CAB240 – Information Security

Bachelor of Information Technology
Queensland University of Technology
Semester 2, 2017

Student Name: John Santias
Student Number: n9983244

Mobile Phone Security Investigation Report Part I

Table of Contents

Executive Summary.. 3

Section 1 - Information Assets 3

Section 2 - Overview of use of device 4

Section 3 - Privacy Policy for an app used frequently 5

Section 4 - Security issue associated with a mobile device application 6

Section 5 - Security issue associated with a mobile device Operating System 7

Section 6 - Security issue associated with a mobile device user behaviour 8

Section 7 - Physical threat to a mobile phone 9

Section 8 - Conclusion 10

References 11

Appendices 12

Appendix A 12

Appendix B 13

Appendix C 14

Appendix D 15

Executive Summary

This document is an investigation about the security of mobile phones. People may not be aware of how critical their personal information is when attackers or strangers get it. This document explains an overview of a mobile device, the use that mobile device, the privacy policy of using your information from a popular social media page, the consequences or threats of getting your information stolen, the vulnerabilities of your device which attackers can attack through, and how they breach the security goals, confidentiality, integrity, and availability.

Section 1 – Information Assets

The Samsung Galaxy S6 Edge smartphone stores my information assets. It includes 32Gb of Internal memory to store data/files like phone contacts, memos, applications etc. Thus, also includes 3Gb of RAM that store programs to boot the smartphone and perform diagnostics. The phone is designed with a strong LCD curved screen, 1440 x 2560 pixels, that also includes a strong protection to prevent cracks, called Gorilla Glass 4. The phone also has two cameras, the primary camera which is located at the back of the phone is a 28mm 16MP camera function with LED flash. The secondary camera has a 22mm 5MP camera located above the LCD screen.

Its battery is a non-removable Li-lon 2550 mAh Battery capable of lasting up to 49 hours if the phone is set to power saving mode, and 17 hours on normal mode. For myself to communicate to others, my phone has LTE and WLAN to connect to the network, SMS and MMS functions to send messages, and Bluetooth to send and receive files directly to another connected device. GPS is also included to locate myself and NFC to exchange information when placing the device next to another device, and lastly, a micro USB to connect to a computer to transfer files.

The phone runs on the Android operating system (version 7 Nougat) which was released in Australia in July 2017. With the latest OS version, the user experience has been enhanced with a few new functions to use such as split screen, layouts, new fonts and notification transitions. It has also improved the most important part for smartphones, a better security hopefully to prevent vulnerability (Android Nougat – Wiki. 2017). Hundreds of applications have been installed on the smartphone and the system has its own apps preloaded. Most of the preloaded installed apps are for the phone to function and some other built in apps are useful everyday tools for the user (Phone, SMS, Clock, memo, camera etc). There are applications I have installed from the App Store which are mostly social media apps like Facebook, Snapchat, Instagram, Skype. There are also important apps that I use sometimes, the Commonwealth Bank app to manage my money and accounts, and the QUT app to view my timetable, messages, grades etc.

Almost all my downloaded applications have my personal information, however, those data aren't stored directly on my smartphone but rather, on the organization's database server. My Snapchat application does store data if I save a picture or a 10-second video that I have taken. A saved picture can use around 600-900MB of internal storage, the size of the file can depend on the width and height of the taken picture, same as the length of the video. Photos and videos take most of my phone's internal memory. However, I can create more space when transferring pictures and videos onto my external hard-drive. Even so, my files can also be uploaded to the Samsung cloud.

As music is one of my interest, I use the Spotify application to listen and download a whole bunch of music. This application still uses my phone's internal memory to store downloaded music. This application can eliminate the use of storage by not downloading anything and just stream using the internet or data. However, streaming uses a big load of data. Spotify also uses a majority of my phone's internal memory, about 8-10Gb of music downloaded.

Section 2 – Overview of use of device

There is so much importance in my valuable asset, my Samsung Galaxy S6 edge. In the case of losing it, all my information and data stored on the phone can be compromised to some stranger. There are a couple of ways in what a stranger might do to my asset. If lucky enough, it could be returned to a shop or police station, however, in most cases, that wouldn't happen.

The stranger could try to break into the phone by unlocking it and going through my own personal data and information like my social accounts, photos, videos, bank accounts, etc, this can be referred to Confidentiality of the C.I.A. security goals or services. The intruder can view all my personal data which I would not like intruders to see, it's valuable personal stuff. The stranger could do also change my information on my social accounts etc. This breaches Integrity of the C.I.A security goals, as the user is modifying my information. This can also lead to being locked out of my accounts if my password was changed.

The last CIA security goal, Accessibility, can be referred to the stranger closing all my accounts or changing passwords which prevent me from being able to access my accounts. This prevents me from communicating with other friends on social media and my friends can be tricked into thinking that the stranger is me.

Almost all my most frequently used apps that I use stores or has my information which can be compromised. My most frequently used apps are Facebook, Snapchat, Instagram, Messenger, Spotify. All these apps, have my information and are all linked to each other by Facebook. The use of my Facebook account to automatically create another account on other apps is common. These applications are very critical as they all share the same information from Facebook. If the stranger can get my login information, he would be able to access all the other accounts associated with it.

The applications that I use less are google maps, commonwealth bank, the QUT app, a few games, and some system apps (clock, contacts, microphone etc). Although they may be used less, these apps still have important information and data like the contacts app which has my friend's contact information which can be passed on to other strangers for them to try to get info. Also, google maps may record my search history of directions to places and strangers could find out where I live by going through this app. Lastly, the Commonwealth

Bank App is very important as it manages my accounts. The intruder can access my accounts transfer all my money

No matter how much I use applications, they mostly have my information and data that can be taken if a stranger was to break into my phone.

Section 3 – Privacy Policy for an app used frequently

Facebook aims to make the world more open and connected. With the use of their social services, our information becomes part of their organization. Facebook collects information from its users from the creating of the user's account by filling in personal details to the use of Facebook's services. Users can communicate with others, share content like photos, videos, statuses, your location, read and watch friend's posts and much more. However, for every activity you do, Facebook records/collect it. Even so, they also collect information on our interactions with groups and other people, the transactions made through Facebook (meaning they record your credit or debit card information, shipping, and contact details), the device that you use to access their services, third party websites, and partners (Facebook, 2016).

For any activity on their social media page, or other associated websites, apps, or third-parties. Facebook records every bit automatically and stores it on their DataCenter (PSafe Blog, 2017).

