiary value and it is the responsibility of the corporation to manage them.

Social: LinkedIn, Facebook and Twitter, if used to discuss organizational details, communicate with customers or suppliers, or otherwise represent the organization can also be considered to fall into the BYOA domain, even if they are personal accounts/ids.

Productivity: Personal office applications from Microsoft, Google, or Apache may be used on mobile or desktop platforms and may expose enterprise documents to outside access.

Bookmarking: Applications and web add-ons for ‘‘read it later” functionality such as Instapaper, Pocket and Evernote, or social bookmarking services such as Delicious, StumbleUpon or Digg may be used by employees doing research, keeping up to date, etc. In some cases, this can be the equivalent of making an employee’s search history public.

In any of these cases, security is highly problematic because users are working outside the application environment provided and controlled by the enterprise. In case of a data breach, there is nothing an IT department can do to protect or wipe data. Add to this the near impossibility of preventing employees from using these applications, and it can create a serious challenge. There are a few ways the problem can be addressed, however. One is to establish acceptable use policies for 3rd party software, which at least communicates the organization’s position.[24]

A more progressive approach taken by some enterprises is to establish an in-house directory of approved applications (apps), or even develop or deploy their own apps to be used instead of the publically available ones.[25] This ‘‘build-your-own” approach can be quite successful. For example, IBM has incorporated enterprise-level social bookmarking into its Lotus Connections product for nearly 10 years. This feature provides social bookmarking similar to Delicious or similar services, but with added functionality and with enterprise ownership and control.

(b) BYOC (Bring Your Own Cloud)

Bring Your Own Cloud (BYOC) is really a subset of BYOA, pertaining only to personal cloud services or a combination of private and public cloud services. It includes both free and paid services, such as Dropbox, Amazon Web Services, Microsoft Skydrive, Google Docs, ownDrive, and so on. There are hundreds of personal cloud vendors available, many of whom offer at least a basic level of service for free.

Many cloud services offer more than just storage. Standard features today include synchronization of stored files across multiple devices, automated cloud backups, file sharing and collaboration, version control, and so on. Many of these services bring associated security risks as discussed in the BYOA section above, and because of newer services such as synchronization, backup and file sharing, a data breach can propagate very quickly.

(c) BYON (Bring Your Own Network)

A third major variant of BYOD is Bring Your Own Network (BYON). After end-point devices and cloud/network based application and storage, the network is the final piece of enterprise infrastructure that has the potential to be bypassed by personal services. BYON usually refers to networks which reach outside the enterprise local area network (LAN), and can apply to both data and voice networks. BYON networks can be of several types:

Mobile Hot Spots: Many locations (airports, hotels, convention centres, coffee shops, shopping malls, etc.) offer WiFi Internet access. Employees using these networks without encryption or VPNs create clear security risks.

Personal Hot Spots: It is possible to tether mobile devices, whether personal or enterprise, to a personal hot spot by using wide area data devices such as a smartphone or tablet. Personal hot spots can also be used to create local peer-to-peer networks. As with mobile hotspots, a personal hotspot may not be secure.

Personal Networks: Many of today's mobile devices support peer-to-peer or personal networking over WiFi or Bluetooth. It can be very easy for users to secure these networks improperly, leaving them open to outside monitoring, keylogging, remote access, or data interception. For example, unless prevented, Bluetooth devices broadcast their address to all other Bluetooth devices within range and services like Apple's AirDrop can be set to transmit to any device it detects. In addition to mobile devices, unsecured home WiFi networks are subject to breaches and intrusions, and are often used for work purposes in the evenings or by telecommuters at any time.

Carrier Networks: Finally, enterprises must consider whether to allow employees to use BYOD devices with their own cellular carriers, or if they

should be forced to switch to the enterprise's provider. In many cases it may be desirable for users to use the enterprise provider, perhaps for financial or administrative reasons, or possibly due to security or other features which might not be identical across multiple carriers.

In many cases, the proper use of a corporate VPN can alleviate most concerns around the use of personal networks, and because VPN technology is so mature, BYON is one of the easier challenges for IT to address as compared with BYOD, BYOA, or BYOC. Naturally VPNs must be properly encrypted and secured (using two-factor authentication or biometrics, for example).

4. RIM CHALLENGES

The preceding sections have provided background and context on BYOD and its variants. Even though BYOD is primarily something which the IT department must resolve, RIM practitioners should be aware of the full range of variants and issues in order to be able to deal with the aspects which affect them and their responsibilities.

RIM practitioners have specific responsibilities when it comes to enterprise records, regardless of format or location. These relate to the information life cycle of record creation, receipt, and capture; distribution and use; storage and retrieval; retention and disposition; and archival preservation, as illustrated in Figure 3.

Each of these phases is affected in some way by an organization's BYOD policy and implementation. In some cases, the issues arise because of BYOD itself. In others, BYOD intensifies or worsens a challenge created by enterprise mobility in general (as opposed to BYOD specifically) because the use of mobile devices and applications has created new types and formats of records which need to be accounted for within the RIM framework, created accessibility or storage problems, made compliance with records policies and procedures harder to monitor, and so on.

