Risk Insights Survey

2023 RESULTS REPORT

A Community Hivemind Project



Lansweeper

Context

Our first attempt at a peer-to-peer survey for Lansweeper Community, with the main goal of capturing peer-to-peer insights (hivemind) that we can share with the rest of our customer community,

WHAT

Lansweeper would like to survey our users about experiences with security and examples of challenges related to the following endpoint management, networking, security and database administration.

WHY

Our community might benefit from hearing how peers in other organizations approach security and measures they are adopting to mitigate risks. This initiative was part of the Cyber Security Awareness month.

A report on the results of the survey will be shared with all participants and the rest of the Lansweeper Community.

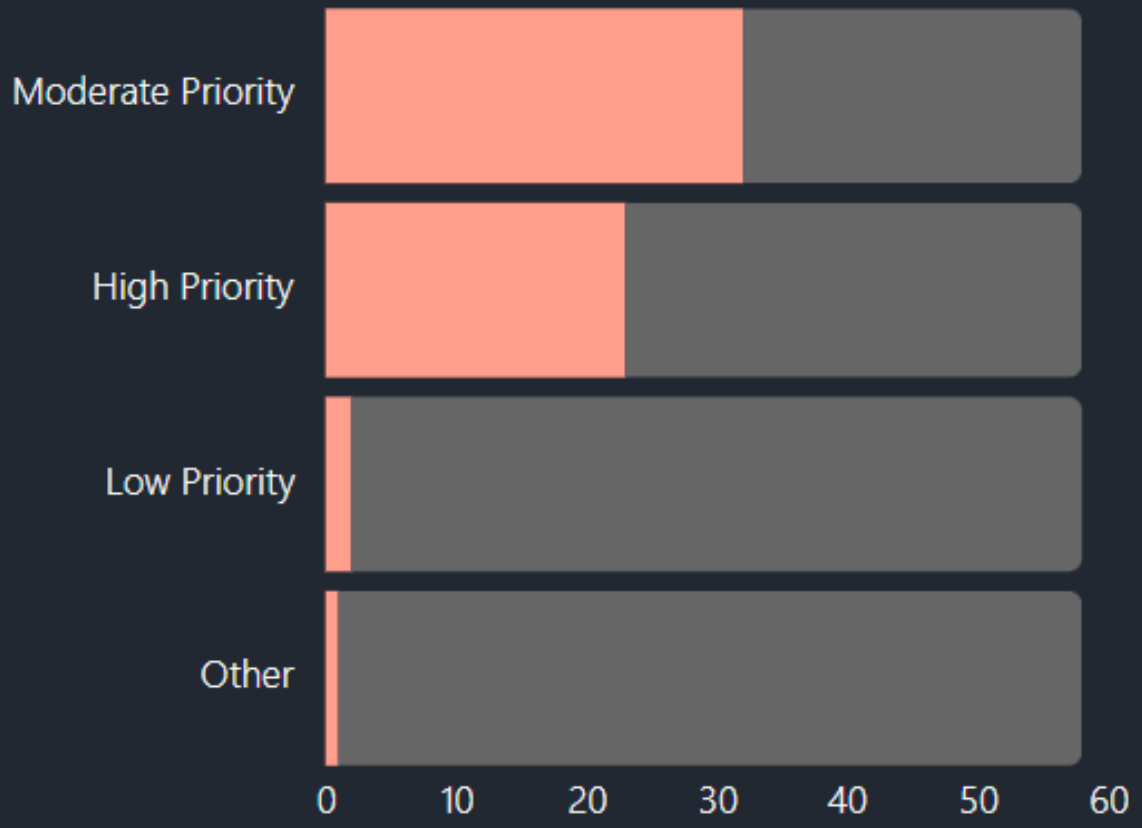
HOW

We created a "Security and Risk Trends 2023" mini survey and invited our Lansweeper community's members such as sys admins, network engineers, security managers and alike to participate in this survey.

