DARKReading RESEARCH

FEBRUARY 2022

2022 The State of Application Data Privacy and Security

skyflow

Executive Summary

Data from Dark Reading's the State of Application Data Privacy and Security 2022 survey shows that software engineering and security teams are working hard to satisfy the need for greater data access while delivering data privacy that meets or exceeds security and compliance requirements. Data privacy is rarely ignored by developers or IT teams anymore, and most engineering teams are at least somewhat knowledgeable about data privacy and security matters.

But at the same time, developers and IT teams still have a lot of work to do in order to gain mastery over data privacy and security. Few organizations have a complete understanding of where their data resides, or consider their in-house personnel to be extremely knowledgeable about security and privacy.

Key findings

This year's survey found that:

Data privacy knowledge is pretty good, but far from perfect

- 76% of organizations have at least a decent understanding of where sensitive data resides within systems and applications, but struggle to translate that into privacy-friendly architectures or suffer visibility gaps.
- Only 18% of organizations report having a perfect understanding of where data resides and then use that knowledge to guide how applications are architected.
- Only 27% of organizations are very knowledgeable about data security issues, and just 24% of respondents say they're very comfortable with data privacy compliance requirements.

Devs are shifting security left

- 83% of respondents say that functional security and data privacy requirements are mandatory in the design stages of new software projects.
- 57% of software builders say that they spend up to a quarter of their time working on satisfying data privacy and security requirements.
- Another 30% say they spend half or more of their time on these requirements.
- 55% of software development teams report that they have a privacy engineer or privacy champion who owns security. Of that group, 16% report having a dedicated person assigned to these duties.
- 23% of software builders meet security and privacy requirements using APIs, and 19% of software builders meet these requirements using pre-built code.

Safe data sharing is still a challenge

- 22% of software builders say they build their encryption functionality from scratch.
- 23% of software builders say they build their own tokenization functionality.
- 86% of respondents say secure data sharing is very important to their organization.
- But only 17% are able to share data externally via APIs; 68% say they don't share data externally due to security concerns.

Basic Software Data Privacy IQ

While many software and security teams have at least a basic awareness of where the sensitive data resides within their systems and applications, most struggle to maintain visibility into what's done with this data or to leverage it in a development process that optimizes data privacy.

Only 18% of organizations report they have a perfect understanding of where sensitive data resides and then use that knowledge to guide how applications are architected **(Figure 1)**. Another 39% say they know very well where the sensitive data is, but have a hard time translating this knowledge into privacy-friendly architectures. And 37% say they have a decent understanding of where the data generally is, but admit to struggling with visibility gaps. The good news is that among implementors, the percentage who say they have a perfect understanding of the data flows that guide privacy-centric design is higher (24%) than the total respondent base (18%).

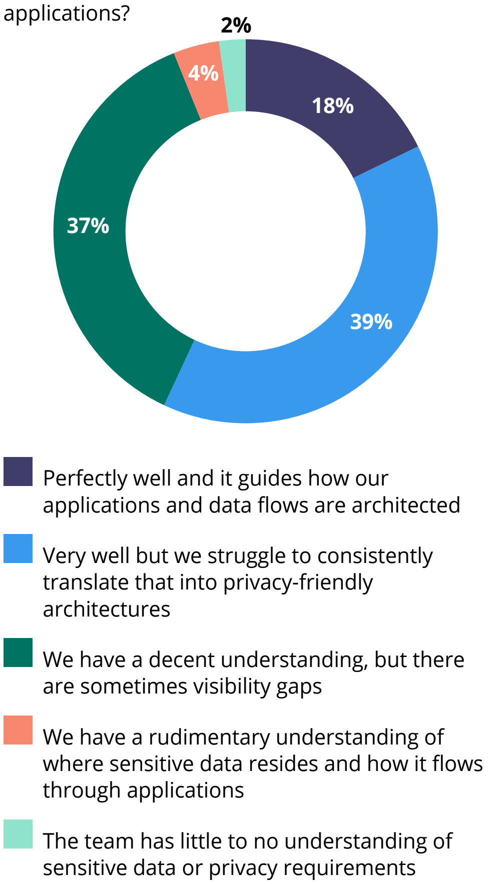
The survey indicates that there may be inflated expectations by application development and IT leaders about the security and data privacy "IQ" of their staffers, compared to what's actually happening out in the field. About 42% of leaders say their team is very knowledgeable about data security issues with regard to application design and architecture, compared to just 23% of implementors who believe the same.

