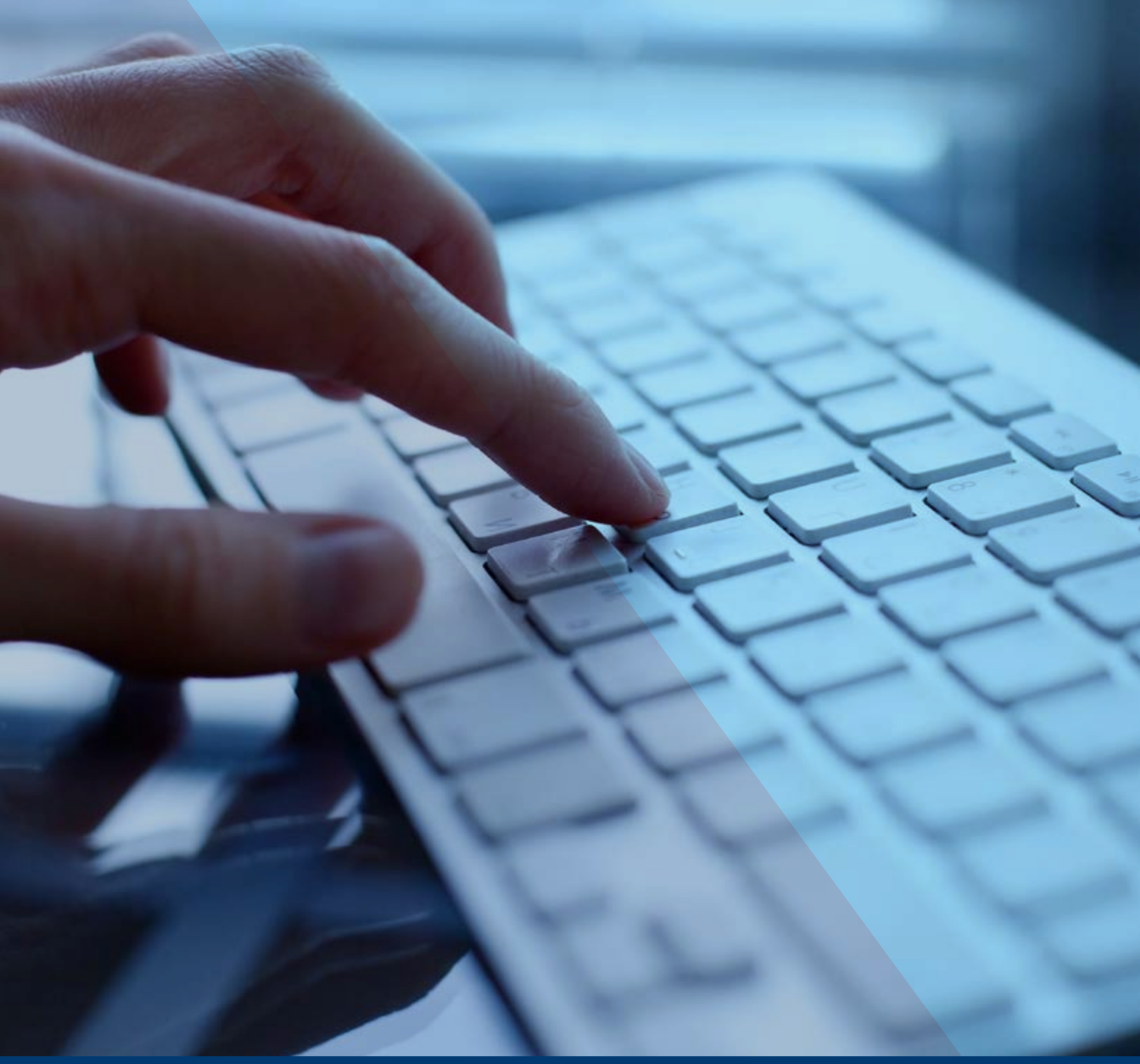


The Surprising State of IT Security

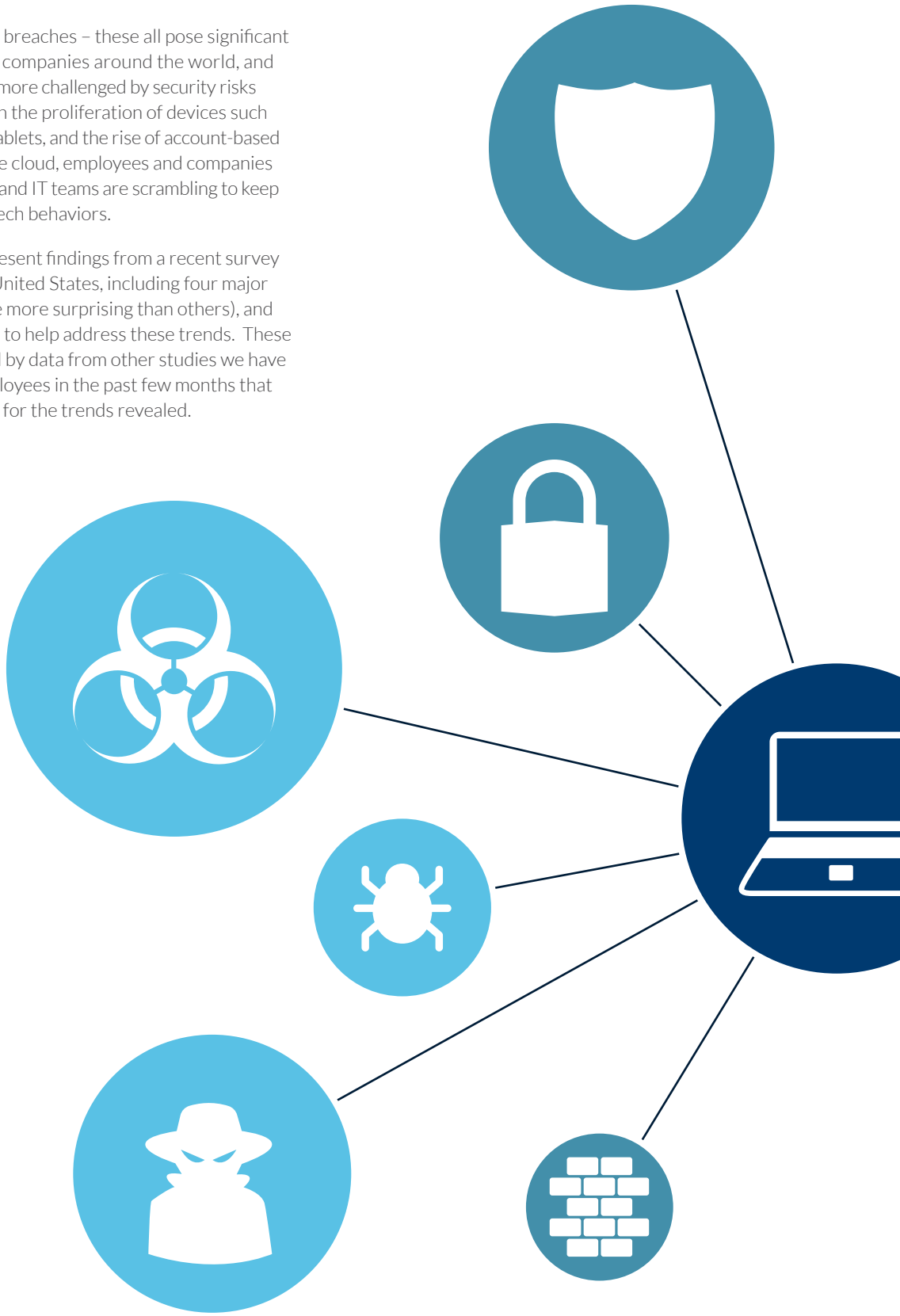
Including 4 Key Trends Among IT Professionals and 3 Steps to Help Protect Your Company From Threats

Central by LogMeIn

INTRODUCTION

Malware, hackers, viruses, breaches – these all pose significant threats to businesses and companies around the world, and rightfully so. IT teams are more challenged by security risks now than ever before. With the proliferation of devices such as laptops, smartphones, tablets, and the rise of account-based information that lives in the cloud, employees and companies are more at risk than ever, and IT teams are scrambling to keep up with rapidly-changing tech behaviors.

In this whitepaper, we'll present findings from a recent survey of IT professionals in the United States, including four major trends in IT security (some more surprising than others), and advice for IT professionals to help address these trends. These findings are supplemented by data from other studies we have conducted among US employees in the past few months that provide additional context for the trends revealed.



