BYOD & MOBILE SECURITY

2016 SPOTLIGHT REPORT

LinkedIn Group Partner

Information Security

Presented by

bitglass | blancco technology group | Check Point SOFTWARE TECHNOLOGIES LTD | Skycure Mobile Threat Defense | SnoopWall | tenable network security

BYOD & MOBILE SECURITY
SPOTLIGHT REPORT

TABLE OF CONTENTS

INTRODUCTION

Security and privacy risks are on the rise with the proliferation of mobile devices and their increasing use in the enterprise.

You're likely familiar with the statistics of our increasingly mobile world: 12.1 billion mobile devices will be in use by 2018; half of the globe's employers require BYOD by 2017; 67 percent of CIOs and IT professionals are convinced that mobility will impact their organizations as much, or more, than the Internet did in the 1990s. As mobility and BYOD grow in the workplace, so do challenges from managing bandwidth and device access to handling the most pressing concerns of security. The 2016 BYOD and Mobile Security Report focuses on these security challenges and offers fresh insights on the state of mobile threats and solutions.

We collected more than 800 survey responses from cybersecurity professionals who are part of the Information Security Community on LinkedIn and distilled the findings into this information-rich study. Inside find valuable data points, benchmarks and insights regarding the latest challenges of securing mobility, the technology choices organizations are making and the responses to the growing security risks associated with enterprise mobility.

I would like to thank all survey participants for sharing their insights. Also, many thanks to our co-sponsors for supporting this exciting project!

Thank you,

Holger Schulze

Holger Schulze
Group Founder
Information Security
Community on LinkedIn

hhschulze@gmail.com

LinkedIn Group Partner
Information Security

KEY FINDINGS

Key Trends Influencing Enterprise BYOD & Mobile Security

1. Increased employee mobility (63 percent), satisfaction (56 percent) and productivity (55 percent) dominate as the top drivers of BYOD. Interestingly, these employee related drivers are considered more important than reduced costs (47 percent).

2. Security (39 percent) and employee privacy (12 percent) are the biggest inhibitors of BYOD adoption. In contrast, management opposition (3 percent) and user experience concerns (4 percent) rank far lower.

3. One in five organizations suffered a mobile security breach, primarily driven by malware and malicious WiFi.

4. Security threats to BYOD impose heavy burdens on organizations' IT resources (35 percent) and help desk workloads (27 percent).

5. Despite increasing mobile security threats, data breaches and new regulations, only 30 percent of organizations are increasing security budgets for BYOD in the next 12 months. Meanwhile, 37 percent have no plans to change their security budgets.

BYOD ADOPTION

BYOD DRIVERS & BENEFITS

With over 4 billion mobile subscribers, we live in a world where mobility is ubiquitous and enterprises have begun to benefit from it. This is supported by the findings of our survey, which found that the top three drivers of BYOD among employees are improved mobility (61 percent), greater satisfaction (56 percent) and increased productivity (55 percent).

Interestingly, these employee-related benefits are considered more important than reduced costs (47 percent).

Q: What are the main drivers and benefits of BYOD for your company?

Responses do not add up to 100% because survey participants selected multiple choices.

ADOPTION OF BYOD

When we asked survey respondents what stage of BYOD adoption had been reached in their companies, the results were a bit surprising. Although 40 percent of organizations make BYOD available to all employees, not all organizations are on board. In fact, 13 percent have no plans to support BYOD, 3 percent gave it a try but abandoned it and 9 percent don't currently offer it (but plan to start in the next 12 months). From these findings, it seems as though at least one quarter of respondents are somewhat cautious and hesitant as to the overall benefits of BYOD and need to be reassured in some way, for example through implementation of security technologies and education for employees that outlines the varying types of security threats on mobile devices, scenarios to avoid and BYOD best practices.

Q: What stage of BYOD adoption has been reached by your company?

