Selling Identity Protection as a Benefit

InfoArmor

Major pain points for employee identity theft and data breaches

Increased liability

- As much as 50 percent of identity theft begins at a victim's place of work[1]
- Identity theft is often perpetrated by fellow employees and sometimes even managers and executives
- Many phishing attacks — which often lead to identity theft — stem from emails designed to appear as if they are from a victim's boss, co-worker, or client
- Courts are increasingly ruling against companies that fail to protect their employees' personal data[2]
- In addition to the lawsuits a company may face from the federal government, cities and states are filing their own suits against companies that they feel don't take employee and customer privacy seriously[3]

Lost productivity

- Resolving identity theft can take up to hundreds of hours and six months of an employee's life[4]
- Missed work and increased distraction can quickly lead to disengagement, resulting in[5]:
  - 20 percent lower sales
  - 17 percent less productivity
  - 21 percent lower profitability
  - Between 24 and 59 percent higher turnover
  - 70 percent more employee safety incidents

Reputation damage and ability to attract and retain top talent

- Customers and prospective clients will likely consider working with the competition
- Failure to provide employee identity protection lessens a company's ability to attract and retain top talent
- 80 percent of employees prefer additional benefits and perks to a pay raise[6]

PrivacyArmor® Features HR Love

- A 90.1 Net Promoter Score (NPS)
- 97 percent implementation satisfaction rate
- 99 percent account management satisfaction rate
- 99 percent client retention
- Easy onboarding that includes comprehensive product education and a dedicated client relationship advisor
- Scalable and flexible payment models that minimize risk
- Expert customer service representatives based in the U.S.
- Accounts protected by two-factor authentication
- Proactive alerts that notify employees on applications for credit cards, wireless carriers, utility accounts, and more
- Monitoring of high-risk identity activity such as employee password resets, fund transfers, unauthorized account access, compromised credentials, and more
- Tools to monitor and preserve an employee's reputation across social networks
- A dedicated advocate to guide and manage an employee's full recovery process
- Identity theft insurance to cover your employee's lost wages, legal fees, medical records request fees, CPA fees, child care fees, and more

General identity theft statistics

- Identity theft has ranked in the top three FTC consumer complaints for 17 years straight[7]
- 40 percent of Americans have either been the victim of identity theft or know someone who has[8]
- Americans now rate criminal hacking as the number one threat to their health, safety, and prosperity[9]
- As a result of the Equifax data breach, 145.5 million Americans — around 80 percent of all working adults — had their personal data stolen[10]

Additional resources:

- Why Companies Should Care When Employees Have Their Identities Stolen
- Identity Protection Helps Attract, Retain, and Engage Employees
- By the Numbers: How Identity Theft Impacts Your Employees, Your Business, and the World
- The HR Guide to Employee Data Protection and Identity Theft Prevention

Sources:

1. Society for Human Resource Management
2. HR Hero
3. L.A. Times
4. The Economist
5. Gallup's State of the American Workplace 2017 Report
6. Glassdoor
7. Insurance Information Institute
8. CNBC
9. Dark Reading
10. The New York Times