Mobile security

As the ubiquity of mobile devices continues to grow, security concerns increase as well.

ebook
An SC Magazine publication

Sponsored by
Hewlett Packard Enterprise

A changing mobile world

CISOs are under increased pressure to provide mobile device security apps to protect corporate data. Jim Romeo reports.

After the devastating attack on a holiday party at the Inland Regional Center in San Bernardino, Calif., on Dec. 2, 2015, the FBI sought the assistance of Apple. It asked the company to unlock an iPhone 5C that was found in the attacker's car.

The demand grew into a complicated legal and ethical issue, but it also sent a message: mobile security is a big deal – for the good guys, the bad guys and just about everyone who uses mobile devices or manages their security.

As the ubiquity of mobile devices continues to grow, security concerns increase as well. Whether a smartphone, tablet or watch, these handy tools are at the vanguard of IT safety, security and risk.

These gadgets have become a daily essential for both personal and professional lives, providing communications, entertainment, news and research, not to mention a fashion accessory.

This is forcing IT security managers and leadership to reevaluate them for they are no longer merely a simple tool but a corporate vulnerability. It is now incumbent on those charged with the security of their enterprise to address how and where these devices are used, who controls what's inside them and, subsequently, to build appropriate security measures to enable their safe use – safe, that is, from a corporate data perspective.

OUR EXPERTS: BYOD

Paul Cotter, senior security architect, West Monroe Partners

Faisai Ghaus, vice president, TechNavio

Jason Gillam, faculty member, Institute for Applied Network Security (IANS)

Andrew Hoog, CEO and founder, NowSecure

Jason Hong, associate professor, Carnegie Mellon

Jerry Irvine, CIO, Prescient Solutions

David Lingenfelter, information security officer, MaaS360 by Fiberlink, an IBM company

"Nearly two-thirds of Americans are now smartphone owners, and for many these devices are a key entry point to the online world," according to a Pew Research Center report, "U.S. Smartphone Use in 2015."

And, the number of smartphones and other mobile devices just keeps rising. Forrester Research states, "As the worldwide population of smartphone users approaches two billion, and tablets numbering in the hundreds of millions, the scope of the mobile computing revolution rivals that of the move from monolithic systems to client/server in the 1990s."

The BYOD factor

Smartphones and mobile devices help manage different facets of our daily lives. When the personal mobile device is used as a resource for employment purposes, its role changes from managing personal lives to professional lives. This is the bedrock of the bring-your-own-device (BYOD) phenomenon. It is alive and well – and growing. How much? According to the market research firm TechNavio, the market is expected to grow at 13 percent compound annual growth rate through 2019.

"Growing BYOD policies among enterprises are helping organizations increase productivity and promote innovation," says Faisai Ghaus, vice president of TechNavio, a London-based global market research firm. "Employees are more comfortable using their own mobile devices, which makes them more productive and also increases the probability of innovation."

However, more users mean more opportunity for a security breach. Consequently security solutions are greatly in demand, he adds.

Mobile

5.2M

Smartphones lost or stolen in the U.S. in 2014.

– Consumer Reports

In the cloud: Employing mobile device security

IT security managers working in today's mobile computing environment are working more closely with cloud applications and data, as well as legacy data based in enterprise applications. The cloud presents new and different challenges, such as how one secures data on a network over which the IT team has no physical control. After speaking with a number of experts, we've assembled some points to consider in building and strengthening security in such environments.

Plan – Before implementing a cloud computing application, plan accordingly. Insure that data privacy, confidentiality and overall integrity are instilled in the baseline data being used.

Study the environment – Take time to understand the environment in which the devices are used. Be it cloud computing, global collaborative communications or one where sensitive data is exchanged, security managers need to know the limits of their environments. This will help determine the tools, technology and investment decisions.

Control – Understand your ability to control device security within the diverse environments in which they are likely to operate. This means being able to disable or enable security features remotely based on circumstances, use and potential misuse. This also means understanding the differences in operating platforms – from one device to another – and the vulnerabilities that each poses.

Vigilance – Be vigilant of the applications that operate on legacy databases and those used by mobile devices. Each might have very different infrastructure and security best practice requirements that could be significantly different.