The information we give to Facebook can be helpful to the improvement and development of their services. For example, your information helps your friends suggest who to tag in a photo by face matching, or suggest a credit/reference to a person who has shared or reposted your content. Using the information given, it provides better communication between the users, by selecting ads that are relevant to our interests.
Our information also provides better safety and security for their account (Facebook, 2016).

Facebook also analyses our information, selects and project advertisements on our social feed. Each ad and services are measured to its effectiveness on users (Facebook, 2016). Facebook uses our information to improve the safety and security of the accounts by locating the user, thus they can detect whether your account has been hacked or the account has been accessed overseas. They can detect if the account has been accessed on an unauthorized device by comparing the device to their collected data.

The collected information is stored for as long as necessary, as they need it to provide the services and products wanted by the user (Facebook, 2016). My information is kept until I have deleted my account. The information that they've recorded is stored in their data centers which run servers that load up their web pages, services, products, and information (The New Stack, 2017).

People you communicate with can see your content and information. The user can decide who can view their content and information by setting their posts to the public, or just friends, or their self. People who can see your content may be able to share it with their own connected friends meaning people you do not know are able to view that content. Facebook also have other companies that are part of their organization, which means the other connected companies have your information. The collected information can also be shared with applications, websites, and third-parties that are using Facebook's services. Our information can be passed on from Facebook to automatically fill in details to use the other company's services (Facebook, 2016).

The information that they've collected is not under Facebook's control. The user controls their own account. With my account still being active and tracked, the information is still in Facebook's database. I can access Facebook's activity log tool to manage the content and information generated through my activities on Facebook. In the case of wanting to delete all my information, I would have to delete my account.

Section 4 – Security issue associated with a mobile device application

Title: Police issue child safety warning over Snapchat maps update that reveals users' locations

Author: Matthew Field

Reference details: The Telegraph. 2017. *Police issue child safety warning over Snapchat maps update that reveals users' locations.* [ONLINE] Available at: http://www.telegraph.co.uk/technology/2017/06/23/police-issue-child-safety-warning-snapchat-maps-update-reveals/. [Accessed 21 August 2017].

Brief summary: Snapchat released a new feature on its own app where users can view their friend's locations. This can be seen when the user enables their GPS location and pinching the photo screen to view the map. In the article it states a warning to parents to turn off the Snap map on their children's snapchat account as it can show the user's location to anyone on their contact lists (#5) or set their location to Ghost mode, where no one can see where you are.

Information asset: The information asset involved is the user's location. Contacts or friends can view each other's location on the map.

Security issue:

- **Threat:** The ability to have the users' location shown to the public can allow contacts to pinpoint where the user lives, go to school or spend time. Another threat of this security issue is that if the user has added unknown contacts, that contact could have the potential of causing harm by looking at where the user is and going to that user. By not preventing the threats, there is a potential of child abduction or stalking users under 18.
- **Vulnerability**: Enabling the user's location can allow others to pinpoint you and track you. Unknown contacts can be dangerous as they may want to know more about you through viewing your snapchat story and location. The users' privacy may be

public which may even put personal security at risk, again unknown people can see the user.

- In the event of showing the user's location, this compromises the user's confidentiality of the security goal, where contacts can find out where you live. This meaning they can reveal your address or even find out the common places that you go to often.

To prevent these security issues, it is best to have contacts that the user personally knows, set privacy to private, and turn on Ghost mode or not have the GPS located.

Section 5 – Security issue associated with a mobile device operating system

Title: Trump's still using his old Android phone. That's very very risky.

Author: Lily Hay Newman

Reference details: WIRED. 2017. *Trump's Android Phone Is a Major Security Concern* | WIRED. [ONLINE] Available at: https://www.wired.com/2017/01/trump-android-phone-security-threat/. [Accessed 21 August 2017].

Brief summary: Google releases updates for Android phones every month, however, not all phones are able to get the update as it may affect the device's themes, skin, features etc. There are many phone brands that run androids such as HTC, LG, Samsung, Huawei and much more. However, not all these brands are able to apply the latest updates to their own phones. The reason for this is that not all android phones run the same phone brand, they are all different, and there are a lot of old phones. Therefore, updates are difficult to apply (#6). Updates are important for phones as it fixes bugs and improves the security of your phone from getting infected with a virus. Not all phones are able to get the recent update as the phone may still be in the process of finding out how to apply the update without damaging the original skin etc (#6).

In the article, Trump still uses an old Android phone which has many vulnerabilities and threats because the phone is not protected from attacks.

Information asset: The information stored on Trump's phone include his friend's contact details in which attackers can target, IDs and passwords used to log in to American government files and emails etc, possibly missile launch codes and confidential files.

Security issue:

- **Threat:** The threat for having an old phone, is if Trump's clicks on a malicious link or attachment, his device can easily be compromised. This can lead to having his phone tracked, attackers watching, listening through the phone's camera and microphone, personal accounts and data being exposed. The confidential information that attackers get can later be used for blackmailing Trump and his government.
- **Vulnerability**: The vulnerabilities in this issue are having an old outdated phone, which attackers can compromise information on the device. The gathered confidential information can be shown to the public.

- **Security issue/attack**: An active attack is possible after the user has gained control of Trump's phone, in which the attacker can watch every activity like watching him sign in to confidential data using his ID and password, allowing him to record or note it down.
- The hacker's goal of breaking into Trump's phone to view his personal information and data is a breach of the security goal, confidentiality. Even so, the hacker can track the phone's location, determining where he himself can be any time (#6).
  The availability security goal can also be breached if the attacker manages to get the data/information and delete every information on Trump's phone, this leads to having no information left that Trump can find.

To prevent Trump's phone from being compromised, it is best to get a new up-to-date smartphone that minimizes the vulnerabilities or allow the manufacturing company to apply the updates to old phones.

Section 6 – Security issue associated with mobile device user behaviour

Title: Five new threats to your mobile device security

Author: Stacy Collett

Reference details: Stacy Collett. 2017. Five new threats to your mobile device security | CSO Online. [ONLINE] Available at: http://www.csoonline.com/article/2157785/data-protection/data-protection-five-new-threats-to-your-mobile-device-security.html. [Accessed 22 August 2017].

Brief summary: Malware, also known as malicious software, targets computers or mobile device systems (smartphones or tablet) to control it remotely or steal personal information stored on the device. Today, malware incidents continue to increase and affect millions of users. No user is immune to this and operating systems such as Android, Apple and more aims to prevent their customer phones being infected with malware and other types of viruses (#7).