40%

BYOD is available to all employees

32%

BYOD is available to select employees

13%

We have no plans to support BYOD

9%

We do not support BYOD, but plan to start in the next 12 months

3%

BYOD was tried but abandoned

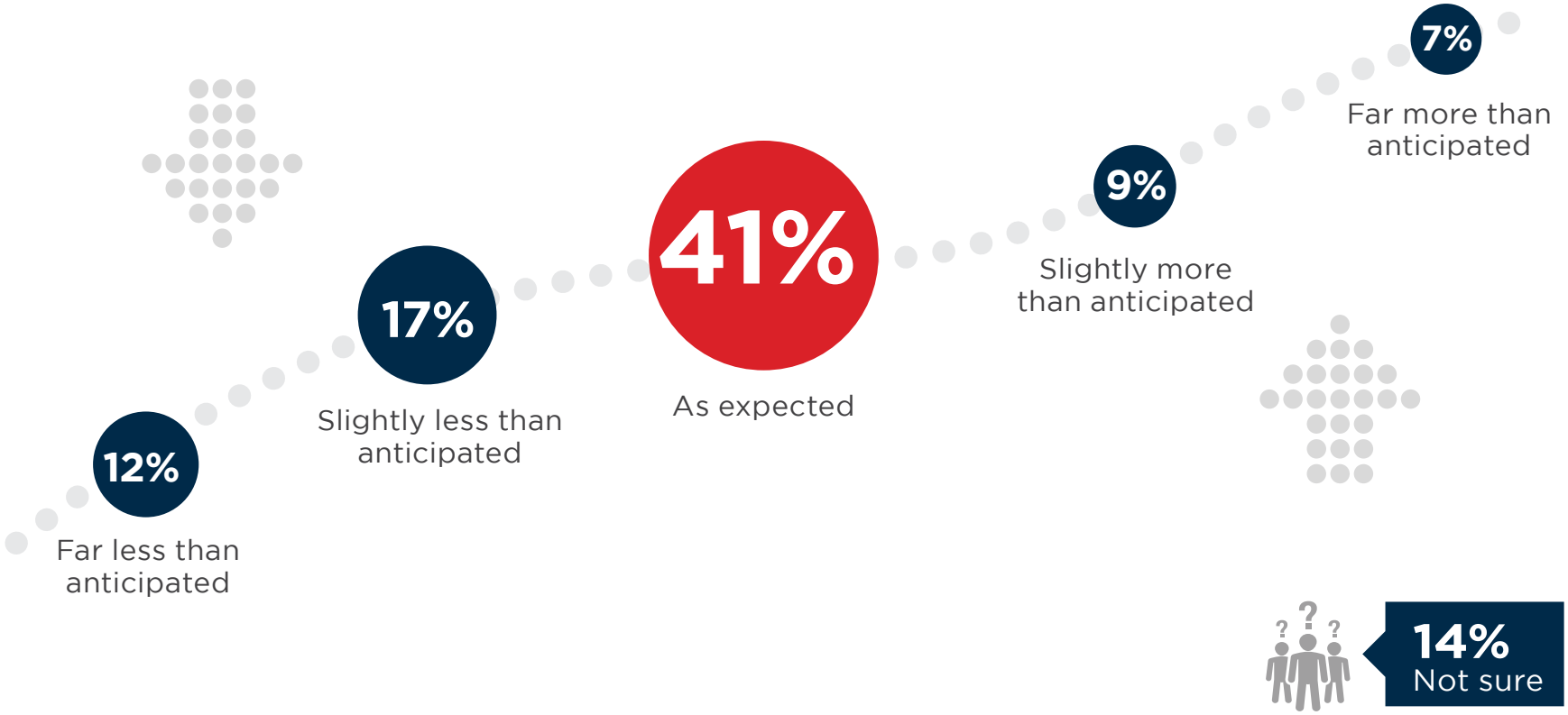
3%

Other

BYOD PROGRESS – REALITY VS. EXPECTATIONS

For 41 percent of organizations that are deploying BYOD, adoption by employees is progressing as expected. However, 29 percent saw adoption lag behind, compared to just 16 percent that experienced better than expected adoption.

Q: How has BYOD adoption progressed compared to your expectations?



BYOD BARRIERS

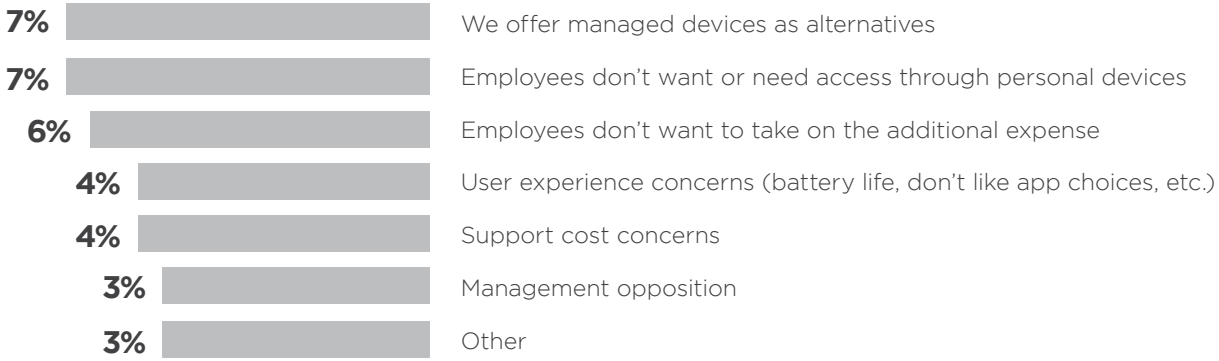
When we asked the survey respondents about the number one inhibitor to BYOD adoption in their companies, 39 percent cited security concerns. For the IT and security teams inside organizations, this points to potential security gaps or weaknesses that may need to be addressed. In contrast, management opposition (3 percent), employees' unwillingness to take on additional expenses (6 percent), and user experience concerns (4 percent) are not considered significant barriers to BYOD adoption.

Q: What do you believe is the number one inhibitor to BYOD adoption in your organization?

39%
Security Concerns

15%
We don't experience any resistance to BYOD adoption

12%
Employee privacy concerns (e.g., over EMM software)

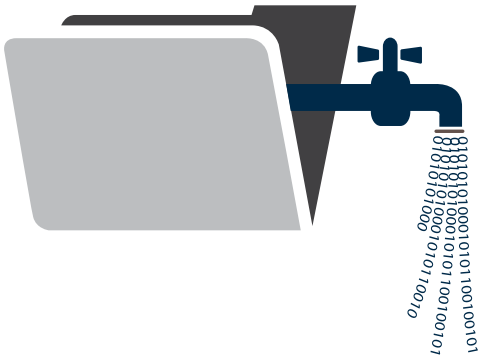


BYOD SECURITY CONCERNS

BYOD SECURITY CONCERNS

Data leakage/loss reigns supreme as the top BYOD security concern among respondents, at 72 percent. Meanwhile, 56 percent of respondents are worried about unauthorized access to company data and systems and 54 percent are concerned that users will download unsafe apps or content. Given the types of concerns expressed by the survey respondents, some organizations may not have the necessary resources, staff or budgets to properly monitor employee use of BYOD devices.

Q: What are your main security concerns related to BYOD?



72%
Data leakage / loss

56%
Unauthorized access to company data and systems

54%
Users download unsafe apps or content

52%
Malware

Lost or stolen devices 50% | Vulnerability exploits 49% | Inability to control endpoint security 48% | Ensuring security software is up-to-date 39% | Compliance with regulations 38% | Device management 37% | Network attacks via WiFi 35% | Other / None 4%

Responses do not add up to 100% because survey participants selected multiple choices.

KEY MOBILE SECURITY REQUIREMENTS

As our previous findings have indicated, BYOD in the workplace comes with several challenges and risks. According to the responses from our survey, protection capabilities (42 percent), integration with existing platforms (33 percent), and visibility into mobile threats (15 percent) are most critical for mobile security.

Q: What is your biggest pain point when it comes to mobile security?

42%

PROTECTION

We need a solution that not only detects threats but also remediates them based on the corporate policy

33%

INTEGRATION

We need a mobile security solution that integrates with our existing network (e.g., SIEM), endpoint (e.g., MDM or EMM), or ITSM (e.g., System Center) platforms

15%

VISIBILITY

We need to see all affected devices and the types of threats

10%

OTHER

NEGATIVE IMPACT OF MOBILE THREATS

As our study findings have shown, there is no shortage of mobile threats and the consequences can be serious and dangerous to business success. In fact, 35 percent of the surveyed respondents said mobile threats to their company have caused them to bring on additional IT resources to manage security incidents. 27 percent said security threats have increased the workload for their help desks.

It's also interesting to see that only 2 percent of respondents believe regulatory fines are a negative consequence of mobile threats. Given the tightening of oversight and enactment of new legislation such as the EU's General Data Protection Regulation, failure to comply with regulation could have significant consequences for organizations, including loss of customers, loss of sales, reduced customer loyalty and heavy legal and financial fines, just to name a few.

Q: What negative impact did mobile threats have on your company in the past 12 months?

