IT Confidential

The State of Security Confidence

ABSOLUTE™

PREFACE

01

OBJECTIVE

Obtain insight into the attitudes, behavior, and confidence levels of IT decision makers when it comes their organization's security

02

KEY FINDINGS

- IT believes the biggest threat is the insider threat
- The gatekeepers are also the gatecrashers, with IT admitting to risky and non-compliant behavior
- Most IT decision-makers believe they will lose their jobs due to a security breach

03

METHODOLOGY

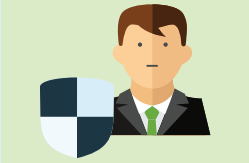
A survey was conducted through the Vision Critical Springboard America online panel. There were a total of 501 US respondents who met the following criteria:

- Work for a company with 50 employees or more
- Work in an IT / information security role and hold one of the following positions: IT Director/Executive, IT Manager, IT Administrator, IT Security (dedicated primarily to security), or Other IT / information security management role.

Any discrepancies in totals are due to rounding.

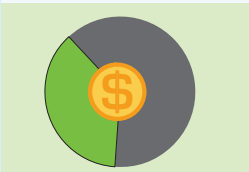
CONFIDENT or Complacent?!

IT says....

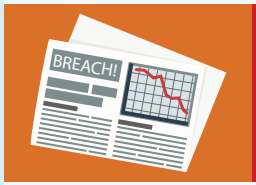


97% security is a top priority for executive team

87% expect increased investment in 2016

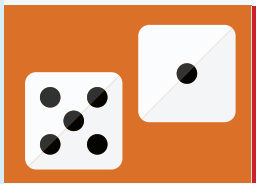


37% of IT budget spent on security



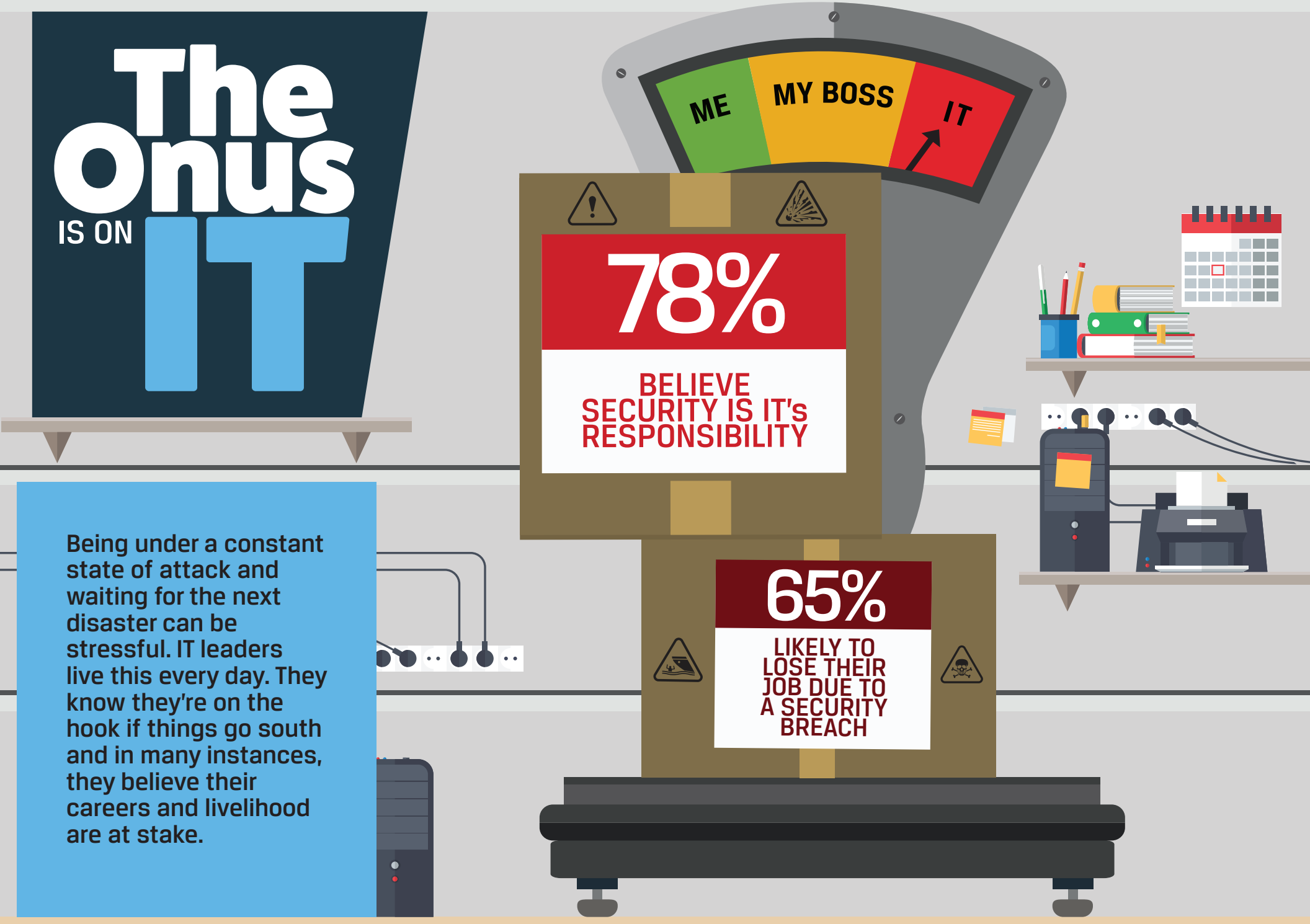
38% suffered data breach within last year

33% of security protocols not being followed



20% do not have security breach response plan in place

The Onus IS ON IT



Being under a constant state of attack and waiting for the next disaster can be stressful. IT leaders live this every day. They know they're on the hook if things go south and in many instances, they believe their careers and livelihood are at stake.

