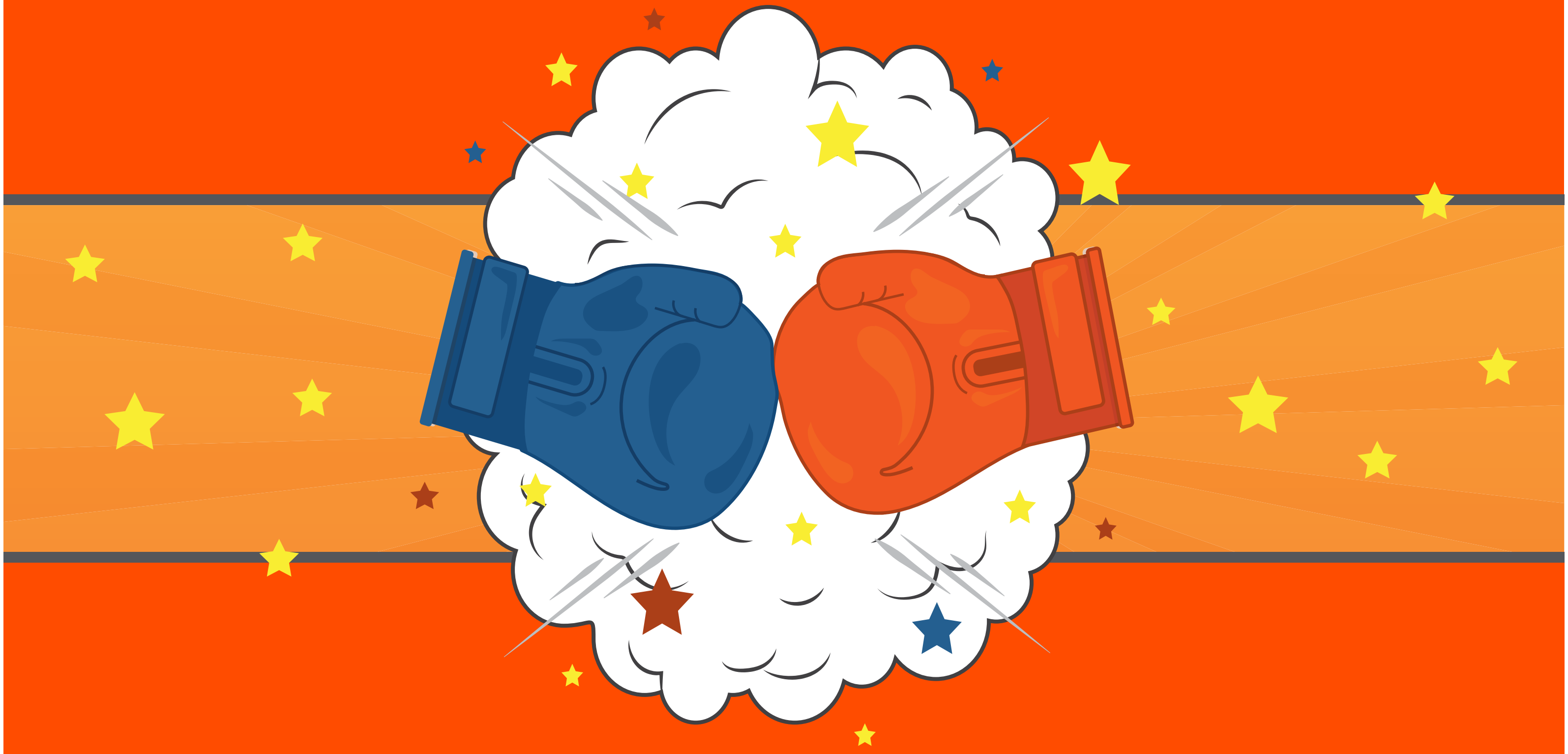
SPICEWORKS
Where IT goes to work.™

Free IT reports on today's hottest tech topics and trends.

December 2015 | #ITSecurity

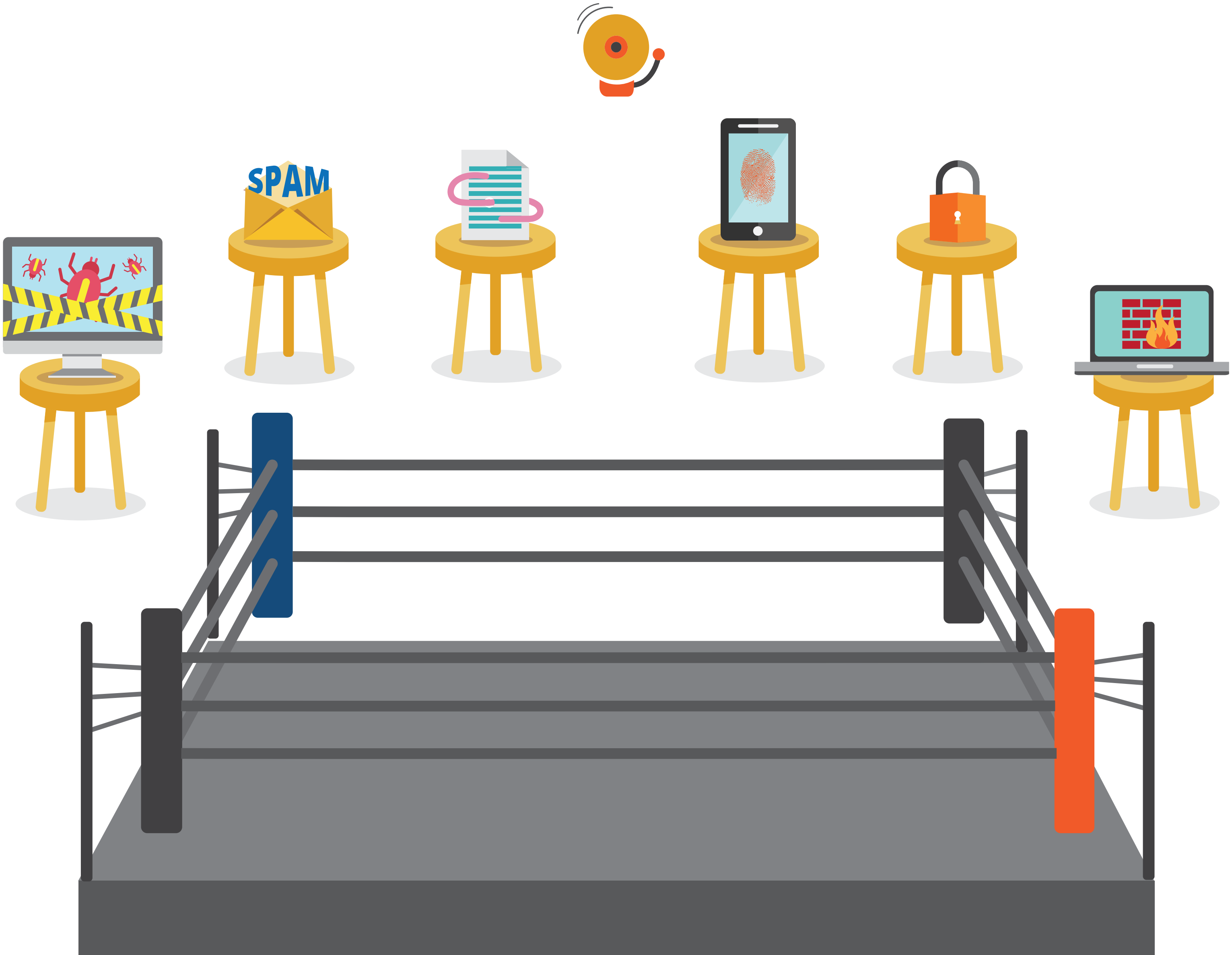
Battling the Big Hack:

