Mobile Security Companion

to

the CIS Critical Security Controls *(Version 6)*

Mobile Security Companion to the CIS Critical Security Controls (Version 6)

Introduction

Mobile devices are starting to replace laptops for regular business use. Organizations are building or porting their applications to mobile platforms, so users are increasingly accessing the same data with mobile as with their laptops. Also, organizations have increasingly implemented Bring Your Own Device (BYOD) policies to manage this trend.

However, many organizations have been struggling with the increase of personal mobile devices, and don't fully understand the security risks they may bring. There are concerns that their compact size makes them easy to lose, that they run newer operating systems that don't have decades of use and examination to uncover their weaknesses, and that there are millions of potentially malicious mobile applications that access data, spy on users, steal credentials, act as ransomware, or even become part of a Distributed Denial of Service (DDOS) botnet.

Like with traditional PC platforms, mobile still has to worry about protecting data from unauthorized access at rest and in transit; traditional network level man-in-the-middle attacks on public Wi-Fi; and similar web application threats (since mobile apps frequently access the same server endpoints as web applications). Employees today may use their mobile devices to perform the same business functions and access the same data as their PCs or laptops; but what is different is they are not physically connected to the corporate network, and likely, not even logged into the corporate domain. There are times when organizations use mobile VPNs to access the corporate network, but more and more frequently, mobile users access cloud services. It is not uncommon for corporate mobile users to access numerous cloud-based applications that reside outside their enterprise. Each of these has its own credentials, again rarely linked to enterprise. Getting visibility on the configuration, threats and behavior of these mobile devices is a challenge, since there are no "eyes" on the device like those attached to the network.

But it doesn't mean you can't track the threats and risks. One great thing about the Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.0 (*CIS Controls*) is that they are universal and high level enough to apply to any technology implementation. Everyone needs to start with: "What do I have?" "What is the configuration?" and "What risks do I need to address?" Basically 1 – 3 of the *CIS Controls.* We have to know what we have to protect it.

The real challenge to mobile security is the multitude of different mobile devices. With desktops, we mostly have commodity hardware running less than half a dozen different operating systems, and through conscientious configuration management, usually a single or only a few different OS versions. Mobile has (generally) 4 different software platforms (in US, more worldwide), with dozens of different hardware vendors, and dozens of different carriers (that do affect the platforms). Just looking at Android, there are 11 OS version families (from Cupcake to Marshmallow, with subversions under them), which on most devices are non-upgradable or forward compatible that might exist on these dozen of hardware platforms and carriers. So the permutations get enormous, and understanding the risks of each of these becomes overwhelming. That's why, for enterprises that have strict security requirements, it's still best to just issue standard devices.

Within the *CIS Controls*, you can see application security (CSC 6), wireless device control (CSC 7), and data loss prevention (CSC 17) all are relevant to mobile. Restricted use of admin rights (CSC 12) is also something that could be implemented, some MDM and mobile security platforms, especially on iOS, have the ability to restrict admin privileges to end users, which will prevent removal of security protections or monitoring. Malware defenses (CSC 5) are very different than traditional PC platforms. We can also apply secure configurations (CSC 10), limit insecure features and functionality (CSC 11), and even provide cloud based boundary defense (CSC 13). All of these areas will be described in more detail in the table below.   Using the *CIS Controls* can be the framework to develop a security method and process to manage mobile security risks in your organization.

Description

If you follow simple security steps: not Rooting or Jailbreaking your device; only get apps from Google Play or Apple Store, not 3rd party stores, or own Enterprise app store; being wary of any app wanting to install a Profile on your mobile device, as well as if there is an “Untrusted App Developer” popup for the app; and not leaving an unlocked phone for long periods of time, you can reduce the likelihood from most Mobile threats. But for specifics for each Control, the table below details the control’s applicability to mobile and specific challenges and considerations for implementation of that control.

CIS Critical Security Controls (Version 6): Mobile Security

CIS Critical Security Controls (Version 6): Mobile Security			
CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
1	Inventory of Authorized and Unauthorized Devices	One must have knowledge of all devices used to access data and resources in the organization. Mobile devices aren’t perpetually attached to the corporate network like other IT systems, so new methods need to be used to maintain the inventory.	An organization can’t get an inventory of mobile devices by running a scan to discover what mobile devices are connected; companies can use email accounts, or ActiveSync to determine what mobile devices are used to access email (which is most popular application for mobile devices). Also, Mobile Device Management (MDM) can support this by installing agents on the mobile devices to push down configuration and security profiles, monitor devices for configuration changes, and provide access controls based on policy.
2	Inventory of Authorized and Unauthorized Software	There are millions of mobile apps across dozens of different platforms. Mobile apps can bring risks and threats to data and credentials. Being able to know what is installed, and	MDM tools can inventory apps, and set policies and whitelisting to promote use of secure versions of apps. However there are privacy considerations in Bring Your Own Device (BYOD) scenarios, as the company may not need to