Where IT Sees SECURITY THREATS

Threats come in all shapes and sizes. For IT, they believe their biggest asset is also their biggest risk with insiders or employees topping the list.

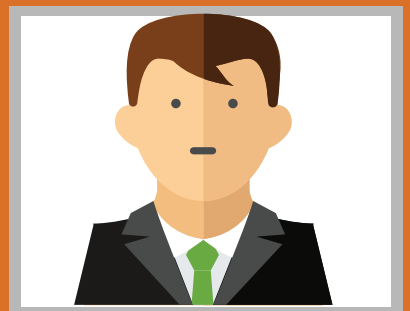
46%

EMPLOYEES

38%

HACKERS

11%



COMPETITORS

5%

PARTNERS

BAD HABITS – IT Exposed

45%

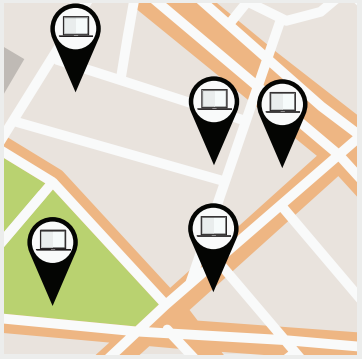
KNOWINGLY CIRCUMVENTED ORGANIZATIONAL SECURITY POLICIES

33%

HAVE SUCCESSFULLY HACKED THEIR OWN OR ANOTHER ORGANIZATION

As security gatekeepers, IT is held to a higher standard of behavior. Surprisingly, they can also be contributors to non-compliant behavior.

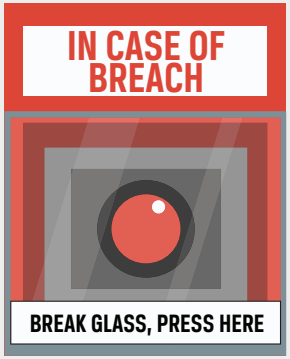
SIZE MATTERS



38%

› 500 EMPLOYEES

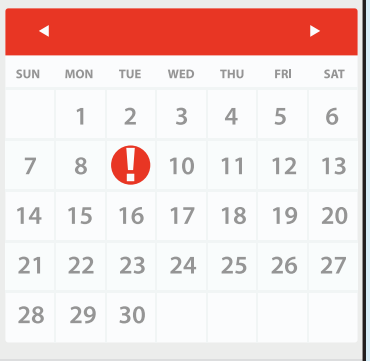
Larger orgs have more staff working outside the local corporate network



75%

50 - 499 EMPLOYEES

Smaller orgs had fewer security breach response plans in place vs large orgs at 83%



41%

› 500 EMPLOYEES

Larger orgs suffered more security breaches in the last year

40%

50 - 499 EMPLOYEES

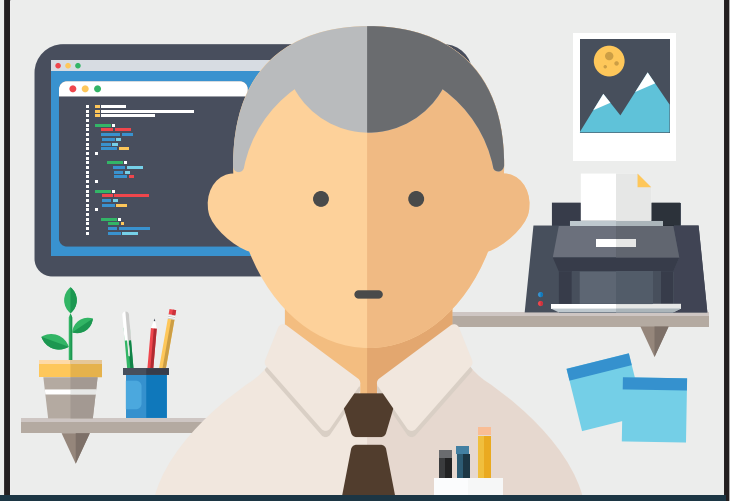
The biggest impact to larger orgs after a data breach is brand reputation damage

35%

› 500 EMPLOYEES

The biggest impact to smaller orgs after a data breach is monetary loss from litigation

NEW Vs. EXPERIENCED



IT decision makers between the ages of 18-44 demonstrate a much more cavalier attitude toward IT security.

IT DECISION MAKERS	AGE 18-44	AGE 45+
Yes, I have hacked my own or another organization	41%	12%
Yes, we are sufficiently staffed to provide effective IT security	89%	75%
Percentage of security protocols NOT being followed	38%	25%
Yes, I am confident our organization can contain a breach	92%	79%

KEY TAKEAWAYS

01

ADAPTIVE SECURITY PROTOCOL

- Collect reliable data so you can determine the context of a security incident
- Select from a range of security commands so you can respond appropriately based on the severity of the incident and the data that's at risk

02

ADDRESS INSIDER THREATS

- Identify behavior and activities that could be precursors to a security incident
- Educate staff on potential threats and develop a formal security breach response plan
- Monitor for non-compliant activity and remotely secure devices that may be at risk

03

DEEPER VISIBILITY

- Maintain persistent oversight across all of your devices and the data they contain - regardless of user or location
- Apply a layered approach including encryption, anti-malware, and endpoint security. Set up proactive alerts so you will know when a layer fails and use remote security capabilities to respond immediately

ABSOLUTE™

CONFIDENT TO THE CORE