The Importance of Securing Embedded and Connected Devices in the Supply Chain

Sponsored by Finite State

Independently conducted by Ponemon Institute LLC

Publication Date: October 2021

The Importance of Securing Embedded and Connected Devices in the Supply Chain

Prepared by Ponemon Institute, October 2021

Part 1. Introduction

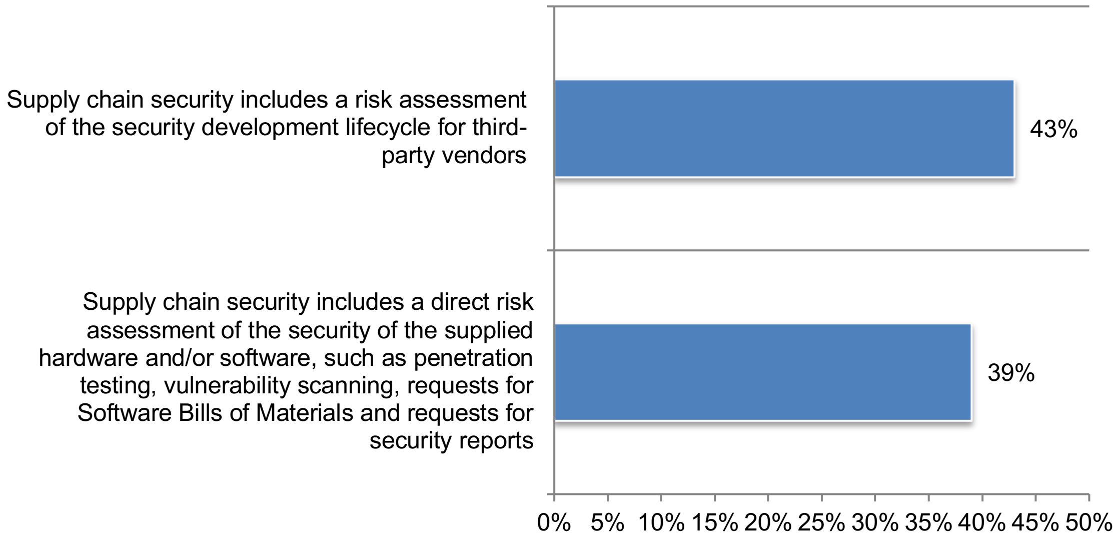
The Kaseya supply chain compromise has demonstrated the threats to supply chains that ransomware groups pose. The supply chain compromise of SolarWinds Orion network management due to the SUNBURST malware has also underscored how vulnerable supply chains are to attacks. According to participants in this research, these compromises and the increase in supply chain and IoT attacks require organizations to rethink supply chain and product security processes.

Sponsored by Finite State, Ponemon Institute surveyed 632 IT and IT security practitioners in the U.S. who are familiar with their organizations' approach to securing embedded and connected devices and have complete or partial responsibility for setting and/or implementing their supply chain security strategies. The research targets device and connected device manufacturers in highly regulated industries.

Seventy-three percent of respondents say their organizations are very committed (40 percent) or committed (33 percent) to achieving a secure supply chain. Twenty-seven percent of respondents say their organizations are only somewhat committed.

While respondents are aware and very concerned about the threats to their organizations' supply chain based on recent compromises, only 39 percent of respondents say there is a direct risk assessment of the security of the supplied hardware and/or software, such as penetration testing, vulnerability scanning, requests for Software Bills of Materials and requests for security reports, as shown in Figure 1. Further, only 43 percent of respondents say their organizations conduct a risk assessment of the security development lifecycle for third-party vendors.

Figure 1. Perceptions about assessments of supply chain security
Yes responses presented



The following findings reveal why organizations are not making supply chain security as important as it should be.

- **Product security is not a priority.** Only 41 percent of respondents say their organizations make it a priority despite the finding that 76 percent of respondents say the security of an IoT device is very important

- **Executives and boards of directors are not involved as they should be in their organizations' product security practices.** Only 27 percent of respondents say the leadership requires assurances that product security is being assessed, managed and monitored appropriately.

- **Product security processes and programs are not reviewed frequently.** Only 24 percent of respondents say such a review occurs frequently to address evolving supply chain risks.

- **Lack of resources and in-house expertise are obstacles to achieving a strong security posture.** When asked what is preventing the development of secure IoT/embedded products, 62 percent of respondents say it is a lack of resources and 60 percent of respondents say it is a lack of in-house expertise.

- **Organizations need more resources to improve product security.** Fifty percent of respondents say their organizations are not increasing investments for product security. As mentioned above, the number one obstacle to improved product security is the lack of resources.

- **Organizations find it difficult to manage supply chain risks.** Sixty percent of respondents say their organizations find it difficult to rapidly respond to new vulnerability disclosures that may affect their devices.

Part 2. Key findings

In this section, we provide an analysis of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following themes.

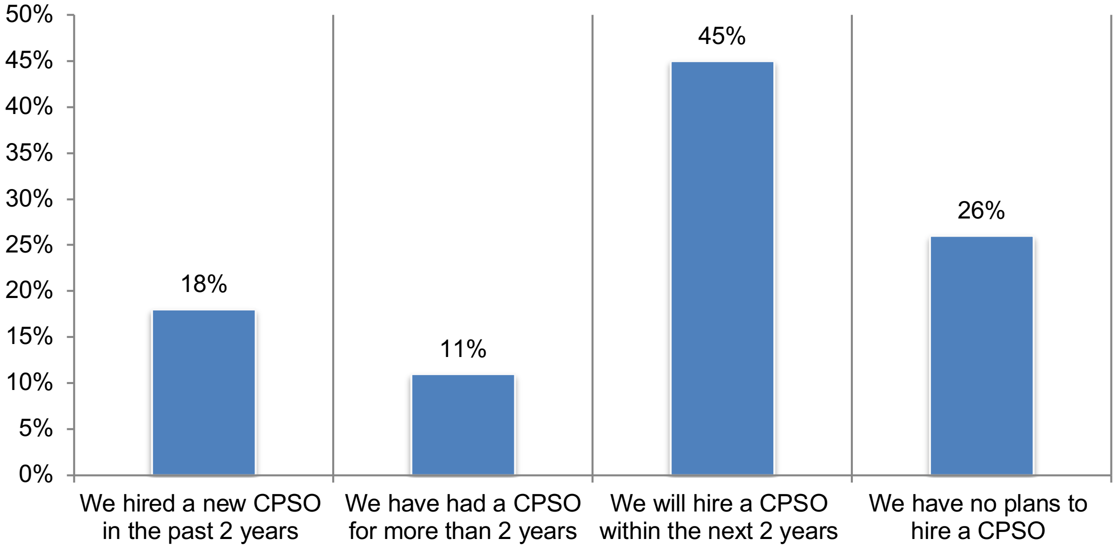
- The value CPSOs bring to product and supply chain security
- Effectiveness of product security and supply chain security programs
- The impact of supply chain security on sales and customer relationships
- Types of security testing
- Regulations and standards

The value CPSOs bring to product and supply chain security

Organizations are hiring CPSOs. As shown in Figure 2, only 26 percent of respondents say their organizations will not hire a CPSO. Currently, 29 percent of respondents have a CPSO, and 45 percent expect their organizations will hire a CPSO within the next two years.

In this section, we present the differences between organizations with CPSOs and those that do not have such a role. As the findings reveal, organizations with a CPSO have a more mature approach to securing their embedded and connected devices in the supply chain.

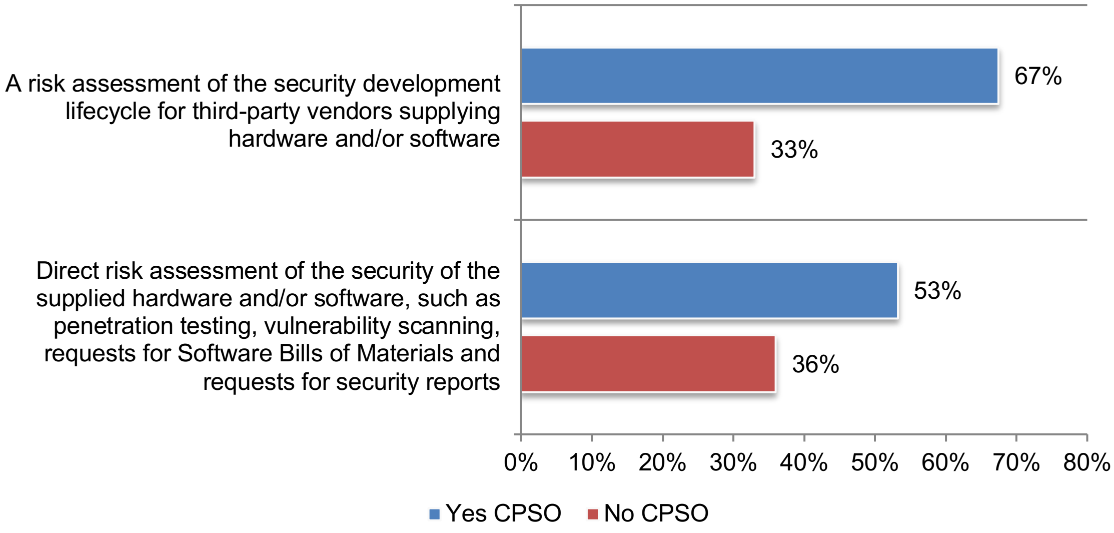
Figure 2. Does your organization have a Chief Product Security Officer (CPSO)?



