THE GROWING THREAT
OF MOBILE DEVICE SECURITY BREACHES
A GLOBAL SURVEY OF SECURITY PROFESSIONALS

April 2017

dimensional research

THE GROWING THREAT
OF MOBILE DEVICE SECURITY BREACHES
A GLOBAL SURVEY OF SECURITY PROFESSIONALS

Dimensional Research | April 2017

It is common knowledge that mobile devices are integral to both our personal and business lives. With cyberattacks against individuals, businesses, and government entities increasing in frequency and sophistication, it is no surprise that mobile devices are now considered by threat actors to be one of the weakest links in the IT infrastructure of most enterprises. This report finds that 2 out of 10 companies have already experienced a mobile cyberattack, with an even larger number completely unaware whether they have been breached. While the cost of a mobile breach is similar to that of a desktop or laptop breach, a third of those surveyed stated the risk of data loss is higher on mobile devices. Meanwhile, two thirds of the survey's participants stated they are doubtful that their organizations can defend against a mobile cyberattack, while nearly all security professionals believe the number of mobile attacks will increase rapidly.

Just over one third of companies have deployed a mobile threat defense solution, with a lack of resources cited as the primary reason for going without advanced mobile security. That said, this research found that just over half of companies are increasing budget and resources to secure mobile devices compared to previous years. Currently, the threat is growing but focus and resource allocation appears insufficient to properly secure mobile devices.

Key Findings

- **Security Professionals Unprepared and Not Confident**
  - 64% of participants are doubtful their organizations can prevent a mobile cyberattack
  - Over 1/3 of companies fail to adequately secure mobile devices
  - More than half believe risk of data loss is equal to or greater than desktops/laptops

- **Mobile Devices to Come Under Increasing Attacks**
  - 20% of companies' mobile devices have been breached, and 24% don't know whether they've experienced an attack
  - 94% expect the frequency of mobile attacks to increase
 - 79% state the difficulty of securing mobile devices is growing

dimensional research
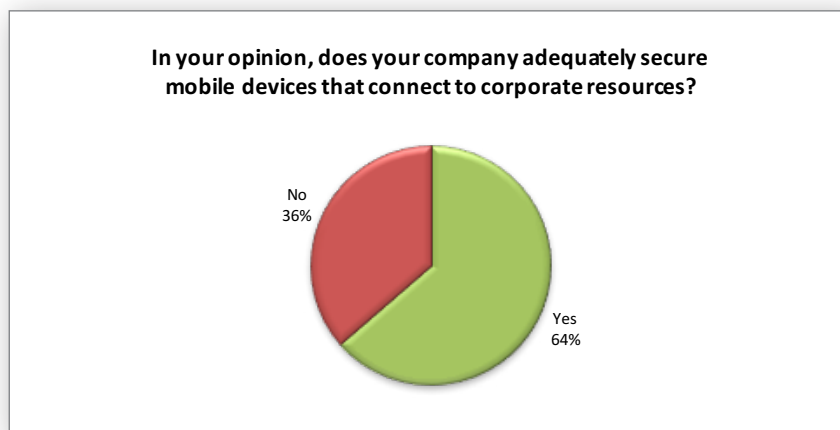
Sponsored by

Check Point®
SOFTWARE TECHNOLOGIES LTD

www.dimensionalresearch.com

Detailed Findings

20% of survey respondents stated that their company has already experienced a mobile device security breach, while just over half stated they have not. Perhaps the most surprising finding is that 24% of the security professionals are unaware if they have been compromised. Often not knowing you have been hacked is worse than knowing. These security professionals have little visibility into the security of the mobile devices in their businesses. Keep in mind that many of the recent and most highly-publicized security breaches revealed that the hacked businesses were oblivious to the breach for quite some time.

Has your company ever experienced a security breach on or from a mobile device?