35%

Additional IT resources needed to manage mobile security

Increased helpdesk workload

Malware infections and related cost

Data loss or leakage occurred

Unauthorized access to corporate data and systems 17% | None 17% | Disrupted business activities 12% | Reduced employee productivity 12% | Increased cost due to devices subscribed to premium pay services 7% | The company had to pay regulatory fines 2% | Other / None 26%

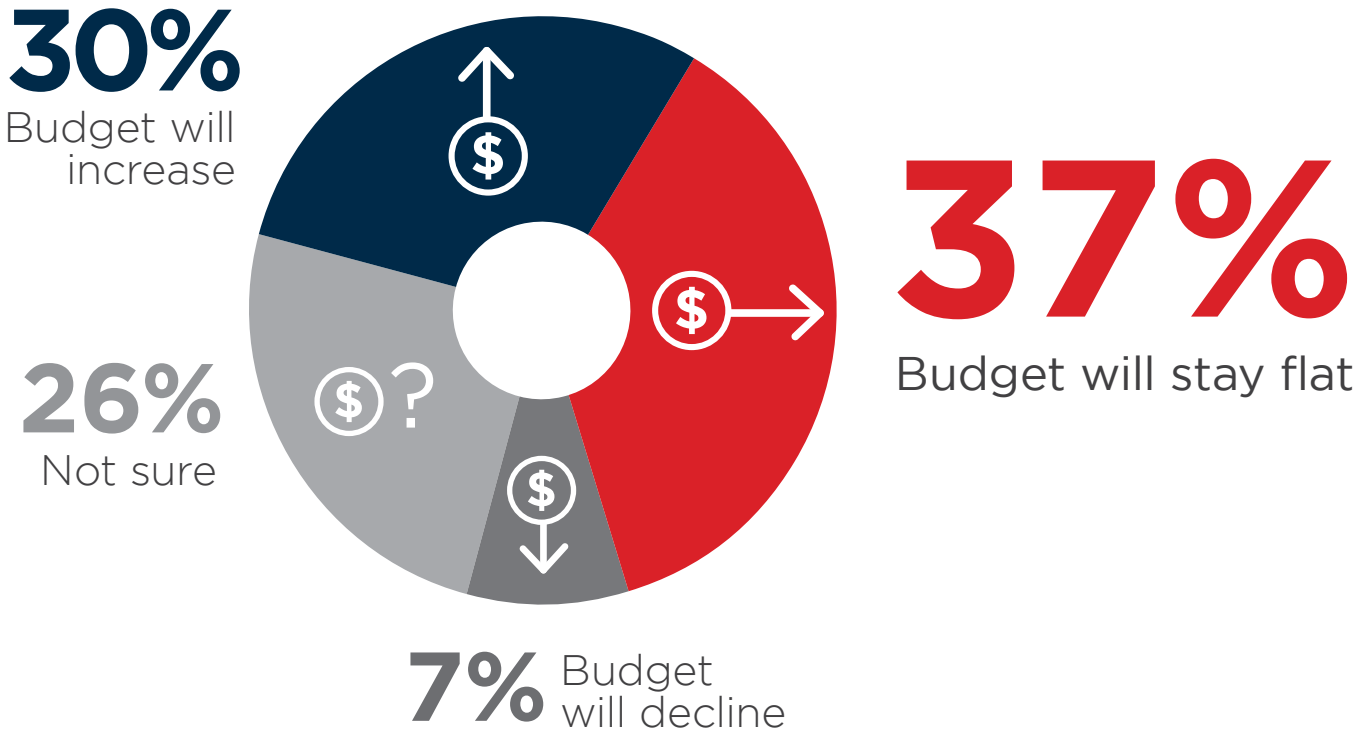
Responses do not add up to 100% because survey participants selected multiple choices.

MOBILE SECURITY BUDGET

2015 was a year of massive data breaches, including OPM, Ashley Madison, TalkTalk, VTech and many others. More often than not, when such data breaches occur, it creates the impetus for IT teams to request increased security budgets. Our survey responses support this pattern with 30 percent stating their mobile security budgets will increase over the next 12 months.

However, one of the more disconcerting findings of our survey is that 37 percent of budgets won't increase at all and 26 percent of respondents are not sure if their budgets will change. Security threats and data breaches will likely continue to increase. But without sufficient cybersecurity budgets, organizations will continue to struggle to detect, protect against and respond to such incidents in the future.

Q: How is your mobile security budget going to change over the next 12 months?

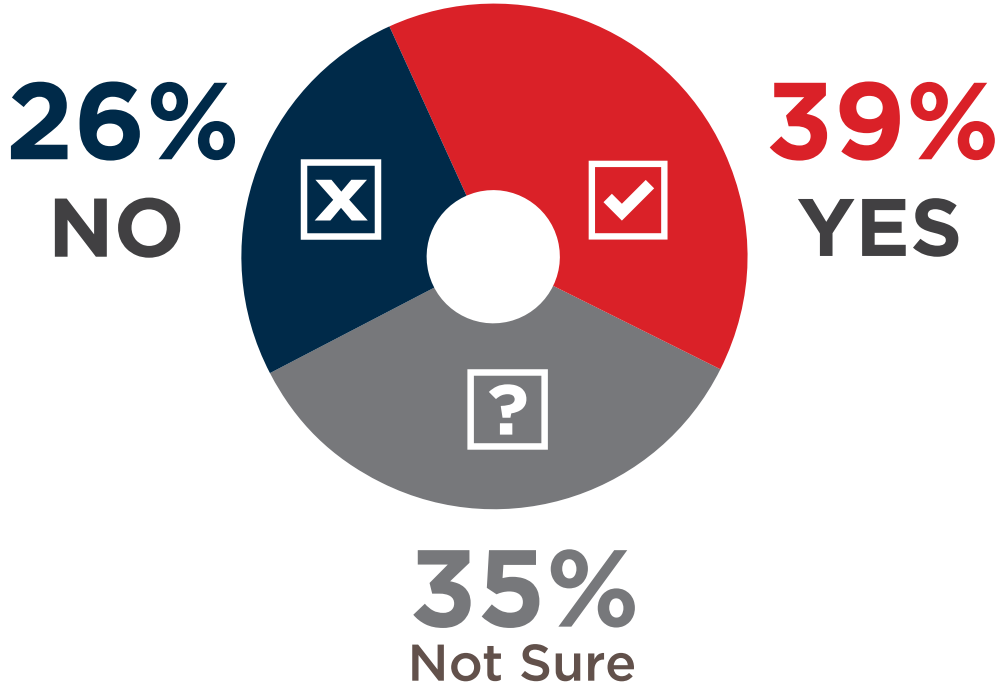


MOBILE SECURITY INCIDENTS

MALWARE THREAT

39 percent of the surveyed organizations reported that BYOD or corporate-owned devices have downloaded malware at some point in the past. More than one-third of the surveyed respondents said they are “not sure” if malware has been downloaded in the past. These findings indicate a lack of or ineffective monitoring of BYOD and corporate-owned devices in the workplace. It is imperative organizations implement BYOD programs in conjunction with the necessary programs to properly monitor device use, implement security technologies to detect and prevent malware penetration and train employees across all departments and levels to protect all data stored on or accessed through mobile devices.

