ElectronicDesign.

Ensuring Security on Embedded Devices

Table of Contents

Table of Contents (continued)

Introduction & Methodology

OVERVIEW

Methodology, data collection and analysis by Electronic Design on behalf of Wind River Systems. Data collected June 8 through 28, 2020.

Methodology conforms to accepted marketing research methods, practices and procedures.

METHODOLOGY

On June 8, 2020, Endeavor Business Media emailed invitations to participate in an online survey to users of Electronic Design.

By June 28, 2020, Endeavor had received 147 completed, qualified surveys.

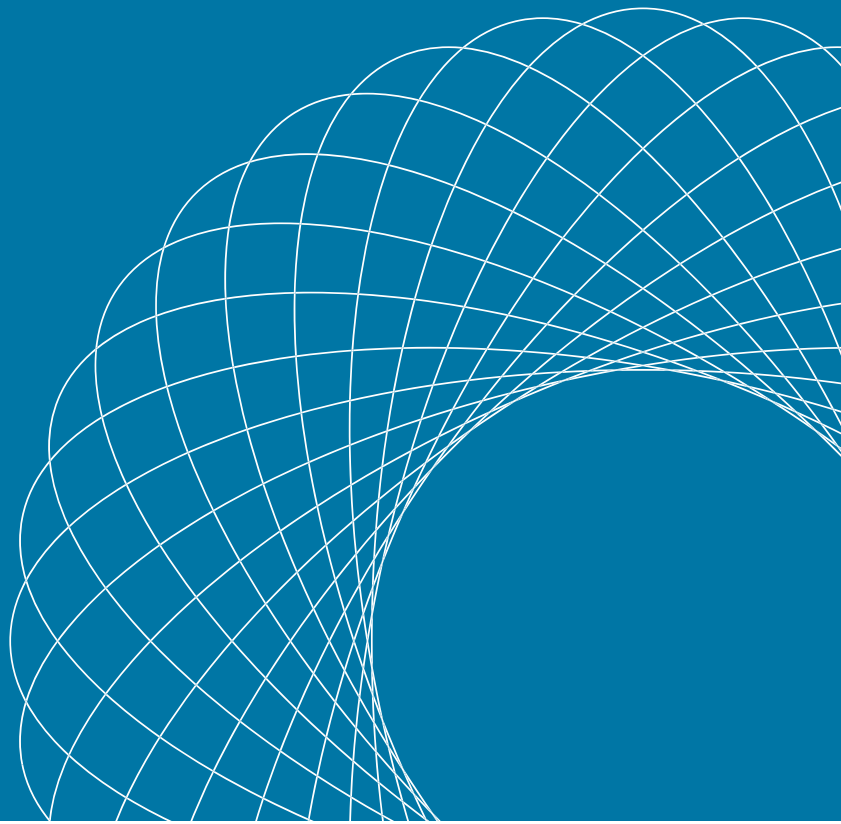
RESPONSIVE MOTIVATION

To encourage prompt response and increase the response rate overall, a live link to the survey was included in the email invitation to route respondents directly to the online survey.

The invitations and survey were branded with the *Electronic Design* logo in an effort to capitalize on user affinity for this valued brand.

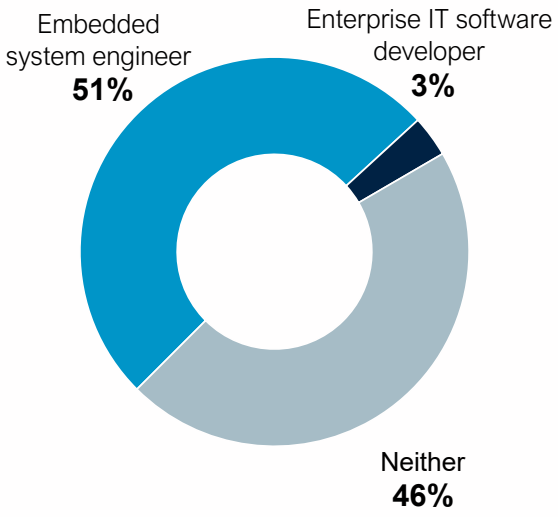
Each respondent was afforded the opportunity to enter a drawing for one of four $100 Visa gift cards.

Respondent Profile



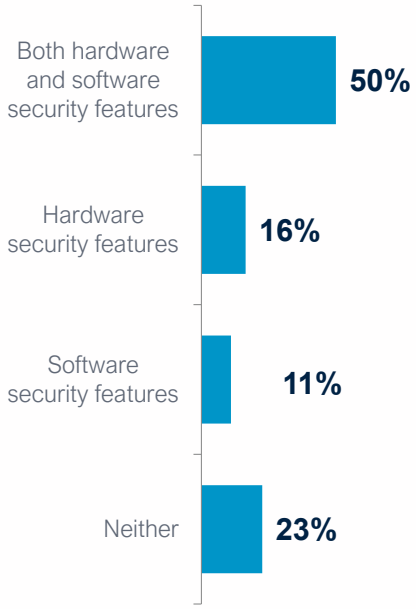
Job Function and Role

Over half of respondents consider themselves an embedded system engineer. Half are focused on both hardware and software security features. Fifty-seven percent of respondents are manager level or above.



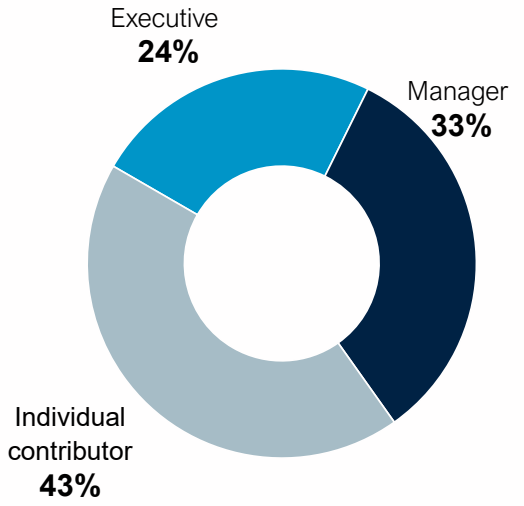
Question: Which do you consider yourself?

Base: All respondents (n=146).



Question: Are you focused on hardware or software security features?

Base: All respondents (n=146).

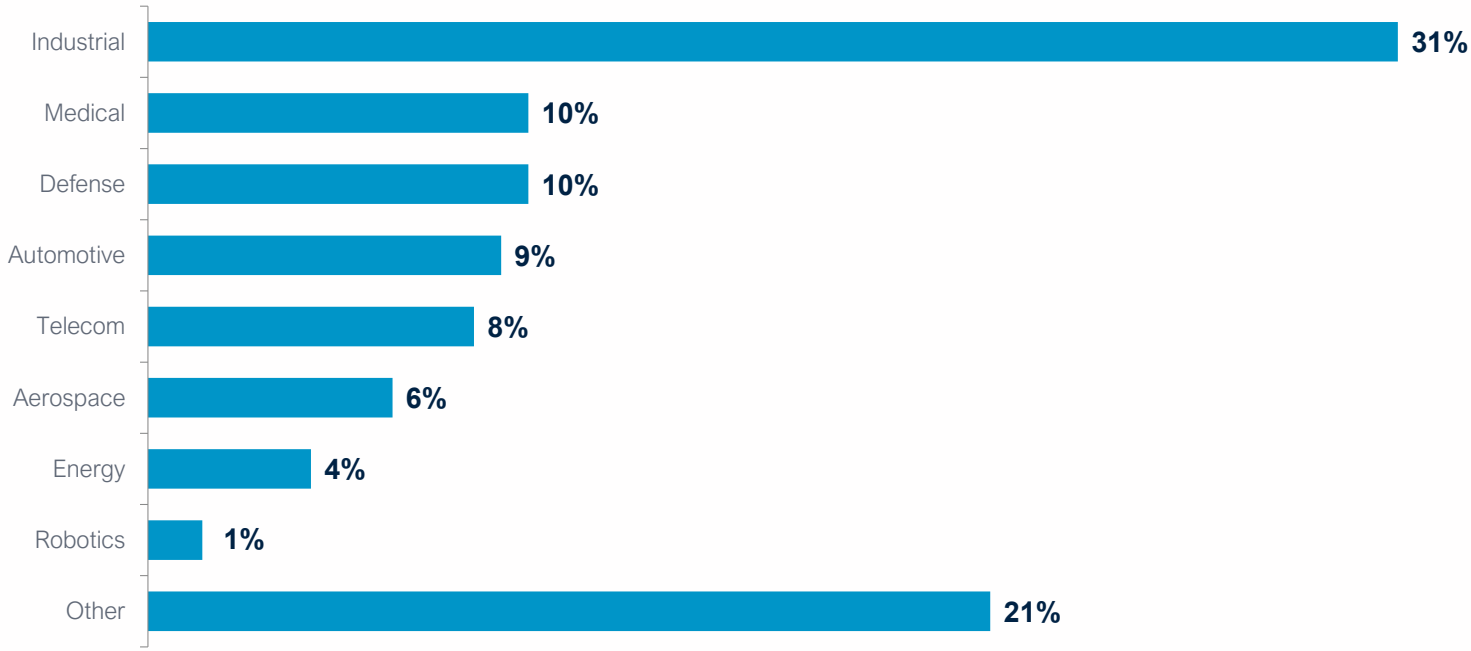


Question: Which of the following best describes your role within your organization?

