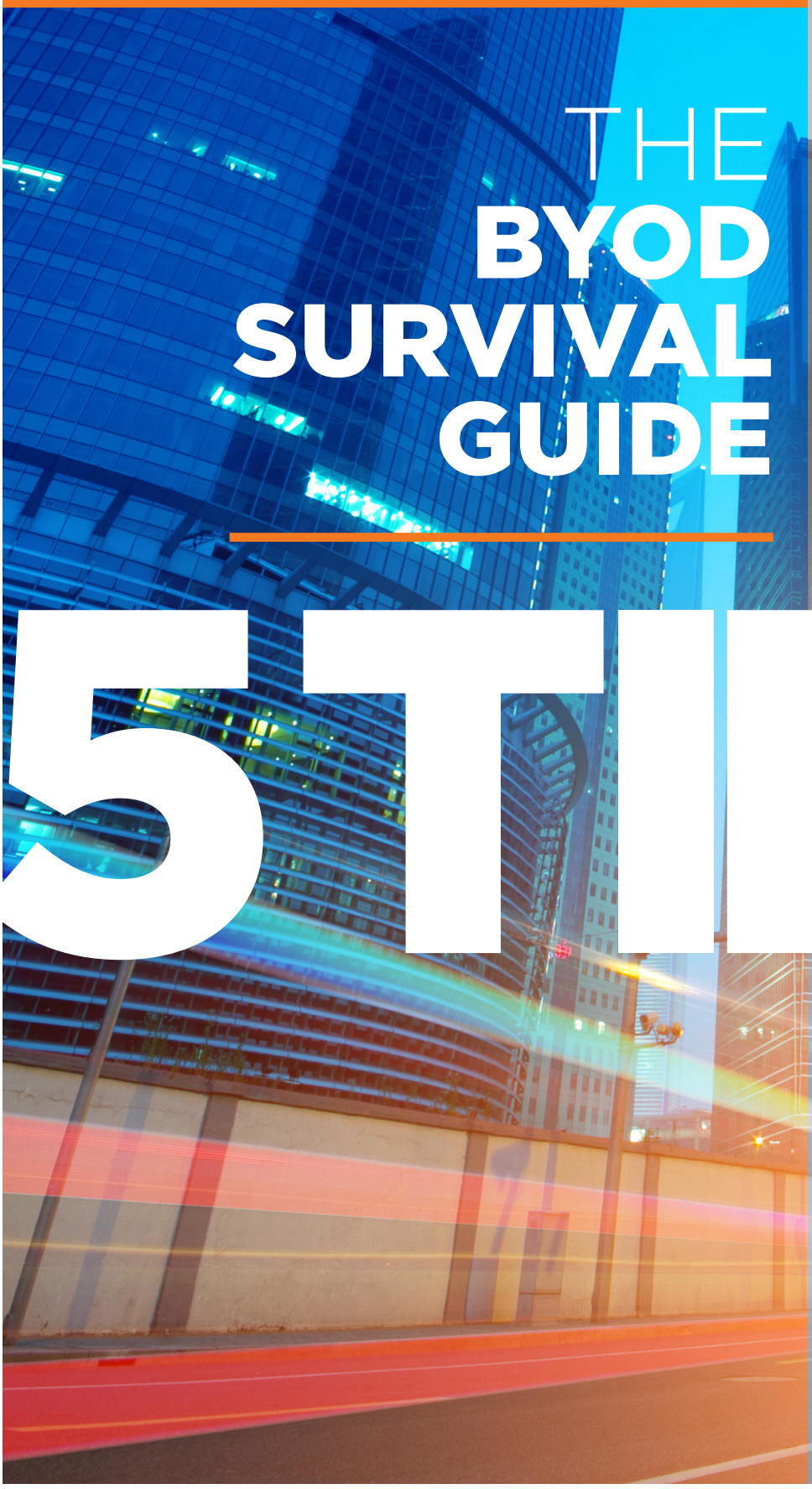
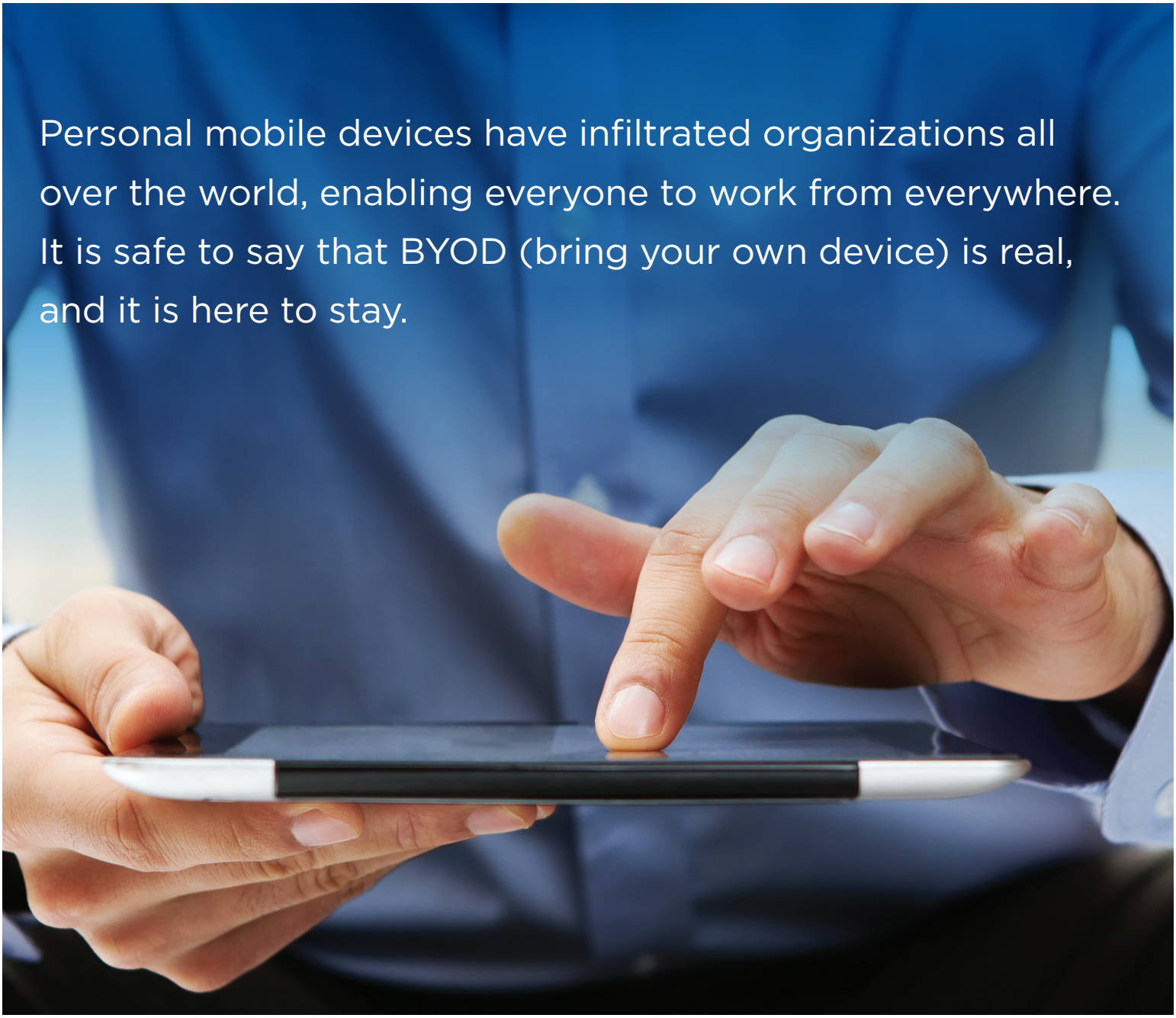
Acronis®

