Mobile Device Management: Opportunities to Strengthen Data Security and Identify Cost Savings

Cotton & Company
Answers Questioned

Loren Schwartz and Matt Gorman

January 19, 2022

Introductions

Cotton & Company
Answers Questioned

- Loren Schwartz – geeky propeller head
- Matt Gorman – geekier bean counter
- Somehow, despite our obvious differences, we work together on projects.

Background

Cotton & Company
Answers Questioned

- Telecommunications is its own, very lucrative and complex industry.
- Every organization, from the smallest to the largest, spends money on telecommunications.
  - Wired communications (telephone networks, cable/internet access and fiber optic communications)
  - Wireless communications (our focus today)
  - Conferencing services

Background

- Raise your virtual hand if you have a mobile device that you use for work.
- Each organization we have worked with is different from a policy and usage perspective, but the common denominator is that we continue to see increases in the usage of mobile devices in the work place.
- Mobile devices bring different security and cost considerations (risks and rewards) than traditional IT.

Background

- Risks can include
  - Physical loss or theft
  - Disclosure of sensitive or proprietary data
  - Inappropriate usage
  - Excessive or unnecessary costs
- Rewards can include
  - Increased connectivity and ease of communication
  - Higher efficiency and productivity of staff

Background

- The goal of this session is to raise awareness of steps that organizations can take to strengthen data security and identify cost savings so that the risks related to mobile device usage are reduced and the rewards are realized.

Background

- Who is this course for?
  - Government and industry
  - Federal, state, and local
  - Management and auditor
  - Finance and IT

Agenda

- The Mobile Device Backdrop
- Managing Mobile Device Inventory
- Monitoring of Plans and Device Usage
- Policies and Procedures for Mobile Device Programs
- Securing Mobile Devices
- Wrap-up

The Mobile Device Backdrop

Cotton & Company
Answers Questioned

- What's a mobile device?
  - Lots of definitions, but almost all include the idea that a mobile device is a portable, technology based piece of equipment.
  - Most definitions include smart phones, tablets, smart watches, e-readers, and handheld gaming consoles. Some definitions include laptops, although most do not.
  - Many people consider peripherals (printers, mice, keyboards, flash drives) mobile devices.
  - For purposes of this presentation we are focused on tables and smart phones which are heavily used in the work place.

The Mobile Device Backdrop

Cotton& Company
Answers Questioned

- Mobile devices are prolific across federal, state and local governments
  - There are an estimated 298 million smartphone in the U.S. This doesn't count other mobile devices (for example, tablets).
  - On average, we spend 263 minutes DAILY on our smartphone. (My teenage daughter assuredly brings up that stat).
  - It is difficult to find reliable/accurate statistics of how many mobile devices are in use at government agencies. The short answer is – a lot.

The Mobile Device Backdrop

Cotton& Company
Answers Questioned

- Telecommunications contracts/invoices can be very confusing
  - There can be an almost endless variety of contract clauses that impact cost/usage of both voice and data for an organization.
  - Telecommunications invoices for even a medium-sized organization can be hundreds of pages long each month (data analytics junkie's dream come true).

The Mobile Device Backdrop

Cotton & Company
Answers Questioned

- There are four primary areas that organizations struggle to control their mobile device programs
  - Managing of device inventory
  - Monitoring of plans and usage
  - Developing adequate policies and procedures for mobile device programs
  - Securing devices, applications, communications, and data

Managing Device Inventory

Cotton & Company
Answers Questioned

- Managing device inventory – can be both a cost issue and a security issue.
- The risks are generally mitigated on the cost side with a bring your own device (BYOD) program, but security risks tend to increase.
- Related to cost...
  - Full retail price for an iPhone 13 (512 gb model) $1,099.99.
  - It's small
  - It's valuable
  - It's a thief's dream target

Managing Device Inventory

Cotton & Company
Answers Questioned

- Managing device inventory
  - If you are a small agency with just 3,000 employees and offer an iPhone for each employee, there is an inventory of 3,000 phones to manage.
  - At any point in time some phones are:
    - Reaching end of life and may be returned to inventory
    - New phones are ordered for new employees
    - New phones are kept in inventory waiting to be issued
    - Phones are returned from terminated employees
    - Phones are lost/stolen
    - Phones are broken and waiting to be fixed