Base: All respondents (n=146).

Industry

Respondents represent a variety of industries.

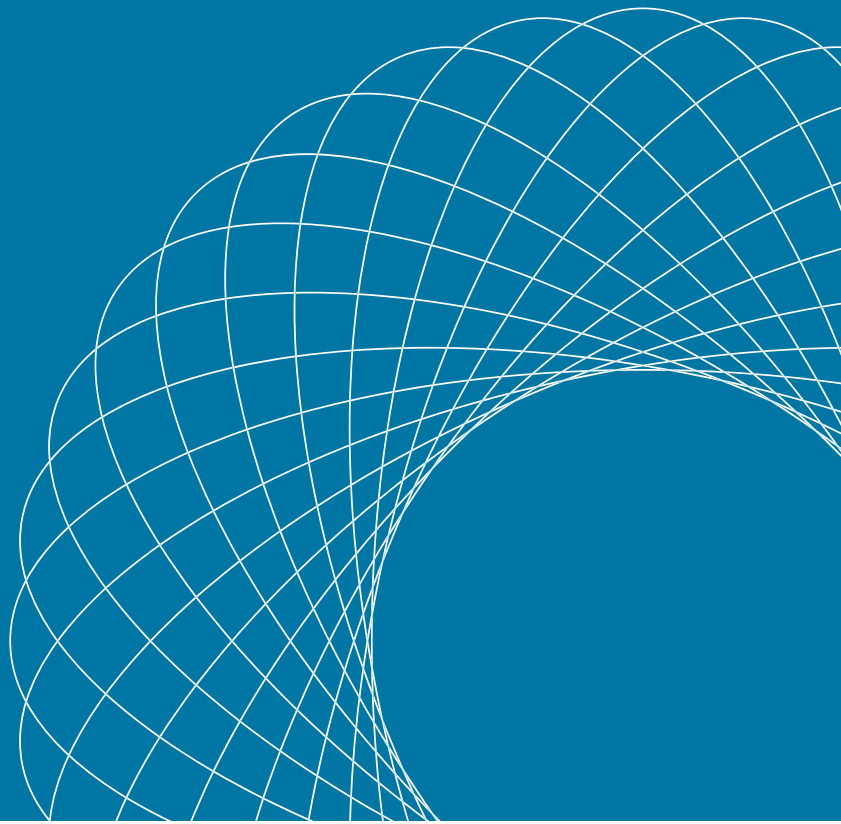


Question: Which industry do you represent?

Base: All respondents (n=147).

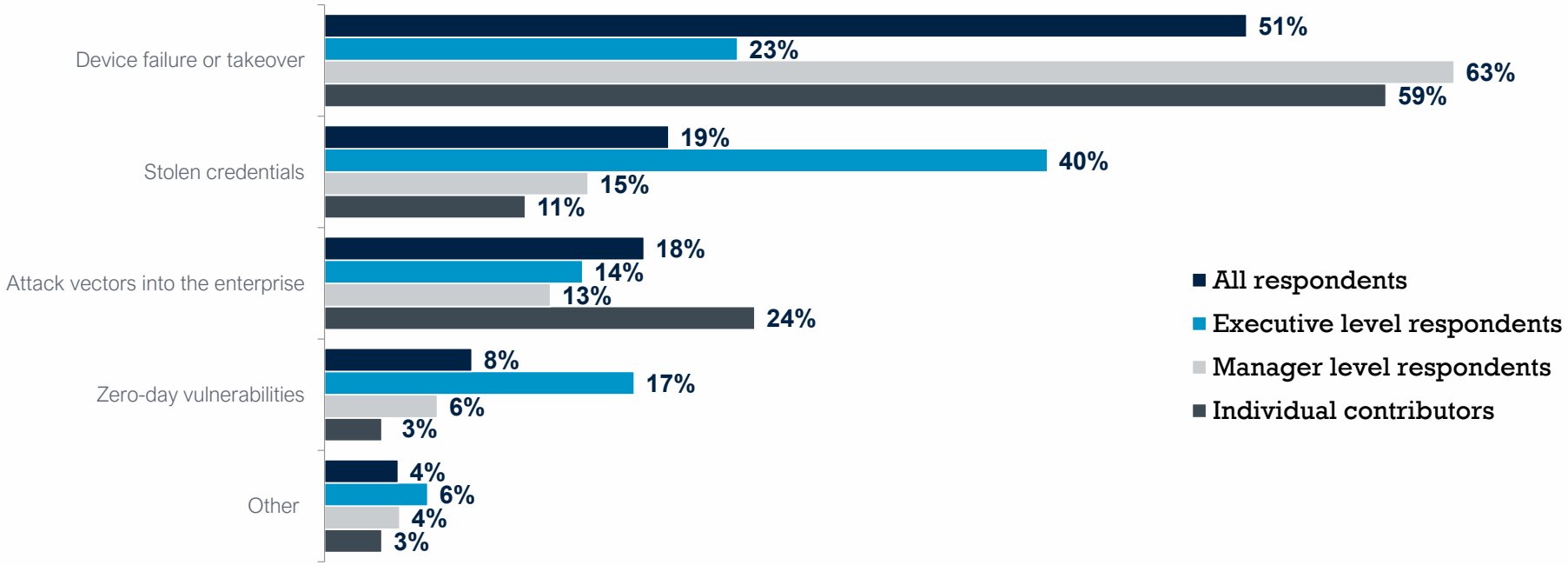
ElectronicDesign.

