Security Conference

Skills Short, Threats Deep

How to Foster and Retain a Security Team amongst a Significant Workforce Gap

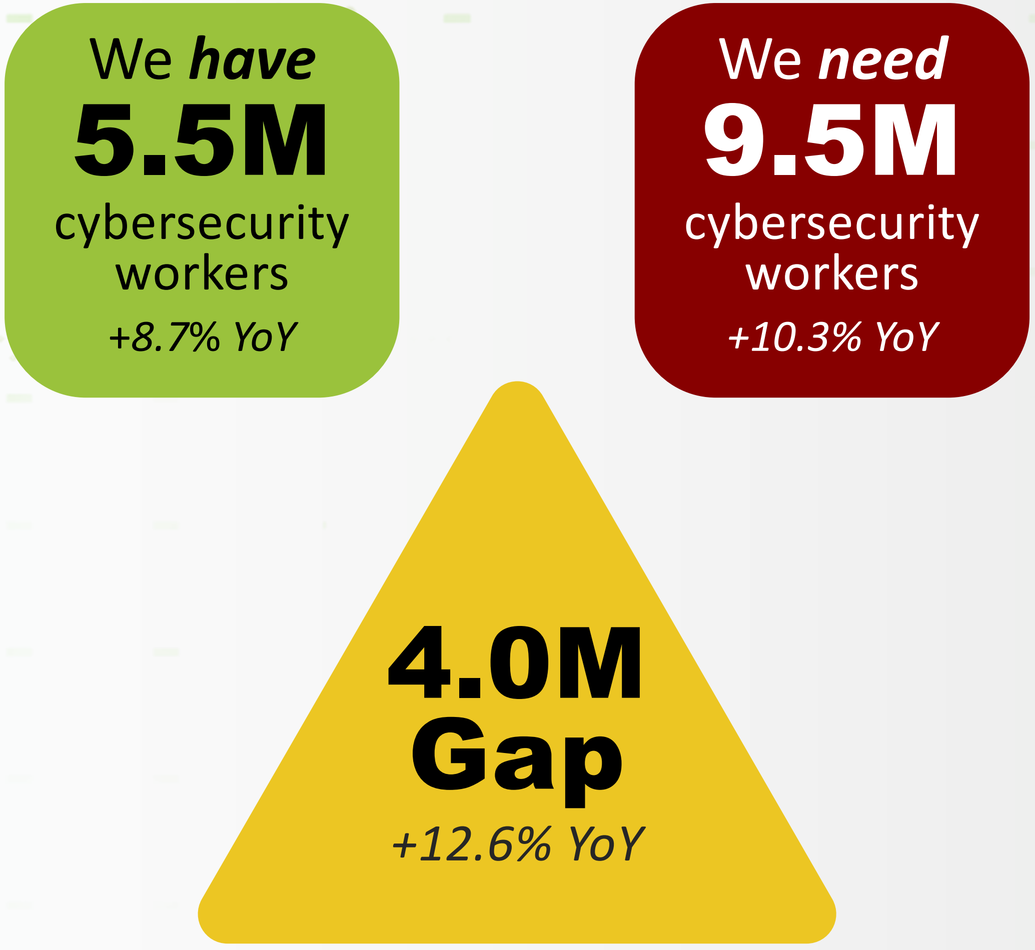
Presented by: Jon France, CISO

18/10/2023

ISC2™

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 500,000 members, candidates and associates around the globe are a force for good, safeguarding the way we live.

Unfilled demand for information and systems security professionals is growing globally