In the same vein, 32% of senior leaders say their team has a very comfortable amount of knowledge specifically about data privacy compliance issues, but only 26% of implementors would say the same.

Figure 1.

Understanding Where Sensitive Data Resides

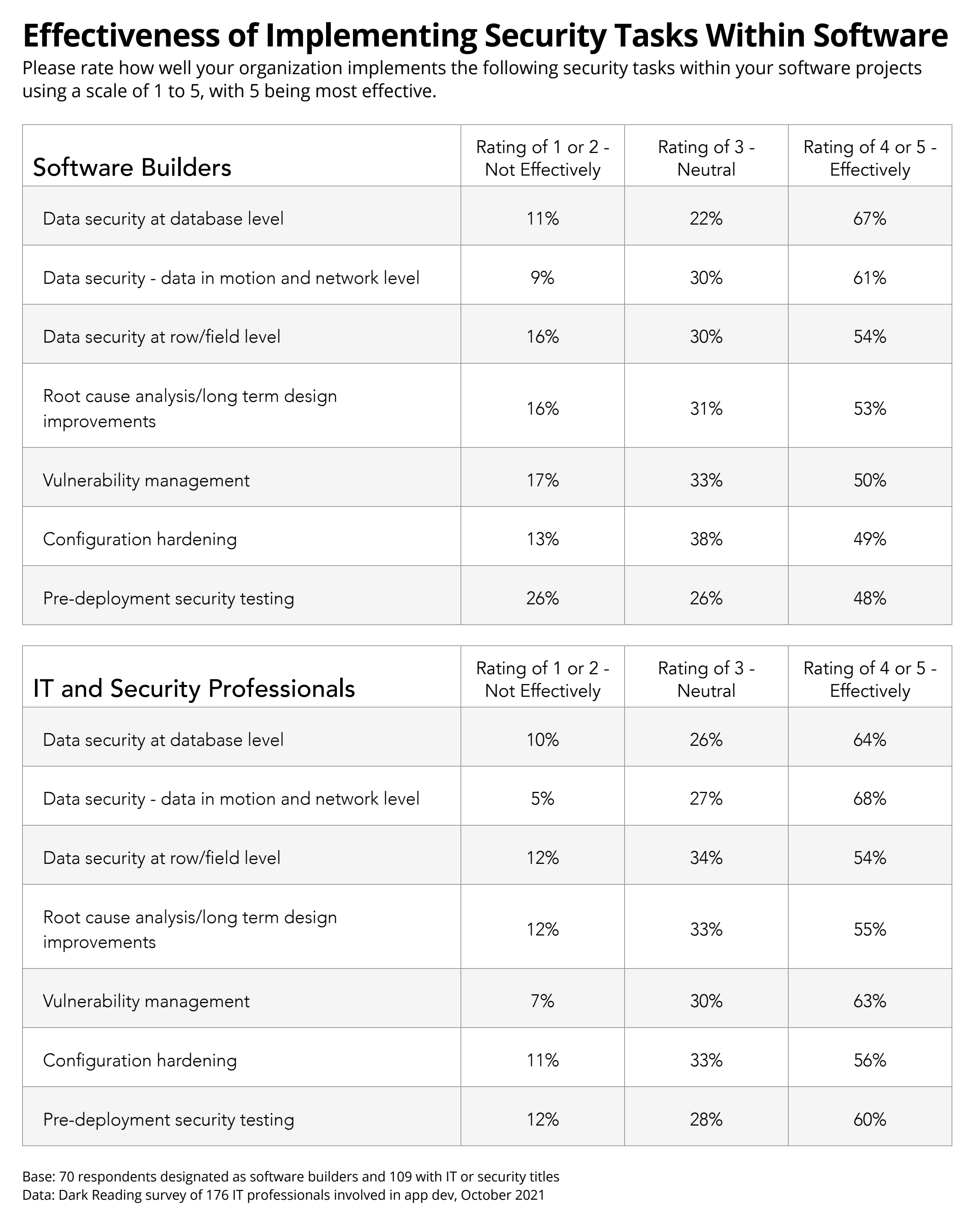
How well does your team understand where sensitive data resides in your systems and applications?



Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

Unsurprisingly, there is also a disparity of data privacy knowledge and comfort levels when comparing the population of software builders to their counterparts in IT operations and security teams. Some 30% of IT and security professionals report they're very knowledgeable about data privacy, while just 23% of builders would say the same. Meanwhile, when it comes to actually executing on that knowledge, there are differing opinions on performance levels. Interestingly, security and general IT practitioners report their organization is doing better than software builders do in many categories — this could be a difference in visibility into the additional security controls in place beyond software architecture. For example, 68% of IT and security professionals say that their organizations are effective to very effective about protecting data in motion and across the network, compared to 61% of software builders **(Figure 2)**.

Figure 2.



Effectiveness of Implementing Security Tasks Within Software

Please rate how well your organization implements the following security tasks within your software projects using a scale of 1 to 5, with 5 being most effective.

Software Builders	Rating of 1 or 2 - Not Effectively	Rating of 3 - Neutral	Rating of 4 or 5 - Effectively
Data security at database level	11%	22%	67%
Data security - data in motion and network level	9%	30%	61%
Data security at row/field level	16%	30%	54%
Root cause analysis/long term design improvements	16%	31%	53%
Vulnerability management	17%	33%	50%
Configuration hardening	13%	38%	49%
Pre-deployment security testing	26%	26%	48%

IT and Security Professionals	Rating of 1 or 2 - Not Effectively	Rating of 3 - Neutral	Rating of 4 or 5 - Effectively
Data security at database level	10%	26%	64%
Data security - data in motion and network level	5%	27%	68%
Data security at row/field level	12%	34%	54%
Root cause analysis/long term design improvements	12%	33%	55%
Vulnerability management	7%	30%	63%
Configuration hardening	11%	33%	56%
Pre-deployment security testing	12%	28%	60%

Base: 70 respondents designated as software builders and 109 with IT or security titles
Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

Many of these disparities could potentially indicate a false sense of security, with the software builders being more realistic about what actually happens day in, day out. For example, 60% of IT and security professionals report a favorable view of pre-deployment security testing, but only 48% report a favorable view among software builders.

Overall, we asked survey participants an open-ended question about their biggest data privacy challenges in building and securing software. Their responses ranged from troubling to predictable:

- "There is no defined data privacy policy for the data. Because of that there [are] no controls or checks in place. Everything is done at the last moment when needed."
- "Maintaining existing controls to data when there are new features which require change in underlying code."
- "Skills, technological interpretations of privacy processes, visibility of data."
- "Inventory challenge. In many organizations, sensitive data is pervasive across systems on premises."
- "Making sure [developers and applications] are compliant with our security certification."

When Data Privacy Is Built Into Applications

One of the core beliefs in the data privacy and security world is that to improve data security architectures, software teams need to "shift left," implementing security and privacy controls earlier in the software development lifecycle.

The results of this survey indicate a bright spot here: Overall, this shift is occurring, with 83% of our total respondent population reporting that when their organization plans a new software project, functional security and data privacy requirements are included at the design stages.

However, it is important to note that when we dig deeper we can see that the engineers in the field are still more challenged than leaders believe when it comes to ensuring that security and privacy requirements are set at the get-go. Approximately 86% of senior leaders say privacy requirements were accounted for at the design stage, compared to 72% of implementors.

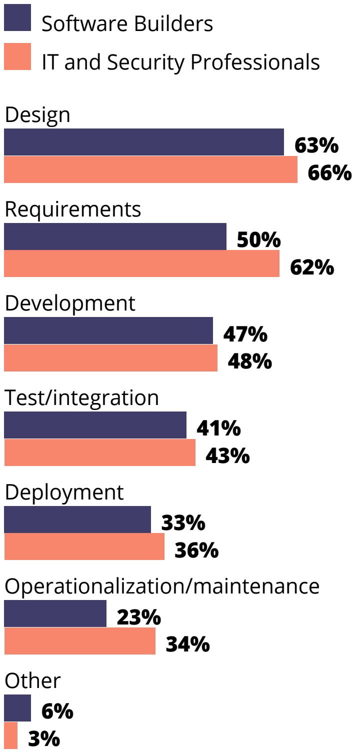
Similarly, there seem to be some differences of opinion between software builders and IT operations and security staff about when the design and implementation of privacy controls occur during the software development lifecycle (SDLC). While 62% of IT and security professionals say privacy compliance requirements come into play early, in the requirements definition phase of software development, only 50% of software builders would say the same **(Figure 3)**.

83% of the total respondent base reports that when their organization plans a new software project, functional security and data privacy requirements are included at the design stages.