Key Findings



Biggest Security Threat

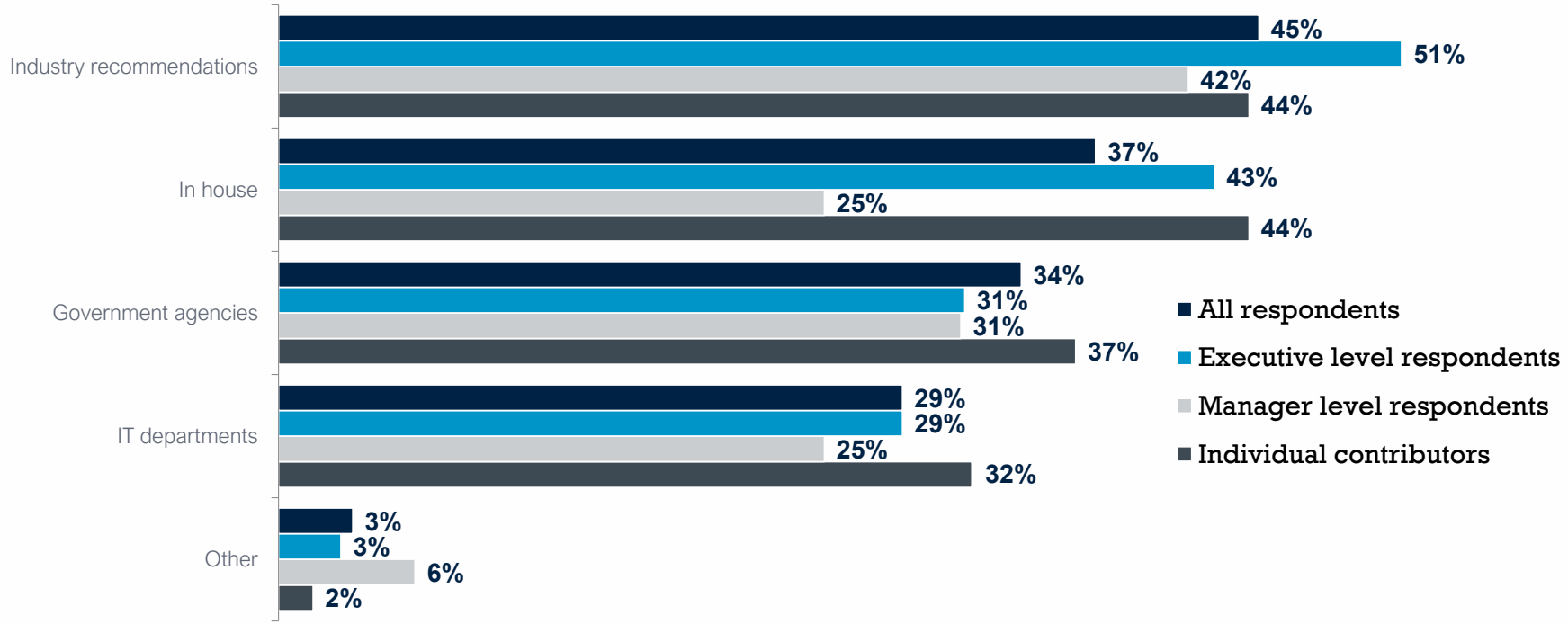
Respondents consider the biggest security threat to be device failure or takeover. Executive level respondents are most concerned with stolen credentials.



Question: What is the biggest security threat facing your industry?
Base: All respondents (n=147).

Source of Security Requirements

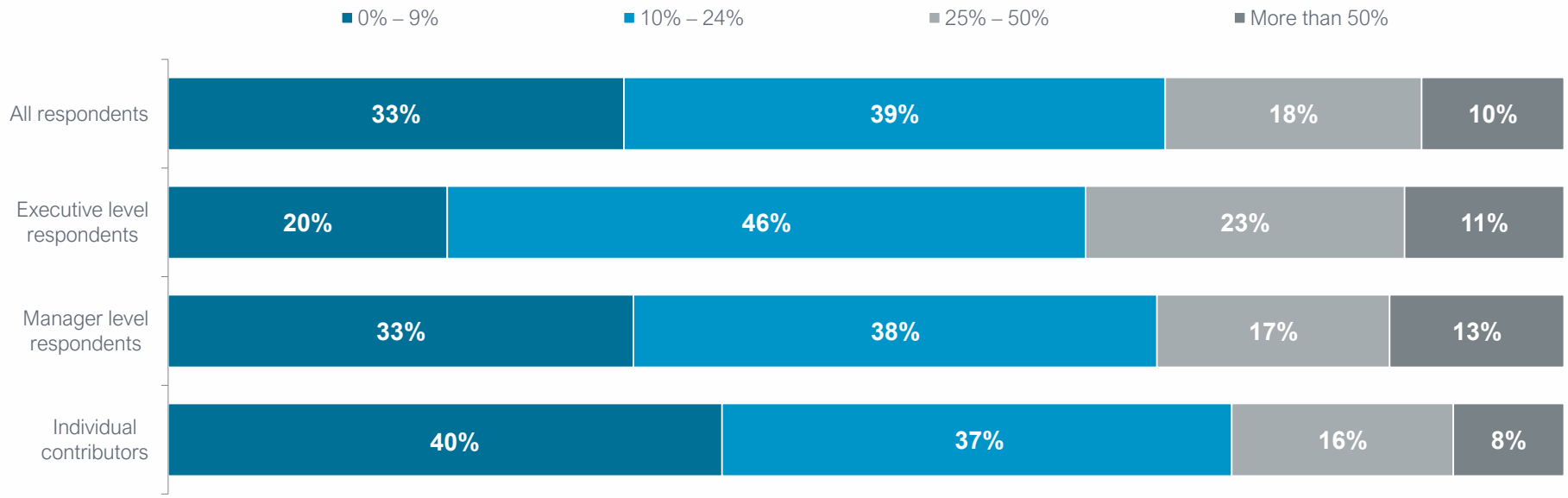
Security requirements are most likely to come from industry recommendations. In house recommendations and government agency recommendations are each used by one third of respondents.



Question: Where are most of your security requirements coming from?
Base: All respondents (n=147). Multiple answers allowed.

Focus on CVE

Respondents are likely to indicate a significant percentage of their organization's focus is on security features and ongoing common vulnerabilities and exposures. Executive level respondents report a higher percentage of their organization's focus on security features and CVE.

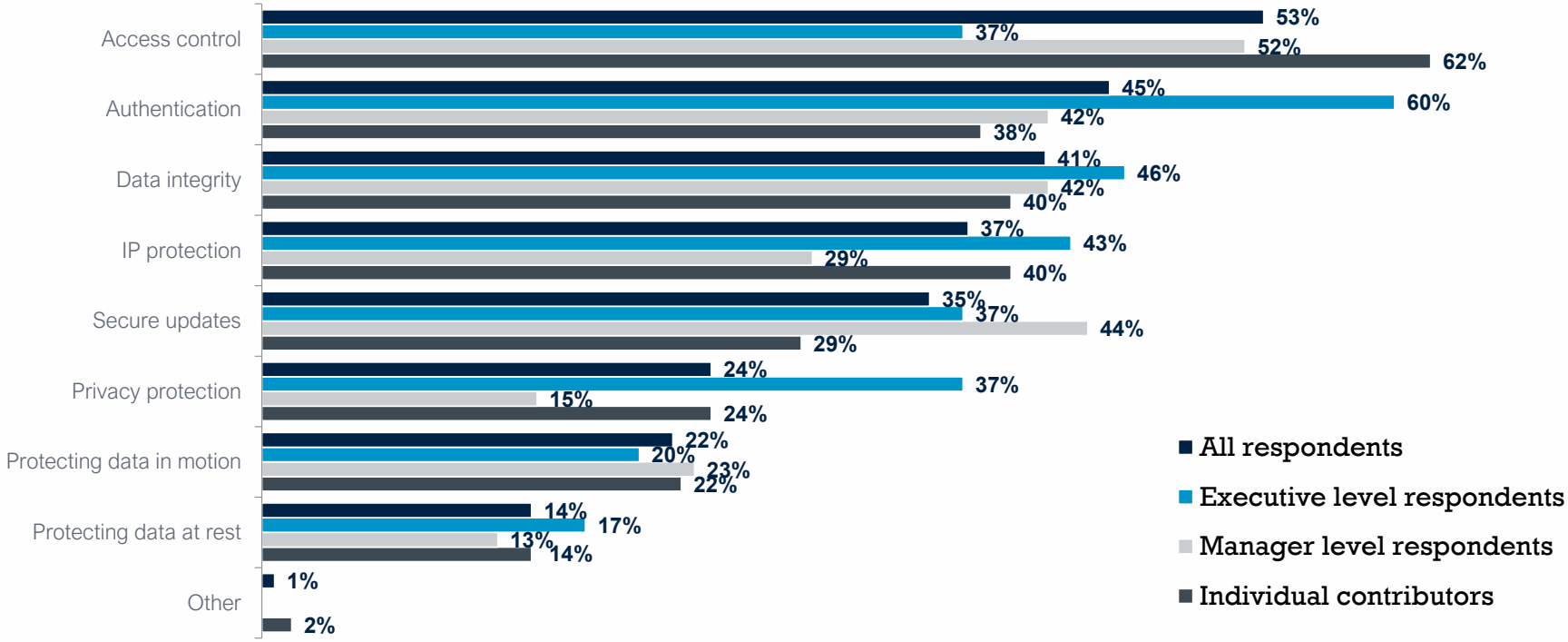


Question: What percentage of your organization's focus would you say is on security features and ongoing common vulnerabilities and exposures (CVE)?

Base: All respondents (n = 147).