- I don't know 24%
- Yes 20%
- No 56%
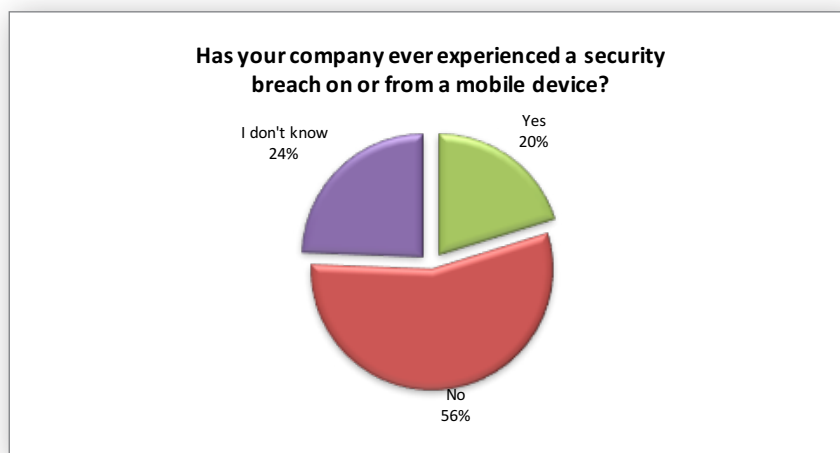
When security professionals were asked directly if their company's mobile devices were adequately secured, only 64% stated they were. Approximately 1/3 of the companies are aware that mobile devices and the data on them are currently at risk – a risk they know and state could be better mitigated. Perhaps some companies believe the data loss or pirated corporate access via mobile devices is just not that dangerous.
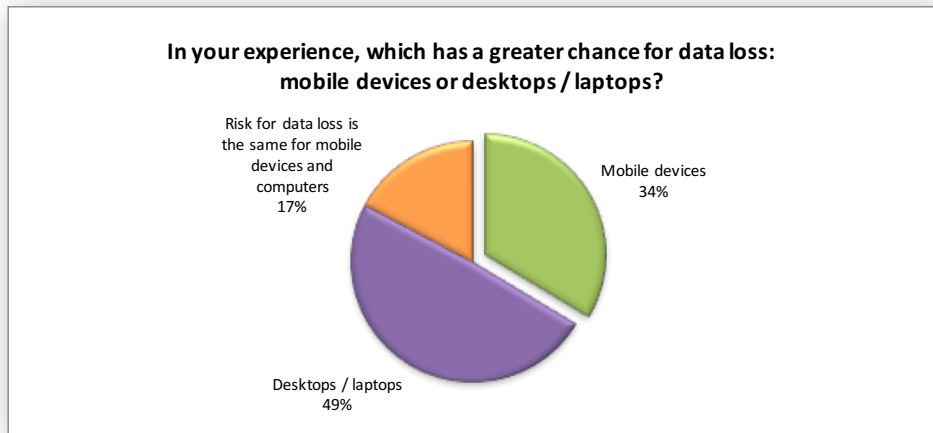
In your opinion, does your company adequately secure mobile devices that connect to corporate resources?
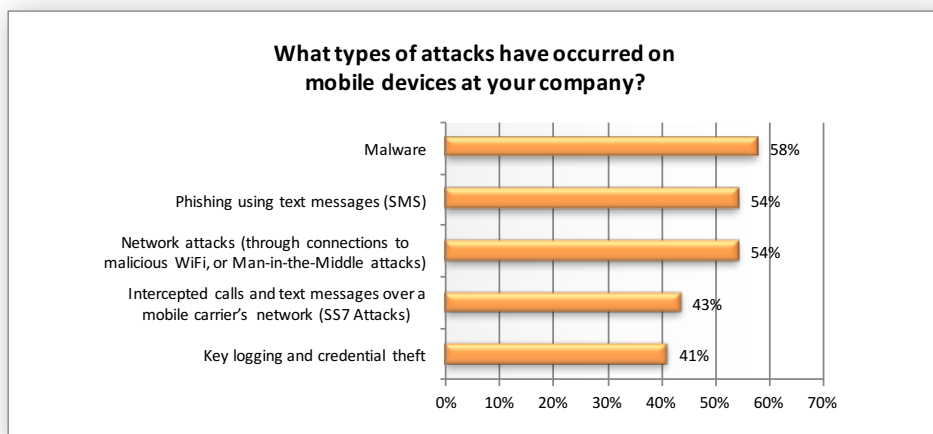
- No 36%
- Yes 64%

Dimensional Research | April 2017

17% of the participants felt the risk of data loss on mobile devices was equal to the risk of data loss with desktop and laptop computers. However, 34%, representing one in three participants, believe the potential for data loss is greater on mobile devices. Perhaps the high level of concern is based on the frequency of mobile device loss or theft, as well as the limited security measures companies use to protect enterprise mobile devices.