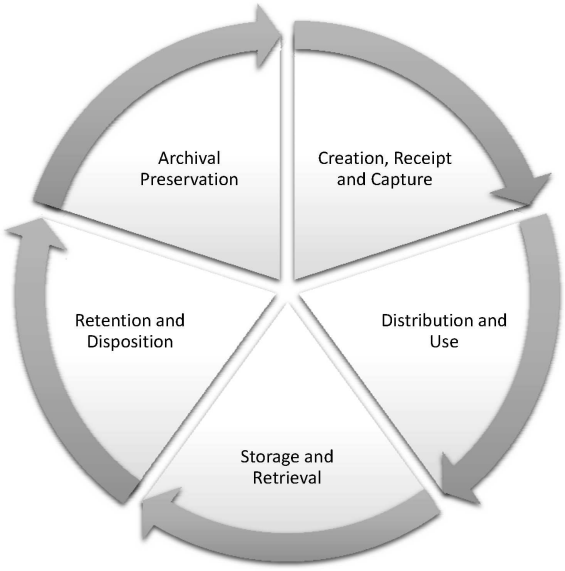
(1) Creation, Receipt and Capture

The beginning of the information life cycle is when information or record is initially created, received, or captured. Record creation means the information is first committed to media, receipt means the information comes into the organization's possession and control, and capture means the information is transferred to a manageable storage media.

At this stage the first responsibility of RIM is to identify whether or not a given piece of data is a record. Not all data generated or encountered by an organization is considered to be a record and, therefore, subject to

management as part of the information life cycle. For example, personal information created by an employee on a personal mobile device should not be considered to be a record. In a BYOD situation, however, it is likely that records and non-records will be stored on the same device, and it may not be possible to separate the two.

Figure 3: Information Life Cycle



A second key issue created by mobile devices, cloud computing, and BYOD is that there are often multiple locations of the same content. For example, an email may be composed on a mobile device. That email may be uploaded to a mail server which retains a copy, and the mobile device may be backed up to the cloud, synced to a desktop PC, or both. At this point in the example there could be at least 4 copies of the same email, and this doesn't even consider the recipient's copies. Which one should be considered to be the official record? BYOD, because of the device ownership and control, makes it problematic to consider the version on the device to be the official record, even though it might be the original version.

In general, there are two main considerations that RIM should take into account with regards to BYOD and record creation:

Is the record complete and authentic? It needs to be possible to verify that information has been captured in its entirety and is authentic, particularly when it may exist in multiple locations and may be subject to frequent alterations,

versions, or updates. For example, if a legal contract exists on an employee's device as well as several different servers, and then one of these copies is amended, how does this affect the record's status?

Where does custody reside? Ideally the information should not reside on a 3rd party device or server. Third party includes the employee's personal device, as well as outside servers where the employee might store the information (such as DropBox, in Google Docs, in a 3rd party webmail application, etc.).

(2) Distribution and Use

It is the responsibility of the RIM function to ensure that, once created, records are distributed to their proper locations and made available for authorized use. The use of BYOD doesn't alter this responsibility, except that it can make it harder to fulfil.

In order to be useful, records must be retrievable and useable by the authorized individuals who need them. It is one thing when information is made available on a shared drive, central file repository, etc. It can be more difficult if the information is located on an individual's personal drive, file cabinet or storage area, but it is generally manageable as long as the employee follows RIM guidelines for classifying and organizing records.

For example, if a service representative or case worker maintains files at his/her workstation for individual cases, that information needs to be organized in such a way that someone else could continue the employee's work in the event of a temporary or permanent absence. If this information is allowed to reside on a personal device, however, it is much less likely that an employee is following the same policies, procedures, and protocols as would be the case for shared or even work-specific storage, and it may not even be possible to obtain access to the personal device if the individual is absent.

RIM, therefore, should keep the following considerations in mind if BYOD devices are involved:

Information distribution: Where exactly are the records located? If they are on a personal device, will that device always be accessible to anyone in the organization who might need access to the work information on the device?

Classification and organization: Is the information on a personal device properly organized according to a common scheme, so that others would be able to find what they need if the situation arose? This might include things like directory structures, naming conventions, metadata, and so on.

Version Control: Does the employee follow proper versioning protocols if s/he alters information stored on the personal device?

Accessibility: As an official record of the organization, there is a legal obligation on the part of the organization to make the information accessible for discovery in legal proceedings, controllable if subject to a legal hold, and available to respond to access to information requests if such legislation applies to the organization. If the information is on a personal device, it must still meet these criteria. This means the device containing the record must be accessible even if the employee is not. Someone besides the employee should have the passwords or other authentication methods to access the information in the employee's absence. There should also be accessible, up-to-date backup mirrors of the employee's device. And there should be a mechanism in place to prevent the record from being deleted in the event of a legal hold.

(3) Storage and Retrieval

The key question when it comes to storing and retrieving records and information is one of ownership, or at least control. Historically this was not an issue, since all records were stored within the physical confines of the organization. The arrival of offsite storage vendors complicated matters, with records no longer being stored on the organization's premises, but this difficulty was solved with contracts and service level agreements (SLAs). Cloud storage vendors extended the offsite storage concept to apply to digital information rather than physical media, but the SLA concept still provides adequate assurance that the information is secure and will be accessible when needed.

A personal device, on the other hand, is entirely different, and steps must be taken to ensure that custody and control are protected, despite physical ownership of the device lying with a third party (the employee). The key issues raised by BYOD relating to storage and retrieval are as follows:

Central storage: Because personal devices are so vulnerable, ensuring they are synced on a regular basis with a central storage repository is essential. Most devices have the ability to be backed up when connected to a desktop PC, but if this process is not sufficient if it is not frequent and automatic. Similarly, many devices can automatically be backed up to a cloud service (either public or operated by the device manufacturer), but if this cloud service is not under enterprise control it still may not be considered to be sufficiently controlled. Ideally a personal device will sync regularly with centralized enterprise servers. Depending on the device and application, it might be feasible for the data to exist only on a central server just to be displayed on the remote device. (This is called a ‘‘thin client" model and will be discussed further in Section 4(4) - Retention and Disposition).