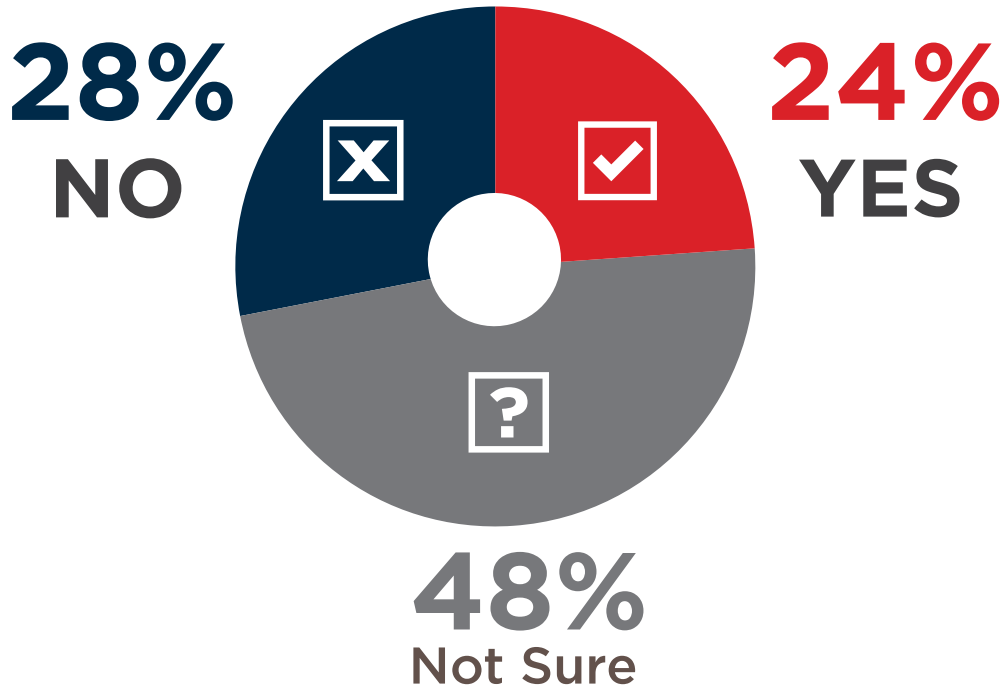
Q: Have any of your BYO or corporate-owned devices downloaded malware in the past?



MALICIOUS WIFI

According to Juniper Research, Wi-Fi networks will carry almost 60 percent of mobile data traffic by 2019, reaching over 115,000 PB (Petabytes). While this growth is impressive, it can open organizations to new vulnerabilities that arise when mobile devices connect to malicious Wi-Fi. As our study reveals, 24 percent of the surveyed organizations confirmed that the BYOD or corporate-owned devices used by employees have, in fact, connected to malicious Wi-Fi in the past. Worse yet, close to half (48 percent) are unsure if this has happened, leaving them even more vulnerable to the possible loss or theft of corporate data.

Q: Have any of your BYO or corporate-owned devices connected to a malicious WiFi in the past?

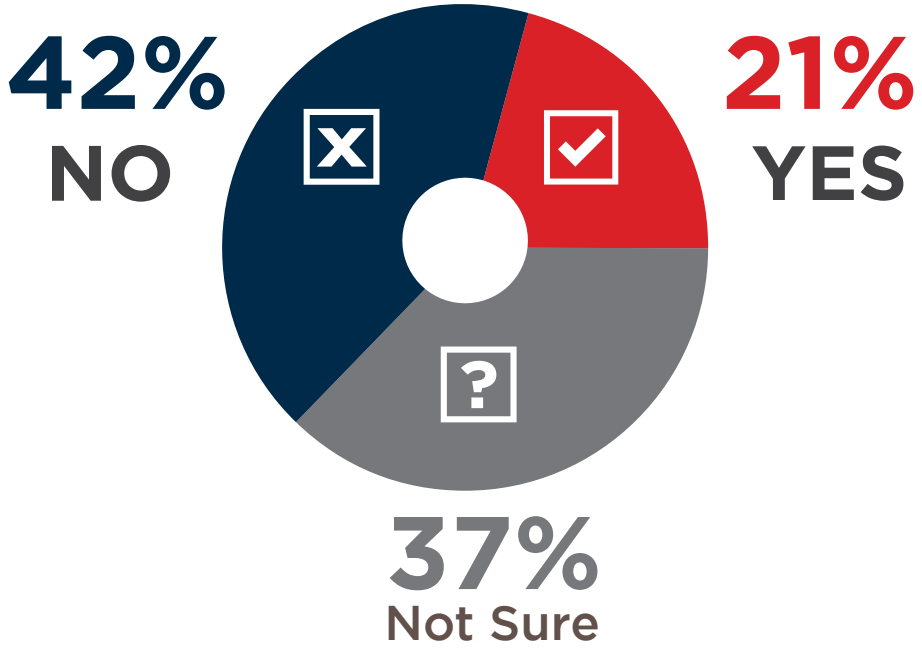


MOBILE SECURITY BREACHES

Nearly one out of five organizations (21 percent) experienced a security breach through the use of BYOD or corporate-owned mobile devices. The fact that 37 percent of the surveyed organizations could not definitively answer this question is problematic and puts organizations at risk of undetected data loss/theft — and the resulting legal, financial and reputational damages that may occur.

Many organizations struggle to protect data once employee devices "hit end of life" or are readied for reuse or resale. It's important for organizations to properly manage data across the entire mobile lifecycle if they want to avoid data leaks. This is especially true if and when employees lose their devices, or have them stolen. Certified mobile data erasure software and device encryption tools, for example, are effective ways to minimize the risks of mobile data loss or theft. Data loss prevention applied to sensitive files at download time can help organizations act on alerts in real-time, thus making it critical to limiting the size and impact of a breach. With contextual data loss prevention, organizations can encrypt, redact or wrap files with digital rights management based on the content of those files.

Q: Have mobile devices been involved in security breaches in your organization in the past?