Information asset: The information involved in the stored username and passwords on devices used to automatically sign in to online accounts. Such information like documents and files can be taken by attackers using the viruses they were able to put on the person's device.

Security issue:

- **Threat:** When a user installs a new application from an unidentified developer, there is a great potential that the application has malware hiding behind without the user knowing. This malware can get the device either rooted or not, then have a proxied IP address and click on ads automatically. Another threat is that they can also steal your IDs and passwords stored on your phone (#7). This is known as Mobile Botnets, which hackers can get your information and generate revenue by pretending to be the user accessing the ads. The ad and click fraud are a growing concern because more users are falling for the trap. This trap starts off with an SMS Phish sent to the user, and if the user clicks on the link, it will automatically download a malicious app. This then allows the hacker to control the smartphone and steal credentials and information. This is a threat where just one small click on a Phishing SMS or link can lead to the user's information being exposed and losing control of their phone (#7). Dead apps can also be a threat, which may still be lying somewhere on the phone. The threat of this is that dead apps can lead to leaking data to third parties or even creating malware.

- **Vulnerability**: Downloading things from the internet especially from unsafe websites are vulnerabilities. Most people are not aware of the risks of getting attacked. Users can download random things to meet their needs which can lead to getting a virus. When users get a virus on their phone by clicking a phishing link or downloading unidentified things etc, it allows the author of the virus to control the infected device and obtain user's personal information.
- **Security issue/attack**: To monitor the user and gain information about the target is a passive attack with the help of getting a virus especially malware.
- When the hacker gets onto the phone, this breaches the Confidentiality security goal, the hacker can look at the user's personal data information such as IDs, passwords, DOB etc. The availability security goal can also be breached when the hacker controls the phone and locks the user out by changing the password or closing the accounts.

People can prevent all these threats and vulnerabilities by adding a security software can prevent these risks and viruses getting on their phones. Also, updating phones and applications regularly, have download settings to only allow identified developers to download apps, user behaviour awareness and training.

Section 7 – Physical threat to mobile phone

Title: Always connected comes with risks

Author: Jaffee Larry

Reference details: ESOE secure resource verification. 2017. *ESOE secure resource verification.* [ONLINE] Available at: https://search-proquest-com.ezp01.library.qut.edu.au/docview/1863564286/fulltextPDF/E36B8E3EC638431BPQ/1?accountid=13380. [Accessed 22 August 2017].

Brief summary: Many organizations make their employees bring their own device (BYOD), as their employees may have much more advanced technologies than what the IT department offers (#8). Although these devices can help them progress in their work, these BYOD devices create more vulnerabilities, in other words, a weakness in the companies' system that an attacker can access or exploit.

In a survey respondent of American citizens using smartphones and tablets at businesses, about 59 percent use their device to access corporate data (#8), although the use of mobile phones is more common. There are risks to having employees use their own personal device, even greater risks when an employee loses or get their device stolen (#8).

When someone within the organization loses or gets their device stolen outside, the organization can receive threats from the person who may have picked it up. When that stranger gets the device, he/she will try to unlock the mobile phone or tablet.

Information asset: The information asset includes the organization's work data,

Security issue:

- **Threat:** When a person from an organization lose their phone to someone, this creates a threat to the company that a stranger knows how to access the company's files etc. Even so, intruders can put viruses to other connected devices in the company. When BYOD get infected with malware, ransomware or spyware etc. These threats lead to losing more work data and money.
- **Vulnerability**: The device may not be secure. The difficulty of unlocking a stolen device can depend on how updated or how old it is. If the device gets lost or stolen, the person picking it can decide to unlock and expose the data.
- **Security issue/attack**: The security issues is that phones can be easily unlocked depending on how secure it is and how the stranger utilises the stolen phone. Stolen devices can also lead to more threats.

Once the person gets into the phone, the intruder can view all information about the authorised user and corporate information. This breaches the confidentiality security goal as information is exposed. Lost or stolen devices can allow intruders to breach the availability security goal by taking data outside of the organization, leaving employees with no available information to continue working on (#8).

To prevent or minimize such threats and vulnerabilities, organizations should create policies on the use of personal devices at work so employees are more educated and aware (#8). Have tools that prevent data leakage, encrypted data or have anti-virus software.

Section 8 – Conclusion

The use of mobile phones continues to increase as more attackers aim to exploit stored information and data. With a use of mobile, people do not realize how critical or unsecured their mobile phone is until they have been attacked by a virus or when they lose their phone. In this investigation on mobile phones, we have determined that there are threats and vulnerabilities on the use of phones and they can breach the CIA security goals, Confidentiality, Integrity, and Availability. We have seen that Facebook collects our information for the improvement of their services and security. Having your GPS location on can create threats. An out dated or an old phone can help attackers get viruses on your phones, downloading things from unidentified developers can have viruses hiding behind. The risks of losing or getting your device stolen can lead to loss of company work data. All these security issues we have investigated can be prevented if mobile users are trained well and are aware of attackers getting your information. If users know how to protect their own phone, then the threats can be minimized so as the number of attackers.

References

Android Nougat - Wikipedia. 2017. *Android Nougat - Wikipedia*. [ONLINE] Available at: https://en.wikipedia.org/wiki/Android_Nougat#Features. [Accessed 01 September 2017].

Facebook. 2016. *Data Policy*. [ONLINE] Available at: https://www.facebook.com/about/privacy/#. [Accessed 1 September 2017].

PSafe Blog . 2017. *What Information Does Facebook Collect About Its Users?*. [ONLINE] Available at: http://www.psafe.com/en/blog/information-facebook-collect-users/. [Accessed 01 September 2017].

The New Stack. 2017. *How Facebook Does Storage - The New Stack*. [ONLINE] Available at: https://thenewstack.io/facebook-storage. [Accessed 01 September 2017].

The Telegraph. 2017. *Police issue child safety warning over Snapchat maps update that reveals users' locations.* [ONLINE] Available at: http://www.telegraph.co.uk/technology/2017/06/23/police-issue-child-safety-warning-snapchat-maps-update-reveals/. [Accessed 21 August 2017].