Security: Enterprise information and records should be stored securely. For personal devices which are often off-premise and are often taken to public locations like airports, restaurants, customer sites, and so on, the information on these devices is at high risk of loss, theft, damage, etc. Backup and synchronization with a central location doesn't provide sufficient security, and the RIM manager must ensure there is sufficient security on the device itself. This might include measures such as encryption of data on the device, strong password protection, security software running on the device, and remote wiping capability.

Disaster Recovery: Any storage plan should include contingencies for data backup, recovery and reconstruction, and this also applies to records on personal media. Therefore, the RIM disaster recovery plan should include BYOD devices.

Media Format: As with all technologies, there is the ever-present risk that the format of the media containing the information may change and become inaccessible over time. When it comes to personal devices the risk is not so much that the physical media will become unreadable, but that the logical/ electronic format of the device may be incompatible with enterprise systems. For example, an employee may choose to store records using non-standard or proprietary file formats, database formats, and so on. Employees might also fail to keep their devices up to date with the latest versions of the operating system, applications, etc.

(4) Retention and Disposition

Retention and disposition of records means being able to ensure records are kept as long as needed and to securely destroy them when the time is right unless they are subject to archival preservation. Records and information residing on personal devices are problematic on both of these fronts. It may be difficult to prevent an employee from deleting a record prematurely, or to ensure the employee transfers archival records for preservation.

In some cases, it may be possible to keep the record in a central depository or file server and have the personal device act as a remote terminal. This is generally known as a ‘‘thin client" model. A ‘‘thin client" is an IT system (such as a remote desktop service) where a device acts as a screen that displays - but does not store - information held on corporate servers. This can help address retention concerns, since all information in the organization's control would remain on its servers and not on multiple personal devices brought into the workplace. Storing information on corporate servers will also enable the organization to better meet access to information requests mandated by applicable legislation.

The main drawback of a thin client approach is that the information is not available on the device whenever it isn't connected to the network, such as on

an airplane, outside of network coverage areas, or during network down time. Despite this, the use of thin clients may be a good alternative for certain applications or types of data.

There may also be a hybrid approach where the data is downloaded to the device for use when the network is inaccessible. In these cases, the official record would still be the centralized one, and the local copy on the device would be considered to be a copy.

(5) Archival Preservation

Because the information/records on a device should be uploaded to a corporate repository, it is probably uncommon that an employee's personal device will contain any unique information or records of archival value, however, there may be some situations where archival concerns apply. For example, if a device is used to capture photographs or recordings of archival value and the device does not automatically sync with a corporate repository, steps should be taken to otherwise preserve those records. Also, for example in rare cases the identity of the employee may determine whether the information on the device has archival value — for example if the person is a media or political figure.

RIM managers should be aware of the possibility of archival material existing on these personal devices and collaboratively work with other stakeholders to take steps to a) ensure it is not destroyed, and b) is secured and managed properly at the time of scheduled disposition or when the device is retired.

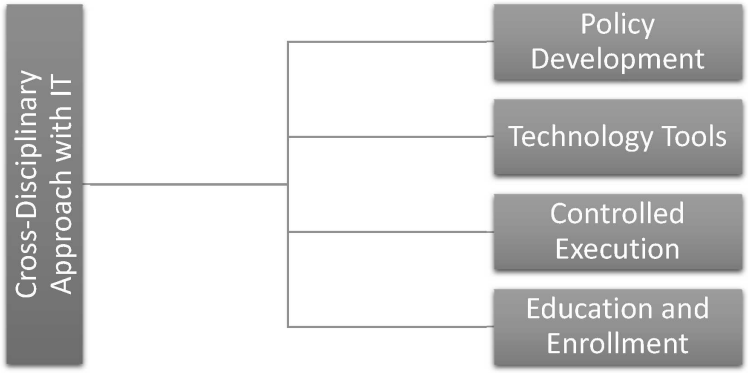
5. RIM Strategies

Many (although perhaps not all) of the concerns arising from BYOD which affect RIM practice will be held by other stakeholders in the organization, primarily IT. In most situations it will be IT driving the rollout and taking responsibility for the success of BYOD. Accordingly, RIM practitioners will need to ensure that their subset of concerns is addressed as part of the overall BYOD initiative.

In addition to embracing and mastering a cross-disciplinary approach, there are four main tools that both IT and RIM have at their disposal to ensure that the BYOD implementation is successful and does not compromise their respective responsibilities.

This strategic framework is shown in diagram form in Figure 4: Strategic Framework for RIM Implementation of BYOD.

Figure 4: Strategic Framework for RIM Implementation of BYOD



We will look at each of these in turn, but first we will examine the other possible option for BYOD: banning it entirely.

(1) The Nuclear Option: Can BYOD be Banned?

As discussed earlier, banning BYOD entirely is a difficult proposition. A high proportion of end users have demonstrated that they are willing to ignore or circumvent IT or information governance (IG) policies in order to access enterprise systems on their own devices, keep enterprise information and records on their personal devices or in personal cloud storage, or use personal devices for work related purposes. Furthermore, even though methods that enforce compliance reduce risk, it only takes one user or one device to create a security breach or inject malware or other problems into an enterprise network.

Beyond the policy level, there are some things that IT can do to prevent unauthorized devices from accessing the network, although all of them have drawbacks and may not be entirely effective:

MAC Filtering: Network access can be restricted using MAC addresses (which are unique identifiers for each network device). Typically, a network can be configured to only allow a whitelist of MAC addresses to have access and will block all other devices. Unfortunately, this can be difficult to maintain if there are thousands or tens of thousands of devices on the network.[26]

IP Blocking: Along the same lines, IT could also block access to public websites, services, and applications that could be used to compromise information assets. This might include cloud services like DropBox or

OneDrive, applications like Google Apps, and so on. Unfortunately, blocking access to these sites is also fairly simple to circumvent, especially for any employees who are offsite, by using cellular networks, public hotspots, or (for telecommuters or mobile employees) simply turning off their enterprise VPNs or using personal VPNs to access banned sites.