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
		control access to malicious apps, and insecure versions of apps is important to protect the organization.	know what apps an individual has installed on their personal device for personal use.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Like with PCs, secure configurations and monitoring of these configurations are critical to maintain trust with these devices.	MDMs can restrict access to cameras, white-list Wi-Fi networks, apply password policy enforcement, and inventory what apps are installed. Be aware, this last feature can be a privacy issue in a BYOD scenario. A company may not want the liability of knowing or having access to employee's personal email, apps that track health information, financial data, personal contacts and calendars, apps used in their personal lifestyle, or their location. MDM tools can scale to hundreds of thousands of devices, and provide the necessary monitoring to be alerted when devices are out of compliance; for instance, if someone installs an unauthorized application, turns off encryption, or jailbreaks or roots their device.
4	Continuous Vulnerability Assessment and Remediation	Mobile vulnerabilities are usually linked to versions of the Operating system, or malicious apps. Since mobile devices aren't attached to the network, you can't identify and manage vulnerabilities like you do on PCs, servers, or other networked devices.	One can't just run vulnerability scans on a network to scrutinize the mobile devices. Therefore, mobile vulnerability assessments must incorporate threat modeling, and understanding the devices, data, users, and their behaviors. MDMs can play a key role in gathering the information for the "what" and "who" for mobile management. Also, there are number of mobile security point solutions that address strong authentication, data and application security,

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
		Mobile vulnerabilities also can apply to many layers; hardware, OS (version), OS (configuration), individual application (of which there are potentially millions), network connection (cellular, Bluetooth, WiFi, NFC), app stores, physical location (i.e., countries where the government monitors mobile devices) and finally, whether the device is corporate-owned or personal (privacy requirements).	security of data at rest and in transit, and protection from network based threats when connected to Wi-Fi, such as man-in-the-middle attacks. Companies can choose to outsource management of their MDM platform and mobile support, similar to using Managed Security Service Providers (MSSPs) to monitor and manage network security devices.
5	Controlled Use of Administrative Privileges	Many intrusions use valid credentials obtained either through social engineering, or captured by other means. One important risk in mobile is protecting credentials stored on the device, because a user's email account could also a system or Domain Admin account. Also, Admin control is different in mobile devices. Malicious apps are taking advantage of unfamiliarity with the mobile admin levels, and there are malicious Android apps that obtain admin rights so they can hide themselves from the user.	Mobile devices are part of the network based on their credentials, not based on their connection. It might not be possible to control admin rights on mobile devices, especially in a BYOD situation; but access based on least privilege may apply. It's dangerous to allow users to Root or JailBreak mobile devices, because it opens up risks to vulnerabilities running at that lowest level.