We *have*

5.5M

cybersecurity workers

+8.7% YoY

We *need*

9.5M

cybersecurity workers

+10.3% YoY

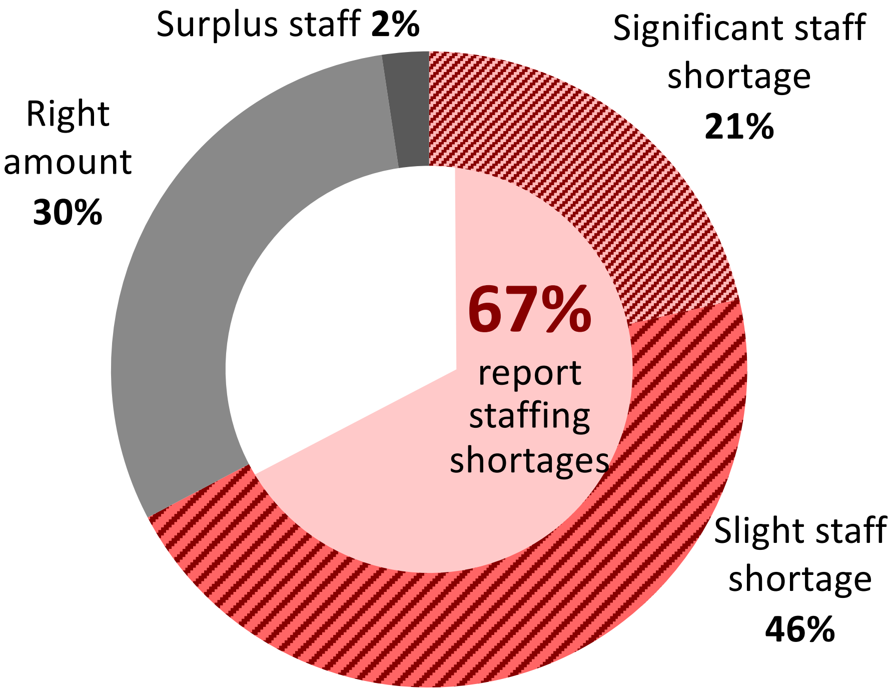
4.0M Gap

+12.6% YoY

+73% Needed to close the gap

Source: 2023 ISC2 Cybersecurity Workforce Study.

There’s a critical need for cybersecurity staff



Industries with the ***greatest*** shortage

Education **(78%)**
Government **(78%)**
Nonprofit **(76%)**
Military/military contractor **(76%)**
Aerospace **(75%)**

Industries with the ***lowest*** shortage

Consulting **(54%)**
Hosted/cloud services **(55%)**
Security software/hardware development **(60%)**
Engineering **(61%)**
Telecommunications **(62%)**

Source: 2023 ISC2 Cybersecurity Workforce Study.

Without enough cybersecurity staff...

50%

Not enough time for proper risk assessment and management

45%

Oversights in process and procedure

38%

Misconfigured systems

38%

Slow to patch critical systems

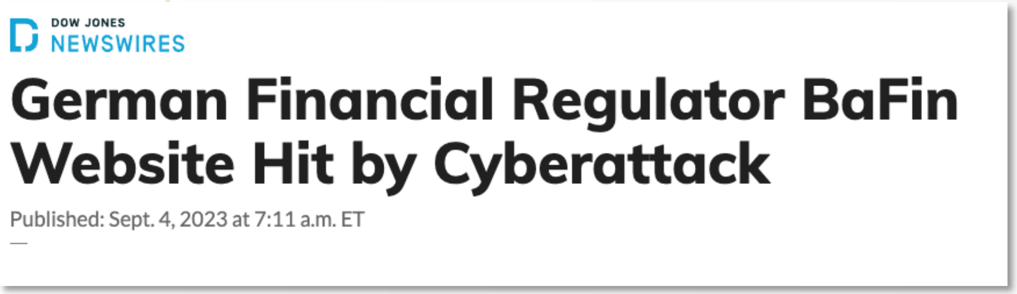
35%

Can't remain aware of all active threats against the network

34%

Not enough time to adequately train each cybersecurity team member

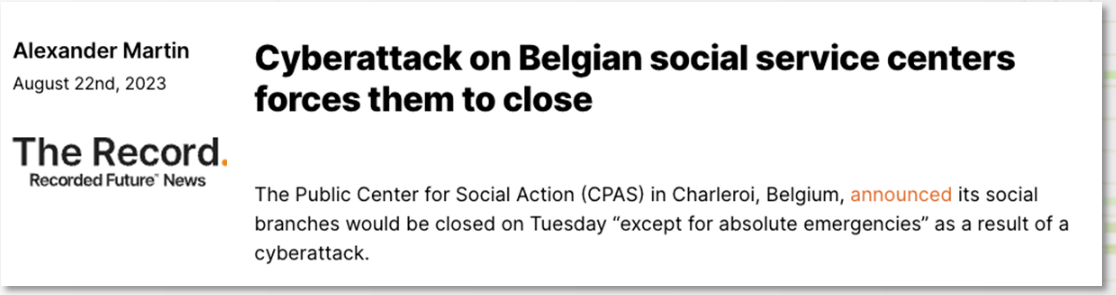
Source: 2023 ISC2 Cybersecurity Workforce Study.



