Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SC Total Security: BYOD Roundtable

J E (John) Rowzee

Data Security – Europe

john.rowzee@checkpoint.com

27 June 2013

BYOD: Its not about Security!

Check Point
SOFTWARE TECHNOLOGIES LTD.

…if it was y solution!

Conventional Thinking: "Protect the Device at all Costs"
(even if it disrupts the business)

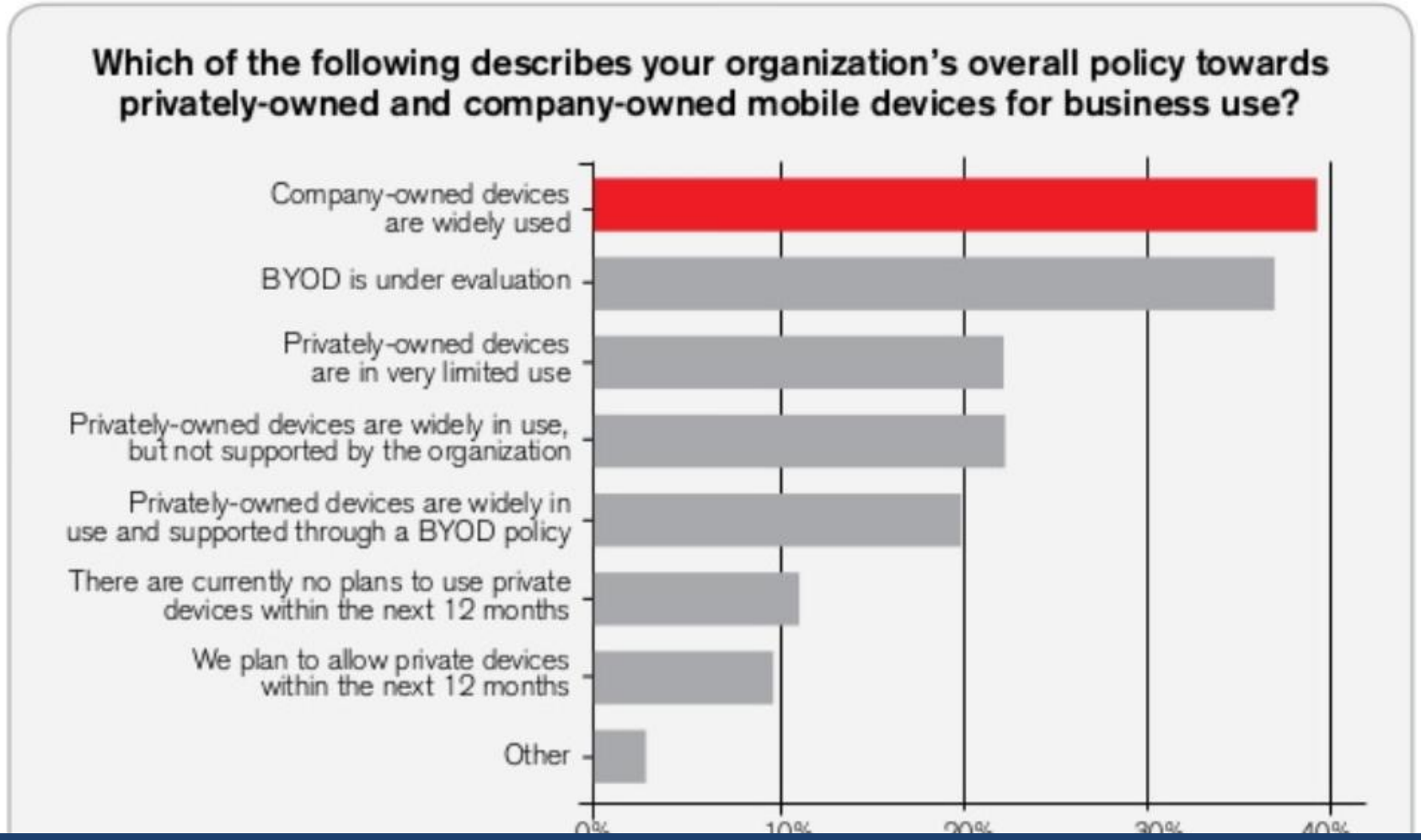
BYOD: You're already doing it…

93%

of Organizations
Allow Mobile Devices
into the Business

…so how much risk does BYOD really involve?

BYOD: But why?