Organizations with a CPSO are far more likely to have a security supply chain policy that includes risk assessments. Thirty-six percent of respondents in organizations with CPSOs say they have a security supply chain policy vs.15 percent of the other respondents who say their organizations have a policy.

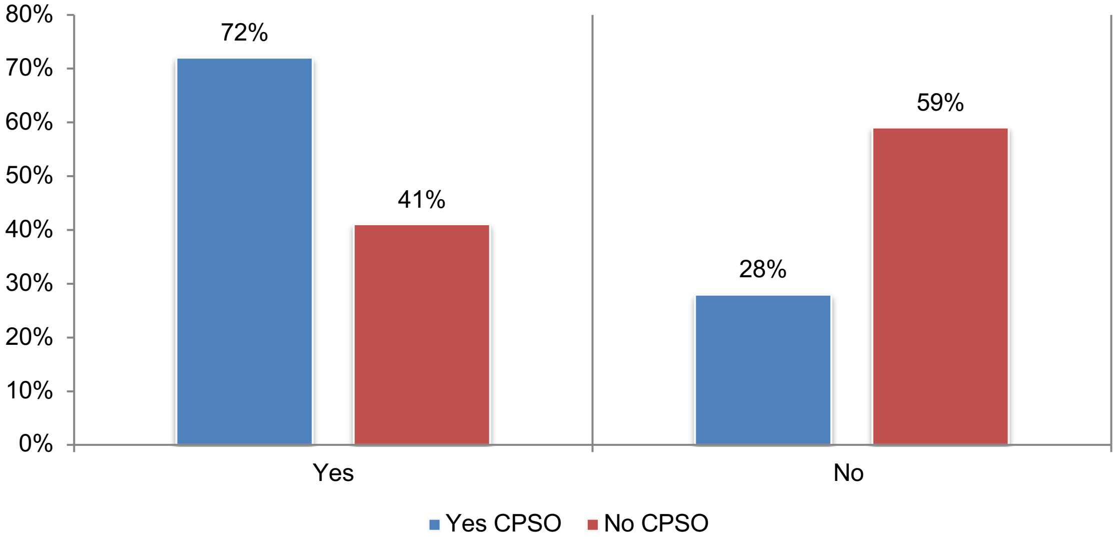
According to Figure 3, 67 percent of respondents with CPSOs say their policies include a risk assessment of the security development lifecycle for third-party vendors supplying hardware and/or software vs. 33 percent in the other organizations. Similarly, more than half (53 percent) of respondents in CPSO organizations assess the risk of the security of supplied hardware and/or software, such as pen testing, vulnerability scanning, requests for Software Bills of Materials and requests for security reports.

Figure 3. What does your organization's security supply chain policy include?



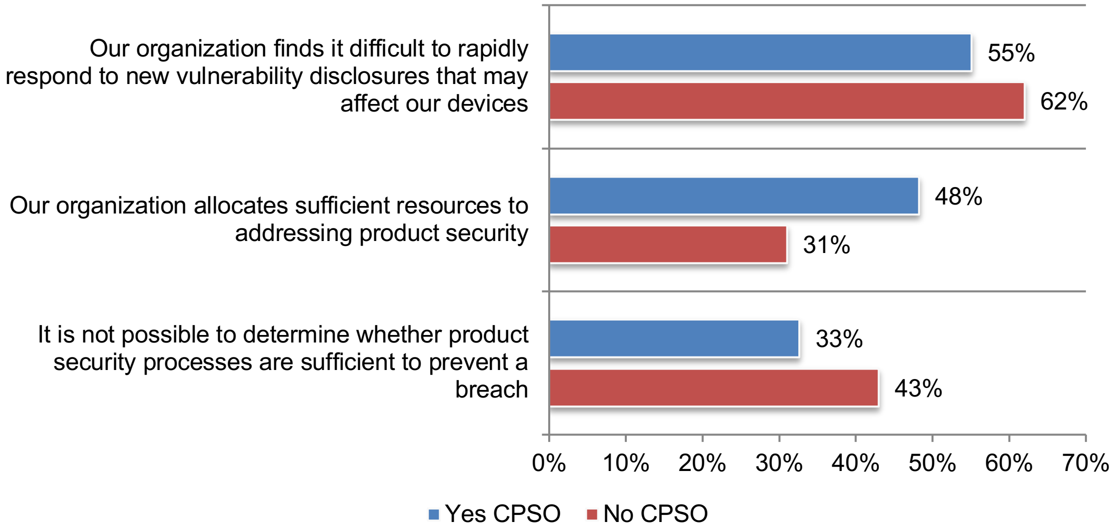
There is a significant difference between CPSO and non-CPSO organizations in the assessment of their own products before they are shipped to customers (72 percent vs. 41 percent of respondents).

Figure 4. Does your organization assess the security of its own products before they are shipped to customers?



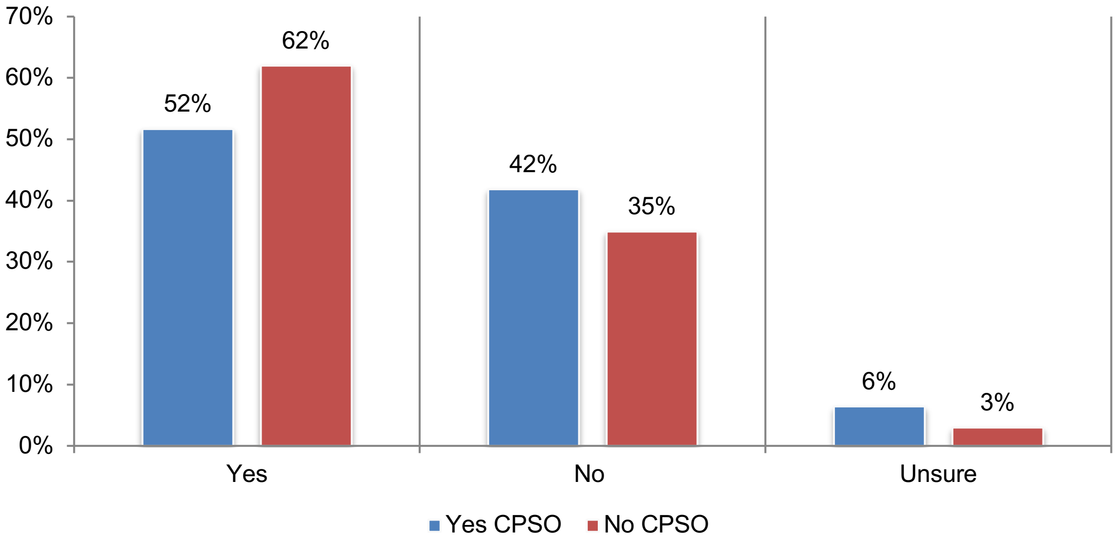
CPSO organizations are more likely to have sufficient resources and are more effective in stopping breaches and quickly responding to vulnerability disclosures. According to Figure 5, 62 percent of organizations without a CPSO find it difficult to rapidly respond to new vulnerability disclosures that may affect their devices. Less than one-third (31 percent) of respondents say their organizations have enough resources to address product security and 43 percent of respondents say it is not possible to determine whether product security processes are sufficient to prevent a breach.

