Lookout®

The Business Case for

Mobile Security

Table of Contents

In this eBook, you'll learn how to gain support for implementing a mobile security solution with your internal stakeholders.

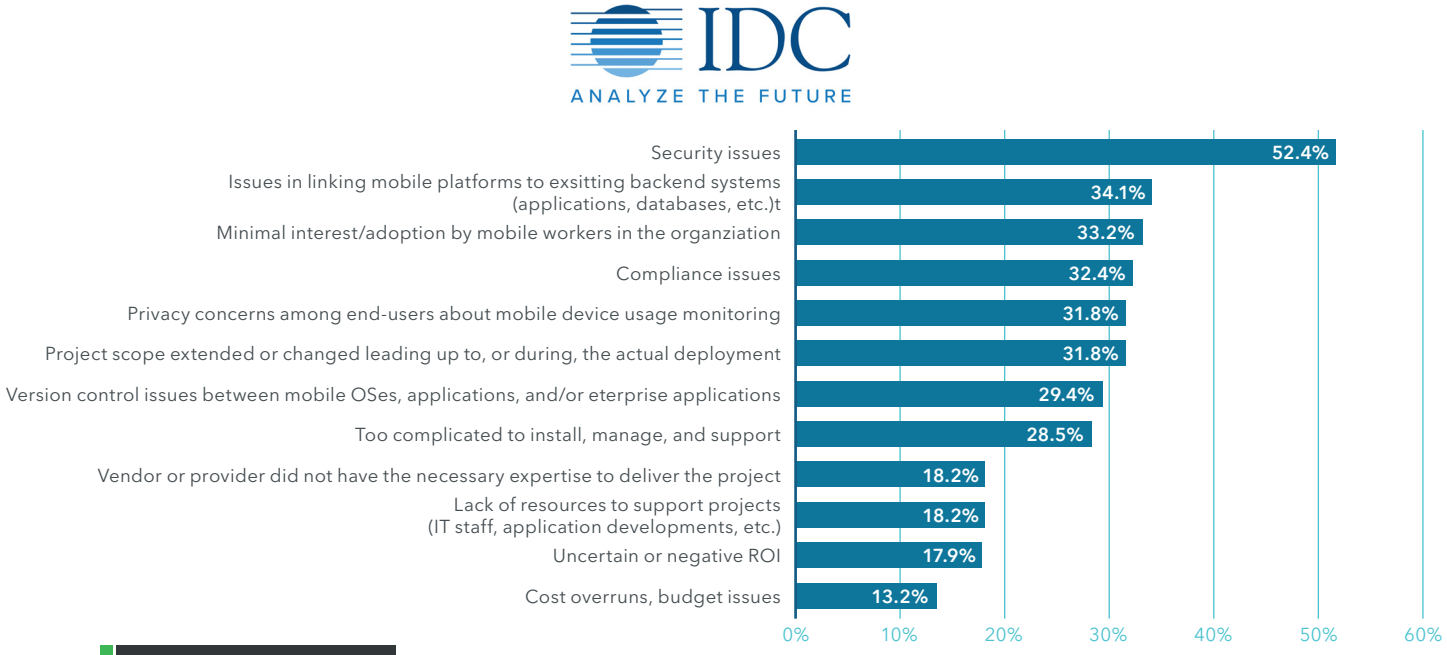
Introduction

Security issues are the biggest challenge for organizations deploying mobile technology in the enterprise according to your peers in the latest IDC Enterprise Mobility Decision Maker Survey[1].

This means it's no surprise that you've identified a gap in your security strategy - everyone's mobile device. Now you need to communicate the need to protect all the endpoints connecting to your corporate cloud data.

In this report you'll get access to tools that will help you make the case for mobile security in your organization, and fill the mobile gap in your security strategy.

Which of the following issues or challenges has your organization experienced when deploying mobile technologies?[1]



THE EXPERTS

In this report you'll hear from two experts on mobile app risks and justifying the cost of mobile security.

Craig Shumard, CISO emeritus

As Cigna Corporation's former Chief Information Security Officer, Craig developed and oversaw the implementation of a 21st century, corporate-wide strategy to safeguard information involving more than 65 million Cigna customers. He is currently a trusted advisor on a number of boards for prominent security companies.

