Why some things SHOULDN'T GO VIRAL.

bitglass whitepaper

PREVENTING BREACHES

IS ONLY AS EFFECTIVE AS YOUR EMPLOYEES' GRIP ON THEIR DEVICES

A lost device, whether for personal or business purposes, holds sensitive company data and access to the company's network. If the keys to the kingdom fall into the wrong hands, loss of trade secrets, business opportunities, and the company's reputation can result – making lost or stolen devices the top mobile security concern of company leaders around the world.

THE BYOD DILEMMA

MOST EMPLOYEES USE PERSONAL DEVICES TO ACCESS COMPANY DATA, IN FACT

Smartphones

Tablets

Laptops

67%

Of employees use personal devices to access company information. This data ranges from emails, to accessing documents in the cloud, to client / partner information & communications.

Studies show that telecommuters are happier, more productive, and work longer days.

Employees are willing to spend their own money to maintain the flexibility and device familiarity that Bring Your Own Device provides.

Bring Your Own Device (BYOD) is mutually beneficial for both companies and employees.

Compared to office workers, Telecommuters:

Work 9.5% longer days

Were 13% more productive

Quit 50% less often

21%

Of those do so despite the presence of anti-BYOD policies

THE AVERAGE AMERICAN BYOD EMPLOYEE

MAKING $45,000 A YEAR

SAVES THEMSELVES ABOUT 81 MINUTES A WEEK WITH BYOD

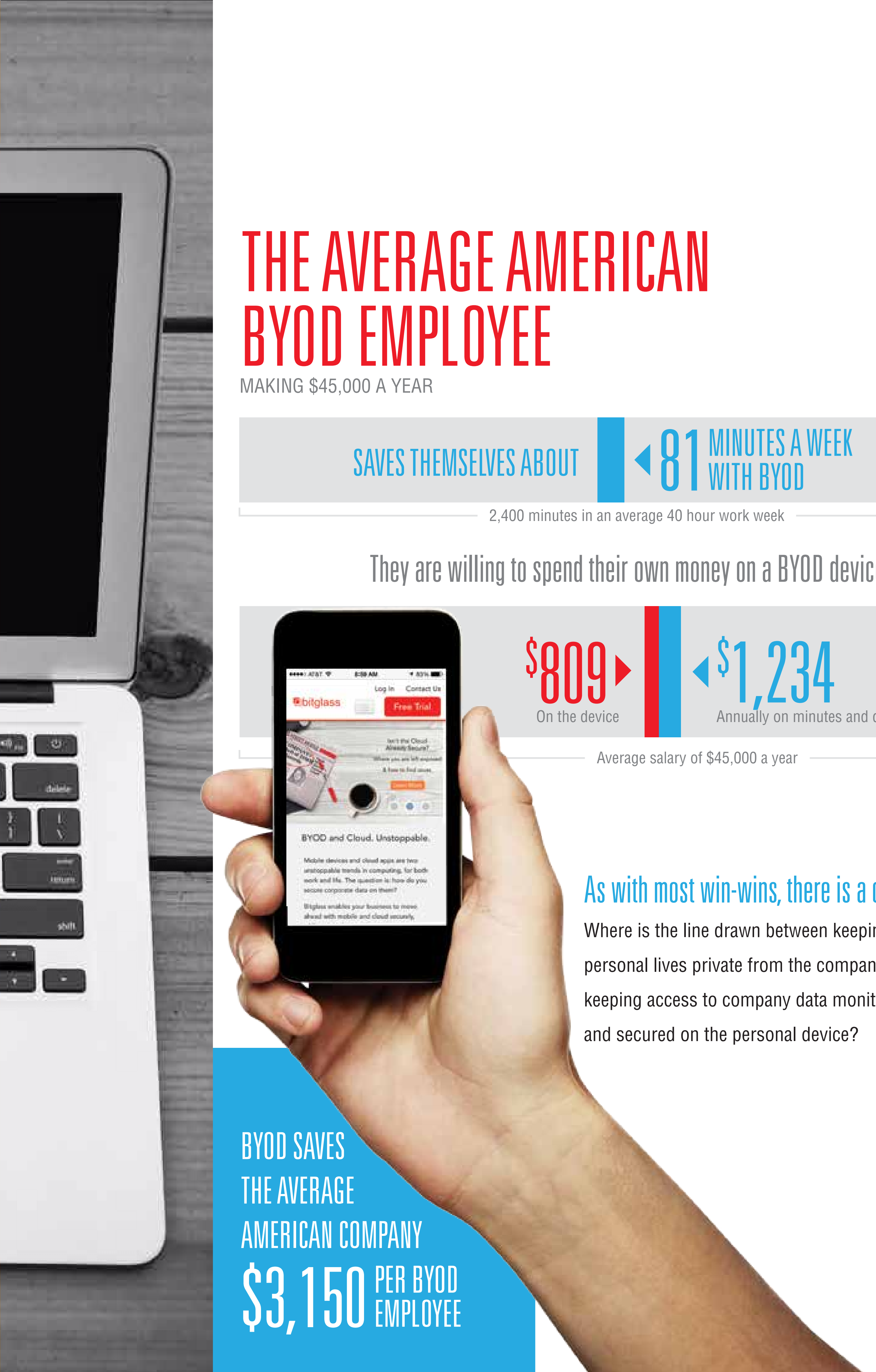
2,400 minutes in an average 40 hour work week