Design-In Security Considerations

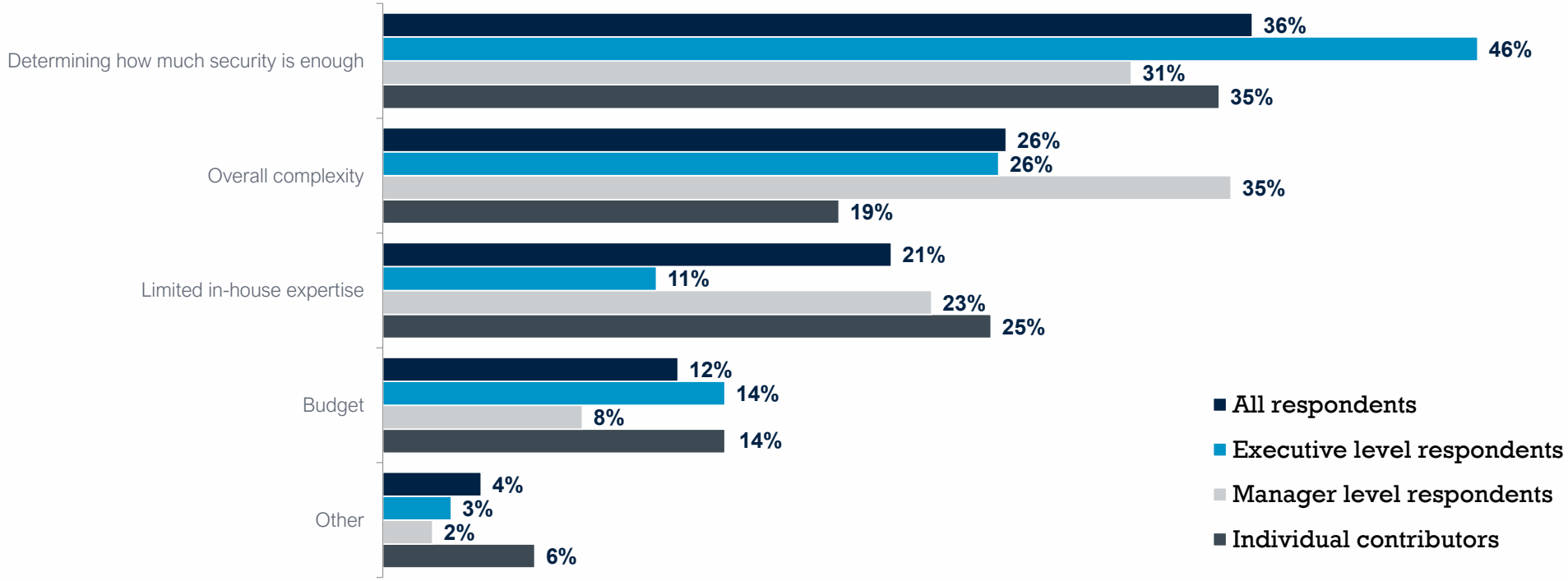
Access control, authentication, and data integrity are the three most important design-in security considerations. The important considerations vary by job level. These findings support the biggest security threats found on page 9.



Question: What are the three most important design-in security considerations?
Base: All respondents (n=147). Up to three answers allowed.

Primary Security Roadblock

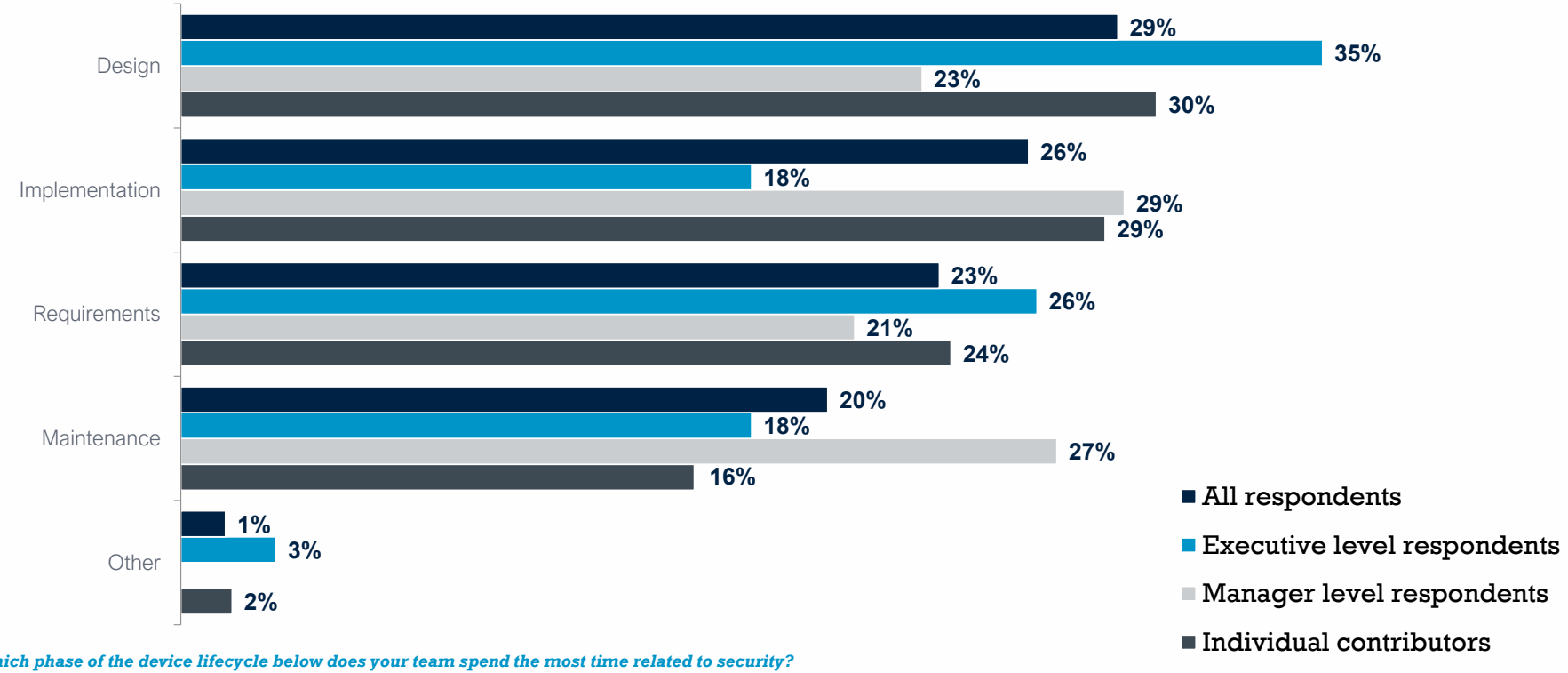
Respondents have varying opinions on the primary roadblock in securing devices. Executive level respondents are likely to believe determining how much security is enough as the primary roadblock. Manager level respondents believe overall complexity is the primary roadblock.



Question: What is the primary roadblock in securing your device?
Base: All respondents (n=146).

