BrainWorks

2023

CYBERSECURITY COMPENSATION GUIDE

BrainWorks

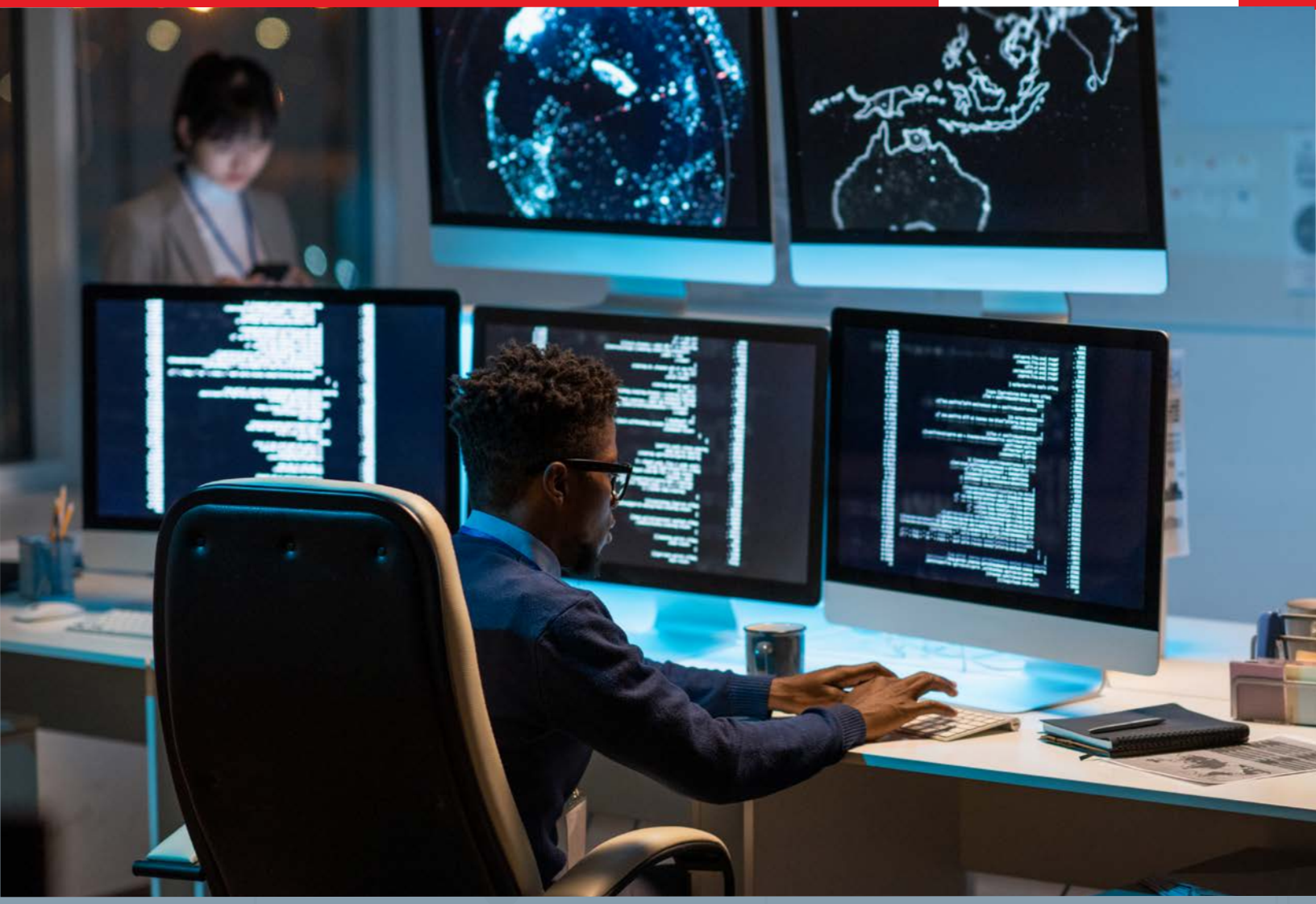
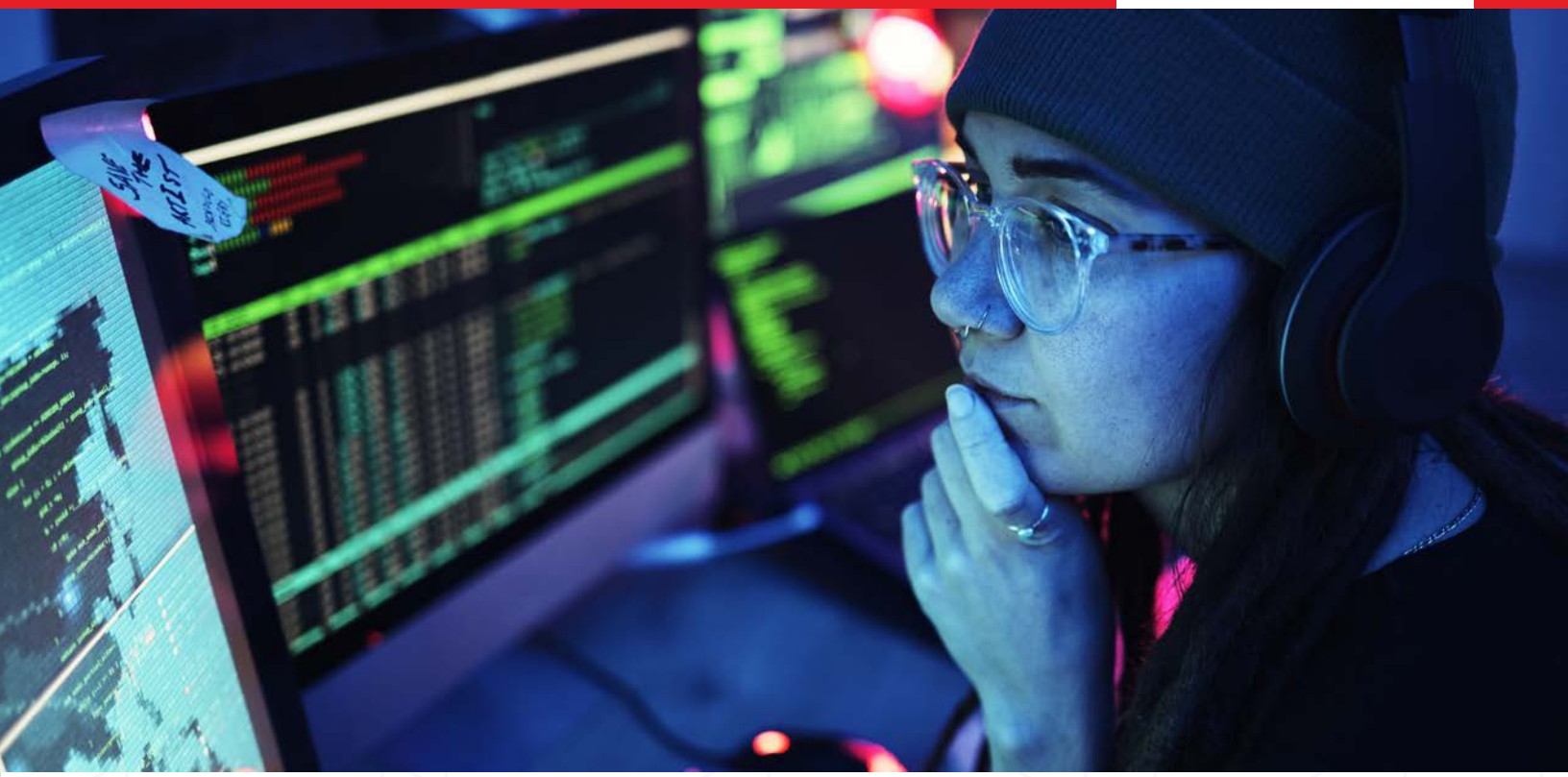