Endpoints – Gain an intimate understanding of how and where mobile and connected devices exactly connect with the cloud. Insure that safe virtual private networks exist for sensitive information and data to transmit among the cloud, the enterprise network and connected devices.

Threats from mobile security stem from a multitude of uses, each requiring different solutions. Risk by involve the device itself or the applications the device is running. These applications can run the gamut from commerce and communication to data access and custom functionality.

"BYOD is forcing everyone to take a much closer look at mobile security than they would have if IT was supplying the hardware," says David Lingenfelter, an information security officer at MaaS360 by Fiberlink, an IBM company based in Blue Bell, Pa., that specializes in smartphone and other mobile device systems. "This is a good thing, as we tend to grow comfortable with our level of security and risk."

However, this also can pose a challenge. While a user might be complacent about security with their own device, that same attitude could cause a corporate vulnerability in a BYOD situation. Lingenfelter cautions that the BYOD movement forces security teams to take a fresh, hard look at their security strategy. Firms often do not want to restrict the convenience of BYOD from their employees, but if allowing it they must be aware of any security vulnerabilities that might exist.

"Employees are going to want to keep their personal information on BYOD devices," says Lingenfelter. "Companies have to understand and develop processes that allow the end-user to do that, all while assuring the end-user the company does not want to control or limit the usability of the devices."

25%

Percentage of mobile devices that encounter a threat each month.

– Skycure

Jerry Irvine, CIO of Prescient Solutions, a Chicago-based IT outsourcer, is quick to point out that the BYOD movement has helped push requirements for mobile security, but has not managed to eliminate vulnerabilities and risks that plague these consumer-grade products.

"Mobile device management (MDM) applications provide the ability to encrypt a phone in total or in part, to delete them remotely if lost, and to manage applications on the phones," says Irvine, who also is a member of the U.S. Chamber of Commerce's Cybersecurity Leadership Council. "Nevertheless, BYOD devices still create significant vulnerabilities due to the requirements for remote connections to internal network resources by end-users."

Because end-users have the ability to install nonstandard applications and access unauthorized sites via their browsers, he points out that vulnerabilities can be transmitted from them to the internal devices in the enterprise that they are allowed to access.

Further, whether the mobile device belongs to an employee or company, it is commonly used with cloud functions, such as personal or corporate data storage or software-as-a-service (SaaS) applications, as well as connecting to corporate applications, such as databases. This hybrid IT model poses its own risk and also demands strong mobile security solutions.

Andrew Hoog, CEO and founder, NowSecure

Lingenfelter says it is easy to lose track of where the actual data resides in a hybrid model. If security managers are not certain where that data is, he notes, they cannot ensure they have the proper levels of protection in place. "Legal responsibility and ownership also come into play in cloud computing and hybrid IT," he says. "Security managers working with cloud computing [providers] should understand who owns the data, who is responsible for its protection and who is responsible for the availability of the system."

From a security perspective, mobile users need an appropriate degree of permissions, authorization and authentication in order to gain access to sensitive information. Shaping such security practices will vary depending on many factors, including the IT environment, and understanding how and where data and information is accessed, used and exchanged.

Managing mobile apps

According to Gartner research, "By the end of 2017, market demand for mobile app development services will grow at least five times faster than internal IT organizations' capacity to deliver them." With this momentum, mobile apps are in the cross hairs of all security managers and climbing the ladder of competing security priorities.

A quarter of all mobile apps have at least one high-risk security flaw, according to the "2016 NowSecure Mobile Security Report. Leaky apps are the number one security problem facing mobile users today, says Andrew Hoog, CEO and founder of NowSecure, an Oak Park, Ill.-based mobile-focused security provider. "They transmit and/or store private user information and have vulnerabilities that can result in the loss of private, sensitive user data."

Jason Hong, an associate professor in the School of Computer Science, Human Computer Interaction Institute at Carnegie Mellon in Pittsburgh, agrees. He says that a key problem is the number of inexperienced mobile application developers. "To be fair, it's very hard to get security right, but it's surprising to see how many apps don't even

$21M

Average U.S. enterprise cost from cybercrime in the financial services sector.

– Ponemon

bother to encrypt network data," Hong says. "This is a long-term problem that will require better tools for developers and for computer science programs to change how they teach students."