The survey was open for participation with a duration of 3 weeks, between October 23 and November 11, 2023.

How do you prioritize security in your organization?

Results



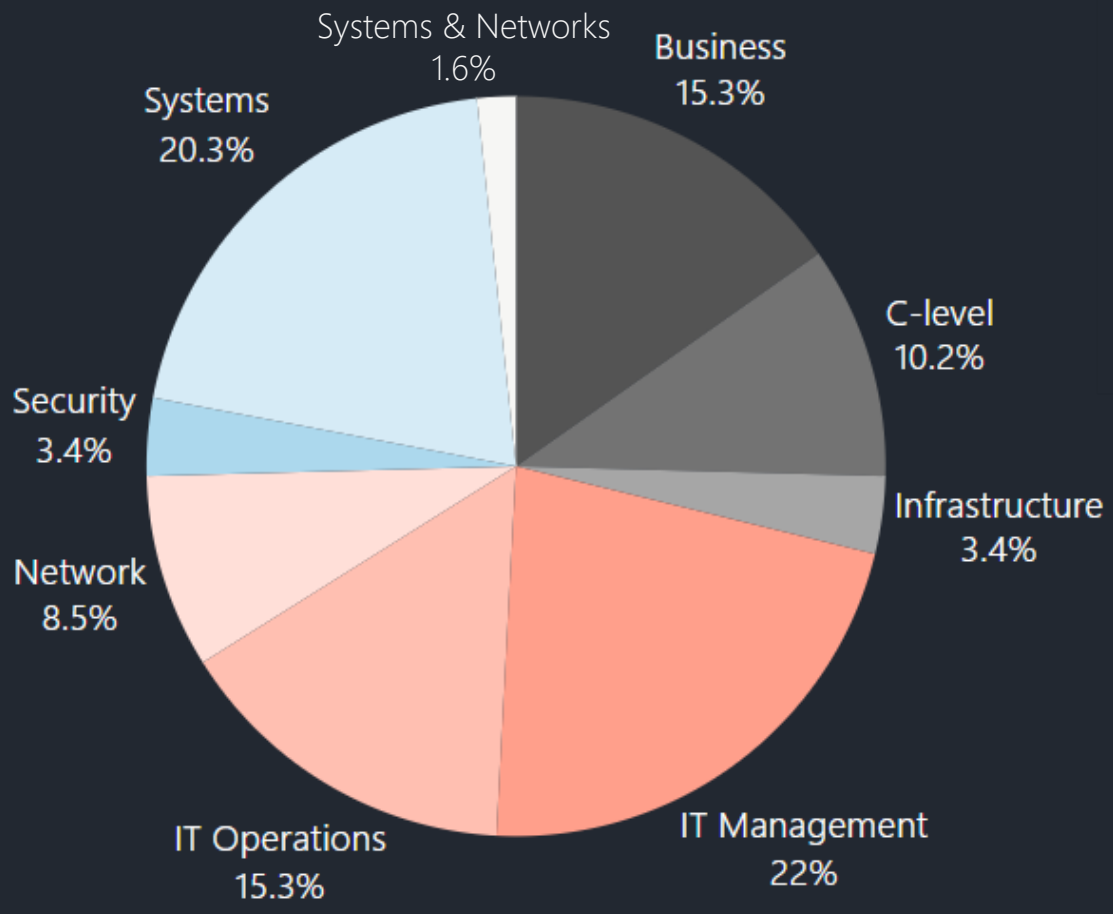
High Priority
A top concern, allocating significant resources.