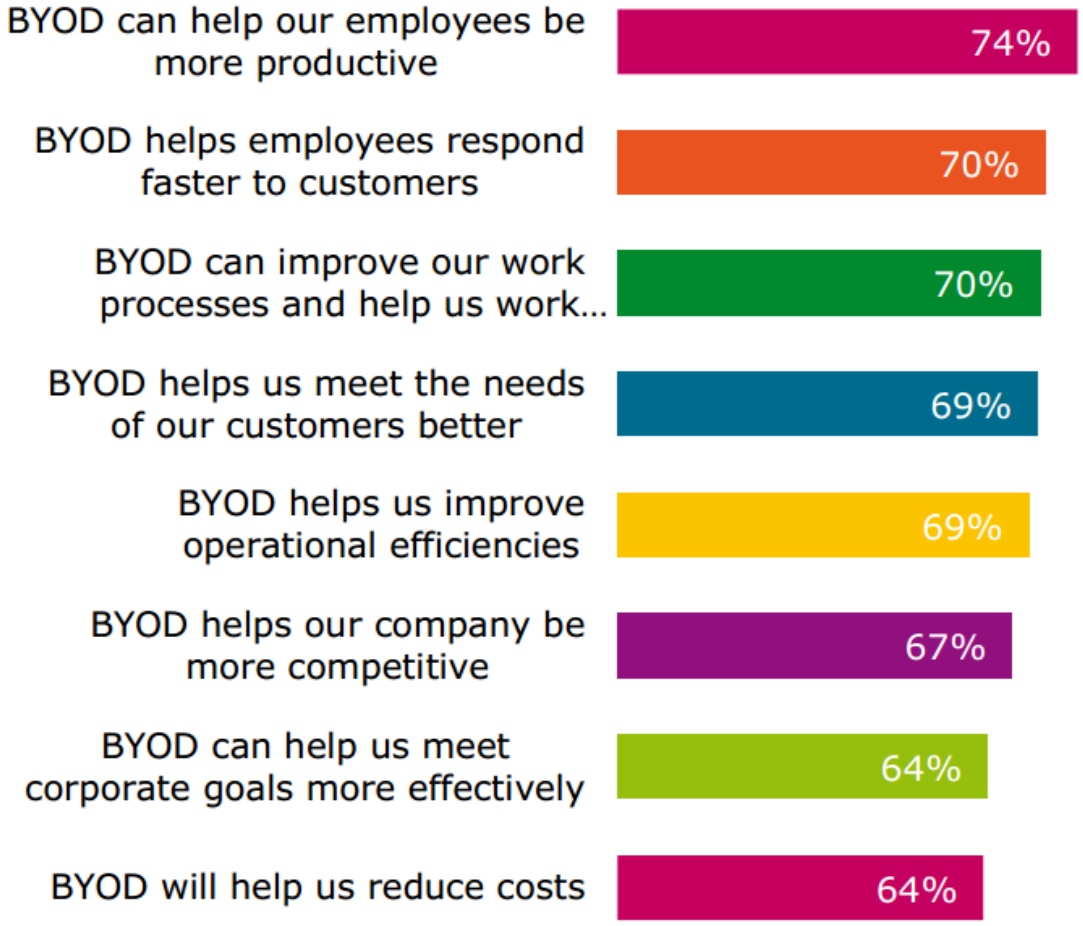


…and why are you doing it? And how's it going?

BYOD: But why?

Check Point SOFTWARE TECHNOLOGIES LTD.

Potential corporate gains from BYOD



Can we balance BYOD efficiencies with effective Security?

In practice, not always as successful

Check Point SOFTWARE TECHNOLOGIES LTD.

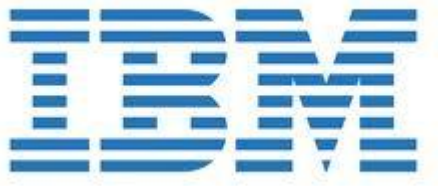
- Case Study: US SEC
  - Started with “voluntary” BYOD security policy
  - Day-to-Day BYOD devices used in the SEC’s Trading and Markets Division were taken to a Black Hat conference
  - This disclosure subsequently forced the conduct of an audit at the SEC, costing in excess of $200K
  - The audit’s findings uncovered an environment where ad-hoc devices were allowed free reign to most sensitive areas of their

What could have helped here?

In practice, not always as successful

Check Point SOFTWARE TECHNOLOGIES LTD.

- Case Study: IBM



  - 60,000 of IBM's 400,000 employees were allowed BYOD access to the company's infrastructure
  - Not only was BYOD not saving IBM money, but the proliferation of devices, with no standardization, caused headaches for the IT Department due to the risks of rogue devices and apps
  - IBM now mandates MDM on BYOD devices, and has imposed multiple configuration controls, including remote wipe, blocking of cloud services, and even Siri

Strict MDM on employee kit: is this really BYOD?

