6 Things That Will Accelerate Enterprise Mobility Security Adoption

A massive cyber-security breach from mobile device vulnerability is coming, and the marketplace isn't prepared for it.

A recent report titled *"The Mobile Economy 2015*[1]*,"* from the GSM (Groupe Speciale Mobile) Association, a global mobile consortium which represents the interests of mobile operators worldwide and produces industry-leading events such as the Mobile World Congresses and the Mobile 360 Series conferences, reveals that the world has now reached 3.6 billion unique mobile subscribers. Half the population on the planet now has a mobile device. And by the year 2020, the GSMA estimates that another billion people worldwide will be connected via at least one mobile device. Also by the year 2020, mobile broadband connections will nearly double and account for more than 70 percent of the global base. When you consider that the Internet as we currently know it, is less than 20 years old, these are staggering numbers.

The world of IT infrastructure and networking has undergone an equally staggering transformation over the past 15-20 years. IT shops are spread incredibly thin with resources trying to maintain SLAs for business and IT service delivery, while maintaining acceptable targets for Information Security (InfoSec) risk and compliance. Considering that 2014 saw 1,541 breach incidents affecting over a billion records – a staggering 78 percent increase from 2013 – it is never been more clear that the CISO of 2015 has his/her work cut out.

Arguably, all the cyber breach publicity is good for InfoSec vendors in that it is creating more marketplace need but what is missing from the increased publicity is information about these breaches, critical to creating a global database of criminal cyber activity for forensics much like Interpol has for other criminal activity. What little information we have about the current ongoing investigations from these breaches is mostly coming from the vendor community frantically trying to bring awareness to public and private industry and government entities that it's not a matter of if you are going to get hacked, but a matter of when. The organizations that have systems, processes and subject matter experts (SMEs) in place to stem the bleeding are going to fare the best with the least impact to customer retention and brand reputation.

Something Mobile is Missing…

Information is available about some of the more recent high profile breaches. For instance, we know that the Target hack during the holiday season of 2013 was the result a hard-to-find virus that infiltrated the RAM of POS transaction terminals in stores across the country. Early

[1] *http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf*

on in the breach, a tech actually notified a manager that something anomalous was afoot but remediation to stem the bleeding did not commence for another two-to-three weeks.

In the case of the Anthem Healthcare breach – the largest healthcare hack to date at the time – it was revealed that in early 2015, it had estimated that the seeds of the attack were planted in May of 2014. But the healthcare provider did not realize that its systems had been breached until January 2015. Spear phishing is said to have been the origins of the attack but as with other high-profile breaches, not much has been revealed about the breach that can be used for forensics as we might see with an FBI or Interpol database, if there were a group of bank robbers targeting high profile banks around the globe. The U.S. Computer Emergency Readiness Team (U.S. CERT) is a Government website that does a great job of collating global threats and issuing alerts via RSS. But at this writing, there appears to be no global database of data assembled for public or government investigative consumption with forensic details that helps authorities track down hackers. Most of this is done at the InfoSec vendor level where competition encourages silos of information about the anatomies of cyber-attacks. We do know that there is a lot that we don't know about cyber-attacks in a unified, structured format available to cyber-crime fighters shared across international borders.

What we do know about high-profile cyber-attacks is that we seldom read about the avenue of intrusion of a breach originating from a mobile device. Yet the data presented earlier in this paper suggests that the mobile endpoint is exploding in adoption; mobile devices and tablet Internet use surpassed desktop computers sometime last summer! When we factor the expansion of BYOD and COPE (corporate owned device personally enabled) in enterprise organizations, one has to deduce that a main avenue of intrusion for endpoint vulnerability must be mobile.

Mobile, however, is missing from this cyber vulnerability equation and until we see a major breach with root cause linked to mobile endpoints, mobile security will continue to be the redheaded stepchild of on premise InfoSec initiatives. This barrier for mobile security adoption only needs a catalyst – a high-profile brand-name breach affecting millions – and the data surrounding mobile suggest a cyber storm is brewing:

- Biggest threat over next 3 years is nation state attackers targeting mobile devices[2]. Mobile devices are highly vulnerable to "rogue towers" in Europe where countries are clustered with close proximity to international borders.
- The growth of connected devices in enterprise systems will make it more difficult to secure access to data. This is the number one inhibitor for securing access to data, systems and physical spaces. Mobility accelerates this.
- Complexity of IT operations coupled with the growth of unstructured data assets will cause a substantial increase in security risks. Mobility accelerates this.
- Mobile payments will create new challenges to existing cyber posture. Mobility accelerates this.