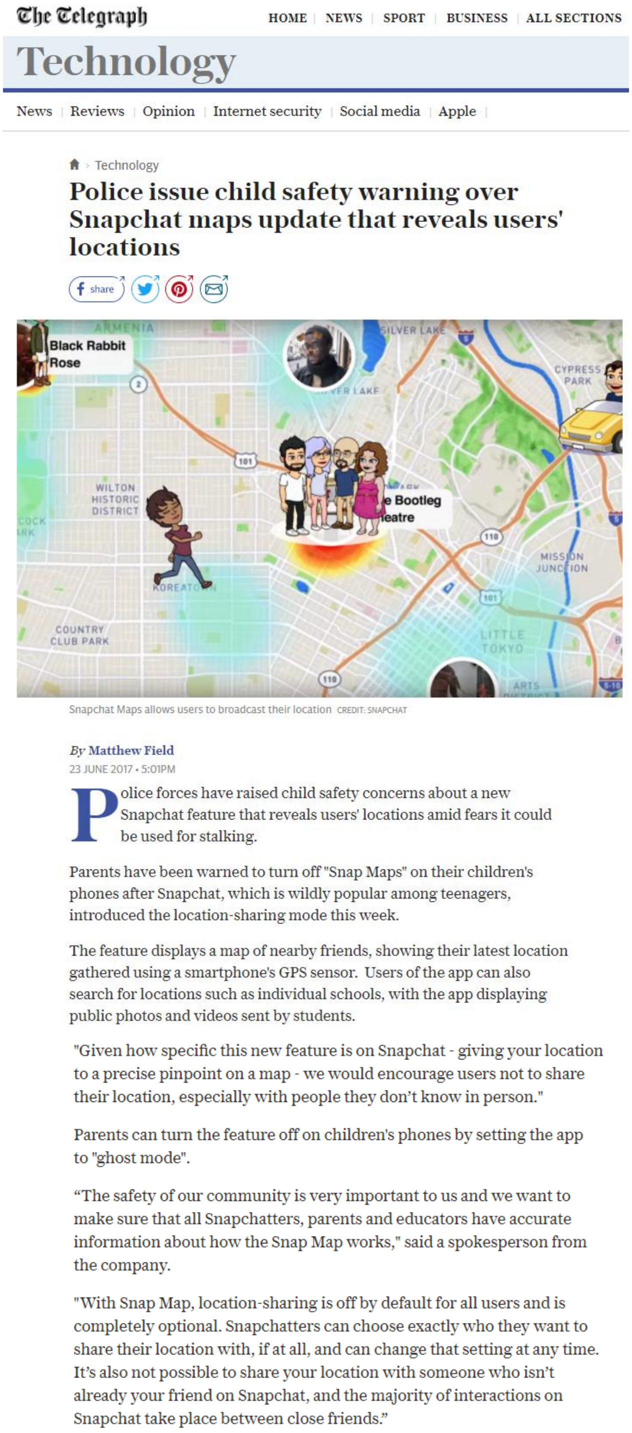
WIRED. 2017. *Trump's Android Phone Is a Major Security Concern* | WIRED. [ONLINE] Available at: https://www.wired.com/2017/01/trump-android-phone-security-threat/. [Accessed 21 August 2017].

Stacy Collett. 2017. Five new threats to your mobile device security | CSO Online. [ONLINE] Available at: http://www.csoonline.com/article/2157785/data-protection/data-protection-five-new-threats-to-your-mobile-device-security.html. [Accessed 22 August 2017].

ESOE secure resource verification. 2017. *ESOE secure resource verification.* [ONLINE] Available at: https://search-proquest-com.ezp01.library.qut.edu.au/docview/1863564286/fulltextPDF/E36B8E3EC638431BPQ/1?accountid=13380. [Accessed 22 August 2017].

Appendices

Appendix A:



Police issue child safety warning over Snapchat maps update that reveals users' locations

Snapchat Maps allows users to broadcast their location CREDIT: SNAPCHAT

By Matthew Field
23 JUNE 2017 • 5:01PM

Police forces have raised child safety concerns about a new Snapchat feature that reveals users' locations amid fears it could be used for stalking.

Parents have been warned to turn off "Snap Maps" on their children's phones after Snapchat, which is wildly popular among teenagers, introduced the location-sharing mode this week.

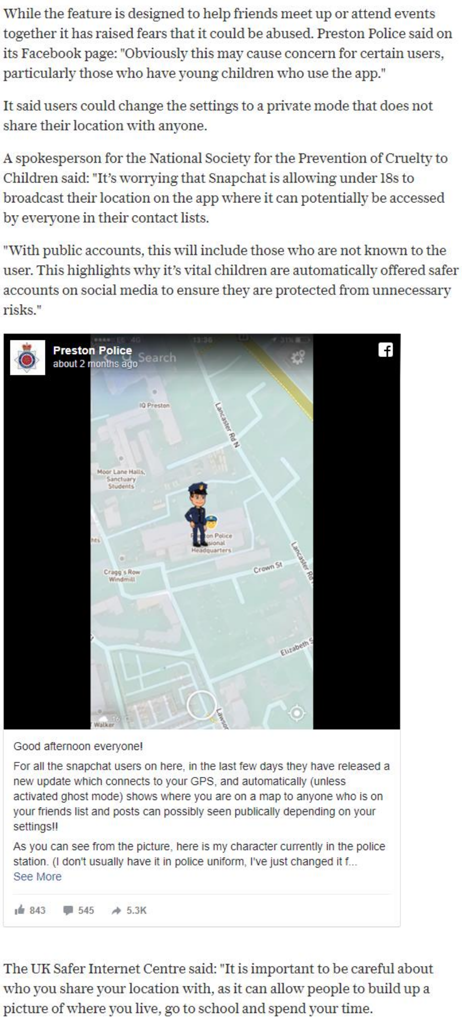
The feature displays a map of nearby friends, showing their latest location gathered using a smartphone's GPS sensor. Users of the app can also search for locations such as individual schools, with the app displaying public photos and videos sent by students.

"Given how specific this new feature is on Snapchat - giving your location to a precise pinpoint on a map - we would encourage users not to share their location, especially with people they don't know in person."

Parents can turn the feature off on children's phones by setting the app to "ghost mode".

"The safety of our community is very important to us and we want to make sure that all Snapchatters, parents and educators have accurate information about how the Snap Map works," said a spokesperson from the company.

"With Snap Map, location-sharing is off by default for all users and is completely optional. Snapchatters can choose exactly who they want to share their location with, if at all, and can change that setting at any time. It's also not possible to share your location with someone who isn't already your friend on Snapchat, and the majority of interactions on Snapchat take place between close friends."



While the feature is designed to help friends meet up or attend events together it has raised fears that it could be abused. Preston Police said on its Facebook page: "Obviously this may cause concern for certain users, particularly those who have young children who use the app."

It said users could change the settings to a private mode that does not share their location with anyone.