Device Lifecycle

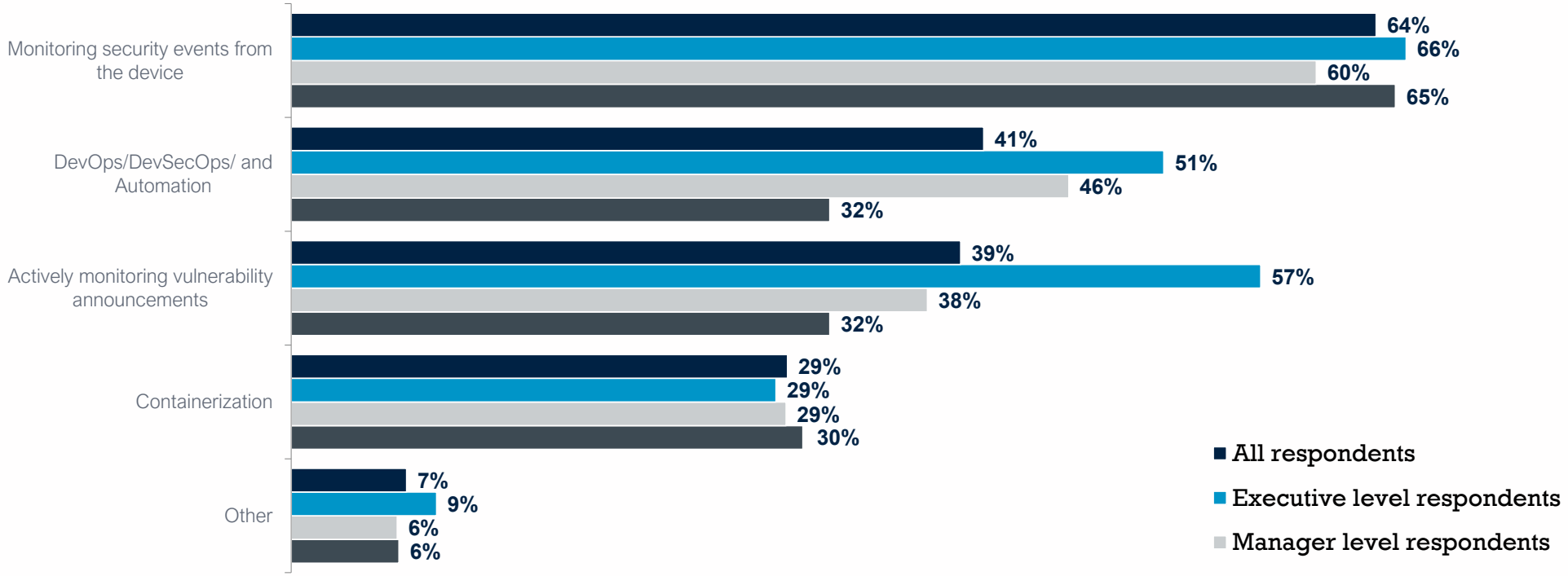
Executive level respondents report their team spends the most time on the design aspects of security, while manager level respondents are more likely to believe time is spent in the implementation or maintenance phase of the lifecycle.



Question: On which phase of the device lifecycle below does your team spend the most time related to security?
Base: All respondents (n=145).

IT Security Practices

Respondents agree that monitoring security events from the device is the security practice from the IT world that is most relevant to embedded system development.

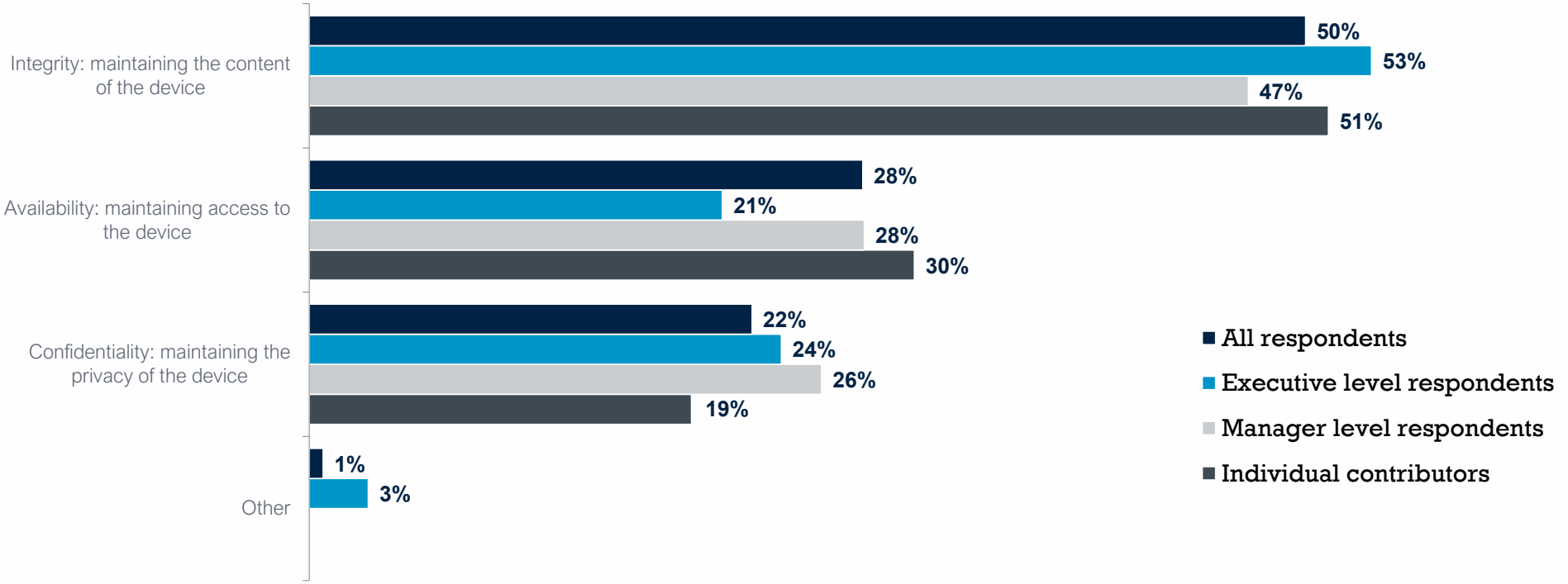


Question: Which security practices from the IT world are most relevant for embedded system development?

Base: All respondents (n=147). Multiple answers allowed.

Most Important Security Principle

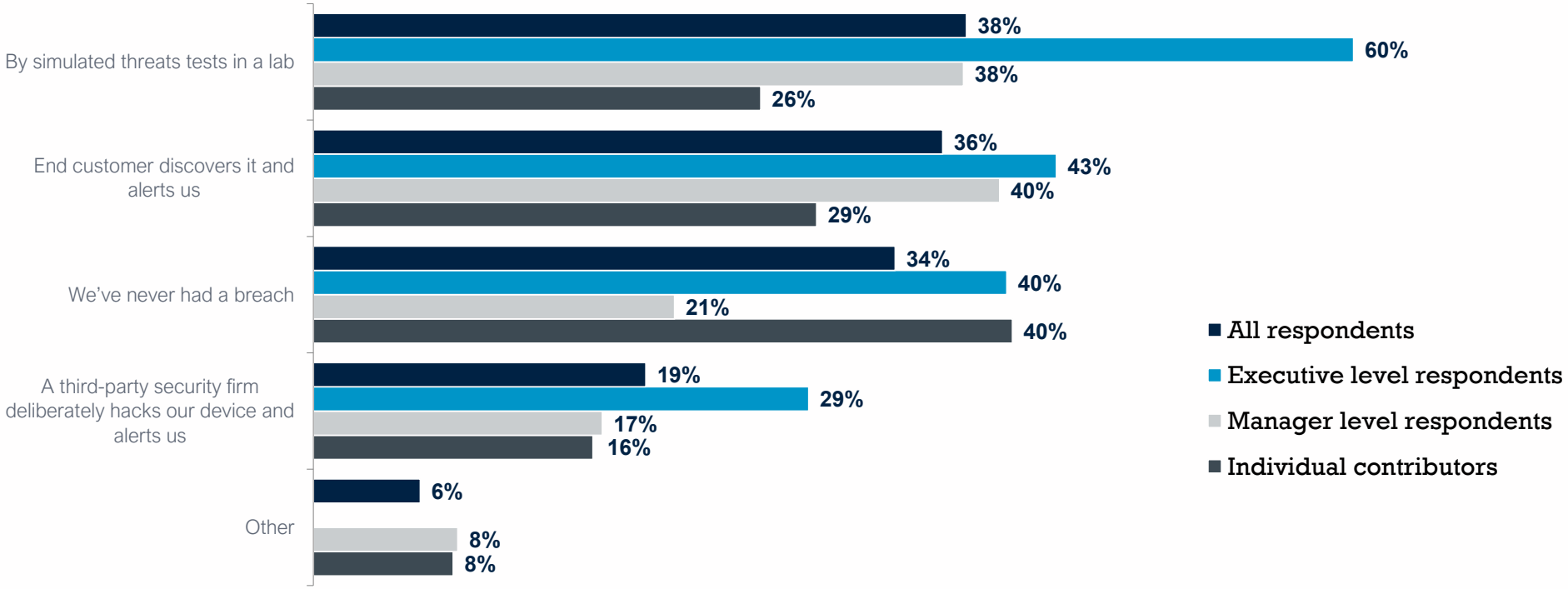
Half of respondents believe that integrity of their device is most important to their project.



Question: Which security principle is most important to your project?
Base: All respondents (n=145).

Security Breach Detection

Six in ten executive level respondents report that breaches are detected by using simulated threat tests in a lab. One in three respondents report they've never had a breach.