TABLE OF CONTENTS



INTRODUCTION

With all industries undergoing some level of digital transformation, businesses large and small are relying on technology to manage their day-to-day activities and processes, making cybersecurity a priority to safeguard data from various online attacks and unauthorized access.

36%
GROWTH

1 of the 20 fastest-growing occupations in the U.S.

770K
VACANCIES

Roles in cybersecurity

1.1M
PEOPLE

Employed in the cybersecurity industry in the U.S.

$265B
EXPECTED

Global ransomware damage costs by 2031

$4.24M
AVERAGE

Cost of a single data breach

3.5M
PEOPLE

Global cybersecurity workforce vacancies in 2021

Those in the cybersecurity profession are increasingly being called to new challenges to identify and proactively prevent threats and are facing increased pressure borne out of a stricter regulatory climate to protect organizations and increase resiliency. The role of a cybersecurity professional is increasingly that of a business risk manager who takes a proactive approach to information and data security, asking how attacks happen and what can be done to avoid them.

While AI and machine learning are increasingly used to identify and respond to cyber threats, and cloud-based security solutions are becoming more popular as organizations look for ways to secure their data in an increasingly complex digital landscape, cybersecurity talent remains scarce, especially in the domains of governance, risk and compliance (GRC).

According to ISC2, **57% of organizations have unfilled roles** for which they cannot find a suitable pool of candidates. Despite the evolution of traditional cybersecurity roles to more cloud-based technology and automation, shifting the existing workforce while others leave the profession entirely, the demand for cybersecurity professionals continues to grow and is one of the most sought-after sectors in the tech industry with **0% unemployment** for job seekers.

With such scarcity of talent, identifying candidates with core skillsets and transferable experience is imperative to filling vacancies and protecting organizations. If organizations can't obtain the skillsets needed to effectively manage cyber risk, then cyber risk will go unmitigated, which will lead to exposures, high cost of insurance (or loss of insurance), and leave the business open to attacks, ransoms, and data breaches.

An economic downturn or potential recession is no time to cut cybersecurity talent. While no industry is truly recession-proof, the cybersecurity industry is largely insulated from market downturns. This seemingly unusual job security is due to the fact that data and digital services are critical to business operations, but also because economic downturns can spur the bad actors when companies are most vulnerable.

Many businesses today understand the importance of cybersecurity, and as cybercrimes continue to increase, they are investing heavily to improve and secure their digital infrastructures and data. The global cyber landscape will only get more hostile and unstable, as cybercrimes continue to increase year over year, prompting businesses to struggle to keep up with the continuously shifting security requirements. In 2023, the cybersecurity market is expected to reach a value of over $200 billion, with cybersecurity jobs now accounting for over 15% of all information technology jobs.

CYBERSECURITY TREND WATCH

The past year was a rough one in the world of cybersecurity, with 66% of organizations globally reporting they were victimized by ransomware in 2022. In addition to several high-profile attacks, the year also saw an increase in cyber threats targeting municipalities, individuals, healthcare, and small businesses. These attacks affected all aspects of daily life, from the price of gas, to what's in stock at the grocery store and which mobile apps compromised personal financial data. The events of 2022 highlighted the need for cyber vigilance in identifying potential threats and protecting networks across all industries as well as the need for cybersecurity to become a national priority, and for countries to quickly invest in cyber defense and recovery capabilities at the national level.

Sectors such as healthcare have come under heavy attack, targeted for the valuable data these organizations store, but also because they cannot endure a shutdown in the aftermath of a breach and must continue operations. These attacks have prompted a renewed focus on disaster recovery and prevention, a theme that will carry into 2023. Highlighting the imperative need for cyber vigilance, research firm Cybersecurity Ventures predicts that in 2023 there will be a new ransomware attack every 2 seconds.

Cybersecurity has experienced several key shifts in the market, driven by digital transformation, advances in technology, threat landscape, and the regulatory environment. Prompted by the drastic increase in cybercrimes – there has been a nearly 40% increase globally in 2022 as compared to 2021 states Check Point Research. As technology advances, cyberattacks are becoming more sophisticated.