Inside the ring and out… IT pros plan to land some blows in 2016.



BIG HACK
IT PRO

TABLE OF CONTENTS



00

Fighting the Good Fight

INTRODUCTION

Will 2016 be the year IT fights back against “the big hack”? It’s looking that way, according to a recent Spiceworks survey on security. IT pros reveal they’re well aware of security risks coming in from myriad sources, and they’re taking them seriously. We’re covering everything from challenges and perceived risks to IT pro thoughts on shadow IT, current security methods, and expected security changes in the coming year.

SURVEY INFORMATION

We asked almost 200 IT pros in North America and EMEA to tell us about their real-world experiences with security threats and breaches. They let us know what—and who—they think is a threat, what actions they're taking in response, and who they believe is ultimately responsible for protecting their organizations.

They also told us about some of the challenges their organizations face, with a clear focus on the way end users fit into—and often complicate—the picture. Will their organizations be more, or less secure in 2016? How will their security investments shift in the next year? Here's the play-by-play:

HIGHLIGHT REEL

1. *Top security challenges are related to end users.* More specifically, IT pros are worried about the vulnerabilities created when employees don't understand or aren't invested in avoiding risky behavior around company data.

2. *They're muscling up security measures.* IT pros expect to increase security in 2016, with plans to implement even some of the newer security solutions such as intrusion detection, penetration testing, and advanced threat protection.

3. *IT pros believe their role is key in maintaining security.* According to our survey respondents, it takes the entire organization—not just the latest technology—to keep data and people safe. That said, they ultimately feel that the responsibility for their organization's security is in the hands of IT.

Is your organization ready to sting like a bee against a growing and evolving field of security threats? Are you up against the ropes, relying only on antivirus software and "security through obscurity"—or are you taking advantage of more advanced technologies? Do employees just want to ignore the issue, or are they actively involved in security?

Read on for a closer look at which security measures IT pros around the world are implementing and how they're working with fellow employees to keep company data safe. You'll also hear from respondents in their own words throughout this report.

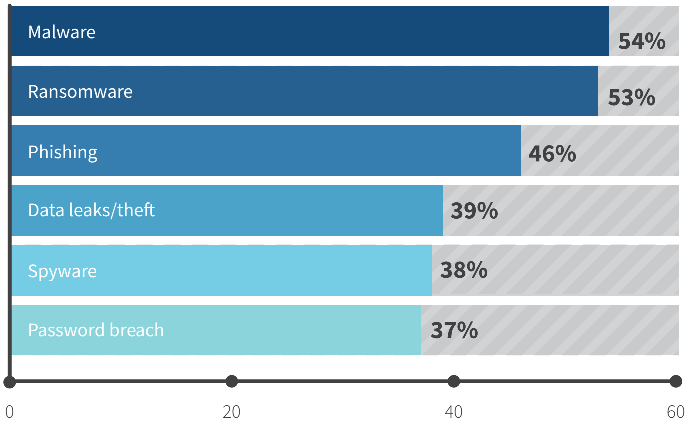
01

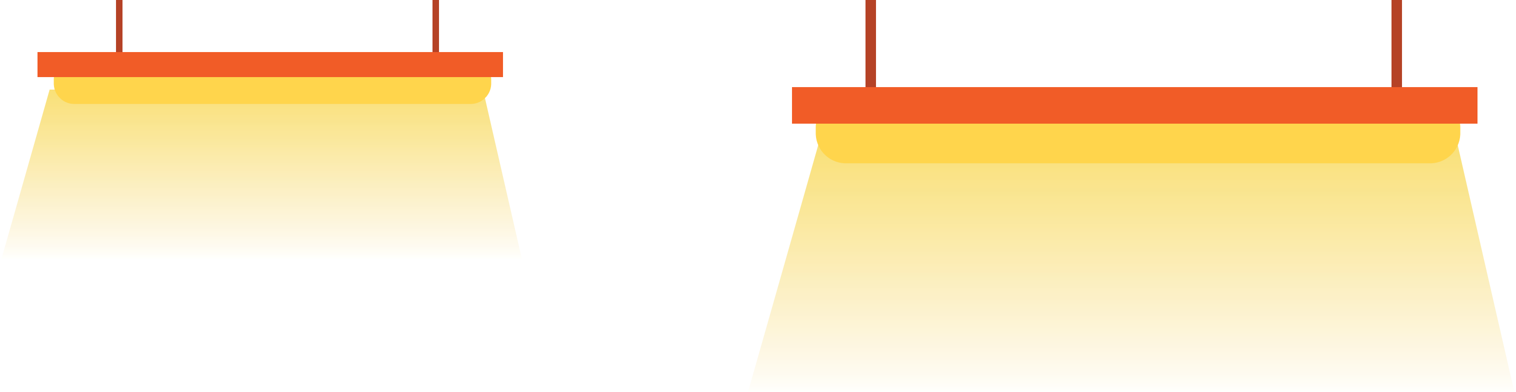
Perceived vs. Actual Security Threats

So what security threats weigh on the minds of IT pros? With so many potential security risks in (and out) of the ring, which ones managed to get some solid jabs in? Almost 55% indicated concern about malware, but ransomware and phishing also packed a punch.

