Section 3: Week 7: Mobile Device Management (Transcript)

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 7, 2020

North Central University

# Mobile Device Management Transcript

## Agenda

Good afternoon, today, we are going to discuss the challenges and opportunities that exist around mobile device management. This discussion will begin with a brief history lesson and an analysis of the legal frameworks that are shaping our journey forward. Afterward, an assessment of the risks specific to mobile device management will guide the conversation toward tooling and frameworks for constraining those threats.

## How Did We Get Here

Legacy network environments heavily rely on centralizing information into a single mainframe or data warehouse. Network security teams could protect these resources through border security solutions, such as firewalls and other network access controls. However, this model lacks the convenience and data portability that users expect, leading to the adoption of Master Data Management systems (MaDaMgmt).

The objective of MaDaMgmt is to enable the sharing of business entities and related feeds across the organization. Now that employees could locally cache information on their corporate laptops and workstations, productivity increased, but ensuring data confidentiality and integrity became more complex. Deploying client management tooling (CMT) allows the administrators to enforce security policy across these edge devices. These CMT products tend to specialize in specific platforms and scenarios, which creates limitations on the corporate Information Technology (IT) departments. Due to these restrictions, rigid homogenous topologies became the norm instead of allowing the best tool for the job.

Modern networks believe that IT enables the business, not stifles innovation. The emersion of the Bring-Your-Own-Device (BYOD) makes this perspective front and center. Since employees are free to use the best tool for their role, it results in highly diverse environments that span multiple technology stacks, like Windows, iOS, and Android. While this freedom improves productivity, at the cost that private information resides on third-party devices that are partially trusted at best.

# Legal Mandates

## International Policies

In 2013, the European Security Strategy set out to achieve cyber-resilience, reduce cybercrime, and define policies that promote its core values. The security posture of the EU continues to evolve from these expectations to include policies like the General Data Protection Regulation (GDPR). This legal framework requires that the infrastructure for services offered to their citizen to reside in Europe, allowing enforcement over the Union’s sovereignty. It uses these legislative teeth to force businesses to take customer privacy seriously. When the business violates the public trust or negligently handles data, the government can issue severe fines for non-compliance. GDPR also declares that information about a user is the property of that person, not the service provider. Since the user owns the data, they can request a copy or its destruction at any time.

## Internal Process Controls

In 2002, several high-profile accounting scandals rocked the financial world (e.g., WorldCom and Enron) intentionally and maliciously falsified documents. A general sense of mistrust began to form across the American investment community. The SOX Act was a direct response to these challenges by mandating internal controls and external auditing procedures. Executives leadership teams must produce documentation about these systems and are personally accountable for inaccuracies. This accountability is punishable by fines or even jail sentences in egregious situations. Along with these official repercussions, shareholders are quick to sell their investment in untrustworthy businesses.

## Health Care Privacy Reform

In 1996, the Health Insurance Portability and Accountability Act, came into existence to protect patient confidentiality and modernize the health care information flow. In 2009, the Health Information Technology for Economic and Clinical Health Act removes loop-holes in HIPAA compliance and forces medical facilities to adopt Electronic Medical Records (EMR).

In 2014, an amendment to the HITECH legislation expanded the definition of Personal Health Information (PHI) by protecting individuals’ privacy for fifty years after being deceased. There are exceptions to this rule, such as a request from the person’s caregiver, provided a written request for confidentiality does not exist. Other exceptions allow release for insurance billing and payment scenarios.

## FERPA

In 1974, the Family Education Rights and Privacy Act gave parents the ability to (1) access; (2) amend; and (3) limit disclosure -- of their child’s educational data. These controls cover any student’s Personally Identifiable Information (PII) and educational records. According to Langlois (2014), these rules apply to any organization that accepts federal funds. She also notes that FERPA is the federal minimum bar, and places like Texas go further with state-level requirements. When a school district violates FERPA, no penalizations exist outside of potentially losing its federal funding. However, the parents are free to file civil suits and seek damages caused by negligence and maliciousness.

## Legal Themes

User privacy is a critical design component across these various legal frameworks. Two reoccurring themes state that the user owns their data and that ownership is relatively broad. Administrators need to be cognizant of this net while defining and implementing mobile device management strategies, especially in BYOD scenarios. The right to privacy can come at odds with personalization and system functionality, forcing a discussion around trade-offs within specific locales. Depending on the region, local regulation can create substantial economic incentives to respect the customer’s privacy. Where those laws are less strict, the business still has an ethical obligation to protect data about those individuals.