BYOD Security Concerns are Real

- Policy Violation or Abuse
- Lack of Passwords and Encryption
- Device Loss/Theft
- Lack of Control for Apps & Data
- Lack of Device Control & Configuration
- BYOD and IP loss
- Unauthorised 3rd Party Data Transmission
- Mobile Malware and Untrusted/Jailbroken platforms
- Lack of Consistency across Platforms

Did I miss anything?

BYOD Security Concerns are Real

24% Source Code

14% Password protected file

7% Email marked as confidential

29% Credit card information

13% Salary compensation information

7% Bank accounts numbers

6% Business data record

54%

of Organizations Experienced Data Loss

- *Source: Check Point 2013 Security Report, 900 companies surveyed, 120,000 hours traffic monitored*

Some Enterprises are flying blind…

Organizations **without** a formal BYOD Policy in place for:

Smartphones – **55%**

Tablets – **49%**

Laptops – **41%**

Compliance Violations
IP Loss/Theft
Malware Propagation
Lack of Visibility/Audit

BYOD: How heavy a hand to apply…

- No controls
- Paper-based Policy – no technology backup
- Network & Access segregation
- Data Containment
- Light or Heavy MDM
- No BYOD allowed

One Approach does not fit all! What's yours?

But users see it differently…

“I already have my own device, I don’t want another one”

“I need access to my work information on the move”

“I’d be happier using a device I’m already comfortable with”

“I want to keep using my personal apps/data as well”

Usability & User Satisfaction

- Platforms & Form Factors
- Use cases: is it fit for purpose?
- Application / Platform familiarity & availability
- IT Support Desk capability
- Security from the User's side: protection of personal data
- The overall goal: **User Acceptance**

One example of a successful BYOD rollout effect:

81 extra minutes productivity/week

BYOD synergy value: $350 – 3150 per year per user

Employees spending an average of $965 out-of pocket on devices

Source: Cisco News Analysis: Comprehensive BYOD Implementation Increases Productivity, Decreases Costs

Other factors to consider

- Regulation & Compliance
- Data Sensitivity & Access
- Policy Management
- Reporting & Auditing
- Industry-specific applications
- Cost

Example: Industry-specific BYOD Rules and Guidance

- Information Commissioners Office (UK Government) 2013

Overview

In a nutshell:

It means you must have appropriate security in place to prevent the personal data you hold from being accidently or deliberately compromised. This is relevant if personal data is being processed on devices which you may not have direct control over.

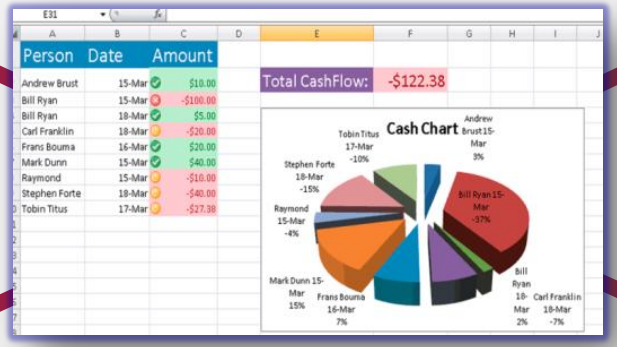
What the DPA says

The seventh principle says: appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data.

BYOD: Check Point's Approach

Organizational Boundaries Disappear

Smartphones and Tablets



Data Collaboration

USB Devices

Email

Uncontrolled BYOD magnifies risks already in place!

Securing BYOD with Check Point

Use Personal Devices for Business Data

Only Business Data is Managed

Remotely Wipe Business Data

On Mobile Devices

Use Business Data within a Secure Business Application

Only Authenticated Users Access the Business Container

On Mobile Devices

Use Business Data within a Secure Business Application

Use Emails Securely

Use Documents Securely

Protect Data with a Multi Layered Solution

Orchestrated Together

Simple to Manage Policy and Incidents

Central Visibility & Reporting

Mobile Information Protection – A Multi Layer Solution

Mobile Security	Enables Secure BYOD
Document Security	Enables Secure Document Sharing
DLP	Keeps Data Away from Wrong Hands
Endpoint Security	Protects Data on PCs and USBs

Summary

Check Point SOFTWARE TECHNOLOGIES LTD.

Protect Business Information Wherever Used

Meets End Users Needs – Enables BYOD & Information Sharing

Multi Layer Solution Protect Data on Mobile Devices, Documents & Endpoints

MOBILE INFORMATION PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Questions?

J E (John) Rowzee

Data Security – Europe

john.rowzee@checkpoint.com

27 June 2013