Device Level Security: In addition to MAC filtering and IP blocking, banning BYOD would also require implementing additional security and controls on the end user devices themselves in order to prevent the installation of custom applications, settings, and so on that could compromise the enterprise network. Aside from the effort and cost of implementing such restrictions, doing so can often unintentionally interfere with authorized uses of the device, cause slowdowns or crashes, and otherwise impact the desired uses of the device.

Add to this the fact that while implementing MAC filtering, IP blocking, or device level security might help control enterprise devices, they offer little protection against employees using personal devices for work purposes. All in all, it is problematic at best to try to eliminate the ‘‘Shadow BYOD” problem, and all indications are that it will become more difficult as consumer/personal technology continues to become more sophisticated and integrated with our day-to-day lives, both at work and at home.

Eventually most organizations will probably offer some level of BYOD rather than attempt to ban it completely. But even if an enterprise decides to ban BYOD, that in itself is still a policy decision and requires some version of policy implementation as described in the following sections. It isn’t enough to simply state that BYOD is not permitted and then hope employees comply. If the policy is ‘‘no BYOD,” then it is still incumbent on the enterprise to communicate, educate, and monitor compliance.

(2) Step One: Embrace a Cross-Disciplinary Approach

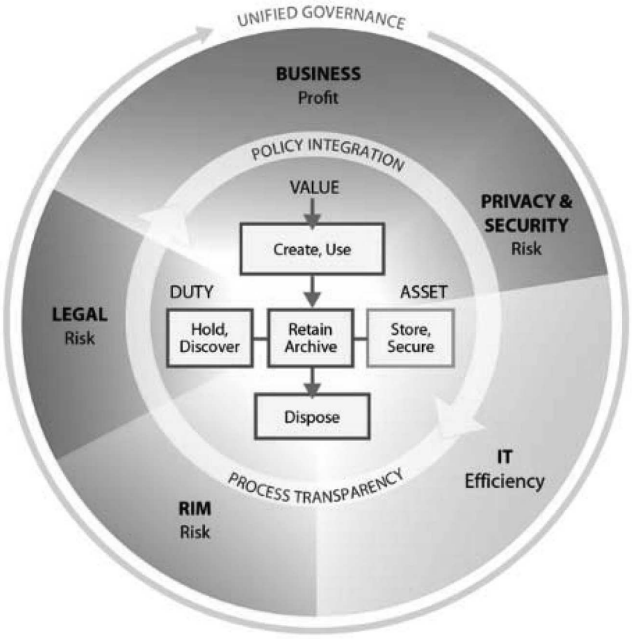
Because BYOD will be primarily an IT driven initiative, resolving RIM issues will require working within the overall framework and timeline set out by IT. Therefore, RIM needs to embrace a cross-disciplinary approach in which IT is enrolled in addressing RIM’s concerns as part of its overall BYOD strategy.

(a) Working in an Information Governance Framework

Information governance (IG) is a strategic approach and formalized organizational framework to assist organizations in managing their information strategically and efficiently. The Information Governance Reference Model (IGRM)[27] identifies the key organizational stakeholders and their roles, and provides an excellent approach for managing multidisciplinary projects for the

management of organizational records and information. Figure 5: Information Governance Reference Model shows the current version of the IGRM.

Figure 5: Information Governance Reference Model



The five key groups identified in the IGRM have a stake in any information-related initiative in an organization, including BYOD. The areas of concern and responsibility of each of these stakeholders is as follows:

RIM: Primarily RIM is concerned with the following areas encompassing the information on BYOD devices:

- Creation of records needed to do the organization's business, record decisions and actions taken, and document activities for which employees are responsible.
- Compliance with approved procedures for managing data/records containing personally identifiable information (PII) or security-classified information.
- Ensure information can be found when needed, i.e., set up directories and files, and file materials (in whatever format) regularly and

carefully so they will be safely stored and can be efficiently retrieved when necessary.

- Apply retention and disposition rules.

IT: With regard to BYOD, the IT department's activities and responsibilities include (at a minimum) the following areas:

- Define what BYOD devices may be used (makes and models).
- Determine service level and types of support to be provided to employees using their own devices.
- Provide BYOD access to organization-related resources.
- Control what applications, databases, etc. can be used on the device.
- Mobile device and application management.
- Control how information will be transferred to/from the device.
- Mobile content management, including synchronizing.
- Perform a remote wipe of a device which is lost/stolen.
- May administer user agreements, acceptable use policies, etc.

Privacy and Security: These groups may be part of IT, connected, or completely separate. This group is distinguished from the preceding IT group in that it is concerned only with privacy and security, whereas the IT function relates to the actual operation of the network and the devices on it. The main concerns of the Privacy and Security group for BYOD are to:

- Define security of corporate data on devices.
- Determine passcode, remote lock, and remote wipe requirements for BYOD devices.
- Define encryption methods and standards to be used.
- Establish any prohibitions or limits on the software applications employees can install on their devices.
- Require use of approved security-related software to access the organization's systems and servers.
- Enforce procedures for retrieving the organization's data when the user's employment is terminated or the device is lost/stolen.
- Define the protection level for cloud storage, data transmission, and data processing.
- Audit BYOD use and compliance with BYOD policies and procedures.

Legal: This function may be filled by the organization's general counsel, outside legal firm, risk manager or auditor, but in any case they also have specific requirements when it comes to BYOD:

- Require employees to sign a waiver or release form before using BYOD.
- Develop a procedure for retrieving a device if it is needed for data collection and preservation in association with a legal hold or to access information needed to respond to an access to information request.
- Ensure the records (legal) hold policy extends to BYOD.
- Consider how organizational policies will be affected, enforced, and audited when it comes to BYOD.