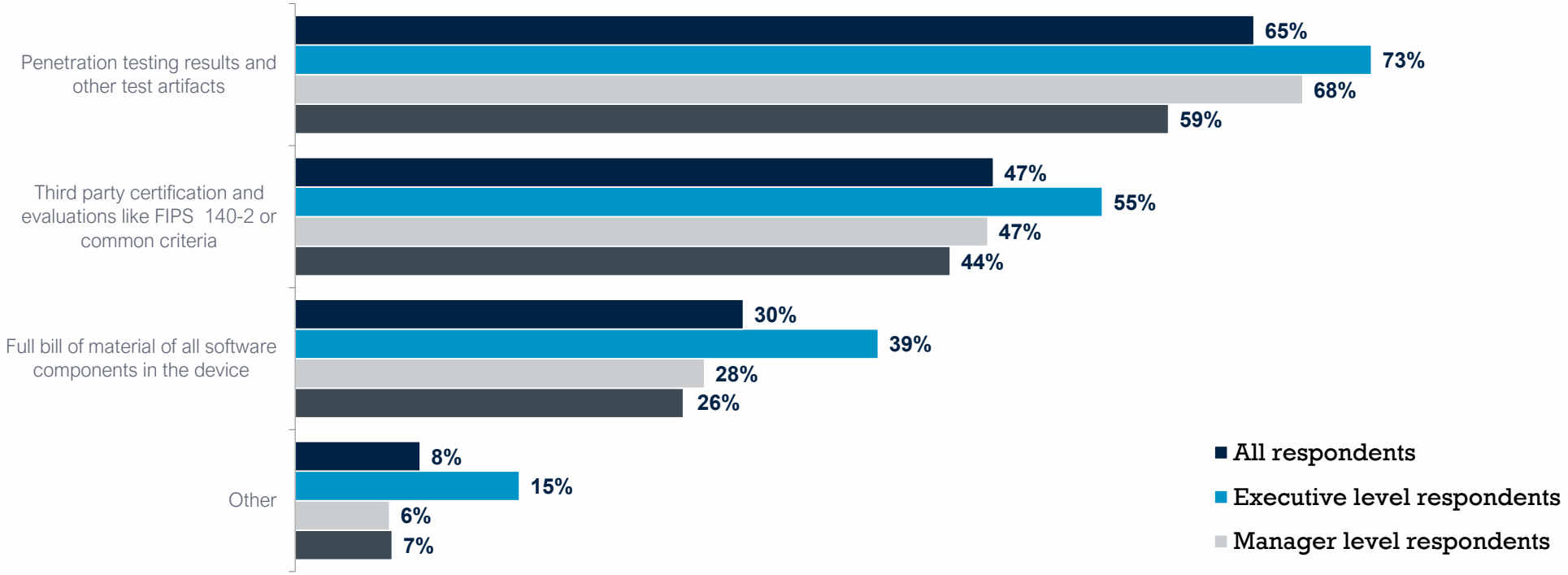


Question: How are security breaches being detected in fielded or deployed devices?

Base: All respondents (n=146). Multiple answers allowed.

Compliance Documentation

To show security compliance, respondents are most likely to believe a software supplier should show penetration testing results and other test artifacts. Over half of executive level respondents would like to see third-party certification.

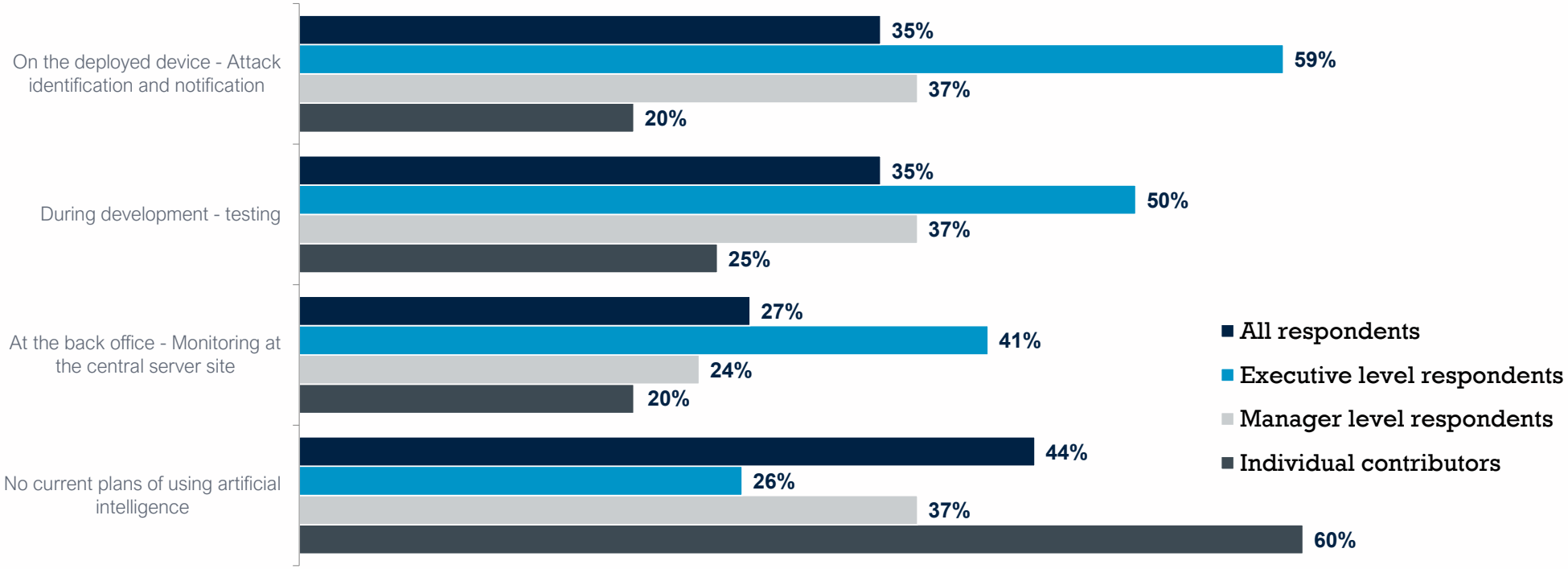


Question: What documentation should a software supplier provide to show security compliance?

Base: All respondents (n=142). Multiple answers allowed.

Role of AI in Securing Devices

Executive level respondents are most likely to have a vision for the use of AI in securing embedded devices.



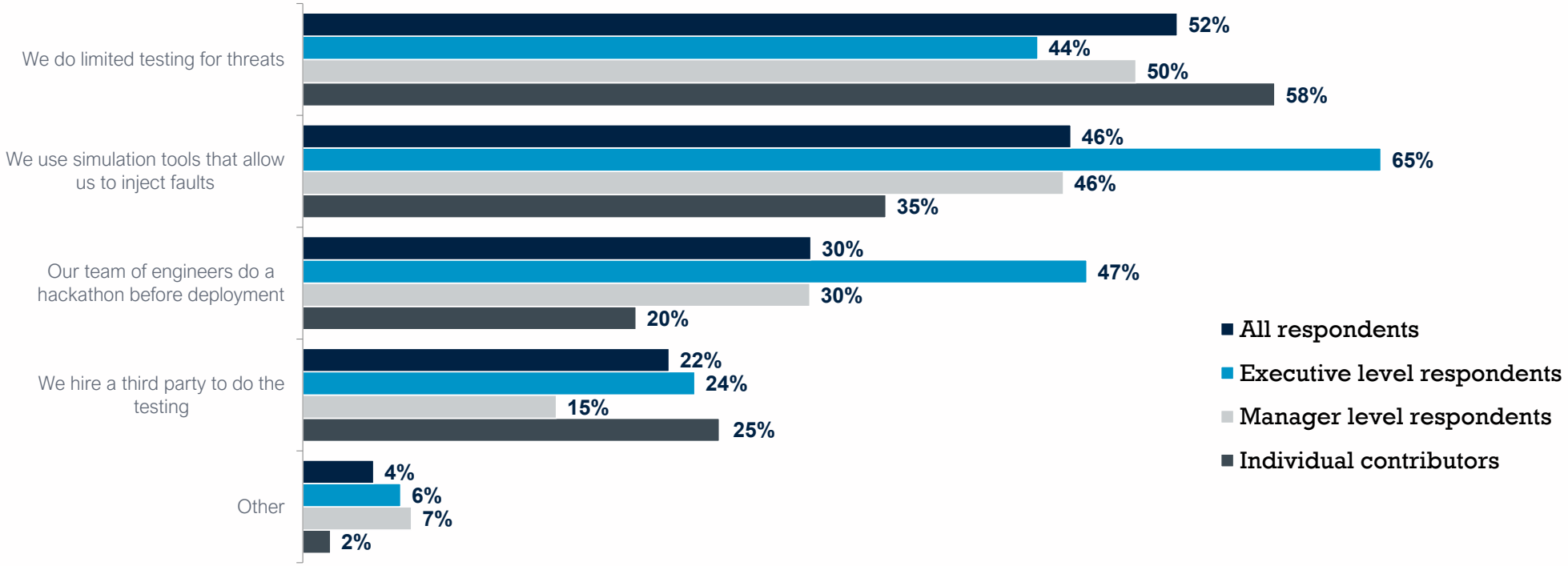
Question: How will AI play a role in securing embedded devices?

