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 II

Table of Contents

Executive Summary

This document is a continued investigation of report I. The control measures have been put into consideration and the action that should be taken to control the issue or reduce the level of harm. Control measures can also involve, technology, policy, and practices, education, training, and awareness. This document explains the control measures for each of the issues investigated in the first report.

Section 1 – Introduction

The Samsung Galaxy S6 Edge smartphone stores my information assets. It uses 32Gb of memory to store my all my data/files. The phone runs on the Android, version 7 Nougat, which was released in Australia in July 2017. This version has enhanced the user experience by adding new features and better security to prevent vulnerabilities. This phone comes with built-in apps like the camera, phone, clock, and more, that are everyday tools for the user. Besides the preloaded apps, I have downloaded other apps mainly for entertainment and socialising with other people. The most important application on my phone would be the Commonwealth Bank app that stores my money and accounts, and the QUT app, that has information about myself, my courses and files submitted. Most of the applications downloaded have my personal information but most aren't stored directly on my smartphone but rather on the database server of the organization.

My valuable asset, the Samsung Galaxy S6 edge is very important. If I was to lose my phone, my information and data can be compromised by the person who stole or found it. The stranger can look at all my personal data and information by going through all my installed applications, breaking the Confidentiality of the security goal or services. The stranger can learn more about me. Even so, the stranger can further change my information which breaches the integrity security goal (modifying my information). The modification of my info can also lead to the deletion of my account or be locked out which then breaches the Availability security goal.

Almost all my apps store my information, most link to each other using my Facebook account. So it would be easy for the stranger to access another app/service using my Facebook account. All information created on my phone is valuable and can breach all security goals (C.I.A) when my phone is in someone else's possession.

Section 2 – Information security issues related to user privacy

Review of Part I (Section 3):

Facebook's goal is to make the world more open and connected. Using their social services, every single bit of activity/information is stored on their DataCenter (PSafe Blog, 2017). Interactions, like communicating with others, sharing contents, just about anything you do on Facebook, is automatically recorded. However, the recorded information can be helpful to the improvement and development of their services and provide better safety and security of our accounts (Facebook, 2016).

The positive side of having our information and activity recorded is that it improves the safety and security of our accounts by comparing devices used to access the accounts and detecting if the account is being hacked. User information is not always under Facebook's control. It's always in the user's control and can be deleted by the user.

This submission – treating the risk:

Title: The Dangers of Facebook Oversharing
Author: Andy O'Donnell
Reference details: Lifewire. 2017. *The Dangers of Facebook Oversharing*. [ONLINE] Available at: https://www.lifewire.com/dangers-of-facebook-oversharing-2487777. [Accessed 20 October 2017].
Threat/Vulnerability/Attack details:
In the article, Andy discussed why oversharing on Facebook can be dangerous. Facebook's timeline gathers friends and public posts. Users can post onto Facebook and depending on the settings, if the post is shared to the public, the post can be seen by dozens or millions of Facebook users. Whether the post is popular/viral, that post could be shared for more people to see. Public posts can be great for lawyers who want to use your post against you in court, even thieves (Lifewire, 2017). Thieves love to target users who have posted their pictures, statuses or location to the public. The threat of having public posts, for example, sharing your location is a good indication for the thief to rob your house or stalk you. Information shared to the public can create big threats to a user's life thieves can learn more about you, stalk you, etc.
Security Goals compromised:
Constant posts every activity or information to the public can breach the user's confidentiality security goal depending on the information shared. Without the user being aware of sharing their confidential information, it still breaches the confidentiality security goal. Their shared information allows the attacker to learn more about the person.

Suggested control measure and explanation:
A control measure to prevent threats and compromising the user's confidentiality security goal is to change the privacy settings from public to either just friends or yourself on the social media account as suggested Trend Micro. Users should understand what the social media site does with the user's information.

Type of control measure:
This is a type of preventive control measure. As suggested by (Social Media Privacy Settings Are Important, 2017), users should manage the privacy of their past and future posts on their social media site. Making all of the information private can prevent identity theft and attacks.

Degree of protection provided:
The user's privacy settings can be enough to prevent strangers, stalkers, thieves etc from having access to the user's posts. However, it can depend on how private the user is. If the user has made everything private, that includes being hard to find through search and unable to know anything, this certainly prevents the public from knowing about this user. If settings are set to make posts and pictures private, then no threats can be made against the user.

Limitations of this control measure:
If the privacy settings allowed only friends or friends of friends to see the post, it may still allow friends to share the post/information to their own friends or even tag them. There may still be a way for attackers to find this secret/private user if one of their friends' account has been taken over by an attacker. That compromised account can still be used to view the user's information shared to just friends.

Reference:
Social Media Privacy Settings Are Important -. 2017. *Social Media Privacy Settings Are Important* -. [ONLINE] Available at: http://blog.trendmicro.com/social-media-privacy-settings-are-important/. [Accessed 21 October 2017].

Section 3 – Security issue associated with a mobile device application

Review of part I (Section 4) article:

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].
Threat/Vulnerability/Attack details:
The article discussed the safety warning issue of showing your child's location on the Snapchat map. Showing your own location on Snapchat allows others to locate you. The ability to have the user's location shown to the public is a threat as it allows contacts to pinpoint the user. The bigger threat of this is if the child has added unknown contacts, there is a greater potential of child abduction or stalking young users. Enabling the user's location is a vulnerability as it allows others to track you. Unknown contacts may want to know more

about the user by viewing the users' story and location. Also, if the user has their privacy settings to public, thousands of unknown people can see the user's posts.