DOW JONES NEWSWIRES

German Financial Regulator BaFin Website Hit by Cyberattack

Published: Sept. 4, 2023 at 7:11 a.m. ET

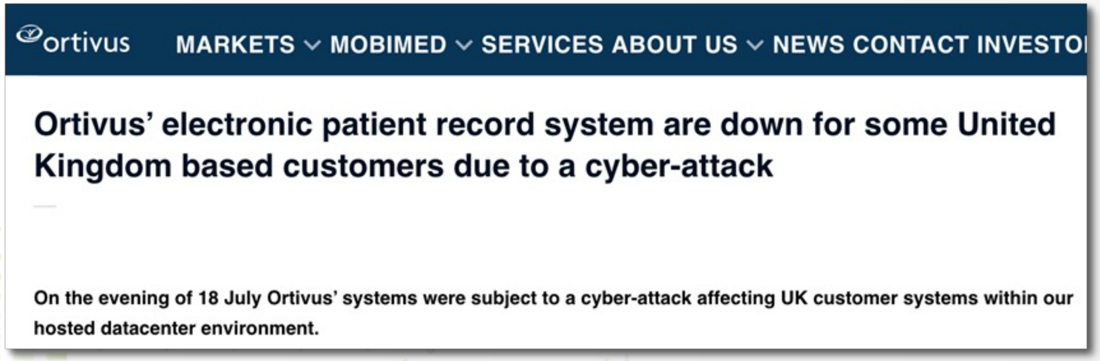


Alexander Martin
August 22nd, 2023

The Record.
Recorded Future® News

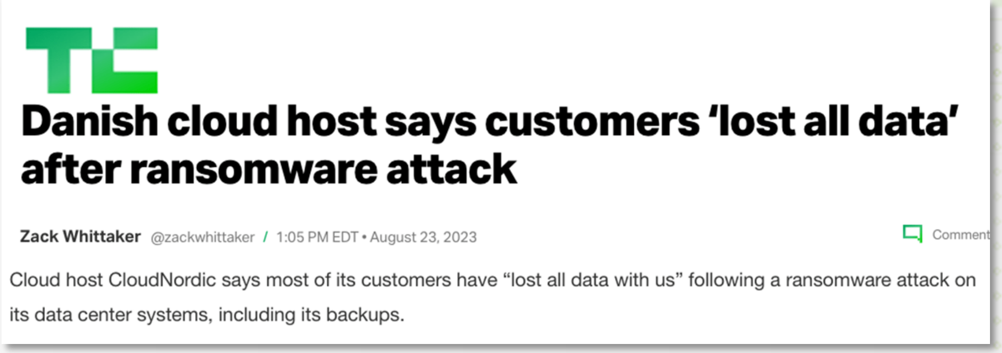
Cyberattack on Belgian social service centers forces them to close

The Public Center for Social Action (CPAS) in Charleroi, Belgium, announced its social branches would be closed on Tuesday "except for absolute emergencies" as a result of a cyberattack.



Ortivus' electronic patient record system are down for some United Kingdom based customers due to a cyber-attack

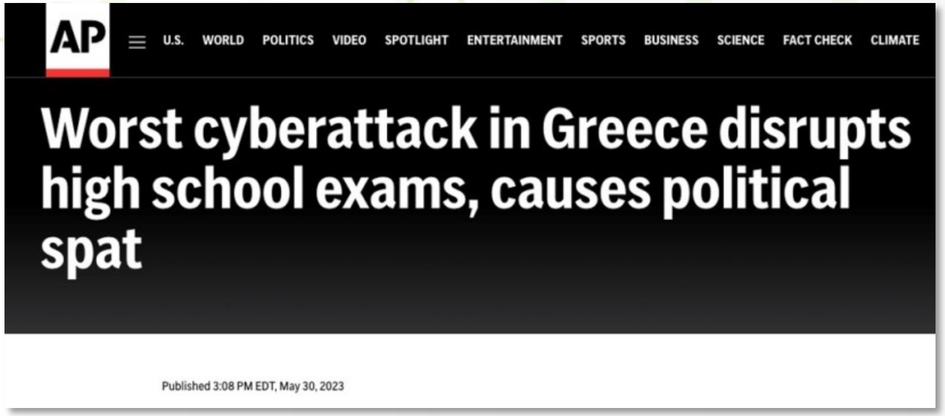
On the evening of 18 July Ortivus' systems were subject to a cyber-attack affecting UK customer systems within our hosted datacenter environment.



Danish cloud host says customers 'lost all data' after ransomware attack

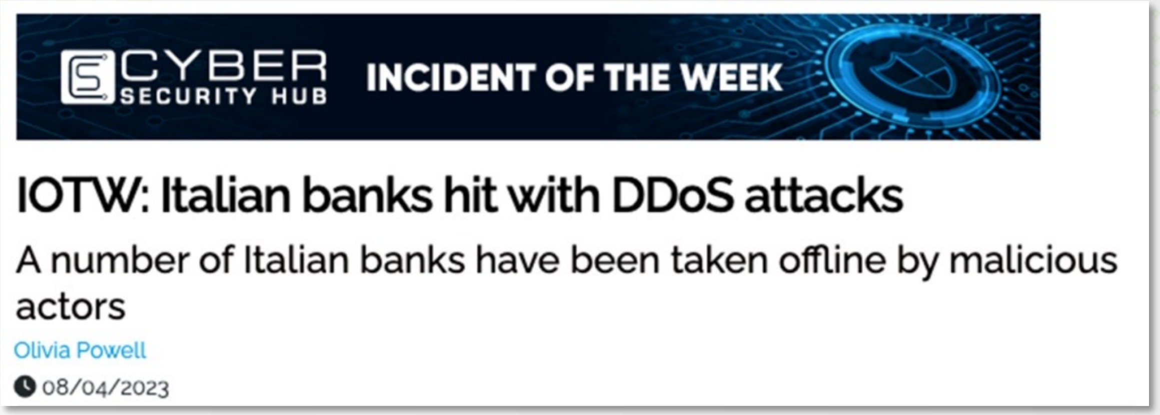
Zack Whittaker @zackwhittaker / 1:05 PM EDT • August 23, 2023

Cloud host CloudNordic says most of its customers have "lost all data with us" following a ransomware attack on its data center systems, including its backups.



Worst cyberattack in Greece disrupts high school exams, causes political spat

Published 3:08 PM EDT, May 30, 2023



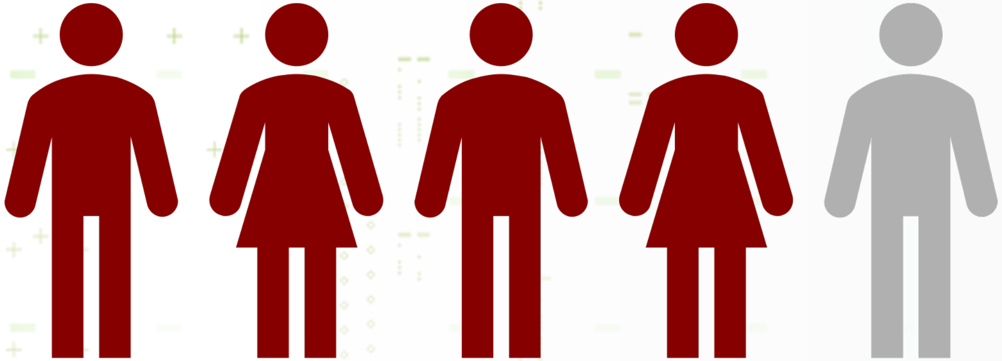
IOTW: Italian banks hit with DDoS attacks

A number of Italian banks have been taken offline by malicious actors

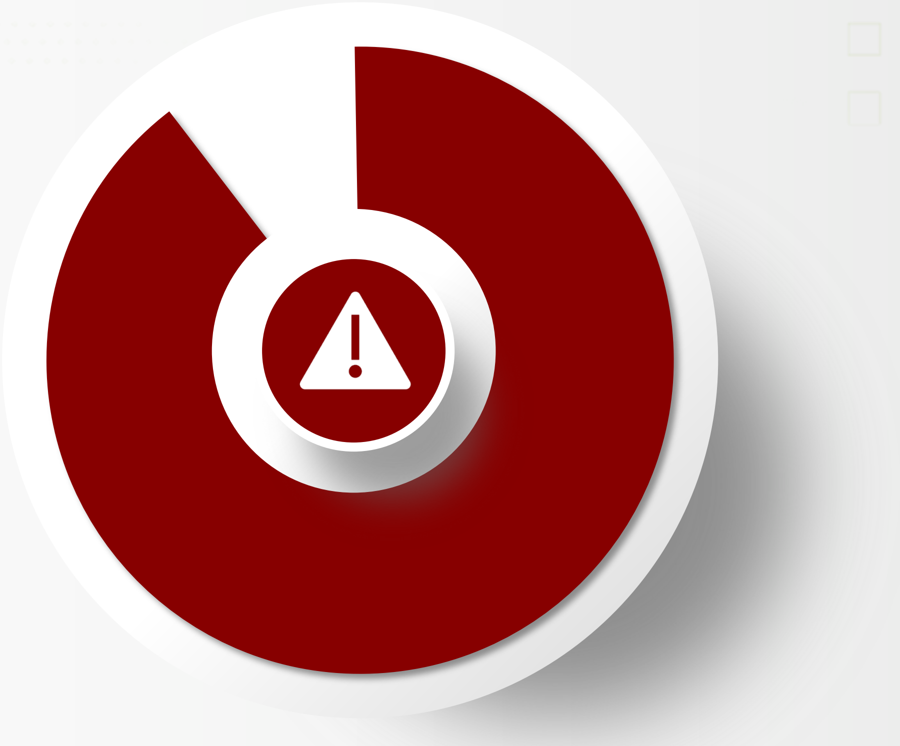
Olivia Powell

08/04/2023

4 out of 5 believe a weakening economy will increase cyber threats



87% believe cyber staff reductions increase risk



Source: 2023 ISC2 research, How the Cybersecurity Workforce Will Weather a Recession
https://www.isc2.org/Research/How-the-Cybersecurity-Workforce-Will-Weather-a-Recession

What can we do???