THE BYOD SURVIVAL GUIDE

5 TIPS

FOR PRACTICING SAFE MOBILE FILE ACCESS AND COLLABORATION





THE BYOD ACHILLES HEEL:

SECURITY BREACHES, LEAKS AND ATTACKS

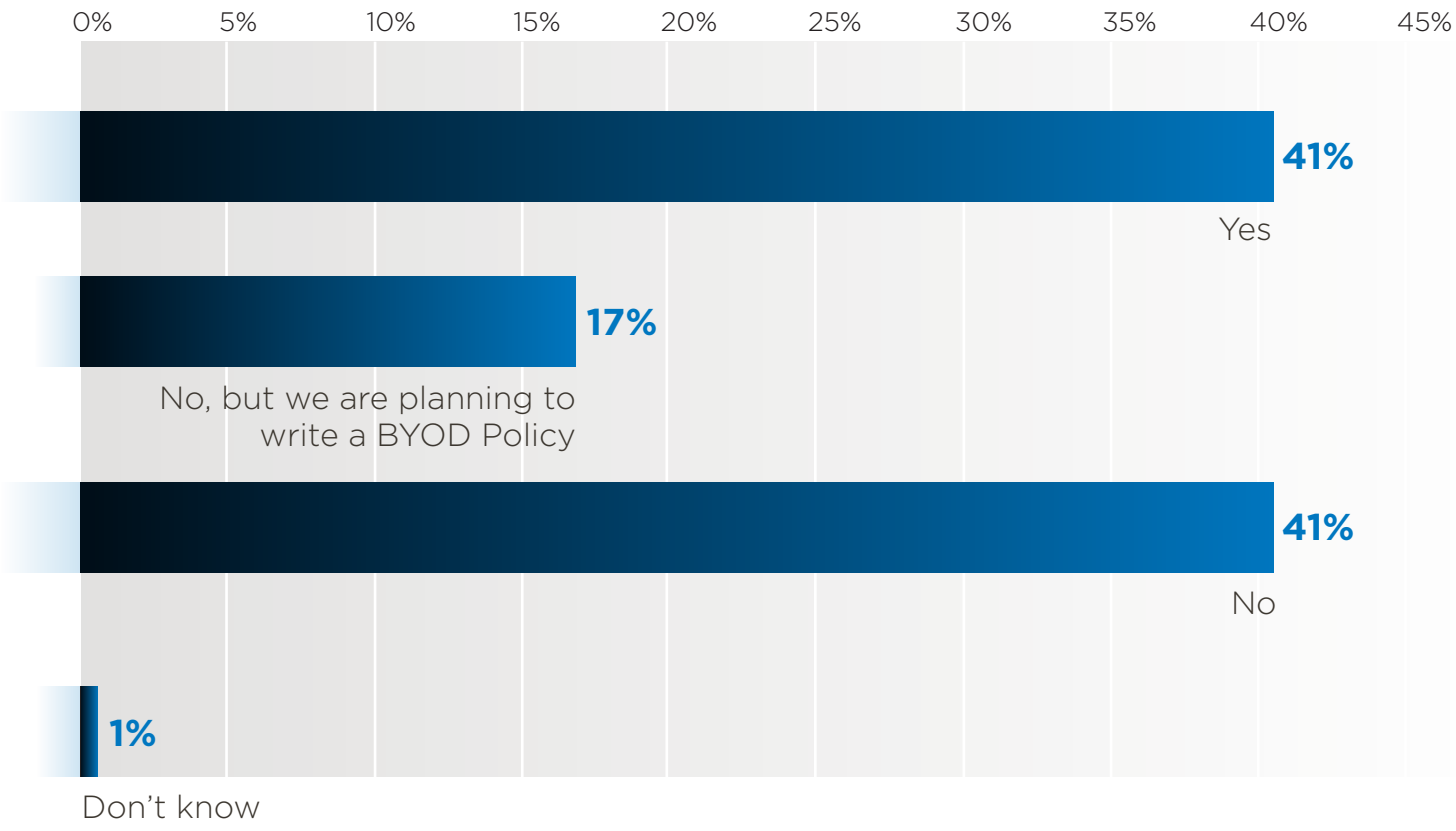
The flip-side to BYOD is data protection, and ensuring that as employees bring devices to-and-from the workplace, confidential corporate data is adequately protected while remaining easily accessible. An important component of data protection, often not addressed by BYOD strategies, includes ensuring that information and records comply with privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX), as well as specific industry and regional privacy regulations.