Security Goals compromised:
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 places that you go 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 don't have the GPS located.

This submission: treating the risk:

Suggested control measure and explanation:
A control measure for this scenario is to limit the use of radios, connections and know what information is being shown to others. Smartphone users should know their smartphone and be aware of what they're doing (Larry Magid, 2017). Young users should limit who can view their location as this app allows others to determine your location. This can be prevented by enabling ghost mode which your location would not be broadcasted to others. (HowStuffWorks, 2017)

Type of control measure:
This is a type of preventive control measure. As suggested by (Larry Magid, 2017), users, especially of young age should limit who is able to view their location. Understanding the use of your phone, looking at what you've used or enabled and be aware of your activities.

Degree of protection provided:
As suggested by (HowStuffWorks, 2017), enabling ghost mode on the Snapchat app can be enough to prevent strangers to determine the location of young users. However, if an attack was to happen on Snapchat, they could go through the databases, people's stories, data, information etc. Attackers may also be able to see every user's location and their location history. Disabling the user's location through phone settings throughout the use of the application may be enough to prevent strangers pinpointing you.

Limitations of this control measure:
Snapchat collects every user activity on the application. Information, especially location, is stored in their database for the improvement of security and service of their app. Since Snapchat collects user locations, this limits the preventive control measure because attackers can see the user's location history and pinpoint the user's favourite spots, most likely the user's home.

Disabling your GPS may not fully prevent user tracking, thus not allowing the location service to be enabled from first using a new account can certainly prevent the stalkers.

Reference details:

Larry Magid. 2017. *How To Control Who Can See Your Location On Snapchat And Other Precautions.* [ONLINE] Available at: https://www.forbes.com/sites/larrymagid/2017/06/23/how-to-control-who-can-see-your-location-on-snapchat-and-other-precautions/#13bede5a1a75. [Accessed 21 October 2017].

Smartphone Signal Interception - Smartphone Signal Interception | HowStuffWorks. 2017. *Smartphone Signal Interception - Smartphone Signal Interception | HowStuffWorks.* [ONLINE] Available at: http://electronics.howstuffworks.com/phone-stalking3.htm. [Accessed 21 October 2017].

Section 4 – Security issue associated with a mobile device operating system

Review of part I (Section 5) article:

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].
Threat/Vulnerability/Attack details:
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. Android can run on many brands like HTC, LG, Samsung etc. However, latest android updates may not be compatible with all brands. Not all Android phones run on the same brand. In the article, Trump still uses an old Android phone, which has many vulnerabilities and threats because the phone is not protected from attacks. The threat of Trump using an old phone is if he clicks on a malicious link or attachment, his device can be compromised. This can lead to strangers watching, tracking him getting his confidential files etc. The vulnerability in this issue is that an old outdated phone can allow attackers to compromise his information on the device and show it to the public.
Security Goals compromised:
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. The hacker can track the phone's location, determining where he himself can be at any time. The availability security goal can also be breached if the attacker manages to eradicate all the data and information on his phone, preventing Trump to access his information.

This submission: treating the risk

Suggested control measure and explanation:
Trump's old phone can easily be compromised but can be prevented by getting a new up-to-date smartphone, which minimizes vulnerabilities. Even better is if the manufacturing company can update old phones. There are other options for Trump if he wants to continue

using his old phone. (Stephanie Crawford, 2017) suggests having the password saving tool package and two-factor authentication.

Type of control measure:
This control measure is preventive to attackers having access to Trump's phone and collects all his information and data. As suggested by (Stephanie Crawford, 2017), a good tool that saves passwords and using two-factor authentication can make it difficult for the attacker to compromise Trump's phone.

Degree of protection provided:
The protection provided can secure Trump's information and data stored on his old phone. The password savings tool may not reliable to use, as it may be easy or hard for attackers to get into. However, a two-factor authentication is a strong second line of defence to Trump's sensitive information. Having this type of authentication is hard for attackers. The authentication needs the Trump's password and something that only he knows.

Limitations of this control measure:
A password storage is a good place to keep all passwords and keep organised. However, depending on how secure the storage is attackers could still get into it. The password storage must have a strong encryption algorithm. Two-factor authentications, on the other hand, can lock out Trump out of his phone and accounts. In (NDTV Gadgets360.com, 2017), Akhil explains that he did not save his recovery codes for his accounts after resetting his phone. He was lucky enough to recover most of his account except for Snapchat which they could not verify that he was the actual user. He had to start again with a new account.

Therefore, it is best for Trump to write his recovery codes and passwords onto a notebook if he forgets or resets his device. It can also be hard for an attacker to get to get his codes and passwords.

Reference:

Stephanie Crawford. 2017. *Could someone stalk you using your own smartphone?.* [ONLINE] Available at: https://www.tomsguide.com/us/old-phones-unsafe,news-24846.html. [Accessed 21 October 2017].

NDTV Gadgets360.com. 2017. *Two-Factor Authentication Is Great, and It's a Mess | NDTV Gadgets360.com.* [ONLINE] Available at: http://gadgets.ndtv.com/internet/opinion/two-factor-2fa-authentication-problems-issues-1761420. [Accessed 21 October 2017].