Managing Device Inventory

Cotton & Company
Answers Questioned

- Managing device inventory
  - Typical telecommunications contracts have some combination of charges for a device, data, and voice.
  - If an agency isn't managing the device inventory, there may be devices that are missing or underutilized for which the organization is paying.
  - It can be difficult to correlate a device (iPhone Asset # 12345) with an employee (employee ID ABCD).
  - Controls around those devices that are in inventory or stock (meaning not distributed) are among the highest risk.

Managing Device Inventory

Cotton & Company
Answers Questioned

- Managing device inventory – security concerns
  - Just like a laptop or some other device with data/information, a mobile device has information, potentially sensitive stored on it.
  - Therefore, when a device is returned or retired, organizations need a process to ensure that the information is protected.
  - A best practice (but not a cheap practice) is utilization of a mobile device management (MDM) software that can assist with these processes.

Managing Device Inventory

Cotton & Company
Answers Questioned

- Managing device inventory – security concerns
  - If a device is lost or stolen, the data on that device is at risk.
    - MDM solutions would allow you to remotely wipe (erase) data on the device.
  - If your organizations employs a BYOD program, there may be disagreement about who “owns” the device and the information on the device.

Managing Device Inventory

Cotton & Company
Answers Questioned

- Immediate step to take
  - Compare the inventory of devices that your organization is paying for to the inventory of assets you have and ensure these can be reconciled.
    - Follow up on anomalies.

Managing of Plans and Device Usage

Cotton & Company
Answers Questioned

- This is the area where the greatest cost savings will be found.
- As previously discussed, a telecommunications contract can be very complex.
- An organization can't manage the plans and devices unless they know and understand their contract.

Managing of Plans and Device Usage

Cotton & Company
Answers Questioned

- These are the two primary areas of waste related to device usage and plans:
  - Mobile devices are deployed and go unused or are underutilized
  - Mobile devices are returned to inventory and the organization doesn't tell the telecommunications provider to terminate the plan
    - Also: excess inventory of phones waiting to be issued

Managing of Plans and Device Usage

Cotton & Company
Answers Questioned

- Mobile devices are deployed and go unused or are underutilized
  - If Jane got a mobile device then I should get one too! Unfortunately politics in an organization will often result in mobile devices being given to individuals who may have little need for them.
  - Additionally, sometimes the organization standard is that certain departments or levels in an organization will automatically get a mobile device, even if some individuals in these departments won't ever use them.

Managing of Plans and Device Usage

Cotton& Company
Answers Questioned

- Mobile devices are returned to inventory and the organization doesn't tell the telecommunications provider to terminate the plan.
  - In many organizations, employees get hired, transferred, and terminated regularly. IT help desk are already over-worked and under-resourced. Simple administrative tasks like communicating to the service provider to discontinue service on a mobile phone is often easily overlooked.

Managing of Plans and Device Usage

Cotton & Company
Answers Questioned

- There is an excess inventory of phones waiting to be issued.
  - Cases where organizations are still purchasing new devices, despite this

Managing of Plans and Device Usage

Cotton& Company
Answers Questioned

- We are in luck. Telecommunications carriers typically have online portals or electronic invoicing that can be easily converted into a workable format for data analytics.

Managing of Plans and Device Usage

Cotton & Company
Answers Questioned

- Immediate step to take
  - Read the contract and understand how billings are calculated.
  - Obtain the latest electronic invoices/reports from the telecommunications carrier. Sort so that you can see which devices were unused (zero usage - minutes and data).
    - Follow up on results (there is much devil in the detail)

Policies and Procedures for Mobile Device Programs

Cotton & Company
Answers Questioned

- Effective internal controls starts with policies and procedures
  - These will differ greatly depending on whether BYOD program exists or not.
  - These will also differ based on whether the organization uses a mobile device management software solution or not.