With more organizations moving their operations to the cloud, there is a growing need for effective cloud security solutions. Add to that a greater emphasis on data privacy, with data protection regulations like GDPR and CCPA increasing demand for solutions to help organizations comply with regulations and protect sensitive data. Until recently, Microsoft's Azure has held the unique position of being the cloud solution that is a security platform first. AWS and Google couldn't really say that until the news of the $5.4 billion acquisition of Mandiant by Google.

The adoption of zero-trust security models also saw a surge in popularity in 2022, a trend that will continue into 2023 and beyond. This security model assumes that all devices and users are potential threats until proven otherwise, and will likely become the status quo, emphasizing the need for strong authentication and access controls. Based on always verifying user identity and access rights, rather than trusting users who are already in the system, this model is helping organizations keep their data and systems secure even when they were accessed from outside their networks. In fact, Gartner believes that Zero Trust Network Access (ZTNA) is the fastest-growing form of network security, which will grow by 31% in 2023 and completely replace VPNs by 2025.

With AI being more prevalent in all market segments, this technology with a combination of machine learning has brought tremendous changes in cybersecurity. The industry is seeing a growing use of AI and machine learning to detect and respond to cyber threats, and with the ability to analyze large volumes of data in real-time and identify patterns that indicate potential risk, AI offers an advantageous tool for cybersecurity professionals to proactively protect networks. While AI is also being used to develop smart malware and attacks to bypass the latest security protocols in controlling data, AI-enabled threat detection systems can predict new attacks and notify admins of any data breach instantly. According to IBM, companies that use AI and automation to detect and respond to data breaches save an average of $3 million compared to those that don't.

In fact, AI was the most discussed theme during the 2023 RSA Conference, with disruptive technologies like ChatGPT central to many organizations' new risk management and security strategies.

Even the U.S. Department of Justice is aware of the potential threats posed by bad actors acquiring, using and abusing AI, forming the Disruptive Technology Strike Force with the U.S. Commerce Department in February to better strengthen supply chains and protect critical technological assets. AI is integral to identity security, access management and zero-trust architecture, and is finding acceptance within the enterprise as a powerful tool to help overworked security professionals better prioritize potential threats and risks.

2022 saw an increase in malware that targets industrial control systems (ICS) and ransomware attacks remain the top financial and operational risk to industrial and manufacturing organizations. Dragos identified 605 ransomware attacks against industrial organizations in 2022, an increase of 87% over the previous year. Many of these organizations still lack the right mitigations needed to reduce risk and maintain operations, causing electric grids, oil and gas pipelines, water systems, and manufacturing plants to continue to struggle with more complex regulatory environments that demand marked progress in shoring up defenses.

As more operational systems are connected to IT networks there is a growing need for integrated security solutions, converging information, and operational technology. While cybersecurity capabilities and awareness are improving, the threat and sophistication of cyberattacks are matching progress, making for a treacherous emerging digital ecosystem. In the current digital environment, every company is now a reachable target. Every company has operations, brand, reputation, and revenue pipelines that are potentially at risk from a breach. The industry in 2023 and beyond will focus heavily on the need to mitigate threats and enhance resiliency and recovery.

With increases in threats and breaches, the cost of becoming cyber insured has also increased dramatically. However, the cyber insurance industry has evolved in a positive direction as it has tightened up underwriting standards that address implementing more appropriate controls, system checks, and monitoring capabilities than ever before. Insurers now routinely question whether organizations have implemented a comprehensive security solution that includes testing and training their employees on phishing and social engineering, recognizing security incidents, password behaviors, endpoint protection, and more.

Many companies still don't take the threat from inside their organizations seriously enough, an issue only compounded by hybrid and remote workers whose incidents are more related to negligence than malice. The impact is still very real, with one estimate claiming a cost of over $15 million to remediate insider incidents annually. A cybersecurity priority in 2023 will be to secure the millions of devices worldwide that are being used for home and remote working. In hybrid and remote work environments, where workers have more latitude to follow their own rules on security at home, policies will need to be rewritten to align with this new reality, underpinned with the right technologies and user education. Cybersecurity professionals will increasingly need to develop programs to educate their organizations and fellow employees, as well as implement powerful and friction-free security controls such as multifactor authentication (MFA), zero-trust policies, and secure access service edge (SASE) deployments.

With the advent and growth of 5G networks, a new era of inter-connectivity will become a reality with the Internet of Things (IoT). Analysts at Gartner predict that in 2023, there will be 43 billion IoT-connected devices in the world. Mobile devices and applications are the new target for cyberattacks, as the highest rate of mobile phishing in history was observed in 2022, with mobile banking being the primary target. Our handheld devices contain photos, financial transactions, emails, messages, and more data – often in the cloud and connected to other devices or networks – making them potential prospects for hackers and malware.