Figure 3.

When Data Privacy Compliance Requirements Are Considered

At which stage of development do data privacy compliance requirements typically first come into play?



Note: Multiple responses allowed
Base: 70 respondents designated as software builders and 109 with IT or security titles
Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

Data Privacy Roles and Responsibilities

Overall, the good news is that very few software teams these days build software without putting at least some work into satisfying security or compliance requirements around data privacy.

Only 6% of software builders say they don't spend any time satisfying security requirements. The majority, approximately 57% of software builders, say that they spend up to a quarter of their time working on satisfying these requirements. And another 20% say they spend up to half of their time doing so.

Slightly less time is spent specifically on compliance, with 66% reporting that they spend up to a quarter of their time on this, and just 7% saying they dedicate half of their time specifically to compliance.

Another bright spot is the indication that it's increasingly common to have privacy specialists (privacy engineers and privacy champions) within organizations. Approximately 16% of our total respondents say that their team has a dedicated data privacy engineer or privacy champion on staff. Another 39% say that while they don't have a dedicated privacy specialist, they do have engineers or personnel who fulfill privacy-related duties.

In response to an open-ended question, the duties of privacy specialist roles varied, but answers tended to center around taking the lead for advocacy and advice, testing, and technical review, as well as documentation and tracking of execution.

One respondent explains that they employ a trained and skilled specialist who is tasked with building privacy into products and services at the technical level.

"This specialist can bring together the legal and compliance elements of privacy and work them into the organization's systems as they are developed," they write.

Interestingly, results indicate that the rise of this role may be the result of a grassroots movement driven by team members looking to better manage the learning and execution of responsibilities around data privacy. When we compare notes between leaders and implementors, only 14% of leaders thought they had privacy specialists on their teams, but 20% of implementors worked with privacy specialists.

As all teams work on improving their data privacy knowledge and satisfying privacy and security requirements, receiving guidance from security experts and legal professionals is key. The survey indicates that among all respondents the traditional route of internal and external training, along with testing and security, remain the top three primary methods for dispensing advice and guidance. However, those practices are still only in use at half (or fewer) of organizations, with the other half presumably leaving their software builders to fend for themselves.

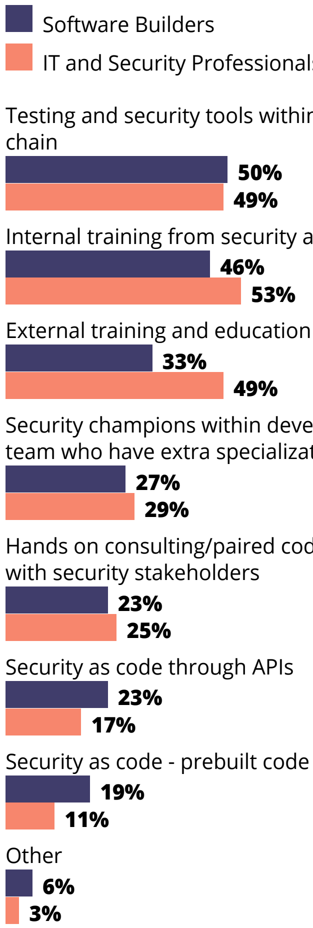
Meanwhile, a small but statistically significant number of organizations do lean on security as code, and use APIs and pre-built code to implement security and privacy controls without having to reinvent the wheel or spend tons of time researching guidance. Interestingly, some software builders seem to be proactively seeking this out on their own because while just 17% of IT and security professionals report the use of "security as code" through APIs, 23% of software builders say they utilize this resource **(Figure 4)**. And similarly, only 11% of IT and security professionals say their software team uses security as code via pre-built code, while 19% of builders say they do.

Nevertheless, there does seem to be a decent — though still minority — number of organizations for which security teams support software teams in their security and privacy work during the SDLC. Approximately 47% of security teams help with security feature integration, 41% provide some sort of security as code, and 34% provide automated testing and security guide rails in the development pipeline.

Figure 4.

Receiving and Implementing Security and Privacy Compliance Guidance

How are you most likely to receive and implement security and privacy compliance guidance regarding your applications?



