SAMSUNG

White Paper:

Building a Cyber Incident Response Plan

Introduction: The Business Foundation for Security

"Incident" is just a word until IT security has been compromised. The mixture of malware, DDoS attacks, lost devices and other threats facing enterprises has never been more complex, which makes it critical to proactively plan and document how your organization would handle a cybersecurity breach. This playbook will help you get started.

While mobile devices represent one threat vector, they are a growing area of focus for bad actors looking to gain access to accounts or data or tamper with servers and systems. That's why it makes sense to begin by considering where mobile device use and policy can leave organizations exposed and how an incident response plan can prevent and mitigate attacks that start there.

Security and mobile devices present complex challenges for many enterprises. While employees need and demand mobile access to business applications and data, IT teams must balance this against security concerns. Despite efforts to raise security awareness, employees often don't understand how malicious hackers prey on mobile devices via Wi-Fi networks, jailbroken systems, password generation tools and many other tactics.

Mobile device management (MDM) or enterprise mobility management (EMM) are essential tools for mitigating the risk of security incidents. Business applications can be containerized, and usage controlled by the IT department. However, no matter how strict your EMM policy implementation, it is impossible to entirely eliminate mobile security risks.

Don't Become a Statistic

According to the Verizon Mobile Security Index 2019, "48 percent of companies sacrificed mobile security for expediency. They were twice 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 technology.

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 can 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 2019 outlined several best practices:

- Deploy an MDM/EMM solution, including containerization.
- Regularly train and communicate to employees on security threats.
- Control public Wi-Fi usage and implement data loss prevention (DLP) systems.

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

> **48%** of companies sacrificed mobile security for expediency. They were twice as likely to suffer data loss or downtime.
>
> - Verizon Mobile Security Index 2019

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 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 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 CEO, 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.

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

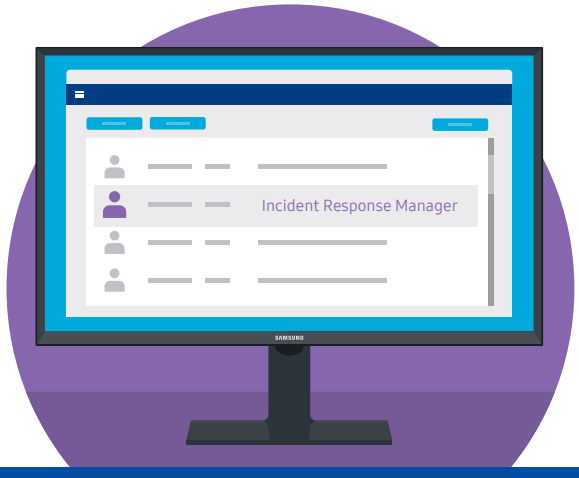
- Were any alerts generated?
- What details are provided within the alerts?
- What additional data can be gleaned by drilling down on alerts?
- Are there pertinent data points just prior to the incident or immediately following the incident?
- Is there a mechanism for holistically cross-referencing alerts 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. Nondisclosure 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's 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 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 — but incident response doesn't end there.

Breaches may begin via mobile device, for instance, but cybercriminals that access them can continue their attacks by changing credentials or logins to systems and servers. After locking or remotely wiping a device, further investigation should determine if attackers have escalated their privileges or found a way to maintain persistence on the network.

At the same time, the incident response plan should include steps to restore the security of mobile devices. This may include patching or updating policies, as well as further employee training.

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. Unfortunately, users frequently don't know or understand that their specific actions created a window of opportunity for a hacker.

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 Be Addressed

- Identify what systems or data could have been accessed by the device.
- 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...?

Successfully addressing a data breach, or even a minor security issue, is always an opportunity to review and improve your incident response plan.

During the course of responding to an unplanned event, for example, the team may have discovered a number of vulnerabilities that easily could make matters worse the next time.

No enterprise is immune to security incidents; many aren't even aware of them. According to the Verizon Mobile Security Index 2019, 56 percent of security breaches took months or longer to discover.

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. With technology changes and never-ending security threats, these activities should be updated several times throughout the year.

Consider the following key questions in relation to your planning and testing protocols:

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, semiannually 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?

Tomorrow: Ensuring Painful Lessons Aren't Repeated

Now that you've learned how to identify and address mobile security threats at the access, device and user levels, it's time to delve into how to prevent such incidents from occurring.

A data breach or other issue may demonstrate that new processes or additional layers of authentication are required to deliver the level of protection the enterprise needs. This could include the use of biometrics, for example, or a PIN in addition to a password. Beyond deploying EMM technology, make sure to create or revise comprehensive policies that complement it.

Whether through an audit for potential vulnerabilities and threats or through post-incident analysis, help employees avoid risk through app blocklisting or web filtering. Proactively protect against the threat of physical disconnection by ensuring device location and remote wipe capabilities are in place. Given that most employees will likely want to use their devices for both professional and personal use, apply containerization to safeguard corporate data and apps, or implement policies requiring additional authentication to access business apps.

This may entail reviewing the device management tools that you have in place. While MDM offers a rich set of features to address security incidents, EMM provides a more holistic approach that includes managing apps and content while providing sophisticated insights about trends and patterns. That means you'll be able to complement the policies you develop with alerts based on unusual behavior or usage patterns in order to get ahead of an incident.

Next, while many organizations have some kind of antivirus tools in place already, determine whether further investment is needed to protect mobile endpoints through additional threat detection or intrusion prevention applications.

The 2019 Verizon Mobile Threat Index showed that employee errors caused 21 percent of security incidents, and 15 percent involved misuse by authorized users. The best incident response planning should ensure ongoing employee training programs provide the most up-to-date information on best practices and potential pitfalls.

