Enterprises hope their mobile users pay attention to security

Most companies worry about communicating and enforcing their internal mobile security policies.
Enterprises hope their mobile users pay attention to security | Network World

To ensure mobile security, enterprises need the whole-hearted cooperation of their workforce. But many workers don’t seem to know or care about their company’s mobile security policies.

That conundrum fits my experience of how these things work in the real world, and it's also one of the conclusions of a new survey—Enterprise Mobility Security Goals & Challenges—conducted by Silicon Valley management services provider NetEnrich.

According to the online poll of 150 enterprise professionals, more than half (54 percent) of respondents said “their biggest challenge when it comes to managing employee use of mobile devices is simply confirming that all employees have received and reviewed their company’s policies.”

Yikes!

I guess that shouldn’t be too surprising. After all, plenty of IT workers have been known to blissfully ignore reminders to read those boring, prescriptive security policies, so rank-and-file resistance seems only natural. And I know folks who would rather have a root canal than attend mandatory security training. Over a long career in tech, I’ve even seen otherwise responsible employees delight in “cheating” their way through online security training classes, manically switching among multiple browser windows in attempt to shave off a few minutes. (Of course, I would never stoop to that level.)

Why the bad behavior when it comes to mobile security? According to the survey, even more respondents (55 percent) said “their biggest challenge is convincing employees that following the company’s mobile device protocols is in their best interests.”

As NetEnrich President and CEO Raju Chekuri said it in a statement, “IT can find itself in hot water with employees, customers and management if mobile...
Enterprises hope their mobile users pay attention to security | Network World

device security protocols are found to compromise end-user experience.”

**End-user experience affected by security protocols**

The fact is that all too often, mobile device security needs do compromise end-user experience, in ways large and small. Whether it’s constantly re-entering passwords, hassling with two-factor authentication, or occasionally not getting access to an application or piece of data when you need it, security best practices often add a noticeable layer of overhead to everyday computer work.

Just as important, the very real benefits of those practices go to the company, but the overhead falls on the individuals. No one gets a lightened load or extra time to do their work so they can deal with ongoing mobile security protocols that keep the company safe. In fact, employees are typically insulated from the direct effects of mobile security problems, even if their lapses played a role in the breach. (That’s not true for IT folks: 60 percent of respondents “said their primary goal was ensuring that they were ‘covered from an accountability perspective’ in the event there was a breach or attack.”)

The survey also showed that these are not idle threats. Almost half (42 percent) said their organizations had lost key data from a mobile device.

Given all that, perhaps the biggest takeaway is that mobile security is an endless journey, not a destination.

“The reality is, enterprise mobile security is a moving target, for which companies and IT professionals must be adjusting constantly,” Chekuri said in a statement. “A policy that works today may not work next year—let alone two to three years from now.”

**RELATED TOPICS**

- Security
- Mobile Security
- Endpoint Security

Fredric Paul

Fredric Paul is Editor in Chief for New Relic, Inc., and has held senior editorial positions at ReadWrite, InformationWeek, CNET and PC World. His opinions are his own.

PREVIOUS POST

Apple iPhone 7 vs. Samsung Galaxy Note 7: Troubled smartphone shootout

NEXT POST

U.S. cellular carriers charge too much, and here’s proof