Note: Maximum of three responses allowed
Base: 70 respondents designated as software builders and 109 with IT or security titles
Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

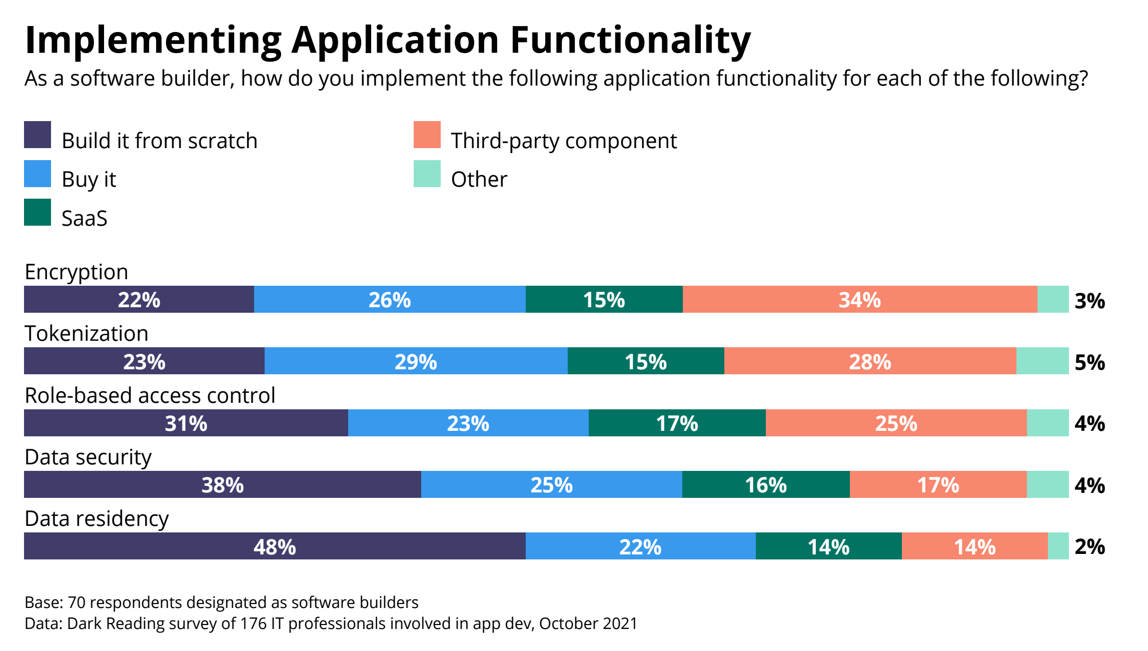
As all teams work on improving their data privacy knowledge and satisfying privacy and security requirements, receiving guidance from security experts and legal professionals is key.

Privacy Implementation Details

One of the oft-quoted sayings in security is "never roll your own crypto" because it is such an egregious example of reinventing the wheel with something that's not nearly as effective. And yet that seems to be exactly what several organizations are doing today.

Approximately 22% of software builders say they build their encryption functionality from scratch, and 23% say they build their own tokenization functionality **(Figure 5)**. Even more of them create their own role-based access control (31%), data security (38%), and data residency (48%) features from scratch.

Figure 5.



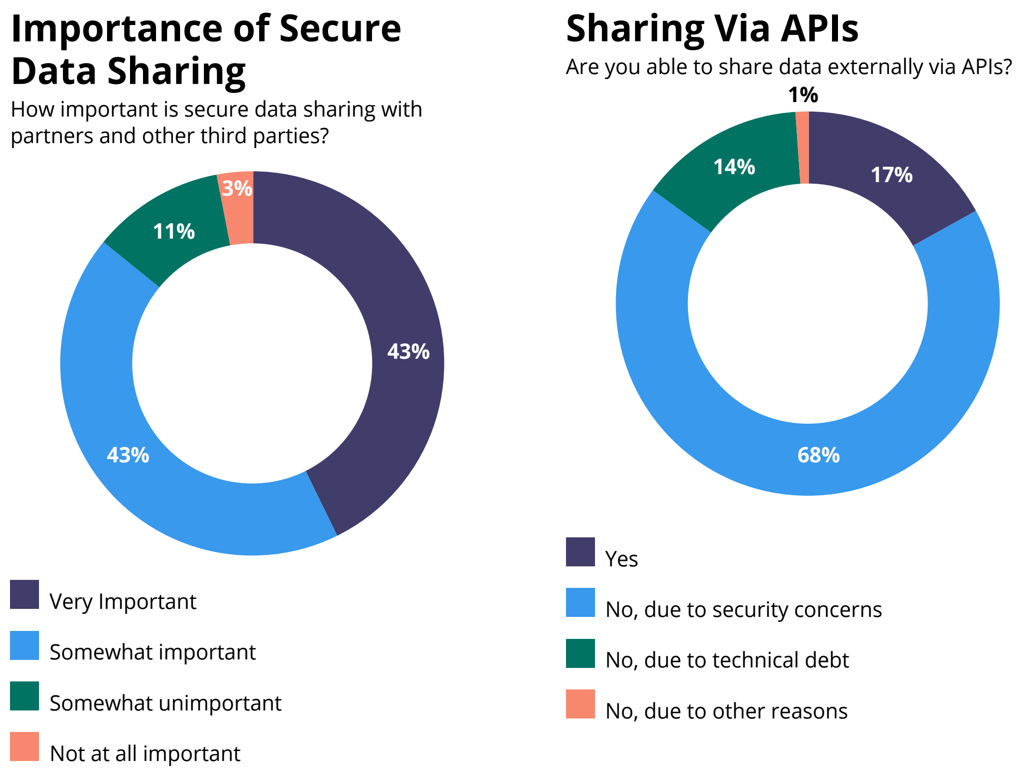
Base: 70 respondents designated as software builders
Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