Figure 5. Perceptions about product security
Strongly agree and Agree responses combined



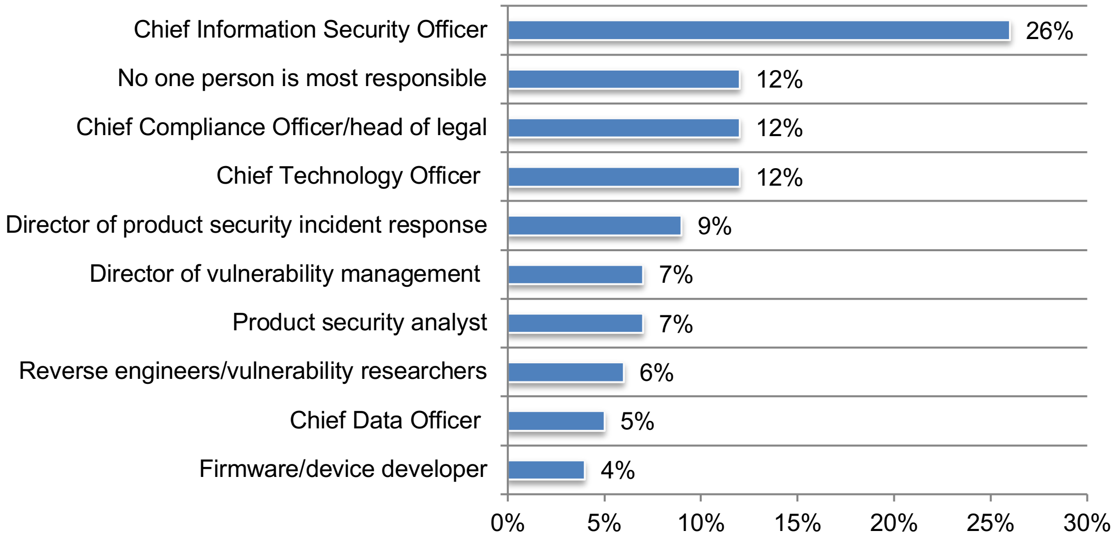
Organizations with CPSOs are less likely to lose customers because of product security, as shown in Figure 6.

Figure 6. Has your organization lost sales because of product security?



Organizations without a CPSO assign responsibility for product security to the CISO.

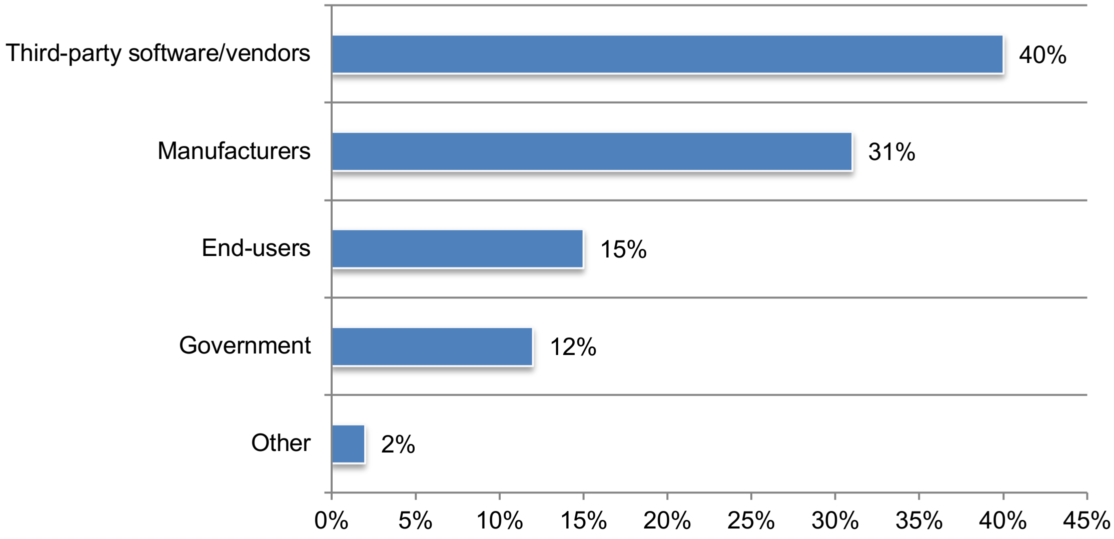
Figure 7. If no CPSO, who is most responsible for product security in your organization?



Effectiveness of product security and supply chain security programs

As IoT devices continue to proliferate in organizations, 40 percent of respondents say third-party software/vendors should be most responsible for ensuring the security of IoT devices followed by 31 percent of respondents who say manufacturers should be most responsible, as shown in Figure 8.

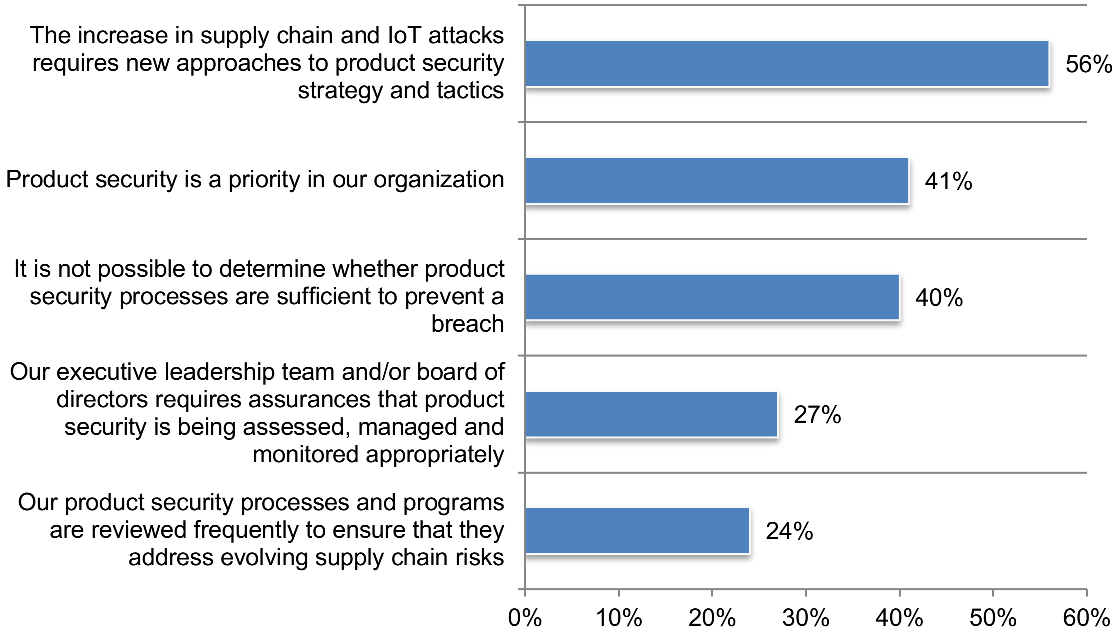
Figure 8. Who should be most responsible for ensuring the security of IoT devices?



The supply chain is vulnerable and requires a shift in product security strategy and tactics. Figure 9 provides insights into how organizations are approaching product security strategy and tactics. Fifty-six percent of respondents say increases in supply chain and IoT attacks require organizations to rethink supply chain and product security. Forty percent of respondents say it is not possible to determine whether product security processes are sufficient to prevent a breach.

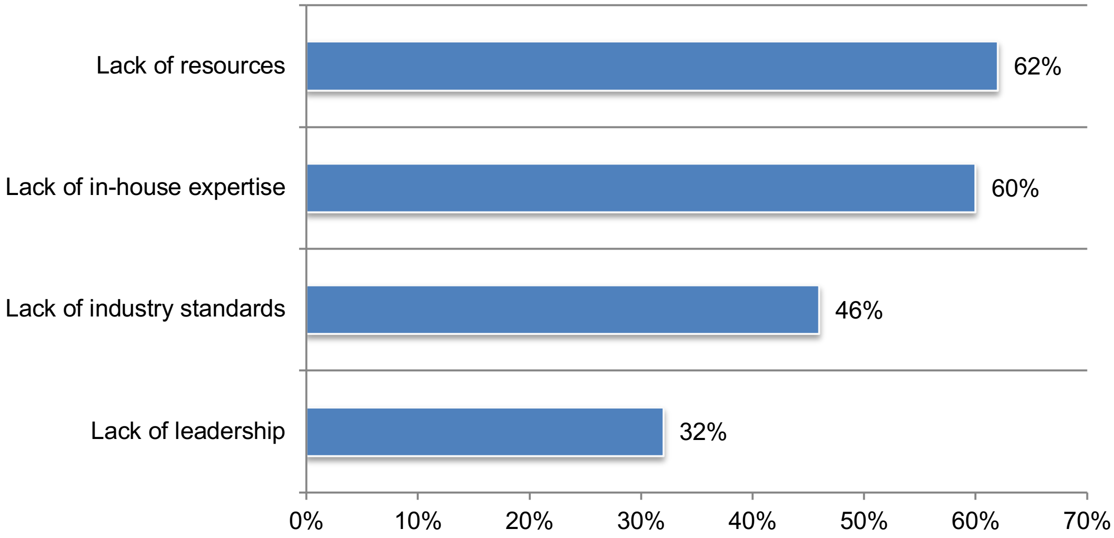
However, barriers to achieving a strong supply chain security posture are also shown below. Only 24 percent of respondents say product security processes and programs are reviewed frequently to ensure that they address evolving supply chain risks and only 27 percent of respondents say their executives and board of directors require assurances that product security is being assessed, managed and monitored appropriately. As a result, only 41 percent of respondents say product security is a priority.

