THE SECURITY DISCONNECT

In a recent survey, Wind River found a significant disconnect between what business executives perceive is happening around security issues and what is actually being implemented in their organizations. Take a look at the survey results below, along with some key takeaways.

1 BIGGEST SECURITY THREAT

40% of executives believe that stolen credentials pose the biggest threat.

63% of managers & **59%** of individual contributors believe that device failure or takeover poses the biggest threat.

*KEY INSIGHT: Executives might be more concerned with loss of credentials, stolen information, and the bad press that accompanies this type breach.

2 DESIGN-IN SECURITY CONSIDERATIONS

Only **22%** of respondents consider protecting data in motion a top design-in security concern, while **14%** consider protecting data at rest as their top design-in worry.

*KEY INSIGHT: New regulations mandate greater security for protecting data.

3 RELEVANT SECURITY PRACTICES

57% of executives think their teams are actively monitoring vulnerability announcements, while only **32%** of individual contributors think this is important.

*KEY INSIGHT: Security is an ongoing effort throughout the lifecycle of devices. Teams must actively monitor all threat announcements.

4 SECURITY TESTING

65% of executives believe that their organizations use simulation tools to inject faults,

VS **35%** of individual contributors who say that they actually use simulation tools.

With **17,000 +** vulnerabilities happening per year, it is unlikely that a breach has not happened. More simulated threat tests should be employed in-house.

*KEY INSIGHT: Security testing is still mostly manual. New, more modern approaches to automating this testing can increase frequency and quality.

5 HANDLING SECURITY UPDATES

SHOCK! **11%** of executives and individual contributors **don't do** any security updates at all.

*KEY INSIGHT: Performing regular updates is the only way to maintain security for embedded systems.

6 TYPE OF OPERATING SYSTEM

62% of executives believe that using a real time operating system (RTOS) achieves security goals versus either Linux or Windows.

NOT A SINGLE EXECUTIVE surveyed said enterprise Linux fulfilled their security need.

*KEY INSIGHT: Every design requires a unique set of security features to meet industry requirements. VxWorks comes with many security features built in.

7 ROADBLOCKS TO SECURING DEVICES

25% of individual contributors believe they lack in-house expertise.

*KEY INSIGHT: Teams can augment their security gaps with experts who have deep industry experience, such as Wind River Professional Services.

8 AI'S ROLE IN SECURING EMBEDDED SYSTEMS

THE DISCONNECT

74% of executives say that AI will play a role in their embedded devices,

VS **60%** of individual contributors say that their company has no current plans to use AI at all.

*KEY INSIGHT: AI will play a greater role in future designs, but it is much harder to implement in current design methodologies.

IN SUMMARY

Security disconnects can be prevented with an agreed-upon security policy. Wind River can assist companies with building a security policy to meet the unique requirements of any device or system deploying into a variety of operational environments.

APPLICABLE INDUSTRIES

Automotive • Telecom • Aerospace • Energy • Robotics
Medical • Defense • Industrial • Many Others

Visit **www.windriver.com/secure-now/** to learn more.

WIND