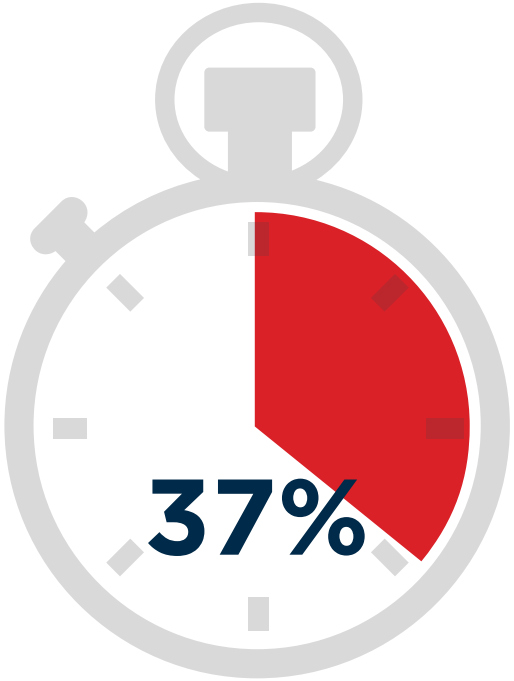
BREACH RECOVERY

RECOVERY FROM MOBILE SECURITY BREACHES

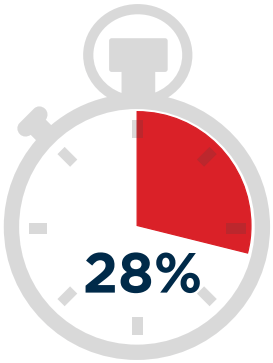
In looking at the various data breaches that have hit companies, it's clear that when and how an organization responds to a security breach is critical to mitigation, recovery and its long-term success. But as previous data breaches have shown, response and recovery times are often too slow. According to our survey findings, 42 percent of organizations reported taking anywhere from one week to more than a month to recover from an incident.

For organizations, this is an opportunity to create comprehensive data breach incidence detection, response and recovery plans and to train IT security teams on such plans. In doing so, organizations may see their recovery times shorten significantly.

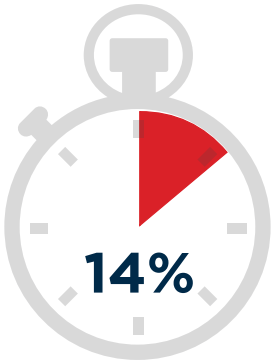
Q: How long did it take your organization to recover from the mobile security breach?



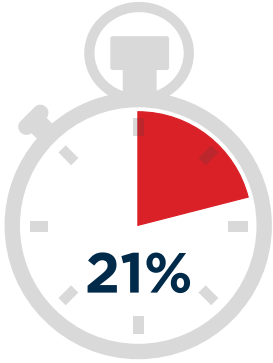
Less than 1 week



From 1 week to 1 month



More than a month



Not Sure

BYOD USERS & APPS

SUPPORTED USERS

In addition to employees (76 percent), some organizations make BYOD available to contractors (23 percent), partners (16 percent) and customers (14 percent). If BYOD is made available externally, organizations must heighten their security posture to protect sensitive company data and systems.

Q: What user group(s) does your organization enable BYOD for?

76%
Employees

Responses do not add up to 100% because survey participants selected multiple choices.

BYOD POLICY OWNERS

The IT department is responsible for BYOD policy in most organizations (69 percent), followed by the security team (55 percent) and compliance (24 percent).

Q: Who is responsible for setting BYOD policy in your organization?

12% Human Resources

6% Other

Responses do not add up to 100% because survey participants selected multiple choices.

PERMITTED MOBILE APPS

Email, calendar and contact management are still the most popular types of mobile apps enabled on bring your own devices (84 percent). The applications designed to boost productivity are the very same applications that can increase the risk of data breaches, intrusions or malware incidents. Finding the right balance between productivity and security will continue to be critical to the success of BYOD in the workplace.

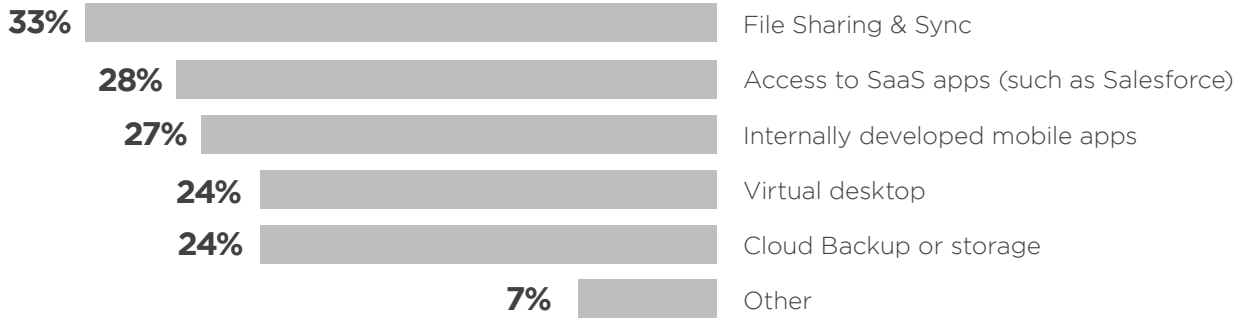
Q: Which of the following applications and use cases do you allow on Bring Your Own Devices?