# Risk Associated with Mobile Device Management

Employees download sensitive information onto their mobile devices and laptops, then leave the safety of the corporate environment. This departure opens these machines up to a series of risks that would not exist on stationary workstations. For instance, the device is roaming around the open world and can be lost or stolen. Other risks come from the system connecting over untrusted and potentially hostile networks, enabling hackers to violate the confidentiality, integrity, and availability of classified information. Additionally, these devices retain the attack surface of traditional workstations and can fall victim to malware and software exploitation.

Enforcing mobile security must expand beyond malicious scenarios and also cover the prevention of negligence. Employees use their devices for both official and personal tasks, and mixing context can cause information leaks. For instance, the user might download an e-mail attachment onto their iPhone device, which automatically backed up to Apple’s iCloud. Now through no intentional action that communication is entirely outside of the managed ecosystem. Specific businesses might desire to track these interactions, but this can lead to privacy concerns and future litigation.

# Building a framework around these issues

## Addressing these issues

Client management tools give the system administrators the ability to define policy centrally and then target groups of workstations. Effective device management needs a similar mechanism that accounts for platform-specific variations. Unified Endpoint Management (UEM) addresses these issues by creating an abstraction layer that can translate corporate governance and policies into device-specific configurations. For instance, the administrator can mandate the installation of all critical operating system patches. The implementation of this action varies between Windows desktops, Apple iPhones, and Android Chromebooks—though the intent remains consistent. In addition to desired configuration and patch management, UEM platforms can perform operations like remotely wiping the device or requesting inventory reports. These actions enable the administrators to address specific challenges like the lost and stolen device scenarios. Advanced solutions like Microsoft Intune and MobileIron, support sandbox technologies that prevent mixing personal and corporate data. The data context tagging also opens the door for smarter remote wipe scenarios that do not touch personal data like family pictures.

## MDM Tooling Recommendation

Gartner enumerates several MDM vendors and calls out strengths and weaknesses among their offerings. Of these providers, Microsoft’s Intune stands out for being both a SaaS-based solution and supportability for most mainstream devices. Service integrations allow connecting existing on-premise CMT solutions like Microsoft Configuration Manager. Administrators can enjoy a wide range of scenario-specific configuration templates and extensive reporting capabilities. Other market leaders include MobileIron, IBM, and VMWare, which come with similar feature sets and unique challenges.

## Building a Privacy First Framework

According to the Global System for Mobile Communication Association (GSMA), the five elements that build accountable information policies are listed below. These foundational components promote the ideas of executive sponsorship that ensure data collection strategies align with corporate values. For instance, a school district might be sensitive to any appearance of encroaching on student privacy or infringing FERPA norms. These values might limit data assemblage within software inventory reports on those devices.

The people, processes, and products of the institution must also be aware of these values and understand how to apply them. This awareness starts with training about industry-specific requirements and the rationale behind these ideas. Next processes, must leverage that training to incorporate the best practices into every business workflow. For example, the business might have various categorizations of customer data, with each category requiring particular retention durations and access policies. Documentation needs to record these decisions and relevant controls for internal and external auditing. Processes that are auditable and transparent encourages staff to make ethical decisions, knowing action scrutiny will follow later. Lastly, no business workflow is perfect, and mistakes are bound to happen. Remediation strategies need to correct erroneous behaviors and restore compliance.

## Integrating with other Frameworks

Risk management systems, like COBIT and NIST Cybersecurity Framework, follow feedback loops that identify threats, plan a response, implements that plan, and confirms the resolution. Each cycle through this process addresses a distinct problem and then mitigates it. Addressing privacy concerns and mobility risks can follow a similar workflow. For example, the organization wants to expand its mobile device management to cover a subsidy in a foreign nation.

First, the leadership team needs to identify any privacy and related laws for that region. This step might involve hiring or contracting a specialist to navigate the overseas legal systems. These results guide a response strategy that influences policies and data collection across those team members. After implementing the plan, there needs to be an audit and process validation with experts to confirm the solution meets the specification. Finally, periodic assessments must identify any policy changes that justify executing another loop iteration.

# Conclusion