panaseer

Panaseer Security Leader's Peer Report

Why poor visibility is hampering cybersecurity

Over the years the emphasis placed on cybersecurity has increased, placing security leaders and their functions at the heart of the modern enterprise. Amidst a fast-changing threat landscape, regulatory hurdles and limited budget and resources, many security leaders are understandably looking to improve their cybersecurity posture.

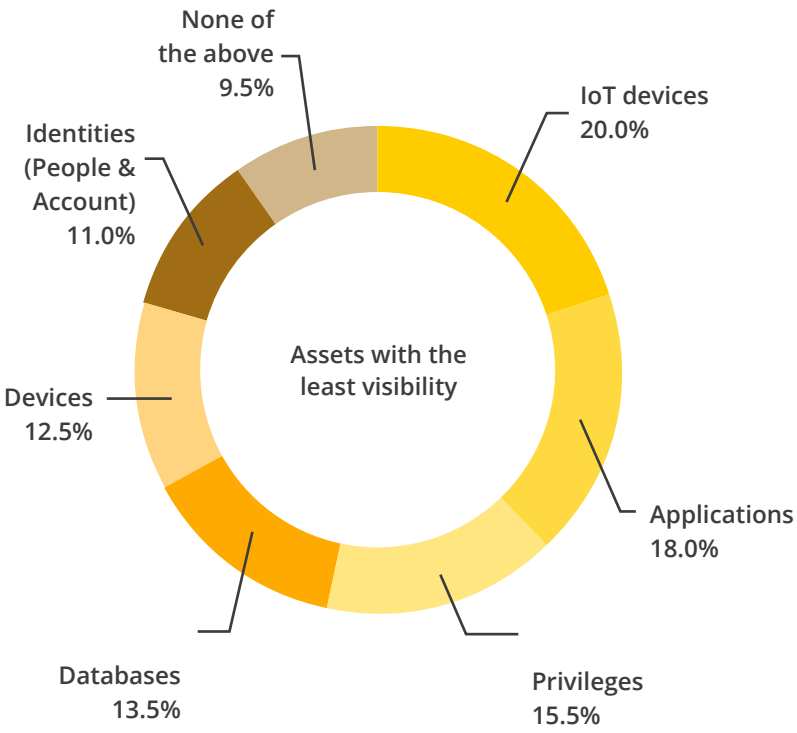
Panaseer commissioned Censuswide to conduct a survey of 200+ senior security leaders working in large enterprises to create a peer report with an objective to understand the issue that hamper cybersecurity posture in an organisation.

The results reveal that efforts to improve cybersecurity posture are being hamstrung because of a lack of visibility into technical assets and security controls — a problem exacerbated by the presence of too many tools (tool overload). Additionally, it is difficult to understand your cybersecurity posture without unified visibility and reporting.

In the dark

The cyber threat landscape is continuously evolving; organisations are bombarded with attempts to phish users, crack open privileged accounts and exploit software vulnerabilities. However, a lack of visibility of technical assets and lack of knowledge of where security controls are deployed leave the security leaders in the dark, making it difficult to understand the true cybersecurity posture of an organisation against the cyber threat landscapes. Also, identifying the right security metrics for cybersecurity and risk posture reporting becomes challenging without clear visibility.

When the security leaders were asked to rank the assets with least visibility, most of the leaders selected IoT, as seen from the ranking to the right:



IoT sensors and endpoints are built into a growing range of systems, including appliances inside the office - for example smart, IoT based, connected office lighting systems. The onus is on security leaders to ensure visibility across all assets including IoT.

70.5%

of organisations do not evaluate a security tool based on its impact on reducing cyber risk.

Tool overload

A common misconception indicates that investing in more security tools will lead to better visibility. However, visibility challenges are exacerbated by the sheer number of security tools in use. Survey results indicate:

55% of organisations have more than 50 tools.

More tools do not lead to improved visibility or help to achieve better reporting, in fact the opposite is true. Tool overload can hinder visibility, especially if the organisation has no way to gain centralised insight from its tools.

Addressing the tool overload issue will enable improved visibility, and the first step is to evaluate the tool's return on investments (ROI). It is interesting to note that, according to the results, **70.5% of organisations do not evaluate a security tool based on its impact on reducing cyber risk.**

Out of control

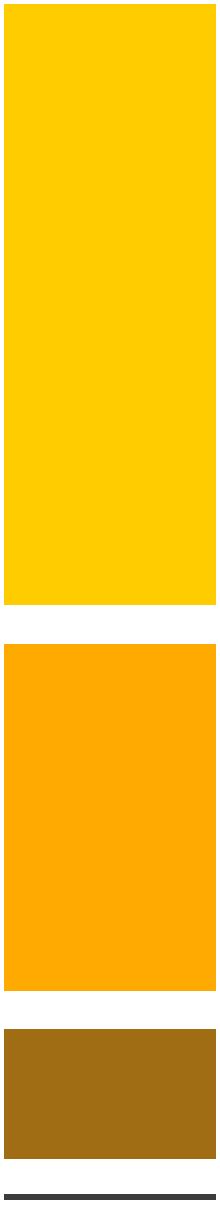
Lack of visibility also leads to lack of confidence in your cybersecurity posture. Without identifying all assets in the organisation, such as devices, applications, people and data, it is difficult to understand if security controls are performing as expected.