84%
Email / Calendar / Contacts

45%
Document access/editing

43%
Access to Sharepoint/Intranet

35%
Video conferencing



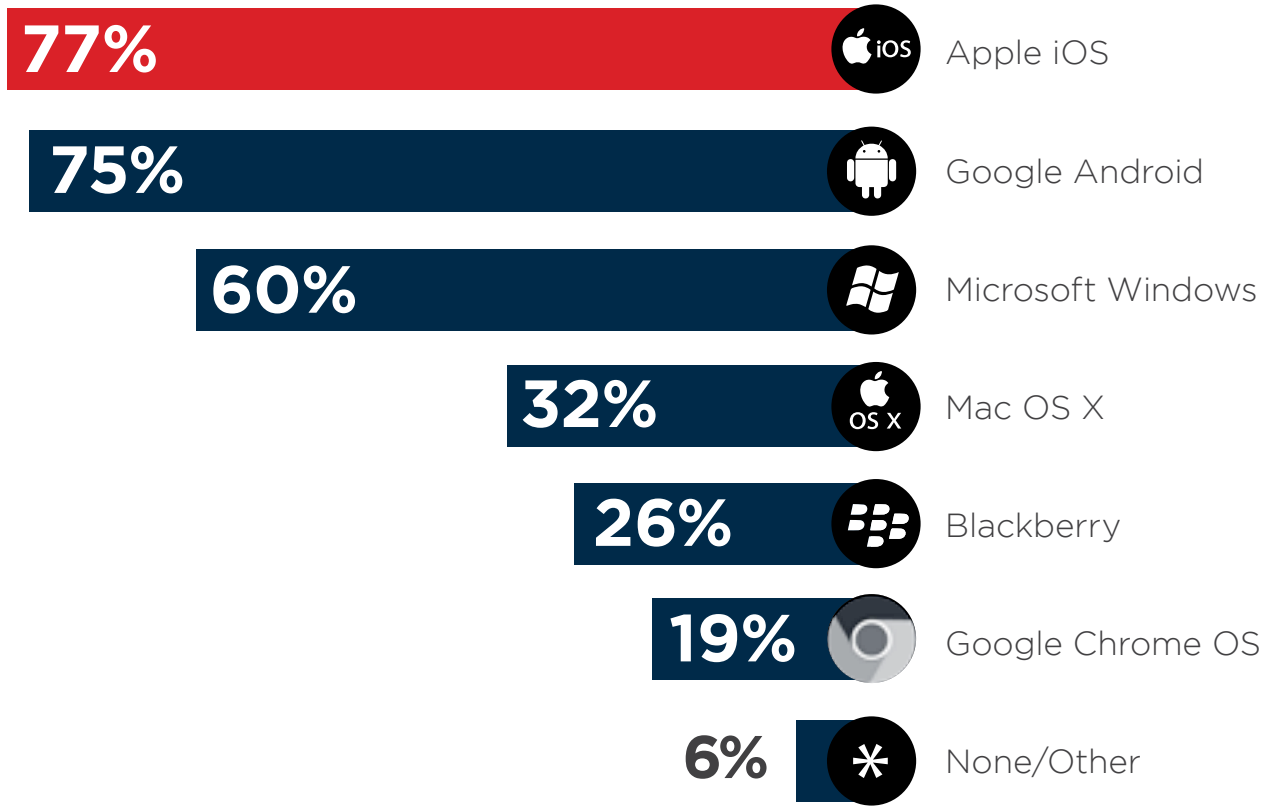
Responses do not add up to 100% because survey participants selected multiple choices.

MOBILE DEVICE PLATFORMS & SUPPORT

MOBILE PLATFORMS

Apple iOS takes the lead among supported BYOD mobile platforms at 77 percent. Meanwhile, Google Android is close behind at 75 percent, followed by Microsoft Windows (60 percent).

Q: Which mobile platforms does your company support?

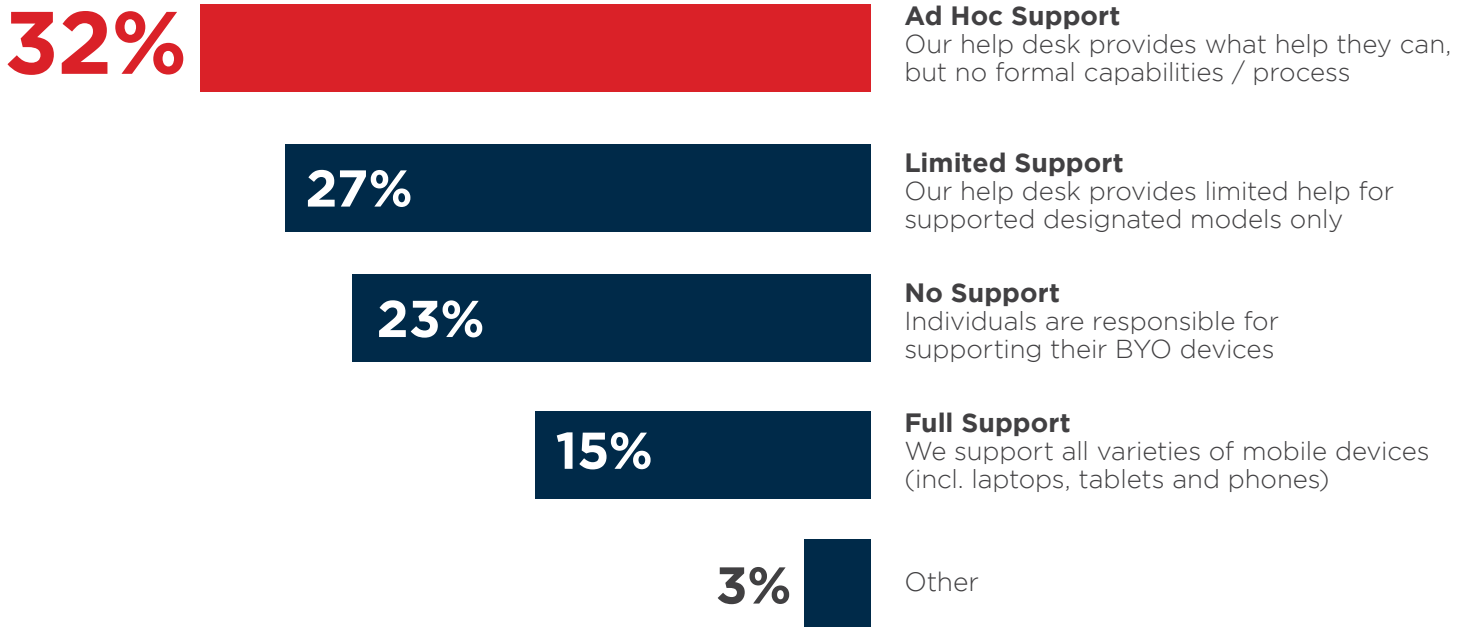


Responses do not add up to 100% because survey participants selected multiple choices.

BYOD SUPPORT LEVELS

The level of organizational support for BYOD users varies. 32 percent of organizations provide ad hoc support, but lack a formal process. 27 percent provide limited support for designated mobile models only and 23 percent provide no support whatsoever, making individuals responsible for supporting their own devices. Only 15 percent of organizations provide full support of all varieties of mobile devices (including laptops, tablets and smartphones).

Q: How do you currently support BYOD users experiencing device / access issues?



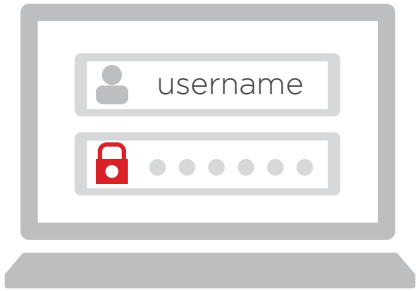
RISK CONTROL MEASURES

RISK CONTROL MEASURES

The most common risk control measure for mobile devices is password protection (63 percent), followed by remote wiping of devices (49 percent) and device encryption (43 percent). Credentials are often compromised as a result of phishing attacks. To limit risk of unauthorized access, organizations must implement more secure means of authentication. Single sign-on, contextual multi-factor authentication and single-use passwords can all help ensure those accessing data are who they say they are.