Another problem, Hong says, is the large amount of sensitive data that apps are collecting about users. "A lot of apps get unique phone ID and location data and use it in unexpected ways, often for advertising, but also for geotagging social media," he says. "This means that employees might be leaking potentially sensitive information, especially in the case of soldiers deployed in theater." He points to one incident where insurgents reportedly destroyed some U.S. helicopters due to a geotagged photo that was shared on social media.

> "Jail-broken devices should not be allowed on the enterprise network."
>
> *– Jerry Irvine, CIO, Prescient Solutions*

To yield the best levels of security, Prescient's Irvine emphasizes the importance of implementing industry best practices and manufacturers' recommended configurations. Devices should be configured to place all enterprise applications and data into separate, encrypted partitions on the device, he says. Only defined, tested and known applications downloaded from the device manufacturer's application sites should be allowed on the device, he says.

"Jail-broken devices should not be allowed on the enterprise network or allowed to access devices on the enterprise network," says Irvine. "Data loss prevention software should be configured to block specific categories of data, as well as data with certain keywords or phrases in them. Mobile device applications should not be allowed to gain access to personally identifiable information."

However, there is some disagreement as to which is the safest method for downloading apps. Downloading software from a vendor conflicts with the consumer security advice of Google and Apple, which recommend that applications be download from their respective app stores. The argument is that only vetted applications approved by the operating system vendors are safe for consumers, while security experts argue that enterprise applications should be downloaded from the vendor sites.

Unified communications and mobile security

"Overall, the security implications with respect to the use of unified communications is a bit of a dichotomy," says Jason Gillam, an expert in IT security and a faculty member of the Institute for Applied Network Security (IANS). "On the technical side, it leads to generally more secure communications because the data streams for most major streaming service providers are encrypted end-to-end."

However, he says, appearances might be deceiving. If you compare a traditional conference call with a newer streamed videoconference, you will find that even if parts of that traditional call are originating from encrypted voice over IP (VoIP), the entire message might not be secure. This is also the case with legacy, unencrypted endpoints, such as Plain Old Telephone Service (POTS), which does not guarantee end-to-end encryption.

To attend the streamed video call, you must use a specific endpoint product, often an app, which typically claims to offer end-to-end encryption. Gillam says that on the human behavior side, we tend to be more careless with matters of confidentiality for this type of technology.

"The sophistication of unified communications, becoming ever more convincing, leads us to behave more and more as if the other parties of the conversation are physically in the same room with us," Gillam says. When discussing confidential matters this might be okay if that room is a conference room or private office,

8%

Percentage of total reported threats that originated from a Wi-Fi network with "Free" in its name.

– Skycure

he says, but not a public location, such as the office lunchroom or an airport. "However, in these types of calls it can be easy to lose sight of where we really are."

In addition, he adds, there is the potential concern of carelessness with video content, such as accidentally displaying a whiteboard with sensitive information in the background. "This is akin to shoulder surfing through the lens of a mobile device. Security managers should be doing the same things for mobile communication solutions that they should also be doing for other technology. This includes using strong, proven crypto ciphers, patch security issues promptly, enforce strong password policies, and so on."

Paul Cotter, senior security architect, West Monroe Partners

The security of a mobile device user who communicates through an established unified communication platform is dependent on the platform provider for much of their security. How much security exists can be dubious or unknown. Paul Cotter, a senior security architect at West Monroe Partners, a Chicago-based business and technology consulting firm, says that applications employed by unified communications service providers are often outside the control of the organization and therefore represent an unmanaged threat for data leakage, malware and vulnerabilities.

A security manager should consider all potential channels as part of the organization's risk assessment, Cotter says, even when the organization doesn't control the communication channels. He posits that mobile devices, in a more dynamic manner than laptops, introduce the additional complexity of having both an online and offline use case, with potentially different handling of malware in those scenarios, both of which must be considered.

The organization should strive to continually understand how each of the tools works, adds Cotter. "Processes and procedures currently in place in their environment enable organizations to address each of these threats, in order to understand where additional investment may be needed in this rapidly-changing environment."