Source: Acronis 2013 Data Protection Trends Research

FACT:

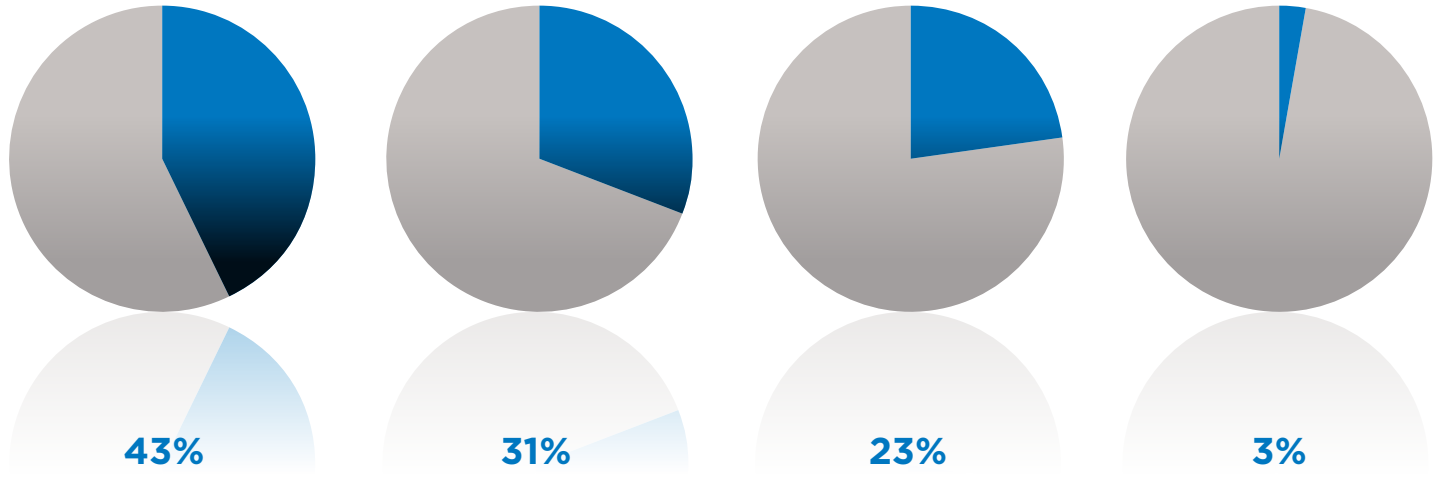
By 2017 Gartner predicts that half of all companies will actually *require* employees to use their own mobile devices for work.

DOES YOUR ORGANIZATION HAVE A POLICY THAT SPECIFIES HOW EMPLOYEES MAY USE THEIR OWN DEVICES IN THE WORKPLACE?



58 % of businesses do not have a mobile device policy in place.

IF YES, **WHAT DOES THE BYOD POLICY REQUIRE?**



43%

Only company-sanctioned personal devices are allowed to access the organization's networks

31%

It strictly forbids the use of any personally-owned device to access the organization's networks

23%

All personally ownded devices are allowed to access the organization's networks

3%

Other

On the other end of the spectrum, **31% of businesses strictly forbid the use of personally-owned devices to access corporate networks.** This is not realistically sustainable, and will force employees to work around corporate policies and rules. Not good.

THE BYOD SURVIVAL GUIDE

5 TIPS TO PRACTICE SAFE BYOD IN YOUR ORGANIZATION

5 TIPS

SURVIVAL TIP 1

CREATE A MOBILE DEVICE SECURITY POLICY

Creating a mobile device security policy doesn't have to be complicated, but it needs to encompass devices, data and files. There are a number of simple things you can do, like require users to key-lock their devices with password protection. Surprisingly, only **31% of businesses are enforcing this. 68 % use VPN or secure gateway connections across networks and systems, and 52 % use Active Directory and/or LDAP**. The simplest place to start is to use device key-lock and password protection. Whether you opt for VPN security, key locks, Active Directory Monitoring or endpoint security, the choice is yours. But it is time to make a policy — and stand by it.

