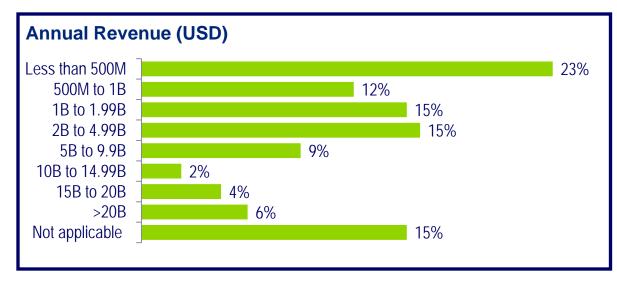
Deloitte.

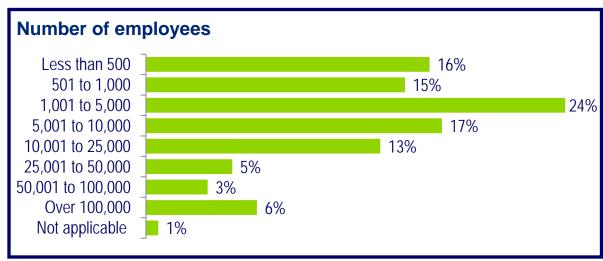
2010 Global TMT Security Study Bounce Back

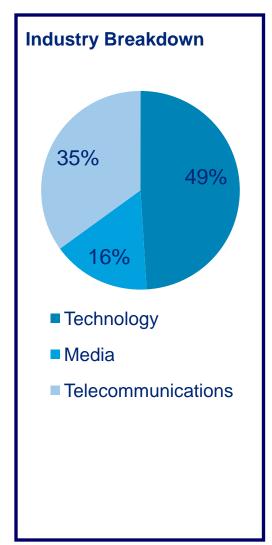


About the Study

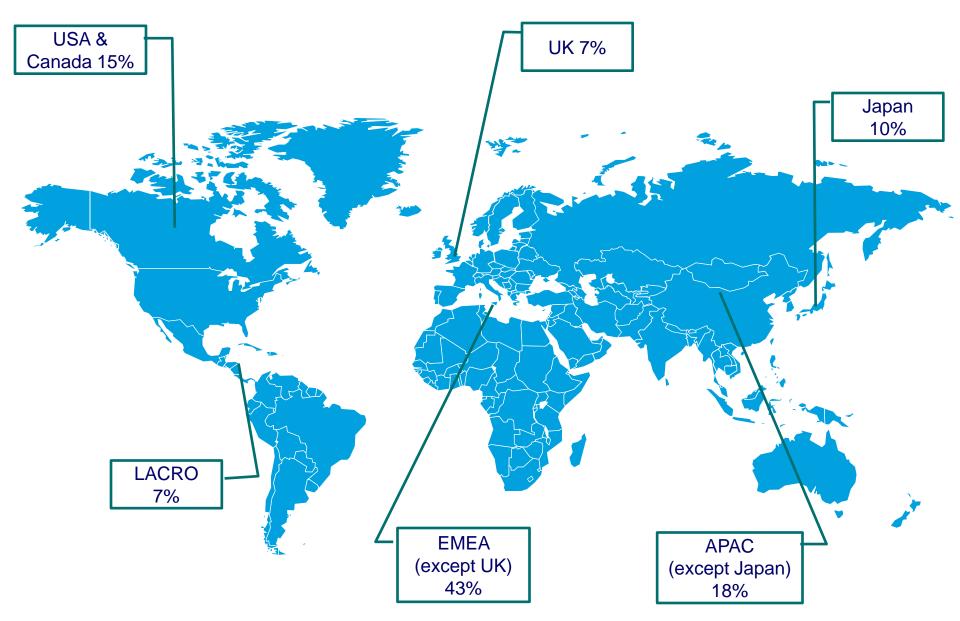
Participant profile







Participants by Region



Key Finding

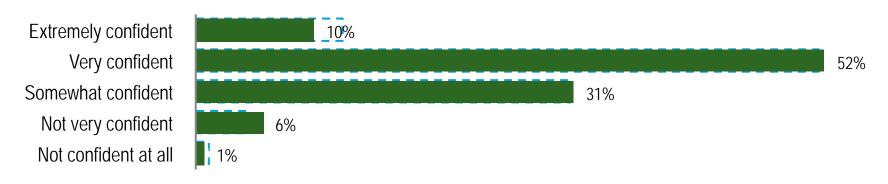
Bounce Back - Key finding

2. Cloud in the forecast

- Cloud computing could fundamentally change how IT Services are delivered
- Cloud computing may in many scenarios be a more efficient way to deliver and manage IT services
- But TMT organizations must address the security & privacy challenges