Section 5 – 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].

Threat/Vulnerability/Attack details:

Malware, also known as malicious software, targets computers or mobile device systems (smartphones or tablet) to control 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. When a user installs a new application from an unidentified developer, there is potential for the application to have malware hiding behind it. Threats like malware, mobile botnets, ad and click, phishing SMS or links, and dead apps can lead to the user's information being exposed and losing control of their phone. Downloading random things from the internet especially form unsafe websites are vulnerabilities. Most mobile owners aren't aware of the risks of downloading random things and when they get attacked, the device can be compromised and the information stored on the phone can be taken.

Security Goals compromised:

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.

This submission: treating the risk

Suggested control measure and explanation:

The suggested control measures is to have an anti-virus software/application installed on their smartphones and always have it up to date. Users must be aware of what they are downloading from the internet and must trust attachments only from people they trust (Runbox, 2017). Backing up files is a good way to recover original files. It can protect the employee's data from ransomware and natural disasters (Naked Security, 2017).

Type of control measure: Detective, corrective

This is a detective and corrective control. The detective control is the adding an anti-virus software that helps detect viruses in files that have been downloaded from the internet. The corrective control is backing up files to a hard drive or their cloud service.

Degree of protection provided:

The anti-virus software protects the user from getting viruses. For every file being downloaded from the internet, the file gets scanned and detects if there are any viruses hiding behind. If a virus has been detected, the program immediately discards the file. On the other hand, backing up files can keep an original file in case the user loses his/her computer files to viruses like ransomware that locks the user out from using their own phone.

Limitations of this control measure:

There are limitations in the use of the backing up files because users could have special applications to run special files. If a ransomware deletes everything on the user's phone, the backed up files can be used to replace the lost/damaged. However, copying backed up applications can be difficult as it may not function correctly. So the user may have to

download and reinstall their applications again. Another limitation is that the user may forget to back up their files. So users must plan ahead on how to constantly back up their own files.

Reference:

Runbox. 2017. *What are computer viruses; how to avoid them - Runbox*. [ONLINE] Available at: https://runbox.com/email-school/what-are-computer-viruses-and-how-to-protect-against-them/. [Accessed 21 October 2017].

Naked Security. 2017. *8 tips for preventing ransomware – Naked Security*. [ONLINE] Available at: https://nakedsecurity.sophos.com/2016/03/24/8-tips-for-preventing-ransomware/. [Accessed 21 October 2017].

Section 6 – 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].
Threat/Vulnerability/Attack details:
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 BYO devices create more vulnerabilities, in other words, a weakness in the companies' system that an attacker can access or exploit. 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. The vulnerability of BYOD is that it may not be secure and the difficulty of unlocking a stolen device can depend on how updated or old it is. The person picking up the phone may decide to unlock and expose the data or if lucky, hand it over to the police.
Security Goals compromised:
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.

This submission: treating the risk

Suggested control measure and explanation:
BYO devices can bring threats to companies. To keep safe from attacks Trend Micro suggests companies must think of the risks of allowing their employees to use their own devices at work, implementation of a formal BYOD policy and give employees the correct rights/access to the needed information. Teaching employees to detect phishing attacks can make them more aware. Trend Micro also suggests encrypting their own data on their device so it can be unreadable to strangers and have a multifactor-authentication to make the phone harder to access.

Type of control measure:
This is a preventative and corrective control measure. By teaching employees to detect phishing, having a policy for BYO devices, encrypting data and have multifactor can prevent an attack (Trend Micro USA, 2017). Implementing an access control for the employee to get their information is a good practice for companies, to correct which person can access the assigned/needed/owned information. This is the corrective control measure.

Degree of protection provided:
A policy for BYO devices will inform their employees about the risks and threats of using their own device. It will keep employees aware of the consequences or problems if an attacker manages to obtain sensitive information from the company. Having a password to unlock the device may not be secure enough to prevent attacks.

Encrypting the device and having a password would be enough to make all data and information unreadable to a stranger. The use of multifactor authentication can be hard for the attacker to crack as it needs a physical object that the user possesses (key or token) and a secret only the user knows, and a characteristic of the users (fingerprint, voice, face).

Limitations of this control measure:
Encrypted data/information can be unreadable to people who picked up the device. However, if the person picking it up has the tools to decrypt the data, then the data and information stored can compromise the confidentiality of the company. Multifactor authentication provides good security for devices, however, it may cost a lot (Samanage Blog, 2017), and the user's possession for authorization can be lost or stolen (Keith Shaw, 2017).

Reference:
Infosec Guide: Dealing with Threats to a Bring Your Own Device (BYOD) Environment - Security News - Trend Micro USA . 2017. *Infosec Guide: Dealing with Threats to a Bring Your Own Device (BYOD) Environment - Security News - Trend Micro USA .* [ONLINE] Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod. [Accessed 21 October 2017].

Samanage Blog. 2017. *Multifactor Authentication: Challenges and Benefits*. [ONLINE] Available at: https://blog.samanage.com/it-asset-management/multifactor-authentication-challenges-and-benefits/. [Accessed 21 October 2017].

