SAMSUNG | stratix

White Paper:

Why You Need an Incident Response Playbook for Mobile Devices

Introduction: The Business Foundation for Security

IT departments struggle with reactive mobile security measures while under constant attack from cyber criminals. What if an incident occurred within your enterprise? This incident response playbook can be used as a template for processes and documentation.

Security and mobile devices present complex challenges for many enterprises. As employees need and demand access to business applications, IT teams struggle with granting access due to security concerns. It's a delicate balance that could create a disaster if not addressed properly.

While many employees just want to gain access to email and a few key applications, they often don't understand how criminal hackers prey on mobile devices via Wi-Fi networks, jailbroken systems, password generation tools and many other tactics. At the same time, untethered workers, including field engineers, temporary construction site staff, on-location deployment teams and many others truly need secure mobile access to corporate applications in order to do their jobs.

Mobile Device Management (MDM) may initially seem to suffice as a mechanism for securing mobile devices. The focus of MDM is security of the device itself, although some MDM solutions blur that line and include basic apps such as email.

Enterprise Mobility Management (EMM) is a more robust solution that includes both device and application security. Business applications can be containerized, and usage is controlled by the IT department. EMM is more secure, provides significantly more configuration options, and is consequently more expensive. However, a primary issue with many EMM solutions is the wide array of devices that are supported and thus the inequivalent policies that can be applied to the myriad of devices.

According to the Verizon Mobile Security Index 2018, "32 percent of companies sacrificed mobile security for expediency. They were 2.4x as likely to suffer data loss or downtime."[1] No enterprise wants to be part of this statistic, but businesses are under constant pressure to adopt new systems.

Incidents such as an employee leaving a phone at an airport can be addressed right away, but what about when business application login credentials are compromised due to a rogue Wi-Fi connection? Within a matter of minutes, a hacker may infiltrate a complex corporate system, undetected, and continue to access these systems. For instance, malicious hackers had access to confidential patient data for nearly a year at a large national health insurance provider before the breach was detected.[2]

Following mobile device security best practices minimizes potential risk, and the Verizon Mobile Security Index 2018 outlined several best practices:

- Create a custom app store
- Deploy an MDM/EMM solution, including containerization
- Train employees and create an Incident Response plan
- Control or eliminate Wi-Fi usage and implement data loss prevention (DLP) systems

> **32%** of companies sacrificed mobile security for expediency. They were 2.4x as likely to suffer data loss or downtime."
>
> - Verizon Mobile Security Index 2018

Mobile security is now a necessary, foundational component that drives budget decisions and resource allocations. Building a strong mobile security solution, including protections for the growing remote fleet, is now a priority.

The implementation of that, however, won't happen overnight. Oftentimes, IT staff must reactively deal with the current systems while proactively architecting the next generation of tighter mobile security in parallel. As such, this how-to guide will be split out based on the following:

- **Today: Playbook for addressing mobile data breaches.** This section will define a playbook that can be implemented as the basis for your incident response.
- **Tomorrow: Ensuring that painful lessons aren't repeated.** This section will discuss creating a go-forward plan focused on an elevated level of security measures.

First a Breach, Then a Response

Today: Playbook for Addressing Mobile Data Breaches

It's every company's worst nightmare: alerts and/or forensics related to a potential breach or hack, and the stark realization that sensitive company data may have leaked. Aside from breaking the unpleasant news to the CIO, there are often legal, regulatory and social obligations to be addressed while investigating and mitigating the issue.

While some issues (such as a DDoS attack) may be minor or perhaps a false positive, having a well-documented and practiced plan of execution is not only a solid business approach but often a regulatory requirement. Important components of this Incident Response plan include a clear definition of processes and expected tasks.

Step 1: Problem Definition: A Little Disaster or a Big Disaster?

The first step in addressing a potential security breach issue is gathering data and forensics, as well as clearly defining the extent of the issue. The steps taken to classify the issue will largely be based on the people and tools already in place.

This data-gathering phase should focus on solid facts and first-hand information, rather than having layers of management refine responses and introduce potential delays. At this juncture, the root cause may or may not be known, and defining the issue should not be confused with attaching blame to any individual or department.

Specifically, the following key questions should be asked as the first phase of fully defining the problem:

The Issue

- When was the issue initially uncovered?
- What is the exact date/time that the issue commenced?
- What is the extent of the security breach?
- Is any data leakage potentially controlled by a regulatory body?
- Was the security hole initiated by a mobile device?