Figure 9. Perceptions about product and supply chain security
Strongly agree and Agree responses presented



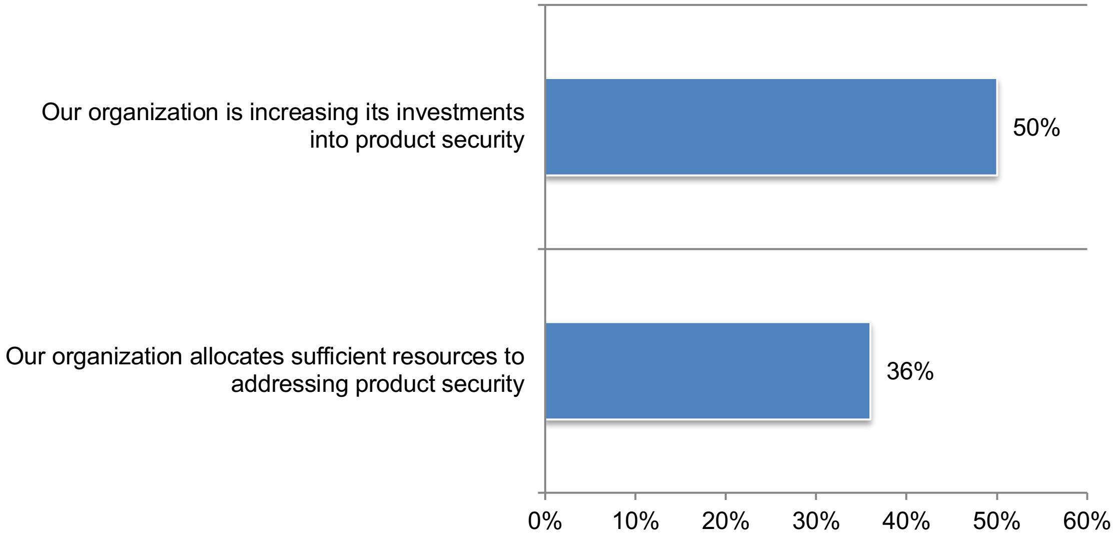
Lack of resources and in-house expertise are the primary obstacles to securing IoT/embedded products. According to Figure 10, when asked what is preventing the development of secure IoT/embedded devices, 62 percent of respondents say it is a lack of resources followed by a lack of in-house expertise (60 percent of respondents). Almost one-third (32 percent) of respondents say it is a lack of leadership.

Figure 10. What are the greatest obstacles to developing secure IoT/embedded products?
Two responses permitted



Despite the risks, only half (50 percent) of respondents say their organizations are increasing investments for product security. As discussed, a lack of resources is the number one obstacle to securing IoT/embedded devices. According to Figure 11, only 36 percent of respondents say their organizations allocate sufficient resources for product security.

Figure 11. Perceptions about product security resources
Strongly agree and Agree responses presented



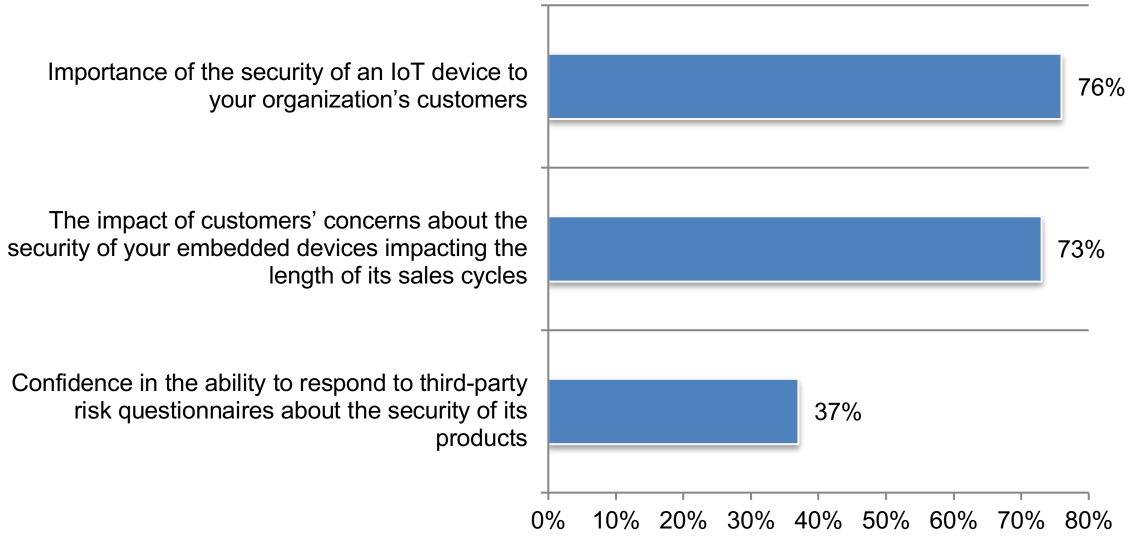
In 2021, organizations are spending an average of $18.5 million on product security ($11.3 million) and embedded device product security ($7.2 million), as shown in Table 1. As discussed previously, only 36 percent of respondents say their organizations allocate sufficient resources to mitigate product security risks.

Table 1. Budget and investment	Dollars allocated
The average 2021 IT budget	$197,000,000
The average IT budget allocated to security (23 percent of ($197 million)	$45,310,000
The average IT security budget allocated to product security activities (25 percent of $45.3 million)	$11,327,500
The average IT security budget allocated to embedded device product security (16 percent of $45.3 million)	$7,249,600
Total investment in product security activities and embedded device supply chain security	$18,577,100

Customers' concern about security and lost sales should be an incentive to improving the security of embedded devices. Respondents were asked to respond to questions regarding the importance of the security of an IoT device to customers, the impact of customers' concerns about the security of embedded devices impacting the length of sales cycles and the ability to respond to third-party risk questionnaires about the security of its products on a scale from 1 = no importance/impact/confidence to 10 = high importance/impact/confidence.

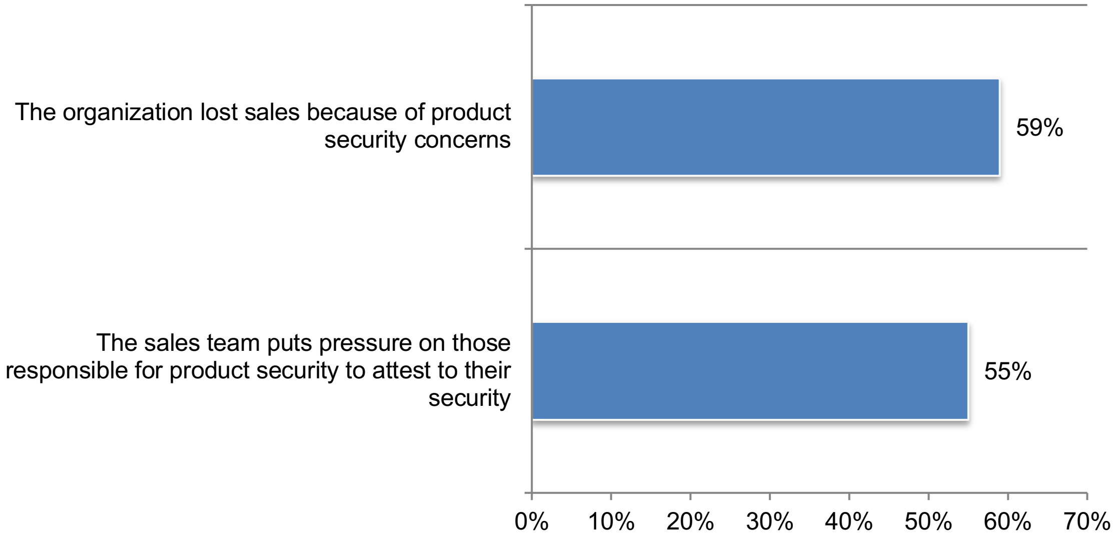
Figure 12 presents the high response rating (7+ responses) for the questions below. Seventy-six percent of respondents say the security of an IoT device is very important for consumers and these concerns about security affect the length of sales cycles (73 percent of respondents). Only 37 percent of respondents say the ability to respond to third-party risk questionnaires about the security of products is very high.

Figure 12. Customers' perceptions about the security of embedded devices
10-point scale from 1 = no importance/impact/ confidence to 10 = high importance/impact/ confidence, 7+ responses presented



Customers' concerns about the security of products results in lost sales. As shown in Figure 13, 59 percent of respondents say their organizations lost sales because of security concerns. As a result, 55 percent of respondents say the sales team is putting pressure on the product security team to attest to the security of these products.