Keith Shaw. 2017. *Two-factor authentication: Pros and cons | Network World.* [ONLINE] Available at: https://www.networkworld.com/article/2869919/lan-wan/two-factor-authentication--pros-and-cons.html. [Accessed 21 October 2017].

Section 7 – Conclusion

Adding control measures on security issues can make people more aware of the dangers of attacks on devices and online. As discussed throughout this report, having a preventive control can prevent any attempts of attackers exploiting vulnerabilities. Also, having detective control also keeps an eye out for any attempts on exploiting vulnerabilities. Lastly, corrective control fixes errors on files or vulnerabilities. Having control measures does prevent/reduce the risks of attacks. Teaching users about the risks can make them more aware of threats and vulnerabilities on their phones. With the control measures discussed, it can make mobile devices secure. Depending on the issue, control measures can be immediately applied, but for adding anti-virus software, it could cost a lot.

Throughout this investigation, learning more about the security issues and the potential threats and vulnerabilities have forced me to apply preventive, and corrective control measures. All my files/information stored on my phone has been encrypted and backed up onto my external hard drive. Also, I have added a two-factor authentication to make it harder for attackers to crack my mobile device.

References

From Report Part I:

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].

This submission:

Lifewire. 2017. The Dangers of Facebook Oversharing. [ONLINE] Available at: https://www.lifewire.com/dangers-of-facebook-oversharing-2487777. [Accessed 20 October 2017].

Social Media Privacy Settings Are Important -. 2017. Social Media Privacy Settings Are Important -. [ONLINE] Available at: http://blog.trendmicro.com/social-media-privacy-settings-are-important/. [Accessed 21 October 2017].

Stephanie Crawford. 2017. Could someone stalk you using your own smartphone?. [ONLINE] Available at: https://www.tomsguide.com/us/old-phones-unsafe,news-24846.html. [Accessed 21 October 2017].

NDTV Gadgets360.com. 2017. Two-Factor Authentication Is Great, and It's a Mess | NDTV Gadgets360.com. [ONLINE] Available at: http://gadgets.ndtv.com/internet/opinion/two-factor-2fa-authentication-problems-issues-1761420. [Accessed 21 October 2017].

Runbox. 2017. What are computer viruses; how to avoid them - Runbox. [ONLINE] Available at: https://runbox.com/email-school/what-are-computer-viruses-and-how-to-protect-against-them/. [Accessed 21 October 2017].

Naked Security. 2017. 8 tips for preventing ransomware – Naked Security. [ONLINE] Available at: https://nakedsecurity.sophos.com/2016/03/24/8-tips-for-preventing-ransomware/. [Accessed 21 October 2017].

Infosec Guide: Dealing with Threats to a Bring Your Own Device (BYOD) Environment - Security News - Trend Micro USA . 2017. Infosec Guide: Dealing with Threats to a Bring Your Own Device (BYOD) Environment - Security News - Trend Micro USA . [ONLINE] Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod. [Accessed 21 October 2017].

Samanage Blog. 2017. Multifactor Authentication: Challenges and Benefits. [ONLINE] Available at: https://blog.samanage.com/it-asset-management/multifactor-authentication-challenges-and-benefits/. [Accessed 21 October 2017].

Keith Shaw. 2017. Two-factor authentication: Pros and cons | Network World. [ONLINE] Available at: https://www.networkworld.com/article/2869919/lan-wan/two-factor-authentication--pros-and-cons.html. [Accessed 21 October 2017].

Appendices

Appendix A:

Lifewire

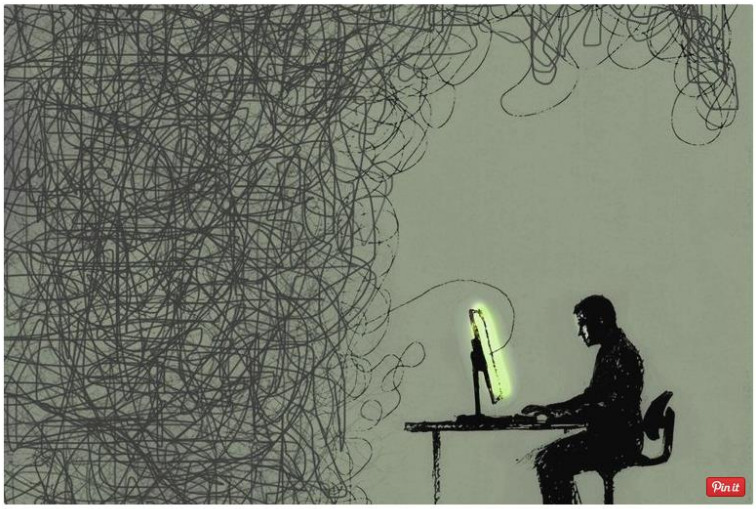
Search

DO MORE › WEB & SEARCH

The Dangers of Facebook Oversharing

Can too much sharing get you in trouble?

Share Pin Email PRINT



Gary Waters/Ikon Images/Getty Images

Web & Search

- Safety & Privacy
- Best of the Web
- Search Engines
- Running a Website

Updated July 14, 2017

How much is too much information when it comes to sharing on Facebook? When does sharing become oversharing, and when does it become a personal safety risk? Some people out there actually like oversharing, and some don't. Let's take a look at both the lovers and the haters of oversharing:

Stalkers love oversharing

Let's face it, the Facebook Timeline is like a scrapbook for stalkers. Timeline provides an easy interface where your friends, and depending on your privacy settings, anyone in the world can have quick access to all the things that you've ever posted on Facebook.