Top concerns regarding threats/breaches in 2016

(Percentage of IT pros who selected "very" or "extremely" concerned)



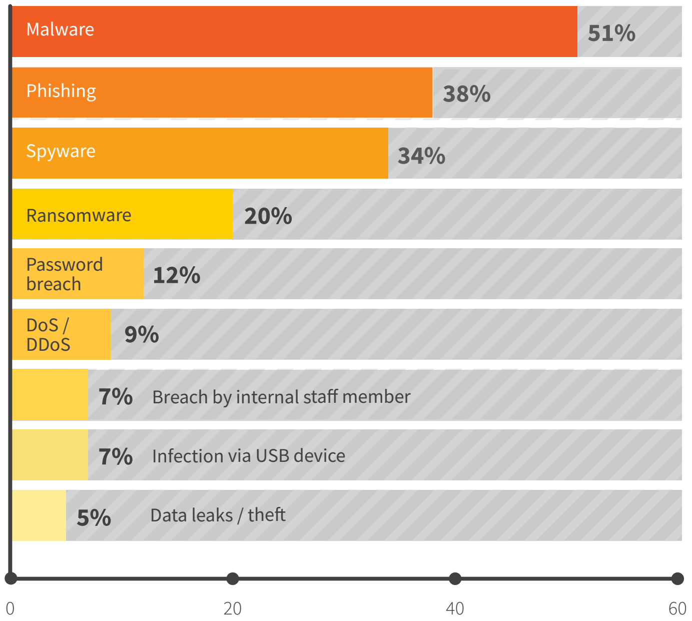


How do these concerns align with threats/breaches organizations have actually experienced in 2015? Just over half of respondents mentioned a malware attack (51%), which tracks pretty closely to the perceived threat (54%). Phishing (38%) and spyware (34%) are next on the list, followed by ransomware (20%). Less common incidents included password breaches, DoS/DDoS attacks, breaches by internal staff or via USB, theft, and leaks.

Only 18% experienced no threats or attacks of any kind. There's a slight disconnect between what keeps IT pros scanning the horizon and what has actually materialized. For instance, more than half have concerns about ransomware attacks in 2016, but only 20% were actually struck with one this year. Their fear of password breaches next year also trended much higher than the actual experience (37% vs. 12%).

Why all the concern over threats not so commonly encountered? It could be that the IT pros surveyed are looking ahead of the curve. It's also possible that prevalent news reports and anecdotes about trends like *ransomware*—a threat that makes for a legitimately alarming story—could be elevating their perception of certain risks.