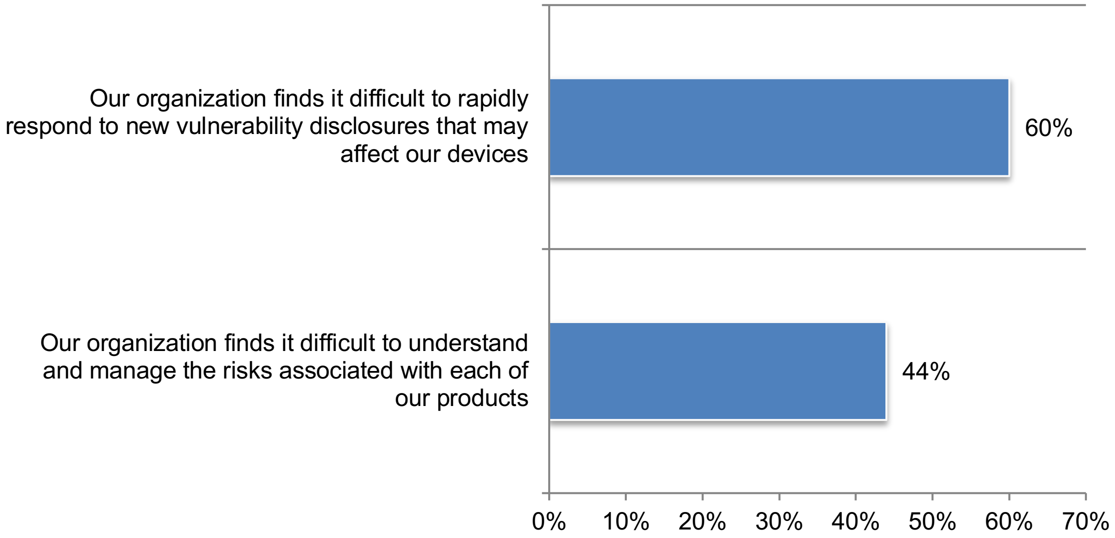
Figure 13. The impact of device security on customer relationships
Yes responses presented



Types of security testing

Organizations are at risk because of the difficulty in quickly responding to new vulnerability disclosures that may affect their devices. As shown in Figure 14, 60 percent of respondents say it is difficult to rapidly respond to new vulnerability disclosures and 44 percent of respondents say it is difficult to understand and manage the risks associated with each of their products.

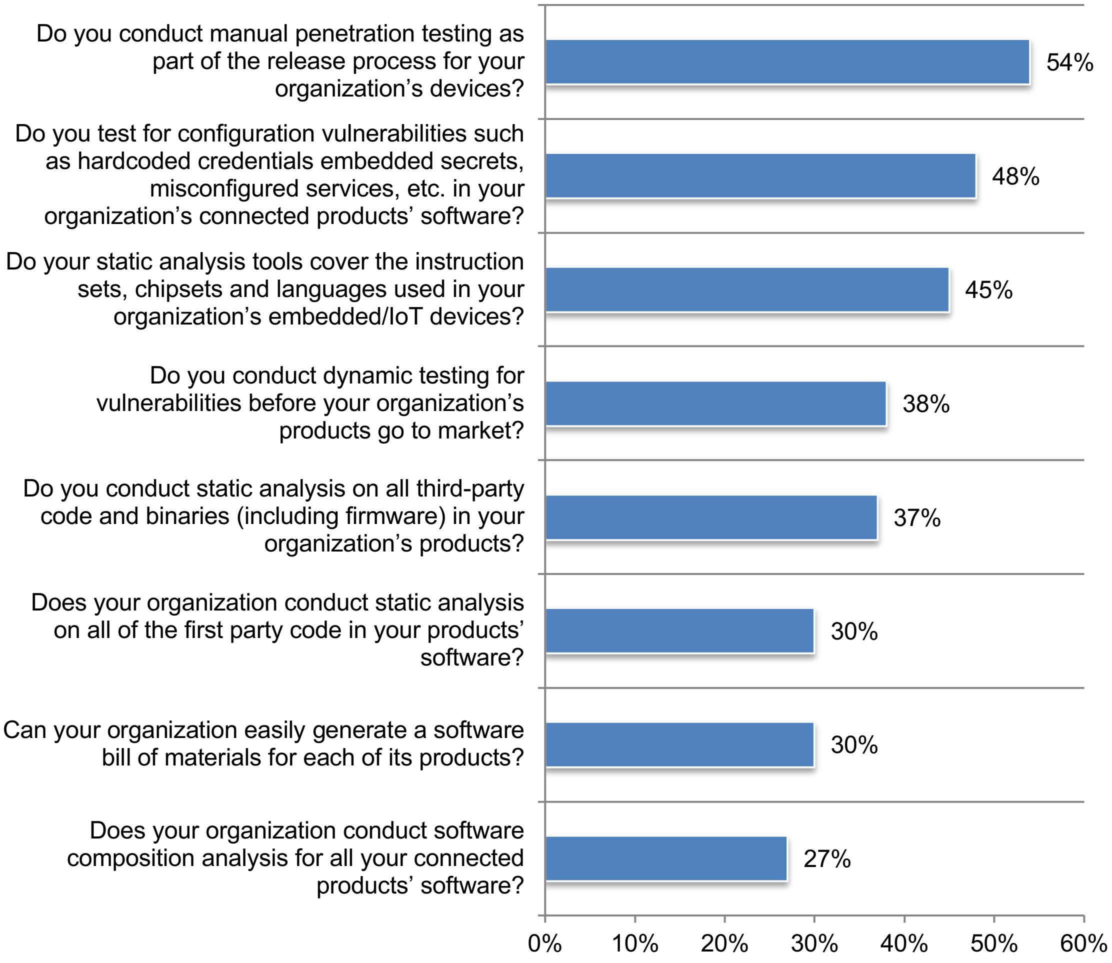
Figure 14. Perceptions about managing risks
Strongly agree and Agree responses presented



More security testing needs to be done. Figure 15 presents the different types of security testing done in the supply chain. As shown, the most frequent test is manual penetration testing as part of the release process for their organization's devices, according to 54 percent of respondents. Only 27 percent of respondents say their organizations conduct software composition analysis (SCA) for all connected products' software. If yes, only 38 percent of respondents say SCA tools work in their embedded/IoT device development processes.

Less than half (48 percent) of respondents say their organizations test for configuration vulnerabilities, such as hardcoded credentials embedded secrets and misconfigured services in their organizations' connected products' software.

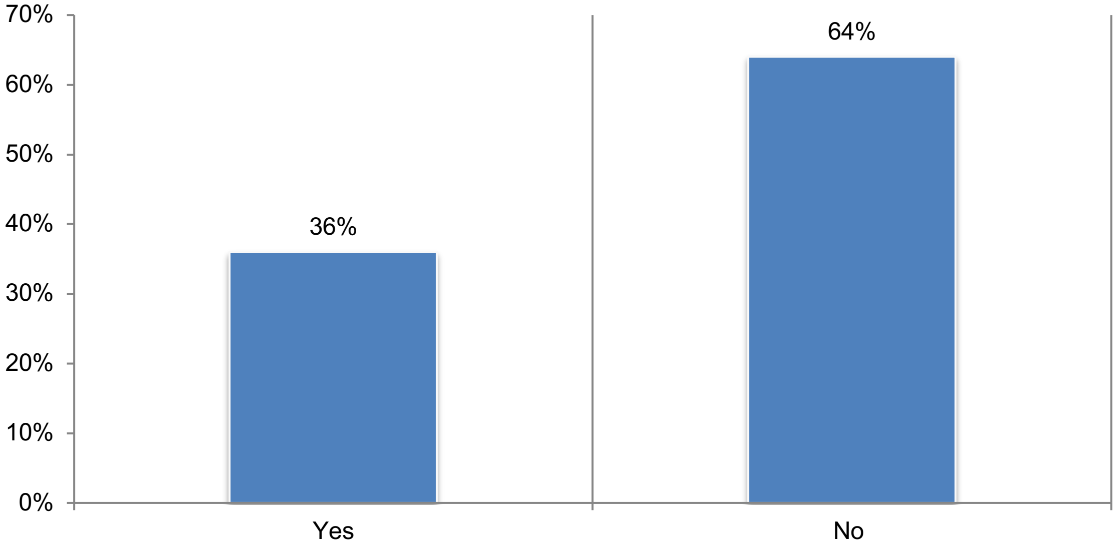
Figure 15. Types of security testing
Yes responses presented



