Q4 Company

NEWS RELEASE

New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed

10/3/2023

Sixty-two percent say that organizations underreport cyberattacks

SCHAUMBURG, Ill.--(BUSINESS WIRE)-- New cybersecurity data hones in on where cybersecurity pros come up short, with soft skills, cloud computing, and security controls emerging as the biggest skills gaps in today's cybersecurity professionals, according to ISACA's annual research report, **State of Cybersecurity 2023, Global Update on Workforce Efforts, Resources and Cyberoperations**.

More than 2,000 security leaders share their insights on the latest cybersecurity threat landscape, hiring challenges and opportunities, budgets, and more in ISACA's ninth annual State of Cybersecurity study. These findings are key to helping shape action plans, as

Fifty-nine percent of cybersecurity leaders say their teams are understaffed, according to the ninth annual survey—which explores the latest cybersecurity threat landscape, hiring challenges and opportunities, and budgets, with insights from more than 2,000 security leaders around the world. The report, sponsored by Adobe, also shows that 50 percent of respondents indicated that they have job openings for nonentry level roles, compared to 21 percent with job openings for entry-level positions.

Staffing and Skills

The research indicates some strides have been made in addressing employee retention, but it continues to be a challenge. More than half (56 percent) of cybersecurity leaders say they have difficulty retaining qualified cybersecurity professionals, though this number is down four points from last year.

Continuing to reduce retention woes may be difficult, however, given that benefits offered to

organizations continue to grapple with a complicated threat landscape and understaffed teams. (Graphic: ISACA)

cybersecurity pros have been declining—potentially driven by economic uncertainty. University tuition reimbursement dropped five percentage points to 28 percent, recruitment bonuses fell two percentage points, and reimbursement of certification fees dropped by a percentage point, compared to 2022.

When hiring, respondents say they are looking for the following top five technical skills in cybersecurity pros:

1. Identity and access management (49 percent)
2. Cloud computing (48 percent)
3. Data protection (44 percent)
4. Incident response (44 percent)
5. DevSecOps (36 percent)

When looking at soft skills, communication (58 percent), critical thinking (54 percent), problem-solving (49 percent), teamwork (45 percent) and attention to detail (36 percent) come in as the top five skills employers are seeking in cybersecurity job candidates. The skills of empathy (13 percent) and honesty (17 percent) came in lower in importance—a noteworthy finding given that 62 percent of respondents believe organizations underreport cybercrime.

Respondents examined where cybersecurity professionals are lacking—citing soft skills (55 percent), cloud computing (47 percent), security controls (35 percent), coding skills (30 percent) and software development-related topics (30 percent) as being the biggest skills gaps they see today.

To mitigate these technical skills gaps, respondents indicate their top three approaches are training nonsecurity staff who are interested in moving into security roles (45 percent), increasing usage of contract employees or outside consultants (38 percent), and increasing use of reskilling programs (21 percent). When addressing nontechnical skills gaps, organizations are leveraging online learning websites (53 percent), mentoring (46 percent), corporate training events (42 percent) and academic tuition reimbursement (20 percent), though the use of tuition reimbursement has fallen by four percentage points.

“The soft skills gaps we see among cybersecurity professionals are part of a concerning systemic issue that our industry needs to take seriously,” says Jon Brandt, ISACA Director, Professional Practices and Innovation. “While there is no simple solution, addressing these needs with a collaborative approach that goes beyond traditional academia to involve hands-on training, mentorship, and other learning pathways can make an impact not only on individual skillsets and enterprise security outcomes, but also on the integrity of the profession as a whole.”

Cybersecurity Threats

When looking at the cybersecurity threat landscape, nearly 48 percent indicate that their organization is experiencing more cyberattacks compared to a year ago. Despite the difficult threat landscape, only 42 percent have a high degree of confidence in their cybersecurity team's ability to detect and respond to cyber threats.

The top three attack concerns remain the same as last year—enterprise reputation (79 percent), data breach concerns (69 percent) and supply chain disruptions (55 percent). Respondents also indicated that social engineering (15 percent) remains the main type of cyberattack they experience, an increase of two percentage points. This is followed by:

- Advanced persistent threats (11 percent)
- Ransomware (10 percent)
- Security misconfiguration (10 percent)
- Unpatched system (10 percent)
- Denial of service (9 percent)
- Sensitive data exposure (9 percent)

Looking Ahead

Seventy-eight percent of survey respondents say demand for technical cybersecurity individual contributors will increase in the next year, and nearly half (48 percent) expect an increased demand for cybersecurity managers. More than half (51 percent) believe that cybersecurity budgets will at least somewhat increase as well next year.

"The cybersecurity workforce specifically faces a significant talent gap. Adobe believes that great talent can come from anywhere – and sustained investment both by our industry and governments worldwide will be critical to developing a diverse pipeline of talent to help us all address this growing gap," says Maarten Van Horenbeeck, Senior Vice President and Chief Security Officer at Adobe. "This is especially critical when it comes to being able to respond to the evolving complexity and ingenuity in the cybersecurity threat landscape, accelerated by AI technologies."

Learn More

Brandt and Van Horenbeeck will discuss these findings further in a webinar taking place on 3 October at 12:00 PM EDT (16:00 UTC). To register, visit **https://store.isaca.org/s/community-event?id=a334w000005hEsVAAU**.

A complimentary copy of the State of Cybersecurity 2023 survey report can be accessed at **www.isaca.org/state-of-cybersecurity-2023**, along with related resources. Additional cybersecurity resources can be found at

www.isaca.org/resources/cybersecurity.

About ISACA

ISACA® (**www.isaca.org**) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 165,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

Twitter: **www.twitter.com/ISACANews**
LinkedIn: **www.linkedin.com/company/isaca**
Facebook: **www.facebook.com/ISACAGlobal**
Instagram: **www.instagram.com/isacanews**

communications@isaca.org
Emily Ayala, +1.847.385.7223
Bridget Drufke, +1.847.660.5554

Source: ISACA