ECCS 3411: Computer Security

LECTURE 1

WELCOME

Preliminaries

- Prerequisites
  - ECCS 2671: DSA 1
- Course Policy
  - Attendance
  - Participation
  - Academic Integrity
- Textbook
  - William Stallings and Lawrie Brown, “Computer Security: Principles and Practice,” 4th ed. Pearson 2018

- Course Webpage (Canvas)
  - Lectures Slides
  - Reading Quizzes and Assignments
  - Labs
  - Projects
- Exams
  - Mid-term: TBD
  - Final: Exam week (May 12)

Grading, Contact and more in the Syllabus
(On Canvas)

ISACA®

State of Cybersecurity 2020

Persistent Hiring Challenges and Retention Issues Demand New Talent Pipelines

New global research from ISACA shows little progress—and, in some cases, worse results—when it comes to cybersecurity hiring and retention.

62% say their organization's cybersecurity team is **understaffed**

57% say they currently have **unfilled** cybersecurity positions on their team

Cybersecurity Hiring Challenges Show No Improvement

State of Cybersecurity 2021

Despite Disruptive Pandemic Year, Cybersecurity Workforce Challenges and Opportunities Remain Consistent

ISACA®

Amidst the COVID-19 pandemic that devastated many industries and career fields, cybersecurity remained relatively unscathed, according to new research from global IT and cybersecurity association ISACA.

But that's not to say everything is rosy. More than 3,600 cybersecurity leaders report consistent challenges finding qualified, well-rounded candidates—and understaffed teams remain strongly correlated to an increasing number of cyberattacks. Despite years of effort by government, industry and academia, and major financial investment to develop a stronger pipeline of cybersecurity candidates, little has changed.

Although cybersecurity jobs are in high demand, few organizations offer entry-level opportunities, limiting entry points into the field. How can we, once and for all, begin making a significant impact to the ongoing skills gap? Visit www.isaca.org/state-of-cybersecurity-2021 for analysis and expert insights.

Hiring Managers Struggle to Find Qualified Candidates

50%

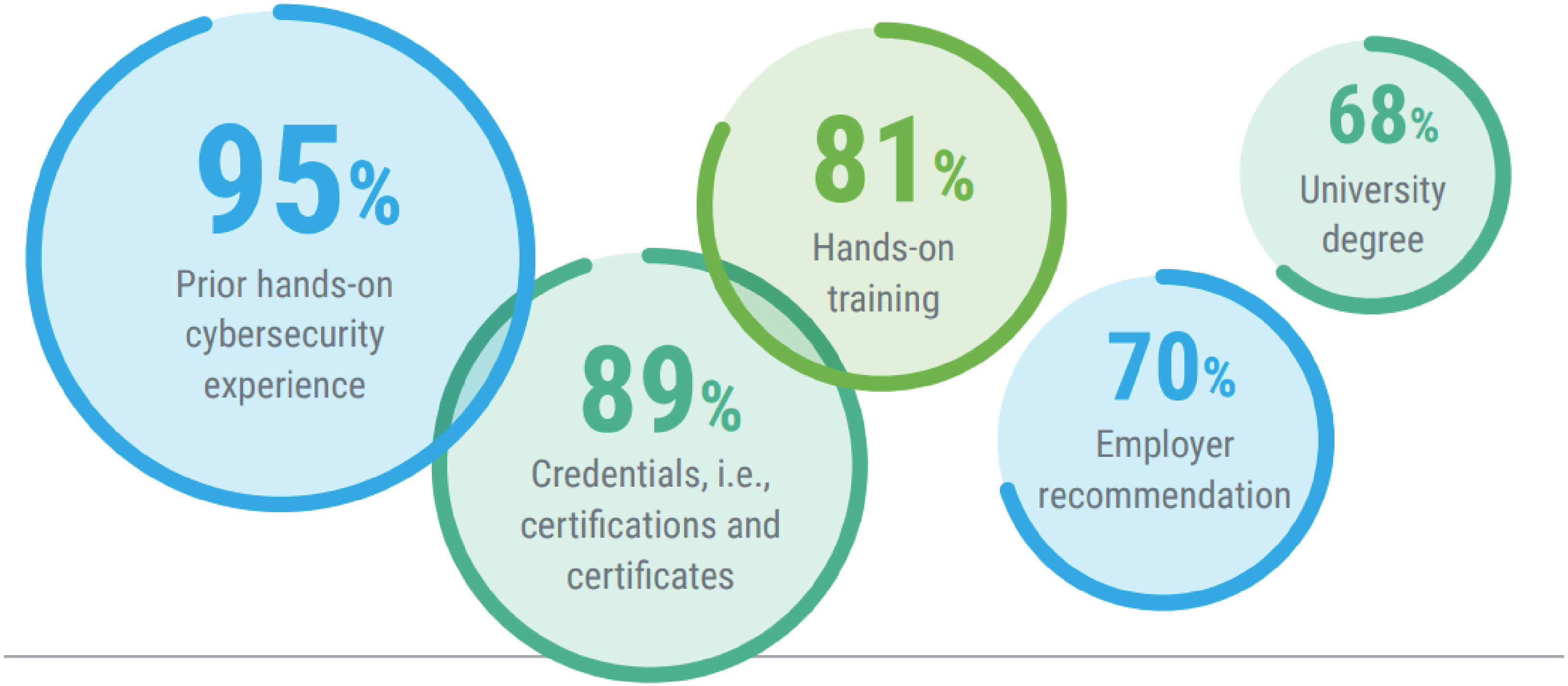
of those surveyed generally do not believe their applicants are well qualified.

72%

of those who reported that less than 25 percent of their applicants are well qualified have unfilled positions longer than three months.

TOP 5 WAYS

Hiring Managers Determine Whether a Candidate is Qualified



95% Prior hands-on cybersecurity experience

89% Credentials, i.e., certifications and certificates

81% Hands-on training

70% Employer recommendation

68% University degree

58% require a degree for entry-level cybersecurity positions.

ONLY 27% say recent university graduates are well prepared for the cybersecurity challenges their organization is facing.

ONLY 31% say HR regularly understands their cybersecurity hiring needs.

Technical Skills Top List of Demand

Technical cybersecurity positions remain the top vacancy.