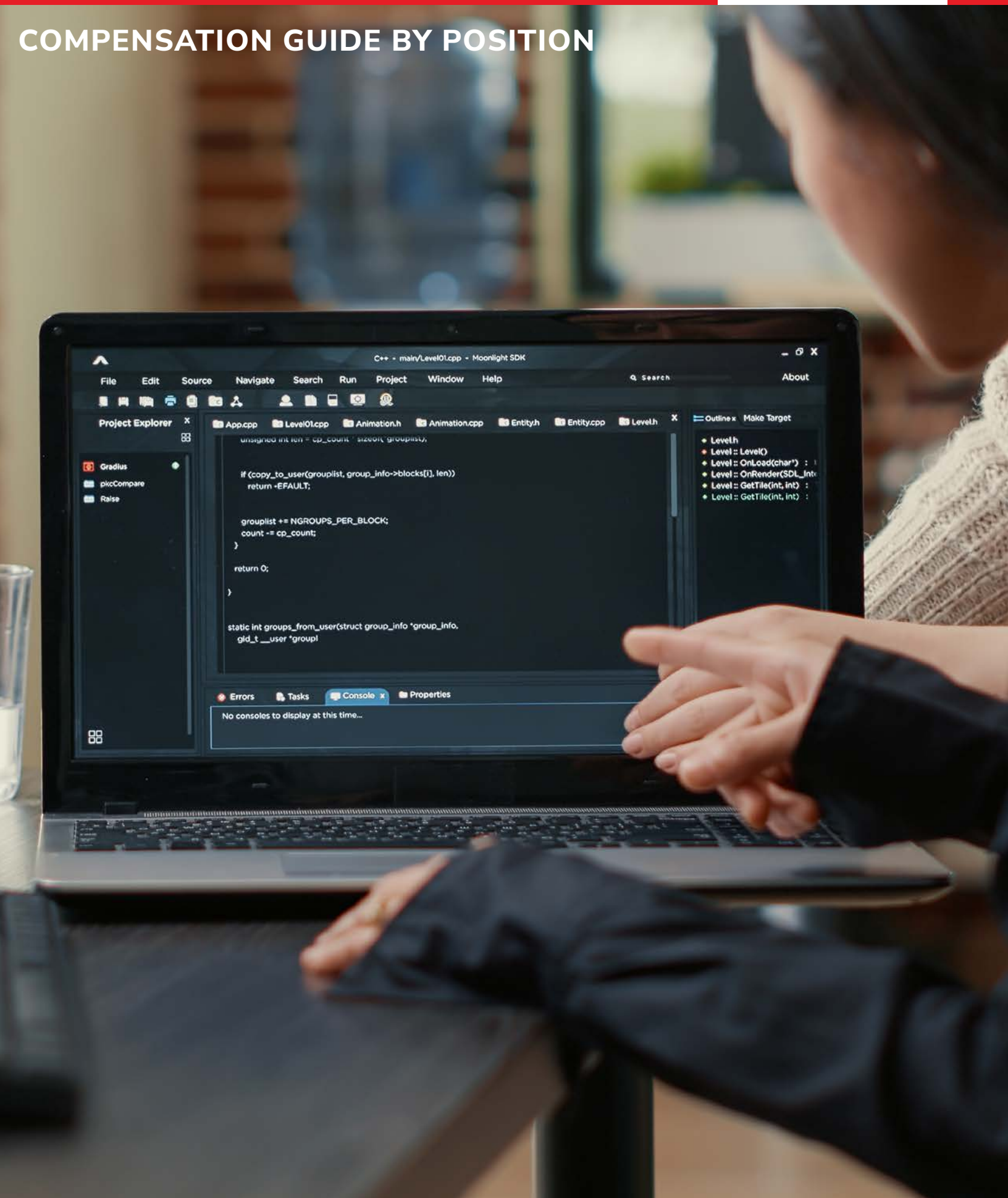
Additionally, the year ahead will see a rise in automotive hacking, as many modern vehicles are packed with automated software creating seamless connectivity for drivers in cruise control, engine timing, door lock, airbags and advanced systems for driver assistance. The Bluetooth and WiFi technologies these vehicles use to communicate also opens them to several vulnerabilities or threats from hackers. Self-driving or autonomous vehicles use an even more complex mechanism that requires strict cybersecurity measures.

UPCOMING REGULATIONS

- A number of national regulations and state privacy laws are slated to take effect in 2023, widely affecting the cybersecurity industry in terms of incident reporting, insurance, privacy and implementing regulations to minimize organizations' security risk. Some to keep an eye on include:
- The Cybersecurity Maturity Model Certification (CMMC) program is a new Department of Defense rule that will likely land in mid-2023, requiring any DoD contractor to certify that their cybersecurity controls are meeting federal requirements.
- The U .S. SEC issued the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure requirements expected to go into effect mid-2023, applies to public companies.
- Executive Order 13984 requires any infrastructure as a service (IaaS) company to verify the identities of their customers. Expected to go into effect in June 2023, the goal is to spot nefarious foreign actors that use U.S.-based IaaS solutions to commit crimes.
- Enforcement of the California Consumer Privacy Act (CPRA) will go into effect in July 2023. Similar to Europe's General Data Protection Regulation, it grants consumers some level of control over how their personal data is handled, including the right to know what a business has collected about them, how that data used, the ability to opt out of allowing a business to use their information, and the ability to request that it be deleted, among other rights.
- The American Data Privacy and Protection Act (ADPPA) is essentially the federal version of the CCPA. While we might not see movement in 2023, businesses need to plan for ADPPA rules coming through eventually.

BrainWorks

COMPENSATION GUIDE BY POSITION



*Base salary compensation ranges vary based on factors such as location, experience, and company size.

ENGINEERING POSITIONS

POSITION TITLE	LOWER	MEDIAN	UPPER
Application Security Engineer	$85,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
CIO (Chief Information Officer)	$150,000 - $200,000	$200,000 - $275,000	$275,000 - $400,000
CISO (Chief Information Security Officer)	$175,000 - $225,000	$225,000 - $300,000	$300,000 - $500,000
Cloud Security Engineer	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $200,000
Cryptographer	$100,000 - $130,000	$130,000 - $170,000	$170,000 - $220,000
Cybersecurity Architect	$100,000 - $130,000	$130,000 - $170,000	$170,000 - $220,000
Cybersecurity Consultant	$80,000 - $120,000	$120,000 - $150,000	$150,000 - $200,000
Cybersecurity Engineer	$70,000 - $110,000	$110,000 - $140,000	$140,000 - $200,000
Cybersecurity Program Manager	$110,000 - $140,000	$140,000 - $170,000	$170,000 - $220,000
Forensic Analyst	$75,000 - $110,000	$110,000 - $140,000	$140,000 - $180,000
Identity and Access Management (IAM) Engineer	$85,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
Incident Response Engineer	$80,000 - $120,000	$120,000 - $150,000	$150,000 - $200,000
Information Security Engineer	$75,000 - $115,000	$115,000 - $145,000	$145,000 - $200,000
Network Security Engineer	$75,000 - $110,000	$110,000 - $140,000	$140,000 - $200,000
Penetration Tester/Ethical Hacker	$80,000 - $120,000	$120,000 - $150,000	$150,000 - $200,000
Security Automation Engineer	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $200,000
Security Compliance Engineer	$80,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
Security Operations Center (SOC) Engineer	$80,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
Security Operations Engineer	$70,000 - $110,000	$110,000 - $140,000	$140,000 - $185,000
Security Researcher	$100,000 - $130,000	$130,000 - $170,000	$170,000 - $220,000
Security Software Engineer	$85,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
Security Solutions Engineer	$80,000 - $110,000	$110,000 - $140,000	$140,000 - $185,000
VP Cryptography (Vice President of Cryptography)	$200,000 - $250,000	$250,000 - $350,000	$350,000 - $500,000
VP of Cybersecurity (Vice President of Cybersecurity)	$200,000 - $250,000	$250,000 - $350,000	$350,000 - $500,000