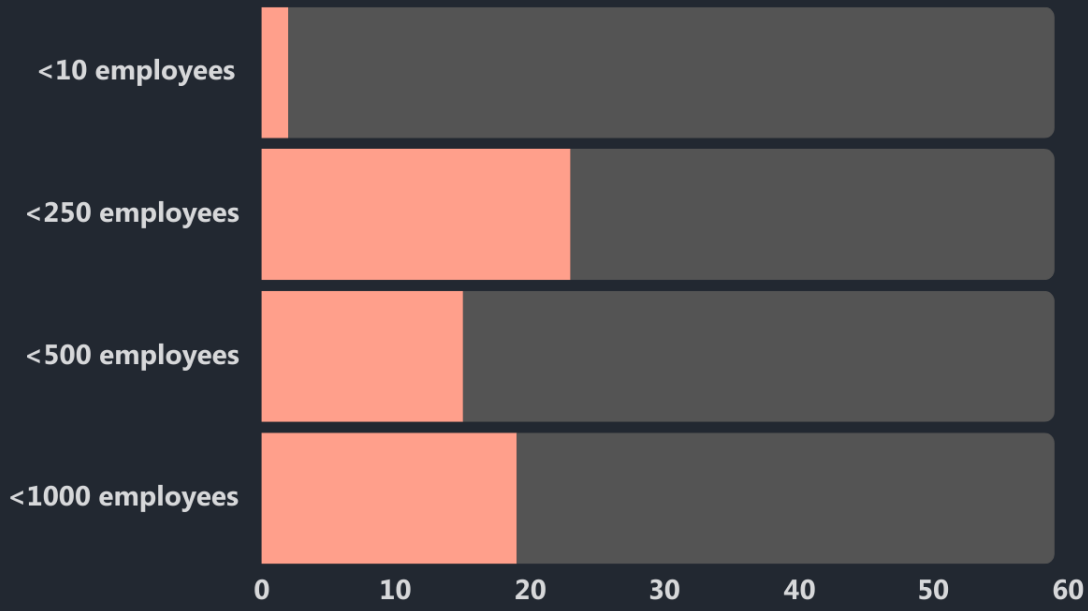
Moderate Priority
Important, resources are balanced with other priorities.

Low Priority
Not a primary focus, resources are limited.

59 Participants

Background





The majority of participants hold positions in IT management and IT system, which include roles such as IT Managers, System Administrators and System Engineers.

39% of participants work for SMEs (<250 employees), followed by 32.2% and 25.4% in large companies of 500 to 1000 employees respectively.

Lansweeper

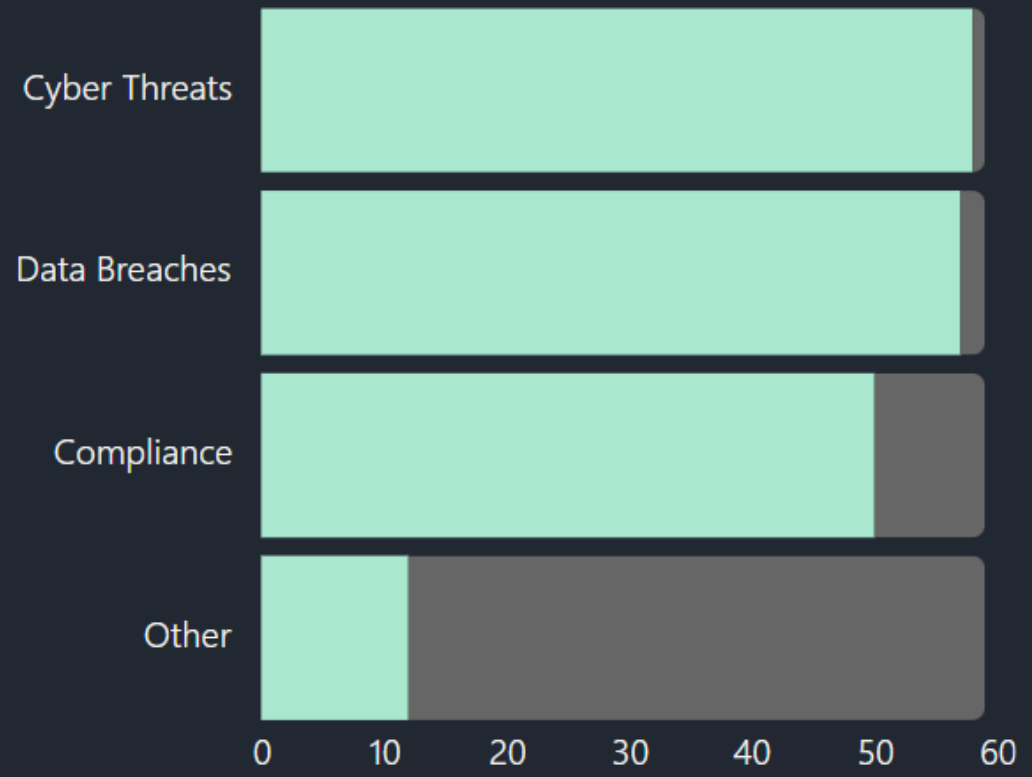
What are the top three challenges you face in this area?