79% say demand for individual contributors with cybersecurity technical skill will increase in

47%

WANTED:

Well-rounded Car

While technical skills remain in significant demand, e
candidates with solid soft skills—but find

BIGGEST SKILLS GAPS:

1. **56%** Soft skills
2. **36%** Security controls
3. **33%** Software development
4. **31%** Data-related topics
4. **31%** Coding skills

HOW ORGANIZATIONS ARE ADDRESSING THEM:

1. **Training non-security staff who are interested in moving to security roles** (43%)
2. **Increasing usage of contract employees or outside consultants** (37%)
3. **Increasing use of reskilling programs** (23%)
4. **Increasing use of performance-based training to build hands-on skill** (22%)
4. **Increasing reliance on AI/automation** (22%)

ISACA®

State of Cybersecurity 2022: Cyber Workforce Challenges

ISACA surveyed information security professionals across the globe for the eighth year in a row. Among the findings: any positive effect the COVID-19 pandemic had on retention is long gone—enterprises are engaged in a powerful struggle to retain cybersecurity staff. And more organizations than ever say they have unfilled cybersecurity positions—perhaps one of the reasons a smaller percentage are requiring university degrees for entry-level positions this year.

See what more than 2,000 security leaders had to say about workforce challenges and opportunities.

Hiring Challenges

63%

HAVE UNFILLED cybersecurity positions (up 8 points from 2021)

62%

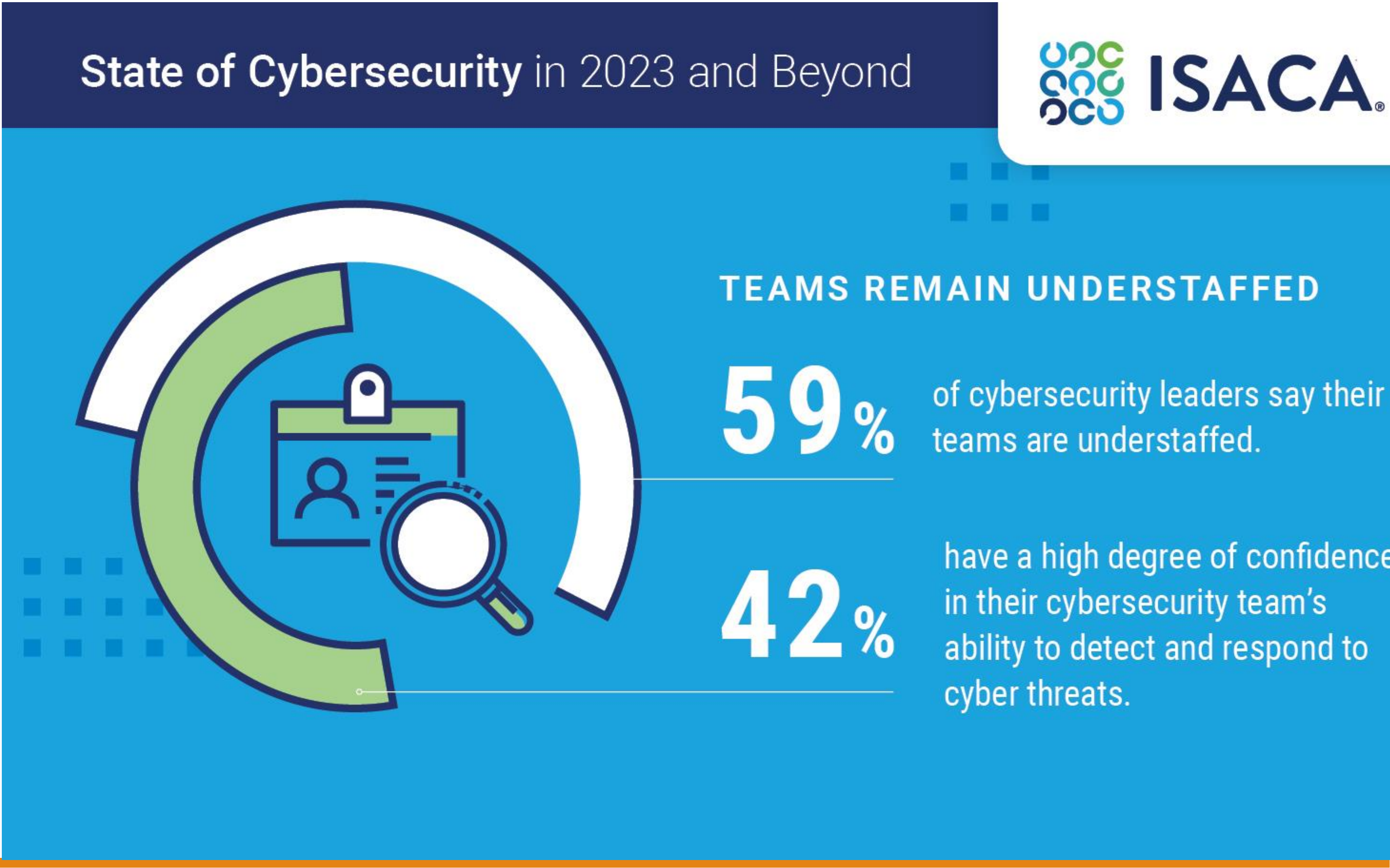
REPORT that their cybersecurity teams are understaffed

52%

REQUIRE university degrees for entry-level positions (down 6 points from 2021)

1 IN 5

say it takes **MORE THAN 6 MONTHS** to find qualified cybersecurity candidates for open positions



