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

## GDPR

The European Security Strategy (2013) set out to achieve cyber-resilience, reduce cybercrime, and define policies to promote core European Union (EU) values. The security posture of the EU continues to evolve from these expectations to include policies as the General Data Protection Regulation (GDPR). This legal framework requires that the infrastructure for services offered to their citizen reside in Europe. The Union can enforce its sovereignty by penalizing any action which viol.

European regulation creates the legislative teeth necessary to ensure that businesses take customer privacy seriously. These include mandatory fines for negligence that violates the public trust and states that individuals are the owner of data associated with them.

## SOX

In 2002, several accounting scandals rocked the financial world (e.g., WorldCom and Enron), resulting in regulation to create audit records and an emphasis on internal controls.

## HIPAA and HITECH

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 several articles, mentions of HIPAA are often accompanying by HITECH.

## Omnibus Rule

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 have state-level requirements that go further. 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.

# Risk Associated with Mobile Device Management

## Stolen Devices

## Mobile Malware and Vulnerabilities

## Advanced Threats

## User Behavior

# Building a framework around these issues

## How to address

## MDM Tooling Recommendation

## Mitigating Privacy Concerns

## Integrating with other Frameworks

# Conclusion