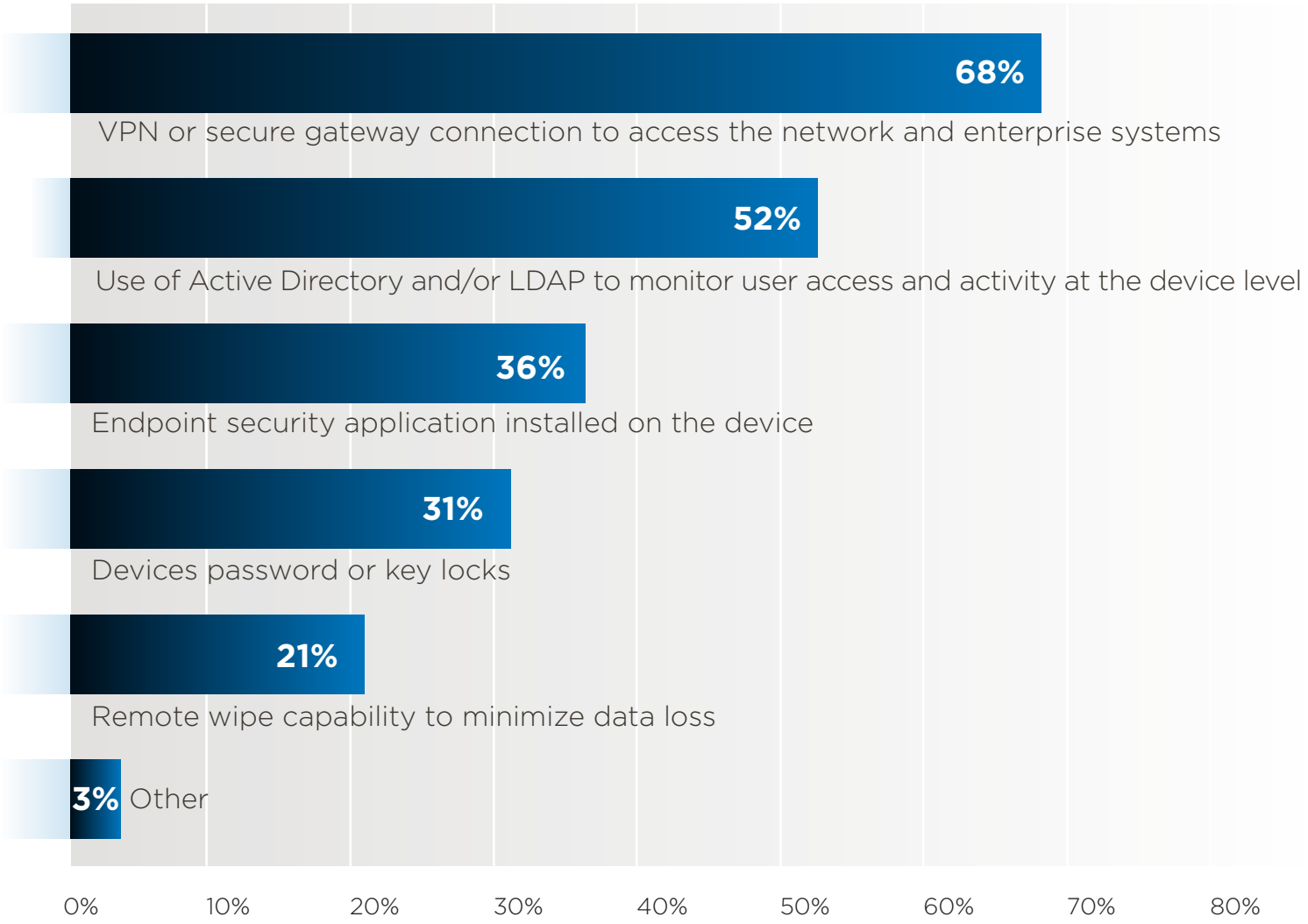
Part of creating and enforcing an effective mobile device security policy is accounting for personally-owned devices entering and leaving the workplace, a movement called take-your-own-device (TYOD). If not properly managed through processes like remote wipe, TYOD could cause major data leakage. **Only 21% of businesses perform remote device wipe** when employees leave the organization.

BONUS TIP:

INCLUDE REMOTE WIPE IN YOUR POLICY.