In your experience, which has a greater chance for data loss: mobile devices or desktops / laptops?

- Risk for data loss is the same for mobile devices and computers 17%
- Mobile devices 34%
- Desktops / laptops 49%

When posed with the question "What types of attacks have occurred on mobile devices at your company?" it was expected that one or two modes of attack would rise to the top. Instead, security professionals reported a broad range of successful attacks against their organization's mobile devices. This places increased challenges not only on security professionals, but on defensive strategies and solutions for mobile devices.
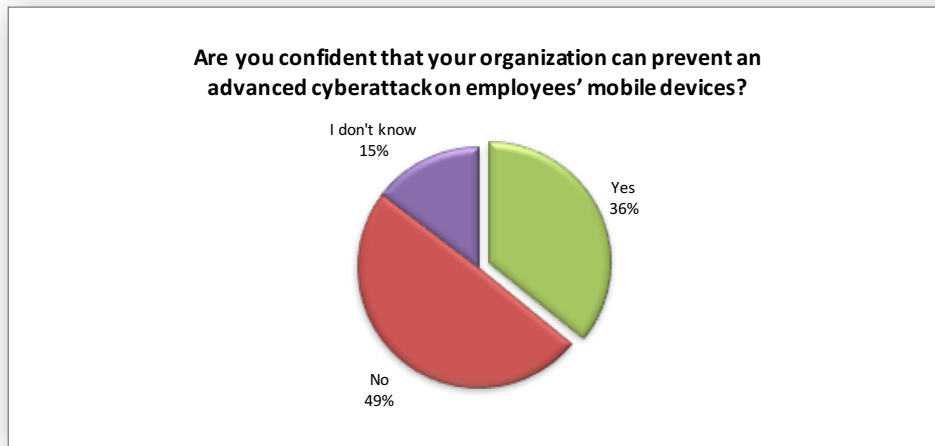
What types of attacks have occurred on mobile devices at your company?

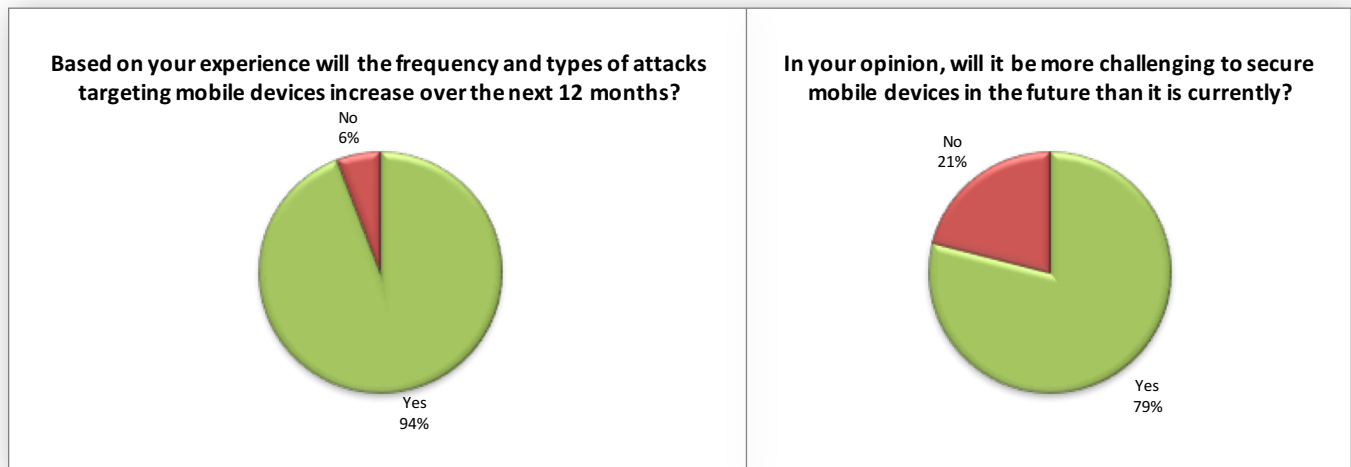| Attack type	Percentage
Malware	58%
Phishing using text messages (SMS)	54%
Network attacks (through connections to malicious "WiFi, or Man-in-the-Middle attacks)	54%
Intercepted calls and text messages over a mobile carrier's network (SS7 Attacks)	43%
Key logging and credential theft	41%