Regulations and standards

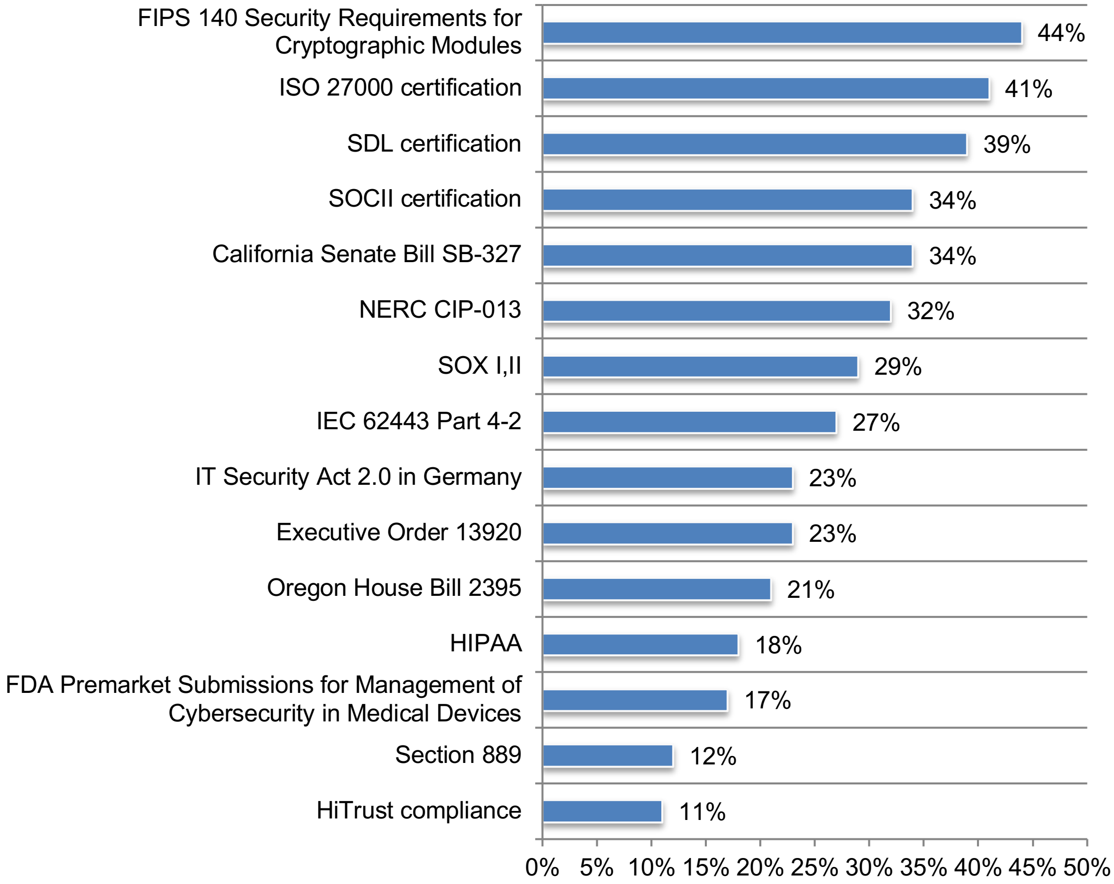
Regulations and compliance frameworks are not relevant to most organizations represented in this research. According to Figure 16, only 36 percent of respondents say the government requires their organization to provide details about the security of devices. Sixty-three percent of respondents say their organizations' ability to respond to these requests is very high.

Figure 16. Does the government (regulators) require your organization to provide details about the components in its devices or attest embedded devices are secure?



According to Figure 17, the top two relevant regulations are FIPS 140 Security Requirements for Cryptographic Modules (44 percent of respondents) followed by ISO 27000 certification (41 percent of respondents).

Figure 17. What regulations and compliance frameworks are relevant to your organization?
More than one response permitted



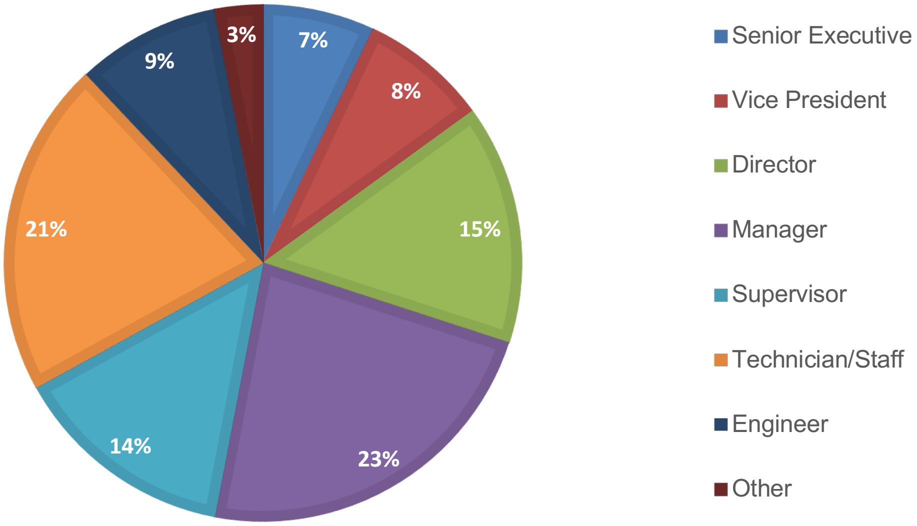
Part 3. Methodology

A sampling frame of 16,788 IT and IT security practitioners in the United States were selected as participants to this survey. All respondents are familiar with their organizations' approach to securing embedded and connected devices and have complete or partial responsibility for setting and/or implementing its supply chain security strategy. Table 2 shows 691 total returns. Screening and reliability checks required the removal of 59 surveys. Our final sample consisted of 632 surveys or a 3.8 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	16,788	100.0%
Total returns	691	4.1%
Rejected or screened surveys	59	0.4%
Final sample	632	3.8%

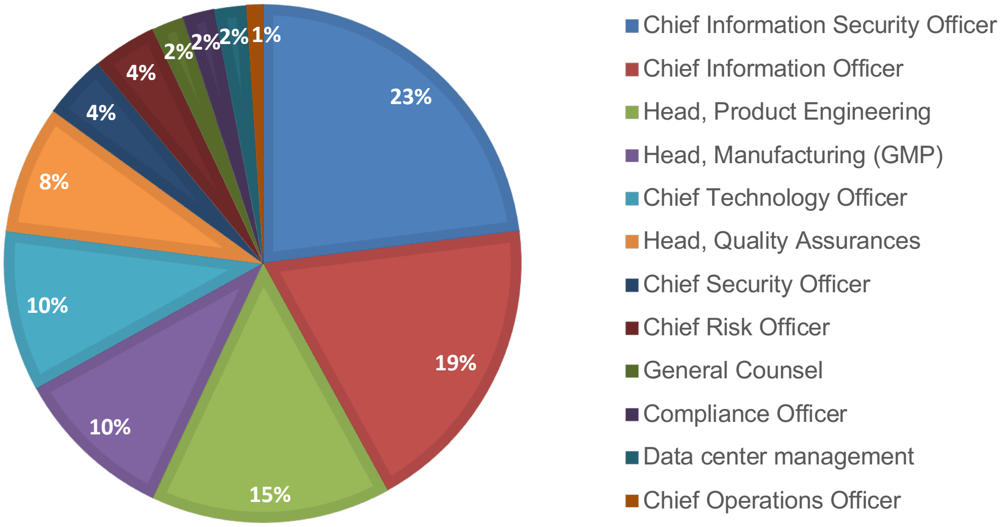
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (67 percent) of respondents are at or above the supervisory levels. The largest category at 23 percent of respondents is manager.

Pie Chart 1. Current position within the organization



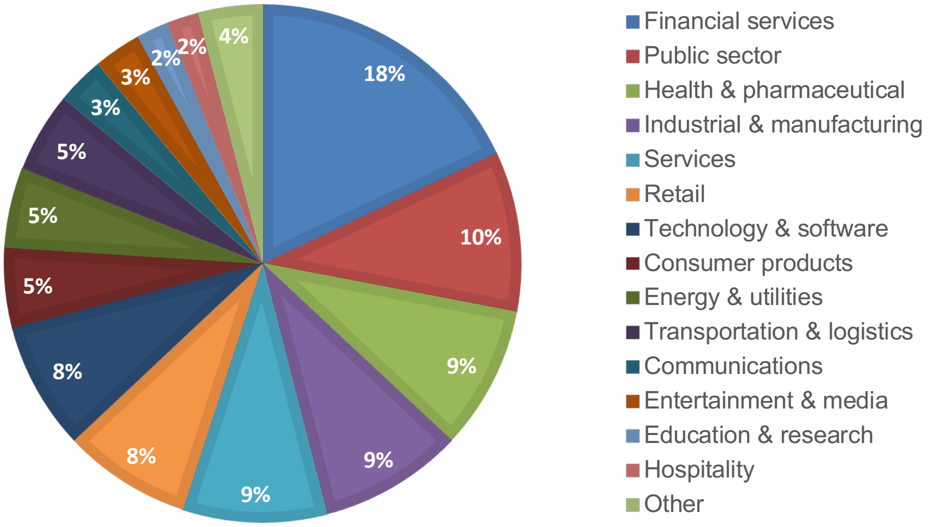
Pie Chart 2 reports the primary person the respondent reports to within the organization. Twenty-three percent of respondents report to the chief information security officer, 19 percent of respondents report to the chief information officer, and 15 percent of respondents report to the head of product engineering.