FOUR KEY TRENDS IN THE IT SECURITY MARKET

1 The modern workplace is here but the modern IT team is not.

IT practices aren't quite up to speed with the modern workplace. From working remotely to Bring Your Own Device (BYOD), there are many new practices and habits that present challenges to IT teams, especially when it comes to security. Cloud security is also an area of concern. More than a third of companies indicate they will be increasing their use of cloud-based apps, and over a third of IT professionals claim that important parts of their business are already cloud based. Still, cloud security is ranked towards the bottom of their security concerns as many companies simply rely on the cloud based app to take care of any security issues.

IT professionals agree and acknowledge that IT teams are not currently ready to deal with the internal fallout from security threats, and things may get worse before they get any better. Over a third of IT teams claim to be understaffed and lack proper training. As a result, damages from security attacks can take days, or even weeks, to deal with.

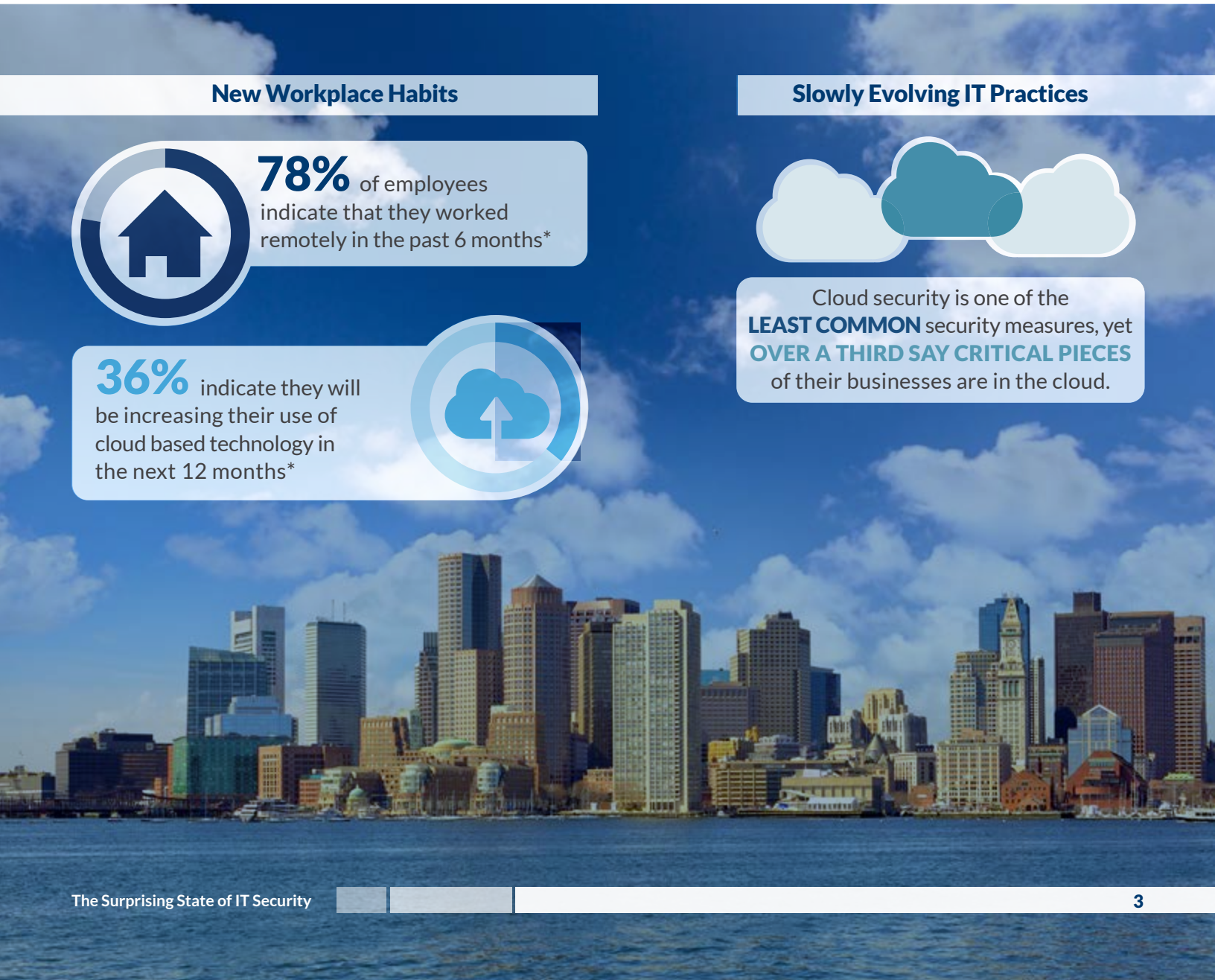
New Workplace Habits

78% of employees indicate that they worked remotely in the past 6 months*

36% indicate they will be increasing their use of cloud based technology in the next 12 months*

Slowly Evolving IT Practices

Cloud security is one of the **LEAST COMMON** security measures, yet **OVER A THIRD SAY CRITICAL PIECES** of their businesses are in the cloud.