It may be impossible to eliminate the risk of IT security incidents completely, but you can ensure worst-case scenarios don't happen, particularly those involving mobile devices. This is where the use of a containerization solution can prove highly effective, separating business apps and data from personal information that might be on a smartphone.

How Samsung Knox Can Protect Your Business

Samsung Knox is a multilayered security platform baked into the hardware of the latest Samsung mobile 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 quickly detects any tampering attempts and locks down at-risk devices.

Additional Samsung Knox services enable enterprises to address mobile device management and security in a holistic way, from initial device registration to configuration, data separation and managing updates. Here's a quick rundown of how Knox can improve your security posture:

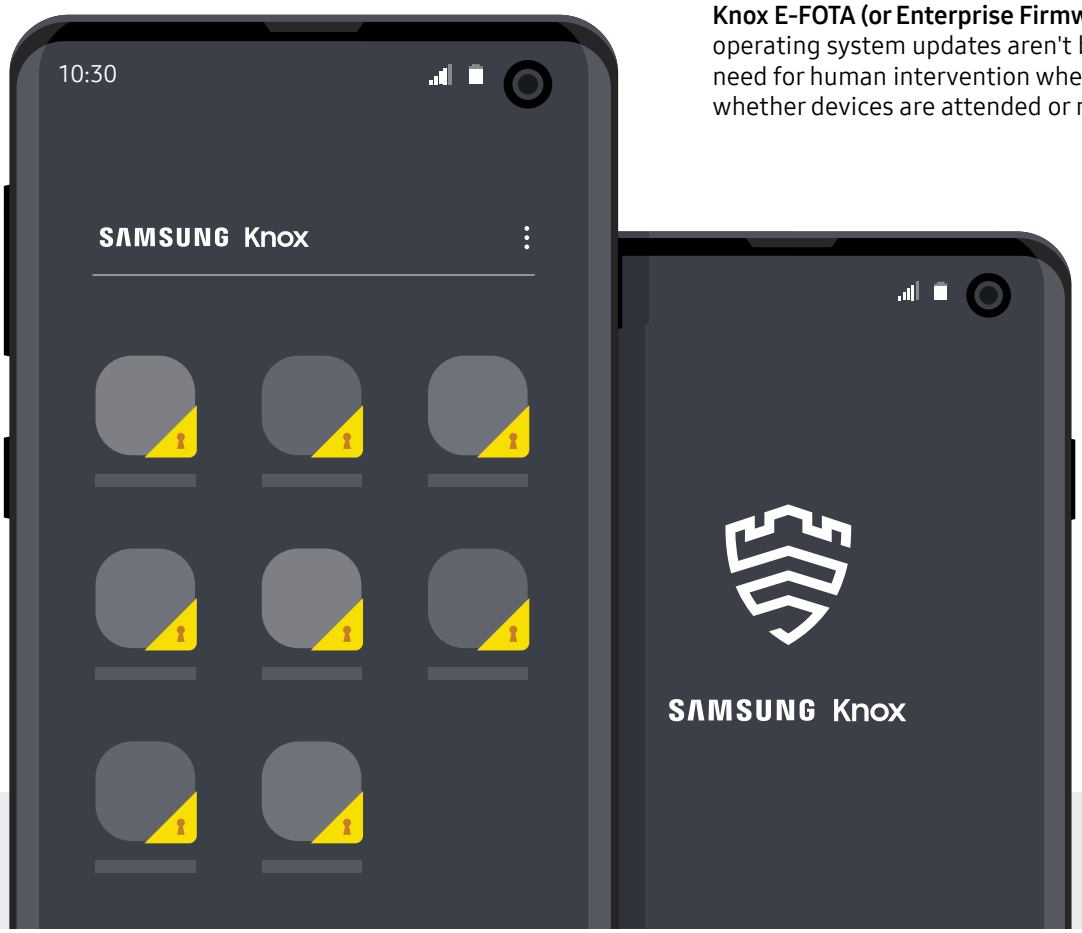
Knox Mobile Enrollment: Automatically enroll thousands of devices simultaneously, so users only need to unbox their phone and turn it on.

Knox Platform for Enterprise: Based on encryption/decryption keys derived from the device chipset, this is an on-device container that provides defense-grade security and policy management for organizations that need capabilities beyond the standard features offered in Android.

Knox Configure: Simplify the out-of-the-box experience for mobile devices and ensure you take a "security-first" approach when customizing for specific business use cases.

Knox Manage: Apply robust MDM policies with a cloud-based command center that works best with Samsung devices but can also be used for other Android and non-Android devices.

Knox E-FOTA (or Enterprise Firmware Over-the-Air): Ensure operating system updates aren't blocked and eliminate the need for human intervention when updates are required, whether devices are attended or not.



Conclusion

Having an up-to-date Incident Response playbook is an essential aspect of an enterprise information security plan. As cyberattacks become increasingly sophisticated, too many businesses are finding themselves playing catch up, attempting to deal with data breaches and downtime without a response plan.

In today's security environment, IT professionals must expect the unexpected, and develop policies and a strategy so they can proactively respond to any circumstances.

In addition to improving readiness, developing an Incident Response playbook is an opportunity to reevaluate mobile security practices and capabilities. While no endpoint security protocol can entirely eliminate risk, by leveraging the right tools and putting in place the right policies, enterprises can reduce their exposure and limit damage to the business when a breach occurs.

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

Footnotes

1. https://enterprise.verizon.com/resources/reports/mobile-security-index/
2. https://healthitsecurity.com/news/42000-adventhealth-patients-impacted-in-yearlong-data-breach