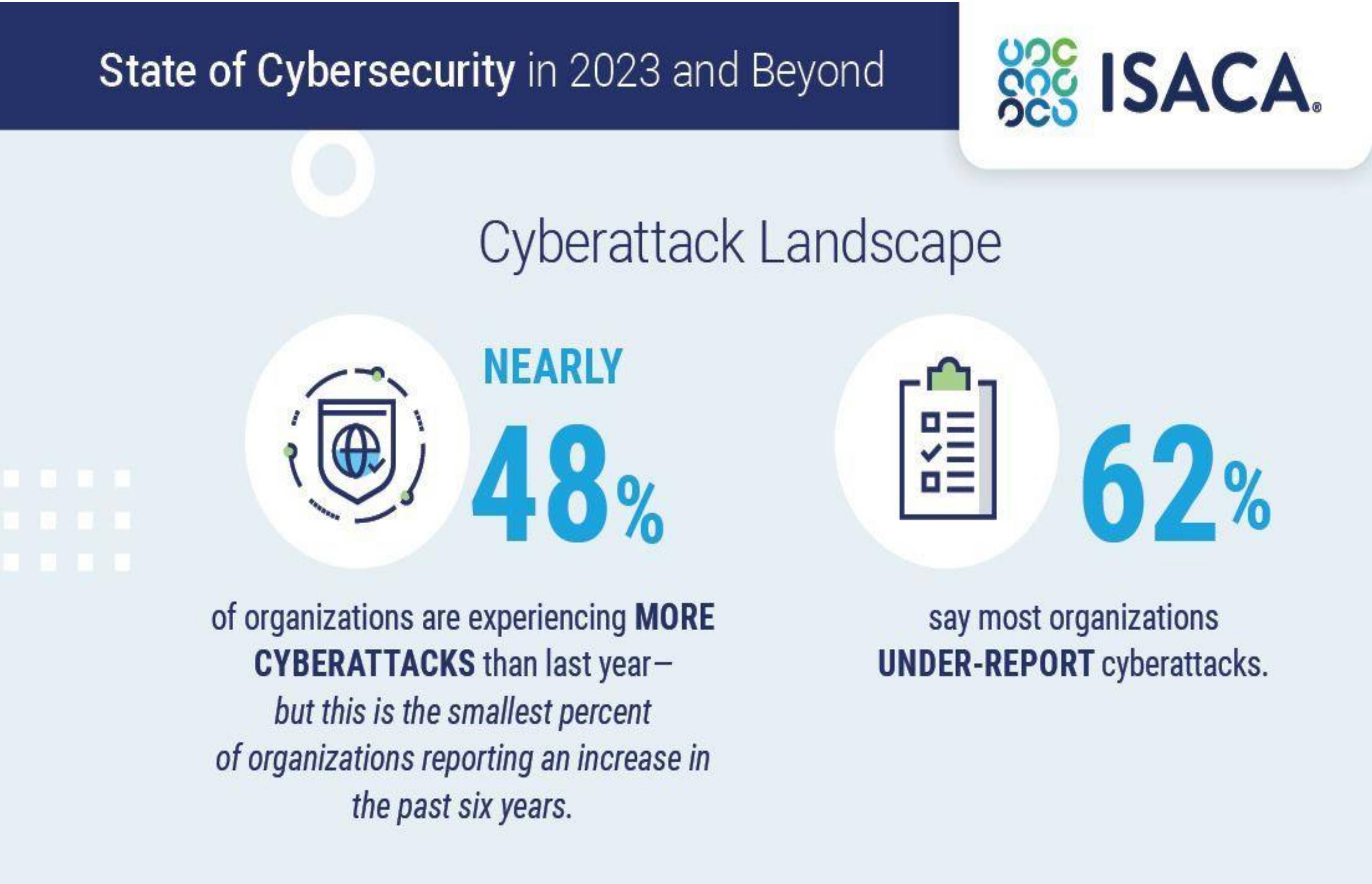
State of Cybersecurity in 2023 and Beyond

ISACA®

TEAMS REMAIN UNDERSTAFFED

59% of cybersecurity leaders say their teams are understaffed.

42% have a high degree of confidence in their cybersecurity team's ability to detect and respond to cyber threats.



State of **Cybersecurity** in 2023 and Beyond

ISACA®

Cyberattack Landscape

NEARLY

48%

of organizations are experiencing **MORE CYBERATTACKS** than last year–
but this is the smallest percent of organizations reporting an increase in the past six years.

62%

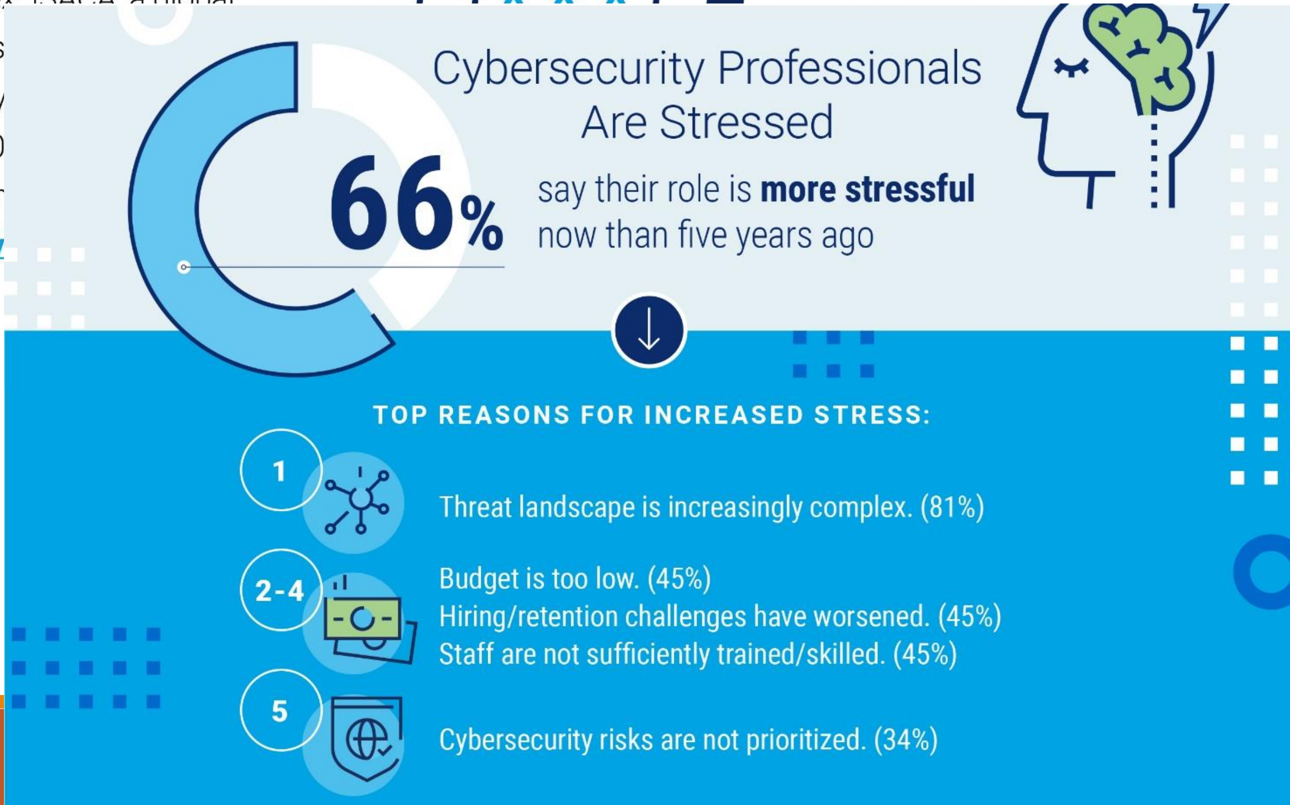
say most organizations **UNDER-REPORT** cyberattacks.