PRODUCT POSITIONS

POSITION TITLE	LOWER	MEDIAN	UPPER
Associate Product Manager	$60,000 - $75,000	$75,000 - $90,000	$90,000 - $110,000+
CPO (Chief Product Officer)	$150,000 - $250,000	$250,000 - $400,000	$400,000 - $600,000
Director of Product Management	$140,000 - $175,000	$175,000 - $225,000	$225,000 - $300,000+
Head of Product	$120,000 - $175,000	$175,000 - $250,000	$250,000 - $400,000+
Innovation Product Manager	$80,000 - $100,000	$120,000 - $150,000	$180,000 - $250,000+
Product Analytics Manager	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
Product Design Manager	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
Product Development Manager	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
Product Growth Manager	$70,000 - $90,000	$100,000 - $130,000	$150,000 - $200,000+
Product Manager	$85,000 - $120,000	$120,000 - $150,000	$150,000 - $190,000
Product Marketing Manager	$80,000 - $100,000	$100,000 - $130,000	$130,000 - $160,000+
Product Operations Manager	$90,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
Product Owner	$80,000 - $110,000	$110,000 - $140,000	$140,000 - $175,000+
Product Solutions Manager	$80,000 - $100,000	$120,000 - $150,000	$180,000 - $250,000+
Product Strategist	$95,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
Security Operations Engineer	$70,000 - $110,000	$110,000 - $140,000	$140,000 - $185,000
Senior Product Manager	$100,000 - $130,000	$130,000 - $160,000	$160,000 - $200,000+
Technical Product Manager	$95,000 - $120,000	$120,000 - $150,000	$150,000 - $185,000+
VP of Product (Vice President of Product)	$150,000 - $200,000	$200,000 - $300,000	$300,000 - $500,000+

SALES & MARKETING POSITIONS

POSITION TITLE	LOWER	MEDIAN	UPPER
Account Executive	$45,000 - $55,000	$75,000 - $90,000	$140,000 - $160,000+
Business Development Manager	$50,000 - $70,000	$90,000 - $115,000	$150,000 - $180,000+
Chief Marketing Officer (CMO)	$130,000 - $150,000	$175,000 - $200,000	$250,000+
Head of Marketing	$100,000 -$120,000	$140,000 - $160,000	$250,000+
Head of Sales	$80,000 - $120,000	$140,000 - $170,000	$200,000 - $250,000+
Marketing Director	$90,000 - $115,000	$130,000 - $160,000	$200,000 - $230,000+
Marketing Manager	$65,000 - $80,000	$100,000 - $140,000	$170,000 - $190,000
Product Marketing Manager	$80,000 - $100,000	$100,000 - $130,000	$130,000 - $160,000+
Sales Engineer	$70,000 - $80,000	$95,000 - $115,000	$150,000 - $170,000+
VP of Sales	$120,000 - $140,000	$170,000 - $200,000	$250,000 - $300,000

FINANCE & OPERATIONS POSITIONS

POSITION TITLE	LOWER	MEDIAN	UPPER
Chief Financial Officer (CFO)	$120,000 - $140,000	$175,000 - $220,000	$250,000 - $300,000+
Director of Operations	$80,000 - $100,000	$120,000 - $150,000	$175,000 - $200,000+
Financial Analyst	$55,000 - $65,000	$75,000 - $85,000	$100,000 - $120,000+
Financial Controller	$75,000 - $90,000	$100,000 - $120,000	$150,000 - $180,000

RISK, COMPLIANCE & LEGAL POSITIONS

POSITION TITLE	LOWER	MEDIAN	UPPER
Chief Risk Officer (CRO)	$135,000 - $160,000	$200,000 - $270,000	$350,000 - $500,000+
Compliance Manager	$70,000 - $90,000	$100,000 - $130,000	$160,000 - $190,000
Legal Counsel	$100,000 - $130,000	$140,000 - $180,000	$200,000 - $300,000+
Risk and Compliance Manager	$80,000 - $120,000	$140,000 - $170,000	$200,000 - $230,000+
Risk Manager	$70,000 - $90,000	$110,000 - $150,000	$170,000 - $200,000
Senior Compliance Officer	$160,000 - $180,000	$240,000 - $280,000	$300,000 - $350,000
Senior Regulatory Counsel	$160,000 - $180,000	$240,000 - $280,000	$300,000 - $350,000

BENEFIT AND RETENTION TRENDS

UPSKILLING

The cybersecurity skills shortage is a reality, and the talent gap is becoming wider every year. Organizations looking to hire cybersecurity professionals need to offer attractive benefits and salaries coupled with learning and development opportunities. To help combat the talent gap and barriers to entry, nonprofit cybersecurity certification organization (ISC)2 launched a free online program called Certified in Cybersecurity to help entry-level cybersecurity candidates learn the basics of cybersecurity including security principles, business continuity (BC), disaster recovery (DR) and incident response concepts, access controls concepts, network security, and security operations. Upskilling opportunities will act as an incentive for current cybersecurity workers to remain in their current roles and promote hiring for non-technical skills and personality attributes.