Business: The business unit is generally the driver for BYOD adoption, and as such their responsibility tends to centre around meeting the demands and needs of the end user:

- Determine what information or applications need to be accessible on a personal device.
- Make the business case justification for BYOD.
- Consider if/how employees will be reimbursed for organization-specific use of a personal device.
- Address any union or other employee concerns or objections to BYOD.

(b) Working in an Absence of an Information Governance Framework

Even if there is no formal IG framework in place, the same general principles should apply in terms of having all key stakeholders represented, maintaining clear areas of responsibility and accountability, and taking an organization-wide strategic view of the BYOD initiative, its benefits, and its drawbacks.

Consider who in the organization has a responsibility connected with the activities and information involved with the BYOD devices under consideration. While not every group necessarily has or needs an equal seat at the table, consider how their views can be assessed and taken into account, otherwise they may find a way to derail the project as it goes forward. In the absence of a functioning, established cross-departmental team resulting from an IG or similar initiative, the key will be to be inclusive without having so many differing viewpoints involved that no progress can be made.

(3) Policy Development: Define a BYOD Policy and End User Agreement

(a) Policy Development Process

Initial Assessment: Before embarking on a policy development initiative it is important to properly assess the current environment and the likely impact of a policy change. The more time it is possible to spend at the initial stage, the smoother the eventual implementation is likely to be. There are five key areas of study that should be undertaken:

1. *Business justification:* Even though, as previously discussed, many organizations support some form of BYOD despite the fact that the costs and risks can actually outweigh the benefits. Nonetheless, it is still important to assess the expected costs vs. benefits of the BYOD program. This is important not only to have a realistic understanding of the undertaking and set expectations for the results of the BYOD program, but also to use as a baseline for measuring success.
2. *Privacy impact:* The Office of the Privacy Commissioner of Canada recommends conducting both a privacy impact assessment (PIA) and a threat assessment before developing a BYOD policy.[28] A PIA is an analysis of what personal information might be at risk of exposure or might be necessary for the individual to disclose under various conditions. Depending on the degree of risk to privacy, the disposition of the organization and employees towards privacy issues, and so on, it may greatly affect the type of BYOD program offered, or preclude it entirely.
3. *Threat assessment:* Not only should the risk to the employee's privacy be assessed, but also any threats to the organization that might be posed by BYOD. Mainly this relates to the security of the organization's data on personal devices, but it might address other risk areas as well.
4. *Technology review:* BYOD is not just a matter of policy. It also requires certain technological capabilities, many of which are discussed in *Section 5(4).* Before embarking on a BYOD initiative, there should be an understanding of the technical effort and investment that is necessary to offer the program successfully.
5. *Key success factors/barriers:* Finally, there should be an assessment of the factors that are essential to the program's success as well as the potential risks and barriers, with at least some thinking towards how to overcome them.

This preliminary research and analysis will go a long way towards being able to develop a policy suited to the organization. It should also provide the

basis for the next step of policy development, which is to decide on the main policy elements themselves.

Decide on key features of BYOD implementation: Based on the information gathered at the initial assessment stage, it should be possible to define the details of the BYOD program at the policy level.

BYOD Program Participants: Which employees will be eligible to participate in the BYOD program? Does it extend to all employees or is it limited to certain types of job functions/roles? Are there specific job functions or categories of employees which should be excluded?

Device Categories to Be Included: The three main potential device categories for BYOD programs are smartphones, tablets, and PCs. Are all three included in the program? Are there exclusions within any of the categories? (for example, are laptops permitted but home PCs excluded?)

Allowed Applications and Resource Access: Which enterprise applications or other resources will be accessible using BYOD devices? Most BYOD initiatives allow access to email, intranet, calendaring software, file servers, collaboration applications, and so on. But what about other systems like HR databases, inventory systems, ERP systems, customer records, and so on?

Separation of Personal and Organizational Data: Will employees be required to install software on their devices to partition/containerize personal data separately from work data?

Capture of Data into Organizational Systems: How will information/records created on the remote device be captured to organizational servers, databases, etc.?

Financial Details: What will the employee pay for and what will the organization pay for? Usually (but not always) the employee bears the cost of the physical device. Are full/partial stipends available for some or all participants in the BYOD program? Who pays for the associated service plan for the device, if applicable? Note that many of these decisions may have accounting repercussions, such as capital valuation and depreciation, which should be taken up with the organization's finance department.

Privacy and Access Details: Under what circumstances will the organization be allowed access to the device? Will the device be subject to monitoring (e.g., location, change logs, call logs, web history)? Will users be required to install special security or other software? While such software might be standard on enterprise-issued devices, will personal devices be required to meet the same standards? How will discovery/access to information requests be handled?

Infringements on Personal Use: Even though a BYOD device is a personal device, will the enterprise insist on any restrictions on how the device is used, what applications are permitted/banned, what kinds of personal content may be stored on the device, etc.? Are there any other limitations on acceptable use of a BYOD device as compared to an entirely personal device not used for BYOD?

Other Requirements or Limitations on Participants: Will users be required to run a specific operating system or specific application versions? Will they be required to

install security patches or other software when instructed? What other specific limitations will users be required to accept?

BYOD Program Termination: What is the process for employees exiting the BYOD program, whether because they no longer wish to participate, because they're leaving their position or leaving the company, or for any another reason?

(b) BYOD Policy Essentials

Once the details of the BYOD policy have been decided, the policy document itself can be drafted. The BYOD policy can be written as a standalone document if desired, but most organizations will probably choose to incorporate it into their overall mobile device policy to avoid duplication and minimize the total number of corporate policies. Related policies that might also be integrated into the larger mobility policy would be a cloud computing policy and a social media policy, for example.