IF PERSONALLY-OWNED DEVICES ARE ALLOWED IN THE WORKPLACE, **HOW IS BYOD SECURITY ENFORCED?**

More than one response permitted

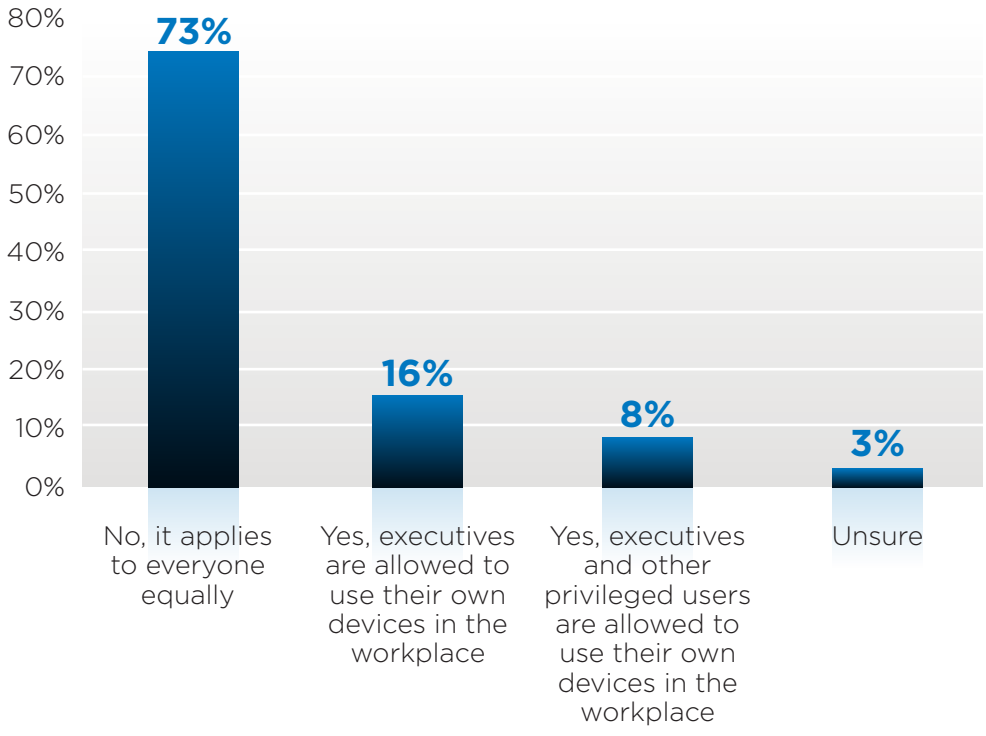


SURVIVAL TIP 2

STOP MAKING EXCEPTIONS TO YOUR POLICY

We all know that rules are not meant to be broken; so why aren't businesses taking their own mobile device policies seriously? **41% do have a BYOD policy in place.** Kudos to them. But nearly **25% make exceptions to policy rules.** Worse, these exceptions apply to executives. Get it? Those with access to presumably the most sensitive data in the organization are allowed to break the rules. Does your CEO know that his tablet could crush his business?

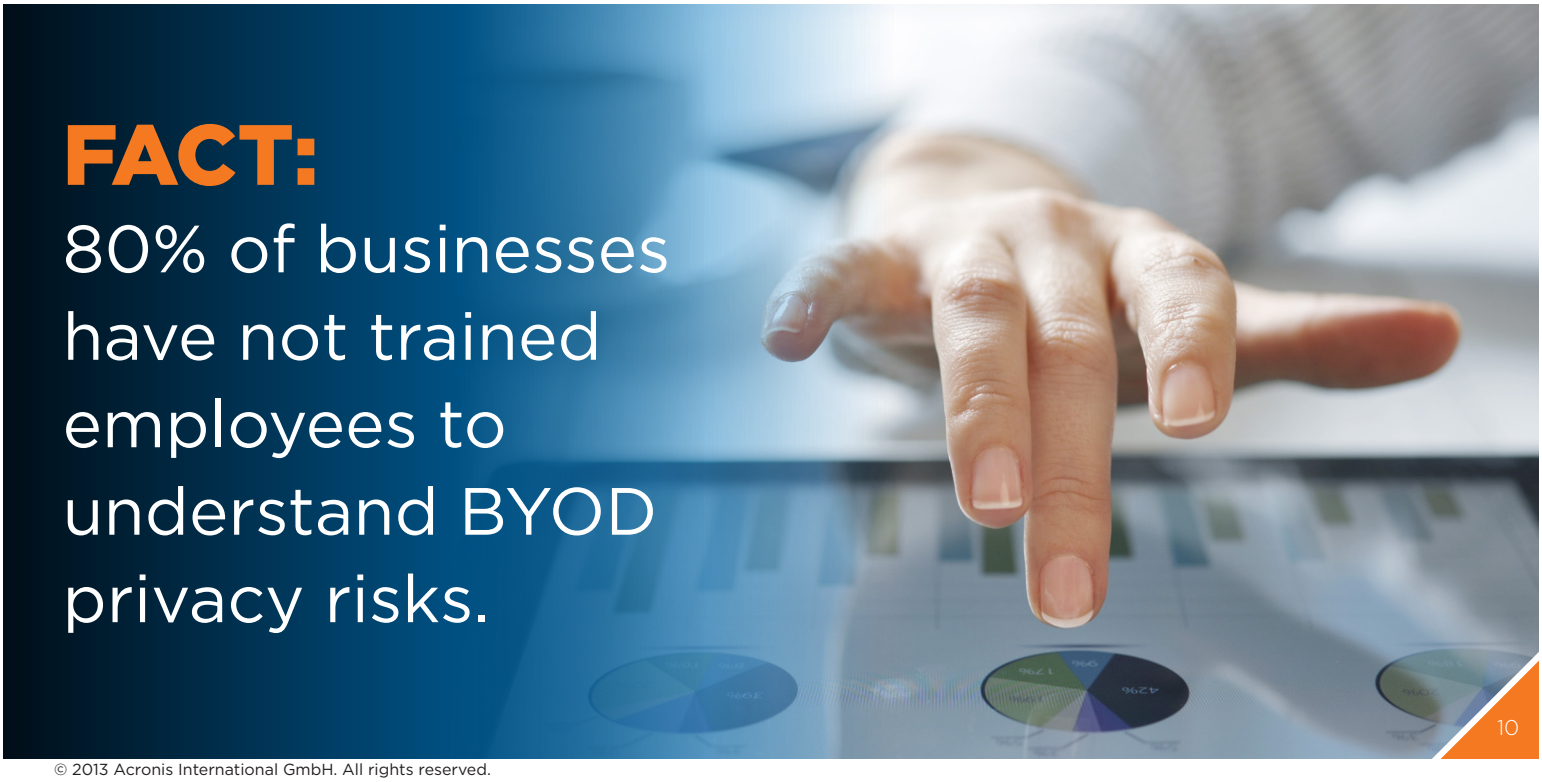
ARE THERE EXCEPTIONS TO THE BYOD POLICY?