ISACA

GLOBAL EDITION

State of Cybersecurity
2024 and Beyond

The majority of cybersecurity professionals say their roles are
increasingly stressful—in large part due to a threat landscape
that continues to become more complex. ISACA, a global
professional association advancing trus
surveyed more than 1,800 cybersecurity
examine the state of cybersecurity in 20
skills gaps and hiring plans to threats ar
results, visit **www.isaca.org/state-of-cy**



Cybersecurity Professionals Are Stressed

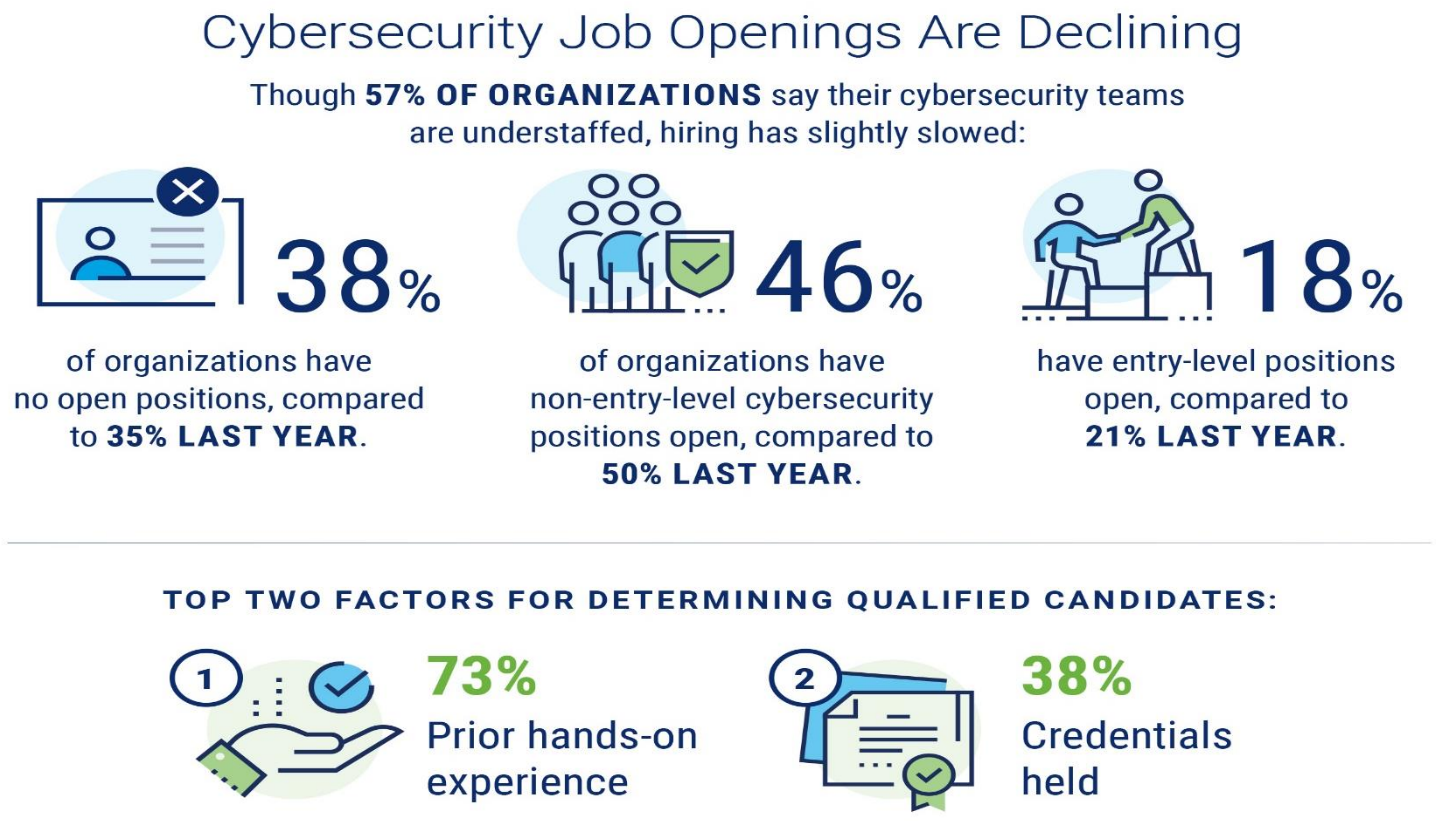
66% say their role is **more stressful** now than five years ago

TOP REASONS FOR INCREASED STRESS:

1 Threat landscape is increasingly complex. (81%)

2-4 Budget is too low. (45%)
Hiring/retention challenges have worsened. (45%)
Staff are not sufficiently trained/skilled. (45%)

5 Cybersecurity risks are not prioritized. (34%)



Cybersecurity Job Openings Are Declining

Though **57% OF ORGANIZATIONS** say their cybersecurity teams are understaffed, hiring has slightly slowed:

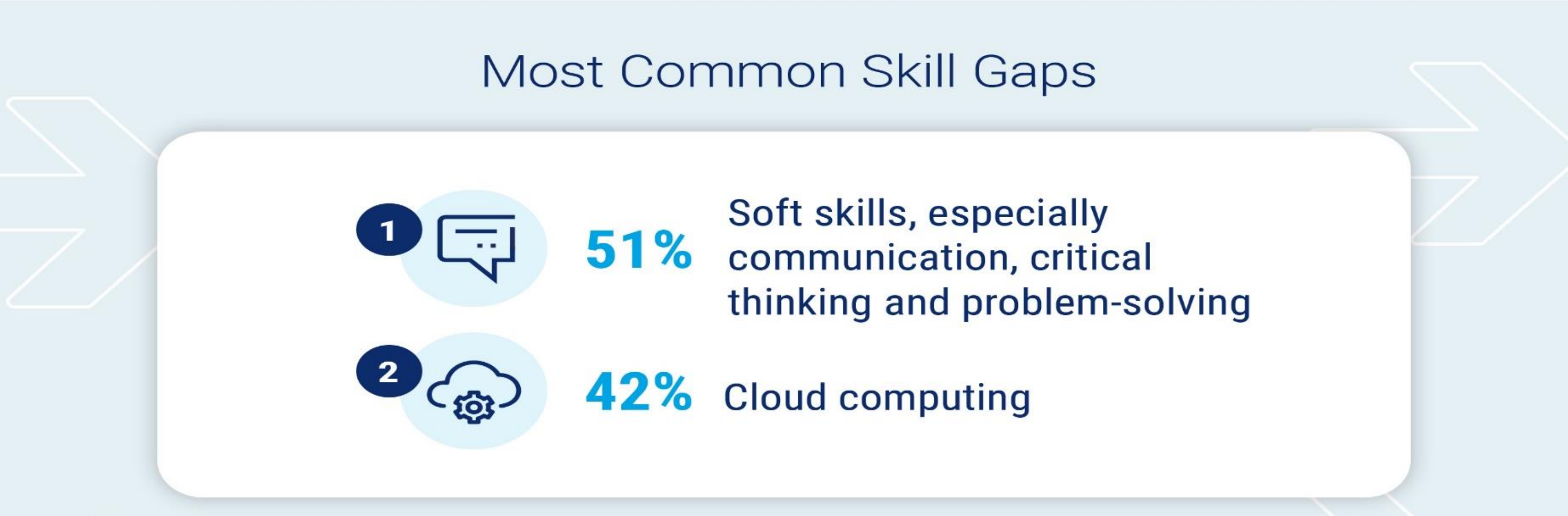
38% of organizations have no open positions, compared to **35% LAST YEAR**.

46% of organizations have non-entry-level cybersecurity positions open, compared to **50% LAST YEAR**.

18% have entry-level positions open, compared to **21% LAST YEAR**.

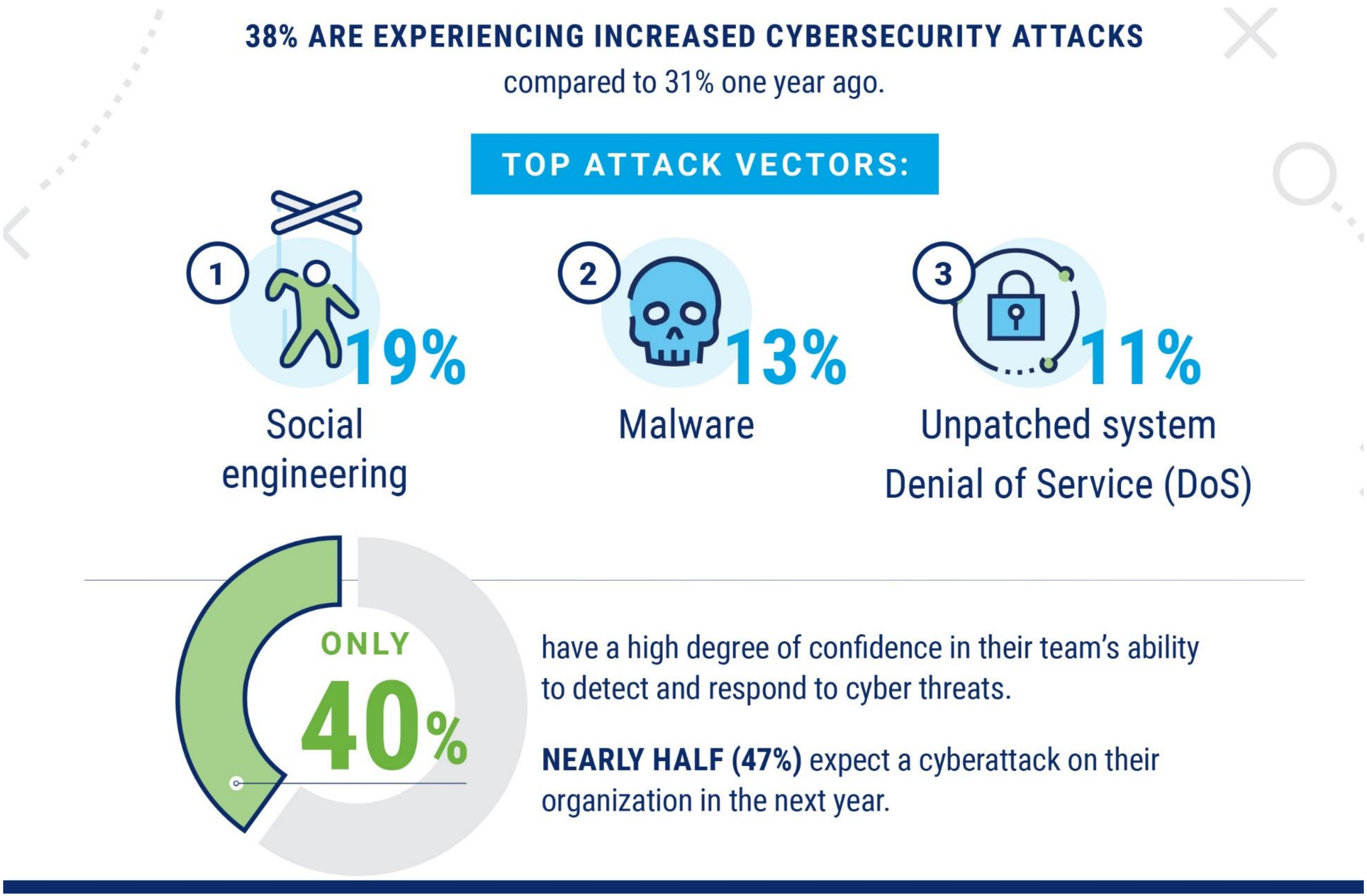
TOP TWO FACTORS FOR DETERMINING QUALIFIED CANDIDATES:

1. **73%** Prior hands-on experience
2. **38%** Credentials held



Most Common Skill Gaps

1. **51%** Soft skills, especially communication, critical thinking and problem-solving
2. **42%** Cloud computing



38% ARE EXPERIENCING INCREASED CYBERSECURITY ATTACKS

compared to 31% one year ago.