The BYOD policy should address the decisions made in Section 5(3)(a), and in broad terms should include the following sections:

- *Acceptable Use*, including any restricted activities, websites, etc.
- *Devices and Support*, including a full list of devices which are permissible and any provisos on configuration or other staging that IT will conduct on the device.
- *Reimbursement*, or lack thereof. This should include any exceptions (e.g., if the company will pay for the monthly plan but not for overage charges).
- *Security*, including encryption, password policy, user privileges, remote monitoring and wiping, etc.
- *Privacy*, addressing both the user's reasonable expectation of privacy as well as any infringements on privacy that may be required, such as device monitoring.
- *Enforcement* and consequences of violation (up to and including termination).
- *Risks/Liabilities/Disclaimers*, for example to indemnify the organization against loss of personal data.

Naturally this template is only a guideline, but it provides an outline of how a typical BYOD policy might be structured. There are many freely available templates and sample policies available on the internet to use as a starting point. This section is derived from the excellent template by Megan Berry at IT Manager Daily, which provides a more detailed view of many of these sections.[29]

(c) Develop Appropriate User Agreements

Of the four tools we are discussing, a properly developed, well-planned policy document is probably the most important tool an organization has in making its BYOD program a success. In addition to providing a clear, simple definition of what the BYOD program is and what it isn't, it is the driver for BYOD technology investment and the basis for employee communication and training.

One of the first uses of the BYOD policy should be to develop an end-user agreement. This document may be quite similar to the policy document, but will be written as an agreement which an employee must sign as a condition for participating in the BYOD program. This is important because it makes it much more likely that the employee will understand the key features and limitations of the program before enrolling.

Unlike the BYOD policy (which is integrated into the larger mobile device policy) this is a standalone document requiring the employee's signature. It requires active agreement from the employee rather than the passive acceptance of the policy, which theoretically should ensure the employee is better informed and more invested in the program.

(4) Technology Tools: Assess Technology Solutions Against Rrequirements

A strong BYOD policy, if done correctly, will provide an excellent foundation for a BYOD initiative. Enabling that policy will require a number of technical capabilities the enterprise may still need to invest in and develop. RIM practitioners should understand the technology tools to support BYOD which are available or under development, both to assess the impact on the RIM program and to influence features and functionality of the various components. Defining detailed requirements is an effort which IT will need to undertake with assistance from the BYOD team. Some of the most common technology requirements for BYOD are described below as a starting point.

(a) Device Monitoring

There are many emerging network management products that include mobile device monitoring. Device monitoring is generally considered to belong to a category of products known as Enterprise Mobility Management (EMM).[30] Sometimes the more dated term, Mobile Device Management (MDM) is used instead. EMM suites provide a central platform for enforcing management policies, mobile security, deploying mobile apps, remote troubleshooting, remote wiping, and auditing/reporting.[31] Leading vendors include IBM, Citrix, Good Technologies, and SAP.

These high end software suites are, unsurprisingly, quite expensive, but there are also many niche solutions available that may meet an organization's requirements for BYOD. The most important thing is the ability to monitor when BYOD/personal devices have connected to the network so they can be given appropriate network privileges, be remotely managed as needed, and have data collected from them when needed for efficient network management.

Device monitoring may also include the ability to connect to asset/ inventory management systems. Even though BYOD devices may not be assets from an accounting point of view, they should be treated as such by IT and RIM in order to maintain control over the BYOD program as a whole. It is also important to know which devices are included in the BYOD program because otherwise it may not be possible to effectively secure the network from non-BYOD devices which gain unauthorized network access.

(b) Containerization

Setting up a secure, encrypted area of a mobile device's memory is known as containerization. The concept is similar to partitioning a hard drive — even though each container shares the same physical medium, they appear as completely separate logical devices. Many of the same vendors of EMM software also provide containerization tools, such as Good Technology or Airwatch.

Mobile containers may be like hard drives set up for file sharing, or they may be dedicated to application specific storage (such as a secure email container). Containers may also be used to securely run specialized applications like enterprise-approved browsers, etc. Running an application in a container rather than just using it for storage is sometimes done using a technique called ‘‘app wrapping,” and is considered to be a subset of containerization technology. Essentially it offers a more secure version of an application (often downloaded from the organization's internal app repository) which is completely separate from other personal apps like Facebook or Instagram.

Containerization is a common feature in BYOD, because it simultaneously helps to satisfy some of the security concerns from the IT side and some of the privacy concerns from the user side. From a RIM perspective, storing records in a dedicated, secure, and encrypted area of memory is a great improvement in addressing records-related concerns.

(c) Syncing and Data Mirroring

Most consumer mobile devices include features that allow the data to be backed up to the cloud or a personal file server. Increasingly this can be done automatically and over a wireless network. The terms ‘‘remote backup”,

‘‘mobile synchronization,” and ‘‘data mirroring” are generally synonymous in referring to this capability, with some small distinctions between them.

In a BYOD scenario, using personal synchronization tools is probably not reliable or robust enough. In an enterprise environment, there are a wide variety of models, methods, and protocols to enable mobile synchronization, and the decision to go with a specific tool or approach can be quite complex.

Whichever approach IT decides on, RIM representatives should take the time to understand the RIM implications, particularly when it comes to thin vs. thick clients, multiple copies, version control, and frequency of synchronization (which can be any set interval up to nearly real-time sync).

(d) Remote Wiping

Remote wiping is considered to be an essential BYOD feature. It is usually considered to be part of (or perhaps an extension of) remote monitoring, and is universally a feature in EMM/MDM suites.