Stalkers just need to click on the year and month that they're interested in and Facebook Timeline takes them right to it.

With the 60 or so new apps that allow for what Facebook execs are calling "frictionless sharing", nearly every aspect of your life is potentially on display for stalkers to follow.

From the music you're listening to, to where you're "checking in" at in the real world, these little tidbits of information can help your stalker learn your patterns so they can know where to find you.

It's best to limit the sharing of your location on Facebook as much as possible or not share it at all. Use Facebook friends lists to organize your friends. Create a list of your most trusted friends and set your privacy settings to allow more access for trusted friends and highly limited access to acquaintances who might end up being stalkers.

Thieves love oversharing

Want to make yourself an easy target for thieves?

The easiest way to do this is to share your location information on Facebook.

If you just "checked-in" at the local gym and posted this to Facebook, then any thief who is trolling Facebook profiles will know that you are not at home. This would be a great time to rob you.

You may have restricted your privacy settings on Facebook to just friends, but what if a friend is logged into a publicly accessible computer, such as at a library, and forgets to log out or has their cell phone stolen?

You can't expect that your friends are the only ones who have access to your status and location just because your privacy settings are set to friends only.

Some Facebook apps that share your location may have more relaxed privacy settings than you are comfortable with and may be blabbing your location without you realizing it.

Check your privacy settings and also check to see what information your Facebook apps are sharing with your friends and the rest of the world. Limit them as much as possible to protect your privacy and personal safety. Never ever post that you are home alone.

Lawyers love oversharing

Anything you do on Facebook can and may be used against you in a court of law. Lawyers absolutely love Facebook because it helps greatly in establishing a person's character and where and when something took place. Facebook does a lot of legwork that a private investigator would normally have to do, such as learning who a person associates with (i.e. who their friends are).

Are you in the middle of a custody battle? Posting pictures on Facebook of yourself getting tanked at a party could help your ex-spouse with their case against you. Facebook postings often reflect our moods. A ranting status post might get you labeled aggressive or abusive by a lawyer trying to make a case against you.

Avoid posting while you're angry or drunk. If you're tagged in a picture that might be considered inappropriate, you can "untag" yourself so that the picture is not associated with your profile.

Remember that even if you removed a posting after it appeared, the post might have still been caught in a screenshot or sent in an email notification. There are no guaranteed take-backs on Facebook, so always think before you post.

Employers hate oversharing

Your employer is probably not a huge fan of oversharing. Whether you're at work or not, your actions can affect your company's image, especially since most people put who they work for in their Facebook profile.

If your employer reviews Facebook activity and sees a ton of it while you're supposed to be working, they might use this against you at some point. If you say you're sick and then your Facebook location says your checking-in at the local movie theater, this might tip off your employer that you're playing hooky.

Potential employers might also request a look at your Facebook profile to learn more about you. You might consider reviewing your Timeline to see if there is anything that might cause them not to hire you.

Worried about your friends posting something stupid on your wall or tagging you in an unflattering picture that might affect a potential job offer? Turn on the Tag Review and Post Review features so that you can decide what gets posted about you before a post goes live.

There are some things you should never post on Facebook. Use your best judgment and take responsibility for what you post about yourself and others.

Check out these other Facebook Security Resources:

Top 5 Facebook Scams to Watch Out For
How to Tell a Facebook Friend From a Facebook Hacker
How to Secure Your Facebook Timeline
How to Backup Your Facebook Data

Appendix B (From Report Part I):

The Telegraph HOME | NEWS | SPO

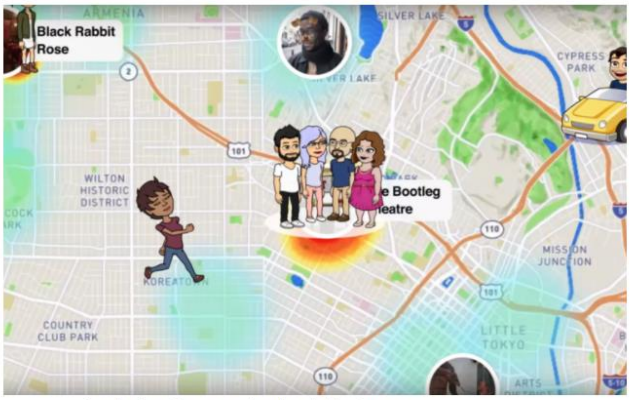
Technology

News | Reviews | Opinion | Internet security | Social media | Apple | Google | News

Technology

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

share 0



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.

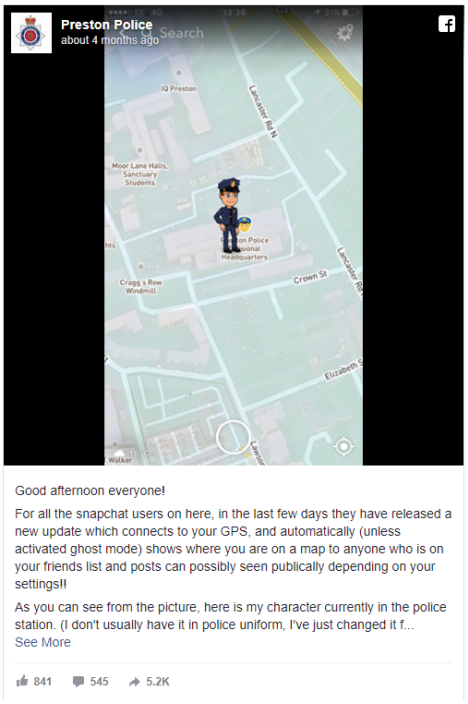
The feature displays a map of nearby friends, showing their latest location gathered using a smartphone's GPS sensor. Users of the app can also search for locations such as individual schools, with the app displaying public photos and videos sent by students.