TOP ATTACK VECTORS:

1 19% Social engineering

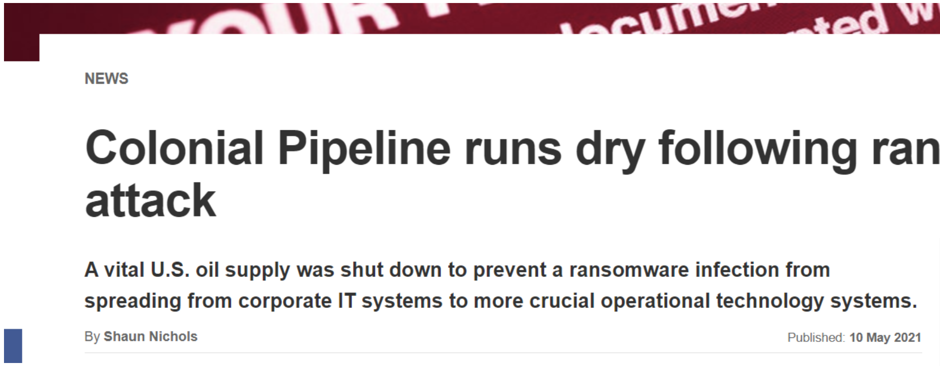
2 13% Malware

3 11% Unpatched system Denial of Service (DoS)

ONLY 40% have a high degree of confidence in their team's ability to detect and respond to cyber threats.

NEARLY HALF (47%) expect a cyberattack on their organization in the next year.

Real-World Attacks



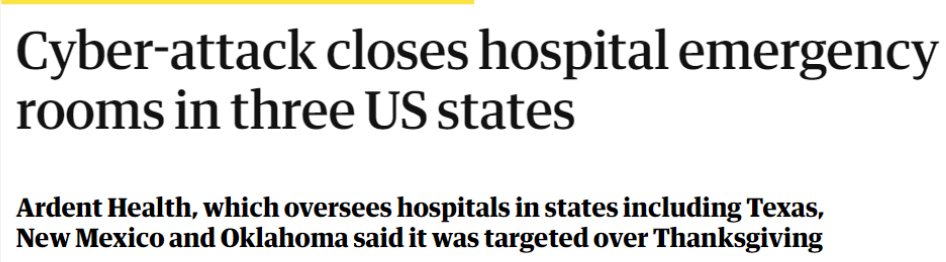
NEWS

Colonial Pipeline runs dry following ransomware attack

A vital U.S. oil supply was shut down to prevent a ransomware infection from spreading from corporate IT systems to more crucial operational technology systems.

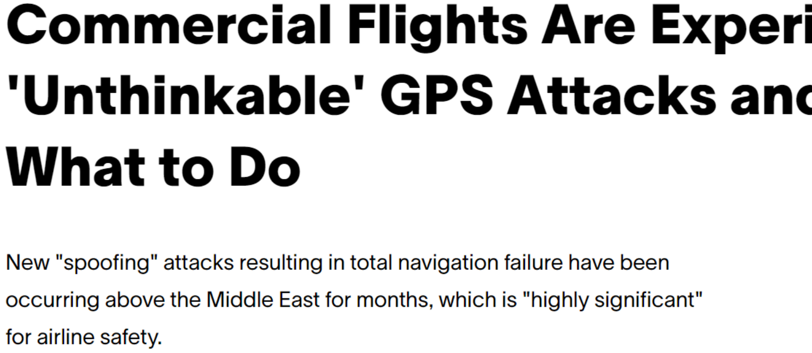
By Shaun Nichols

Published: 10 May 2021



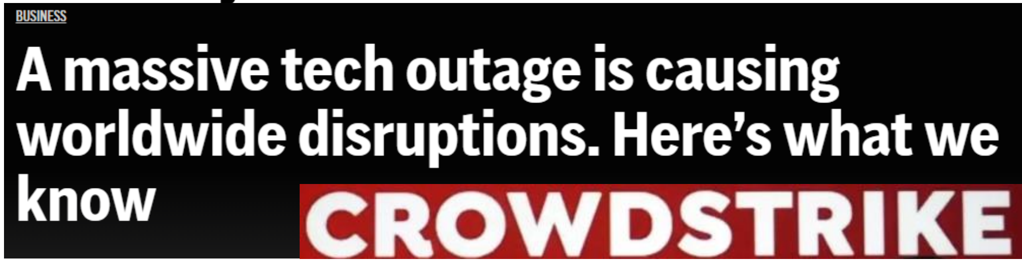
Cyber-attack closes hospital emergency rooms in three US states

Ardent Health, which oversees hospitals in states including Texas, New Mexico and Oklahoma said it was targeted over Thanksgiving



Commercial Flights Are Experiencing 'Unthinkable' GPS Attacks and Nobody Knows What to Do

New "spoofing" attacks resulting in total navigation failure have been occurring above the Middle East for months, which is "highly significant" for airline safety.