Serge Beaulieu, Former Director of IT Security

Serge is a seasoned information security consultant whose experience includes being Director of Technical Security Strategy at Cigna Corporation. Serge is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

[1] IDC, 2020 Enterprise Mobility Decision Maker Survey: Security Highlights, Doc # US46766420, August 2020

1. The foundation of your business case: Reducing mobile risks

To successfully make a business case for mobile security, focus your attention on how it will measurably reduce the risks facing your organization from mobile devices.

A few of the risks could include:

- Damaged brand reputation
- Revenue loss[2]
- Fines
- Low emplyee morale
- Potential job loss

Breaches reach beyond technology damage, and wind up impacting serious business metrics.

A compelling business case for mobile security requires clearly communicating that protecting against mobile threats enables you to reduce business risks.

Your requirements for mobile security need to be tailored for specific security, technology, and business leaders:

For security leaders risk usually means: malware, device vulnerabilities, app vulnerabilities, data leakage, non-compliant apps, network attacks, and social engineering attacks.

For IT leaders risk usually means: data leakage, "non-compliant"[3] apps, and driving user adoption of a new security solution.

For mobility leaders risk usually means: a roadblock that prevents them from enabling workers to be more productive.

The reason that every company has some element of mobile risk is that mobile devices – the computers that live in our pockets – have become critical enterprise productivity tools.

Employees start responding to emails on the commute to work. They quickly pull up documents in an offsite meeting. They take pictures of a strategy they just "white-boarded" and send it to themselves. They submit expenses, update customer information, respond to support queries, review presentations, finalize budgets, and some even make phone calls. Your employees use these same devices to communicate via SMS, Slack, WhatsApp and other social media apps.

All of this mobile data introduces potential risk, which is exactly what mobile security solutions are created to mitigate.

DID YOU KNOW? There are hundreds of millions of downloads of Word, Excel, and PowerPoint as individual apps on Android and iOS.[4]

[2] What is the cost of a data breach?" CSO, August 2020
https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

[3] Non-compliant apps: a wide array of apps that exhibit behavior which may be benign in the right context, but may violate your organization's security posture (e.g. an app that sends contact data to foreign servers).

[4] https://venturebeat.com/2020/02/19/microsoft-office-mobile-app-replaces-word-excel-powerpoint/

2. Enterprise mobile threat vectors today

Many organizations have zero visibility into the mobile risks they face. Depending on your security posture, that lack of visibility may be enough to bring on a mobile security solution.

For the majority of organizations, you'll want to start by educating your broader team on what enterprise mobile threat vectors look like today.

Helping your leadership team understand the most significant mobile risks is the first step towards making a business case for a mobile security solution. The risk to your organization's sensitive data from mobile devices, however, may not look like what you expect.

Here's a bird's eye view of what you can find on a device.

Your organization's data is mobile

2.1. Requirements for mobile security

As more mobile devices access corporate data, they increasingly become targets for attackers. Mobile security identifies mobile threats across all attack vectors:

Mobile Phishing

THREAT: Phishing is the most common way attackers lure users to malicious websites to deliver drive-by downloads or inject code onto a device.

SOLUTION: Mobile security alerts users to phishing attempts not only from browser and email apps, but also SMS, messaging,social media and other apps on a mobile device in real-time.

App-based Threats

THREAT: Malicious and non-compliant apps leak sensitive personal and organizational data.

SOLUTION: Mobile security protects against viruses, spyware, malware, and trojans via real-time threat detection and on-device remediation.

Network Threats

THREAT: Unsafe network connections create opportunity for traffic interception and decryption of sensitive data.

SOLUTION: Mobile security analyzes network connections from a global sensor network, and effectively mitigate false positives while detecting high impact threats.

Device Vulnerabilities

THREAT: Missing OS security patches create security vulnerabilities.

SOLUTION: Mobile security creates a fingerprint of each mobile device and compares it against fingerprints of millions devices to identify anomalies and risks.

3. Mobile Risk Assessment

It's natural to want to understand your mobile risk exposure before investing in a security solution. You may have data on your managed devices in the mobile device management, but likely can't use this data to determine if the mobile devices with access to corporate data are at risk or not.

One of the ways you can advance the conversation about the specific mobile risks facing your company is to request a Mobile Risk Assessment (MRA) from Lookout.

