OTRS Spotlight:
Corporate Security 2023 | Singapore/Malaysia

Part 1: How security teams collaborate with others
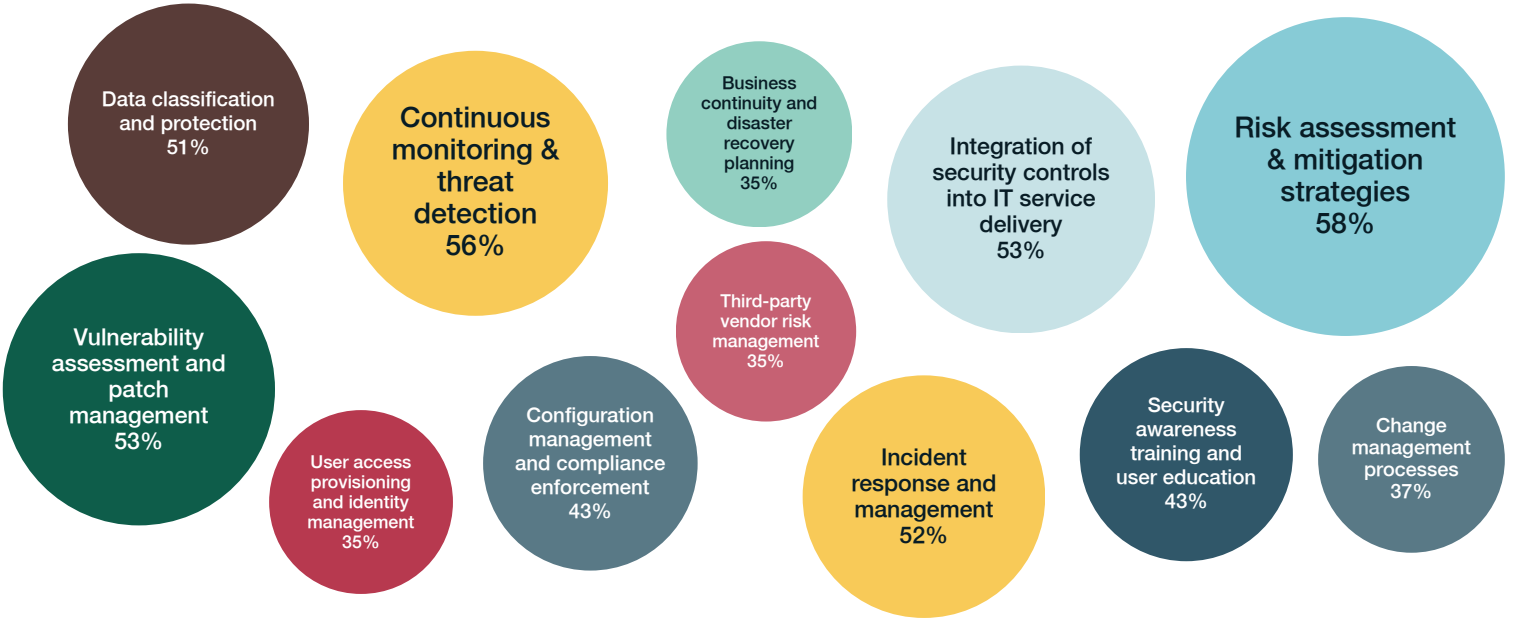
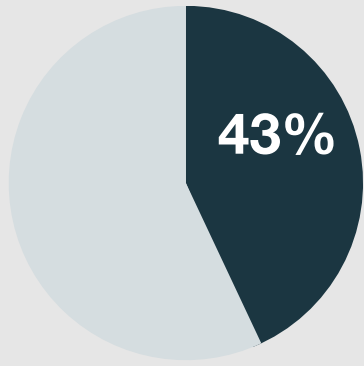**35%**

of IT and cyber security professionals rate the IT department as the most difficult to collaborate with on security initiatives.

Top most challenging departments to collaborate with on security initiatives:

Operations & production (40%)	IT (35%)	Marketing (25%)	Legal and compliance (24%)
	Finance & accounting (31%)	Customer support (24%)	Sales (23%)
Development/ Engineering (30%)	Research & development (28%)	Admin (27%)	Logistics (22%)	Office management (17%)
			Executive leadership (19%)	Human resources (16%)	Facility management (15%)
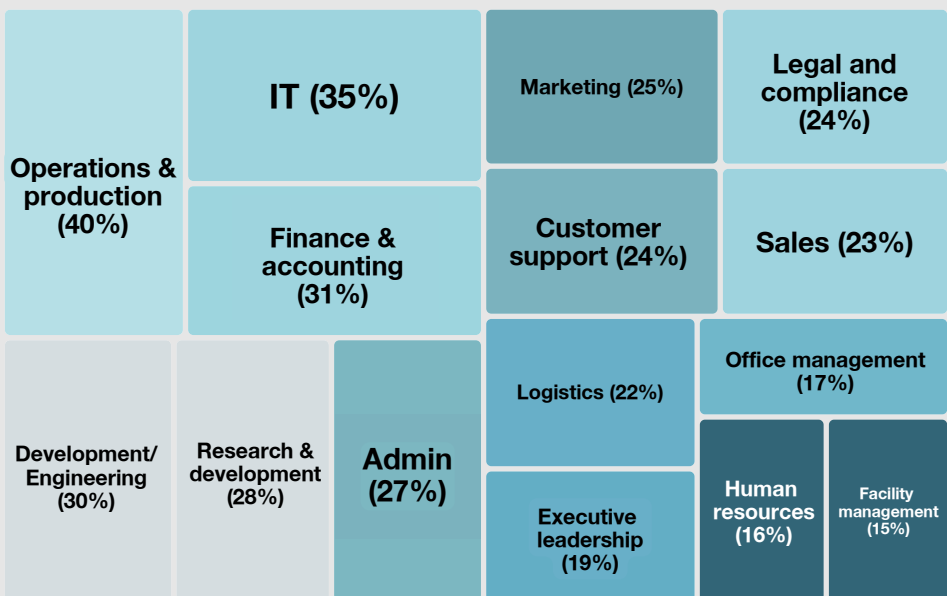
Areas in which IT and cyber security teams collaborate with ITSM most often:

- Data classification and protection 51%
- Continuous monitoring & threat detection 56%
- Business continuity and disaster recovery planning 35%
- Integration of security controls into IT service delivery 53%
- Risk assessment & mitigation strategies 58%
- Vulnerability assessment and patch management 53%
- Third-party vendor risk management 35%
- User access provisioning and identity management 35%
- Configuration management and compliance enforcement 43%
- Incident response and management 52%
- Security awareness training and user education 43%
- Change management processes 37%

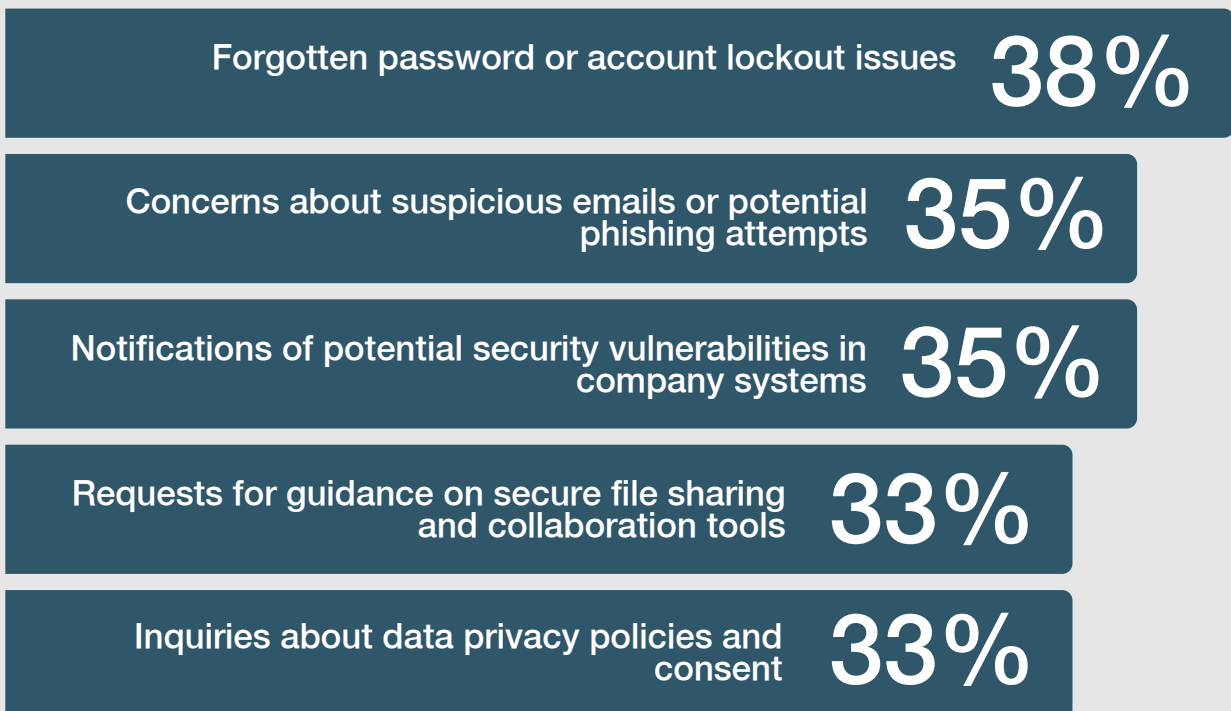**43%**

of IT and cybersecurity professionals already collaborate with ITSM on security awareness training and user education.

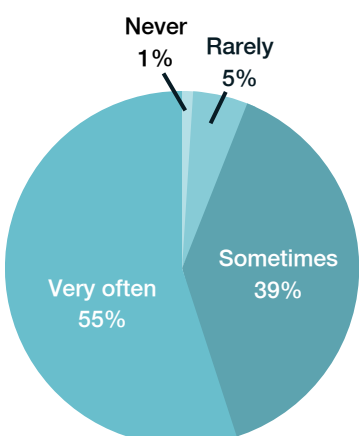Top important benefits of collaborating with ITSM:

Long-term stability and resilience of IT systems and services	27%
Improved risk assessment and mitigation strategies	25%
Early detection and prevention of threats	23%
Faster response times	23%

Issues that have caused organizations the biggest risk or damage in the past:

- Data privacy and consent issues 18%
- Unsecured file sharing and usage of collaboration tools 15%
- Unauthorized software or app downloads or updates 11%
- Vulnerabilities in corporate systems 10%
- Lack of multi-factor authentication (MFA) 9%

Top 5 most common types of complaints or requests related to IT security that security teams receive from users within their organization:

Forgotten password or account lockout issues	38%
Concerns about suspicious emails or potential phishing attempts	35%
Notifications of potential security vulnerabilities in company systems	35%
Requests for guidance on secure file sharing and collaboration tools	33%
Inquiries about data privacy policies and consent	33%

How often do you collaborate with ITSM teams to integrate security practices?

- Never 1%
- Rarely 5%
- Very often 55%
- Sometimes 39%

To work more effectively and increase overall security, many think their organization needs to invest more in …

- Software 34%
- Security awareness training 30%
- Infrastructure 23%
- Personnel 18%

OTRS