Base: All respondents (n=141). Multiple answers allowed.

ElectronicDesign.

Testing Security of Embedded Device

Nearly two-thirds of executive level respondents typically test an embedded device for security risks through the use of simulation tools. Forty-seven percent of executive level respondents report their team of engineers do a hackathon before deployment.

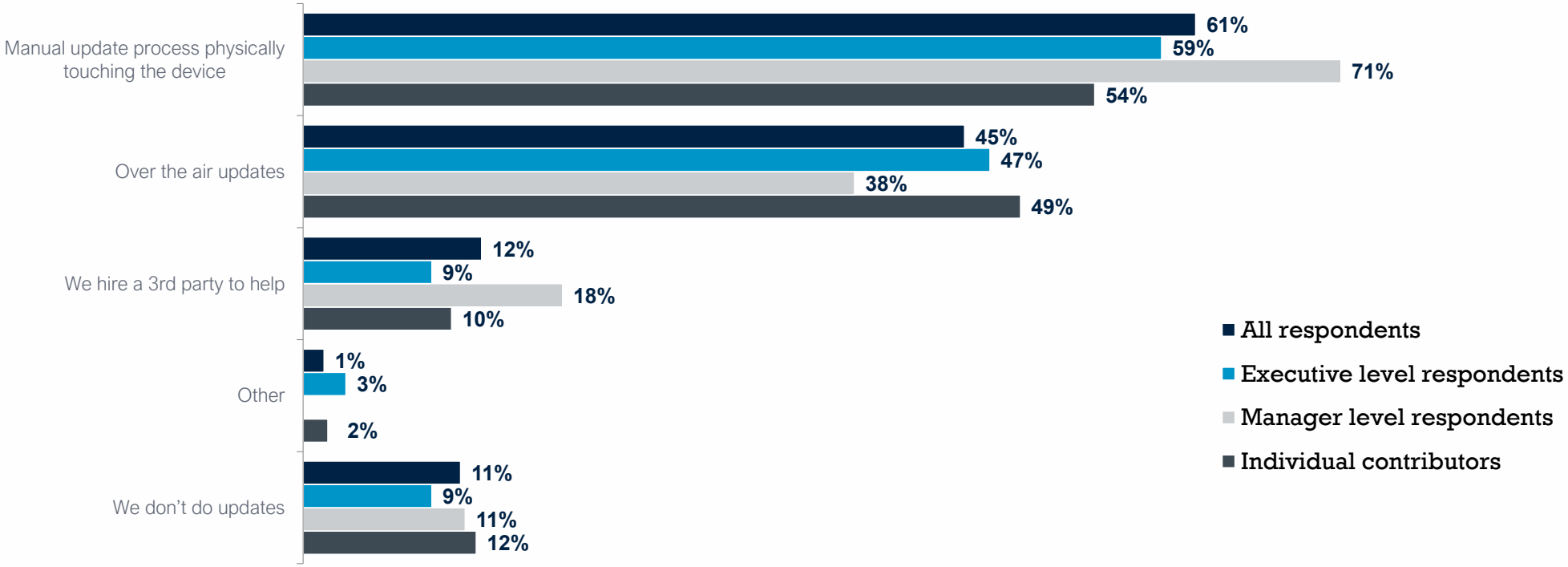


Question: How do you typically test your embedded device for security risks?

Base: All respondents (n=141). Multiple answers allowed.

Security Maintenance and Updates

Ongoing security maintenance, updates, and patches are typically handled through manual update processes.

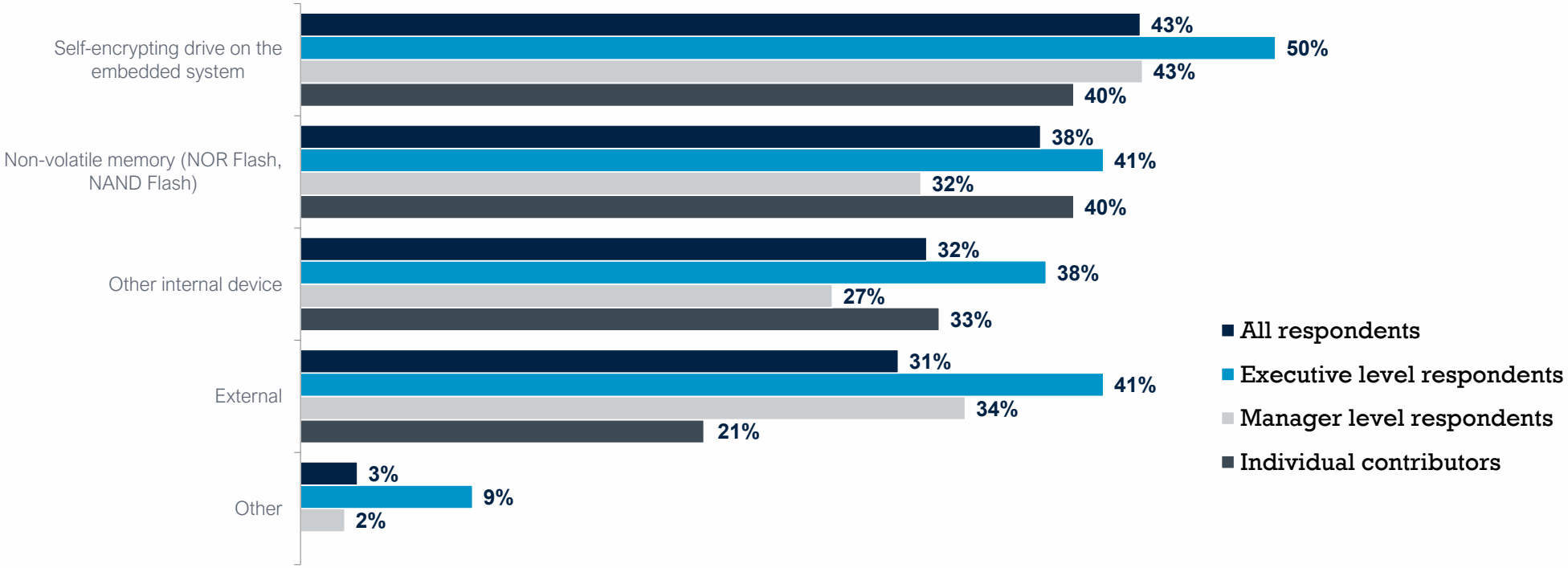


Question: How do you handle ongoing security maintenance, updates and patches your deployed device today?

Base: All respondents (n=139). Multiple answers allowed.

Data Storage

Respondents indicate a variety of hardware types store their most sensitive application and/or data.

