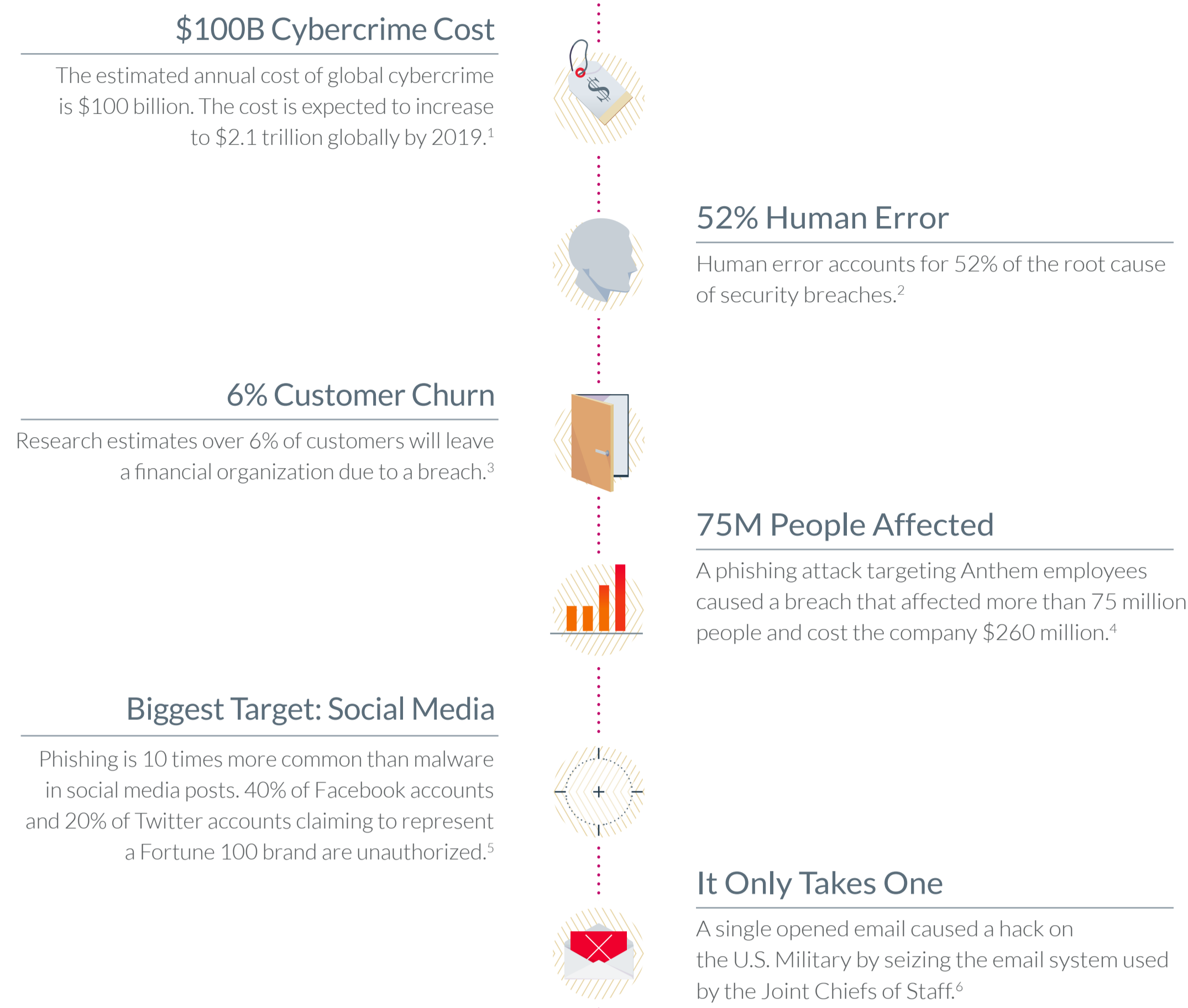


# Cybersecurity

## A PEOPLE PROBLEM

Find out why you need to pay attention to what behavioral data is telling you, and what you and your employees could do to protect your organization.

### The Human Element



Sources: <sup>1</sup>Forbes, <sup>2</sup>SC Magazine, <sup>3</sup>IBM, <sup>4</sup>OnTheWire, <sup>5</sup>Proofpoint, <sup>6</sup>Business Insider

### What do you need to ask yourself?

- How am I measuring my employees' ability to protect the organization from cyber threats?
- Can my employees identify red flags of social engineering attempts?
- Do my employees take proper steps reporting suspicious emails?

## THE BIG QUESTION

“Is there data that uncovers these risks within my organization?”



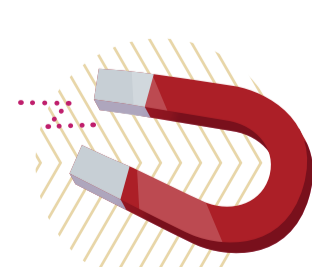
## Benchmark employees' behaviors

AND PROTECT YOUR ORGANIZATION FROM RISK EXPOSURE WITH



### Scholar

Truly adaptive, analytics-rich learning solutions for better business results: modular compliance training for employees and actionable behavioral data for legal, risk, and compliance leaders.



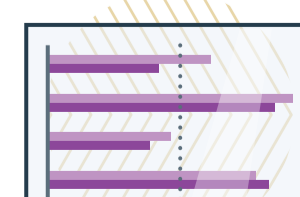
#### Engage

Reduce training fatigue with intuitive, interactive, and rewarding experiences that use advanced learning methods, game mechanics, and motivational techniques to keep learners tuned in.



#### Educate

Optimize time spent on each topic with adaptive activities and personalized feedback. Each employee achieves 100% proficiency with the level of practice they personally need.



#### Analyze

Market-leading analytics put actionable insights in your hands: measure return on training investments, drive change, and strategically strengthen ethics and compliance programs.