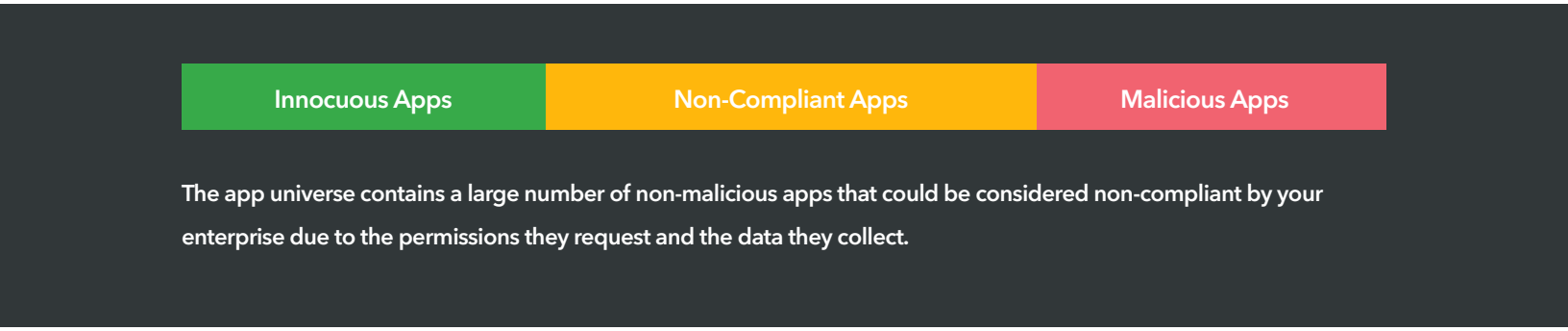
The MRA pulls data from the Lookout global sensor network of nearly 200 million mobile devices in order to determine what mobile threats may already exist on a company's network.

The MRA will evaluate threats that it finds based on three criteria:

- The prevalence of the threat, or how widespread it is.
- The severity of the threat, or how much damage it could.
- The complexity of the threat, or how sophisticated its technology is.

3.1. Preventing data leakage: non-compliant versus malicious apps

Once you've established a baseline of potential malicious threats facing your organization, the next step is to make a case for mitigating potential threats from apps that are not intended to do harm, but still are a potential risk for data leakage because of the types of data they collect.



The app universe contains a large number of non-malicious apps that could be considered non-compliant by your enterprise due to the permissions they request and the data they collect.

Innocuous apps are safe for your employees to use, and don't pose a risk to your employee or organizational data. Because these apps pose no risk, they can be added to your organization's AllowList of approved apps.

Malicious apps set out to harm a device or the data on the device. They often steal personal or organizational data, commit fraud, negatively impact device performance, and more. These apps are defined by their malevolent aim or malicious intent, and should be included in your organizations DenyList of apps.

Let's take a deeper look at non-compliant apps.

Non-compliant apps aren't classified according to a binary "good" or "bad," but an enterprise may deem apps to be non-compliant based on their specific security posture and regulatory requirements.

For example, apps that collect location data may pose great risk to an enterprise or government organization deploying employees to sensitive locations. A doctor working for a healthcare organization might store patient contact information in her phone's contacts and will want to restrict apps that access contact information in order to maintain HIPAA compliance.

Which apps your enterprise deems non-compliant is highly dependent on your industry and the kinds of data your mobile devices – both managed and unmanaged – have access to.

A big part of the business case for mobile security is that it allows IT and security teams to establish security policies to prevent data leakage to which end-user devices must adhere.

These teams also no longer have to maintain manual black/whitelists, as the solution will detect apps that fall into the non-compliant as well as malicious ranges and automatically convict them as they appear on employees' devices.

The ability to replace manual blacklisted and whitelisted apps will enable enterprise IT and security teams to work more efficiently, a benefit that tends to pique the interest of decision-makers on both sides of the aisle.

4. Enabling mobile productivity

Many enterprises now have projects underway to improve productivity and respond to employee requests for using mobile devices at work through a bring-your-own-device (BYOD), corporate-owned-personally-enabled (COPE), or another mobility program.

One of the major challenges facing these programs is that all employees are also consumers, and their approach to mobile technology is, "If I like it, I'll use it. If I don't, I won't." If they don't trust the security technology or they feel that it inhibits their usage of the device, they will try to work around the technology or they won't use it altogether.

Whether a device is owned by your organization or your employee, mobile devices are inherently more personal devices, so users are more reluctant to accept monitoring or security that impacts their device. That is why it's important to evaluate the user experience of the endpoint app of any solution you're considering.