It is likely the combination of successful mobile attacks, lack of visibility and inadequately secured devices drove 64% of those surveyed to state they are not confident they can prevent a cyberattack targeted at mobile devices. Another factor contributing to the lack of confidence is the constant evolution of threats and the relentless barrage from hackers. Company executives should be highly concerned, as only one of three of those charged with securing devices used in the enterprise are confident they can do so.

Are you confident that your organization can prevent an advanced cyberattack on employees' mobile devices?

- I don't know 15%
- Yes 36%
- No 49%

The future looks more daunting and the risk appears to be increasing, as 94% of those surveyed expect the frequency of mobile device attacks to increase, and 79% expect the task of securing mobile devices to become increasingly difficult. Given the lack of confidence today and the growing threats in the future, it appears that mobile device security will become an increasingly vulnerable spot in most companies' cybersecurity defenses.

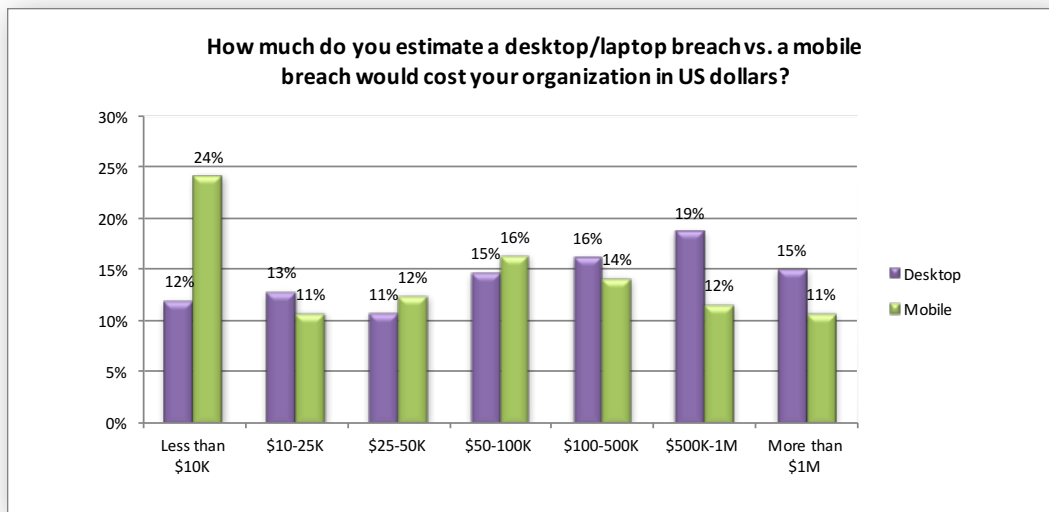**Based on your experience will the frequency and types of attacks targeting mobile devices increase over the next 12 months?**

- No 6%
- Yes 94%

In your opinion, will it be more challenging to secure mobile devices in the future than it is currently?