Nevertheless, these DIY methods are still in the minority — combine answers for buying, picking up a service, or dropping in a third-party component, and you see that software builders still primarily look for help in one way or another. For encryption and role-based access control, a slim plurality looks to third-party components. For tokenization, data security, and data residency, builders are more likely to lean toward buying from an outside source.

When organizations do seek out tooling and services to help them implement data privacy functionality and systems, the No. 1 feature they look for is key management, followed closely by fine-grained access control. The third place is a tie between third-party integrations and auditability.

For all organizations, secure data sharing is an extremely important factor for the business. Eighty-six percent say it is somewhat important to very important to their organization **(Figure 6)**. However, how they provide that capability is highly variable.

Figure 6.



Importance of Secure Data Sharing

How important is secure data sharing with partners and other third parties?

Sharing Via APIs

Are you able to share data externally via APIs?

Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

Only about 17% are able to share data externally via APIs — 68% say they do not do so due to security concerns.

Meanwhile, when asked about other methods, answers included approaches as rudimentary as using VPNs, manual controls, and utilizing encrypted connections, highlighting the fact that secure data sharing is a big challenge for organizations.

How Organization Size Impacts Data Privacy Execution

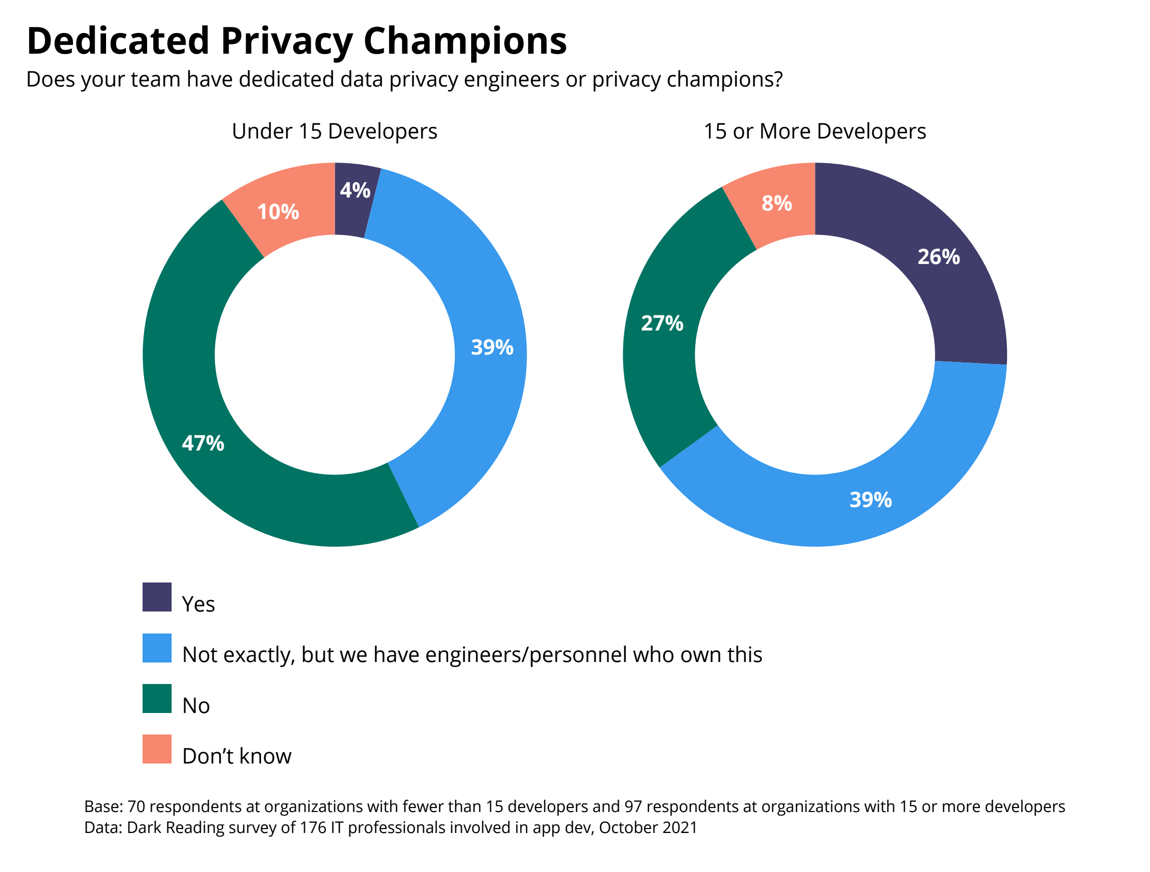
When we broke down survey results by organization size, differentiations definitely arose between smaller and larger teams. The data was examined with two main participant pools: those companies with fewer than 15 developers, and those with 15 or more. The general insight is that most companies of any size have concerns about their internal data privacy or security expertise, their processes, and their organization's depth of understanding of their data privacy issues. Also, it appears that all of these concerns are markedly more acute in smaller development teams.

