CTRL-Z

WHO WE SURVEYED

800
IT Decision Makers, including CIOs and CISOs

400
Business Decision Makers, including CEOs

USA
UK
Germany

CTRL-Z

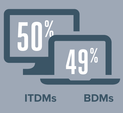
CTRL-Z is a globally recognised means of saying "undo." It is an instinctive action when we make a mistake — and a metaphor for security, control and agility.

83%
of ITDMs have wished they had an undo button to erase a security breach.

79%
of BDMs have wished they had an undo button to remove all traces of of an IT mistake they've made.

YOU NEED TO SPOT RISK SOONER

According to ITDMs and BDMs, **almost half of all corporate data** is held on endpoint devices.



At the same time, **75% of CEOs** and **52% of BDMs** admit that they use unauthorized applications/ programs.

91% of CEOs and **83% of BDMs** believe their actions could be considered a security risk to their organization.

It will be up to CIO/CISOs to help their businesses adapt to the realities of the new threatscape in 2017, say 66% of BDMs and 65% of ITDMs. The question is, if not the CIO or CISO, then who should take leadership on this front?

THE ENTERPRISE MUST BE ABLE TO ALWAYS BOUNCE BACK

say losing all the data at the endpoint could destroy their business.

At the same time, the threat landscape is ever-expanding and increasingly focused on the enterprise. Many enterprises admit to suffering a breach in the last 18 months:

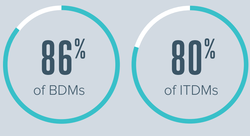
51% of BDMs **45%** of ITDMs admit their companies have suffered a recent breach.

It's not if your business will experience a breach, it's when. Are you capable of a rapid response to reverse the potentially business-destroying consequences of a

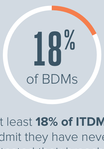
significant data loss?

PRODUCTIVITY IS DIRECTLY LINKED TO THE ENTERPRISE'S ABILITY TO MOVE FORWARD FASTER

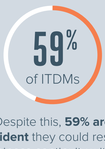
Commitment to backup isn't in question.
It is whether you can get back what you lost that matters.



do have a breach recovery plan in place.



At least **18% of ITDMs** admit they have never tested their breach recovery plans.



Despite this, **59% are confident** they could restore business continuity within 24 hours, but can they?

Ultimately, 88% of enterprise ITDMs and 83% of BDMs believe that their companies will have to improve their breach recovery ability in the next 12 months!

In the modern data-driven economy, security and productivity are intrinsically linked.

Recovery — and not prevention — is the way forward.

Code42 is your CTRL-Z!