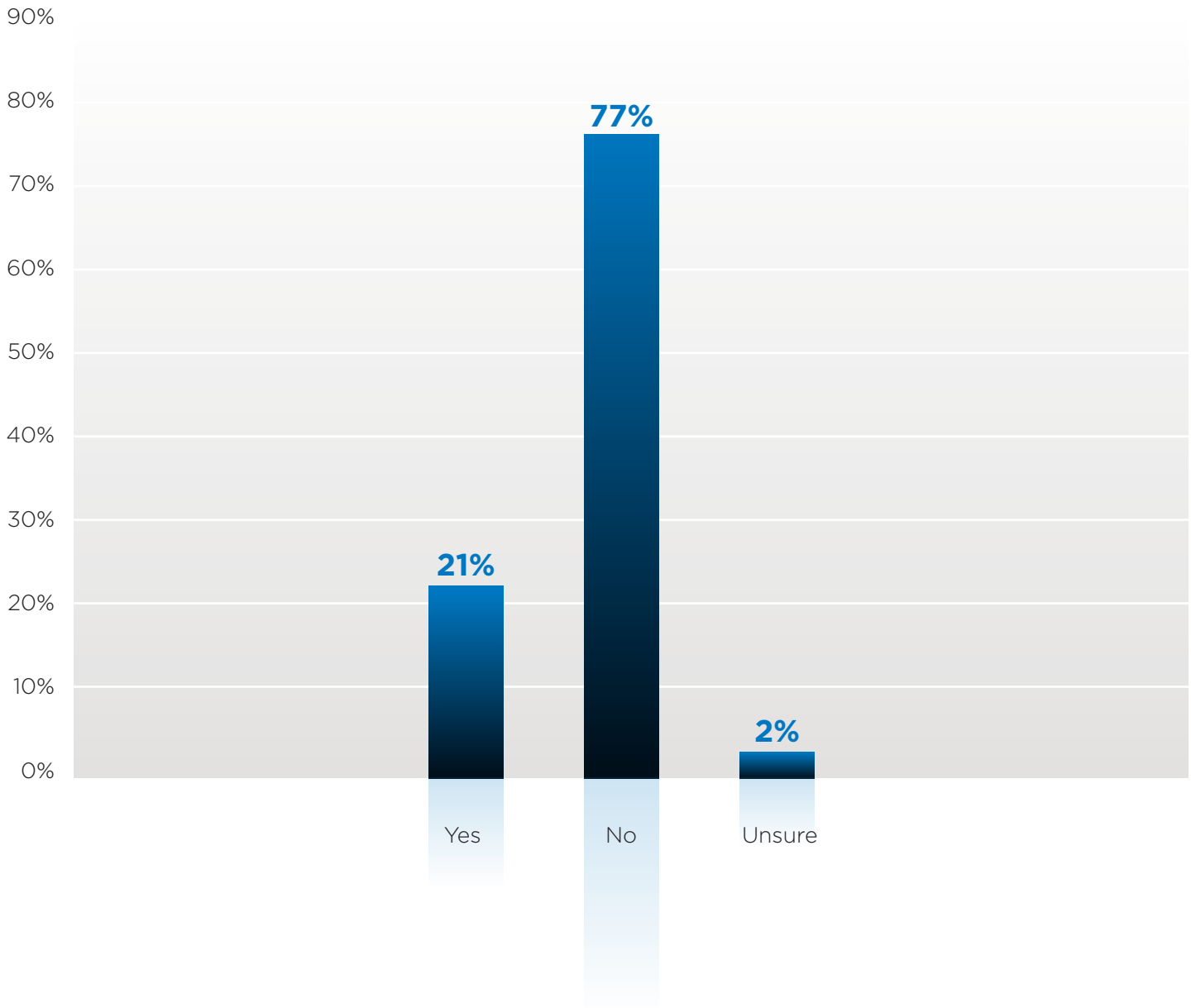
SURVIVAL TIP 3

MAKE "SAFE BYOD" EVERYONE'S RESPONSIBILITY

Let's go back to the BYOD spectrum for a minute. Some of you allow employees to bring smartphones, tablets and even their own Macs into the office. You know this improves productivity and increases collaboration and sharing. Then there are those of you who are on complete BYOD lockdown. Either way, a little bit of education can go a long way. If employees understand the privacy risks involved with BYOD, maybe your data could be a little bit safer — and maybe you would feel more comfortable loosening the reigns.