They are willing to spend their own money on a BYOD device

$809 On the device

$1,234 Annually on minutes and data plans

Average salary of $45,000 a year



BYOD and Cloud. Unstoppable.

Mobile devices and cloud apps are two unstoppable trends in computing, for both work and life. The question is: how do you secure corporate data on them?

Bitglass enables your business to move ahead with mobile and cloud securely.

As with most win-wins, there is a catch!

Where is the line drawn between keeping personal lives private from the company, and keeping access to company data monitored and secured on the personal device?

BYOD SAVES THE AVERAGE AMERICAN COMPANY $3,150 PER BYOD EMPLOYEE

STANDARD POLICIES

FOR THE MOBILE WORKFORCE

68% OF COMPANIES ALLOW BYOD

In 2014, aaccording to a recent report from InformationWeek.

41%

Require device management software on personal devices

45%

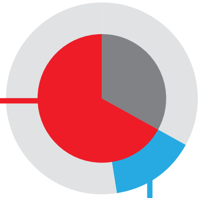
Use the honor code, asking users to “agree to rules”

55%

Include mobile in their security-awareness training

ROGUE TECHNOLOGY

67%



OF SMARTPHONE TOTING EMPLOYEES ADMIT TO ACCESSING COMPANY DATA ON PERSONAL PHONES

15.4% admitted to accessing company data without the IT department’s knowledge

ROGUE TEAM COMMUNICATIONS

22% sourced their own file sync and sharing apps

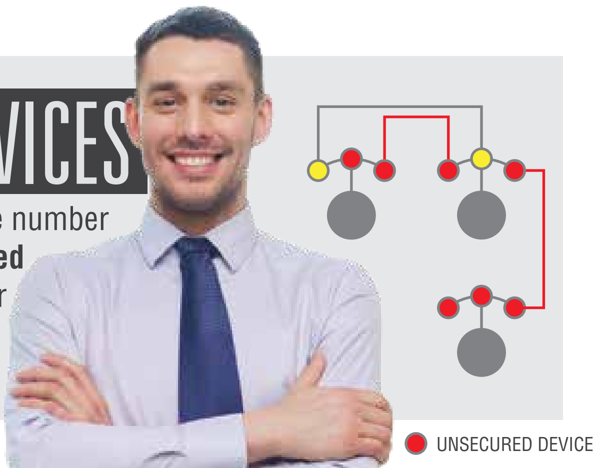
31% found their own IM/VoIP apps

26% found their own enterprise social networking apps

Sharing with potentially non-secured devices

3.3 DEVICES

the average number of **connected devices** per employee



Communications even between secured devices, are not secured because they are ‘rogue’

THIS ROGUE SPREAD

HAPPENS COMPLETELY OFF OF THE COMPANY RADAR

It’s important to note that **most “rogue employees” are not purposefully acting as spying saboteurs.** Most are driven employees, spending their own money on available technology– striving for higher productivity and company success.