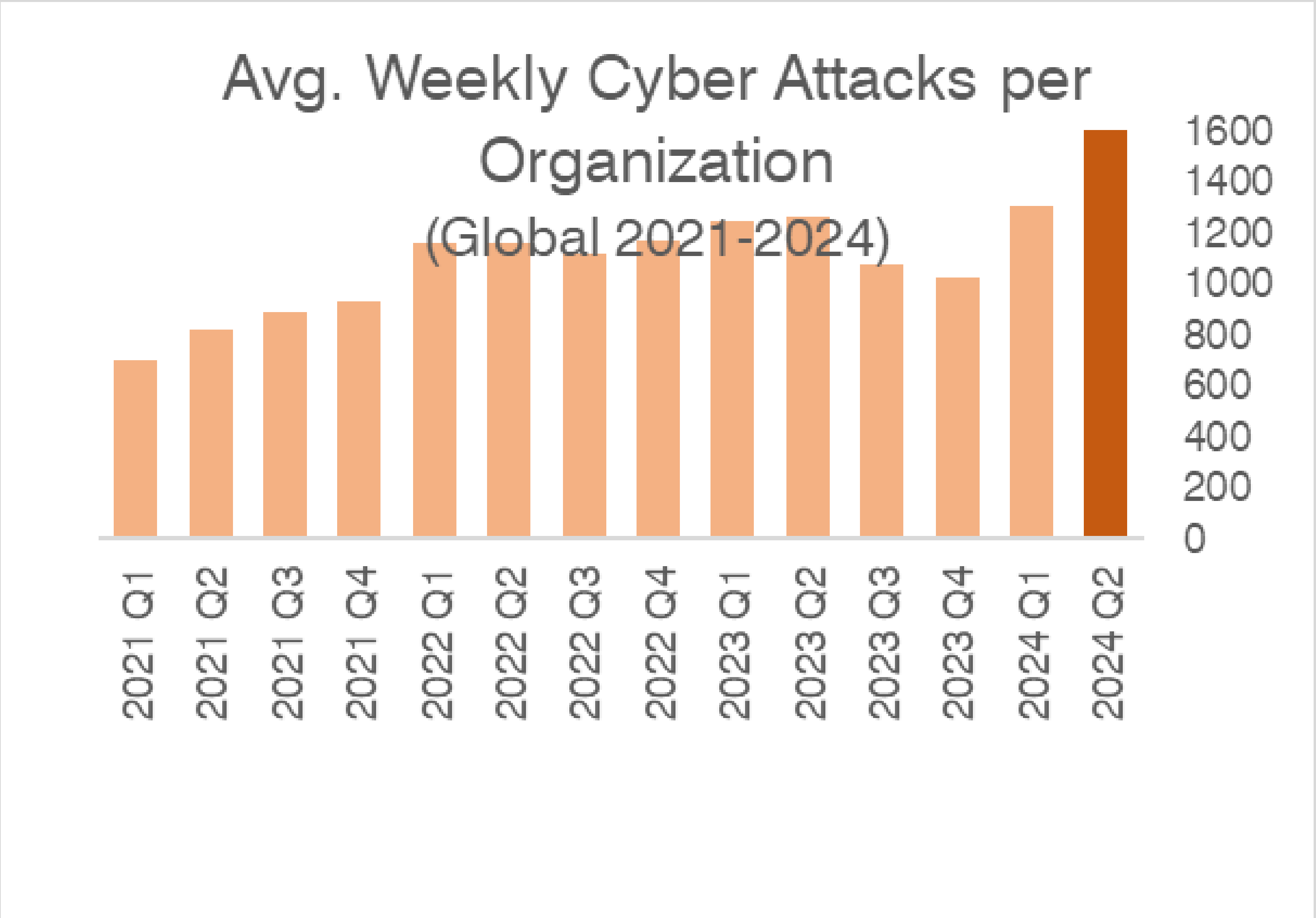


BUSINESS

A massive tech outage is causing worldwide disruptions. Here's what we know

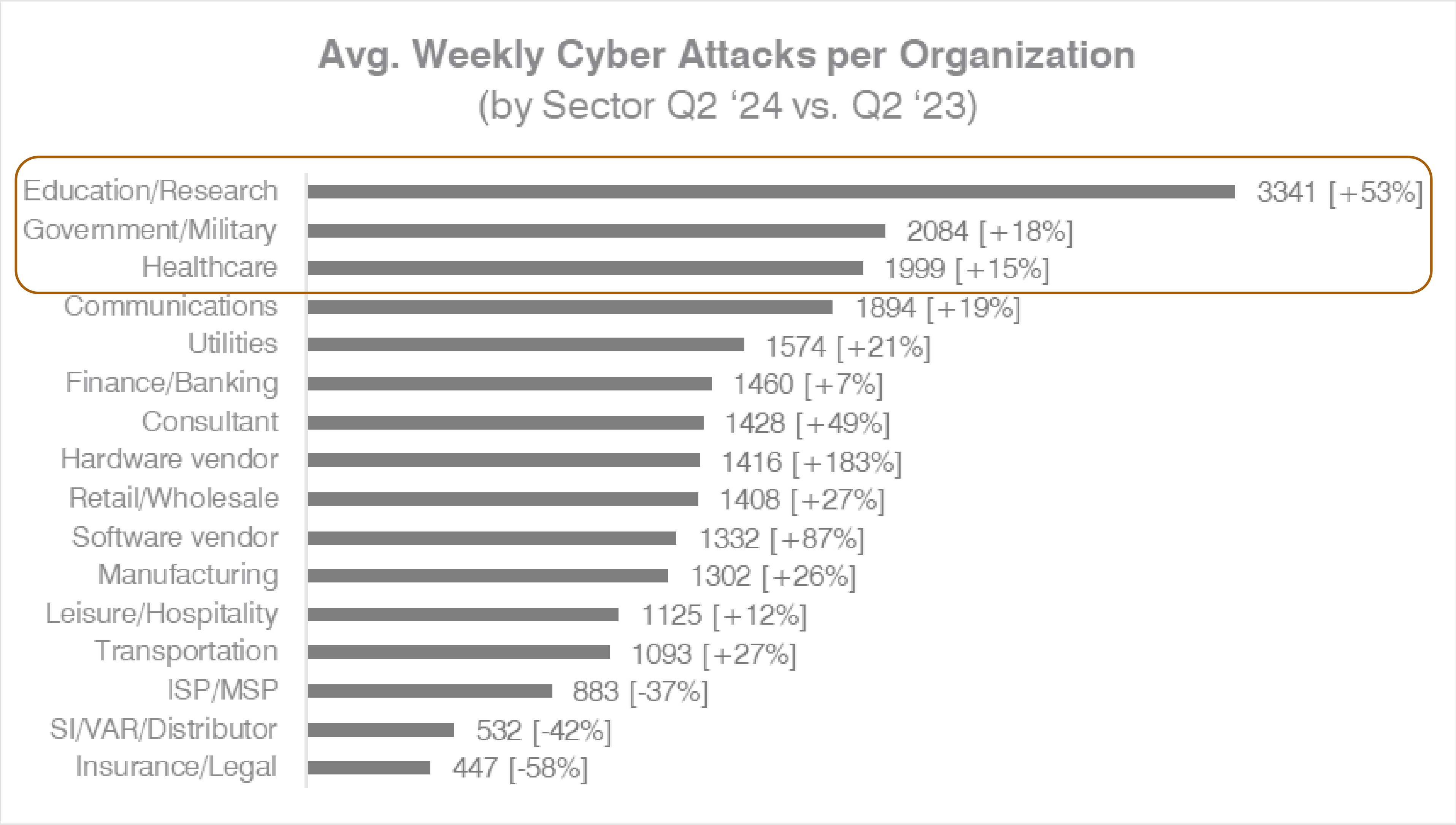
[1] https://www.techtarget.com/searchsecurity/news/252500544/Colonial-Pipeline-runs-dry-following-ransomware-attack
[2] https://www.theguardian.com/us-news/2023/nov/28/cyber-attack-us-hospitals-texas-oklahoma-new-mexico
[3] https://www.vice.com/en/article/m7bk3v/commercial-flights-are-experiencing-unthinkable-gps-attacks-and-nobody-knows-what-to-do
[4] https://apnews.com/article/what-is-crowdstrike-worldwide-outage-94b4fc5ac6eed46ddcd565a5f1e4b916