Type of security threats/breaches experienced in 2015

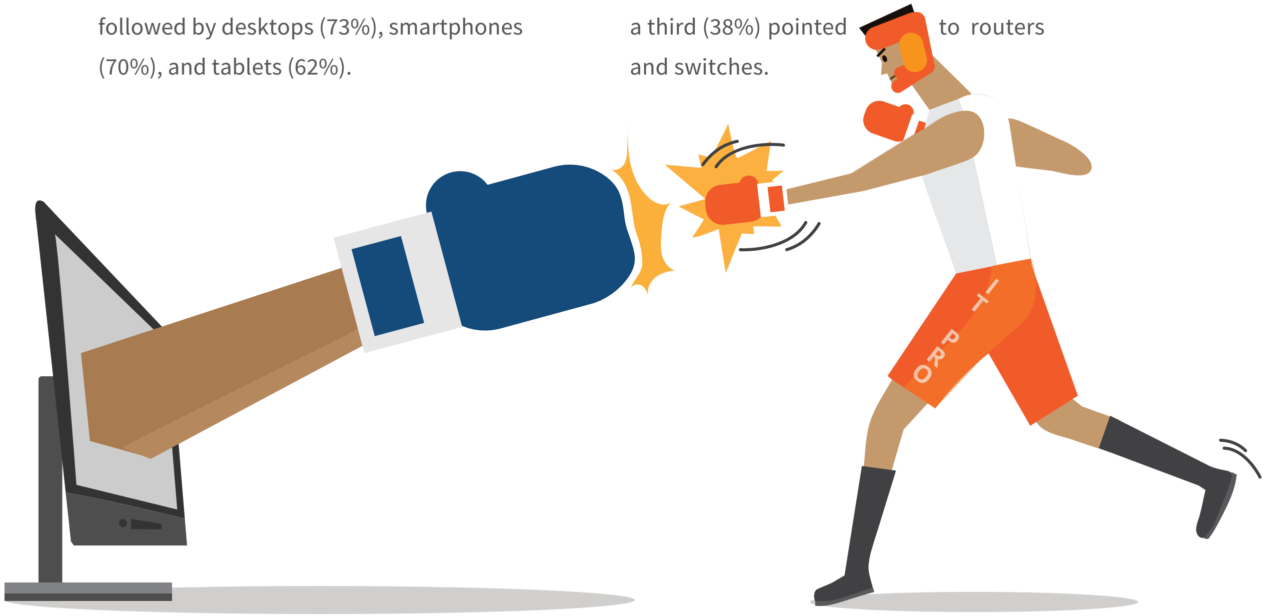


02

Common Points of Entry

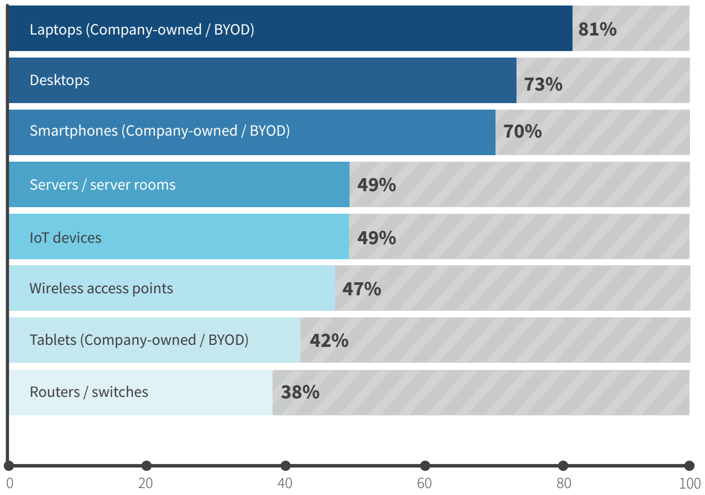
Now that we've examined the *what* of security threats, we can move on to *where*; that is, where IT pros think their networks are most vulnerable to a breach. The majority pointed to laptops (81%)—both company-owned and BYOD—as the network-connected endpoints at highest risk, followed by desktops (73%), smartphones (70%), and tablets (62%).

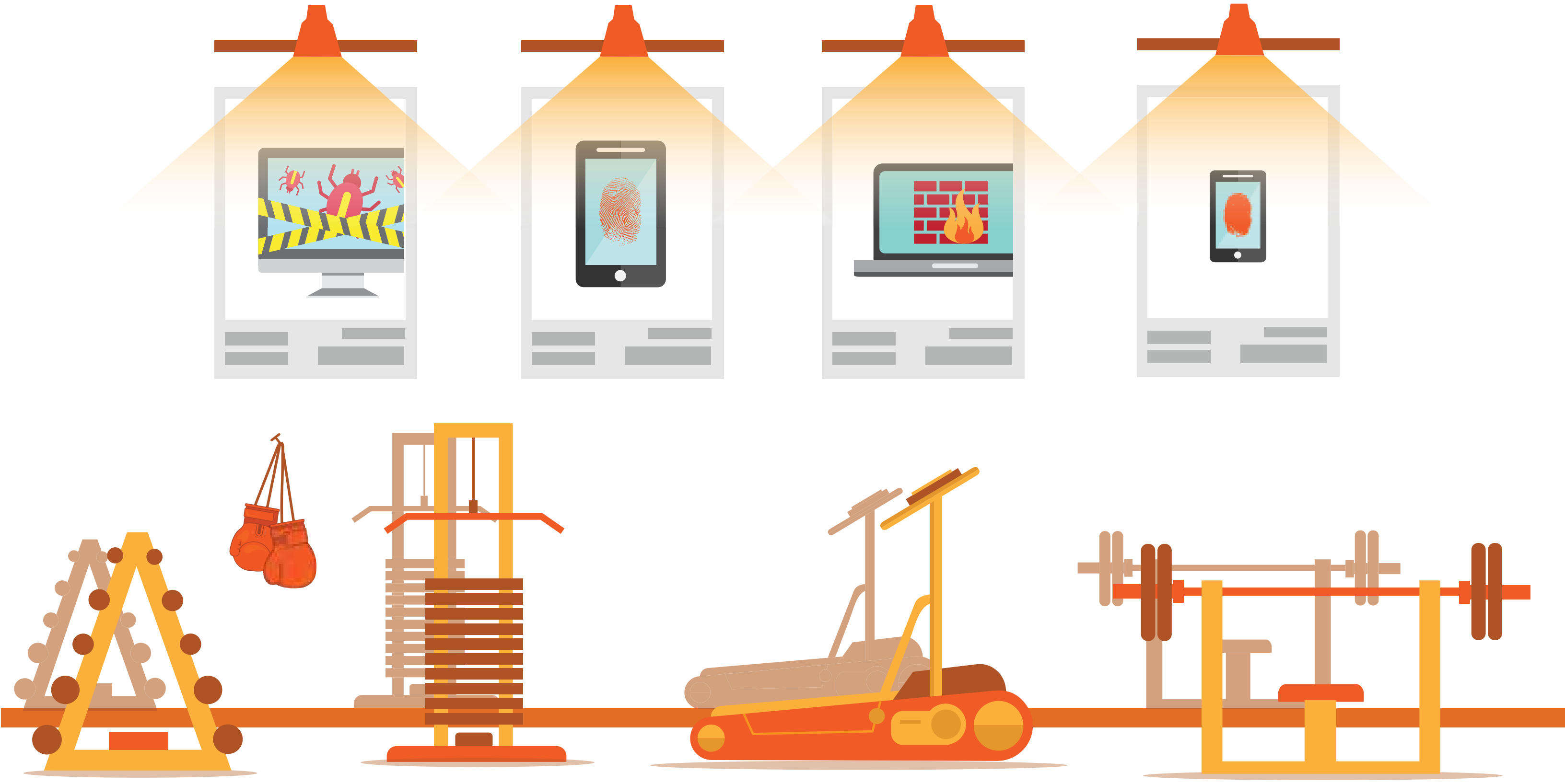
As with laptops, respondents saw the risk to smartphones and tablets as applying to both company-owned and BYOD devices. Just under half of respondents listed servers (49%), Internet of Things devices (49%), and wireless access points (47%) as being at risk, and well over a third (38%) pointed to routers and switches.



Perceived risk of network-connected endpoints in 2016

(Percentage of IT pros who selected "moderate" or "high" risk)



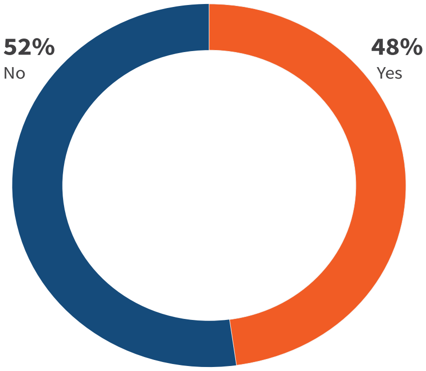


03

Who’s the Real Enemy?