Remote wiping is a ‘‘last line of defense” against security breaches when a device has been lost or stolen. It can be objectionable to end users if they aren’t yet prepared to wipe their personal data (e.g., if they think they might still recover the device), or if their data is wiped accidently. For example, some systems are configured to remotely wipe a device after a set number of incorrect password entries.

(e) Carrier/Public Network Services

A final technology consideration, which is not so much a question of investment as it is a question of supplier/ vendor selection, is the choice of a carrier/network service provider for when the mobile device is outside of the organization’s network and must access it through a public cellular or Wi-Fi network. The enterprise’s choice of network provider may be affected by certain features offered, flavour of VPN support, network coverage, pricing, and other details. In most cases the selection of carrier should not make much if any difference, but the enterprise may have its own reasons for selecting a particular carrier.

If this is the case, the employee may be required to sign up with a particular carrier for cellular voice/data service. The RIM implications of this are likely negligible.

(5) Controlled Execution: Develop a Phased BYOD Implementation Plan

Now with a strong policy and the technology tools needed to support it, the enterprise can apply a third tool or method which will help the BYOD program

be successful: a well-planned, carefully controlled implementation. It is at this point where BYOD goes from theory into practice, even if it is on a small scale, and this tends to be the time when there is the most to learn. Accordingly, the RIM members of the BYOD team need to stay involved and informed throughout the implementation process.

(a) Pilot

One of the advantages of BYOD is that it can be implemented on a very small scale initially, and even a small pilot project can provide a wealth of useful data and opportunities to improve and fine tune the program. Even in a large organization, a pilot project could be limited to a group as small as ten users. Initial participation in the program could even be on a random or voluntary selection basis, rather than most technology innovations which often must be rolled out on a trial basis to an entire department or work area.

A second advantage is that the pilot project can be scaled up very gradually, even by just a few users at a time. Thirdly, pilot participants can be selected from a wide cross section across the organization, giving the opportunity to address issues that might not be visible within a more homogenous user group.

Keep in mind the importance of having RIM representation involved in the pilot in order to learn the RIM pitfalls and address any RIM specific issues that may arise.

(b) Phased Rollout

Following the pilot, even if it has been gradually ramped up, a phased rollout should be planned rather than launching the full program. During the rollout, the BYOD program can be offered to larger population groups within the organization. This might be staged on a department by department basis, or perhaps by job function (e.g., sales, field technicians, etc.), or by some other identifiable group (e.g., executives, telecommuters, etc.). The main purpose of this stage is to test the ‘‘soft” aspects of the program, such as communication, training, business processes, etc. The pilot phase generally just implements the technology and gets it to work as intended, whereas a limited rollout is intended to test the program as a whole but on a small scale.

As more and more groups are added to the rollout, the implementation will start to ‘‘stress test” the processes and support mechanisms that have been put in place, so it is important to look for needed process improvements or resource reallocations in order to keep the program running smoothly.

(c) Support and Incident Management

From the pilot phase forward, it is important that end users understand the technical support resources available to them, and the process they should

follow if they require help with their device, particularly if there are any differences between BYOD support and support for other enterprise technologies. This would include a defined incident management process,[32] designed particularly to deal with BYOD specific issues such as privacy and security breaches.

(6) Education and Enrolment: Communication is the Key

The final tool the BYOD implementation team has to ensure success is communication. Communication and transparency will be important throughout the entire process, but especially when the BYOD program goes wide throughout the organization. There are three key methods of communication which the BYOD team needs to address.

Education: Everyone involved in BYOD, from senior management sponsors to fellow BYOD team members to business unit leaders to end users, should be educated on the BYOD program. There should be a common understanding of what BYOD is, why the organization is implementing it, and what results are expected. If employees have questions or objections, there should be a defined way of addressing them.

Enrollment: In addition to giving employees the facts, the BYOD team should be trying to enroll stakeholders, decision makers, and end users in the BYOD concept. The advantages and benefits of whatever version of BYOD the enterprise has decided upon (as defined in the BYOD policy) need to be emphasized and objections overcome. It may be wise to engage other groups to assist in this such as human resources, employee relations, etc.

Training and Support: Once the BYOD program has been launched, proper training should be supplied in the form of whatever documented procedures, guidelines, instructions, etc. may be needed. Help desk support, or at least a documented troubleshooting and support process should be available. It may be that having a personal device instead of a device issued by the organization makes little difference in how an employee works, but whatever differences there may be in terms of workflow, using and managing the device, etc. need to be clearly illustrated.

In summary, RIM involvement in developing a BYOD program will contribute to its success and ensure RIM concerns are addressed. Even though IT is likely the key driver of the program, RIM (and other stakeholders in the organization's information management practices) are necessary contributors to the BYOD team. Through well-researched, intelligent policy design; establishing needed technological capabilities and infrastructure; conducting a sound, well supported implementation; and maintaining clear communication, education, and enrollment from start to finish, the BYOD program will further RIM's ability to meet the information management

challenges of mobile technology and support the ‘‘anytime, anyplace” work environment which has increasingly become the norm.

6. About the Author

Sheila Taylor is a Certified Records Manager (CRM) and Information Governance Professional (IGP) with more than twenty-five years’ records and information management (RIM) experience. She is the Partner & CEO of Ergo Information Management Consulting, a product-independent information management consultancy based in Georgetown, Ontario, Canada.

Sheila’s articles and book reviews have appeared in publications such as Association Magazine, Information Management Journal, and Municipal World, and she blogs at http://impress.eimc.ca.

Sheila is a frequent speaker on RIM topics at conferences and other education events in Canada and the United States.

She is also a member of ARMA International’s Content Editorial Board which assists ARMA to unify and streamline content development processes across all formats (i.e., books, standards/technical reports/guidelines, Information Management magazine, conference education, online education).