CHART: Cyberattacks rose globally in the past 2 years, 30% increase in Q2 2024, 1,636 attacks per org per week.

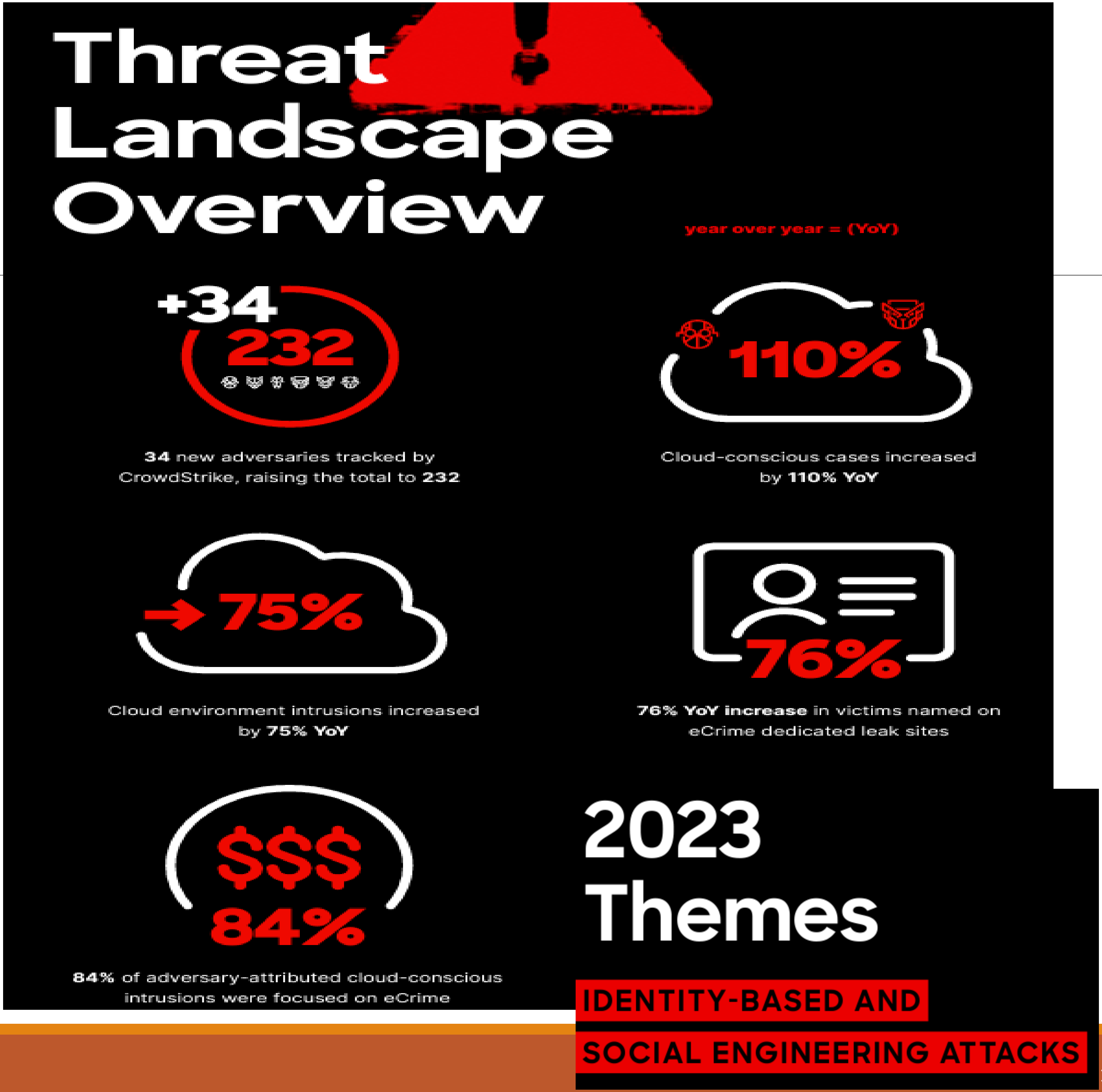


Source: https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

CHART: Top 3 most attacked Org.- Edu./Research, Gov./Military, Healthcare



Source: https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/



Threat Landscape Overview

year over year = (YoY)

+34
232

34 new adversaries tracked by CrowdStrike, raising the total to **232**

110%

Cloud-conscious cases increased by **110% YoY**

75%

Cloud environment intrusions increased by **75% YoY**

76%

76% YoY increase in victims named on eCrime dedicated leak sites

$$$
84%

84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

2023 Themes

IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

What will you learn

- Basics of computer security
- How to secure an existing system and/or build a secure system
- Security mechanisms such as Encryption
- Software, Network* and Web Security
- Get a feeling of real-world security problems
  - Hands-on assignments and Labs
- Business Perspective and Ethics
- “Researching” a topic
- Possibly … Continue to get a Cybersecurity Certification
  - CompTIA Security+, CEH, CISSP, CISM, GSEC, CISA, etc.

What will you NOT learn

- Become a pro Hacker
- Write/design/build invulnerable code/software/system
- Exploring the dark web