INTERNAL MOBILITY

Professionals are no longer thinking of career growth in terms of the traditional ladder. Instead, the “lattice” trend is increasing how professionals make career moves, signaling a growing internal mobility trend. Professionals are developing their own personalized career paths based on goals and interest areas, while upskilling and acquiring more transferrable skills across departments and roles. By investing in internal mobility strategies, using AI talent analytics, workforce planning and talent development, companies are able to identify promising internal candidates for open and critical roles while attracting top talent and developing more diverse hiring pipelines. Internal talent mobility efforts also shorten onboarding timelines and allow leaders to have more immediate impact in their new roles. While cybersecurity is not a common major for colleges to offer, there are a large range of related majors that can build experience and skills needed for a job in the field. Candidates interested in entering the cybersecurity field should be prepared to answer not what their college major was, but instead what they have learned thus far that prepares them for a career in cybersecurity.

BOOMERANG EMPLOYEES

More organizations are realizing the value in their offboarding processes and maintaining professional relationships with former employees, making sure they know the door is open if they choose to return. Whether executives who decided to retire early or mid-level managers who transitioned to another company or industry for a higher position, many companies are reaping the benefits of hiring former or "boomerang" employees who have institutional knowledge and proven skill sets in addition to tangential skills and experience they acquired elsewhere.

SCENARIO-BASED TALENT ACQUISITION STRATEGY

If there's anything organizations have learned in the past few years, it's to be prepared for not only the worst but also average and best-case economic conditions and agilely shift focus during a downturn as well as a recovery. In order to respond to markets dynamically and with a right-sized workforce, companies are looking to talent acquisition professionals who are using AI and predictive analytics to forecast the right roles, skills and geographies for changing business strategies. Additionally, hiring managers are more deliberate in their demand planning, removing silos and collaborating with leaders across business functions to better understand their needs and forecast demand for leadership roles.

HYBRID WORKPLACES ARE THE NORM

Many more companies are offering hybrid work arrangements to attract top talent and allow employees to enjoy the freedom of remote work while reaping the benefits of being in the office for professional development, collaboration or team brainstorming. Remote work productivity largely depends on an organization's needs, roles and people, and some organizations may require remote-first candidates to live within a certain geographic radius so they can visit the office when needed. However, with a hybrid employment model companies are able to maintain the best of both worlds: happy, highly engaged employees and productive outcomes. The year ahead continues to present a very candidate-driven market, and workers want the flexibility of remote or hybrid workplaces. In order to attract top talent and maintain high productivity, companies will continue to implement hybrid work arrangements. For critical roles that impact the business dramatically, hiring managers are increasingly not allowing location of the ideal candidate to factor into their consideration, allowing for more flexibility with remote and hybrid schedules.

WORK-LIFE INTEGRATION

The last few years of remote and hybrid work have shifted employee focus from work-life balance and a traditional 8-to-5 toward a more fluid schedule. More candidates are looking for companies that promote work-life integration, where success is assessed by employee output rather than the timeframe of their workday. Schedules that allow employees to put in hours when it's most convenient around their personal responsibilities, for instance working a few hours in the morning, taking an afternoon break for an appointment or to pick up kids from school, and then working more in the evening. Consequently, working from home is most popular with workers between ages 26 and 57, while the majority of employees don't want a 4-day work week. Younger workers who are earlier in their careers are likely to have less comfort or more distractions at home compared with workers later in their careers. By listening to what employees truly want, employers can prioritize the benefits that support work-life balance for employees and show an understanding of their needs as a whole person beyond their role in the company.

SALARY TRANSPARENCY

We're seeing increasing trends in many cities and states bringing forward legislation requiring salary disclosure across industries and roles, in an effort toward more pay transparency and equity.

MENTAL HEALTH AND WELLNESS

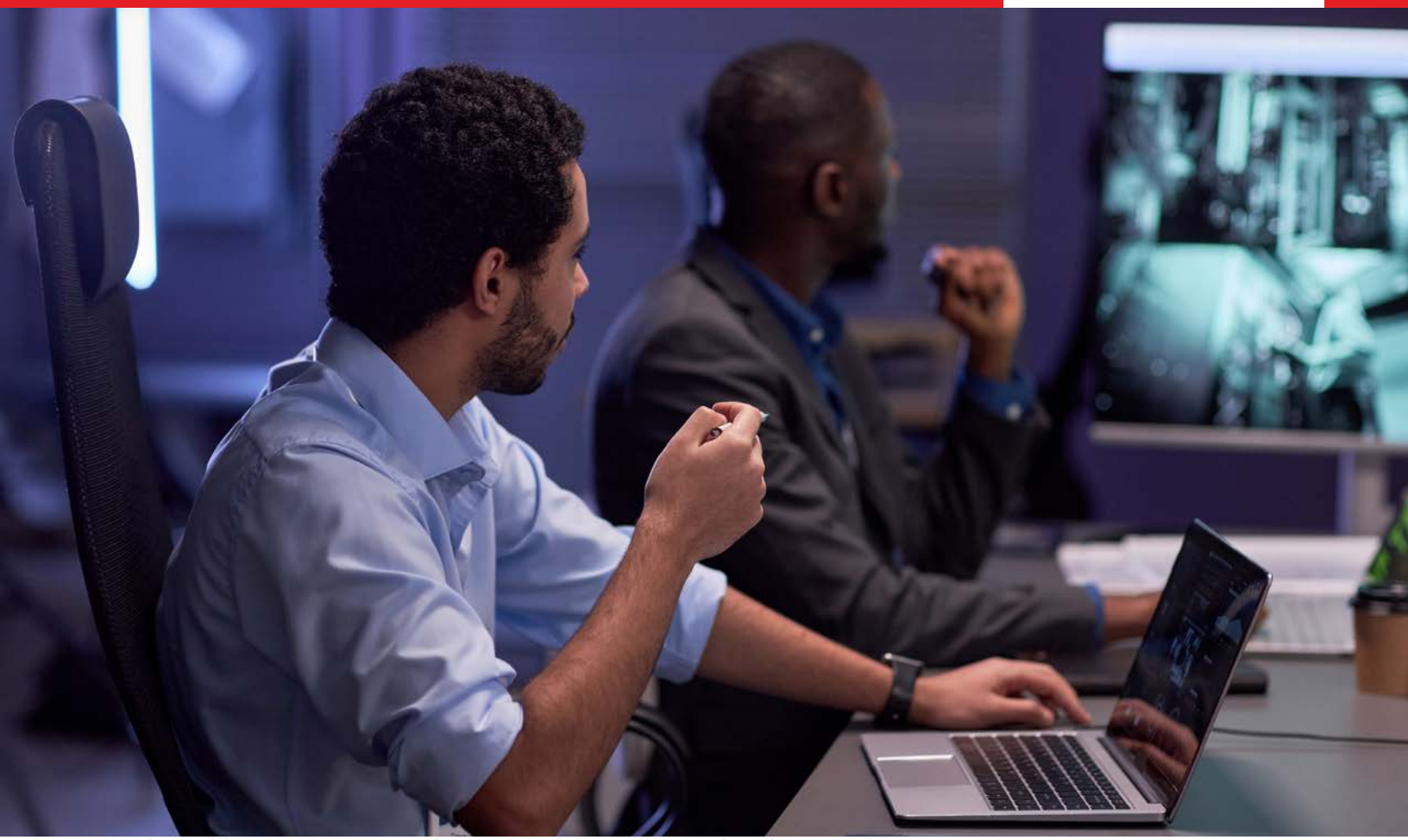
The country experienced an extraordinary consciousness of mental wellness post-pandemic, and many have been focused on the instability the global pandemic caused and its impact on employees. Currently, many employees are experiencing elevated stress, burnout and poor mental health due to inflation, increased job duties and the lingering effects of the pandemic. While mental health and wellness is top of mind for many employees and potential candidates, workplace programming and offerings are largely dependent on individual companies. While many employers enhanced their mental health and well-being benefits to better support workers in response to the pandemic, more employers are expected to prioritize employee well-being in 2023. Many organizations have created employee resource groups who advocate for and help implement mental wellness initiatives in companies and departments. Employee benefits, perks and wellness programs are expected to become more holistic to address employee mental, physical and financial well-being. Employee stress and burnout are one of the major reasons why employees leave their jobs. A Forrester survey shows that 51% of cybersecurity professionals experienced extreme stress or burnout, with 65% saying they had considered leaving their job because of job stress. In addition to offering a competitive salary, the right set of benefits will fight burnout and help retain employees, including financial wellness programs to help employees weather potential recession and reduce finance-related stressors.