Yet, after all of this unknown, unmonitored and unprotected access and communication of company secrets...

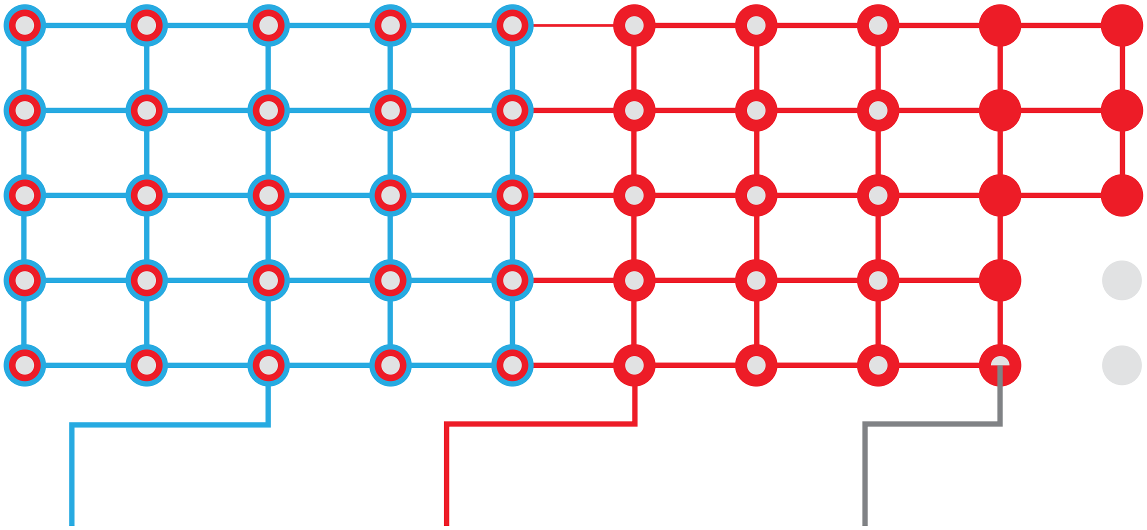
45% → OF COMPANIES REPORTED LOST OR STOLEN PHONES LAST YEAR WITH KNOWN ACCESS TO THEIR CORPORATE DATA.

Who knows how many had losses they didn’t know about.

WHAT HAPPENS TO LOST DEVICES?

An informative social experiment was done to see what people actually do after finding a phone.

50 unprotected phones were loaded with fake personal and corporate data, then left in random locations. Once these phones were found, the phone activity was monitored to see what happened, and the results were shocking!



50%

OF THOSE WHO FOUND A PHONE

ATTEMPTED TO RETURN IT TO THE OWNER.

96%

SEARCHED THROUGH THE PHONE

ACCESSING PRIVATE DATA & APPLICATIONS.