A spokesperson for the National Society for the Prevention of Cruelty to Children said: "It's worrying that Snapchat is allowing under 18s to broadcast their location on the app where it can potentially be accessed by everyone in their contact lists.

"With public accounts, this will include those who are not known to the user. This highlights why it's vital children are automatically offered safer accounts on social media to ensure they are protected from unnecessary risks."

Good afternoon everyone!

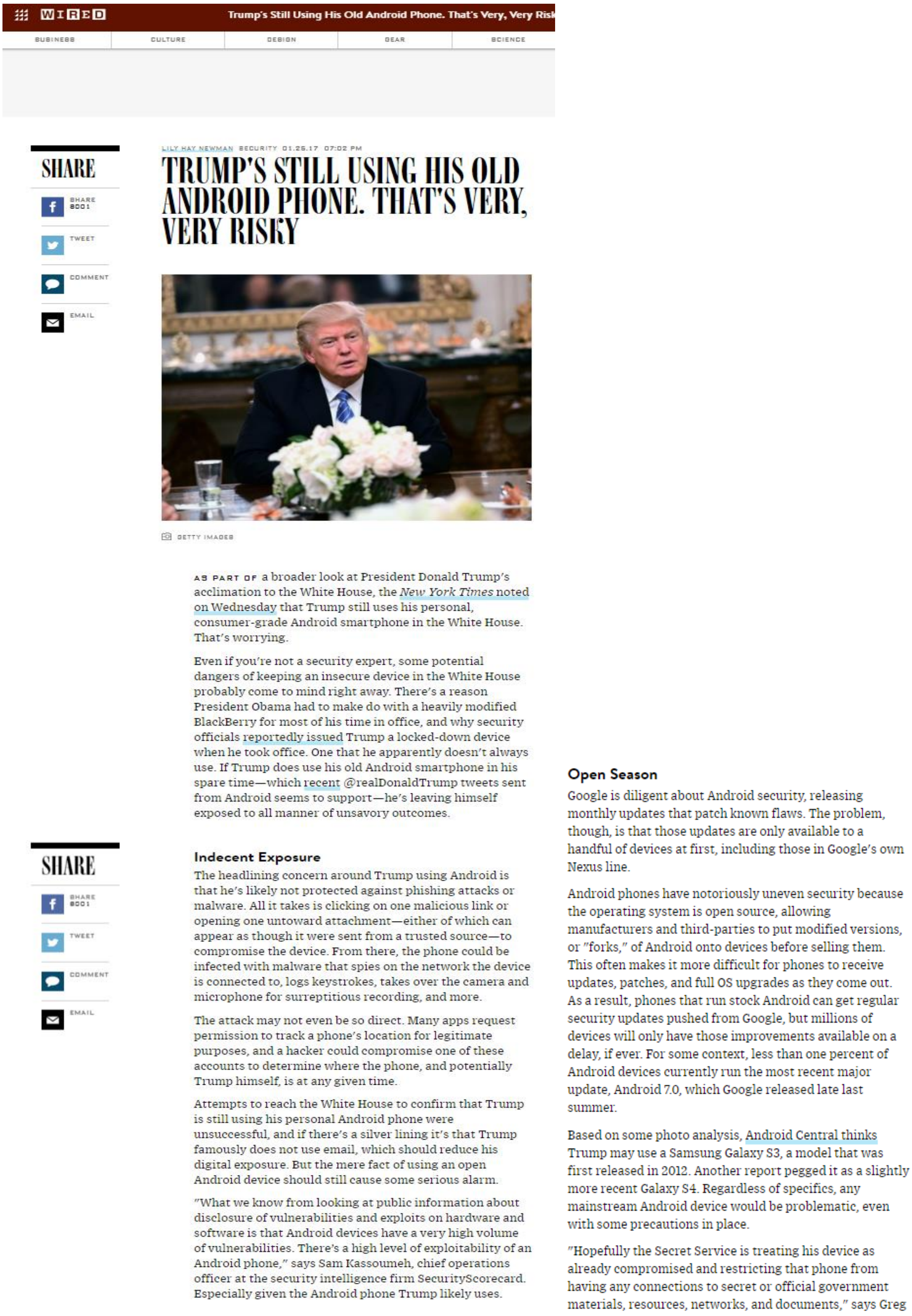
For all the snapchat users on here, in the last few days they have released a new update which connects to your GPS, and automatically (unless activated ghost mode) shows where you are on a map to anyone who is on your friends list and posts can possibly seen publically depending on your settings!!

As you can see from the picture, here is my character currently in the police station. (I don't usually have it in police uniform, I've just changed it f...
See More

843 545 5.3K

The UK Safer Internet Centre said: "It is important to be careful about who you share your location with, as it can allow people to build up a picture of where you live, go to school and spend your time.

Appendix B:



LILY HAY NEWMAN SECURITY 01.26.17 07:02 PM

TRUMP'S STILL USING HIS OLD ANDROID PHONE. THAT'S VERY, VERY RISKY

AS PART OF a broader look at President Donald Trump's acclimation to the White House, the *New York Times* noted on Wednesday that Trump still uses his personal, consumer-grade Android smartphone in the White House. That's worrying.

Even if you're not a security expert, some potential dangers of keeping an insecure device in the White House probably come to mind right away. There's a reason President Obama had to make do with a heavily modified BlackBerry for most of his time in office, and why security officials reportedly issued Trump a locked-down device when he took office. One that he apparently doesn't always use. If Trump does use his old Android smartphone in his spare time—which recent @realDonaldTrump tweets sent from Android seems to support—he's leaving himself exposed to all manner of unsavory outcomes.

Indecent Exposure

The headlining concern around Trump using Android is that he's likely not protected against phishing attacks or malware. All it takes is clicking on one malicious link or opening one untoward attachment—either of which can appear as though it were sent from a trusted source—to compromise the device. From there, the phone could be infected with malware that spies on the network the device is connected to, logs keystrokes, takes over the camera and microphone for surreptitious recording, and more.

The attack may not even be so direct. Many apps request permission to track a phone's location for legitimate purposes, and a hacker could compromise one of these accounts to determine where the phone, and potentially Trump himself, is at any given time.

Attempts to reach the White House to confirm that Trump is still using his personal Android phone were unsuccessful, and if there's a silver lining it's that Trump famously does not use email, which should reduce his digital exposure. But the mere fact of using an open Android device should still cause some serious alarm.

"What we know from looking at public information about disclosure of vulnerabilities and exploits on hardware and software is that Android devices have a very high volume of vulnerabilities. There's a high level of exploitability of an Android phone," says Sam Kassoumeh, chief operations officer at the security intelligence firm SecurityScorecard. Especially given the Android phone Trump likely uses.