Policies and Procedures for Mobile Device Programs

Cotton & Company
Answers Questioned

- Key elements of mobile device policies and procedures include
  - Appropriate usage – this is foundational and often includes
    - What networks you can connect to
    - Personal vs business usage
    - Appropriate applications to use
  - Technical configurations (encryption, passwords, software updates etc.)
  - Incident response (if a phone is lost or compromised)

Policies and Procedures for Mobile Device Programs

Cotton & Company
Answers Questioned

- Immediate steps to take
  - Gap analysis of current mobile device policies and procedures against best practices.

Securing Mobile Devices

Cotton & Company
Answers Questioned

- Specifically, securing devices, applications, communications, and data
- A standard device configuration is the most efficient and typically most effective way to secure devices.
  - Within the standard build, don't allow end users to change settings.
    - This ensures the standard configuration is maintained
  - A standard configuration allows administrators to prepare devices quickly.

Securing Mobile Devices

Cotton& Company
Answers Questioned

- Control the application store
  - With some technology, the app store can be controlled so that only business appropriate applications are used.
    - This mitigates risks around appropriate usage and reputational risk.

Securing Mobile Devices

Cotton & Company
Answers Questioned

- You will have different security considerations and approaches for BYOD programs.
  - This needs to be weighed when first devising and implementing a mobile device program and determining whether to issue phones or BYOD.