One would think that hackers are the people IT pros are most concerned about when it comes to security… but end users can also be formidable opponents. Case in point: users create a phenomenon called *shadow IT*, which refers to employees going outside of protocol and installing unauthorized apps like Dropbox to their computers or mobile devices, or even setting up IT services—*without IT’s blessing*. Roughly half the respondents said they thought shadow IT poses a security risk to their organizations.

Belief that shadow IT poses a security threat to the organization

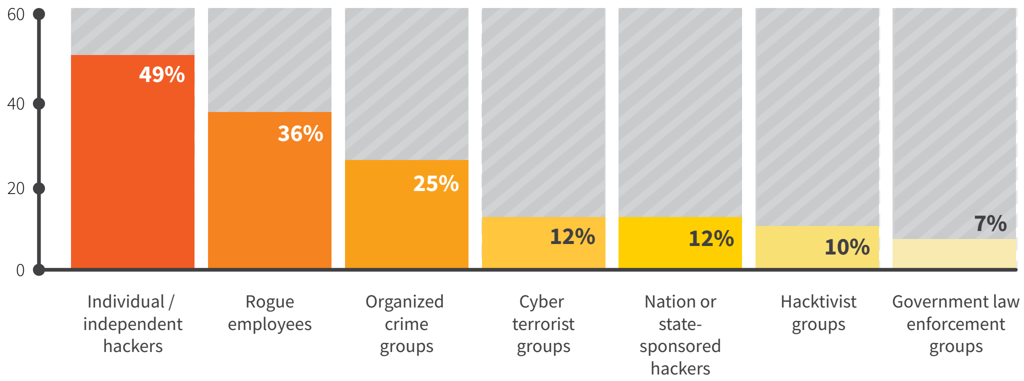


Many IT pros stated that employees often don't stop to think about the risk of a virus joining the company in the ring, so they download and install apps without notifying IT. By doing so, they actually compound the security risk because IT doesn't have a chance to stave off a poor decision or make sure devices are properly hardened to withstand attack. In the words of one wise IT pro, "Freeware is like a box of chocolate: you never know what you're gonna get."

Many respondents also pointed out that end users don't necessarily know about the other risks above and beyond the possibility of viruses—like performance bottlenecks, IT time lost to resolving problems, or making the organization more susceptible to hackers.

And who's considered to be the biggest security threat in 2016? About half thought independent hackers were the main suspects, while 36% named rogue employees—putting this group *ahead* of organized crime (25%), cyber terrorists (12%), and hacktivists (10%).

Perceived sources of IT security threats in 2016



TAKING ACTION: THE 1+2 COMBO

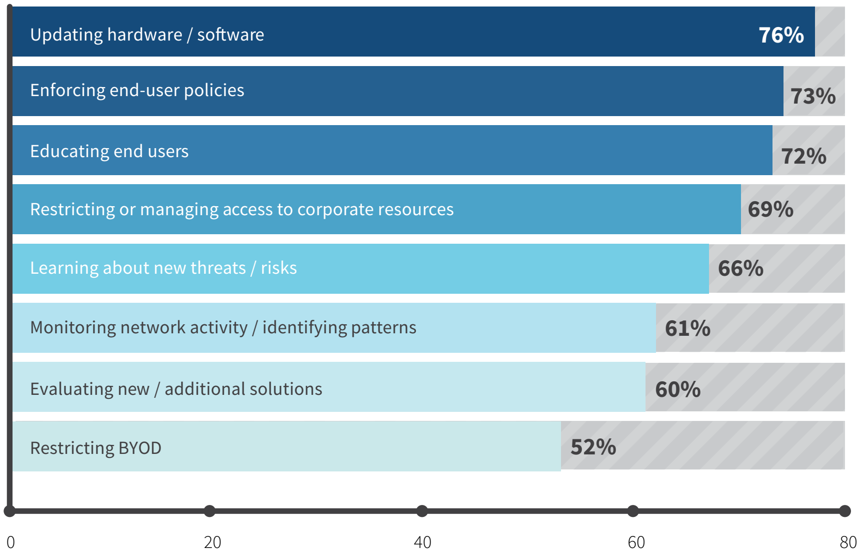
Given these rankings, it's not surprising that top actions taken against threats include efforts to head off problems caused by end user behavior—inadvertent or otherwise. Just over three-quarters mention the importance of regular updates to hardware and software, which helps protect employees from external threats (or maybe the occasional lapse in judgment).

The vast majority of respondents (86%) also have an end user initiative in place, and 68% have a formal IT security policy, too.

Such initiatives and policies include enforcement, education, restricting access to key resources, and ongoing research to make sure IT knows about new threats and risks as they emerge.

In other words, IT pros are trying not only to batten down the hatches, but also to educate themselves and employees on how to mitigate the risk of breaches. A common thread running through all of these measures is an effort to make security part of day-to-day operations and culture across the organization… as well as across the network.