Results

Cyber Threats
Dealing with malware, phishing, and other cybersecurity threats.

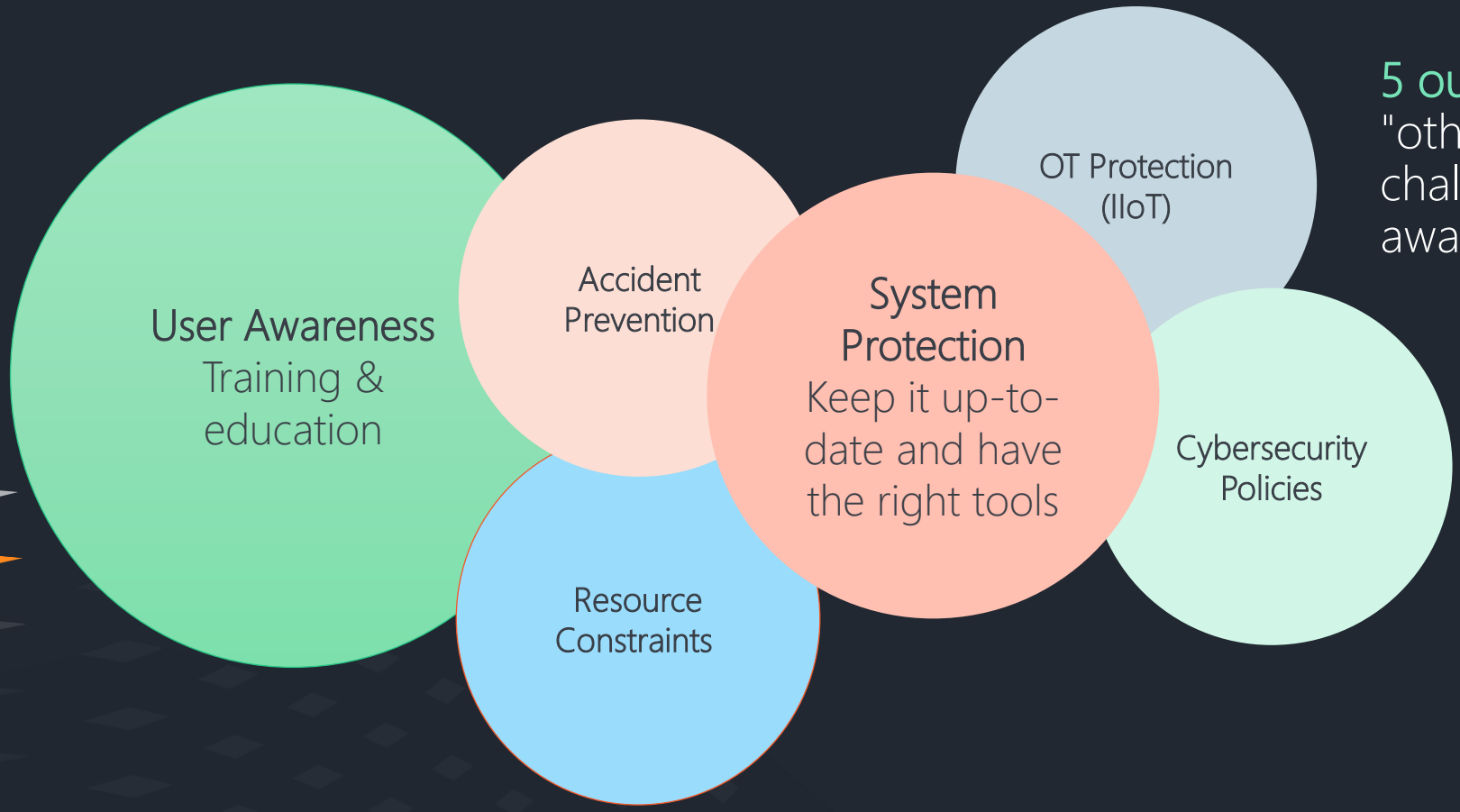
Data Breaches
Protecting sensitive data from unauthorized access.