Why hire entry- and junior-level staff?

1 in 3 C-suite execs agree: It’s cheaper! (🤣🤣🤣)

Entry- and junior-level staff focus on day-to-day tasks, freeing up senior staff

Source: 2023 ISC2 research, How the Cybersecurity Workforce Will Weather a Recession
https://www.isc2.org/Research/How-the-Cybersecurity-Workforce-Will-Weather-a-Recession

Top 5 Tasks for Entry-Level Staff

(Less than 1 Year of Experience)

35%	Alert and Event Monitoring
35%	Documenting Processes & Procedures
29%	Using Scripting Language
28%	Incident Response
26%	Reporting *(Developing/ Producing Reports)*

Top 5 Tasks for Junior-Level Staff

(1–3 Years of Experience)

48%	Information Assurance *(Authentication, Privacy)*
48%	Backup, Recovery, & Business Continuity
47%	Intrusion Detection
47%	Encryption
46%	Penetration Testing

Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

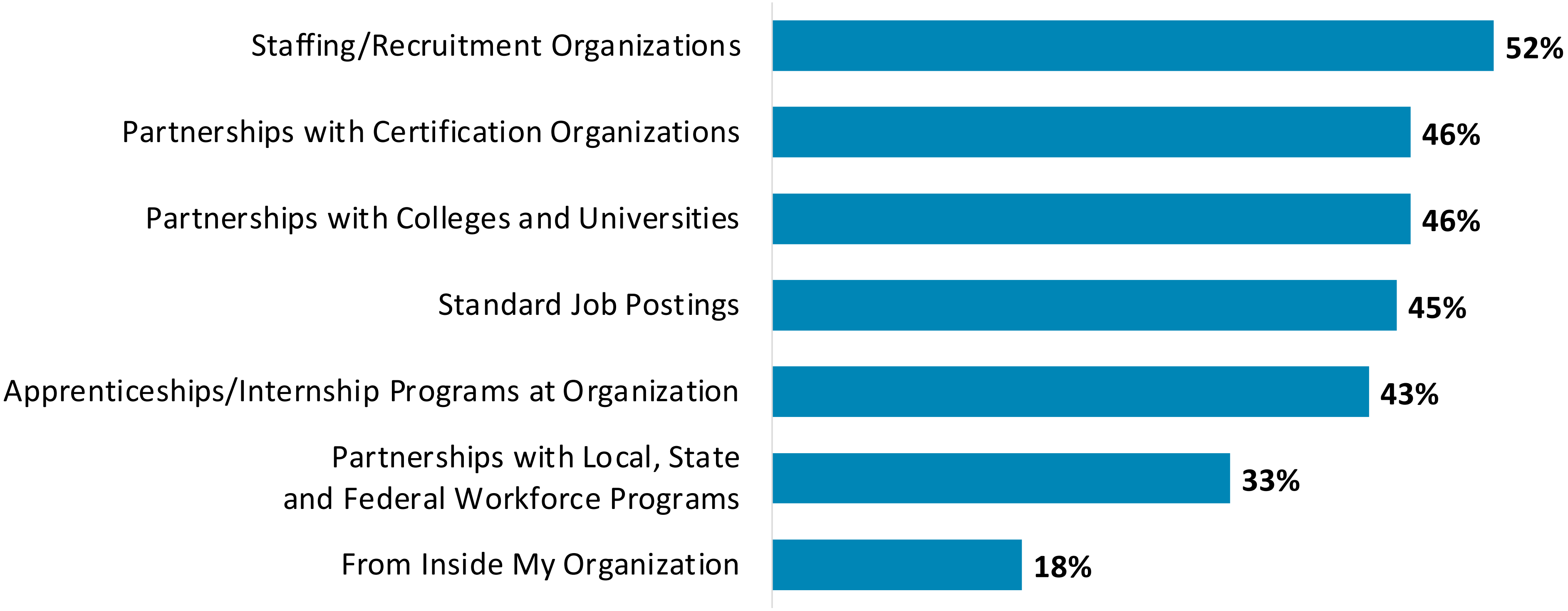
“They often bring an element of creativity and out-of-the-box thinking to the team.”

Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

"They often bring an element of creativity and out-of-the-box thinking to the team."

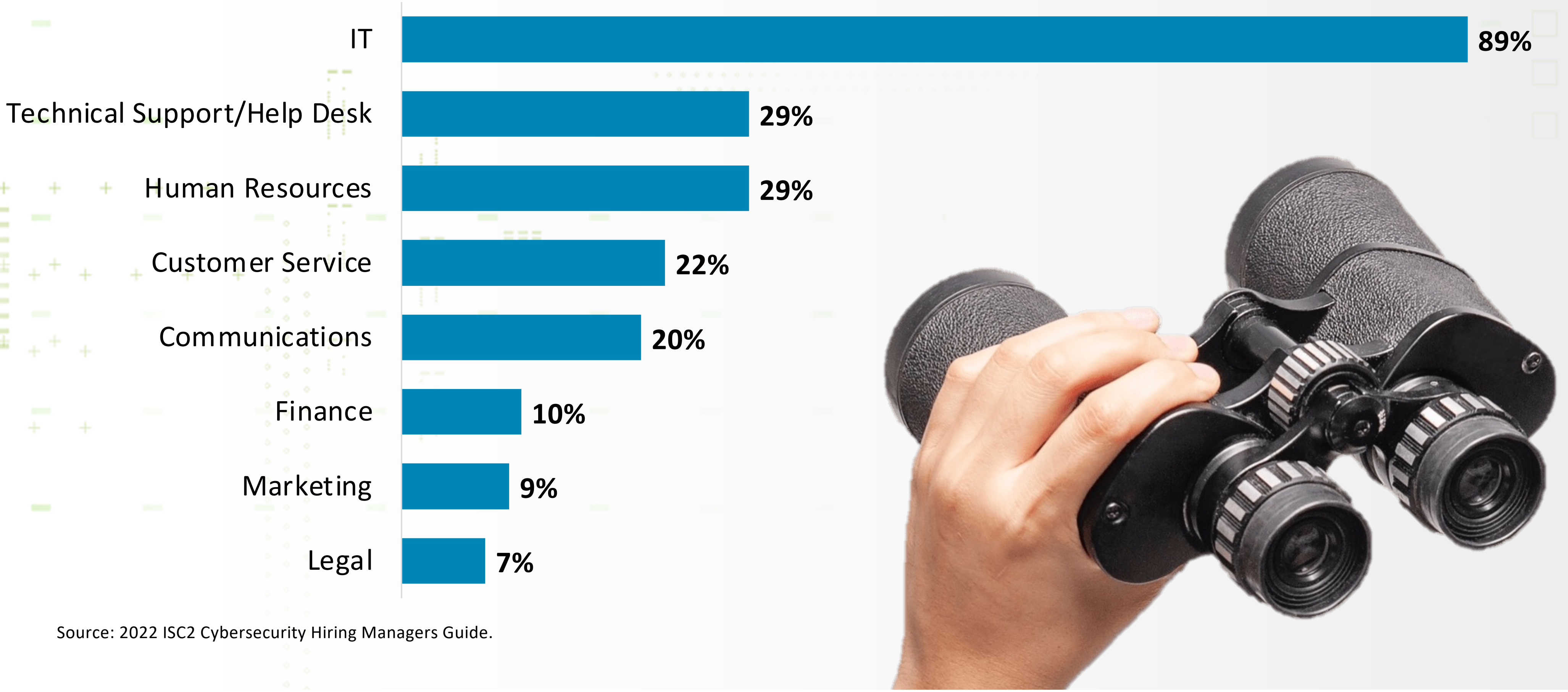
Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

Source of talent



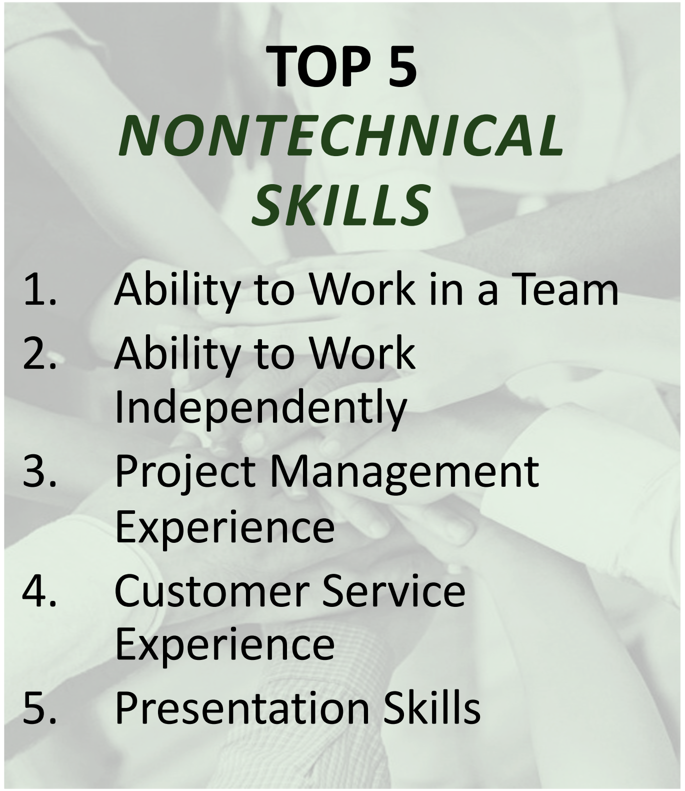
Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

Where to find talent inside your organization



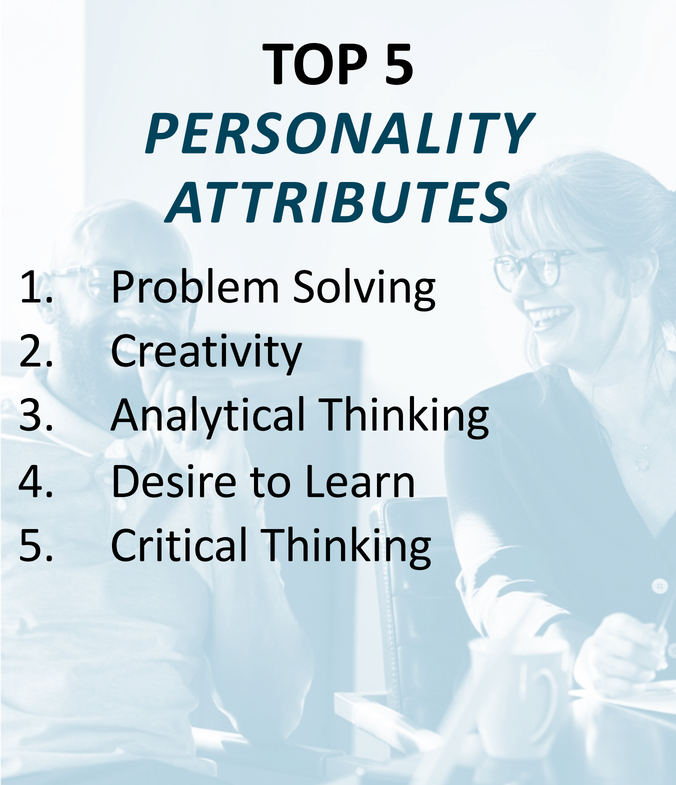
Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

Look for these traits when hiring entry- and junior-level team members



TOP 5 *NONTECHNICAL SKILLS*

1. Ability to Work in a Team
2. Ability to Work Independently
3. Project Management Experience
4. Customer Service Experience
5. Presentation Skills



TOP 5 *PERSONALITY ATTRIBUTES*

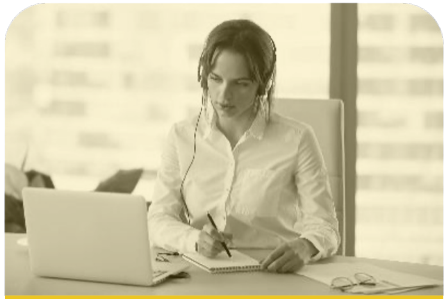
1. Problem Solving
2. Creativity
3. Analytical Thinking
4. Desire to Learn
5. Critical Thinking

Source: 2022 ISC2 Cybersecurity Hiring Managers Guide.

Who is the best person on your cybersecurity team? Why?