A mobile security app should build trust between IT and employees. Communicate to your company's mobility team that this solution is intended to protect employees' devices and data just as much as it is intended to protect enterprise data. The bottom line they want to hear is that end-users are free to go about their business, using apps that make them more productive.

This is the beauty of mobile devices: everyone has incentives to protect them. Many people's work phone or tablet is also their home phone or tablet. A mobile security product will protect any data, regardless of whether it's enterprise or personal, incentivizing the employee to use it.

5. Selling mobile security internally

You may already recognize the need for a mobile security solution in your organization, but tailoring your case to other key stakeholders is a critical part of getting sign-off on a mobile security initiative.

Key stakeholders:

- CISO
- CIO
- CEO
- Other line of business stakeholders
- CFO
- Head of HR
- Head of Sales

Understand how to speak to each of these stakeholders and the value they can expect from making secure mobile devices a reality in your organization.

6. Making the case to your CISO

CISOs care about the overall health and risk posture of an organization and have likely invested a significant amount of money keeping the business – and its data – safe. They often think in terms of managing risk that has a high degree of uncertainty, where traditional risk management calculations don't work. CISOs rarely have accurate estimates for the chances of security-related events happening or the damage caused by these events. However, before allocating budget to a mobile security solution your CISO may want to create a mobile threat model to quantify the risk to your business.

Key considerations:

- Mobile phishing is a massive problem on a small screen. Learn about mobile phishing encounter rates in your country.
- The impact and likelihood of mobile threat is growing as organizations rely on mobility.
- The risk of business data leaking is increasingly likely as more employees access corporate resources from their personal mobile devices and/or to use their company-provided mobile devices for both personal and business use.
- Your organization does not have visibility into all the devices your employees use, the latest cybersecurity threats to those devices, and the vulnerabilities within mobile operating systems and apps.

Focus areas for your CISO:

A mobile security solution:

- Would enable the organization to securely allow mobile devices access to the corporate network, promoting enhanced workforce productivity.
- Aligns with any potential BYOD goals and objectives.
- Provides proactive incident response capabilities if a malware outbreak were to occur.
- Would ensure a consistent level of security defenses across all types of endpoints.
- Would maintain and strengthen regulatory and audit compliance posture.
- Would provide a necessary security infrastructure to defend against the growing mobile threat landscape.

7. Making the case to your CIO

From her perspective, mobile devices are a potential source of headaches and she'll want to ensure they are protected. CIOs care about making sure the company keeps humming along from a digital perspective – downtime is unacceptable.

Key considerations:

- Adopt technology that enables productivity gains – an overall win for any business
- Technologies should be easily implemented and managed
- Ensure IT systems adhere to applicable laws and regulations
- Ensure the protection of all proprietary organization data and information systems
- Establish and uphold written policies and procedures regarding all computer operations
- An attack could have major impact on the organization, such as a leaked email server or lengthy downtime, which could result in job loss.

Focus areas for your CIO:

- Proposal should outline a clear business case and value add for technology investments.
- Mobile security works equally well with or without UEM, but managing mobile devices is not securing mobile devices and creates gaps in endpoint security.
- Highlight ability to deliver secure BYOD, particularly for devices connecting to corporate cloud data.
- Provide clear implementation plans.
- Proposed vendor should have deep understanding in security compliance and risk management.

THE EXPERT

"Total cost of ownership, especially with security products, has to be viewed in the context of risk mitigation and business enablement. People always want to see a cost justification, but it really has to be looked at terms of your brand reputation, how well you deliver secure services to your employees, other stakeholders, and your consumers."

Serge Beaulieu
FORMER DIRECTOR OF IT SECURITY

- Proposed vendor should also have a proven track record of successfully enabling end-user adoption and usage, resulting in lower helpdesk tickets.
- A vendor with a track record of success, in similar lines of business, with similarly-sized clients.
- Thought leadership and guidance on data management, governance, security, architecture.
- 24/7 global support capabilities.

8. Making the case to your CEO

CEOs will look at any proposal from a business growth perspective. This includes ensuring customer and employee data is safe to build and retain brand trust. Focus on showing the business advantages to protecting your organization's mobile devices.