Compliance
Meeting regulatory and industry security requirements.



What are the top three challenges you face in this area?

Results



5 out of 12 answers that specify "other" shared the same challenge in tackling user awareness.

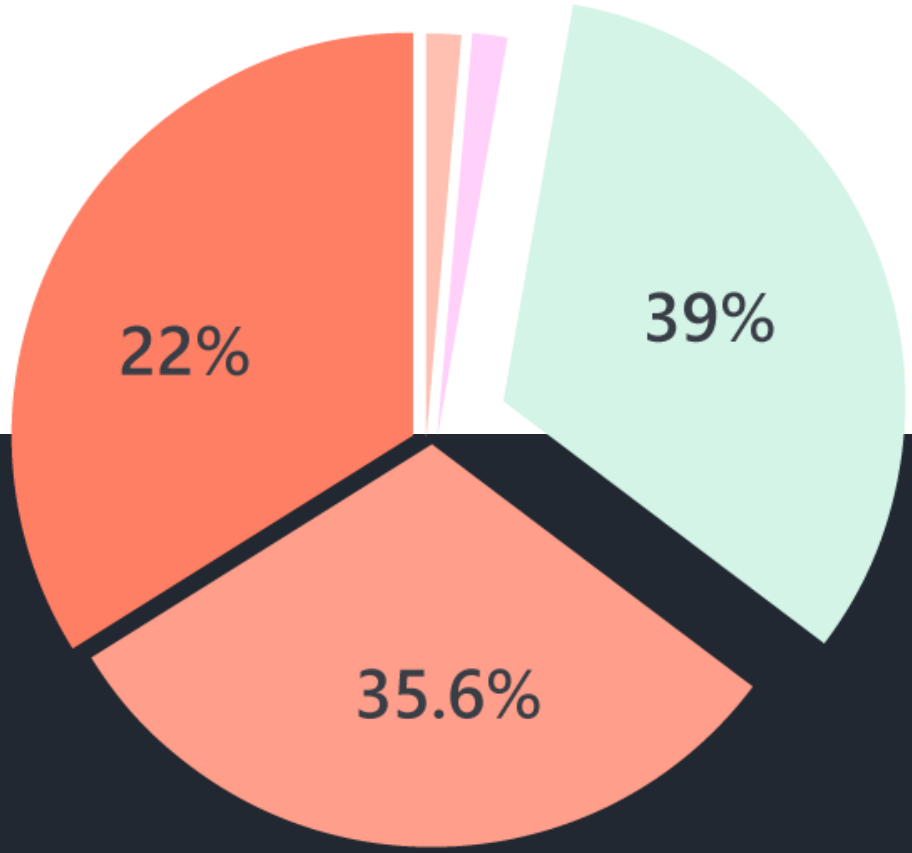
How do you monitor for potential vulnerabilities?