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."



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.

"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."

How to turn on ghost mode

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.

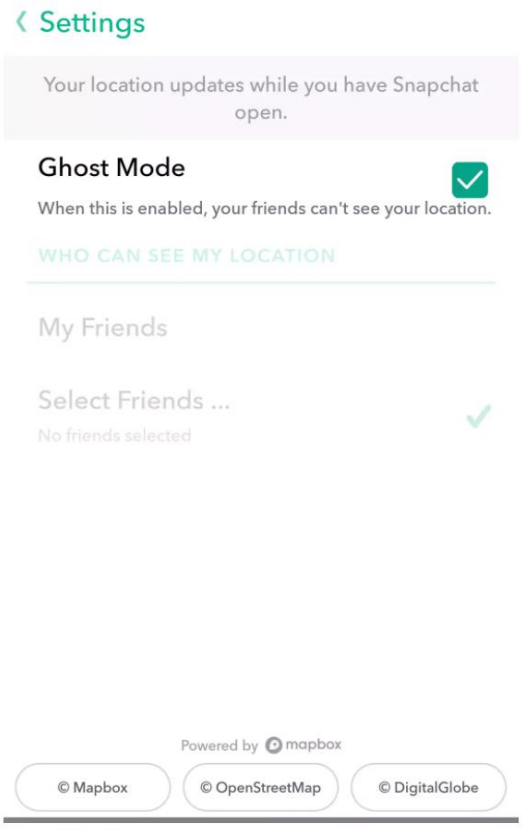
"Given how specific this new feature is on Snapchat - giving your location to a precise pinpoint on a map - we would encourage users not to share their location, especially with people they don't know in person."

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."

How to turn on ghost mode



How to disable Snapmaps

To hide your location from friends, you can easily turn on ghost mode in Snap Map. To do this, pinch the screen when you are in selfie mode to bring up Snap Map. Then, click the settings icon in the top right hand corner and set the phone to "ghost mode". Then Snapchat will stop sharing your location.

Related Topics

Children Social media Apps Snapchat Police Internet

share 0

Show comments

Paid content

Appendix C (From Report Part I):

LILY HAY NEWMAN SECURITY 01.25.17 07:02 PM

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

GETTY IMAGES

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 Linares, a security researcher who specializes in threats intelligence and reverse engineering. "Exploitation of Android devices, for the most part, is not as trivial as it was even a few years ago. Attackers would still need to develop a reliable exploit and deliver it to the President. But since it is a non-hardened device, the level of threat is rather high."

Security Slips

The smartphone revelation joins a number of recent concerns about the Trump administration's cyber hygiene. The hacker known as "WauchulaGhost" told CNN this week that the @POTUS, @FLOTUS, and @VP Twitter accounts are all prime targets for attack because they use easily guessed email addresses and don't take advantage of two-factor authentication. Meanwhile, some White House staffers, including Sean Spicer and Jared Kushner, still maintain email accounts through the Republican National Committee. The practice is legal, but dicey given controversy over George W. Bush's use of the same system and Hillary Clinton's use of a private email server, not to mention that Russian hackers breached the RNC email system during the 2016 presidential campaign season.

Ultimately, whether Trump uses his old Android device is his own choice. The intelligence community can't dictate what devices he does and doesn't use; presidents are not legally required to abide by anyone's technology recommendations. And Trump may see his Android as a net good. "In theory you want them to have the most productive tools to make sure that they're using their time the most efficiently," says SecurityScorecard's Kassoumeh. "On the flip side, there's a risk. If they have tools that can potentially be used against them or misappropriated, it can introduce some pretty dire scenarios."

There's hope that the Secret Service has taken extensive precautions to keep the leader of the free world's Android device from jeopardizing national security. But as long as it has the mainstream access and connectivity that Trump reportedly feared losing in the first place, it's a risk. As researcher Linares notes, "A device's security ultimately comes down to the user operating it."

#DONALD TRUMP #MOBILE #NATIONAL SECURITY #SMARTPHONES

Appendix D (From Report Part I):

FEATURE

Five new threats to your mobile 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 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.

1. Persistent, enterprise-class spyware

Employees use their mobile devices in nearly every aspect of their lives with mobile devices never more than arm's-length away. With such close proximity to corporate network access, voice activation and GPS tracking, state actors are looking at ways to infect mobile devices with spyware. The tactic has proven version for Android that masquerades as a normal app download, while secretly gaining root access to a device to do broad surveillance on the user over time. Since then, Google has bolstered security measures, including Play Protect security within the Play Store.

"If you're a nation state actor and you want to compromise a company, one possible route would be to compromise a mobile device that you know is going into a particular organization," Shier says. "We still have organizations that are allowing their mobile device to exist on the corporate network along with some of their other devices of higher value."