Key considerations:

- Protecting brand reputation from a mobile breach that makes headlines.
- Knowing that mobile device usage is continuously increasing, a CEO will want to ensure that critical infrastructure is protected.
- CEOs accept that the risk of a breach needs to be managed, but will want to confirm that the company has a prepared strategy to get back up and running quickly following an attack.
- CEOs may also have to deliver on client expectations that they are protecting mobile devices used by employees connecting to a client's corporate network.
- Overall operational efficiency, which ties closely to productivity, is one of the CEO's main concerns

Focus areas for your CEO:

- Be able to show the board of directors that there is a plan in place to protect critical infrastructure and remediate mobile threats.
- Mobile security includes protecting employee mobile devices, but also securing your company's own apps from a breach that damages the brand reputation, especially if customer information is involved. In regulated industries, litigation can be brought by affected customers.[5]
- Establish a relationship with a mobile security vendor that can help the company to move quickly in response to an attack to minimize damage.
- Mobile security will give necessary visibility to attacks actively happening on employees' mobile devices.
- Mobile security can help employees around the world to safely and frictionlessly, connect to the corporate network.

[5] Equifax Data Breach Settlement Totals Up To $700 Million : NPR

9. Making the case to your CFO

Your CFO naturally wants to ensure that they are getting the biggest bang for their buck in every aspect of the business. Financial loss, however, can come in a number of forms, one of which being diminished brand reputation or client loss from a data breach.

Similar to the CIO's concerns, it can also costs a significant amount to triage a breach – the Ponemon Institute quotes the total potential cost of a data breach via a mobile device at $26 million. This figure takes into account a number of factors including "direct costs," such as device replacement, threat investigation, forensics, and diminished employee productivity; as well as "indirect costs" such as costs of non-compliance and diminished reputation.

Key considerations:

- Cash flow, income statements, and balance sheets can all be affected by a public, or even a "small," private breach that results in data loss.
- A mobile breach may cause the loss of important information or systems, and needs to be cleaned up.
- Productivity loss is felt in the sales and marketing operations around a breach, assuaging customer fears, and maintaining client relations.
- The CFO understands where all the data in your organization may live, including Human Resources apps like Oracle or Workday; procurement apps like Coupa; financial apps like Netsuite; and customer data like Salesforce. Help your CFO to see how a mobile security solution protects this data, and reduces the risk of breach through a cloud application.

Focus areas for your CFO:

- Modern mobile security should be a cloud product that does not require a capital expense that needs to be depreciated.
- The endpoint apps that protect individual mobile devices can be deployed quickly to employees globally, delivering value in a short amount of time compared to other IT projects.
- Mobile security is a productivity enabler for every line of business.
- CFOs will push CIOs and CISOs to look for a solution that addresses threat detection, compliance management, and vulnerability management in order to minimize vendors and get maximum value.
- Confidential data, including financial data, that lives outside company walls is significantly safer when the employees who access that data have a mobile security app on their smartphone and/or tablet.

10. Making the case to other executives

THE CMO: Chief Marketing Officers may be even more sensitive than a CEO to a damaged brand reputation, as it will lead to a suboptimal environment for customer engagement. Marketing leaders want to drive positive customer experiences. Mobile security helps protect the experiences that lead to positive brand sentiment.

HEAD OF HR: Organizations are under pressure to have robust support for mobile devices in order to recruit new employees. The Head of HR will also need to communicate the benefits of a mobile security product to existing employees. This is a great opportunity to use mobile security as an added employee benefit: employees get top-of-line protection for the corporate information they access, and their personal information.

HEAD OF SALES: Sales representatives are often traveling, pulling up customer information on the go, looking at sensitive documents, connecting to whatever Wi-Fi they can to access the information they need to clinch the deal. The Head of Sales will want to make sure that customer and prospect data is secure, while not stifling the salesperson's ability to access what they need whenever they need it.

Focusing on the messaging that each stakeholder cares about will expedite your procurement cycle — and enable you to deliver the measurable reduction in mobile risk that everyone needs.

Conclusion

Today more than half of the devices employees use to access your organization's data run iOS, Android and Chrome OS. Organizations that don't have visibility into these endpoints run the risk of company brand damage, revenue loss, regulatory fines, and potential job losses.

Use the tools in this guide to make the case for adding modern endpoint security to provide the visibility and controls needed fill gaps in your overall security strategy.

Now, become a true expert. Using Read More callout "Learn more about a platform that makes your organization unstoppable" – by stopping phishing attacks, ransomware and data breaches.

Lookout®

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo