Hewlett Packard
Enterprise

2023 Cybersecurity Annual Report

At HPE, we believe that our individual and collective success lies in our ability to share learnings, ideas, and opportunities. When it comes to securing our respective organizations, we're all plagued by the same challenges: a global cybersecurity skills shortage, an expanding attack surface, distributed data, and increasing demands for transparency from stakeholders. And in protecting an edge-to-cloud world, how do we decide who does what? We believe cybersecurity has become a shared responsibility, as a single weak link can impact all of us. This report showcases some of the work we've done on that front during 2022 and some predictions for 2023. We're grateful for the opportunity to share it with you-our customers, partners, and peers.

Contents

2022 by the numbers

2.6B

Our Enterprise SIEM logged over 2.6 billion events per day, prompting triage, investigation, and resolution by our Cyber Fusion Center.

2.2K

The HPE GreenLake edge-to-cloud platform continuously applies more than 2,200 separate security controls to protect customers and their data in real time.

1.9K

We improved visibility across our cloud estate, continuously monitoring for more than 1,900 cloud security controls.

1K

We blocked an average of 1,060 phishing emails received at HPE every day. In total, we blocked approximately 1 billion email threat vectors.

334

HPE's Product Security Response Team published 187 security bulletins, covering 334 CVEs across 450 products, including 46 HPE-issued CVEs. All impactful CVEs were remediated according to HPE security policies, and patches were made available to ensure the minimum possible impact to the security and availability of customer environments.

58

HPE holds Global ISO 27001 Certificates at 58 sites in 36 countries, adding 11 sites in 2022 with approval for an additional 16 sites pending in 2023. Our compliance program has expanded to include SOC 1 and SOC 2 attestation for a number of our customer support centers, as well as FedRAMP for Aruba Central and CSA STAR assessments for our cloud management platforms.

33

HPE undertook 33 threat hunts with the purpose of uncovering advanced persistent threat actors within the network. The results of these threat hunts were used to improve our monitoring rulesets.

98%

More than 55,000, or 98%, of HPE employees completed annual cybersecurity awareness training.

50%+

In line with industry trends, more than half of the cybersecurity incidents investigated by HPE's Cyber Fusion Center could be attributed to user actions such as the attempted installation of infected software, disabling security tools, or running crypto-mining software, which were blocked by our security controls.

Antonio Neri
Chief Executive Officer
HPE

We prioritize security

At Hewlett Packard Enterprise, we help customers use technology to turn ideas into value. Those ideas need a secure place to be nurtured, which is why we have placed a distinct focus on protecting them and the systems where they are cultivated.

Today, we manage more than 2 million devices and over 1 exabyte of data through the HPE GreenLake platform, and that's a responsibility we take seriously. In the past year, we have strengthened our position across security categories and have diligently invested in cybersecurity research, controls, and talent development.

To further demonstrate our commitment to security, we recently acquired Axis Security, which will enable us to expand our edge-to-cloud security capabilities and address the need for improved application performance and increased network security as enterprises continue to migrate applications to the cloud.

This report underscores Hewlett Packard Enterprise's commitment to cybersecurity and to the responsibility we all share.

Bobby Ford
Chief Security Officer
HPE

A new approach to cybersecurity

It's not often in a CSO's career that they're presented with the opportunity to join a global tech company that is actively transforming and creating a new market. It's exciting and challenging, and I believe that at Hewlett Packard Enterprise, we're changing the way the industry thinks about the cloud. The cloud is not just a destination but also an experience, and with HPE GreenLake, it's an experience that can be brought to you.

One thing that became clear to me when I joined HPE was that Cybersecurity and Digital Risk Management would be responsible for not only protecting HPE's business but also securing the cloud experience that we deliver to our customers. So a lot of the work my team has been doing over the past 18 months has been focused on that-understanding the risk that is introduced as workloads are migrated from secure, on-premises data centers out to public cloud, the edge, and anywhere in between, as part of a hybrid cloud experience.

As we enter 2023, the changing economic climate has tightened budgets across industries. And a global shortage of candidates available to fill the vast number of job vacancies continues to stifle even the most mature cybersecurity programs.

As cybersecurity and technology leaders, we have the opportunity to make an impact on our businesses and our people as we take on all of these concerns. This report showcases some of the initiatives we launched in 2022 to meet these challenges and deliver a secure edge-to-cloud experience for our customers. These initiatives have created a foundation for us to build upon in 2023 and beyond, always with the aim of helping you transform your business.

Threat landscape

New and increasingly serious threats are on the rise

HPE isn't just a leading global technology organization; it's also a target that cybercriminals attempt to infiltrate and attack every day. We know we have to stay one step ahead of the adversaries, so we actively monitor different threat vectors, including:

Hostile nation-states are on the rise.