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.

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.

EXAMPLES OF MOBILE MALWARE

MALWARE	DEVICES AFFECTED	DATE FIRST DISCOVERED	HOW IT WORKS
AceDeceiver	iOS	Early 2016	Hides in downloaded apps and steals Apple IDs and passwords
Ghost Push	Android	Late 2015	Gains root access to push advertising or download malicious code
Gooligan	Android	Mid-2016	Ghost Push variant that downloads malicious code
Hummingbad	Android	Mid-2016	Disguises ad clicks to generate revenue for the perpetrator
Pegasus	iOS, Android	August 2016	Masquerades as an app to gain root access and harvest data or do surveillance
Viking Hoard	Android	Mid-2016	creates a botnet on any rooted or non-rooted device that uses proxied IP addresses to disguise ad clicks
XcodeGhost	iOS	Late 2015	Used to develop apps that can then be remotely controlled to steal information or direct users to malicious websites

IDG

"In the beginning, we saw them used for adware purposes," Padon says. "Now we've seen them rooting millions of devices, with malware opening back doors on infected devices, which could potentially be used for any purpose, including stealing sensitive data."

While mobile devices don't have the bandwidth and computational throughput as a desktop computer, botnet functions don't require a lot of compute power to pose a threat. What's more, mobile devices are often on all the time, which gives that botnet owner 24/7 access to large numbers of potential zombie bots.

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.

The scary part, Padon says, is that "they start as adware, but they can just as easily decide to spread spyware to the entire botnet. Then you have 10 million devices that record their owners' every move. It has a devastating potential with just a click on the app," he says.

4. IoT

Internet of Things (IoT) malware is still in its infancy, but it hasn't stopped malware authors from making the jump, says Irfan Asrar, senior manager in mobile malware research at McAfee. "The number of [IoT malware] families out there is just 10, and most of them are just variations of the same code base, but we're starting to see in the underground sites that people are peddling mobile malware kits and are moving into the IoT arena," and many IoT devices are largely connected to and being configured by smart phones and devices, such as mobile entry into a building or through a checkpoint.

"With targeted attack efforts, they are focused on getting to a destination," Asrar says. "They don't care what means they use – just the one with least resistance – and right now it's IoT where there's very little measures in place for security, and device manufacturers are just now beginning to follow some standards."

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.

[**Related:** SandBlast Mobile simplifies mobile security]

"Especially if you have an Android device, you will have at least a couple [apps] that were removed from the store, but they are still on your device," he says. "You probably don't want to hang on to them anymore."

What can companies do?

"It's really hard to protect your entire mobile network because it's so fragmented," Padon says.

He recommends requiring that security software be installed on every mobile device. "It's one thing if your Candy Crush app downloads a simple update, but it's a completely different story if it downloads an update and then launches a malicious activity. This is exactly where Google and Apple lack control," he adds.

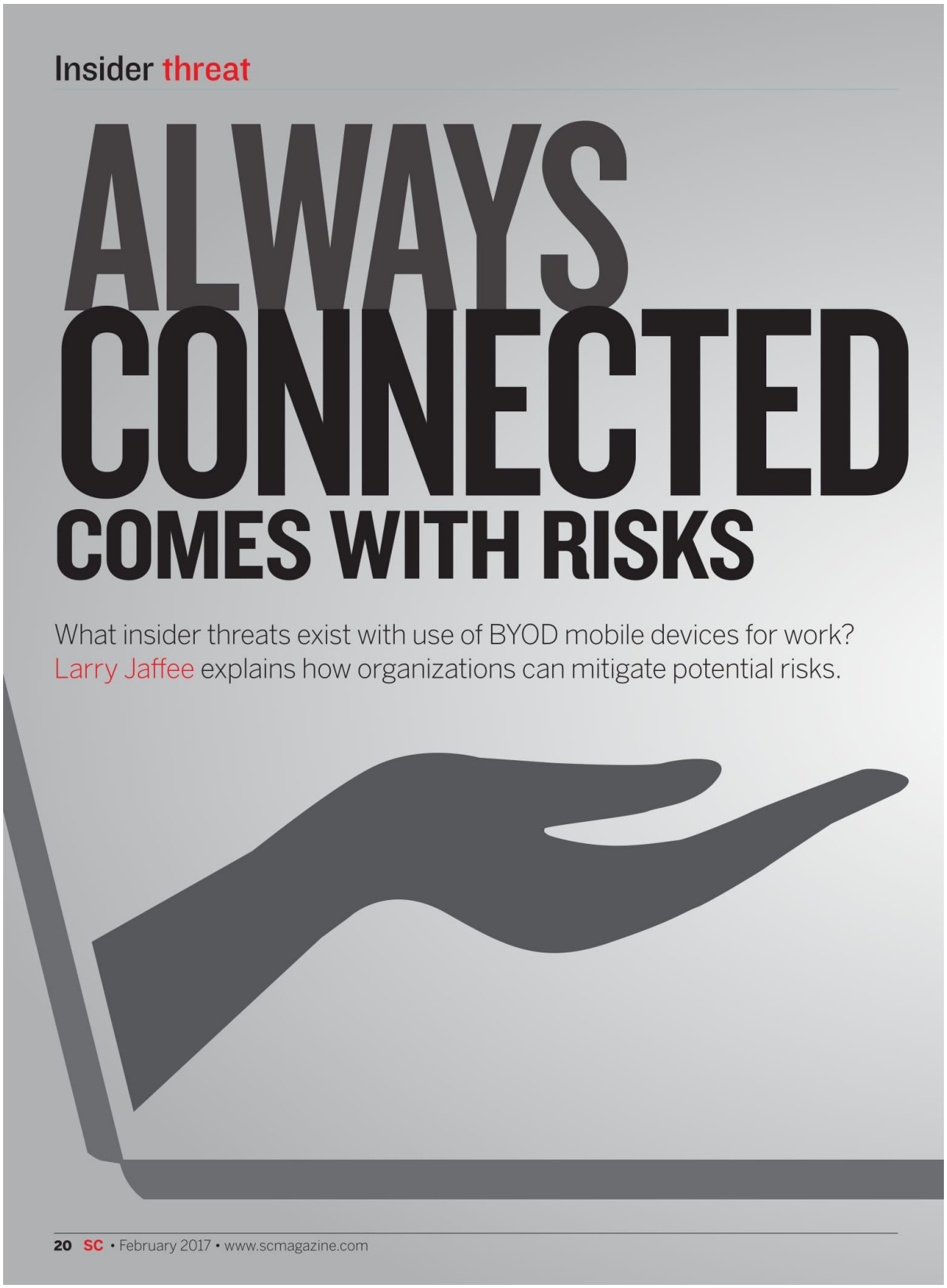
User behavior awareness and training should also continue to evolve with the threats, mobile researchers say. "It's all about reducing risk," Shier adds, through encryption and visibility into all devices that have access to the network.