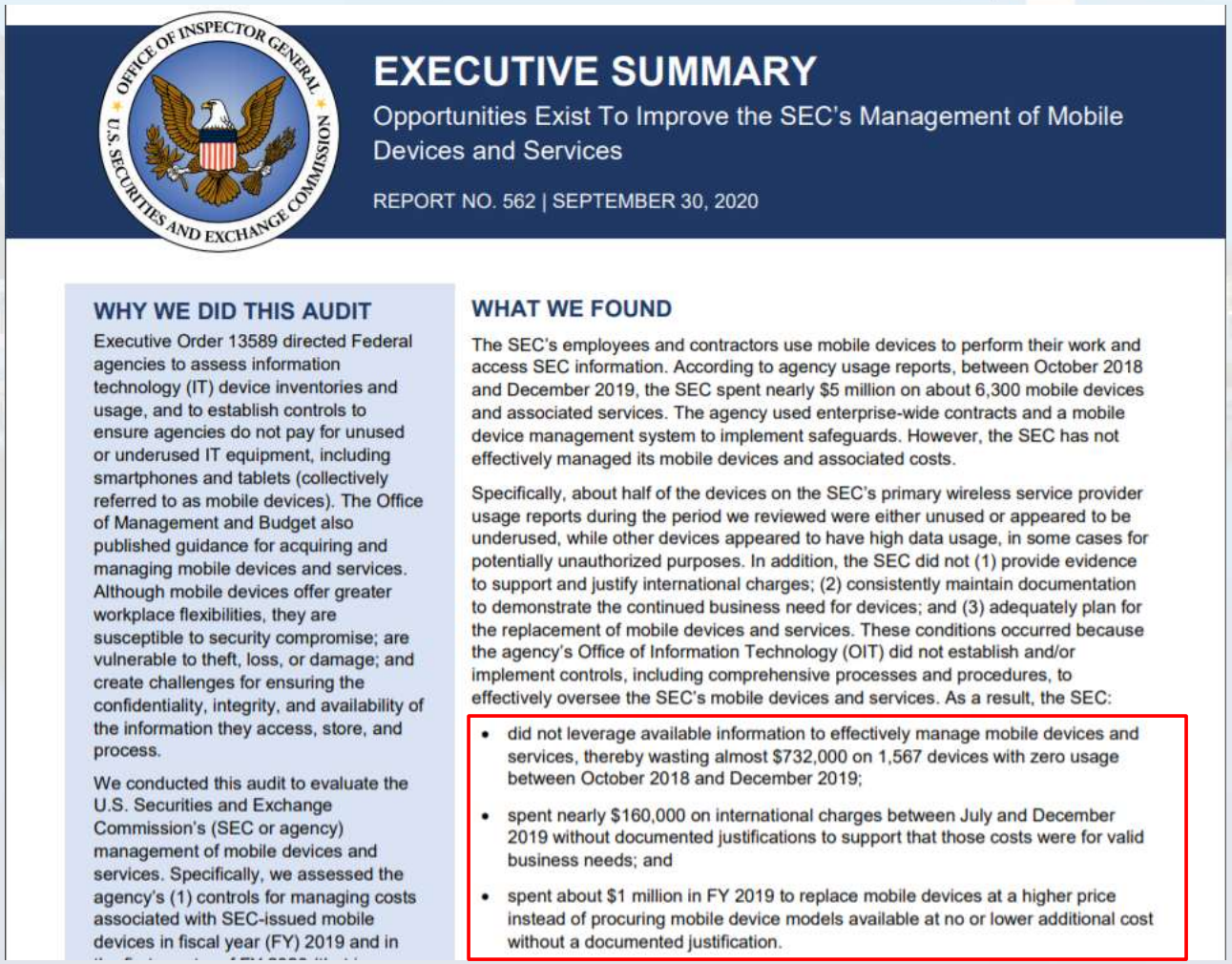
Securing Mobile Devices

Cotton & Company
Answers Questioned

- Immediate step to take
  - Determine whether a standard, technical configuration is in place.
    - There are some standard configurations to compare against for devices running Apple's iOS to assist.

Wrap-up

Cotton & Company
Answers Questioned



EXECUTIVE SUMMARY

Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services

REPORT NO. 562 | SEPTEMBER 30, 2020

WHY WE DID THIS AUDIT

Executive Order 13589 directed Federal agencies to assess information technology (IT) device inventories and usage, and to establish controls to ensure agencies do not pay for unused or underused IT equipment, including smartphones and tablets (collectively referred to as mobile devices). The Office of Management and Budget also published guidance for acquiring and managing mobile devices and services. Although mobile devices offer greater workplace flexibilities, they are susceptible to security compromise; are vulnerable to theft, loss, or damage; and create challenges for ensuring the confidentiality, integrity, and availability of the information they access, store, and process.

We conducted this audit to evaluate the U.S. Securities and Exchange Commission's (SEC or agency) management of mobile devices and services. Specifically, we assessed the agency's (1) controls for managing costs associated with SEC-issued mobile devices in fiscal year (FY) 2019 and in

WHAT WE FOUND

The SEC's employees and contractors use mobile devices to perform their work and access SEC information. According to agency usage reports, between October 2018 and December 2019, the SEC spent nearly $5 million on about 6,300 mobile devices and associated services. The agency used enterprise-wide contracts and a mobile device management system to implement safeguards. However, the SEC has not effectively managed its mobile devices and associated costs.

Specifically, about half of the devices on the SEC's primary wireless service provider usage reports during the period we reviewed were either unused or appeared to be underused, while other devices appeared to have high data usage, in some cases for potentially unauthorized purposes. In addition, the SEC did not (1) provide evidence to support and justify international charges; (2) consistently maintain documentation to demonstrate the continued business need for devices; and (3) adequately plan for the replacement of mobile devices and services. These conditions occurred because the agency's Office of Information Technology (OIT) did not establish and/or implement controls, including comprehensive processes and procedures, to effectively oversee the SEC's mobile devices and services. As a result, the SEC:

- did not leverage available information to effectively manage mobile devices and services, thereby wasting almost $732,000 on 1,567 devices with zero usage between October 2018 and December 2019;
- spent nearly $160,000 on international charges between July and December 2019 without documented justifications to support that those costs were for valid business needs; and
- spent about $1 million in FY 2019 to replace mobile devices at a higher price instead of procuring mobile device models available at no or lower additional cost without a documented justification.

Wrap-up

Cotton & Company
Answers Questioned

- An assessment of mobile devices can pay for itself
  - Strong likelihood of questioned costs/funds put to better use
- This cybersecurity-related topic is a high visibility, high priority area of the Federal Government
  - Get ahead of potential issues by assessing this area

Wrap-up

Cotton & Company
Answers Questioned

- What we presented to you today is just a small segment of telecommunications spend. There are companies dedicated to telecom expense management (TEM) and will help to reduce wasteful telecom spend that nearly every large organization has.