E-commerce and data protection

According to research from Custora, a predictive marketing platform vendor, nearly a third of U.S. holiday retail sales in 2015 were conducted via smartphones or tablets. Overall sales in 2015 saw approximately a 12 percent increase over the previous year.

Marketing suite vendor Criteo also issues quarterly reports on the state of mobile consumers. Its 4Q 2015 report, "State of Mobile Commerce," found that about 30 percent of all e-commerce transactions are conducted via mobile phone. In 4Q 2014, Criteo described mobile commerce as "growing like a weed." The company said that transaction levels in the United States are on a steady course to reach 50 percent via mobile device, approaching levels in Asia where they are greater than half of all transactions.

Assuming these statistics are accurate, that means a lot of personally identifiable information stored on mobile devices – such as credit card numbers, birthdates and account numbers – is potentially at risk.

"Organizations need to carefully consider what datasets they will allow to be stored on a mobile device for offline use, versus what should only be accessed in an online/connected manner," says Cotter at West Monroe Partners. "Any data that is synchronized offline should be considered a potential dataset that could be leaked from the mobile device in the event that a mobile device is compromised or lost."

He advises that a system-patching strategy should be reviewed and updated to incor-

40%

Number of U.S. employees of large companies that use their personal device for work.

– Gartner

porate the availability and enforcement strategies available for mobile devices. Unlike normal laptops and desktops, mobile device patch availability might be constrained and ultimately determined by updates released by the mobile communications carriers.

Organizations also need to consider if and how the devices can support audit requirements for access to data, Cotter says. He uses the example of medical records. If such records are synchronized to a mobile device and that device is accessed by multiple employees, the security team needs to know, with a high degree of confidence and reliability, who and when has access and when updates were made. Knowing the detailed elements of usage will factor into the company's overall regulatory compliance and security posture.

At the same time, the security team must be cautious to protect against malicious software or malware designed to target a mobile device and cause damage or disruption. ■

For more information about ebooks from SC Magazine, please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

20M

Estimated number of apps that will have malware by the end of 2016.

– TrendMicro

Sponsor

Hewlett Packard Enterprise

Hewlett Packard Enterprise is an industry leading technology company that enables customers to go further, faster. With the industry's most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive and more secure.

Additional information about HP Enterprise Security Products is available at http://www8.hp.com/us/en/software-solutions/enterprise-security.html.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Brian Wask
brian.wask@haymarketmedia.com