Results

- By staying alert and on top of trends: Tech news, forums, NHS Digital - Cyber Alerts, CISA, Vendor notifications, audits and reports from vendors
- By deploying a security stack – a mix of tools and software
- By investing in raising user awareness
- By having strict hardware configurations
- By having an in-house security team or an outsourced security operations center (SOC)
- Through firewall, endpoint protection (EPP), next-generation antivirus (NGAV) and network access control (NAC) approaches
- Through an intrusion detection system
- Through daily reporting
- Through OT & IT network scanning
- Through vulnerability assessments
- Through external penetration tests

How would you rate your organization's security posture compared to peers in similar sized businesses?

Results



39% of participants rated their security posture slightly better than peers in businesses of a similar size.

35.6% think they are about the same, while 22% are confident that their organizations have a stronger security posture.

Lansweeper

What security measures/tools have you adopted in the last year to mitigate risk?

Results

- Outsource security operations, such as a managed EDR or a third-party company
- Enforce a stricter admin-level access
- Remove older or end-of-life technologies
- Build firewall redundancy
- Use the security software's features better or more effectively
- Have a strong security culture (employee training or user education about phishing emails and cyber threats)
- Adopt the Extended Detection and Response (XDR) and Software-defined Wide Area Network (SD-WAN) approaches
- Implement Security Information and Event Management (SIEM) technology
- Implement Single Sign-on (SSO), Multi-Factor Authentication (MFA), conditional access
- Implement Privileged Access Management (PAM), an information security (infosec) mechanism

MEASURES

Lansweeper

What security measures/tools have you adopted in the last year to mitigate risk?

Results

- Perform security audits, encryption patching, OT scanning
- Perform deeper reporting from a security software mix of external and their own IDS solution
- Perform vulnerability assessments from EDR providers and Lansweeper
- Create network segmentation
- Deploy firewall technology with a next-generation firewall (NGFW)
- Use a Radius server or LAN
- Set up VPN (for office workers/engineers and IIoT assets)
- Remove admin rights from endpoint users
- Automate sandbox analysis
- Use cloud storage and have offline backups of servers
- Participate in Cybersecurity Safety Awareness training
- Implement additional anti-virus software
- Use Endpoint detection and response (EDR) cybersecurity solution

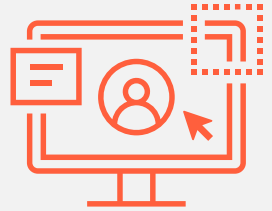
MEASURES

Lansweeper

What security measures/tools have you adopted in the last year to mitigate risk?

Results

- AlienVault
- Arctic Wolf
- Armis
- Avast
- Azure
- BatchPatch
- Bitdefender
- CommVault
- Crowdstrike
- Cryptospike
- CyberArk
- Darktrace
- Fing
- Fortinet (Fortinet Firewalls, FortiSASE)
- Kaspersky
- Lansweeper
- Microsoft Defender, LAPS
- Nessus
- Netwrix
- Ninja
- Okta
- PingCastle
- PRTG
- Qualys
- Rapid7
- Sentinel One XDR
- Sophos UTM, XDR
- Splunk
- Wazuh



TOOLS

How do you keep your team updated with the latest security best practices and are there any resources or platforms that you find particularly useful?

Results

Trusted Online Sources

Participants shared that they subscribe to newsletters, follow forums and news from companies they trust.

(CISA,NIST, Redmondmag, BleepingComputer, HackerNews, Heise Online, CIS benchmarks. CyberMAXX, Usecure io, Lansweeper)

Peers & Vendor Alerts

Another method indicated was having regular meetings and discussions to learn from others in their team or company, peers in the industry and through word of mouth.

Some rely on their vendors or partners to alert them of new trends or requirements. This is likely due to a lack of time and resources.

Training & courses.

E-learning is a popular choice amongst participants for expanding knowledge in security via platforms such as UDEMY, Cybrary and LinkedIn Learning.

Gratitude to all contributors who provided valuable insights through this survey to our community.

Lansweeper