Top actions taken to protect against threats



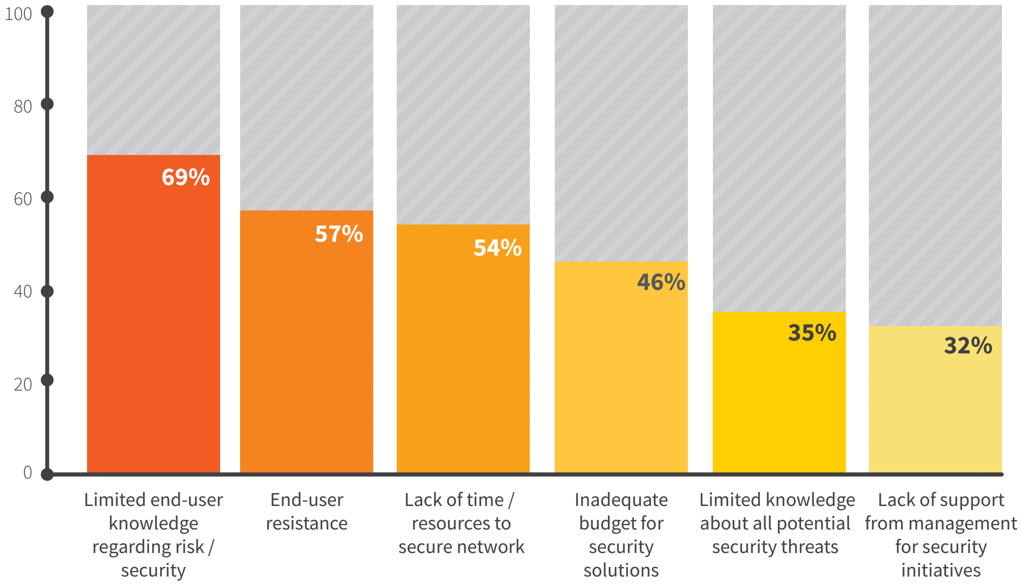
SECURITY BLOWS

So what, exactly, are IT pros up against in their epic battle against “the big hack”? Once again, their frustrations with users outweigh other obstacles. In one corner, they’re dealing with limited end user knowledge (69%) and in the other, outright resistance (57%). Some employees don’t know—or even care—about the consequences of, say, letting their kids play on a work laptop, or downloading torrents of digital tunes over the company network. Others are more focused on convenience and deadlines than on security, and would rather just quickly download the app they want and be done with it than involve IT, especially when they think no one else will be affected. And some seem to believe that security policies only exist to monitor employees.

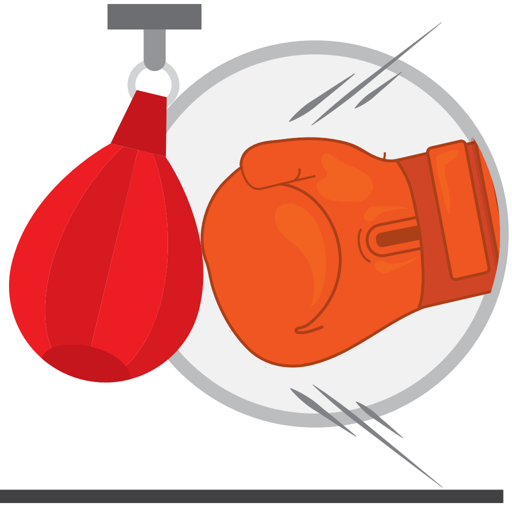
> *“Users think our security policies exist to restrict them, and not to protect company assets and data.”*
>
> – IT pro

As for the typical amount of time that’s devoted to IT security, IT pros spend almost 20% of the work week on it. So is that number high or low? It’s tricky, given that we’re talking about professionals who spend their time doing things that aren’t primarily about security per se, but have the effect of strengthening it—such as updating software.

Top IT security challenges



04

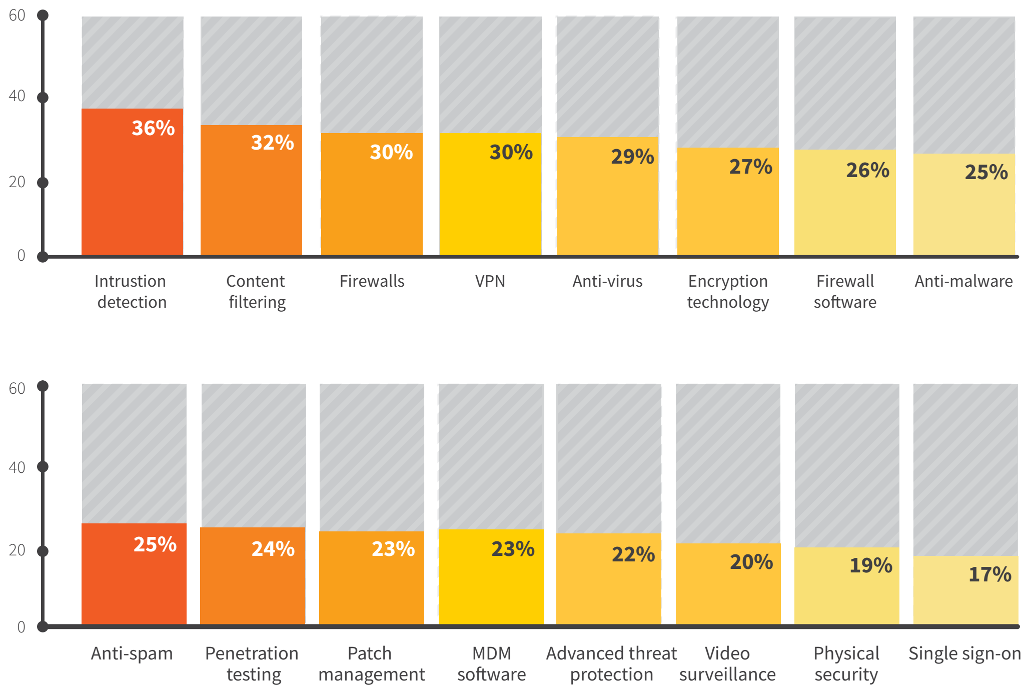


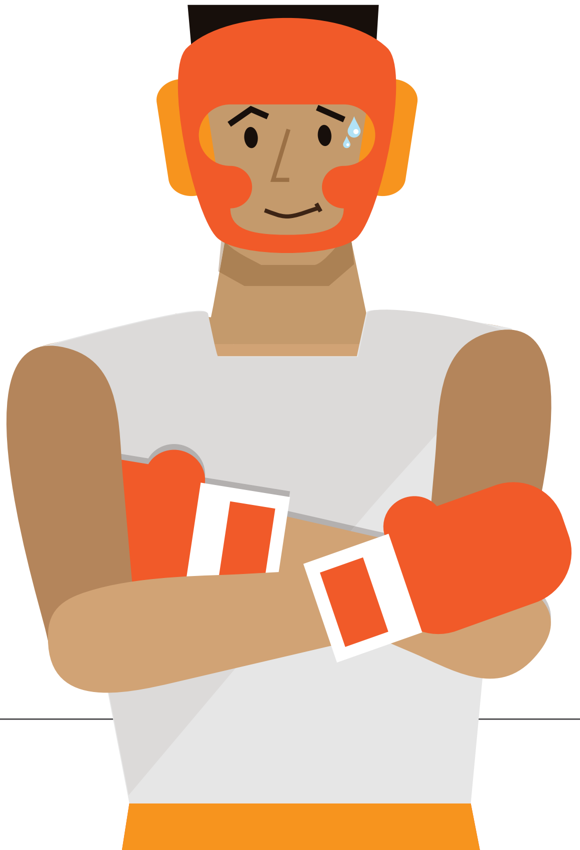
The Future: Threats in Training

Which elements of IT security do IT pros expect to invest more in over the coming year? It seems there's no silver bullet, as responses were fairly even and relatively low across the board. Instead of focusing on individual solutions, they're taking a more holistic approach that covers all of their bases and includes security measures such as intrusion detection, content filtering, and firewalls.