- No 21%
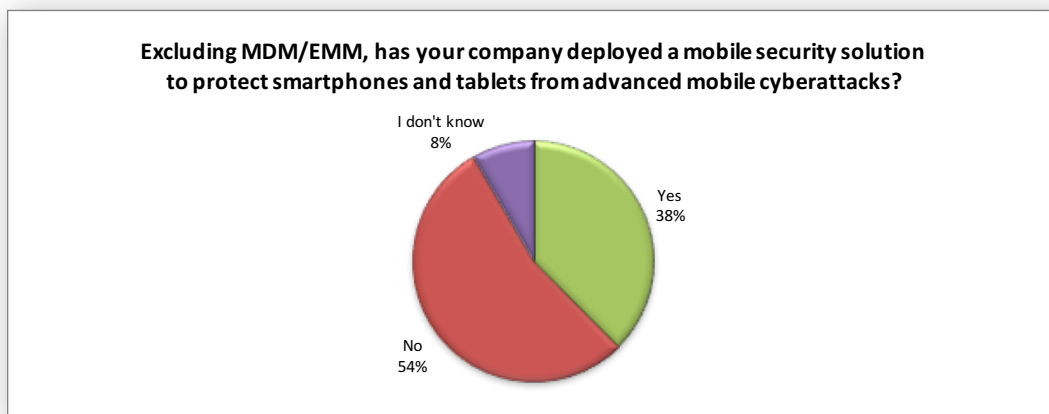- Yes 79%

But often the time, budget, and resources focused on enterprise security initiatives are directly related to the cost of a breach on the company. In the figure below, participants quantified the cost of a cyberattack to an enterprise mobile device and compared it to that of a desktop or laptop attack. While at the bottom end we see a cheaper cost per breach for mobile devices, the rest of the data shows that the costs are somewhat similar. While some of the data indicates that a mobile breach may cost less, it is not a dramatic difference, with over 20% of the participants saying that a mobile breach could cost the company more than $500 thousand dollars. It's clear that the survey's respondents consider the data lost in a potential cyberattack on enterprise mobile highly valuable. That perceived value of enterprise data from such a mobile attack is obviously shared by hackers, who have clearly increased their focus of attacks on mobile devices.

How much do you estimate a desktop/laptop breach vs. a mobile breach would cost your organization in US dollars?

Earlier in this report, those surveyed showed a lack of confidence in their current mobile device security and were extremely doubtful of their organization's ability to prevent an attack. This finding – that only 38% of the companies have a dedicated mobile device security solution – may be the key reason. More than half the organizations surveyed use only enterprise mobile management platforms to protect devices against advanced cyberattacks.
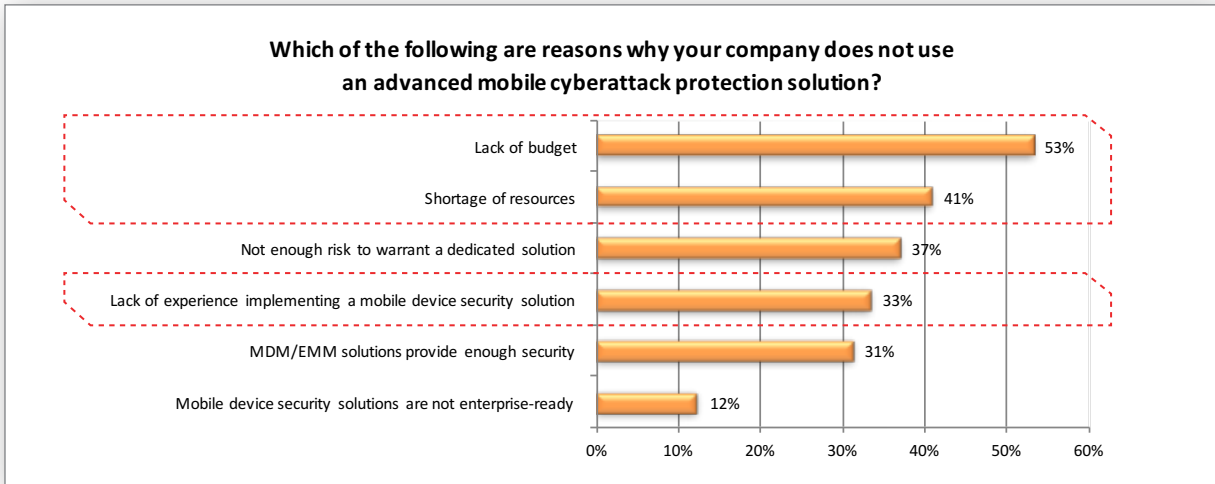