For example, when judging the understanding of where sensitive data resides, only 12% of smaller teams could say that they have a perfect understanding, while 22% of larger teams report the same. An even more stark comparison comes when examining the ratios of teams who say they have privacy engineers or privacy champions.

Approximately 57% of smaller development teams say they don't have someone who owns these responsibilities or don't know if they have such an expert **(Figure 7)**. That's far more than the 35% of larger teams who report the same.

These results aren't surprising — the smaller the team, the less likely they are to be able to assemble the kind of special expertise and talent needed to build very strong data privacy infrastructure, and the more likely they are to have competing priorities spread across a smaller number of developers. They have the same privacy, security, and compliance issues as bigger teams, but fewer resources available to handle them.

Figure 7.



Dedicated Privacy Champions

Does your team have dedicated data privacy engineers or privacy champions?

Base: 70 respondents at organizations with fewer than 15 developers and 97 respondents at organizations with 15 or more developers
Data: Dark Reading survey of 176 IT professionals involved in app dev, October 2021

About skyflow

The team at Skyflow is dedicated to ensuring that sensitive data is stored and utilized safely and securely. Skyflow was founded in 2019. Our inspiration was the zero trust data privacy vaults giant companies like Apple and Netflix pioneered to protect, store, and manage the sensitive customer information that was at the core of their businesses. Our mission is to deliver data privacy vaults via a simple and elegant API, so every app and system can have best-of-breed data privacy.

Visit skyflow.com.

Survey methodology

Dark Reading conducted an online survey on behalf of Skyflow in October 2021 to explore trends in cloud security. The final data set is made up of 176 application development, IT, cybersecurity, and software engineering professionals at primarily North American organizations of all sizes. Respondents' titles range from CIO/CTO/CISO (18%), IT manager or group leader (22%), application development management (11%), cybersecurity management (10%), and other titles such as architect, IT staff, app dev staff, cybersecurity staff, and engineer. Sixty-four percent of respondents work at companies with 1,000 or more employees, and 20 industry sectors are represented.

Respondents were recruited via email invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Endnote

In looking at the various roles surveyed, we found it useful to aggregate survey participants into three groups: software builders, implementers, and IT and security professionals.

- Software builders are those most directly involved with designing and creating software. They include software engineers and other application development staff, and also include managers and leaders on the application development team and senior technical leaders (CTOs and architects).
- Implementers include those who create or interact directly with software. They include software engineers, other engineers, and staff members on application development, security, and general IT teams.
- IT and security professionals are those with a title of CIO, CISO, CSO, head of the security team, manager of the security team or IT team, engineer, or IT or security staff.