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
6	Maintenance, Monitoring & Analysis of Audit Logs	Monitoring is irrelevant if there isn't a process to identify events and respond to them. And this response must be matched with the potential impact of the event. This is the human aspect: determining what events or alerts can potentially damage the organization, and execute response in a timely fashion based on that.	MDM and mobile security tools can provide visibility by having agents on phones that send events and alerts to a central server. These can be integrated with traditional Security Operations platforms. Different types of mobile monitoring sources can provide different data. MDMs use the more traditional network operations type of approach: Is the device live? What is the make model and version? Is it up to date? What applications are installed? Has the device been rooted or jailbroken? How much traffic is it sending and receiving? The security tools have more granular logging, such as installation of known bad or suspicious applications, application-level changes to data, network routing changes, SSL certificates used, VPN launching, and in the case of cloud filtering; traditional perimeter gateway logs for web traffic, or other application traffic. There is also the practice of monitoring account connections to the network domain or a specific application. Metrics should be actionable, not just "how many" of an event happened. More effective things to track are: Am I getting data from everything I should (how many devices are sending events)? Is the right data being collected (are all data logs the correct ones)? Another item to track is the turnover rate of my mobile devices, which is much higher than laptops. You will find user accounts having multiple devices attributed to them.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
7	Email and Web Browser Protections	Mobile devices change the traditional enterprise architecture by not only extending it outside a traditional perimeter, but also bypassing the need to route much or all traffic through the enterprise network due to use of cloud services. However, web and email threats are still a concern with mobile devices.	Traditional email gateway security controls for SPAM and phishing reduction, and malware and malicious URL links apply to mobile. Mobile security tools use an agent-based approach that gives a view to threats on and to the mobile device, such as malicious applications and profiles, and malicious WiFi networks or Man in the Middle web proxy attacks. There are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
8	Malware Defenses	Mobile doesn't have same concept of malware as with PCs. Mobile malware is really about malicious apps. It takes more diligence to understand current threats, and the behavior of known malicious apps, which often are re-packaged legitimate apps. Preventing the user from installing these apps, intentionally or unintentionally is key. From a BYOD perspective, personal phones are a greater risk, as users download a larger number of apps for personal use than business use. Also, mobile devices themselves are also risks to PCs. Email attachments forwarded from mobile devices might have PC malware that doesn't affect the mobile device, but could infect the PC. Mobile devices connected via USB to a PC could also have malicious PC files as they can act as removable media. PC AV also cannot always scan mobile devices like a traditional USB drive.	Traditional techniques of using Anti-Virus (AV) do not apply to mobile. AV is not feasible on iOS, due to the platform not allowing access at a level where applications can have general knowledge about other applications running on the device, and many argue that it is equally not effective on Android. Most iOS vulnerabilities only affect jailbroken devices; but that is recently becoming less true. Application whitelisting is a common approach to mitigate malicious apps. But user behavior is also important. Users must not install Profiles for apps that shouldn't require one. There are mobile security tools that scrutinize apps for validate if they are legitimate, and compare versions to known-bad repackaged apps. Traditional PC USB port monitoring can help with threat of mobile device connected to PC.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
9	Limitations and Control of Network Ports, Protocols and Services	The concept of network ports and protocols don’t apply to Mobile like they do to PCs. The only correlation is the turning on of different wireless interfaces, such as WiFi, Bluetooth, or Near Field Communications (NFC). These should be controlled, as they my broadcast presence of the mobile device to the surrounding area.	Traditional guidance on limiting interfaces to only those required for purpose, and restricting viewing or connecting to these interfaces apply.
10	Data Recovery Capability	Data recovery has always been inherent to the mobile process; unlike with PCs. Mobile devices are replaced on a more frequent basis. And with portability comes ease of loss, damage, or theft. So, mobile has always had the ability to backup data (mostly to the cloud) for easy transfer of contacts and phone numbers, or restoration of data to a new device, which promotes testing the restore process.	One should verify and review backup (e.g., iCloud) settings to make sure it’s backing up what is needed, and not what it shouldn’t. This might include corporate email, corporate contacts or calendar, or documents to personal backup. The former would be stored on the corporate Exchange server already. There might be corporate policy against backing up this data to a public cloud. Also, ensure there is a good password or strong credentials protecting that cloud backup.
11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	This section has less little direct affect on mobile security. There is guidance on WiFi security, but it applies to all computing devices.	