College degree not necessarily required

Ways to bring entry- and junior-level staff up to speed

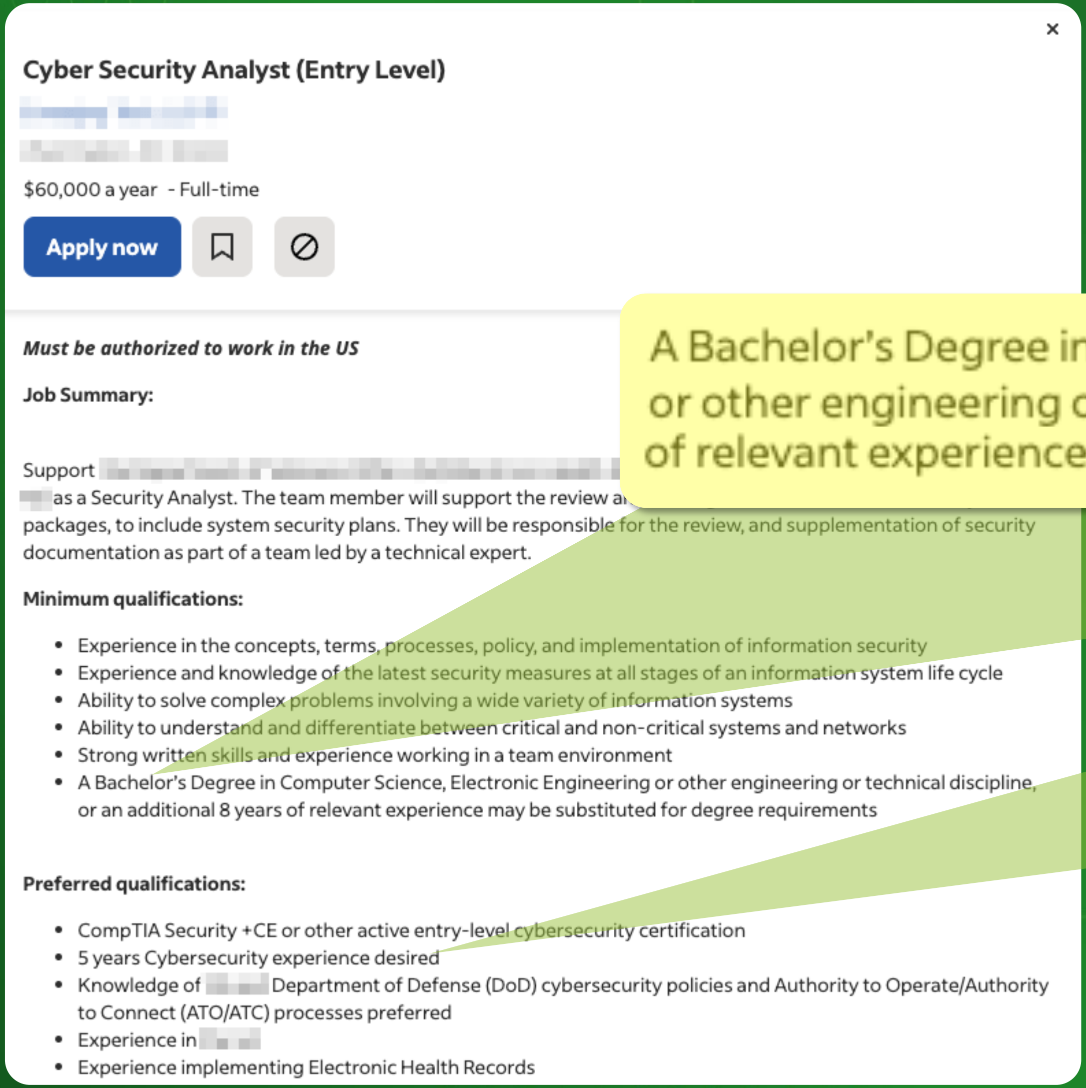


Formal on-the-job training

Exposure training

Apprenticeships

Mentorship



Cyber Security Analyst (Entry Level)

[redacted]

[redacted]

$60,000 a year - Full-time

Must be authorized to work in the US

Job Summary:

Support [redacted] [redacted] as a Security Analyst. The team member will support the review a packages, to include system security plans. They will be responsible for the review, and supplementation of security documentation as part of a team led by a technical expert.

Minimum qualifications:

- Experience in the concepts, terms, processes, policy, and implementation of information security
- Experience and knowledge of the latest security measures at all stages of an information system life cycle
- Ability to solve complex problems involving a wide variety of information systems
- Ability to understand and differentiate between critical and non-critical systems and networks
- Strong written skills and experience working in a team environment
- A Bachelor's Degree in Computer Science, Electronic Engineering or other engineering or technical discipline, or an additional 8 years of relevant experience may be substituted for degree requirements

Preferred qualifications:

- CompTIA Security +CE or other active entry-level cybersecurity certification
- 5 years Cybersecurity experience desired
- Knowledge of [redacted] Department of Defense (DoD) cybersecurity policies and Authority to Operate/Authority to Connect (ATO/ATC) processes preferred
- Experience in [redacted]
- Experience implementing Electronic Health Records

A Bachelor's Degree in Computer Science, Electronic Engineering or other engineering or technical discipline, or an additional 8 years of relevant experience may be substituted for degree requirements

5 years Cybersecurity experience desired

Seek out nontraditional fishing grounds

Main takeaways

The 3.4 million cybersecurity workforce gap puts organizations at risk

Look within your organization for cyber talent

Hire entry- and junior-level staff to take on day-to-day tasks and inject fresh thinking

Look for nontechnical skills and attributes; you can teach the rest later

Think outside the IT box when hiring staff

Set your team up for success with good salaries, fair treatment and training

Thank You!

Jon France, CISO, ISC2

jfrance@isc2.org

Any questions?

ISC2™