IS YOUR DATA SAFE?

The alarming rate of security noncompliance by employees today

By the end of 2015, more than 75 percent of U.S. employees (and more than 1.3 billion workers worldwide) will routinely work remotely. The growth of this mobile workforce means that more sensitive business data (customer information, financial records, trade secrets) will be at increased risk from hackers, scammers, and cyberthieves.

You feel lucky you can rely on your employees to ensure that your valuable business data and devices are secure and protected.

Or can you?

SHAKY SECURITY

Malware on mobile devices is on the rise—even a phone with security measures in place is not immune if a malicious application is unintentionally downloaded from a trusted web store. In fact, a modern smartphone provides an excellent platform for advanced persistent threats (APTs) and cyberespionage.

30% of parents let kids play, download, and shop on their mobile work device.

49% of people participate in bring-your-own-device (BYOD) programs, using their personal devices for work-related activities.

Almost half of those who own a mobile device don't protect it with a password or other basic security measures.

WHAT WERE THE TWO MOST COMMON PASSWORDS IN 2013?

"1 2 3 4 5 6" and "p a s s w o r d"

WHY IS SECURITY SO LAX?

COMPLEXITY

Companies make security measures too difficult for employees to comply with. For example, by 2016, overly restrictive mobile device management measures will cause 20% of enterprise BYOD programs to fail, according to research firm Gartner.

PASSWORD FATIGUE

The average user has 26 password-protected accounts (but only five different passwords).

RESISTANCE

38% of people surveyed would rather clean a toilet than come up with a new password.

HIGH COST OF CYBERCRIME

75% of breaches in 2012 were financially motivated cyberattacks.

IN 2013, BREACHES INCREASED 58% WHILE THE NUMBER OF IDENTITIES EXPOSED INCREASED 3.5 TIMES TO MORE THAN 342 MILLION

HOW MUCH IS YOUR IDENTITY WORTH?

Average number of breached records	Average total organizational cost of data breach (US$)	Average lost business costs (US$)
AUSTRALIA 34,249	UNITED STATES $5.4 million+	UNITED STATES $3.03 million+
UNITED STATES 28,765	GERMANY $4.8 million+	AUSTRALIA $1.95 million+
INDIA 26,586	AUSTRALIA $4.1 million+	GERMANY $1.74 million+
GERMANY 24,280	FRANCE $3.76 million+	FRANCE $1.56 million+
UNITED KINGDOM 23,833	UNITED KINGDOM $3.14 million+	UNITED KINGDOM $1.41 million+

WHO IS MOST AT RISK?

VICTIMS OF CYBERCRIME ARE MORE LIKELY TO BE

- Male 64%
- Millennial 66%
- Mobile device user 63%
- Social network user 68%
- Public/unsecured Wi-Fi user 68%
- Parent of child age 8–17 65%

TOP INDUSTRIES ATTACKED IN 2013

- Professional services 20.1%
- Nontraditional services 18.5%
- Public administration 14.8%
- Finance, insurance, and real estate 13.4%
- Manufacturing 11.1%

BETTER SOLUTION FOR MORE SECURE FUTURE

THE NO. 1 CAUSE OF BREACHES AND COMPROMISED RECORDS IN LARGE ORGANIZATIONS?

STOLEN CREDENTIALS

Strong authentication methods such as **two-factor authentication (2FA)** or **multifactor authentication (MFA)** combine two or more factors for increased security. This is often a combination of the following:

SOMETHING THE EMPLOYEE KNOWS (e.g., a user name and a password) + SOMETHING THE EMPLOYEE HAS (e.g., a token, a smart card, etc.) + SOMETHING THE EMPLOYEE IS (e.g., a fingerprint or even a behavioral pattern)

80% of data breaches could have been eliminated with the use of 2FA.

With data breaches and malware on the rise, the stakes are higher than ever. **Enterprises today require the following:**

1. **2FA solution that is cost effective, scalable, and secure, but still provides a user-friendly experience**
2. **Unified solution that can provide employees with secure access to applications and networks while preventing access by malicious outside parties**
3. **Solution that is easy to roll out across a large organization**

PASSWORDS ARE NOT A SMART SECURITY MEASURE BECAUSE

- We often write passwords down.
- We use predictable patterns that thieves anticipate.
- We tend to use the same password for multiple accounts.
- We are often careless and fall victim to thieves who are "shoulder surfing."
- Cracking, hacking, malware, and man-in-the-middle, brute force, dictionary, and behavior-based attacks are all on the rise today.
- A dedicated password-cracking machine can crack an eight-character password in about five hours.

SMALL BUSINESSES INCREASINGLY AT RISK

One in five small businesses is a victim of cybercrime each year.

CLOSED CLOSED

Almost **two-thirds** of victims go out of business within six months of attack.

SMALL BUSINESS CYBERCRIME

61% of all targeted attacks in 2013 were aimed at businesses with fewer than **2,500 employees**.

30% of attacks were directed at businesses with fewer than **250 employees**.

> **"Just as nuclear was the strategic warfare of the industrial era, cyberwarfare has become the strategic war of the information era."**
>
> U.S. Secretary of Defense Leon Panetta

SYMANTEC STRONG AUTHENTICATION SOLUTIONS

Symantec solutions have the features and capabilities to provide your enterprise with strong, scalable, and manageable authentication for protecting online identities and interactions between consumers, business partners, and employees.

To learn more, call your Symantec account representative or visit www.symantec.com.

Symantec™

Part number: 21330416

SOURCES

"Intelligence Report," Symantec, December 2013.
"2013 Norton Report," Symantec, October 2013.
"Reaping the Benefits of Strong, Smarter User Authentication," Symantec, October 2013.
"Authentication Solutions Buyer's Guide," Symantec, May 2013.
"Internet Security Threat Report," Symantec, April 2013.
"Two-Factor Authentication: A TCO Viewpoint," Symantec, August 2012.
"2013 Cost of Data Breach Study: Global Analysis," Symantec and Ponemon Institute, June 2013.
"The Immediate Future of Passwords," SC Magazine (November 13, 2013), www.scmagazine.com/the-immediate-future-of-passwords/article/320823/.
EyeVerify newsletter, January 2014.
"Data Breach Investigations Report," Verizon, April 2013.