Open Season

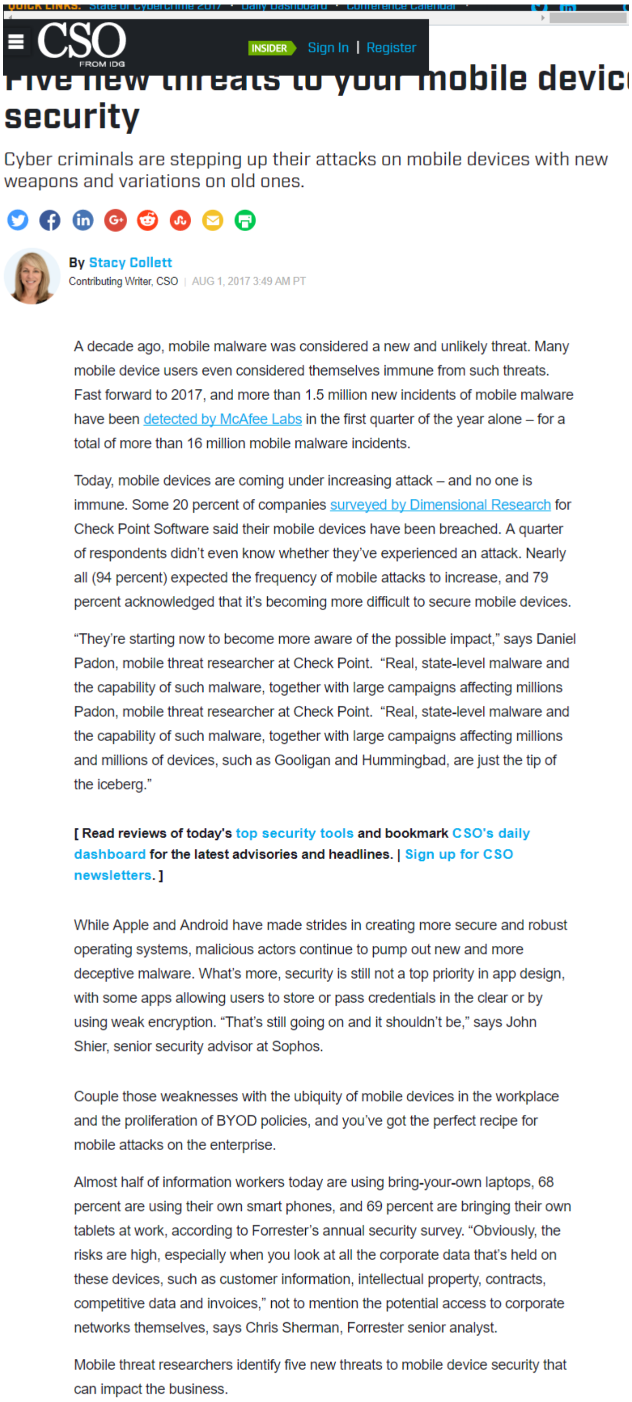
Google is diligent about Android security, releasing monthly updates that patch known flaws. The problem, though, is that those updates are only available to a handful of devices at first, including those in Google's own Nexus line.

Android phones have notoriously uneven security because the operating system is open source, allowing manufacturers and third-parties to put modified versions, or "forks," of Android onto devices before selling them. This often makes it more difficult for phones to receive updates, patches, and full OS upgrades as they come out. As a result, phones that run stock Android can get regular security updates pushed from Google, but millions of devices will only have those improvements available on a delay, if ever. For some context, less than one percent of Android devices currently run the most recent major update, Android 7.0, which Google released late last summer.

Based on some photo analysis, Android Central thinks Trump may use a Samsung Galaxy S3, a model that was first released in 2012. Another report pegged it as a slightly more recent Galaxy S4. Regardless of specifics, any mainstream Android device would be problematic, even with some precautions in place.

"Hopefully the Secret Service is treating his device as already compromised and restricting that phone from having any connections to secret or official government materials, resources, networks, and documents," says Greg

Appendix C:



QUICK LINKS: State of Cybercrime 2017 • Daily Dashboard • Conference Calendar •
CSO
FROM IDG
INSIDER
Sign In | Register

Five new threats to your mobile devic security

Cyber criminals are stepping up their attacks on mobile devices with new weapons and variations on old ones.

By **Stacy Collett**
Contributing Writer, CSO | AUG 1, 2017 3:49 AM PT

A decade ago, mobile malware was considered a new and unlikely threat. Many mobile device users even considered themselves immune from such threats. Fast forward to 2017, and more than 1.5 million new incidents of mobile malware have been detected by McAfee Labs in the first quarter of the year alone – for a total of more than 16 million mobile malware incidents.

Today, mobile devices are coming under increasing attack – and no one is immune. Some 20 percent of companies surveyed by Dimensional Research for Check Point Software said their mobile devices have been breached. A quarter of respondents didn't even know whether they've experienced an attack. Nearly all (94 percent) expected the frequency of mobile attacks to increase, and 79 percent acknowledged that it's becoming more difficult to secure mobile devices.

"They're starting now to become more aware of the possible impact," says Daniel Padon, mobile threat researcher at Check Point. "Real, state-level malware and the capability of such malware, together with large campaigns affecting millions Padon, mobile threat researcher at Check Point. "Real, state-level malware and the capability of such malware, together with large campaigns affecting millions and millions of devices, such as Gooligan and Hummingbad, are just the tip of the iceberg."

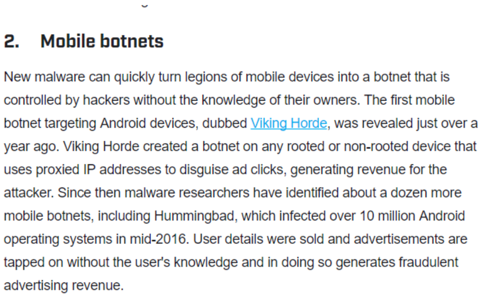
[Read reviews of today's top security tools and bookmark CSO's daily dashboard for the latest advisories and headlines. | Sign up for CSO newsletters.]

While Apple and Android have made strides in creating more secure and robust operating systems, malicious actors continue to pump out new and more deceptive malware. What's more, security is still not a top priority in app design, with some apps allowing users to store or pass credentials in the clear or by using weak encryption. "That's still going on and it shouldn't be," says John Shier, senior security advisor at Sophos.