Complex and fragmented IT environments have compounded the visibility challenges for security teams. It is no wonder that the survey results indicate that:

89% of large enterprises have concerns based on lack of visibility and insight into trusted data.

Ranked from least to most, the survey results point to security control areas that the security leaders have least confidence in:

- Phishing and user awareness testing 16.50%
- Endpoint Management 14.50%
- Identity & Access Management 14.50%
- Privileged Access Management 13.00%
- Vulnerability Management 12.00%
- Patch Management 10.50%
- Application Security 9.50%
- I am confident in all security areas 9.50%



Metrics deficit

Lack of visibility also ties in with issues around lack of trusted security metrics. In most organisations, security data is either unavailable or not up-to-date; the onus is on the security and IT teams to collect and collate data to report on the overall cybersecurity posture. Also, there is a requirement to report on security projects and initiatives to highlight progress and indicate return on investment (ROI).

Survey results indicate that the key drivers for security initiatives are:

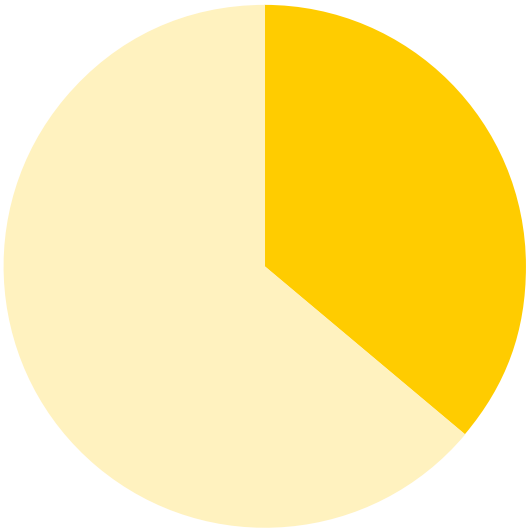
External factors = 55.50%
Internal factors = 32.00%
No driver = 12.00%
Others = 0.50%

Most of the security initiatives are driven by external factors such as regulations and audit points, and internal factors such as board driven initiatives. Since they all involve high-level stakeholders, it is the responsibility of senior security leaders to ensure that the security reports created by the security and IT teams are based on trusted data.

However, this has become one of the biggest pain-points for security leaders. Without clear visibility and insight into technical assets and security controls coverage, security leaders can't be confident about the trustworthiness of their data. They risk wasting time on inefficient manual data collection processes which are incomplete, not up-to-date and provide only siloed assessments.

Survey results indicate that:

36.26% of a security team's time is spent on reporting

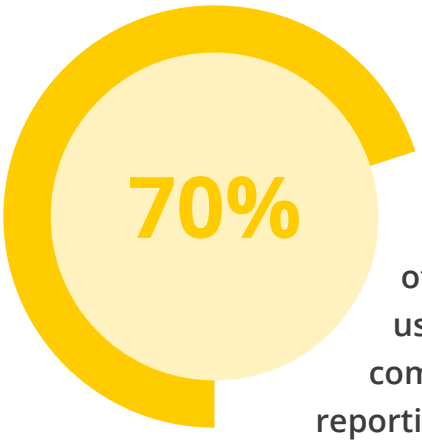


which includes extracting, moving, cleaning and merging data, as well as making, formatting and presenting calculations.

Security leaders are concerned that the productivity of their team is adversely impacted because of time spent on reporting.

Additionally, manual reporting seems to be a common pain-point across most organisations.

Survey results indicate that:



of organisations use manually compiled data for reporting to the Board.

The Last Word

Research conducted for the security leaders peer review report indicates that lack of visibility is a common issue that impedes improvement to cybersecurity posture in an organisation. The need of the hour is to unify security and IT data from different lines of an organisation to get a holistic, real-time view of cybersecurity posture. This is easier said than done - automating data unification to monitor controls and measure their performance continuously will pave the way for improved visibility.

Cybersecurity posture cannot be improved by just addressing security issues and reducing risk; it is important to measure and sustain the risk reduction by continuously monitoring controls and ensuring that they're performing as expected.

If you would like to know more on how to improve your cybersecurity posture, drop us a line at success@panaseer.com