One of the more startling findings from our survey is that only 38 percent of organizations currently implement data removal at the time of employee separation or device disposal. As we have seen in many industry studies, failing to remove data properly from devices in these scenarios could leave hundreds of thousands of emails, SMS/IM messages, photos, videos and other sensitive information accessible by cyber criminals. This finding underscores the importance that organizations manage sensitive data across the entire lifecycle - from creation to storage to transfer to removal.

Q: Which risk control measures are in place for mobile devices?



63% Password protection

49%
Remote wipe

43%
Device encryption

38%
Data removal at employee separation or device disposal

DLP / Access Control 28% | Stopping access to sensitive information or systems for high-risk devices 25% | Auditing of mobile devices 25% | Endpoint Integrity Checking 24% | Quarantine high-risk devices 20% | Attack and penetration testing of mobile applications 13% | Automated remediation using other security systems 12% | Not Sure 10% | None 8% | Other 2%

Responses do not add up to 100% because survey participants selected multiple choices.

TOOLS TO MANAGE MOBILE DEVICE SECURITY

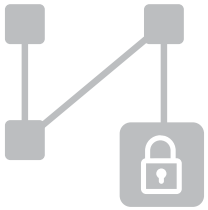
43 percent of organizations use mobile device management (MDM) tools to manage mobile devices, followed by endpoint security tools (28 percent) and Network Access Controls (NAC) with 27 percent.

These findings reinforce just how important it is for organizations to protect data after it is downloaded to the end user's device. It is also critical that organizations take into account unmanaged device blind spots and address them by implementing a data-centric security strategy that safeguards data across all devices on any network.

Q: What tools does your organization use to manage mobile device security?

43%

Mobile Device Management (MDM)



28%

Endpoint Security Tools (incl. Malware Protection)

27%

Network Access Control (NAC)

Enterprise Mobility Management (EMM) 17% | None 15% | Mobile Application Management (MAM) 14% | Configuration Controls / Lifecycle Management 12% | Mobile Threat Defense & Management (MTM) 11% | Mobile Device Diagnostics 8% | Certified Data Erasure 7% | Not Sure / Other 19%

Responses do not add up to 100% because survey participants selected multiple choices.

MAM CHALLENGES

Employee privacy is the most cited challenge of implementing Mobile Application Management (MAM) solutions (29 percent of organizations), followed by employee reluctance to use mandated mobile apps (22 percent).

Q: What challenges have you encountered with Mobile Application Management (MAM)?

29%

Employee privacy concerns

22%

Employees don't like the required mail and file share apps required by our MAM solution

13%

None

9%

Inability to containerize / wrap cloud apps

5%

Inability to containerize / wrap built-in apps like mail client and browser

5%

App wrappers breaking applications

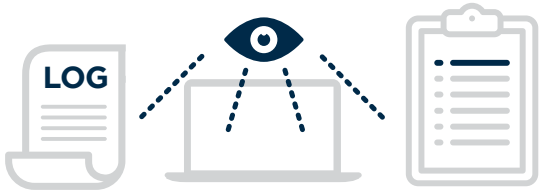
17%

Not Sure / Other

KEY REQUIREMENTS FOR MTM

The most requested capabilities for mobile threat management solutions are logging, monitoring and reporting (80 percent), indicating the need for better visibility into security threats and their impact on mobile devices across the organizations. This response is virtually tied with malware protection (79 percent).

Q: In your opinion, what key capabilities are required for Mobile Threat Management solutions?



80%

Logging, monitoring and reporting

79%

Malware protection

71%

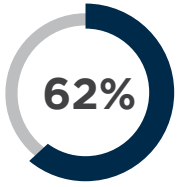
Vulnerability exploit defense

66%

Ease of deployment

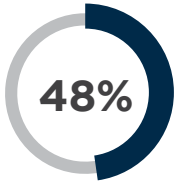
Network / WiFi attack defense

Cross-platform support



Role-based access control

Device configuration



Integration with other Endpoint Management Systems

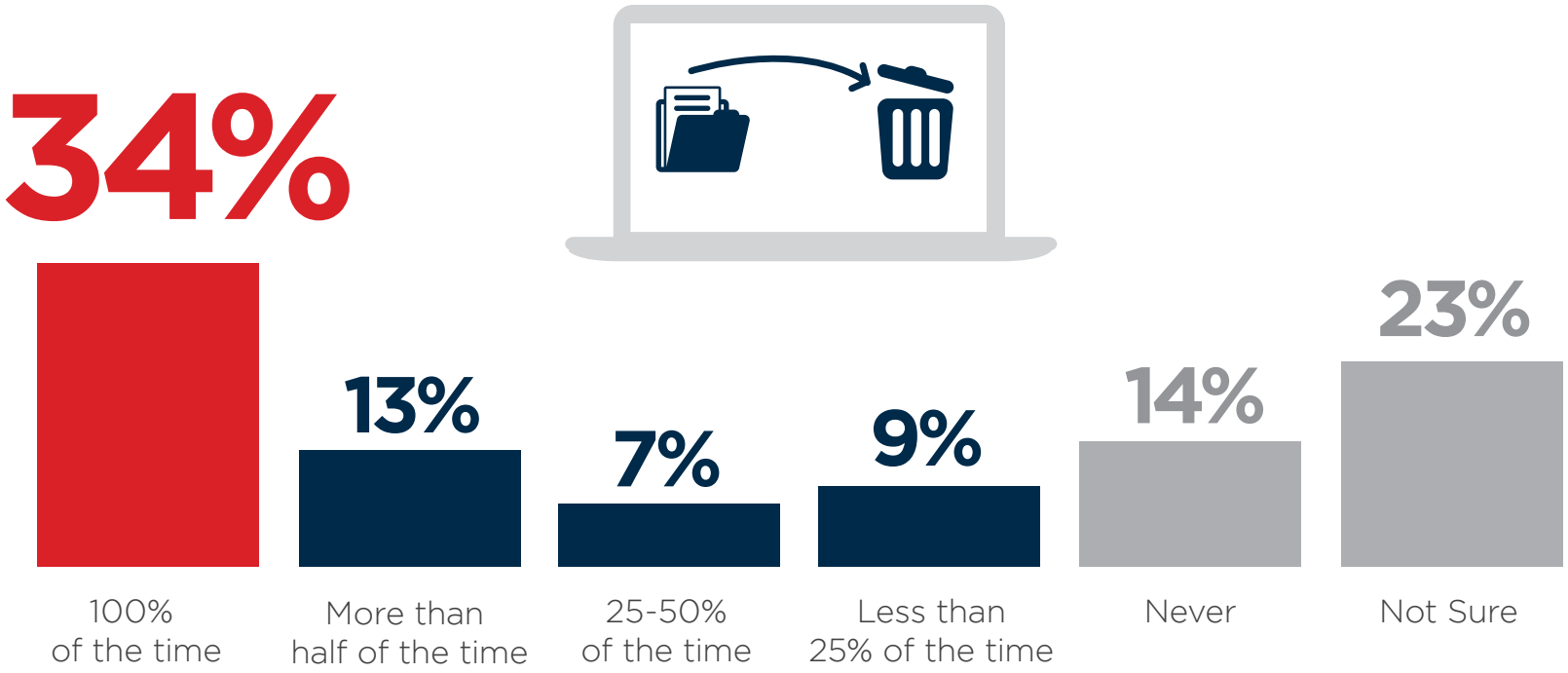
Responses do not add up to 100% because survey participants selected multiple choices.