Alerts and Forensics

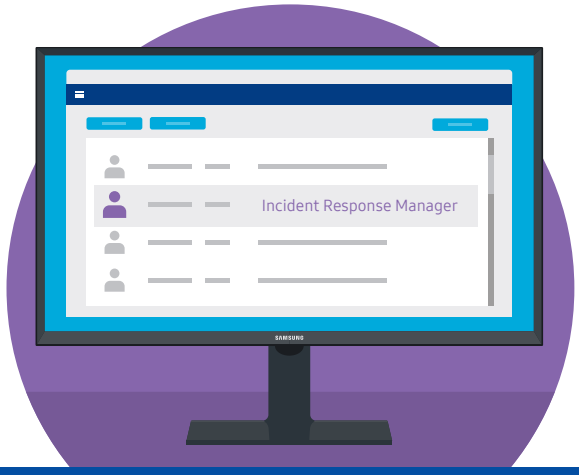
- Were any alerts generated?
- What details are provided within the alerts?
- What additional data can be gleaned by drilling down on alerts?
- Are there pertinent data points just prior to the incident or immediately following the incident?
- Is there a mechanism for holistically cross-referencing alerts with other systems?

Current Status

- What is the status of systems?
- Which systems were affected?
- Are any external systems impacted, including partner companies?
- Are all systems currently operational?
- Is it possible to keep systems operational or could that potentially perpetuate the issue?
- Are there any automated mechanisms that may minimize the issue or that may potentially cause the issue to increase in magnitude?
- What is the impact of shutting down some or all systems immediately?

Step 2: Responsibilities: Who's in Charge of What?

Next, having a game plan in place to determine specific individual and group responsibilities assures that each person is working cohesively toward defining and addressing the problem. Not only does this prevent overlap and gaps, but it also ensures that internal politicking and knee-jerk reactions are minimized.



In some cases, the declaration of a major incident causes some individuals to assume temporary, elevated or altered roles, while other employees may be advised to stand down. For example, a project manager may take the centralized leadership role of Incident Response Manager for the duration of the investigation.

Documenting the exact role of each person and group may be based on individual names, role description or job titles. Defining responsibilities becomes even more complicated when contractors and partners play a role in incident response plans. Non-disclosure agreements (NDAs) and confidentiality statements should be incorporated as part of the plan so as to avoid last-minute definitions and legalities.

It is imperative to update definitions frequently due to job changes. For example, merely stating that Lee is responsible for reviewing alert data and forensics after a major incident is useless if Lee is no longer with the company.

Particularly in regulated industries, it may be necessary to involve legal teams, public relations staff, and/or government entities. Likewise, the contact information for those individuals and teams should be documented.

These specific questions should be core components related to defining responsibilities:

Internal Employees

- Who will review alerts and forensics? Do these individuals have credentials to access the required systems?
- Who will serve as the Incident Response Manager and what specific authority will this individual have?
- What specific role will the security team and management/executives take?
- If a public statement is required, who will own this?
- Is it necessary to involve corporate lawyers or trained incident response individuals?