Mobile security adoption has gained a foothold over the past 10 years, but the vendors have approached the marketplace with an all-or-nothing approach. The result has been overkill for closing the door to the root cause of the primary mobile device vulnerability – the application layer. A recent Gartner press release from the Gartner Risk Management Summit in Dubai, September 2014, reported that 75 percent of mobile applications will fail basic security tests through 2015. The proximity of personal applications on mobile devices to network applications and their proximity to corporate and government IP (some of which is a matter of national security) begs the question "why isn't the marketplace enabling enterprise mobile application security on a wide-scale basis?"

[2] *http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf*

The Answer is Threefold:

1 *The traditional African proverb, "It takes a village to raise a child," is never truer than in our mobile security space.*

Corporations and government trying to deploy effective mobile security solutions lack the subject matter expertise in-house to move the needle to better security, less risk. Their expertise lies within their product/service scope and capability. This is why software vendors and consultancy groups have thrived over the years; if it were so easy to do custom enterprise app deployments, then this would be the norm, but they are not. Corporations and government know what they are good at and outsource what they know they need SMEs for.

2 *Because of lack of wide-scale adoption, most mobility security deployments are custom installations.*

Our industry lacks a standard default deployment structure that can be documented and scaled to meet other enterprise systems' needs. Without such a guided and systematic approach to deployment, each engagement is an exercise in "we don't know what we will get into next, we'll just have to wait and see what comes up and try to fix it as we go."

3 *Cost. The pricing model favors large-scale and months- or even years-long deployment cycles with exponentially greater services (installation} fees than the licenses themselves.*

When you factor in the cost of human resource hours consumed to learn the systems (and relearn them when resources rotate in and out of organizations), the price can be staggering. With the recent Good Technology acquisition from BlackBerry, the potential for competition to bring the price of per-seat licenses down has been all but negated. There are now less than a handful of mobile security vendors capable of enterprise-sized deployments. Until more players enter this space, a manopoly-like ecosystem exists that stunts the growth of competitive pricing.

6 accelerators for wide-scale enterprise mobility adoption – it will improve down the road because of:

1. Internet of Things:

Simply put, the Internet of Things, or IoT, is the networking of objects embedded with software that are connected to one another. The objects collect and exchange data with the intent of creating improved interactions between device and human. An example of IoT might be sensors put in concrete in a bridge in Minnesota that warns oncoming traffic of ice on the road. The two machines connected (M2M) in this example would be 1) concrete-with-sensors and 2) mobile device (or wireless onboard automobile device).

> According to a recent Gartner press release, 75% of mobile applications do not include basic security testing.

The enabler or access point for IoT is your mobile phone. Your device ideally has a secure connection to your network but who is securing the IoT connection? The previously-referred-to GSMA report on mobile adoption reports that as of 2014, there were more than 700,000 M2M connections. By 2020, the IoT will surpass 1 billion M2M connections, all accessible by your handheld (or perhaps bodily implanted by then) mobile device. Your mobile connection to the IoT will be your lifeline to all that is necessary for day-to-day functions – home, office, vehicle accesses; banking access; shopping payment processing access; literally every access point to your daily lives. One only has to gain control of the IoT (or mobile) access point to take control of your business and personal lives. Very soon we will be adding to our IT complexity issue new complexity creating a new breeding ground for network compromise accelerated by IoT and mobile. If the "big one" originating from mobile device source is to happen, it will be IoT that is the catalyst.

