



FAST FACTS

IAM and Security Statistics

- Identity Management improves security by reducing users with excessive or toxic privileges by as much as 60%. (Forrester Research, 2015)
- 76% of organizations were affected by a successful cyber attack in 2015 – up from 70% in 2014 and 62% in 2013. (Cyberthreat Defense Report, 2016)
- The average cost of a breach has risen to \$4 million per incident—up 29% since 2013. 59% in direct costs and 41% in indirect costs. (Ponemon Institute, 2016)
- The average cost per stolen record has grown to \$158. However, the cost in some industries is much higher, such as Healthcare (\$355), Education (\$246), Financial (\$221), and Retail (\$172). (Ponemon Institute, 2016)
- Organizations don't discover breaches until well after-the-fact. In 2015, the median number of days an organization was compromised before discovering the breach was 146. (Mandiant Consulting, 2016)
- Legitimate user credentials were used in most data breaches, with 63% involving weak, default, or stolen passwords. (Verizon DBIR, 2016)
- 43% of data loss was caused by internal actors, half of which is intentional, half accidental. (Intel Security Report, 2015)
- 65% of organizations are aware that their employees are using unsanctioned file sharing tools, with 60% citing a lack of visibility into what users are sharing and accessing as a top concern. (AIIM, 2016)
- 90% of ex-employees retain access to their former employers' software applications. Another 49% were shown to have logged into a company account after no longer working there. (Intermedia, 2014)

Yet, despite these facts...

- Nearly two thirds of organizations do not have well-defined and automated Identity and Access Management programs. (EY's Global Information Security Survey, 2015)

Looking to experience the benefits of modernizing your identity and access solution? If so please contact us at [877-221-8401](tel:877-221-8401) or sales@identityautomation.com to request a demo today.

IDENTITYAUTOMATION