BUSINESS TECHNOLOGY BRIEFING

The State of BYOD *(Bring Your Own Device):* GLOBAL TRENDS, SHIFTS, AND OPPORTUNITIES.

FUTURUM.

Q1 2017

Welcome to Futurum's Business Technology Briefing series. Futurum briefings are designed to convey critical and time-sensitive insights to decision-makers in the most concise and time-effective format possible. While our reports offer deep dives into new and emerging business technologies and critical Digital Transformation topics, our Briefings identify new opportunities and threats in the market, highlight shifts and trends most likely to impact your business, and prioritize insights to paint the clearest possible picture in the shortest amount of time.

Net ROI Value: BYOD as a productivity booster

Mobility continues to be one of the most transformative forces in the business world today. The more connected a workforce is, the more productive it tends to be. We note a direct correlation between the degree to which employees are connected to their work via smartphones and changes in their productivity. A recent study by Fliplet shows that an employee with 24/7 access to his or her work via smartphone can deliver as many as 240 hours of additional productivity per year. This increase in productivity translates into 6 weeks per year, per employee.

That figure focuses on the median of highly engaged and moderately engaged employees. We estimate that in the case of highly engaged teams, that number comes closer to 584 hours of additional productivity per year, or 14.6 weeks per employee.

Global trend lines: The BYOD model is gaining mainstream acceptance

The first of several key challenges for businesses, regardless of size, is deciding whether to supply their employees with company-owned smartphones or let them use their own. While businesses around the globe are split on which direction to take, we are noting a significant shift towards BYOD policies across all regions. Here is our summary from the trenches:

GLOBALLY:

85%

of organizations already allow employees to bring their own devices to work

GLOBALLY:

1/3

of businesses stopped providing devices to their employees last year (2016).

GLOBALLY:

50%

of employers now require employees to supply their own devices for work purposes.

For reference: Global smartphone shipments amounted to 480 million units in 2016. 65% of these devices are estimated to be currently used in a BYOD capacity.

Mobile workforce forecasts 2020:

GLOBALLY:

1.75 BILLION WORKERS

(42% of the global workforce)

US:

105 MILLION WORKERS

(73% of the US workforce)

Employee empowerment and adoption

In regards to employee preference, 77% of workers report that using only one device for personal and professional use is the most convenient option. 80% believe that being able to use mobile devices for work makes them more productive.

Productivity and convenience far outweigh perceived security risks

Although data security is the principal concern for companies considering BYOD policies, 61% of businesses agree that BYOD improve employee mobility, 55% signal that BYOD improves employee productivity, and 47% report that BYOD reduces the overall cost of business. By all accounts, the threat-to-opportunity equation appears to favor opportunity over threat:

We note that while globally, security is the #1 objection to BYOD policies, and the combined threat of data leaks and unauthorized outside access to sensitive company data and systems tends to come up as the #1 concern for IT departments when discussing whether or not to deploy or scale a BYOD policy, nearly 70% of businesses report that they do not plan to increase mobile security budgets in the foreseeable future.

BYOD and mobile device security overview: closing the vulnerability gap

One important reason for the gap between the gravity of the perceived threat of mobile vulnerabilities and what our analysts would qualify as an anemic call to action in response to that threat may be that only 21% of businesses report that mobile devices were involved in security breaches in the last two years. Ad-

13%

of organizations are currently operating under a strict No BYOD policy

32%

of organizations make BYOD available to select employees.

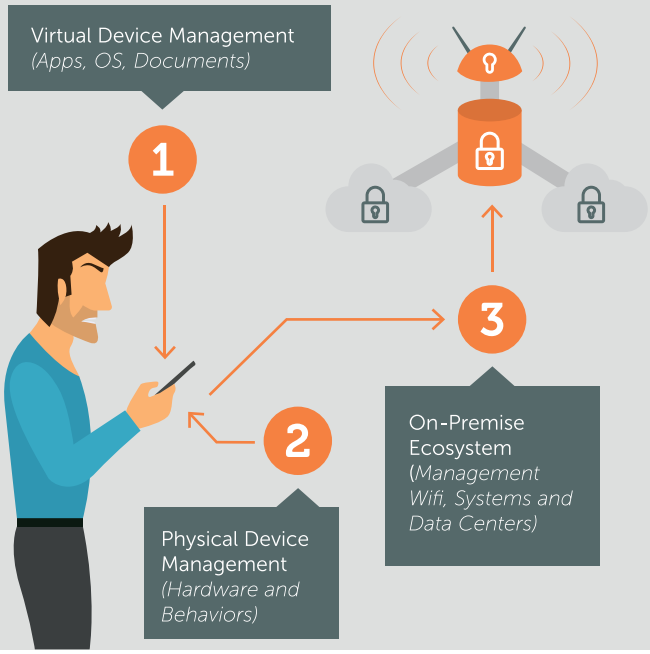
40%

of organizations make BYOD available to all employees.

ditionally, we note that these security breaches were not limited to personal devices used in a BYOD capacity, but also include company-supplied devices.

As the universal vulnerability of mobile devices helps invalidate arguments against BYOD policies, organizations are shifting their focus away from hardware management to software and procedural solutions that will help them secure unauthorized mobile access to their data and systems:

BYOD and Mobile Device Security: Closing the Vulnerability Gap



Diving deeper into Virtual Device Management, here is a short list of mobile Security products worthy of note, by category:

PHYSICAL DEVICE MANAGEMENT:

Roughly 50% of mobile security breaches can be traced back to either malware downloaded by employees, or lost and stolen devices. To address these specific vulnerabilities, organizations can easily combine employee training and device management protocols without having to invest in complex or expensive IT solutions.

ON-PREMISE ECOSYSTEM MANAGEMENT:

On-premise IT security products can help secure vulnerable in-house wifi networks, systems and data centers.

VIRTUAL DEVICE MANAGEMENT:

For more pernicious and deliberate mobile-related security breaches, the deployment of enterprise-class mobile security products, as well as collaboration products with built-in end-to-end encryption usually helps close gaps not already filled in the cloud by solutions providers.

- **VIRTUAL DEVICE MANAGEMENT:**

  Samsung Knox*: provides a solution native to Samsung devices, conveniently eliminating the need for additional security product purchases.

  Apple iOS*: provides layers of built-in encryption

- **AFTERMARKET SECURITY LAYER:**

  Microsoft Enterprise Mobility Suite: provides an aftermarket security solution that integrates naturally into Microsoft productivity and collaboration ecosystems.

  IBM MaaS 360: provides an all-in-one aftermarket mobility security solution for the enterprise.

- **SECURE APPLICATION LAYER:**

  Cisco Spark: Provides an agile, endpoint-agnostic collaboration ecosystem with a built-in end-to-end encryption.

**Note: >85% of mobile devices used in BYOD professional environments are iOS and Android.*

Conclusion

Our outlook regarding BYOD within the scope of a Digital Transformation initiative is overwhelmingly positive. With adequate security protocols and systems in place – as outlined above, - enterprise-class companies and SMBs alike can easily and cost-effectively transition to agile, BYOD-friendly, cloud-based productivity and collaboration models with minimal risk to their operations and infrastructure.