Confidence in the level of protection from an external attack

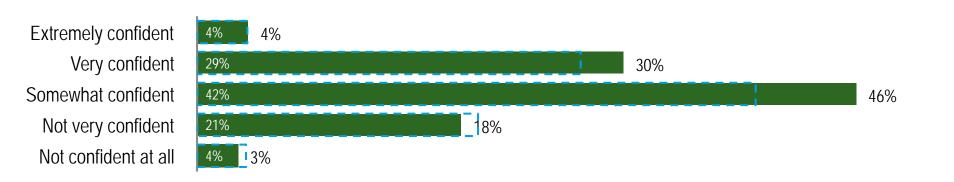
62% of respondents believe that their organizations are well protected against external attacks involving information systems. Another 31% is only somewhat confident.



7

Confidence in the level of protection from an internal attack

34% of respondents believe that their organization is protected against internal attacks involving information systems. Another 46% are somewhat confident, indicating that attacks originating internally are still a concern for organizations.



Dealing with third-party capabilities and dependencies

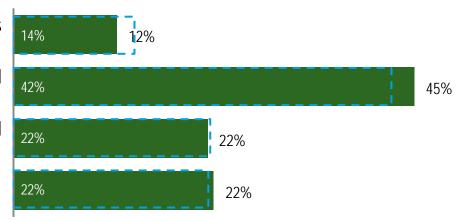
Third-party capabilities and dependencies should be reviewed and tested periodically to ensure these extended business relationships are delivering as promised. Yet only 22% of respondents do such reviews and testing on a regular basis.

Third-party security capabilities, controls and dependencies are unknown

Third-party security capabilities, controls and organizational dependencies have been identified

Third-party security capabilities, controls and organizational dependencies are regularly reviewed and tested

Not applicable / do not know



Ensuring that security practices of third parties are adequate

The top three methods are "Sign confidentiality / Non-disclosure agreements" (69%), "Address information security issues in the contract" (56%), and "Control what access third parties have to systems and data" (48%).

Sign confidentiality and/or Non Disclosure Agreements

Address information security issues in the contract

Control what access third parties have to systems and data

Impose organization's security policy and controls on third party

Identify risks related to third parties as part of information risk assessments

Require some form of independent attestation

Regularly monitor and review third party services

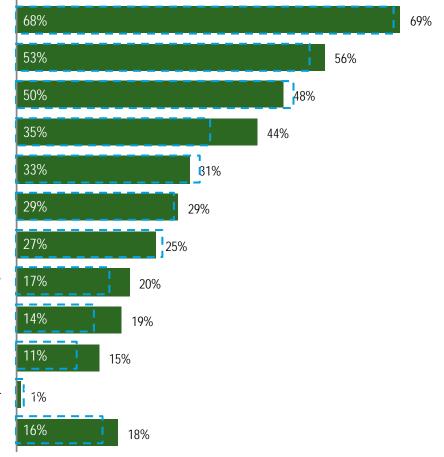
Where allowed, perform background verification checks on select high -risk, third party employees

Perform random spot checks of third parties' sites

Engage an independent third party to assess third parties' capabilities

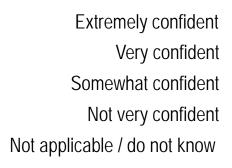
Other

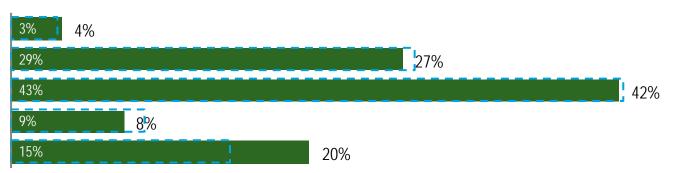
Not applicable / do not know



Confidence in third-party security practices

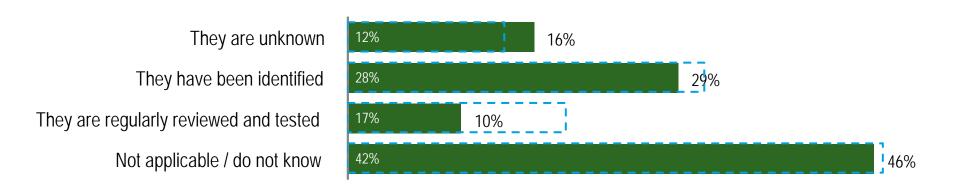
Only 27% of respondents are "Very confident" in their third parties' information security practices, while 50% of respondents are "Not very confident" or "Somewhat confident." Only a few technology companies (7%) are "Extremely confident" in their third parties' security practices.