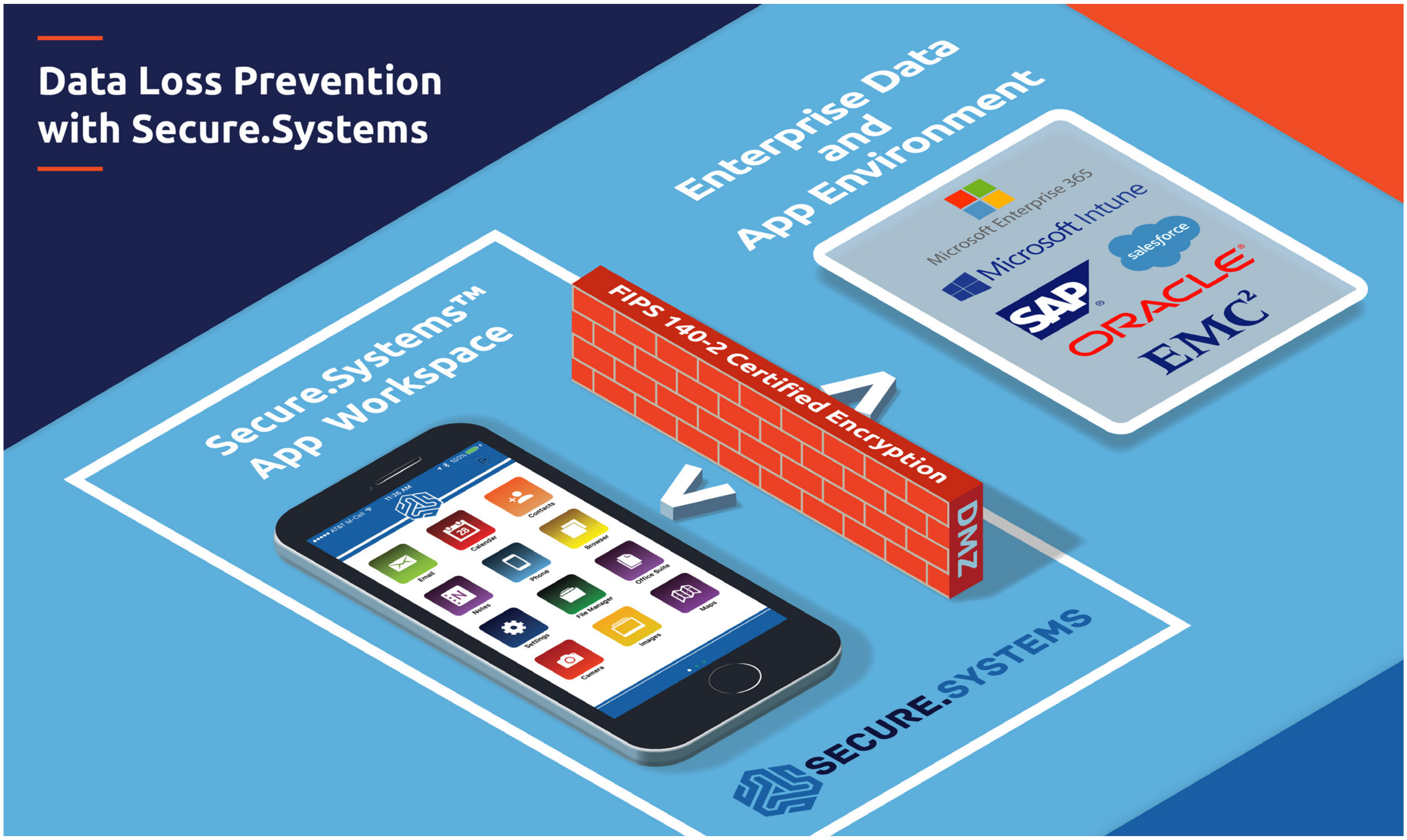
2. The expansion of the mobile app stack must include more than just the Microsoft Office apps and web browsers:

Enterprises have taken notice of the aforementioned Gartner press release stating that 75 percent of mobile applications don't include basic security testing. The response from the marketplace has been to limit mobile app deployments to basic business productivity apps. What you won't find as a self-contained app built for mobile are enterprise decision-support applications affecting manufacturing, HR or other critical business processes easily accessed on premise from desktops or terminals.

The enabling technology that will accelerate more business decision-support mobile applications is the containerization of the mobile workspace, creating segmented partitions on mobile devices where business-procured IP is untouchable from other personal applications on the device.

3. The mobile "big bang" attack:

When it happens, if there is any information about the breach and its roots to mobile, it will be, oddly enough, good for the acceleration of more wide-scale adoption of mobile security deployments. The big question however, is what legislation will come from the breach and how well will mobile security initiatives be aligned to other security initiatives in enterprise datacenters? Many



InfoSec pros just don't see mobile security as a necessity. When asked in a recent Spiceworks survey[3] titled "Weathering the Mobile Storm," one InfoSec pro had this to say: "We don't use mobile device security because too many other things are bigger issues; we haven't yet experienced a problem with mobile security to cause it to be a higher priority."