Excluding MDM/EMM, has your company deployed a mobile security solution to protect smartphones and tablets from advanced mobile cyberattacks?
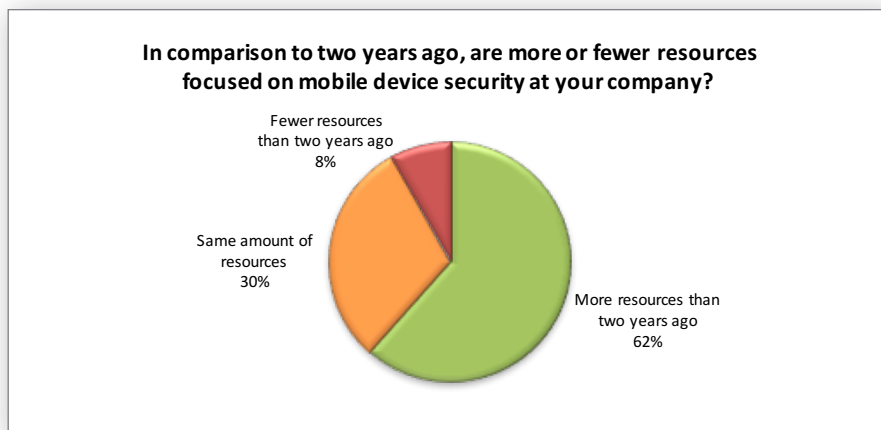
We then asked survey participants why their company hadn't deployed a mobile device security solution. Over 60% of respondents indicated some lack of resources (i.e. budget, shortage of personnel) or lack of experience as the key drivers. Only 37% made a conscious appraisal for their company and decided there was not enough risk to warrant the investment.

Which of the following are reasons why your company does not use an advanced mobile cyberattack protection solution?

- Lack of budget — 53%
- Shortage of resources — 41%
- Not enough risk to warrant a dedicated solution — 37%
- Lack of experience implementing a mobile device security solution — 33%
- MDM/EMM solutions provide enough security — 31%
- Mobile device security solutions are not enterprise-ready — 12%

With the generally accepted rise in mobile malware and attacks, it was not surprising that 62% of companies are dedicating more resources to the growing threat. This data supports the earlier finding that resources are constraining the ability to deploy adequate mobile device security solutions. Meanwhile, 8% of the surveyed companies were actually allocating fewer resources to the growing problem of mobile security.
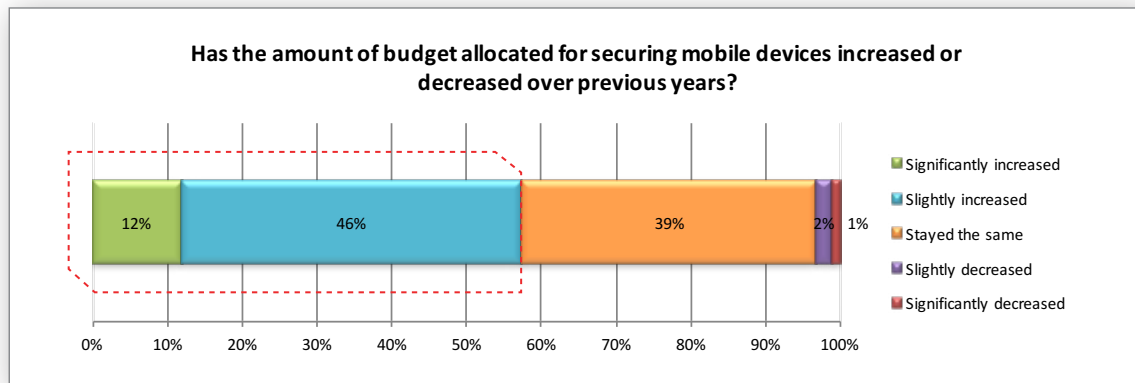
In comparison to two years ago, are more or fewer resources focused on mobile device security at your company?

- Fewer resources than two years ago 8%
- Same amount of resources 30%
- More resources than two years ago 62%

Dimensional Research | April 2017

The other component of the lack of resources cited earlier is budgeting. Here, just over half of the surveyed companies (58%) will receive more budget to mitigate the mobile device security threat, and 39% are left with the same budget they had in 2016. It is clear why so many security professionals are doubtful about their ability to prevent cyberattacks on mobile devices given the lack of resources, budget, and dedicated mobile device security solutions.

Has the amount of budget allocated for securing mobile devices increased or decreased over previous years?

