OTRS Spotlight: Corporate Security 2023 | U.S.
Part 1: How security teams collaborate with others

Top most challenging departments to collaborate with on security initiatives:

- Office management: 27%
- Executive leadership: 21%
- Operations & production: 24%
- Finance & accounting: 22%
- Human resources: 22%
- Marketing: 17%
- Sales: 17%
- Development/engineering: 12%

Integration of IT and cybersecurity professionals:

- 34% of IT and cyber security professionals rate the IT department as the most difficult to collaborate with on security initiatives.

Areas in which IT and cyber security teams collaborate with ITSM most often:

- Security awareness training & user education: 43%
- Vulnerability assessment & patch management: 42%
- Risk assessment & mitigation strategies: 39%
- Continuous monitoring & threat detection: 38%
- Data classification & protection: 37%
- Incident response & management: 34%
- Configuration management & compliance enforcement: 33%
- User access provisioning & identity management: 29%
- Business continuity & disaster recovery planning: 29%
- Change management processes: 28%
- Third-party vendor risk management: 24%
- Executive leadership: 27%
- Customer support: 25%
- Logistics: 19%
- Development: 18%
- Marketing: 17%
- Sales: 17%
- Admin: 12%

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

- Phishing emails: 10%
- Data privacy and consent issues: 13%
- Lost or stolen devices containing sensitive data: 15%
- Forgotten password/account lockout issues: 15%
- Vulnerabilities in corporate systems: 20%
- Reduced vulnerability management: 22%
- Security-conscious organizational culture through joint efforts in security training: 23%
- Early detection and prevention of potential incidents: 24%
- Improved overall organizational resilience: 33%

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

- Requests for assistance with setting up multi-factor authentication (MFA): 38%
- Concerns about suspicious emails or potential phishing attempts: 36%
- Concerns about the security of personal devices used for work: 33%
- Questions about the legitimacy of software or app downloads or updates: 31%
- Requests for guidance on secure file sharing and collaboration tools: 28%

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

- Never: 12%
- Rarely: 15%
- Sometimes: 21%
- Very often: 31%

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

- Personnel: 5%
- Software: 22%
- Security awareness training: 16%
- Infrastructure: 15%