Sheila was an instructor in the records management certificate programs at The iSchool Institute of the University of Toronto’s Faculty of Information for more than fifteen years and has also been a RIM instructor at Mohawk College in Hamilton, Ontario. She recently taught the Managing Organizational Records I course in the Master of Information Science program at the University of Toronto.

7. Bibliography

AIIM Market Intelligence. 2015. *Mobile and Cloud Industry Watch Report.* Survey, AIIM.

Archives and Records Association, UK & Ireland. 2010. “Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud.” *http://www.archives.org.uk/.* August. Accessed January 2016. http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf.

Berry, Megan. 2013. *BYOD Policy Template.* Accessed January 2016. http://www.itmanagerdaily.com/byod-policy-template/.

Cavoukian, Ann. 2013. “BYOD: (Bring Your Own Device) Is Your Organization Ready?” *www.ipc.on.ca.* December. Accessed January 2016. https://www.ipc.on.ca/images/Resources/pbd-byod.pdf.

City of Phoenix. 2014. *Bring Your Own Device: Resistance is Futile.* Phoenix, AZ, July.

EDRM. n.d. *Information Governance Reference Model (IGRM).* Accessed January 2016. http://www.edrm.net/projects/igrm.

Forrester Research Inc. 2012. *BYOD in Government: Prepare for the Rising Tide.* October.

Gartner Inc. 2013. *Gartner Research Circle: 2013 Future of Mobility.* August.

Gartner Inc. 2014. *Research Circle Results: 2014 BYOD Survey.* March.

Gatewood, Brent, CRM. November/December 2012. "The Nuts and Bolts of Making BYOD Work." *Information Management* 26-30.

Good Technology. 2013. "Good BYOD Report 2013." *www.continuums.net.* Accessed January 2016. http://www.continuums.net/docs/2_25926_Good-BYOD-Report-2013.pdf.

Intel IT Center. 2012. *Insights on the Current State of BYOD in the Enterprise: Intel's IT Manager Survey.* Survey Summary, Intel IT Center.

Law Society of British Columbia. 2013. "Law Society of British Columbia Cloud Computing Checklist." *www.lawsociety.bc.ca.* January. Accessed January 2016. https://www.lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf.

Lookout. 2015. "Feds: You Have a BYOD Program Whether You Like It or Not." *Lookout.com.* Accessed January 2015. https://www.lookout.com/resources/reports/federal-byod.

Mintz, Marc. 2015. *LinkedIn.* April 15. Accessed January 2016. https://www.linkedin.com/pulse/how-prevent-byod-devices-your-network-marc-mintz.

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of British Columbia, Office of the Information and Privacy Commissioner of Alberta. 2015. "Is a BYOD (Bring Your Own Device) Program the Right Choice for your Organization? Privacy and Security Risks of a BYOD Program (August 2015)." *www.priv.gc.ca.* August. Accessed January 2016. https://www.priv.gc.ca/information/pub/gd_byod_201508_e.pdf .

Ovum Consulting. 2012. "BYOD: an emerging market trend in more ways than one." *www.us.logicalis.com.* Accessed January 2016.

Queensland State Archives. 2013. "Recordkeeping Implications of Mobile and Smart Devices." *www.archives.qld.gov.au.* April. Accessed January 2016. http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/MobileDeviceGuideline.pdf.

Rouse, Margaret. 2014. *Techtarget.* September. Accessed January 2016. http://searchsecurity.techtarget.com/definition/bring-your-own-apps-BYOA.

Smith, Richard. 2015. *Who Made The List? Gartner's 2015 Magic Quadrant For Enterprise Mobility Management.* June 16. Accessed January 2016. http://www.business2community.com/tech-gadgets/who-made-the-list-gartners-2015-magic-quadrant-for-enterprise-mobility-management-01252148#oFezHIq01dHxdfaq.97.

Stroud, Forrest. n.d. *Webopedia - Bring Your Own Apps.* Accessed January 2016. http://www.webopedia.com/TERM/B/byoa-bring-your-own-apps.html.

Taylor, Sheila. 2015. "RIM and BYOD (Bring Your Own Device)." *ARMA PEI Chapter Conference.* Charlotte, PEI, November.

ENDNOTES

1. For more on this, see Section 3(2) – Shadow BYOD.
2. (Intel IT Center 2012).
3. (Gartner Inc. 2014).
4. (Gartner Inc. 2014).
5. (Gartner Inc. 2014).
6. (Gartner Inc. 2014).
7. (Good Technology 2013).
8. (Ovum Consulting 2012).
9. (Gartner Inc. 2014).
10. (Gartner Inc. 2013).
11. (Intel IT Center 2012).
12. (AIIM Market Intelligence 2015).
13. (Good Technology 2013).
14. (Ovum Consulting 2012).
15. (Forrester Research Inc. 2012).
16. (Intel IT Center 2012).
17. (Gartner Inc. 2013).
18. The 69% adoption rate contrasts with the much lower rate reported in the next year, even though the survey methodology and sample population largely shared the same characteristics..
19. (Gartner Inc. 2014).
20. (AIIM Market Intelligence 2015).
21. (Forrester Research Inc. 2012).
22. (Lookout 2015).
23. (Intel IT Center 2012).

24. (Rouse 2014).

25. (Stroud n.d.).

26. (Mintz 2015).

27. (EDRM n.d.).

28. (Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of British Columbia, Office of the Information and Privacy Commissioner of Alberta 2015).

29. (Berry 2013).

30. (Gartner Inc. 2014).

31. (Smith 2015).

32. (Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of British Columbia, Office of the Information and Privacy Commissioner of Alberta 2015).