2 Budget is still king.

Regardless of your role or function, there will never be enough budget, and within IT operations is no exception. In fact, as more security threats continue to emerge and evolve, and concern among IT professionals rises, the IT budget is not increasing in parallel. Despite the increase of the present and future usage of cloud based technologies,only slightly more than a third (36%) indicate they will increase their investment in cloud security in 2016.

This impacts both technology and personnel: On the technology side, just over a third of IT professionals indicate they are increasing their investment in cloud-based security, despite increasing their usage of this technology. An even lower percentage (18%) claim they will invest in hiring. The threat of large security breaches is even more concerning for small companies considering nearly two in five (37%) allocate less than 5% of their IT budget on security management.

Instead of simply reacting to security issues after they occur, companies should take a more proactive approach and invest a larger percentage of their budget in IT security practices, technology and personnel.

TOP 3 USES OF SECURITY BUDGET

- anti-virus management software
- firewalls
- activity monitoring

44%

say that budget is the biggest threat to managing the company's IT security

81% say **25%** or less of the IT budget goes to security management

72%

are investing the **same amount of money or less** in security than they were in 2015

70%

of IT is concerned about employee behavior causing security risks, but training employees is not a top priority

NEARLY
30%

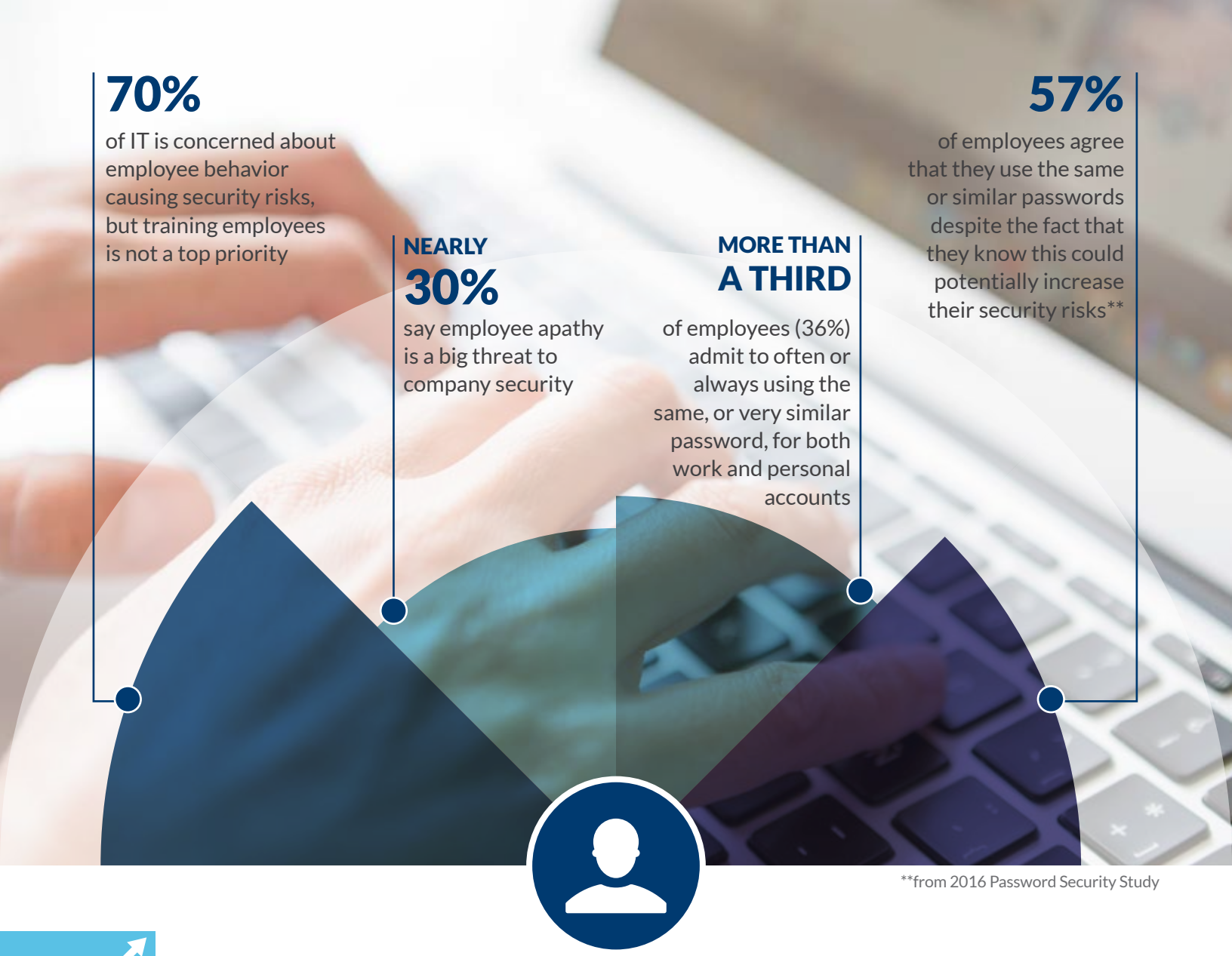
say employee apathy is a big threat to company security