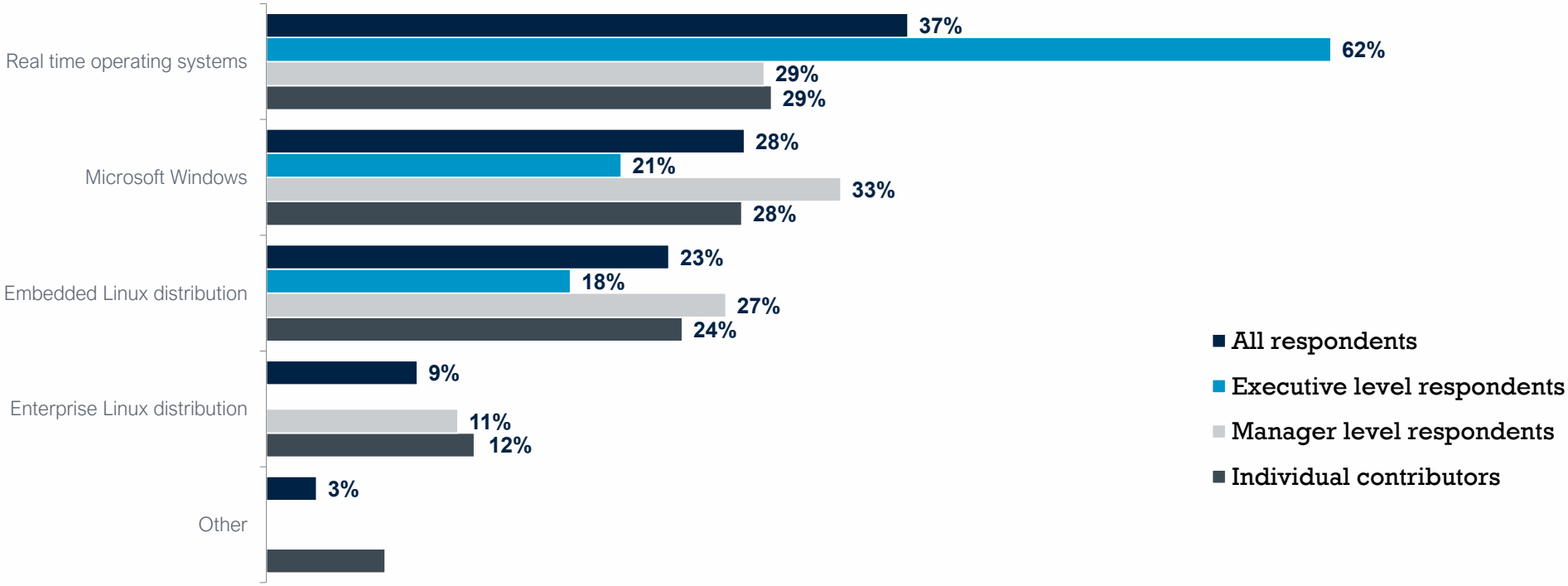


Question: What type of hardware stores your most sensitive application and/or data?

Base: All respondents (n=137). Multiple answers allowed.

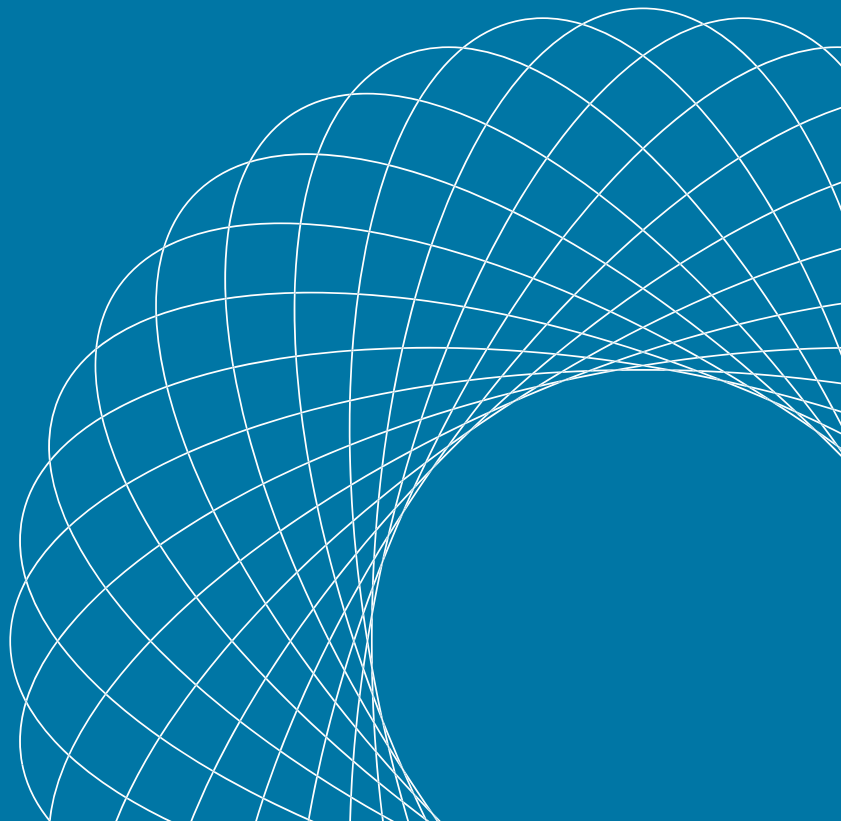
Operating System

While executive-level respondents have a clear preference for real time operating systems, respondents at lower levels within their companies vary in their opinion of the best operating systems.



Question: What operating systems do you believe fulfills the most security requirements you are faced with meeting?
Base: All respondents (n=137).

Write-in Comments



Write-in comments

Which industry do you represent? Other responses:

- Agricultural – 2 mentions
- All the above – 2 mentions
- ATE
- Audio Visual
- Chemical
- Construction
- Consumer – 3 mentions
- Consumer Electronics
- Education – 3 mentions
- Embedded and stand alone sensors
- Embedded consulting engineer
- Government consultant
- Governmental
- IIoT, Healthcare, Retail, etc
- Multiple consultant
- office buildings
- Pharmaceutical
- Physical Security
- Rail
- Real Estate
- Scientific research
- Storage
- Technical
- Test and measurement
- Testing

What is the biggest security threat facing your industry? Other responses:

- Biosecurity
- Counterfeit Parts
- Internal user failures
- People copying design
- X filtration of data

Where are most of your security requirements coming from? Other responses:

- Customer requirements
- NIST
- OEM requirements

Write-in comments

What are the three most important design-in security considerations? Other responses:

- Key exchange

What is the primary roadblock in securing your device? Other responses:

- Budget on what public is willing to pay for security sets the expectations to support in-house development
- Low IQ devices
- Schedule
- User issues

On which phase of the device lifecycle below does your team spend the most time related to security? Other responses:

- Design and requirements
- Equal Requirements-Design-Implementation

Which security practices from the IT world are most relevant for embedded system development? Other responses:

- Actively monitoring patterns and anomalies
- Air gap
- Attacks
- Employee turnover - frequent
- Principle of least privilege
- Repair

Which security principle is most important to your project? Other responses:

- Continuous operation

Write-in comments

How are security breaches being detected in fielded or deployed devices? Other responses:

- In-house tools

What documentation should a software supplier provide to show security compliance? Other responses:

- Accepting liabilities
- Debugging
- Full lab test as to vulnerabilities and mitigation
- Masking and control
- Negotiated

How do you typically test your embedded device for security risks? Other responses:

- DISA provides test frameworks and testing criteria
- Dump illegal commands with CRC verification
- In-house tools
- Not in charge of that section/competence, which is handled by other division (at different country)of the group
- tech support

How do you handle ongoing security maintenance, updates and patches your deployed device today? Other responses:

- automation of updates via R/O media via customer (classified sites)

What type of hardware stores your most sensitive application and/or data? Other responses:

- Cloud database

What operating systems do you believe fulfills the most security requirements you are faced with meeting? Other responses

- Bare metal
- Bare Metal Booting
- Internal proprietary
- Windows IoT

Write-in comments

What packaged or Open Source security solutions are you currently considering to meet your security requirements?

- ACAS
- Apache HTTP server
- Avast
- embedded Linux
- Government security protocols.
- Hackers' hacking
- In house program
- IOS security
- Juniper Contaril
- Linux – 4 mentions
- Lynx, VxWorks, stripped down Linux
- Mcafee
- MICROSOFT
- New software
- None. Custom Hardening
- OpenEmbedded Linux
- OpenSSL and SWUpdate
- Ratproxy,Vega
- repair and debug virus using several specical procedures to fix security
- SiFive's World Guard solution
- Solutions bundled with Linux and RTOS distributions
- SPARQ Global
- There are many that we use and these are segregated by type
- VMWare + RHLinux
- We are considering a security suite with many options
- Windows 10

Thank you!