Couple those weaknesses with the ubiquity of mobile devices in the workplace and the proliferation of BYOD policies, and you've got the perfect recipe for mobile attacks on the enterprise.

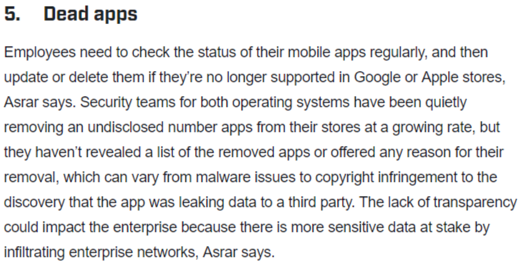
Almost half of information workers today are using bring-your-own laptops, 68 percent are using their own smart phones, and 69 percent are bringing their own tablets at work, according to Forrester's annual security survey. "Obviously, the risks are high, especially when you look at all the corporate data that's held on these devices, such as customer information, intellectual property, contracts, competitive data and invoices," not to mention the potential access to corporate networks themselves, says Chris Sherman, Forrester senior analyst.

Mobile threat researchers identify five new threats to mobile device security that can impact the business.



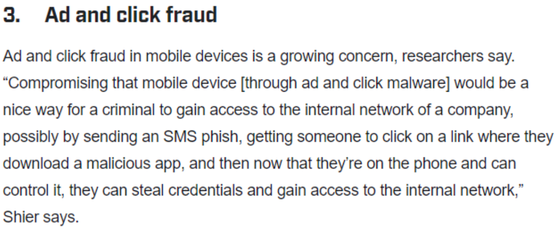
2. Mobile botnets

New malware can quickly turn legions of mobile devices into a botnet that is controlled by hackers without the knowledge of their owners. The first mobile botnet targeting Android devices, dubbed Viking Horde, was revealed just over a year ago. Viking Horde created a botnet on any rooted or non-rooted device that uses proxied IP addresses to disguise ad clicks, generating revenue for the attacker. Since then malware researchers have identified about a dozen more mobile botnets, including Hummingbad, which infected over 10 million Android operating systems in mid-2016. User details were sold and advertisements are tapped on without the user's knowledge and in doing so generates fraudulent advertising revenue.



5. Dead apps

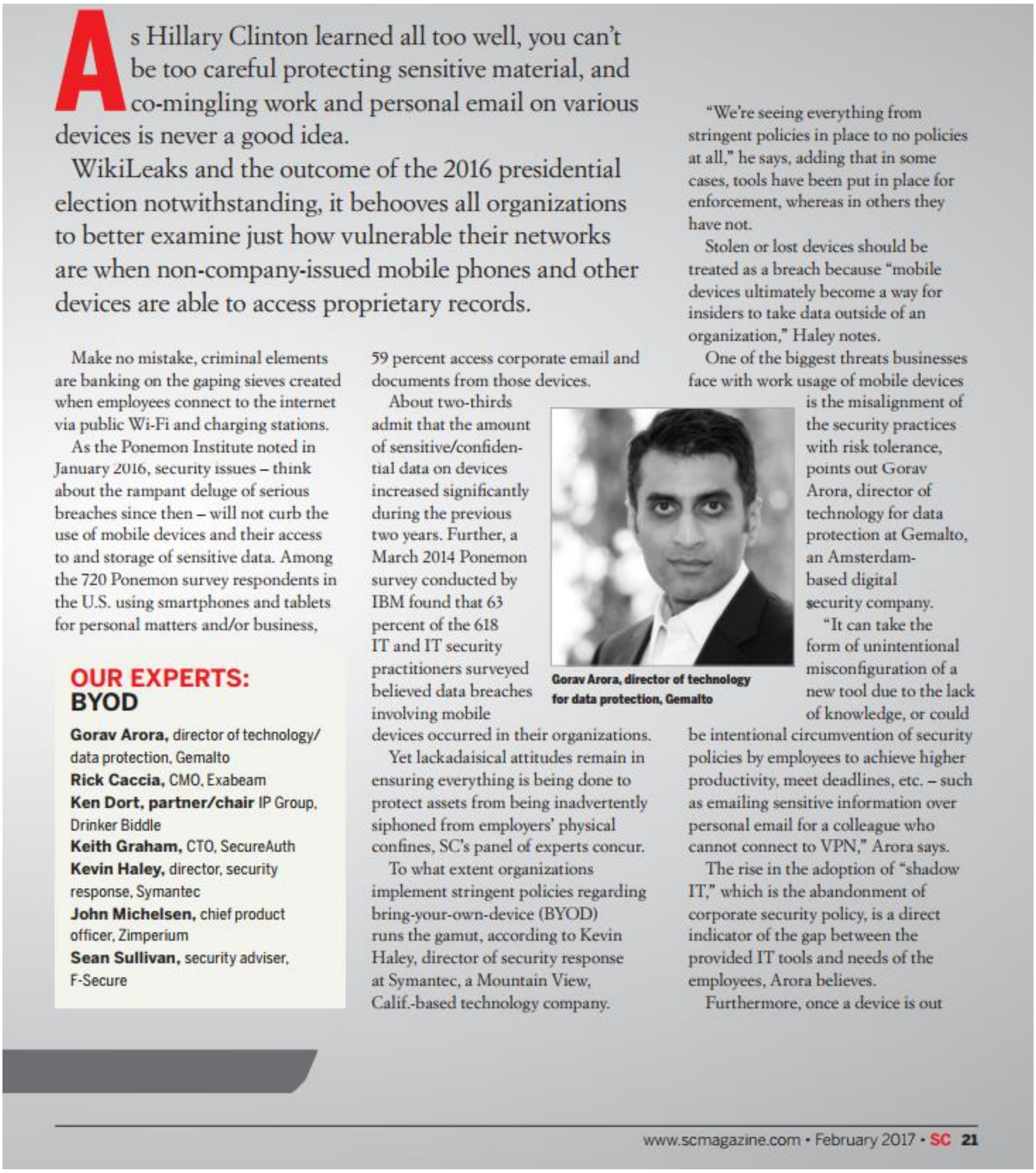
Employees need to check the status of their mobile apps regularly, and then update or delete them if they're no longer supported in Google or Apple stores, Asrar says. Security teams for both operating systems have been quietly removing an undisclosed number apps from their stores at a growing rate, but they haven't revealed a list of the removed apps or offered any reason for their removal, which can vary from malware issues to copyright infringement to the discovery that the app was leaking data to a third party. The lack of transparency could impact the enterprise because there is more sensitive data at stake by infiltrating enterprise networks, Asrar says.