MORE THAN
A THIRD

of employees (36%) admit to often or always using the same, or very similar password, for both work and personal accounts

57%

of employees agree that they use the same or similar passwords despite the fact that they know this could potentially increase their security risks**



**from 2016 Password Security Study

3 People are the problem.

Employees can be a company's biggest asset, but when it comes to security, they can also be a one of the biggest threats. A company is only as secure as its least security-minded employee – one employee with bad practices can compromise the entire company. Each device and cloud-based account that employees use presents a new door that hackers could potentially break down in a breach. Most employees are well aware of the potential threats that come with poor security habits - especially when it comes to password security - yet many do little to improve these bad habits, with 36% using same or similar passwords for both personal and work accounts. But companies are also not doing enough to keep these security issues and concerns top-of-mind, as initial and ongoing training is not a top priority.

With employees' sometimes nonchalant attitudes towards password security, companies big and small are increasingly vulnerable to security breaches and hacks. In order to combat apathy when it comes to security, companies should set up and manage security protocols for their employees to follow. Setting up strong guidelines, and ensuring their employees are abiding by these rules, will help to minimize these security threats.

4 Breaches are common, but concern is fleeting.

Target, Sony, Home Depot – unfortunately the list of security breaches is getting longer. And these are just the high-profile cases, whereas many more are happening on a smaller scale. In reality, two thirds of companies have suffered a security breach at least once in the past (with almost 20% just in the past year!), yet only 30% believe their company is at risk to suffer a security breach or attack in the future.

As a result of smaller budgets, smaller companies are also more likely to cut corners on security, leaving these companies more vulnerable than ever to security breaches and hackers. More than half of small businesses do not implement personal device encryption, and nearly 20% of companies do not even implement basic password security.

Despite the fact that breaches are becoming more commonplace, nearly 90% are confident that their company's security measures are effective. Companies, however, should not fall into the trap of being overly confident about their security measures, as security should always be a core focus for the company.

30%

believe their company is likely to suffer a security breach or attack

ALMOST 1 IN 5

(18%) had to deal with a malicious attack in the past year

86%

are confident that their security measures are effective

30%

of respondents believe there is nothing else they could do to protect the security of their company

THREE WAYS TO PROTECT YOUR ORGANIZATION

1 Audit, Assess, Analyze

The first step to ensuring your organization, including all of your confidential and proprietary data is protected, is to understand where your weaknesses are. This might be IT practices, IT team knowledge, employee habits, budget, or any number of factors.

Take the time to audit the company's current security status. You can even give yourself a grade. With this understanding at the beginning of each fiscal year, you'll be able to better articulate your needs as an IT team and vouch for whatever budget you might need (software, employee training, IT head count, etc.). Your research and overview of the company's security will help make security a priority with others, especially employees.

of companies audit their anti-virus management software every year

TOP 3 SECURITY MEASURES TAKEN

89%
firewalls

86%
anti-virus management software

73%
Employee training & policies

2 Establish Proactive Measures

You're likely managing many computers, potentially hundreds or even thousands, so it's nearly impossible to know what's going on with each machine. However, with IT automation software you can manage all of your computers through a centralized dashboard so you can view status and initiate changes from one single screen – regardless of how many end points you have.

