Insecurity Issues: A survey of around 9,500 executives in 122 countries by PwC found 44% said they lack an overall information security strategy, 47% don’t mandate employee training on privacy policies and 49% don’t have an accurate inventory of personal data in their company’s possession. Fewer than a third of respondents said their board actively participates in security and privacy risk reviews; 39% expressed confidence their organization knows what it’s most sensitive and valuable digital assets are. “For CEOs and boards the existential question is less about the future of privacy and more about the future of their own organization: Will the company muster the will and imagination needed to jolt stalled privacy risk management into action?” the report said. “Will it leverage that momentum and integrate cybersecurity, striving to become a trusted brand for responsible innovation and data usage? Or will it cede its place in the market to more committed competitors?”

No Training: A survey of 1,600 U.S. small-business owners by online directory Manta found 47% said they don’t offer sexual-harassment training to their employees; three-fourths said they have formal sexual harassment policies in place.

ROI Invisible: A survey of 304 chief financial officers by professional services firm Grant Thornton found 41% said they don’t have good metrics to measure the return on their IT spending.

Hiring Priorities: A survey of 500 senior-level human resources executives by staffing and recruitment services firm Allegis Group found 37% said their organization includes diversity among its hiring goals, while 31% said their diversity goals include fairness in compensation.

Chain of Disruption: A survey of around 250 senior procurement executives by supply chain risk management firm Riskmethods found 47% said their company suffered between one and five severe supply chain disruptions in the past year; 13% reported 20 or more incidents.

Ransom Lessons: A survey of 1,200 IT security executives from 17 countries by security firm CyberEdge Group found 49% of the firms that suffered ransomware attacks and paid the ransom actually recovered their data, while 87% of those firms that refused to pay a ransom recovered their data.
**Inconsistent Response:** A survey of around 2,800 global IT and security professionals by IBM Security and Ponemon Institute found 77% said their organization doesn’t have an incident-response plan that is applied consistently across the company.

[Full Report](#)

**No Privileges:** A review of around 500 organizations globally by account management firm Thycotic found 64% said they don’t include privileged accounts and passwords to their access-control policies. Forty percent don’t do anything to identify privileged accounts and 55% don’t revoke access after an employee is terminated. (Same question throughout)

[Full Report](#)

**Analytics Analysis:** A survey of 1,500 chief audit executives world-wide by consultancy Protiviti found 76% of auditors in Europe and the Asia-Pacific region use data analytics in the audit process, while 63% of auditors in North America do so.

[Full Report](#)

**Not a Factor:** A survey of around 1,000 IT decision-makers by digital security company Gemalto found 61% admitted they still don’t mandate two-factor authentication to gain network access.

[Full Report](#)