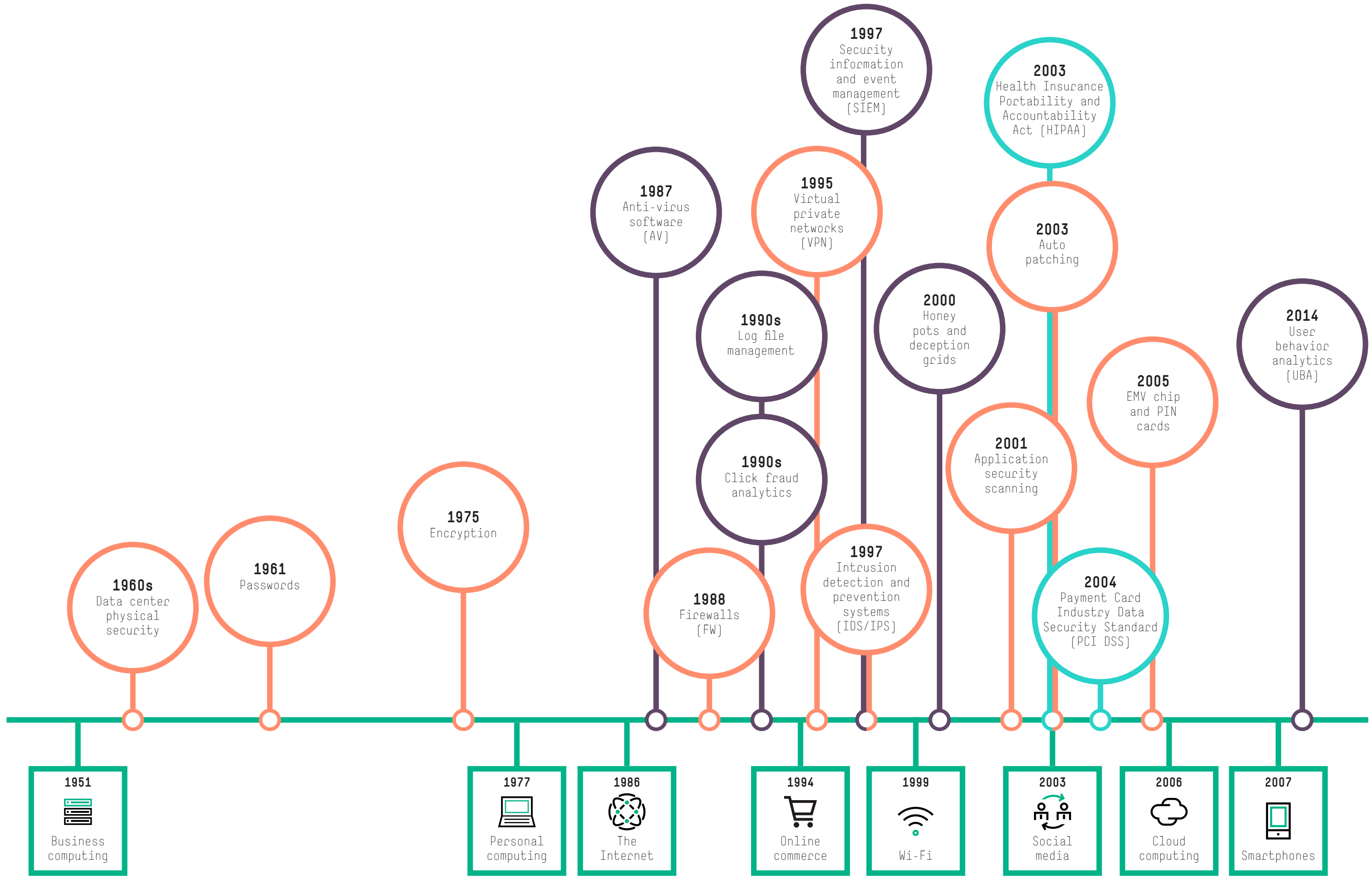
SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
EAST COAST SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

Hewlett Packard
Enterprise

Timeline of disruption

Security technologies are implemented to disrupt attackers by making their attacks more difficult to execute and/or less profitable. The timeline provides a brief history of information technology innovations and the enterprise security defenses developed to disrupt cyber-attacks.

Are your business innovations aligned with your security defenses?
hpe.com/software/BusinessOfHacking



1960s Data center physical security

1961 Passwords

1975 Encryption

1987 Anti-virus software (AV)

1988 Firewalls (FW)

1990s Log file management

1990s Click fraud analytics

1995 Virtual private networks (VPN)

1997 Security information and event management (SIEM)

1997 Intrusion detection and prevention systems (IDS/IPS)

2000 Honey pots and deception grids

2001 Application security scanning

2003 Health Insurance Portability and Accountability Act (HIPAA)

2003 Auto patching

2004 Payment Card Industry Data Security Standard (PCI DSS)

2005 EMV chip and PIN cards

2014 User behavior analytics (UBA)

1951 Business computing

1977 Personal computing

1986 The Internet

1994 Online commerce

1999 Wi-Fi

2003 Social media

2006 Cloud computing

2007 Smartphones

🟧 **Build it in: Technology built into the enterprise to block access and attacks**

🟪 **Detect and respond: Technology used to more effectively identify attacks**

🟦 **Recover and comply: Processes to improve overall security programs**

1961
Passwords introduced

Now
67% of organizations enforce strong password policies.

**UBM, *Most Effective Security Technologies and Practices*, May 2016.*

1975
Encryption introduced

Now
65% utilize data encryption.

**UBM, *Most Effective Security Technologies and Practices*, May 2016.*

2001
Application security scanning introduced

Now
75% of mobile applications have at least one high- or critical-severity vulnerability.

**HPE, *2016 Cyber Risk Report*, February 2016.*

2005
EMV chip and PIN cards introduced

Now
EMV cards can fetch more than 4X the price of swipe cards.

**HPE, *The Business of Hacking*, May 2016.*

4AA6-5111ENW, April 2016