Pie Chart 2. Primary person respondent reports to within the organization



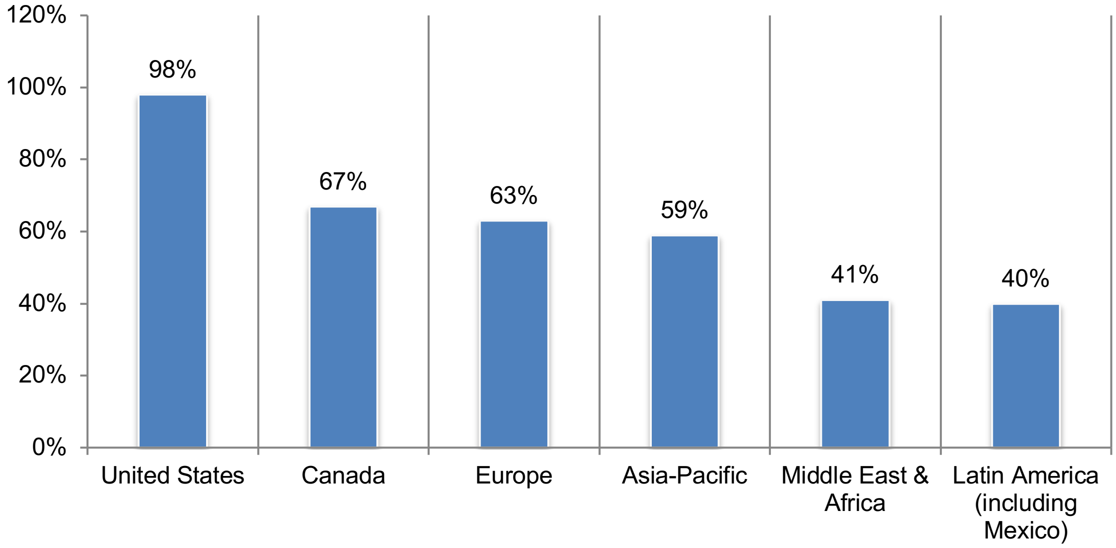
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (10 percent of respondents), health and pharmaceutical, industrial and manufacturing, and services (each at 9 percent of respondents).

Pie Chart 3. Primary industry classification



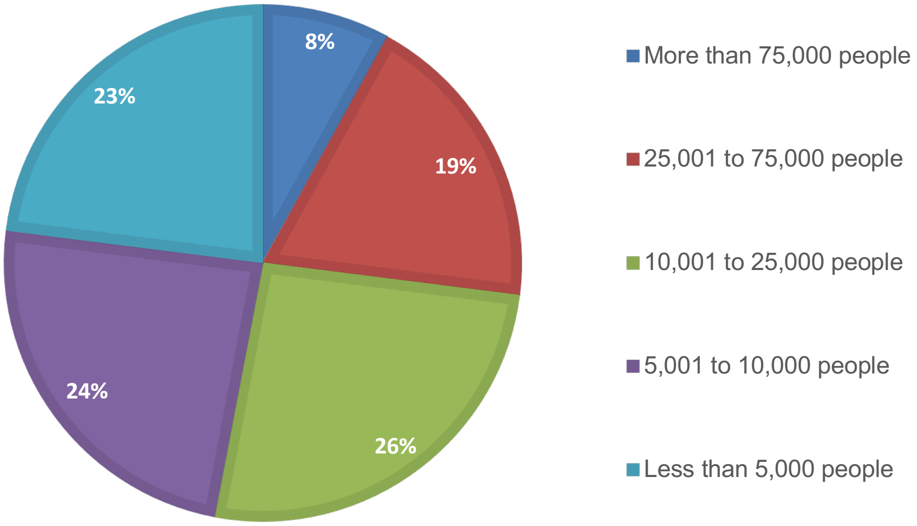
When asked to identify where their organizations' employees are located, 98 percent of respondents said the United States, followed by Canada (67 percent of respondents), Europe (63 percent of respondents), Asia-Pacific (59 percent of respondents), the Middle East and Africa (41 percent of respondents), and Latin America (40 percent of respondents).

Figure 18. Global distribution of employees



As shown in Figure 19, 53 percent of respondents are from organizations with a global headcount of more than 10,000 employees. The largest category at 24 percent of respondents is 5,000 to 10,000 employees.

Figure 19. Global full-time headcount



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT security practitioners located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in July 2021.

Survey Response	Freq
Total sampling frame	16,788
Total number of returns	691
Rejected surveys	59
Final sample	632
Response rate	3.8%

Part 1. Screening Questions

S1. How familiar are you with your organization's approach to securing embedded and connected devices?	Pct%
Very familiar	35%
Familiar	34%
Somewhat familiar	31%
Not familiar (stop	0%
Total	100%

S2. How much responsibility do you have for setting and/or implementing your organization's supply chain security strategy?	Pct%
I have complete responsibility for the strategy	36%
I share responsibility with others	64%
I have no responsibility (stop)	0%
Total	100%

S3. What is your organization's commitment to achieving a secure supply chain?	Pct%
Very committed	40%
Committed	33%
Somewhat committed	27%
Not committed (stop)	0%
Total	100%

Part 2. Background

Q1a. Does your organization have a Chief Product Security Officer (CPSO)?	Pct%
Yes, we hired a new CPSO in the past two years	18%
Yes, we have had a CPSO for more than two years	11%
No, but we will hire a CPSO within the next two years (please skip to Q2)	45%
No, and we have no plans to hire a CPSO (please skip to Q2)	26%
Total	100%

Q1b. If yes, is the CPSO most responsible for product security in your organization?	Pct%
Yes	55%
No	45%
Total	100%

Q2. If no, who is most responsible for product security in your organization? Please select one choice only.	Pct%
Chief Information Security Officer (CISO)	26%
Chief Technology Officer (CTO)	12%
Chief Compliance Officer (CCO)/head of legal	12%
Chief Data Officer (CDO)	5%
Product security analyst	7%
Director of product security incident response	9%
Firmware/device developer	4%
Director of vulnerability management	7%
Reverse engineers/vulnerability researchers	6%
No one person is most responsible	12%
Other (please specify)	0%
Total	100%

Q3a. Does your organization have a product security program for connected devices and/or embedded systems?	Pct%
Yes	41%
No (please skip to Q4)	59%
Total	100%

Q3b. If yes, how effective is the product security program on a scale from 1= not effective to 10 = high effectiveness.	Pct%
1 or 2	13%
3 or 4	27%
5 or 6	26%
7 or 8	24%
9 or 10	10%
Total	100%
Extrapolated value	5.32

Q4. What are the greatest obstacles to developing secure IoT/embedded products? Please select the **top two** obstacles only.	Pct%
Lack of industry standards	46%
Lack of resources	62%
Lack of in-house expertise	60%
Lack of leadership	32%
Other (please specify)	0%
Total	200%

Q5. Approximately, what range best defines your organization's 2021 IT budget?	Pct%
< $1 million	0%
$1 to 5 million	1%
$6 to $10 million	10%
$11 to $50 million	16%
$51 to $100 million	25%
$101 to $250 million	20%
$251 to $500 million	18%
$501 to $750 million	7%
$751 million to $1 billion	3%
More than $1 billion	0%
Total	100%
Extrapolated value (US$ Millions)	$ 197

Q6. Approximately, what percentage of the IT budget will be allocated to IT security?	Pct%
< 1%	0%
1% to 2%	2%
3% to 5%	4%
6% to 10%	9%
11% to 15%	13%
16% to 20%	26%
21% to 30%	19%
31% to 40%	16%
41% to 50%	11%
More than 50%	0%
Total	100%
Extrapolated value	23%

Q7. Approximately, what percentage of the IT security budget will be allocated to product security activities such as investment in technologies, personnel security and services?	Pct%
< 1%	0%
1% to 2%	0%
3% to 5%	2%
6% to 10%	5%
11% to 15%	13%
16% to 20%	26%
21% to 30%	20%
31% to 40%	19%
41% to 50%	15%
More than 50%	0%
Total	100%
Extrapolated value	25%

Q8. Approximately, what percentage of the IT security budget will be allocated to embedded device product security?	Pct%
< 1%	8%
1% to 2%	9%
3% to 5%	8%
6% to 10%	16%
11% to 15%	10%
16% to 20%	14%
21% to 30%	21%
31% to 40%	12%
41% to 50%	2%
More than 50%	0%
Total	100%
Extrapolated value	16%

Part 3. Supply chain security

Q9. How confident is your organization that it knows all vendors involved in the supply chain for each of its devices? Please use the 10-point scale below from 1 = no confidence to 10 = full confidence.	Pct%
1 or 2	20%
3 or 4	28%
5 or 6	30%
7 or 8	12%
9 or 10	10%
Total	100%
Extrapolated value	4.78

