Multi-Factor Authentication

Passwords have failed, so what's next?

MFA

Breaches are prevalent and weak passwords are to blame.

Password security is one of the most important issues facing information security today. According to the 2017 Verizon Data Breach Report, 81 percent of data breaches are caused by weak or stolen passwords. To overcome these challenges, many organizations are looking to multi-factor authentication (MFA) technology to help deliver a layered approach and mitigate the role passwords play when providing access.

But unfortunately, traditional MFA solutions are often difficult for small and midsize organizations to implement and manage. To better understand the current state of password security and MFA usage, WatchGuard commissioned a survey of business owners and IT decision-makers running companies with between 100-1,000 employees in the United States, the UK and Australia. Here's what was found.

25%

According to WatchGuard research **25% of SMBs** claim to have **experienced a breach** in the last **18 months**.

Business owners and IT decision-makers surveyed believe their employees engage in weak password practices:

- **47%** — 47% of employees use **simple or weak passwords**
- **31%** — 31% use network passwords for **personal applications**
- **30%** — 30% **share passwords**
- **40%** — 40% click on **phishing emails, etc.**
- **36%** — 36% use **unsecure Wi-Fi**

User Name
****

The problem will NOT be solved with training

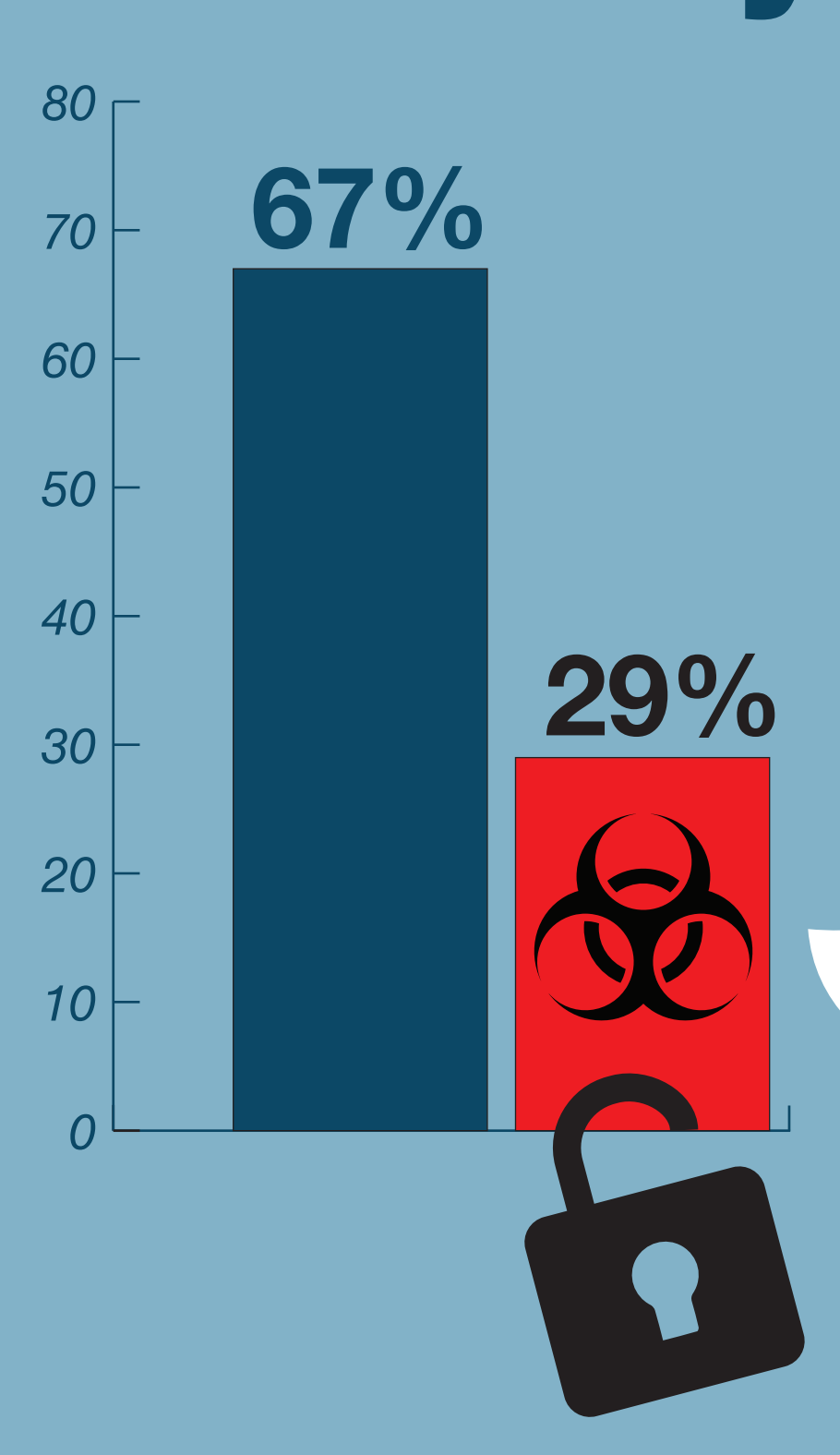
80% of companies claim to be **providing password training** to their employees, **yet the problems persist**.

Companies are seeking a better solution and 84% note that they would rather have a technology in place than rely on password policies.

The solution is Multi-Factor Authentication

Multi-factor authentication (MFA) is a method of logon verification that adds a layer of security beyond just a simple username and password. It prevents unauthorized access that can result from lost or stolen passwords, while enabling verified users to easily access their accounts and information.

How Many SMBs Actually Use MFA?



67% of companies use MFA solutions **BUT 29% DO NOT!***

It's time to add MFA, or reevaluate existing solutions. Of those with MFA today, 47% use SMS, which can be easily spoofed or intercepted by an attacker. Also, 38% of companies use hardware tokens, which are hard to manage, and can be lost or stolen.

**4% of respondents stated that they were unsure whether or not they are using MFA*

Why?

So why aren't more SMBs adopting the latest MFA technologies?

- 61% feel most solutions are **designed for larger companies**
- 24% say **difficult to maintain and support**
- 24% say **difficult to implement**
- 24% say **too expensive**
- 22% say **resistance from within**
- **17% say they JUST DON'T NEED MFA SOLUTIONS!**

Amongst companies interested in buying:

- **65%** have plans to purchase in the future
- **83%** are interested in using MFA
- **54%** would prefer Cloud-based servers

Passwords are no longer enough. Don't let one employee's weak password compromise your company's assets and information – check out AuthPoint today!

WatchGuard AuthPoint

WatchGuard's AuthPoint provides multi-factor authentifcation (MFA) on an easy-to-use, Cloud-based platform. Since it's based in the Cloud, there's no hardware to deploy and access can be managed from anywhere. The mobile app makes each logon attempt visible and easy for users to approve or deny logins. AuthPoint also features many 3rd party integrations, including popular Cloud applications, web services, VPNs, and networks.

Learn more at www.watchguard.com/authpoint

WatchGuard®