But IT pros definitely recognize that security is a worthy investment. In fact, the majority (84%) expects security investments to increase in at least one area, with 71% expecting their organizations to be more secure in 2016. Perhaps they feel they're more seasoned fighters, with shiny new gloves in the form of, say, advanced threat protection to help them keep their guard up.

IT security solutions expected to have an increased investment in 2016





But who’s most responsible for keeping organizations safe? IT pros overwhelmingly point to themselves (87%). However, they also point out that everyone from individual employees (43%) to high-level executives (41%) has a role to play.

> *“The biggest misconception about IT security is that it is a product or event when, in fact, it is a process. It requires participation by every employee at every point of exposure.”*
>
> – IT pro

05

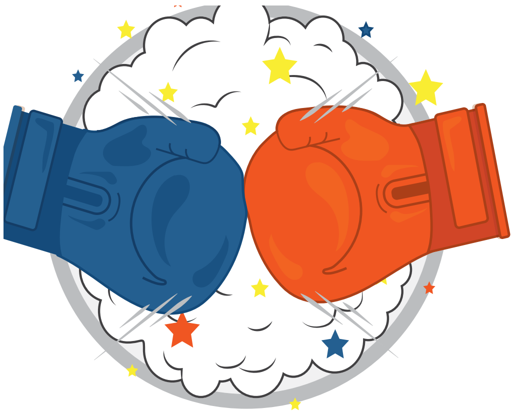
The Final Round

Malware, ransomware, and phishing schemes aren't going away anytime soon. In fact, they're likely to get more sophisticated in the coming years. But IT pros are better equipped than ever to fight these threats… and knock them out. They're working proactively to keep their systems updated and to educate and engage end users. They also have a better idea of what they're up against.

Organizations may worry they're down for the count in their battle against security threats; but don't throw in the towel just yet. Continue to empower IT to look for new and better ways to protect everyone and everything that's connected to the network, build on a strong experience base, and make security awareness and training a bedrock part of company culture. In doing so, organizations can turn the very weaknesses attackers exploit into smart defenses that can flexibly respond to emerging threats. And the heavyweight champ is… data security!

> *"This is going to be an ongoing arms race for quite some time. All we can do as IT professionals is to mitigate the issues and do our best to educate and protect our end users."*
>
> – IT pro

BIG HACK • IT PRO
VS.

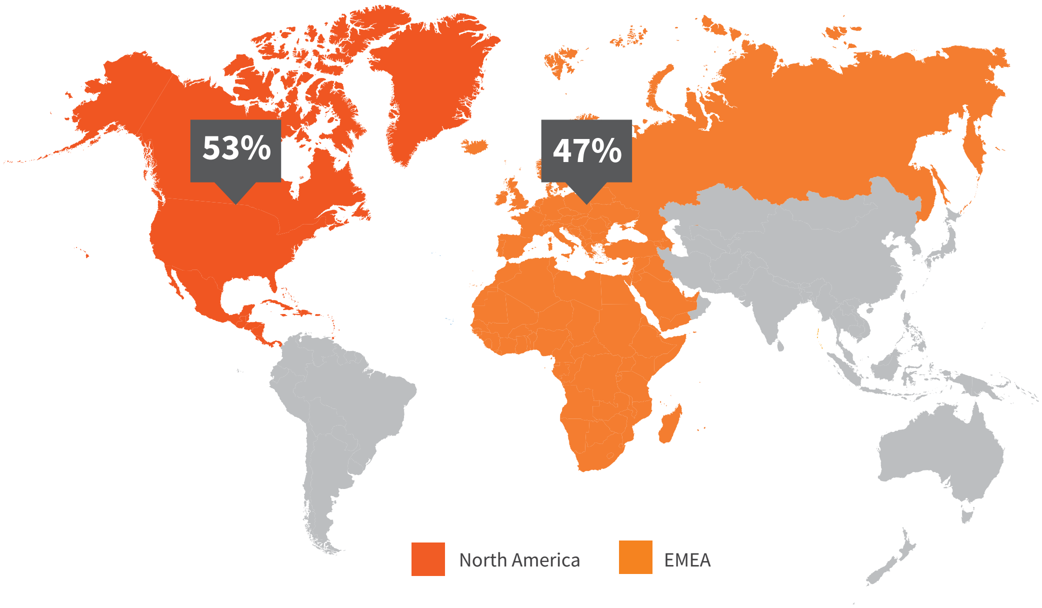


06

Details on the Data

You’ve just read Spiceworks’ version of data gone spicy: Our answer to humdrum data. We tackle the tech issues of today... and what’s coming soon to a server room near you. And we deliver it all with more originality and spice than your typical run-of-the-mill reports. Drawing from a user base of millions of IT pros, it’s a glimpse into tech you can’t get anywhere else!