Q10. What impact have recent supply chain compromises such as the SolarWinds and Kaseya hack had on increasing investment in device and supply chain security? Please use the 10-point scale below from 1 = no impact to 10 = high impact.	Pct%
1 or 2	0%
3 or 4	6%
5 or 6	15%
7 or 8	35%
9 or 10	44%
Total	100%
Extrapolated value	7.84

Q11a. Does your organization have a security supply chain policy?	Pct%
Yes	21%
No (please skip to Q12)	79%
Total	100%

Q11b. If yes, does it include a risk assessment of the security development lifecycle (SDL) for third-party vendors supplying your organization with hardware and/or software?	Pct%
Yes	43%
No	57%
Total	100%

Q11c. If yes, does it include a direct risk assessment of the security of the supplied hardware and/or software, such as penetration testing, vulnerability scanning, requests for Software Bills of Materials and requests for security reports.	Pct%
Yes	39%
No	61%
Total	100%

Q12. Does your organization assess the security of its own products before they are shipped to customers?	Pct%
Yes	50%
No	50%
Total	100%

Part 4. Government regulation

Q13. Who should be **most responsible** for ensuring the security of IoT devices? Please select only one choice.	Pct%
Government	12%
Manufacturers	31%
Third-party software/vendors	40%
End-users	15%
Other (please specify)	2%
Total	100%

Q14a. Does the government (regulators) require your organization to provide details about the components in its devices or attest that embedded devices are secure?	Pct%
Yes	36%
No (please skip to Q15)	64%
Total	100%

Q14b. If yes, what is the ability of your organization to respond to these requests? Please use the 10-point scale below from 1 = no ability to 10 = high ability.	Pct%
1 or 2	5%
3 or 4	15%
5 or 6	17%
7 or 8	33%
9 or 10	30%
Total	100%
Extrapolated value	6.86

Part 5. Attributions about product security: Please respond to the following questions using the 5-point agreement scale from strongly agree to strongly disagree. **Strongly Agree and Agree response presented**.	Pct%
Q15. Product security is a priority in our organization.	41%
Q16. Our organization allocates sufficient resources to addressing product security.	36%
Q17. Our executive leadership team and/or board of directors requires assurances that product security is being assessed, managed and monitored appropriately.	27%
Q18. It is not possible to determine whether product security processes are sufficient to prevent a breach.	40%
Q19. Our product security processes and programs are reviewed frequently to ensure that they address evolving supply chain risks.	24%
Q20. The increase in supply chain and IoT attacks requires new approaches to product security strategy and tactics.	56%
Q21. Our organization finds it difficult to understand and manage the risks associated with each of our products.	44%
Q22. Our organization is increasing its investments into product security.	50%
Q23. Our organization finds it difficult to rapidly respond to new vulnerability disclosures that may affect our devices.	60%

Part 6. Types of security testing

Q24a. Does your organization conduct software composition analysis (SCA) for all your connected products' software?	Pct%
Yes	27%
No (please skip to Q25)	73%
Total	100%

Q24b. If yes, do your SCA tools work in your embedded/IoT device development processes?	Pct%
Yes	38%
No	62%
Total	100%

Q25. Can your organization easily generate a software bill of materials (SBOM) for each of its products?	Pct%
Yes	30%
No	70%
Total	100%

Q26. Does your organization conduct static analysis on all of the first party code in your products' software?	Pct%
Yes	30%
No	62%
Unsure	8%
Total	100%

Q27. Do your static analysis tools cover the instruction sets, chipsets and languages used in your organization's embedded/IoT devices?	Pct%
Yes	45%
No	48%
Unsure	7%
Total	100%

Q28. Do you conduct static analysis on all third-party code and binaries (including firmware) in your organization's products?	Pct%
Yes	37%
No	53%
Unsure	10%
Total	100%

Q29. Do you conduct dynamic testing for vulnerabilities before your organization's products go to market?	Pct%
Yes	38%
No	54%
Unsure	8%
Total	100%

Q30. Do you test for configuration vulnerabilities such as hardcoded credentials embedded secrets, misconfigured services, etc. in your organization's connected products' software?	Pct%
Yes	48%
No	43%
Unsure	9%
Total	100%

Q31. On average, what percentage of devices does your organization conduct manual penetration testing as part of the security review process?	Pct%
None	5%
1 to 10%	8%
11 to 20%	20%
21 to 30%	24%
31 to 40%	13%
41 to 50%	19%
51 to 75%	9%
76 to 100%	2%
Total	100%
Extrapolated value	30%

Q32a. Do you conduct manual penetration testing as part of the release process for your organization's devices?	Pct%
Yes	54%
No (please skip to Q33a)	46%
Total	100%

Q32b. If yes, how often do you conduct these tests?	Pct%
Annually	20%
Monthly	10%
As part of each major release	23%
As part of each software update	21%
Testing is not pre-scheduled	24%
Unsure	2%
Total	100%

Part 7. The impact of supply chain security on sales and customer relationships

Q33a. Do your organization's customers request detailed information about the components in its devices (e.g. SBOM, HBOM, SCA), when considering a purchase?	Pct%
Yes	45%
No (please skip to Q34)	55%
Total	100%

Q33b. If yes, what is the ability of your organization to respond to these requests? Please use the 10-point scale below from 1 = no ability to 10 = high ability.	Pct%
1 or 2	6%
3 or 4	11%
5 or 6	21%
7 or 8	35%
9 or 10	27%
Total	100%
Extrapolated value	6.82

Q34. How important is the security of an IoT device to your organization's customers? Please use the 10-point scale below from 1 = not important to 10 = high importance.	Pct%
1 or 2	3%
3 or 4	9%
5 or 6	12%
7 or 8	40%
9 or 10	36%
Total	100%
Extrapolated value	7.44

Q35. What is the impact of customers' concerns about the security of your organization's embedded devices impacting the length of its sales cycles? Please use the 10-point scale below from 1 = no impact to 10 = high impact.	Pct%
1 or 2	6%
3 or 4	8%
5 or 6	13%
7 or 8	37%
9 or 10	36%
Total	100%
Extrapolated value	7.28

Q36. How confident is your organization about its ability to respond to third-party risk questionnaires about the security of its products? Please use the 10-point scale below from 1 = no confidence to 10 = high confidence.	Pct%
1 or 2	12%
3 or 4	26%
5 or 6	25%
7 or 8	26%
9 or 10	11%
Total	100%
Extrapolated value	5.46

Q37. Does the sales team put pressure on those responsible for product security to attest to their security?	Pct%
Yes	55%
No	40%
Unsure	5%
Total	100%

Q38. Has your organization lost sales because of product security concerns?	Pct%
Yes	59%
No	37%
Unsure	4%
Total	100%

Q39. What regulations and compliance frameworks are relevant to your organization? Please select all that apply.	Pct%
NERC CIP-013	32%
IEC 62443 Part 4-2	27%
Executive Order 13920	23%
FDA Premarket Submissions for Management of Cybersecurity in Medical Devices	17%
California Senate Bill SB-327	34%
Oregon House Bill 2395	21%
FIPS 140 Security Requirements for Cryptographic Modules	44%
IT Security Act 2.0 in Germany	23%
HIPAA	18%
HiTrust compliance	11%
SDL certification	39%
SOCII certification	34%
ISO 27000 certification	41%
SOX I,II	29%
Section 889	12%
Total	405%

Part 8. Your Role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	7%
Vice President	8%
Director	15%
Manager	23%
Supervisor	14%
Technician/Staff	21%
Contractor	1%
Engineer	9%
Other	2%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
Chief Financial Officer	0%
Chief Operations Officer	1%
General Counsel	2%
Head, Manufacturing (GMP)	10%
Head, Product Engineering	15%
Head, Quality Assurances	8%
Chief Information Officer	19%
Chief Technology Officer	10%
Chief Information Security Officer	23%
Chief Security Officer	4%
Compliance Officer	2%
Data center management	2%
Chief Risk Officer	4%
Other	0%
Total	100%

D3. What best describes your organization's primary industry sector?	Pc%
Aerospace & defense	1%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Education & research	2%
Energy & utilities	5%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	9%
Hospitality	2%
Industrial & manufacturing	9%
Public sector	10%
Retail	8%
Services	9%
Technology & software	8%
Transportation & logistics	5%
Other	2%
Total	100%

D4. Where are your employees or contractors located? (check all that apply):	Pct%
United States	98%
Canada	67%
Europe	63%
Middle East & Africa	41%
Asia-Pacific	59%
Latin America (including Mexico)	40%

D5. What is the worldwide headcount of your organization?	Pct%
Less than 5,000 people	23%
5,001 to 10,000 people	24%
10,001 to 25,000 people	26%
25,001 to 75,000 people	19%
More than 75,000 people	8%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.