■	Significantly increased
■	Slightly increased
■	Stayed the same
■	Slightly decreased
■	Significantly decreased

Conclusion

This research indicates that many companies are under imminent risk, as 64% of security professionals who are charged with protecting mobile devices from cyberattacks are doubtful they can do so. Over a third of these professionals stated that today their mobile devices are not sufficiently protected or secure. With the proliferation of mobile devices as business tools it is hard to believe than only 38% of the companies have a security solution focused on protecting mobile devices and the data on them. This research shows that security professionals lack the resources and tools to be properly prepared, but even more surprising is that nearly a quarter of them don't know if their company's mobile devices have been breached or are leaking corporate data. Over 1/3 of those surveyed believe that the risk of data loss from a mobile device is higher than desktop or laptop computers.

These findings illustrate that the mobile device risk is real for businesses today and that 1 out of every 5 companies admitted to already being breached. The future is bleak for security professionals as 94% shared that their expert perspective is that the frequency of mobile device attacks will increase and 79% stated that it will become even more difficult to secure mobile devices. Without a change to these trends, the frequency and success of mobile devices attacks will rapidly increase. The dichotomy of management trying to control costs and security professionals struggling with insufficient tools to repel attackers is not a new story line in most enterprises. Unfortunately, the story usually ends sadly with a huge, embarrassing event with the press blazing headlines of a costly hack and the company suffering brand damage and loss of customer confidence. Will 2017 be the year of the first humiliating public hack via a mobile device? That remains to be seen.
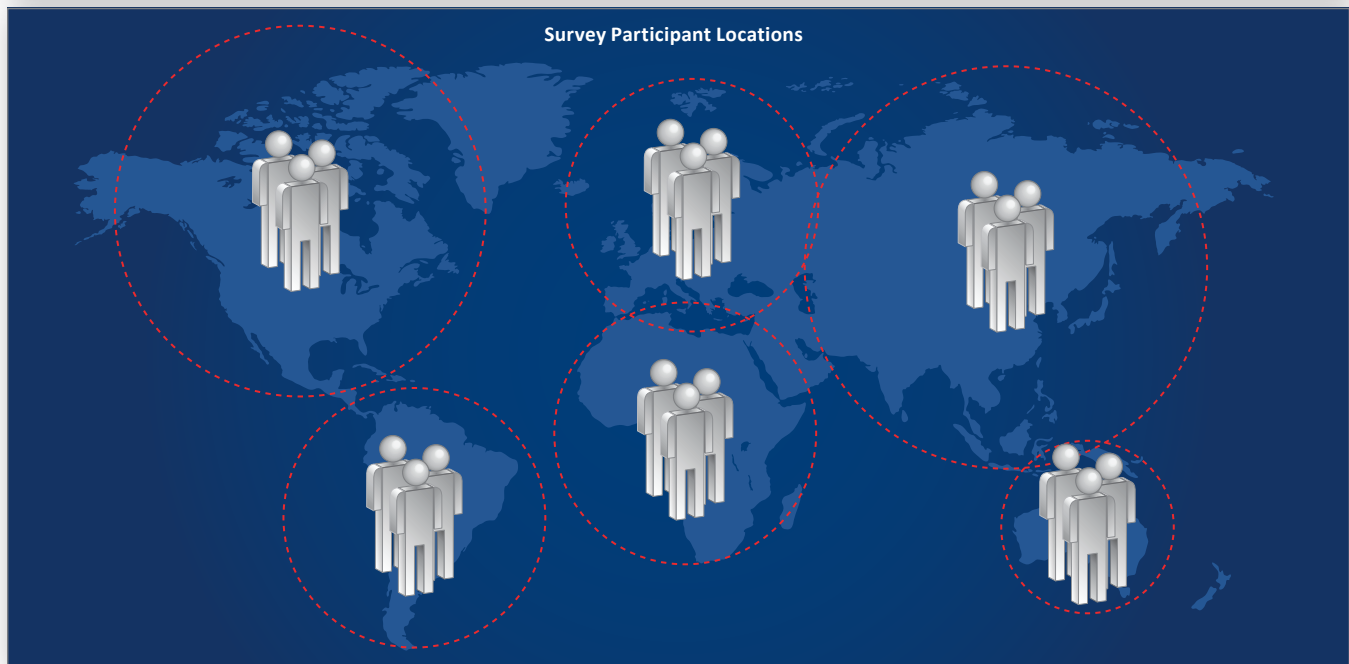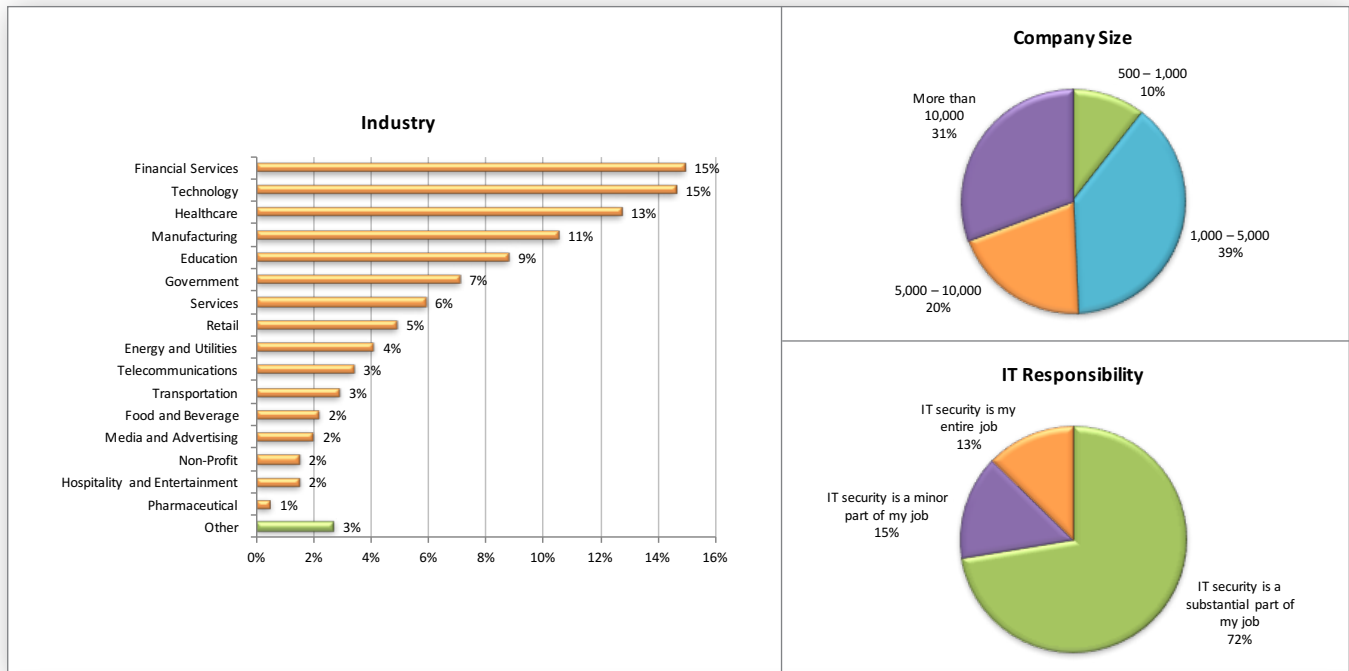
Dimensional Research | April 2017