Next read this:

- *The 5 cyber attacks you're most likely to face*
- *Cybersecurity headhunter shares 10 secrets from Black Hat 2017*
- *Why SSL/TLS attacks are on the rise*
- *The 10 Windows group policy settings you need to get right*
- *Why the scanners on VirusTotal flagged Hello World as harmful*

Related: Information Security | Mobile Security | Social Engineering | Social Networking

Appendix E (From Report Part I):



Insider threat

ALWAYS CONNECTED COMES WITH RISKS

What insider threats exist with use of BYOD mobile devices for work? Larry Jaffee explains how organizations can mitigate potential risks.

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.

Gorav Arora, director of technology for data protection, Gemalto

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

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

Insider threat

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.

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

Keith Graham, CTO, SecureAuth

Sean Sullivan, security adviser, F-Secure

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.

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.

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.

been intercepted and stolen from the mobile device using malware," Graham notes. This, of course, enables attackers – with already compromised usernames and passwords – to bypass the second factor.

Meanwhile, Haley points out that mobile phones are "great spying tools" that can take pictures and record audio and video, and even report the location to an insider who could control the device.

A social engineering ploy that tricks an employee to click on an emailed, malware-infested link accessed from a BYOD can easily result in a data loss, or worse.

"Business email compromise (BEC) exploits the hyper connectivity and mobility of the workforce," Arora notes. "Often such threats start with phishing attacks to have unwitting trusted insiders allow privileged access to untrusted outsiders, leading to the installation of malware or ransomware," he says. In June the FBI estimated such attacks have resulted in $3 billion being swindled from businesses around the world, he adds.

Back to basics

Organizations need to go back to basics. "There is no substitute for continuous security training and education of all employees to ensure the security mindset permeates through every business transaction and is weaved into company culture," Arora points out.

To mitigate risk, organizations need to shift their mindset toward "breach acceptance" rather than prevention, he believes.

Although mobile devices allow the unification of multiple accounts, many users end up using personal accounts for work. "Not good," notes Sean Sullivan, security adviser for F-Secure, a cybersecurity and privacy company based in Helsinki, Finland. "There should be a clear division between personal and professional accounts," he says.

He also urges employees to learn how to archive. "There is almost no good reason to keep 10 years of communications at your fingertips," he says. A desktop client can sync a mailbox and archive the old stuff to an offline file. "Then delete and sync. If you don't know how, get an IT staffer to assist."

> **"There is no substitute for continuous security training..."**
> – Gorav Arora, director of technology, Gemalto

Not taking all the precautions in protecting health and financial data, for example, opens an organization to legal liabilities. Ken Dort, a partner in the IP Group of Chicago law firm Drinker Biddle and chairman of the firm's Technology Committee, notes that companies have regulatory responsibilities in safeguarding personally identifiable information (PII) relating to employees or customers, and personal health information of patients held by health care providers.

Proprietary and/or confidential information – such as research and development plans, corporate financial data, marketing plans and pricing information – can be valuable to competitors.

"The ubiquitous use of mobile devices to permit the flexibility of today's workforce has exposed sensitive data to greater risk of loss as these devices leave the secure facilities or systems of companies with otherwise solid security practices," Dort says.

The fact is mobile data faces a higher risk of loss than data kept within the walls of a company's secure framework. "Given the small size of most mobile devices, intentional theft of data by disloyal insiders becomes easier as the capacity of these devices grows ever larger," he adds.

Arora notes that the data perimeter has been eroded by the mobile workforce and adoption of the cloud. Focus should instead be on securing the data through encryption and strict access controls, and using strong authentication to elevate the assurance of the end-user identity, he says. ■