4. Government intervention:

When the big mobile bang does happen, what will be the reaction from the U.S. Government? There have been some gestures made – the January 2015 Stanford University Cyber Summit led by President Obama[4]; the recent incident notification guidelines from FISMA for notifying US-CERT[5] – but until compliance standards with stronger punitive teeth are mandated (i.e. HIPAA, Sarbanes-Oxley, IRS Pub. 1075, etc…), other bigger issues in enterprise datacenters will continue to be front and center for InfoSec managers.

5. Cheaper options, faster to deploy:

Competition just got worse with the recent acquisition of Good Technology by BlackBerry[6]. The list of mobile security vendors with containerized work stations is two – SyncDog, Inc. and BlackBerry by way of Good acquisition. SyncDog offers simple and affordable pricing for application security (Secure.Systems™) across the SyncDog secure deployment framework. The cost is per seat and the secure framework provides a standard, repeatable process for installation that even includes a cloud-based developer testing environment called Mobilization as a Service (MaaS).

BlackBerry is likely to keep the subject matter expertise acquired by Good in place because it is uncharted technology for BlackBerry. However, it is unlikely that the pricing structure for Good will deviate much from the current model. With only one true competitor in SyncDog – who operates across a different pricing model – BlackBerry has no motivation to alter its margins.

6. The distance between CISO and CEO/BOD must shrink:

Alarming numbers come from the Ponemon Global Megatrends in Cybersecurity research report commissioned by Ratheon[7] -- only 14 percent of CISOs report to CEOs, and just 22 percent of CISOs brief boards of directors on cyber strategies. These numbers validate the comments from the IT pro from the Spiceworks survey "too many other things are bigger issues; we haven't yet experienced a problem with mobile security to cause it to be a higher priority." Wide-scale mobile security adoption in large enterprises will take off when c-level executives and boards of directors consider it a strategic initiative and drive it down to the lower levels of their respective organizations. Perhaps the "big mobile bang" breach will be the brand-damaging factor that initiates this change. Whatever the case may be, there continues to be bigger issues on the plates of InfoSec managers that keep them from putting mobile security front and center. Clearly a storm is brewing and change awaits in the wings.

InfoSec is a big and complex initiative within a large enterprise of 10,000 or more employees. In addition to the thousands of endpoints, email and network data that needs to be secured, other sub-initiatives vie for

[3] *https://itreports.spiceworks.com/reports/Weathering-Mobile-Storm-Report-October-2014.pdf*
[4] *https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit*
[5] *https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf*
[6] *http://press.blackberry.com/press/2015/blackberry_to_acquire_good_technology.html*
[7] *http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf*

human resource allocation. Network managers and systems' administrators maintain a diligent firefighting effort to optimize business service levels while adhering to compliance initiatives. Amongst the chaos and complexity, avenues of intrusion for malicious hackers must be shored up. And somewhere beneath the covers of all of this work, the exploding number of mobile devices and vulnerable applications they bring to your network have to be accounted for and managed. Mobile security is being embraced in enterprises across the globe but internally there is a lot of competition for the resource allocated to it. The organizations that see the potential for threat penetration from IoT, escalation in mobile adoption, and general application vulnerability are going to be the best prepared to deal with breach containment.

Best-in-class enterprise mobile security today must be a team effort between security vendor, application developer and the deploying organization. Each has its area of expertise and understands its contribution to the overall strategy. The security vendor brings functional capability in monitoring and management tools to stem the bleeding in the event of a breach. Ideally, the security vendor has a proactive enough approach to prevent a breach.

The application developer must understand that their tools are another piece to a cluster of remote applications that keep remote employees connected with enough decision support data and app functionality to perform job duties as if they were on premise, running the apps from a desktop/laptop. As an integral piece of the application stack, they need to understand that security be an integral part of application testing and deployment.

The enterprise's role in all of this is service provider in as low-risk and high compliance method as possible. It is the enterprise that delivers secure tools to its employees and partners to turn the optimal profit to perpetuate the business or public service. The onus is on the enterprise to understand the leadership role in wide-scale adoption of deeper mobile security strategies. The threat is real and it is staring our InfoSec industry square in the face with ample data that supports the premise that a mobile vulnerability storm is brewing. Throughout our industry – as we do with client security strategies – we need to take a proactive approach to wide-scale enterprise mobile security adoption and prepare for the future. The sophistication of malicious hackers today has reached unprecedented heights.

As an industry, we InfoSec professionals need to be the flag bearers of wide-scale enterprise mobile security adoption. The alternative is letting another Target- or Anthem-type breach dictate our next steps for embracing enterprise mobile security. The former is definitely the better option.