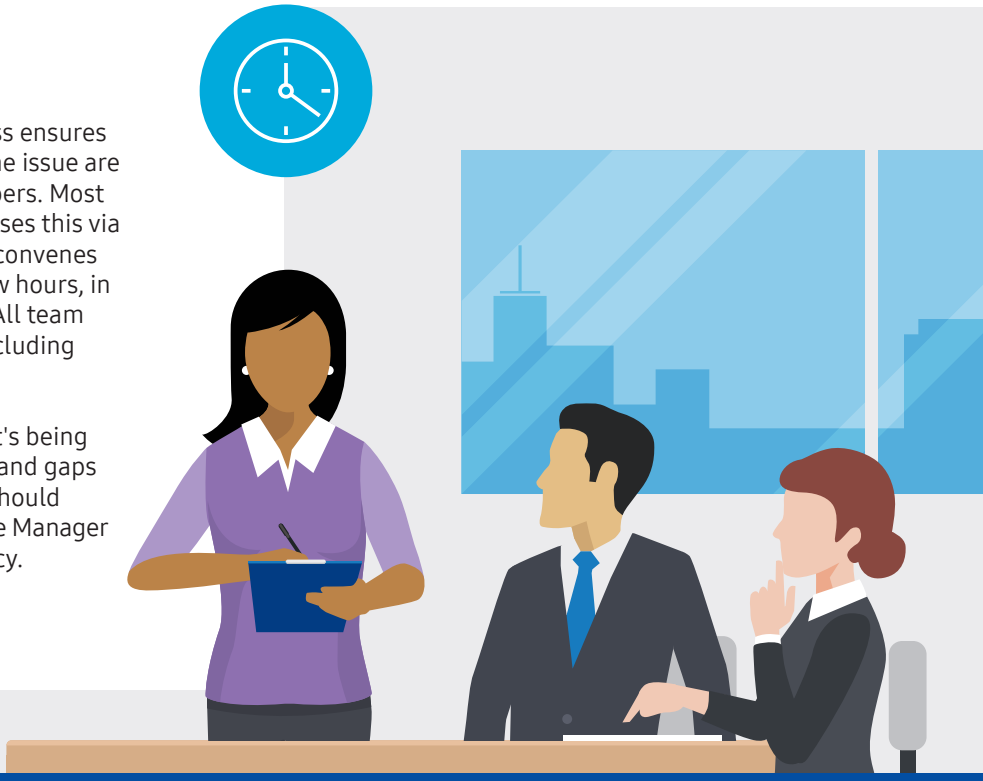
Extended Contacts

- If it is necessary to inform a regulatory body, who will take responsibility for doing so and is that contact information up to date?
- If leaked data or access involved partners, who will communicate with them?

Step 3: Communications: Updates and Timelines

Following this, defining the communication process ensures that all the individuals involved with addressing the issue are kept abreast as to the goings-on of all team members. Most commonly, the Incident Response Manager addresses this via an "all hands on deck" teleconference bridge that convenes at regular intervals, such as every hour or every few hours, in order to provide updates and expected timelines. All team members are encouraged to overcommunicate, including details that may initially appear to lack relevance.

It is important for communications to include what's being done, by whom and when, to ensure that overlaps and gaps don't exist. Although the Incident Response plan should contain detailed information, the Incident Response Manager may need to adjust based on the current emergency.



These specific items should be incorporated into the communications plan:

Incident Response Manager (IRM)

- Who will be part of the interval conference calls?
- What documentation is required, both during the incident and following the incident?
- Where is the documentation repository, and who else has access to it?
- Where or how will the IRM post updates suitable for consumption by all employees?
- How will the IRM communicate with executives and external entities?
- If any facets of the Incidence Response plan fail, what authority does the IRM have to make decisions?

Resources and Timelines

- How will risk, timeline and resource decisions be prioritized?
- If additional resources are required to address specific items because the IT staff is overloaded, how will budget approvals be handled?
- If any assigned tasks fall behind schedule, how will these be addressed?

Step 4: Remediation: Addressing the Technical Solution

Assuming an MDM or EMM solution is in place, administrators can take decisive action such as shutting off or wiping phones.

Today's cybersecurity intrusions may require additional effort specifically targeted at making user phones more secure. This may include patching or updating policies. And more than likely, it means learning about and adhering to industry best practices.

For example, if an intrusion occurred because users were allowed to attach to any public Wi-Fi and a hacker pulled passwords and other information from the data stream, then policies would need to be revisited. Security incidents are not always brute force attacks; oftentimes, a hacker will gain access via a single mechanism and then slowly infiltrate other systems. Unfortunately, users frequently don't know or understand that their specific actions created a window of opportunity for a hacker.

But what if the hacker copied an image of the phone? Depending on the phone manufacturer, it's quite possible that the hacker would consequently now possess all business and user data — including social network accounts, personal and business email, banking information and so much more.

Regarding remediation, the following key items should be part of the Incident Response plan:

MDM/EMM Solution

- How quickly can patches and updated policies be implemented?
- What emergency lockdown capabilities exist within the current toolset?
- Is additional training necessary for IT staff to fully understand the capabilities of the current solution?
- Is the existing system overly complicated and susceptible to mistakes?
- Are there gaps between the current solution and the required or desired state?
- Is a more robust EMM solution necessary in order to ensure adequate security?

IT Items to Address

- Are there any anomalies or alerts that indicate intrusion into other systems?
- Has sufficient user training been made available so users understand security impacts?