83%

OF THOSE WHO FOUND A PHONE

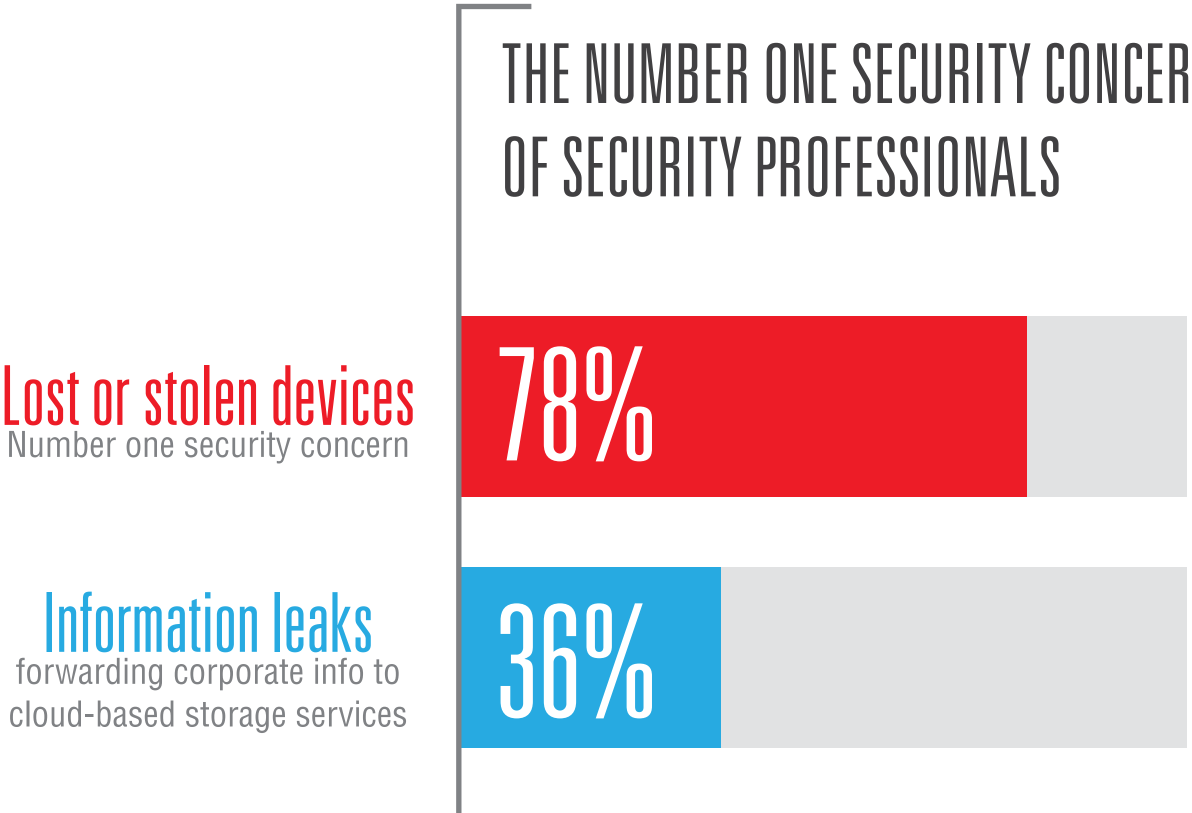
ACCESSED THE CORPORATE DATA ON THE PHONE.

THE DANGERS OF LEAKED COMPANY DATA

A COMPROMISED PHONE CAN REVEAL SECRETS, BUT WORSE YET, IT CAN ALLOW ACCESS TO SYSTEMS

The costs from lost trust, reputation mitigation, and physically fixing IT breaches from just one lost device, can threaten the future of an entire business.

THE NUMBER ONE SECURITY CONCERN OF SECURITY PROFESSIONALS



BEST PRACTICES FOR A MOBILE BYOD WORKFORCE

An informative social experiment was done to see - what people actually do after finding a phone.

Step 1 - **Accept the fact that employees are going to bring in their own devices,** access and share company data, and inevitably lose their unprotected devices. You can't stop them, don't try.

Step 2 - **Educate employees about the threats of mobile security** and the devastating potential that seemingly harmless acts of sharing company data or losing sensitive phones has on the company.

Step 3 - **Establish employee trust** by informing the employee that they don't have to worry about any of this, because company data is protected

Step 4 - **Employ technology that protects corporate data on personally owned devices** without violating employee privacy, slowing employees down or forcing draconian policies on their devices. Focus on the ability to track, control, and wipe corporate data from personal mobile devices.

WHY BITGLASS?

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they were developed to secure the corporate network perimeter. Bitglass delivers innovative technologies that transcend the network perimeter to deliver total data protection for the enterprise - in the cloud, on mobile devices and anywhere on the Internet.

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Bitglass is based in Silicon Valley and backed by venture capital from NEA and Norwest.

REGAIN CONTROL WITH BITGLASS

For IT: Secure cloud and mobile

For Employees: Privacy and unencumbered mobility

Learn more at: **Bitglass.com**

bitglass