Survey Methodology

Security professionals worldwide from an independent global database were invited to participate in a survey on the topic of mobile device security. A total of 410 participants who have security leadership or frontline responsibilities completed the global survey. Participants represented each of the five continents with the full spectrum of job responsibilities and company sizes. The survey was administered electronically and participants were offered a token compensation for their participation.

Industry

Industry	%
Financial Services	15%
Technology	15%
Healthcare	13%
Manufacturing	11%
Education	9%
Government	7%
Services	6%
Retail	5%
Energy and Utilities	4%
Telecommunications	3%
Transportation	3%
Food and Beverage	2%
Media and Advertising	2%
Non-Profit	2%
Hospitality and Entertainment	2%
Pharmaceutical	1%
Other	3%

Company Size

- 500 – 1,000: 10%
- 1,000 – 5,000: 39%
- 5,000 – 10,000: 20%
- More than 10,000: 31%

IT Responsibility

- IT security is my entire job: 13%
- IT security is a minor part of my job: 15%
- IT security is a substantial part of my job: 72%

Survey Participant Locations

www.dimensionalresearch.com

About Dimensional Research

Dimensional Research® provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information, visit www.dimensionalresearch.com.

About CheckPoint Software Technologies

Check Point Software Technologies Ltd. is the largest network cybersecurity vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

For more information, please visit http://www.checkpoint.com/