3. Ad and click fraud

Ad and click fraud in mobile devices is a growing concern, researchers say. "Compromising that mobile device [through ad and click malware] would be a nice way for a criminal to gain access to the internal network of a company, possibly by sending an SMS phish, getting someone to click on a link where they download a malicious app, and then now that they're on the phone and can control it, they can steal credentials and gain access to the internal network," Shier says.

Appendix D:



As Hillary Clinton learned all too well, you can't be too careful protecting sensitive material, and co-mingling work and personal email on various devices is never a good idea.

WikiLeaks and the outcome of the 2016 presidential election notwithstanding, it behooves all organizations to better examine just how vulnerable their networks are when non-company-issued mobile phones and other devices are able to access proprietary records.

Make no mistake, criminal elements are banking on the gaping sieves created when employees connect to the internet via public Wi-Fi and charging stations.

As the Ponemon Institute noted in January 2016, security issues – think about the rampant deluge of serious breaches since then – will not curb the use of mobile devices and their access to and storage of sensitive data. Among the 720 Ponemon survey respondents in the U.S. using smartphones and tablets for personal matters and/or business, 59 percent access corporate email and documents from those devices.

About two-thirds admit that the amount of sensitive/confidential data on devices increased significantly during the previous two years. Further, a March 2014 Ponemon survey conducted by IBM found that 63 percent of the 618 IT and IT security practitioners surveyed believed data breaches involving mobile devices occurred in their organizations.

Yet lackadaisical attitudes remain in ensuring everything is being done to protect assets from being inadvertently siphoned from employers' physical confines, SC's panel of experts concur.

To what extent organizations implement stringent policies regarding bring-your-own-device (BYOD) runs the gamut, according to Kevin Haley, director of security response at Symantec, a Mountain View, Calif.-based technology company.

"We're seeing everything from stringent policies in place to no policies at all," he says, adding that in some cases, tools have been put in place for enforcement, whereas in others they have not.

Stolen or lost devices should be treated as a breach because "mobile devices ultimately become a way for insiders to take data outside of an organization," Haley notes.

One of the biggest threats businesses face with work usage of mobile devices is the misalignment of the security practices with risk tolerance, points out Gorav Arora, director of technology for data protection at Gemalto, an Amsterdam-based digital security company.

"It can take the form of unintentional misconfiguration of a new tool due to the lack of knowledge, or could be intentional circumvention of security policies by employees to achieve higher productivity, meet deadlines, etc. – such as emailing sensitive information over personal email for a colleague who cannot connect to VPN," Arora says.

The rise in the adoption of "shadow IT," which is the abandonment of corporate security policy, is a direct indicator of the gap between the provided IT tools and needs of the employees, Arora believes.

Furthermore, once a device is out

Gorav Arora, director of technology for data protection, Gemalto

OUR EXPERTS: BYOD

Gorav Arora, director of technology/data protection, Gemalto
Rick Caccia, CMO, Exabeam
Ken Dort, partner/chair IP Group, Drinker Biddle
Keith Graham, CTO, SecureAuth
Kevin Haley, director, security response, Symantec
John Michelsen, chief product officer, Zimperium
Sean Sullivan, security adviser, F-Secure

www.scmagazine.com • February 2017 • SC 21 of the company or an employee's possession, it's typically mined for credentials, company data and personal information, points out John Michelsen, chief product officer at Zimperium, a San Francisco-based mobile security company which recently collected data from 7,000 mobile devices used by a client's employees. It found 60 percent of the devices to be exposed to known vulnerabilities, six percent recorded a critical threat event and one percent to be infected with a malicious app. (Adding to those findings, Symantec's "Internet Security Report," identified a 77 percent increase in Android malware variants from 2014 to 2015, with even more expected in 2016.)

"This 24/7 access, outside the corporate firewall, likely raises the tendency of employees to share inappropriate information with others," Michelsen says. Organizations should implement solutions from mobile device manufacturers that provide strong authentication, document tracking/tracing and data loss prevention features, he adds.

Authentication required

As BYOD became prevalent, device manufacturers are turning on security by default, essentially building in two-factor authentication to secure company data, notes Arora at Gemalto. Only two-fifths of enterprises use authentication to protect all of their resources, but it should be a standard business practice, he adds.

Organizations should ensure that if applications are being accessed from mobile devices, suitable authentication safeguards are being used such as ensuring that adaptive authentication and second-factor methods are in place, agrees Keith Graham, CTO at SecureAuth, an Irvine, Calif.-based provider of two-factor authentication and single sign-on tools.

> Mobile doesn't create new types of insider threats."
>
> – Rick Caccia, CMO, Exabeam

If a device is compromised and any credentials being used on the device are stolen, adaptive and second-factor authentication "helps ensure that attackers cannot use these stolen usernames and passwords to gain access," he adds.

Paying attention to what's going on in the network is critical whether the employee is in the office or working remotely. "Log analytics, particularly those that use behavioral analytics, can identify risky access patterns early in the process," says Rick Caccia, CMO of Exabeam, a San Mateo, Calif.-based computer security services firm whose specialty is behavior analytics.

Keith Graham, CTO, SecureAuth

Sean Sullivan, security adviser, F-Secure

Caccia believes that putting more security on the device itself has only marginal benefit. "It's much better to increase monitoring and detection throughout the network itself, and then to link that to cloud services in use," he explains. That way, even if an employee switches devices, the firm can detect unusual behavior.

The mobile arena, because of less device management, "can make it easier for a malicious insider to copy and remove sensitive information," he points out. "Mobile doesn't create new types of insider threats, it just makes the most common types easier to execute and harder to detect."

Part of the problem is an office desktop computer and server mentality is influencing IT departments without acknowledging workflows have changed dramatically. By their very nature, mobile phones are reliant on non-desktop technologies.

"We've seen numerous cases of attacks orchestrated where a one-time-password sent to a phone via SMS has

MINIMIZE THREATS: Four must-haves

How can organizations reduce and mitigate the mobile threat posed by its own employees? Kevin Haley, director, security response at Symantec, lays out four simple must-haves that organizations should implement to reduce and mitigate the threat:

1. **Policies**: Have policies about the use of data and ensure users are educated on them
2. **Tools**: Use tools to both alert and prevent data leakage
3. **Encryption**: Leverage encryption on mobile devices to protect data
4. **Scanning**: Ensure devices are scanned for spyware and malware

Haley also suggests any mobile toolkit should include protections such as two-factor authentication, data leak prevention, and encryption/remote wipe technology.