Step 5: Testing: What If ... ?

Congratulations! An incident occurred, and fortunately, it was minor and addressed quickly by wiping a single user's phone. You were lucky this time, but during the course of this unplanned event, you discovered a number of vulnerabilities that easily could have been the root cause of a dreadful incident.

What if a serious incident were to occur? It's unlikely that your enterprise is immune to security incidents. According to the Verizon Mobile Security Index 2018, 27 percent of respondents stated that "during the past year their company had experienced a security incident resulting in data loss or system downtime where mobile devices played a key role."

In addition to thorough documentation, testing is a critical element. Exploring numerous "what if" scenarios will ensure that the various teams are as ready as possible to address mobile security threats; whiteboard conceptual testing is not sufficient.

Writing and testing an Incident Response plan is not a one-time event. Especially with technology changes and never-ending security threats, these activities should be updated several times throughout the year.

Some key items related to planning and testing:

Planning

- Do you have the detailed processes in place based on thorough documentation to ensure that a mobile security incident would be addressed properly?
- Who is responsible for updating the mobile device incident response plan?
- Have you adequately prepared for various "what if" scenarios?
- Has your plan been reviewed with external consultants and/or auditors, including regulators?

Testing

- Will testing be performed quarterly, semi-annually or annually?
- Have testing and potential remediation steps been budgeted appropriately?
- What type of tests will be run? Will IT staff be made aware of tests to be run ahead of time or will they be presented with a mock scenario for each iteration?
- Will tests be run by IT staff or external consultants and/or auditors?
- If any facets of the testing process fail, how will these failures be documented and addressed?

A Better Plan

Tomorrow: Ensuring Painful Lessons Aren't Repeated

Today's mobile security infringements require a tougher degree of security measures, and this Incident Response playbook provides the framework for the mobile component of an enterprise disaster recovery plan. Now that we've learned how to identify and address mobile security threats at the access, device and user levels, let's delve into how to prevent such incidents from occurring.

Android Security

First, let's talk about the enterprise mobility workplace. Android-based devices represent more than 80 percent of the mobile operating system market share, but the security of Android devices is often questioned because the OS was not initially designed for the business market.[3] Further, each Android device manufacturer has the option of appending proprietary hardware and software; Samsung packages its additional security components under the umbrella of Samsung Knox.

Samsung Knox is a multilayered security platform baked into the hardware and software of all new Samsung devices from the chip up. Rather than merely validate the integrity of the device at boot-up or login, Knox constantly verifies device integrity via a chain of security checks starting at the hardware level and extending to the operating system. Knox detects any tampering attempts to ensure that your data is always secure. Data is encrypted with the encryption key stored in the TrustZone in the device chipset, even when the device is turned off or reset.

Samsung Knox enables enterprises to address mobile device security in a holistic way and encompasses all facets of security, ranging from initial device registration to policies to updates. Starting with Knox Mobile Enrollment, thousands of devices can be automatically enrolled such that the user only needs to unbox the phone and turn it on. Knox Platform for Enterprise provides an on-device container, which is based on encryption/decryption keys derived from the device chipset. Knox Configure and Knox Manage provide robust policies and management of devices, while Knox E-FOTA (or Enterprise Firmware Over-the-Air) gives you control over updates to the operating system version.

As a result, the various hardware and software components of Samsung Knox uniquely enable enterprises to incorporate an exceptional level of mobile device security.

Conclusion

Having an up-to-date Incident Response playbook is an essential aspect of an enterprise disaster recovery plan. After dissecting all the steps that are necessary for a reactive mobile security platform, it's clear that mediocre solutions require additional time, money and effort — and adrenaline. A more robust solution like Samsung Knox provides unprecedented and unmatched software and hardware security solutions that enable your enterprise to fully achieve your mobile security strategy goals.

Learn more about the Samsung Knox security stack and how it protects your mobile fleet — and the enterprise.

Footnotes

1. Verizon Mobile Security Index 2018
2. Cyber Attack on Healthcare
3. Gartner Newsroom Report

Learn More samsung.com/business insights.samsung.com
Product Support 1-866-SAM4BIZ
Follow us youtube.com/samsungbizusa @SamsungBizUSA

SAMSUNG | stratix

WHP-HHP-INCIDENT-RESPONSE-DEC18SW