HAS YOUR ORGANIZATION TRAINED EMPLOYEES TO UNDERSTAND BYOD PRIVACY RISKS?



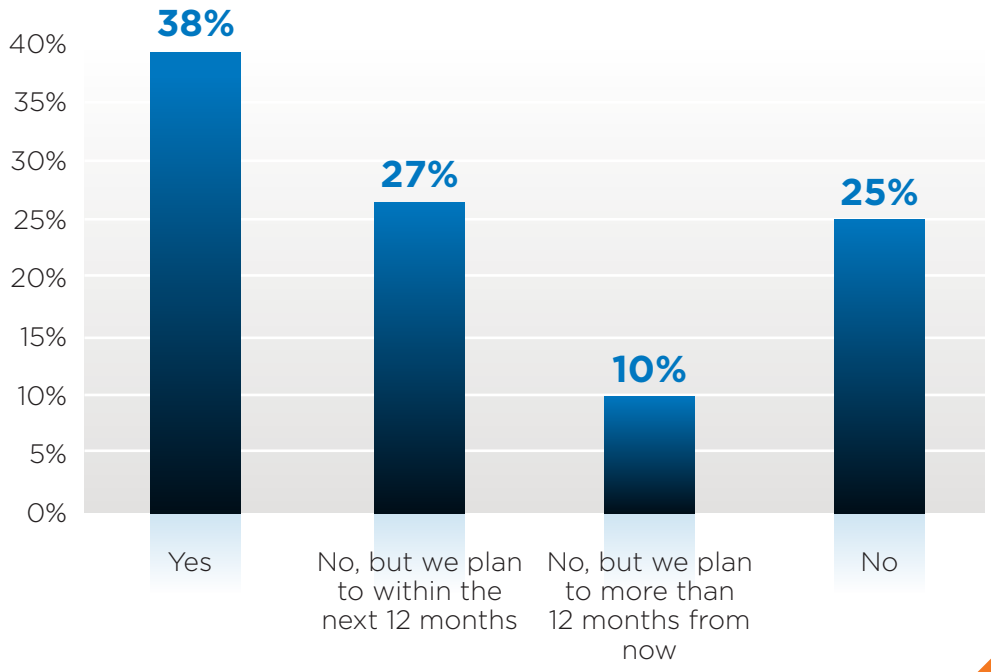
SURVIVAL TIP 4

PREPARE FOR THE COMING OF APPLE®

65% OF BUSINESSES WILL SUPPORT MACS IN THE NEXT 10 MONTHS AND 75% IN THE NEXT TWO YEARS.

Nowadays, people rarely leave home without their iPhone and iPad — some even with their Mac laptop. This means Apple devices are inundating the workplace: You can run from Apple integration, but you definitely cannot hide. If you fall off the bandwagon — or never get on it in the first place — you run the risk of driving away a desirable pool of employees, not to mention, you could miss out on exciting new technology and applications. The **57% of businesses that state compatibility and interoperability issues** as roadblocks to Apple integration no longer have a valid argument — there are solutions out there to help solve these challenges.

DOES YOUR ORGANIZATION SUPPORT APPLE IN ADDITION TO WINDOWS OR LINUX?