EMPLOYEE DEPARTURE

Only 34 percent of organizations claim to wipe sensitive data off employee devices when they leave the company. Our study found that 29 percent wipe mobile devices occasionally and 14 percent never wipe devices.

These findings should be cause for concern. Failing to properly and completely erase data from devices when employees leave means a large amount of both personal and corporate information can be accessed, retrieved and stolen by unauthorized parties. If that happens, it doesn't just put the privacy of employees at risk, it also leaves corporate and customer data vulnerable to data loss and theft. This risk can be addressed by implementing enterprise-class, certified mobile data erasure solutions that erase data permanently and provide a tamper-proof audit trail for regulatory compliance.

Q: When an employee leaves (regardless of reason), what percent of the time do you actually wipe their devices?



DATA REMOVAL

The most popular data removal process for mobile devices is data deletion (29 percent), followed by device reformatting (26 percent). Certified data erasure tools are only used by 17 percent of organizations. This is problematic for many reasons. First, we know from several research studies that a factory reset does not properly erase data from Android devices; it only removes pointers to the data, not the data itself. Second, reformatting is not a fail-proof data removal method either; it can still leave data behind. These unreliable data removal methods put corporate, customer and employee data at risk.

Q: When employees leave the company, what device data removal processes do you use?

29%
Data Deletion

26%
Device Reformat

17%
Certified Data Erasure Tools

None

Free data erasure tools

Not Sure
Other

Responses do not add up to 100% because survey participants selected multiple choices.

SPONSORS

SPONSORS

Bitglass | www.bitglass.com

In a cloud-first, mobile-first environment, enabling secure BYOD is critical. While demand for BYOD continues to rise, adoption of MDM has stagnated due to privacy concerns, underscoring the need for an agentless, data-centric solution. Bitglass is the first and only agentless mobile security solution, capable of protecting corporate data across any device, anywhere, without installing agents or profiles. Founded in 2013 by industry veterans with a proven track record of innovation, Bitglass is based in Silicon Valley and backed by venture capital from NEA, Norwest and Singtel Innov8.

Blancco Technology Group | www.blanccotechnologygroup.com

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Check Point Software Technologies | www.checkpoint.com

Check Point Software Technologies Ltd. is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

SPONSORS

Skycure | www.skycure.com

Skycure is a predictive mobile threat defense (MTD) company with proactive defense solutions that actively detect and prevent mobile cyberattacks while preserving user privacy and experience and reducing the burden on IT. Skycure's mission is to secure both BYO and corporate-owned mobile devices to allow companies to mobilize without compromise. Skycure closes the mobile security gaps in organizations to protect against network-based threats, malware, vulnerability exploits, and other targeted attacks originating from both internal and external sources. Skycure's predictive technology is based on mobile threat intelligence gathered via massive crowd intelligence and sophisticated machine learning.

SnoopWall | www.snoopwall.com

The convergence of consumer privacy and mobile business security has arrived. MobileSHIELD ensures BYOD flexibility by enabling administrator control over device settings, applications, application privileges, ports and mobile data connectivity while connected to corporate networks and owner control when not. MobileSHIELD may be deployed on any mobile device/ tablet or installed on laptops and PCs to enhance corporate IT security oversight and control. MobileSHIELD is available as an agent-based solution as well as an application overlay SDK.

Tenable Network Security | www.tenable.com

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring.

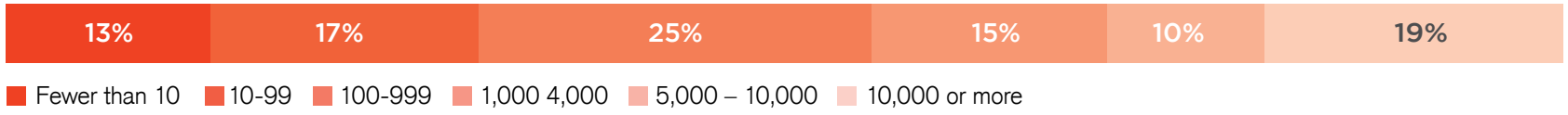
METHODOLOGY & DEMOGRAPHICS

The BYOD & Mobile Security Report is based on the results of a comprehensive survey of over 882 professionals across a broad cross-section of organizations about their adoption of BYOD related concerns and practices. Their answers provide a comprehensive perspective on the state of BYOD & Mobile Security today.

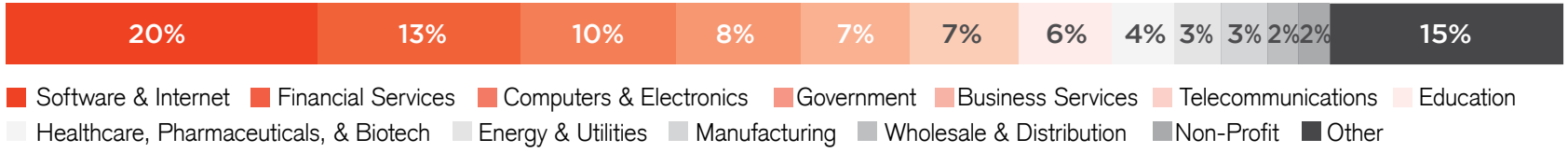
CAREER LEVEL

DEPARTMENT

COMPANY SIZE



INDUSTRY



CONTACT US

Interested in co-sponsoring the next security research report?

Contact us to learn more.

info@crowdresearchpartners.com

Produced by:

Crowd Research Partners

LinkedIn Group Partner
Information Security