Dealing with third-party business continuity management capabilities, controls, and organizational dependencies

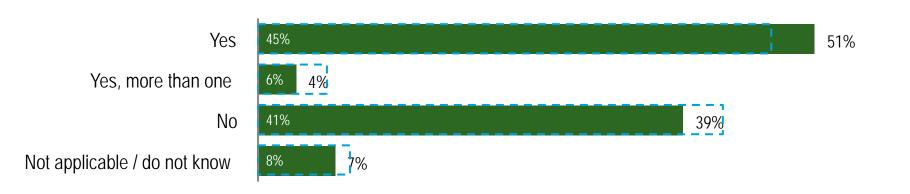
Third-party business continuity management capabilities, controls, and dependencies should be reviewed and tested periodically to ensure these extended business relationships are delivering as promised. Yet only 10% of TMT respondents do such reviews and testing on a regular basis, compared with 17% across all industries.



12 ©Deloitte

Presence of an executive responsible for privacy

This year's study shows that 51% of the technology, media, and telecommunications companies has appointed an executive responsible for privacy. The technology subindustry was most likely to have an executive responsible for privacy (56%).



13 ©Deloitte

Privacy program maturity

Almost one-fifth of respondents indicated that they have no privacy program in place. Almost one-third however indicate that a privacy program has been developed and is managing key initiatives. The state of privacy programs varies greatly per respondent.

No privacy program is in place

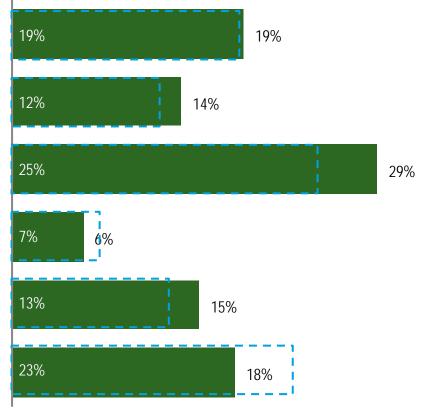
Privacy program is just starting to become staffed and organized

Privacy program has been developed and is managing key initiatives

Privacy program has been developed and is managing and measuring the effectiveness of key initiatives

Privacy program has been developed and is in maintenance mode focusing on program evaluation and continual improvement

Not applicable / do not know



Audit findings

Excessive access rights

Lack of sufficient segregation of duties

Excessive developers' access to production systems and data

Audit trails/logging issues

Lack of clean up of access rules following a transfer or termination

Lack of documented security policies and supporting guidelines and procedures

Business continuity and disaster recovery

Security policies and standards have not been operationalized

Use of production data in testing

Ineffective password management

Sharing of user IDs with a commonly known password

Lack of security awareness programs

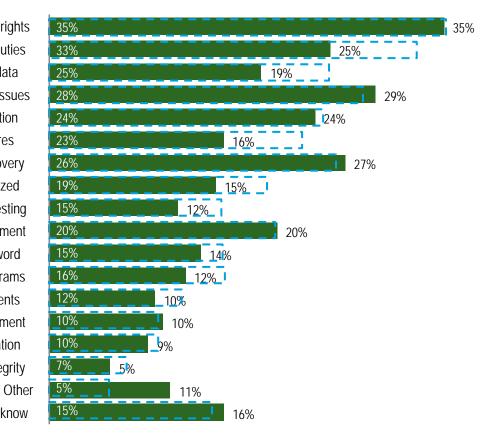
Lack of oversight and compliance to control requirements

Lack of separate testing environment

Lack of authorization of changes prior to implementation

Maintaining control environment integrity

Not applicable / do not know



Most common audit findings for TMT industry:

- 1. Excessive access rights
- 2. Audit trails/logging issues

Most common audit findings across all industries:

- Excessive access rights
- 2. Lack of sufficient segregation of duties

15 ©Deloitte

Contacts Details

Contact details

François Vergez: fvergez@deloitte.fr

www.deloitte.fr

Deloitte.