DE&I

As business grows increasingly global and complex, more companies are becoming aware that to solve big business challenges they need inclusive teams and diverse perspectives. Diversity, Equity and Inclusion in recruitment and hiring is simply intentional hiring using procedures that are free from biases, with the goal of developing a more diverse, equitable and innovative workforce. Some organizations are hiring diversity officers to lead their efforts, while others are empowering hiring managers to play an active role in setting company strategies for centering diversity, equity and inclusion at the core of the business. Additionally, the cybersecurity industry is recognizing the lack of diversity and is prioritizing hiring more women and people of color to cybersecurity roles. Organizations are becoming more cognizant that this lack of diversity in the cybersecurity field matters because it can lead to a lack of understanding of the needs of different communities, a lack of trust in the industry, and can lead to a lack of innovation and creativity in the field. Diversity in the cybersecurity industry can help improve online defenses by introducing new perspectives and ideas.

BOOMERS ARE RETIRING

In the decade before 2020, many in the Baby Boomer generation–some 76 million Americans born between 1946 and 1964–put off retiring due to a variety of reasons, including improved health, shifting industry patterns, financial necessity, and a sheer reluctance to leave the workforce. The majority of the labor growth between the end of the Great Recession and the start of the pandemic came from workers 55 and older, and in 2019, a record 57% of Americans in their early 60s were still working. By comparison, those born into the Silent Generation before the Boomers number just 47 million people, and Generation X number a mere 55 million. By working just a few years longer than anticipated, Boomers helped reshape the entire labor market for a decade. Nearly all of them are now in their 60s and 70s and are retiring and leaving the workforce for good, creating a structural labor shortage that will affect the economy and present difficulties in combating inflation. A smaller pool of workers means companies will have to raise pay and most likely prices in competition for workers. Additionally, an economy where fewer people are working is one that cannot grow as quickly.



ADDRESSING HEALTH CARE COSTS AND EXPANDING VOLUNTARY BENEFITS

Finding ways to reign in rising health care costs while keeping benefits affordable is critical for employers. A diverse, distributed workforce will continue to put pressure on employers to shift away from a one-size-fits-all approach to benefits. Instead, employers will find value in creating packages that have the flexibility to serve people with varied needs and priorities. The year ahead will see employers explore contemporary benefits like family planning and reproductive care, elder care, tuition reimbursement, and pet care as critical additions to mainstays like major medical, dental, vision, and disability. Adoption assistance can also foster a family-friendly corporate culture and help make adoption more affordable. Keeping a lid on rising health care costs will likely remain at the forefront for organizations this year. But to remain appealing to current and potential employees, many employers are choosing to absorb premium increases, rather than pass them along to workers. To hold down costs for themselves while appealing to employees, a growing number of employers will likely turn to voluntary benefits, such as life insurance and supplemental health coverage that can assist in providing financial security and help fill in financial gaps that may be left by core health plans. Updating family leave policies and mandatory paid time off are valuable benefits to employees.

BUILDING CULTURE

Employees and employers are aligned on the most important elements of company culture: work-life balance, building trust, and team camaraderie. Trust between employees and the company is a two-way street, with 20% of employees surveyed saying it's important to be trusted by their peers and superiors, and 27% of employers agreed building trust with employees is important. Employers are exploring avenues other than after-hours teambuilding to meet the goals of building trust and improving work-life balance for employees.

HIRING TRENDS & EMPLOYMENT OUTLOOK

C-SUITE AND TOP EXECUTIVES

Overall employment of top executives is projected to grow 6% through 2031, about as fast as the average for all occupations. About 318,100 openings for top executives in all industries are projected each year, on average, over the decade, with many of those openings expected to result from the need to replace workers who transfer to different occupations or retire.