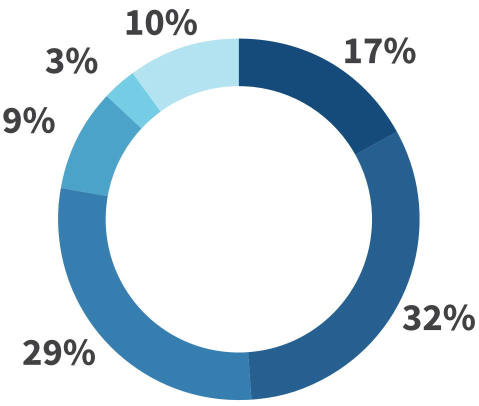
Region

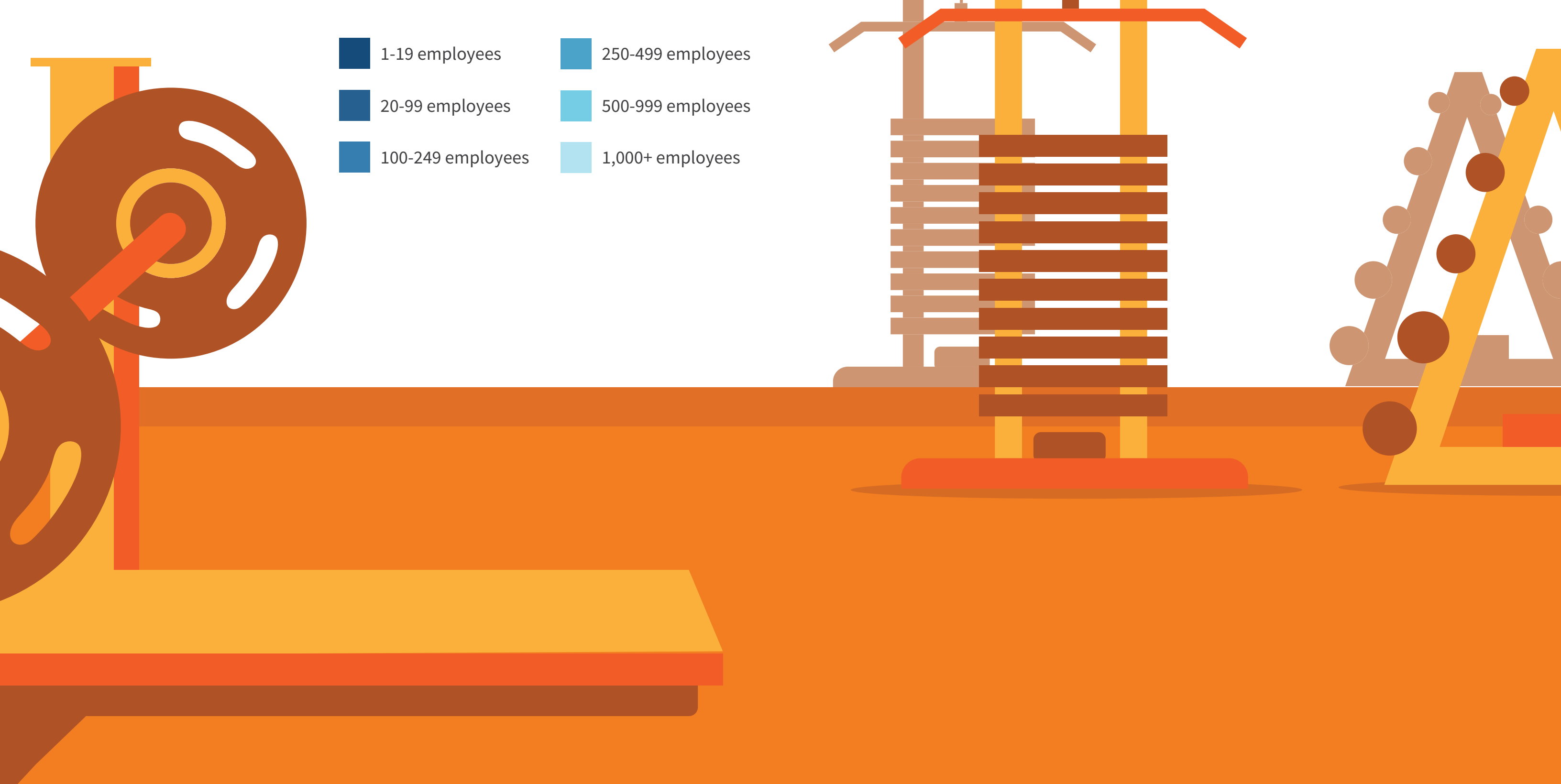


Industry

13%	13%	12%	9%	6%	6%	6%	5%
Education	IT Services	Marketing	Healthcare	Construction	Finance	Non-Profit	Consulting

Company Size





■ 1-19 employees	■ 250-499 employees
■ 20-99 employees	■ 500-999 employees
■ 100-249 employees	■ 1,000+ employees

Credits

Research: Tracy Peto, Jace Recio

Copy & editing: Mary Summerall, Lisa Young, Andrew Baron, Priscilla Brave

Illustration & design: Clarice Bajkowski

SPICEWORKS
Voice of IT®

About Spiceworks Voice of IT®

The Spiceworks Voice of IT market insights program publishes stats, trends and opinions collected from technology professionals that are among the more than 6 million users of Spiceworks. Survey panelists opt-in to answer questions on technology trends important to them. To find out more about our research capabilities, email insights@spiceworks.com.

About Spiceworks

Spiceworks is the professional network millions of IT professionals use to connect with one another and thousands of technology brands. The company simplifies how IT professionals discover, buy and manage an estimated $600 billion in technology products and services each year. Headquartered in Austin, Texas, Spiceworks is backed by Adams Street Partners, Austin Ventures, Institutional Venture Partners (IVP), Goldman Sachs, Shasta Ventures and Tenaya Capital. For more information, visit www.spiceworks.com.

For other Spiceworks Voice of IT reports visit:
www.spiceworks.com/marketing/resources/

Follow Spiceworks on Twitter and connect with Spiceworks on Facebook.

This report contains information of fact relating to parties other than Spiceworks. Although the information has been obtained from, and is based on sources that Spiceworks believes to be reliable, Spiceworks does not guarantee the accuracy, and any such information might be incomplete or condensed. Any estimates included in this report constitute Spiceworks' judgment as of the date of compilation, and are subject to change without notice. This report is for information purposes only. All responsibility for any interpretations or actions based on the information or commentary contained within this report lie solely with the recipient.

SPICEWORKS

Where IT goes to work.™