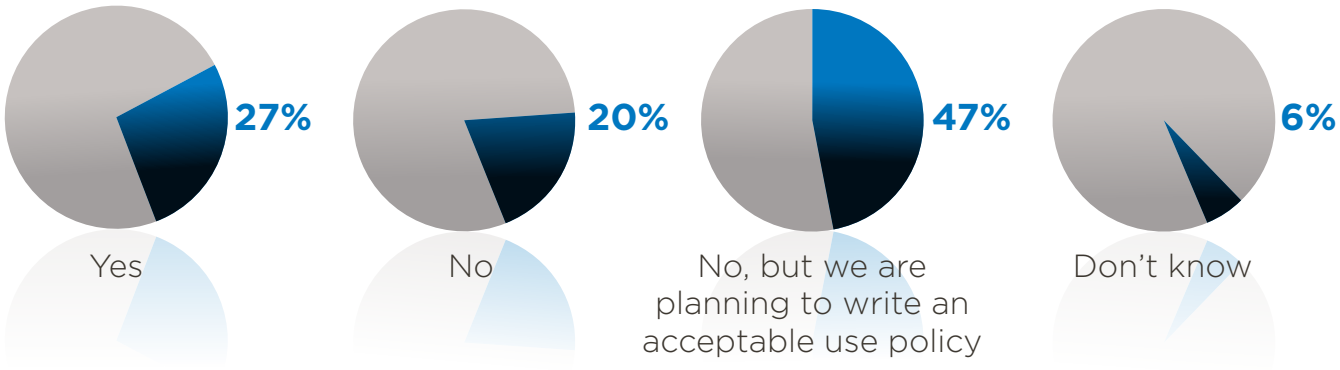


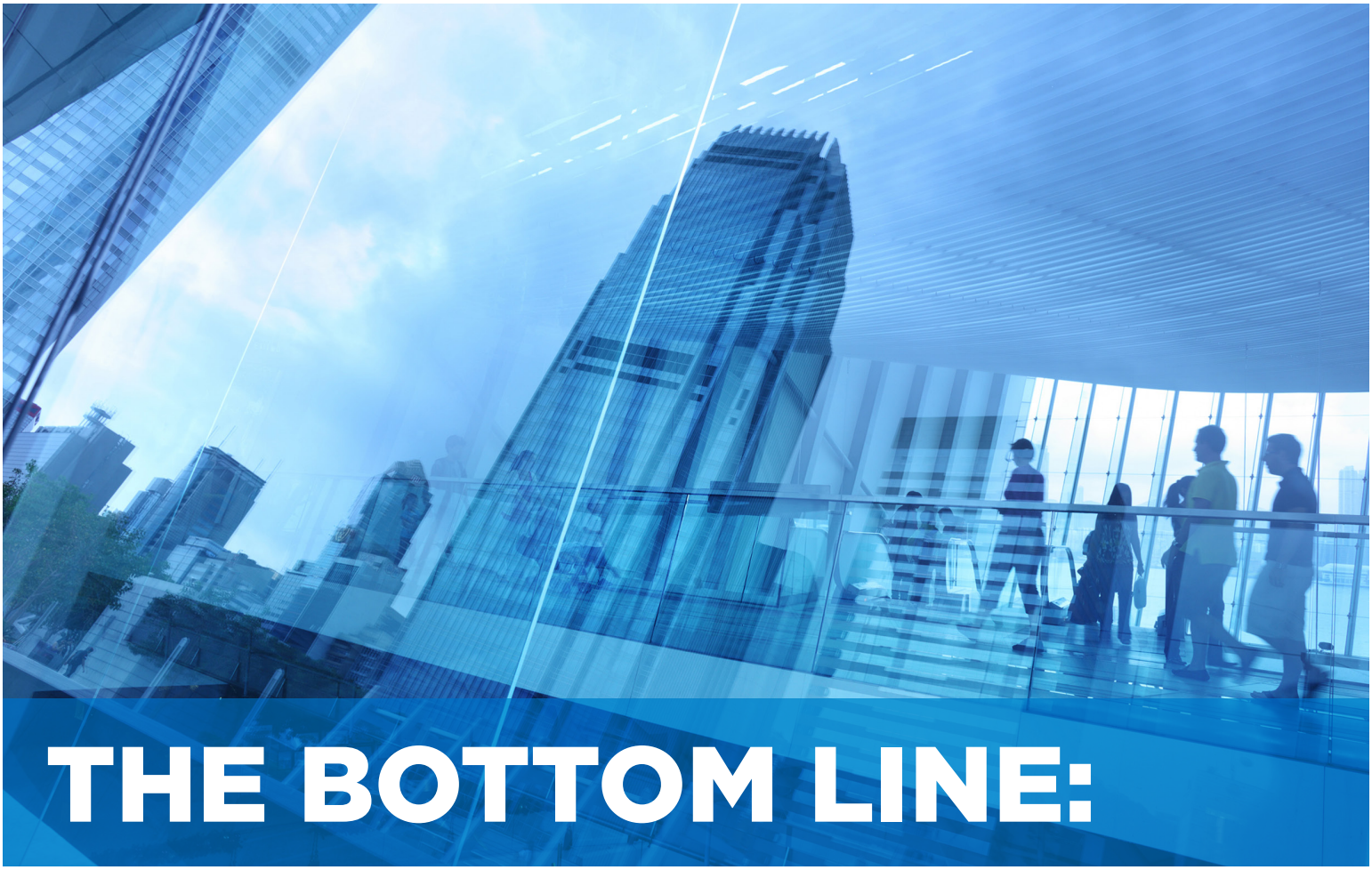
SURVIVAL TIP 5

DON'T UNDERESTIMATE THE DANGERS OF PUBLIC CLOUDS

When it comes to data protection, you have to worry about more than just devices. Everyone, at some point, has been guilty of saving corporate presentations or other files and documents in free public clouds, like Dropbox and Google Drive. It's convenient instant access, right? True, but public clouds are not secure, and leave data constantly vulnerable in the digital ether. Plus, public cloud application environments are often incompatible, causing business processes to become disjointed, and employee productivity to slow down. IT departments are well aware of the threats associated with using public cloud environments, so why aren't they mandating policies around bring-your-own-cloud (BYOC)? **67% of businesses do not have a policy in place that specifies sharing corporate files in a public cloud.**

DOES YOUR ORGANIZATION HAVE A POLICY THAT SPECIFIES PERMISSION TO **SHARE BUSINESS FILES IN A PUBLIC CLOUD ENVIRONMENT?**





THE BOTTOM LINE:

It is time to stop sugar coating (or ignoring) the risks and challenges that accompany BYOD bliss. Decide which end of the spectrum you fall on, and find a solution that enables secure mobile file access and management, and Apple integration. No more excuses. You are now equipped with tips to start practicing safe BYOD and ensuring adequate data protection across the many devices that pass through your organization.

JUMPSTART YOUR SURVIVAL WITH **ACRONIS:**

- Test drive: Acronis® mobilEcho®
- Test drive: Acronis® ExtremeZ-IP®
- Test drive: Acronis® activEcho™
- Test drive: Acronis Backup & Recovery® for Mac

Source: Acronis 2013 Data Protection Trends Research

Acronis®

300 TradeCenter, Suite 6700 | Woburn, MA 01801 | USA

+1 781 782-9000 | info@acronis.com | www.acronis.com