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
12	Boundary Defense	Mobile devices remove the concept of the infrastructure boundary by often accessing cloud-based services directly, without routing through corporate infrastructure. However, Boundary Defense applies to Mobile as traditional firewall restrictions, security monitoring sensors, email, web gateway filters, IDS and IPS alerts, and proper logging of events and alerts to feed the incident response process are all important. These can be implemented in a cloud-filtering infrastructure where mobile devices are routed instead of through the enterprise. Coordination or integration with cloud vendors can implement change control to customize these rules, or performing the same with direct control of these rules will be required. Consider these filters an extension of your perimeter, and apply the same rigor to applying of policy, change control, and system monitoring.	Organizations can choose to VPN Mobile traffic to their infrastructure, where traditional boundary defense guidance applies. However, there are also tools and approaches that funnel mobile traffic through filtering cloud infrastructures that perform web gateway filtering and security functions.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
13	Data Protection	Almost all mobile devices have the ability to encrypt their data at rest, and include a PIN or password (or biometric) to restrict access. Some devices can link encryption or identity to a hardware root of trust. Mobile devices can use traditional VPNs for network or application access. Though most mobile applications store data in cloud, which could require partner or vendor protection requirements built into the agreement. We also need to look at the entire data supply chain, not just at collection points. Is this data flowing to a back end system? Is data stored in multiple places? Is this data in a cloud? In what country is this data stored (for privacy considerations)?	Traditional guidance on encrypting data one the devices, and using a VPN with good encryption for protecting sensitive data in transit still apply to Mobile. There are VPNs that allow mobile devices to connect to corporate network to access applications or data shares, as well as application specific VPNs that encrypt the data in transit for that application. Some of these technologies include a hardware component, such as a microSD chip, for encryption key management. Traditional enterprise Data Loss Prevention can be helpful for email and network stored data. But cloud applications and data may be more difficult to get visibility from mobile device and user access. There are tools that leverage cloud service APIs to gain this visibility, or filtering clouds that proxy mobile users to these external services, which can provide a source for data access controls. Organizations with Bring Your Own Device (BYOD) programs will need to consider end user privacy implications within policies and security monitoring and operations procedures.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
14	Controlled Access Based on the Need to Know	This control is has no specific application to Mobile, as the concept of controlled access to data is universal for different data access. Since mobile devices are more personal devices, and don’t usually store data like PCs, access controls are at closer to where the data is stored.	Traditional access and authorization control guidance applies to Mobile.
15	Wireless Access Control	WiFi controls still apply to Mobile, such as restricting connection to only authorized devices, and use of encryption and authentication, but with mobile devices wireless includes cellular, Bluetooth, and potentially NFC as well. Unlike with PCs, there is limited risk to remote connection to the device, like connecting via Telnet or SSH to the mobile device, like on a PC; but, there are network level man-in-the-middle attacks, which can sniff unencrypted traffic, or re-route traffic to insecure web sites that can steal credentials.	Traditional guidance on WiFi security with use of strong credentials for connectivity, encrypted links, and restricting unauthorized device connectivity. Mobile security tools use an agent-based approach that gives a view to threats on and to the mobile device, such as malicious applications and profiles, alerting to malicious WiFi networks or Man in the Middle SSL/TLS web proxy attacks.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
16	Account Monitoring and Control	Account monitoring is performed mostly on enterprise platforms, and not on the mobile device. However, the always-remote access, and use of cloud-based applications not one the network can complicate visibility and auditing.	Many organizations are using cloud applications, like SalesForce, DropBox, or one of a hundred of others; those additional credentials will need to be disabled during employee separation as well. Keeping track of these external credentials might take management, or federating these credentials with identify management tools.
17	Security Skills Assessment and Appropriate Training to Fill Gaps	This control doesn't specifically apply to Mobile.	Training users and administrators on risks and threats specific to mobile platforms is prudent.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
18	Application Software Security	Many organizations are concerned about mobile application security, especially with the millions of apps available for personal and business use. Luckily, secure web application development and security testing has a long history, and directly applies to mobile apps. Many mobile apps are simply web based, while those using a native app running on the mobile device are just a client for a web-based application. Mobile primary application risks are the mobile apps themselves, attempting to access data on the phone, or in the case of Android, a few nasty applications can corrupt the underlying operation system in something called a rootkit, which then renders all OS behavior untrusted. Some additional threats for malicious native apps include affecting device itself by turning on the camera or microphone, accessing contacts or emails, logging geolocation, capturing credentials, initiating toll calls or texts, or nuisance issues like resource saturation that drains the battery.	We still recommend web application security techniques when building secure mobile apps, including following the Open Web Application Security Project (OWASP) Top 10. The quick win is to make sure you have the legitimate version of an app; and that it's up to date. Legitimate because if you don't download an app from the Apple App store or Google Play store, you are at much greater risk of installing a malicious app, or "evil twin" or "repackaged" version of the legitimate app you expected. Some of the other guidance, like error checking on user input, testing in-house and 3rd party apps, and hardening the back end all directly apply when developing secure mobile applications. Agent-based mobile security tools can also reduce the risk of malicious behavior of mobile apps, be preventing installing Profiles, or preventing Man in the Middle website request hijacking or redirect attacks.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
19	Incident Response and Management	Like with PCs, now that many users access company data and services with mobile devices, the need to identify, investigate, respond and recover from incidents involving mobile devices is important.	Traditional Incident response guidance applies to Mobile. This includes the need for planning, defining roles and responsibilities, and escalation path. You will also need to train operations personnel and incident responders on what to look for with unusual behavior on the mobile devices. Having visibility into mobile operations, such as we described previously in CSC 6, will help in identifying these events. One challenge is the vast quantity of different types mobile device hardware, even among generations of products. When talking about data forensics on mobile devices, there is a wealth of different types of data available to support the objective of the acquisition; be it eDiscovery, miss-use, or evidence collection to support a criminal case. People have their whole life on their phones, from calendar, phonebook, and to do list, to photos, video and voice recordings (including messages). There is the geolocation data from pictures, social networking check-ins and a few applications store ones “last active location.” You get the history of whom a person communicated with from phone logs, text messages, email, and social networking. For more information on mobile forensics procedures, you can refer to NIST SP 800-101 Guidelines on Mobile Device Forensics.

CIS Critical Security Controls (Version 6): Mobile Security

CSC #	Control Name	Applicability to Mobile	Mobile Security Challenges and Considerations
20	Penetration Tests and Red Team Exercises	With traditional Pen testing, the cycle of running scans to see what ports are open, and what services are running to see if there are vulnerable versions of those services to exploit doesn't apply. However, phishing and other social engineering are relevant to mobile.	There is the ability to sniff traffic over the air, perform man-in-the-middle on a mobile session, and even do application re-direction attacks; but the primary threat vectors are the mobile apps themselves, as discussed in CSC 18. The traditional approach for mobile app testing has been code review tools, but standard web proxy tools and web application penetration testing techniques apply. Use of test lab and devices for more thorough hardware examination is relevant to mobile.