In addition to salaries, total compensation for corporate executives often includes stock options and other performance bonuses. These executives also may enjoy benefits such as access to expense allowances, use of company-owned aircraft and cars, and membership to exclusive clubs.

INFORMATION SECURITY ANALYSTS

Employment of information security analysts is projected to grow 35% through 2031, much faster than the average for all occupations. About 19,500 openings for information security analysts are projected each year, on average, over the decade.

COMPUTER AND INFORMATION SYSTEMS MANAGERS

Employment of computer and information systems managers is projected to grow 16% through 2031, much faster than the average for all occupations. About 48,500 openings for computer and information systems managers are projected each year, on average, over the decade.

SOFTWARE DEVELOPERS, QUALITY ASSURANCE ANALYSTS, AND TESTERS

Overall employment of software developers, quality assurance analysts, and testers is projected to grow 25% through 2031, much faster than the average for all occupations. Increased demand for software developers, software quality assurance analysts, and testers will stem from the continued expansion of software development for artificial intelligence (AI), Internet of Things (IoT), robotics, and other automation applications. In response to concerns over threats to computer security, organizations are expected to increase investment in software that protects their electronic networks and infrastructure, resulting in an increased demand for developers to create security software and for quality assurance analysts and testers to create and execute software tests. About 162,900 openings for software developers, quality assurance analysts, and testers are projected each year, on average, over the decade.

COMPUTER AND INFORMATION RESEARCH SCIENTISTS

Employment of computer and information research scientists is projected to grow 21% through 2031, much faster than the average for all occupations. The research and development conducted by computer and information research scientists turn ideas into technology. Computer and information research scientists will be needed to write algorithms that help businesses make sense of very large amounts of data. A growing emphasis on cybersecurity also should lead to new jobs because computer and information research scientists will be needed to find innovative ways to prevent potential cyberattacks. About 3,300 openings for computer and information research scientists are projected each year, on average, over the decade.

Source: U.S. Bureau of Labor Statistics Occupational Outlook Handbook

CONCLUSION

As interconnectivity increases, so do the opportunities for bad actors to steal, damage, or disrupt, severely impacting businesses operationally and financially. The recovery and impact cost of a ransomware attack can cost an organization upwards of $5 million, a hit many companies can't afford to take. The rise in cybercrime has fueled a rapid demand for cybersecurity professionals, with job outlook expected to grow 35% over the next five years.

However, the scarcity of talent is a very real threat to organizations, almost as much a threat as the cyberattacks themselves. The ongoing shortage of qualified cybersecurity personnel continues to expose organizations to cyber risks, made even more glaring by insufficient automation of tasks needed to execute good cybersecurity. With economic pressure leading companies to consider thinning their security teams to save money and cybercriminals seeking to take advantage of easy access to malware-as-a-service, the world needs as many talented professionals as possible to defend and protect digital environments.

With a vast number of different specializations and roles one can work in, those who are detail-oriented, curious and motivated, with a knack for mathematics and other fields can foster their talents in compliance, incident management, security operations center management, or other roles in this exciting and fast-paced industry.

Are you looking for talent to fill a role in your organization, or are you exploring opportunities for a career move in cybersecurity?

Contact BrainWorks Executive Search:

https://brainworksinc.com/practice-areas/cybersecurity/

Guy O. Gomis, SVP, Partner & Practice Leader
(908) 608-8855
guy@brainworksinc.com

ABOUT BRAINWORKS

BrainWorks is a recruiting organization that connects top organizations with their industry's leading candidates, partnering with clients to match them with recruiters who are experts in meeting their needs. With more than 15 areas of specialization, we solve your hiring challenges by leveraging our vast network of highly skilled talent and our extensive, time-tested industry expertise.

You can't settle for less than world-class talent, and we know how to help you get it – fast. At BrainWorks, we are goal-oriented and time sensitive. We help our clients find the right people who will drive future success. Hiring is tough in today's historically tight labor market. BrainWorks has the tools to help organizations like yours overcome it. Our executive recruiters build trusted partnerships with leading organizations and connect them with A-level candidates, time and time again. We can do the same for you.

We Believe:

1. A strong process is the foundation of effective recruiting.
2. Planning is the first step in any search.
3. The most qualified candidate may not be the one actively looking.
4. You have to dig deeper and respond faster to win top talent.
5. Honesty and transparency are essential in communication.
6. A successful hire doesn't end when an offer is accepted.

To learn more about how BrainWorks can help you, contact us at:

https://brainworksinc.com/practice-areas/cybersecurity/

Guy O. Gomis, SVP, Partner & Practice Leader

(908) 608-8860

guy@brainworksinc.com

Sources:

Barracuda Cybersecurity Year in Review: https://blog.barracuda.com
Cybercrime Magazinae, https://cybersecurityventures.com
Deloitte Insights, https://www2.deloitte.com/us/en/insights.html
Dragos ICS/OT Year in Review, www.dragos.com
Forbes, www.forbes.com
Fortune, https://fortune.com
Gartner Insights, www.gartner.com/en/cybersecurity
Gitnux, https://blog.gitnux.com/cybersecurity-diversity-statistics/
Korn Ferry, www.kornferry.com
Logicgate, www.logicgate.com
New York Times, www.nytimes.com
RSA Conference, www.rsaconference.com/usa
SC Magazine, www.scmagazine.com
Security Boulevard, https://securityboulevard.com
Security Magazine, www.securitymagazine.com
Splunk The State of Security 2023
Tech Target, www.techtarget.com
The Hacker News, https://thehackernews.com
The Wall Street Journal, www.wsj.com
Tilson HR, www.tilsonhr.com
U.S. Bureau of Labor Statistics Occupational Outlook Handbook, www.bls.gov/ooh

BrainWorks

16 Mount Bethel Road, Suite 292 Warren, NJ 07059
(908) 771 0600
adminteam@brainworksinc.com

www.brainworksinc.com