. More than 98% of respondents either already have an XDR solution in production, are planning to implement one, or are currently evaluating solutions (page 6).

. While organizations are most interested in gaining the ability to automatically detect and respond to threats and better prioritize responses, all of the use cases we asked about were rated highly (page 7).

. More than half of respondents (51.4%) said that ease of use was what they most needed in an XDR solution (page 8).

A . While 45.8% of respondents said that accurate threat detection was among the most important factors for choosing an XDR solution, only 30.8% cited cost (page 8).

. Nearly 40% of respondents believe that EDR, DLP, NDP, and TIP capabilities should be part of a cohesive, uni□ed XDR solution (page 9).

. Approximately 40% of survey participants view NDR and TIP as particularly important to integrate with an XDR solution (page 10).

. As a market category, XDR remains immature. As a result, there's a lack of agreement about which tools' capabilities should be included in an XDR solution, and which should be integrated (page 9 and page 10).

. Over 93% of respondents agree that implementing XDR will improve their organization's ability to mitigate cyber threat risks and lower costs (page 11).

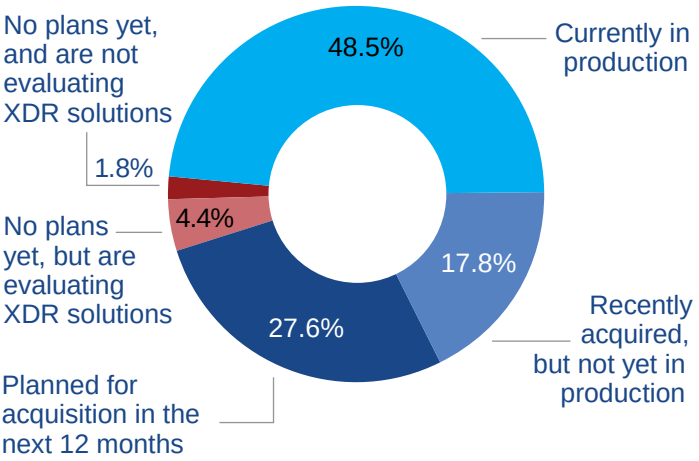


Figure 1: Percentage of organizations with XDR solutions currently in production, as well as organizations with and without plans to acquire them.

XDR is an emerging technology category that's received a great deal of analyst and media attention of late because it promises to improve e□ciency in security operations, as well as to enhance the visibility and capabilities that even resource-constrained teams can achieve. In this survey, we asked participants if they had already adopted and implemented an XDR solution, or if they were planning to do so within the next 12 months (see Figure 1).

A large majority of respondents (more than 98%) reported that they already have an XDR solution in production, are planning to acquire one or implement one, or are currently evaluating vendors and solutions.

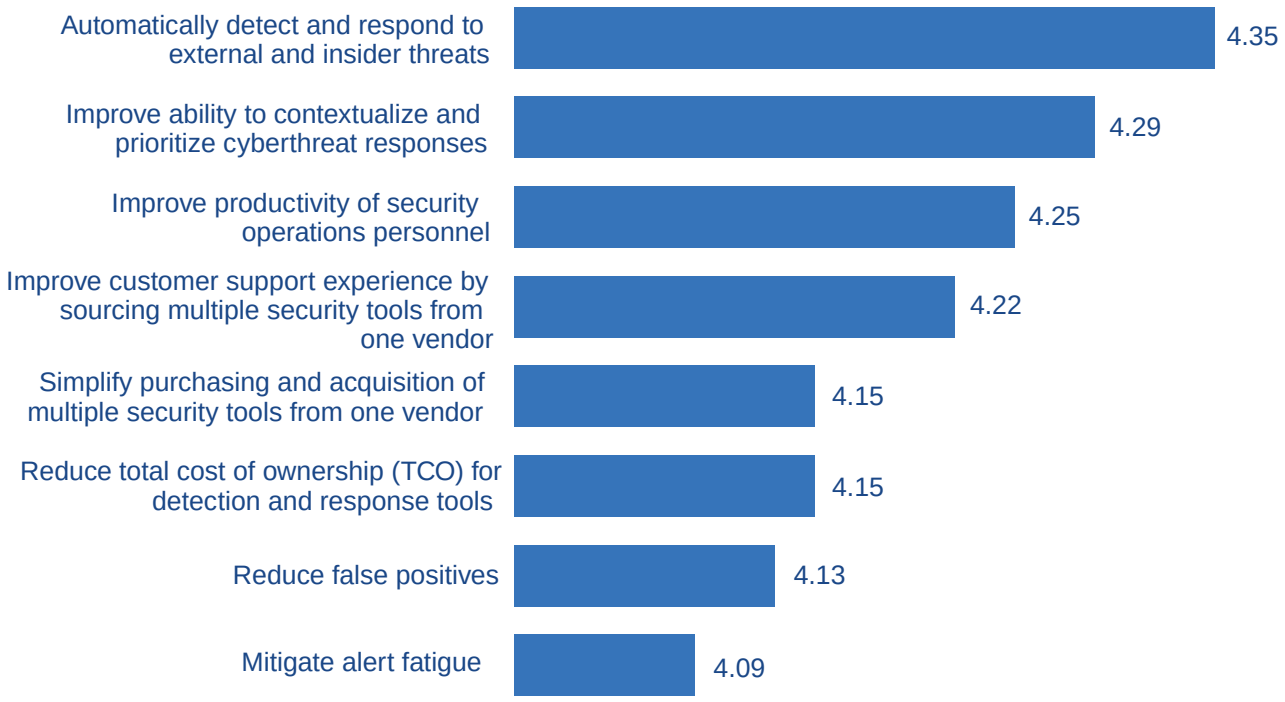


Figure 2: Most important use cases for XDR

We've already determined that organizations are embracing XDR. With more than 98% of organizations already having a solution in place or planning to implement or acquire one (see Figure 1), it's clear that awareness of the bene□ts of this emerging technology is high.

To better understand the motivations of organizations that are enthusiastically adopting XDR, we asked survey participants which XDR use cases were most important to them. As it turns out, all of them!

Every one of the use cases we asked about was rated higher than 4.0 on a □ve-point scale where 1 is of little importance and 5 is the highest level of importance (see Figure 2). Responses were tightly clustered, meaning that all use cases were considered to be similarly important.

The two use cases with the highest importance ratings were automatically detecting and responding to external and insider threats (4.35) and improving the ability to contextualize and prioritize cyberthreat responses (4.29). But even the use case with the lowest importance rating, mitigating alert fatigue, was still considered to be of the highest importance by 38% of respondents. In fact, all the use cases were rated as having high (4) or highest (5) importance by more than 76% of respondents.

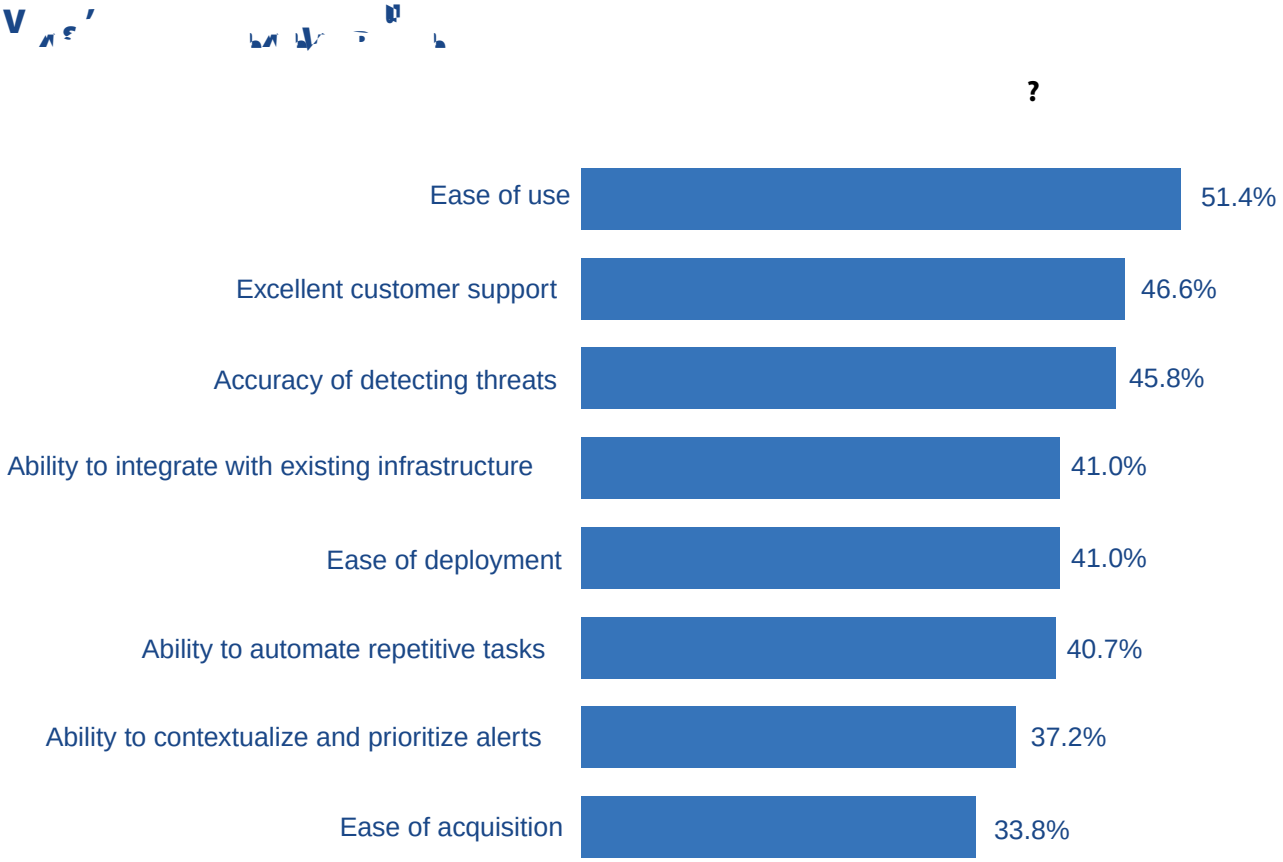


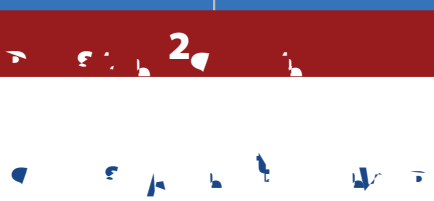
Figure 3: Most important factors when evaluating XDR vendors.

Many security programs are implementing or seeking out XDR solutions with hopes of enhancing their security team's productivity and strengthening detection and response capabilities. However, the number of vendors entering this fast-growing market is rapidly increasing. We were curious which factors were most important to XDR solution buyers, and what key differentiators might set best-of-breed solutions apart.

The most often-cited qualities that organizations are looking for in an XDR solution include ease of use (cited by 51.4% of respondents) and excellent customer support (cited by 46.6% of respondents) (see Figure 3). XDR's perceived complexity is apparently a concern for many potential buyers, who want to find solutions that will make security operations teams' jobs easier while enabling them to accomplish more. Also important was accuracy of detecting threats (cited by 45.8% of respondents). For 40.7% of respondents, the ability to automate repetitive tasks mattered.

Third-party validation (by analyst firms such as Gartner or Forrester) was the least important factor overall, mentioned by only 19.9% of respondents. This suggests that a vendor who is able to demonstrate a solution's accuracy, ease of use, and top-notch customer support may be able to overcome a lack of third-party validation to gain market share.

Cost was also among the least important factors, with only 30.8% of respondents indicating that they thought it was important. It's likely that many organizations expect that implementing XDR will help them to lower security operational costs overall, so much so that the cost of the solution itself isn't deemed critically important.



.69.5351 0.1 18 ( ) -4.,

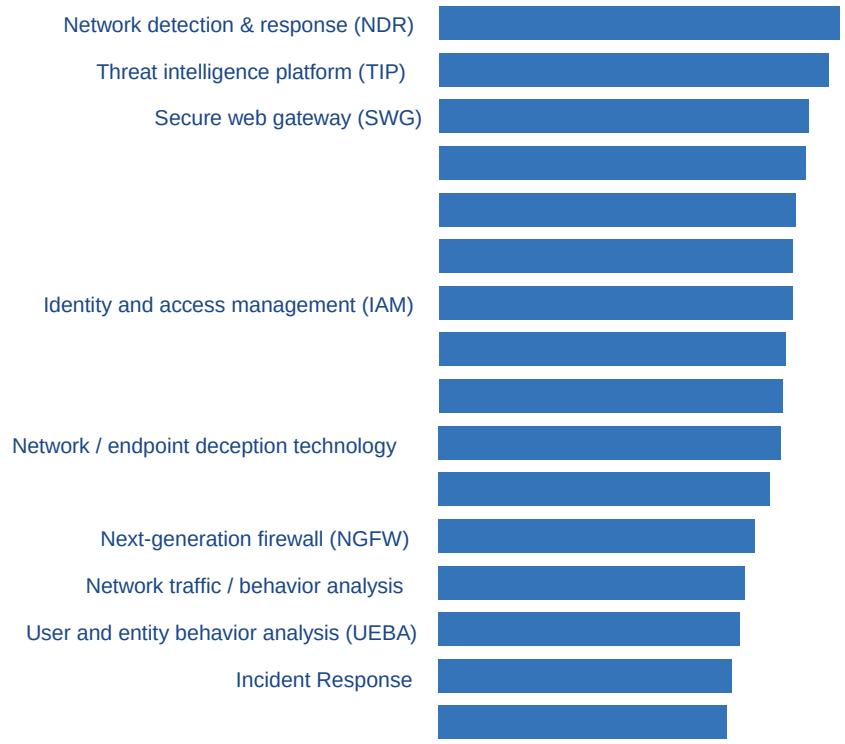


Figure 5: Tools that should be integrated to achieve comprehensive XDR.

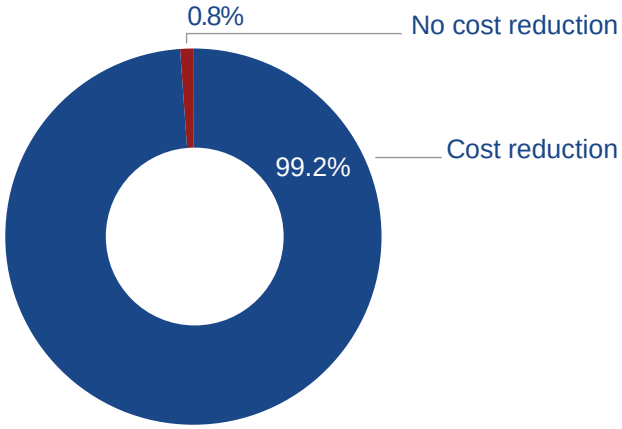


Figure 8: Percentage of organizations expecting to see a cost reduction from XDR's adoption.

There's great con□dence among security leaders and practitioners that XDR will quickly pay for itself, and this con□dence is consistent across industries and geographies. Over 99% of survey participants said that they expect to see a cost reduction from implementing XDR (see Figure 8). The global mean cost reduction that they expected to see was 25.0%.

Organizations in some highly regulated industries are anticipating particularly large cost reductions from implementing XDR. Respondents in □nancial services are expecting to see a mean cost reduction of 32.9%, while those in healthcare expect to see a 27.4% cost reduction (see Figure 9).

Overall, it's clear that there's near-universal agreement in the market that XDR's adoption has the potential to create e□ciencies that will lower costs. With cybersecurity spending continuing to climb year after year, this is among XDR's most promising possible bene□ts.

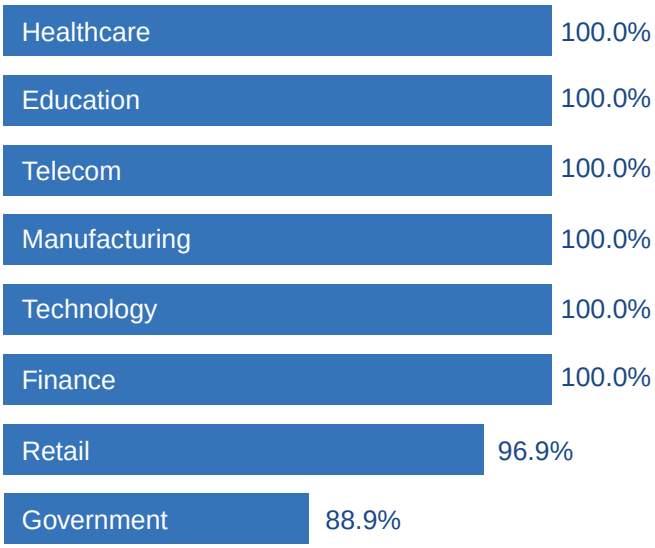


Figure 9: Percentage of organizations expecting to see a cost reduction from XDR's adoption, by industry.

Figure 10: Security operations staff efficiency improvements to be realized from implementing XDR.

We took a closer look to see which security operations staff efficiency improvements, commonly realized by organizations embracing XDR, were perceived as most impactful by survey participants. All of the efficiency improvements we asked about were perceived as important by a majority or near-majority of respondents (see Figure 10). Even the improvement that was ranked as important least often, streamlining communication across disparate security teams, was still considered important by 46.8% of respondents.

Given the enthusiasm for XDR's adoption, it's unsurprising that more than 98% of respondents believe that XDR will improve security operations staff efficiency. Beyond this general agreement, reducing the average time to remediate successful cyberattacks was ranked among the most impactful efficiency improvements by 58.3% of respondents, while 55.7% ranked reducing the average time to respond to security alerts as most impactful.

Of course, when it comes to reducing the impact of a security incident, time is of the essence, so it's only to be expected that speeding remediation and response would be important to security professionals. However, given the extent of the challenges that today's security operations teams face, it's logical that all efficiency improvements to be gained from adopting XDR would be of significant value.

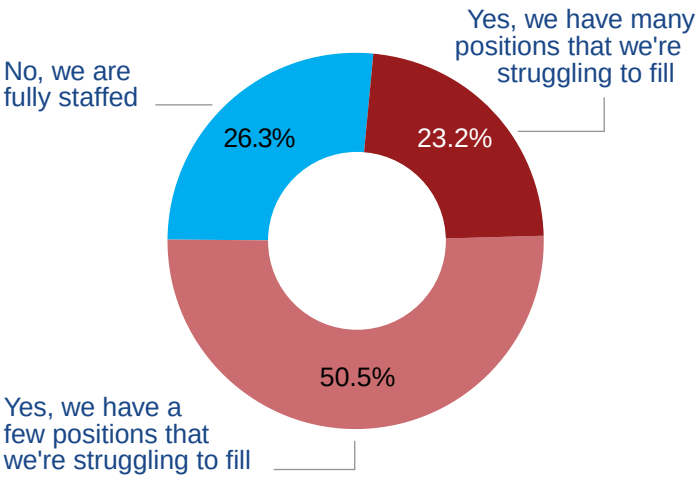


Figure 11: Percentage of organizations experiencing IT security personnel shortages.

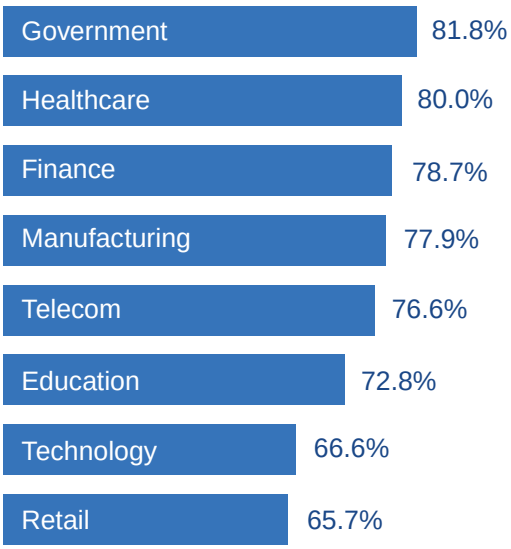


Figure 12: Percentage of organizations experiencing IT security personnel shortages, by industry.

?

We're all aware that the scarcity of talent is a perennial problem in the cybersecurity industry. We wanted to see how broadly this issue was re□ected in the survey participant population, so we asked how many respondents were currently experiencing shortages of skilled IT security personnel. More than 73% of respondents are in organizations that are currently struggling to □ll at least some positions (see Figure 11).

Sta□ng shortages are particularly acute in highly regulated industries like □nancial services, where 78.7% of organizations have un□lled IT security positions, healthcare, where 80% of organizations have un□lled positions, and government, where 81.8% of organizations have un□lled positions (see Figure 12). Severe sta□ng shortages—in which organizations have many positions that they're struggling to □ll—are particularly prevalent in the U.S., impacting 37.5% of respondents there.

If anything, we were surprised to see that 26.3% of survey participants say that their security program was fully sta□ed. Even so, the need for e□ciency improvements that can be gained from implementing technologies like XDR is readily apparent elsewhere in this survey

?

Figure 15: Most important factors when evaluating MXDR providers.

1

This report is based on survey responses from 400 qualified participants from eight countries (see Figure 16). Each respondent was required to have a role as a leader or practitioner in IT security (see Figure 17). One-third (33%) of respondents held executive positions such as Chief Information Officer (CIO), Chief Information Security Officer (CISO), or VP of IT security operations. More than two-thirds (77%) held management or executive positions.

1

All participants in this survey were working for organizations with 500 or more employees (see Figure 18). They spanned 17 industries (plus "Other") with no single industry composing more than 16% of the total participants. For selected questions, additional analysis was conducted based on the industries with larger numbers of respondents (see Figure 19). Those eight industries—government, telecommunications, retail, □nance, manufacturing, education, and healthcare—had almost three-fourths of all participants.

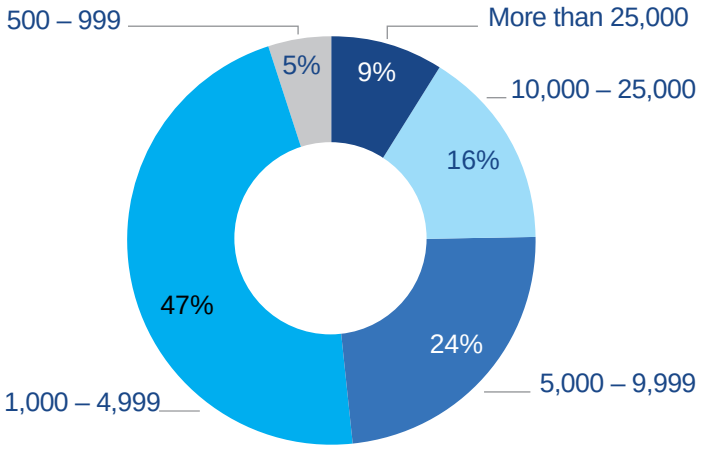


Figure 18: Survey respondents by organization employee count.

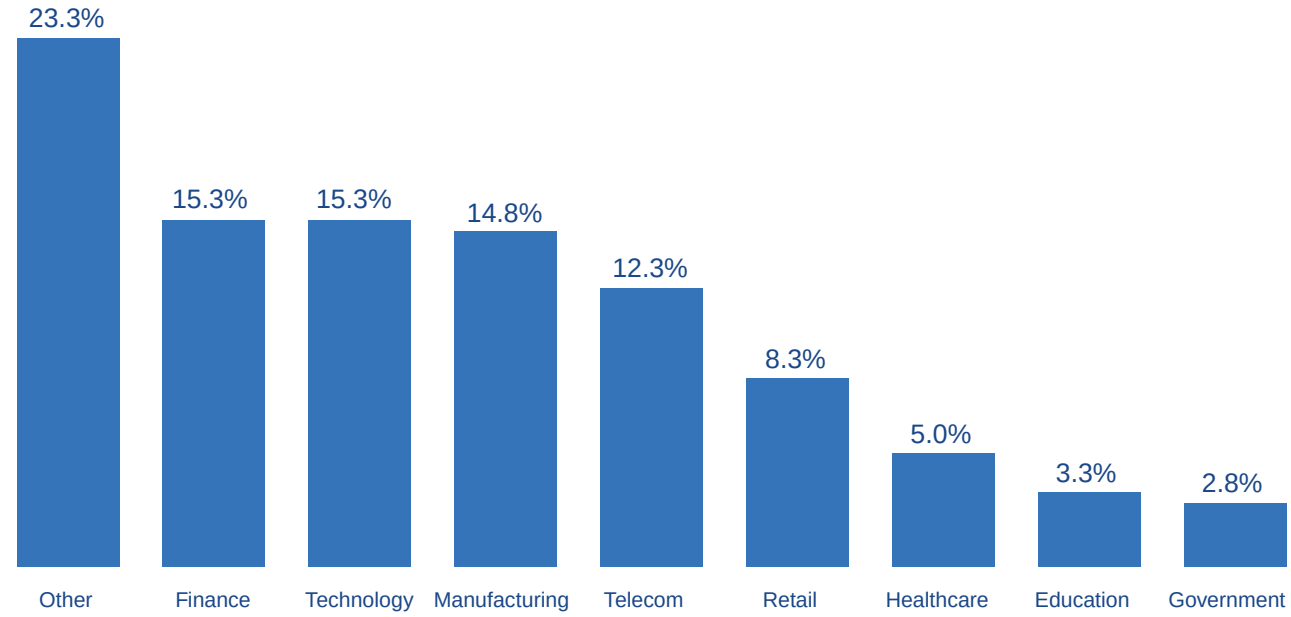


Figure 19: Survey respondents by industry.

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

800.327.8711

WWW.CYBER-EDGE.COM

INFO@CYBER-EDGE.COM