There are many ways automated software enables your IT team to be proactive, including:

- **Alerts:** Setup alerts so you're notified when specific activity occurs on a machine, such as outdated anti-virus software, connectivity problems, disk space limits, and more.
- **Tasks:** Execute routine tasks automatically such as software installations, remote commands, run batch files, distribute files, and more.
- **Scans:** Many IT automation software providers allow you to run scans on your endpoints to search for malware and viruses so you know when a machine is at risk.

86%
of companies use anti-virus management software

THREE QUARTERS
of those include automated monitoring including ongoing virus detection, anti-virus software updates and deep computer scans

3 Educate Employees

Your company is only as strong as your least-informed, most insecure employee. It's worth the time and investment to educate your employees, reinforce the risks of weak security habits and instill good password practices.

Areas where further employee education and training could help decrease security risks for companies include:

- **Password security:** Educate employees on what it means to have secure passwords. This means not only creating strong passwords, but also not sharing them with co-workers, friends and family, using a password manager to store passwords, changing passwords often, and using unique passwords for multiple accounts. It might sound like a no-brainer but make sure employees are not using the same passwords for both personal and work accounts.
- **Device management:** Instill good practices, such as locking your computer before walking away, encrypting your devices, and not bringing outside hard drives to connect to work computers.
- **Internet browsing awareness:** Be aware of potential phishing attempts by not opening emails from unknown sources to avoid spam or clicking on suspicious links that could lead to malware.
- **Install and maintain antivirus software on employees' devices:** Antivirus software is typically the last line of defense once a security threat emerges, and ensuring that your software is up to date with the most current definitions helps to minimize these threats.
- **Update your software regularly:** Software companies push updates and patches to their software regularly, and as such, employees should make sure they are running the most up-to-date versions.
- **Regular backups:** If your company does encounter a data breach, having backups of your data will ensure that your data is still safe and reachable. Personal computers should be backed up completely on a weekly basis at a minimum.

20% of consumers do not consider themselves informed on the best practices for password protection

&

30% feel that all the talk about password protection is overrated**

MOST COMMON **SECURITY POLICIES**

93% PASSWORD

87% REMOTE ACCESS

86% ADMIN RIGHTS

77% BACKUP REQUIRED

ALMOST TWO IN THREE consumers (65%) either mostly or always use the same password

&

38% say they feel annoyed when creating a password**

**from 2016 Password Security Study

LogMeIn Central: Simple, Secure IT Automation & Management

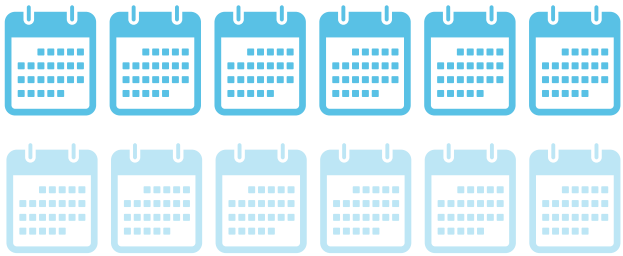
Now includes Kaspersky Endpoint Security!

Whenever you're managing tens or even hundreds of computers, it's a challenge to keep your eyes and ears on everything. When it comes to security though, you can't let a single threat get by.

With LogMeIn Central Premier, you have the control you need to remotely monitor and manage all of your computers easily and securely. With Central, every computer in your network is equipped with premium remote access so you can troubleshoot anytime, anywhere. Central Premier also keeps your systems up-to-date by automatically applying Windows updates when needed, and provides monitoring on all machines so you can identify issues and fix them quickly.

Now Central Premier includes Kaspersky Endpoint Security for all of your managed computers. Together, Central Premier & Kaspersky protect your business and your customers from known and unknown threats, including malware, viruses, spam, and more. As an IT team leader, you'll have one centralized dashboard where you can manage anti-virus status for all computers, servers, and mobile devices, and set security controls for all end users ensuring corporate policies are maintained.

ONLY HALF
audit anti-virus management software annually



and **A QUARTER** have
NO TIMEFRAME for doing so.

Try it free!

Start a free trial of Central Premier today to experience fast, reliable remote control, group users and computers, see how anti-virus management gives you a single-view status into all end points, and more.

Get started now at LogMeIn.com.

Central by LogMeIn

www.LogMeIn.com