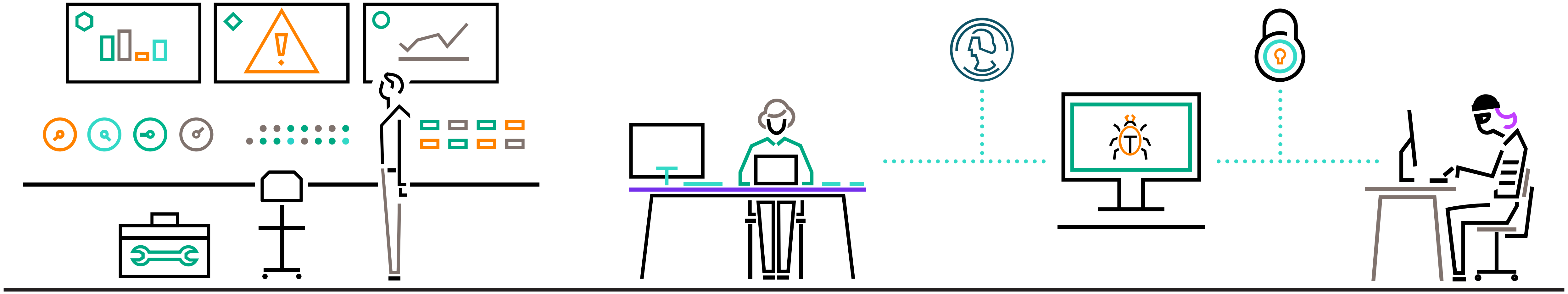
Advanced persistent threats (APTs) continue to cause concern in numerous industries and on a global scale. The actors responsible for creating APTs are richly funded, highly skilled, well organized, and may be military organizations or contracted security professionals. As these hostile actors continue to target the semiconductor, telecommunications, and infrastructure sectors in search of information related to high-performance computing, Big Data, and ML/AI, HPE continues to track and protect against APT-related activities with the goal of preventing economic espionage.

Phishing remains an epidemic.

The human element is always the weakest link in a company's security defenses. Phishing has long been a critical cybersecurity problem, with a new phishing site popping up on the internet every 20 seconds. At HPE, we block more than 1,000 distinctly unique phishing attempts every day, making it the largest threat vector used against the company. While using technology to identify and block almost all of these attacks is key, training team members to recognize these increasingly sophisticated attacks remains a priority. We run a successful annual cybersecurity awareness training program and deploy regular phishing campaigns to keep team members up to speed.

Ransomware attacks get simpler than ever.

Years ago, cybercriminals had to be sophisticated masters of programming, hardware design, networking, and more. That's all changed as teams of cybercriminals develop malware toolkits and make them available to criminals "as a service." This has made launching cyberattacks, such as ransomware, a point-and-click affair. Attackers no longer need any real level of sophistication to carry out these initiatives but only a target and the desire to plan an attack. This has led to an explosion in ransomware-related cyberattacks in recent months. At HPE, we have sophisticated defenses against these attack vectors, and we also provide advisory services and build solutions for our customers looking for best practices around ransomware defense and recovery.



Threat landscape

New and increasingly serious threats are on the rise

Insider attacks are increasing.

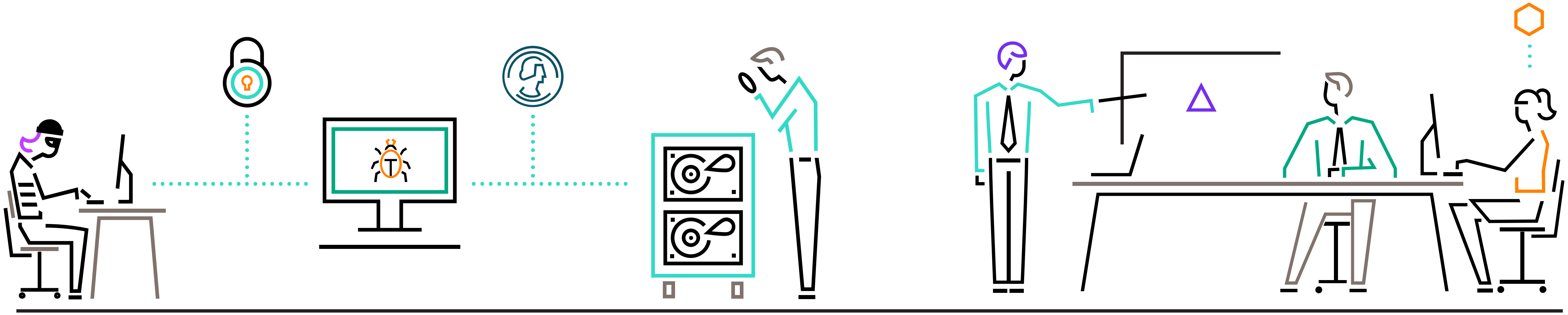
Whether due to malicious intent or simple negligence, employees remain a key vector for attacks of all types. These attacks can be much harder to detect and, as a result, can inflict far more damage than traditional outsider attacks. Many organizations overlook the dangers of insider threats, but insider attacks represent another key threat that must be mitigated. As a big technology organization, we not only have to be aware of disgruntled employees wishing to cause harm to HPE, but also the potential for team members to be lured into involvement with information theft by well-funded parties. Cybersecurity awareness training continues to play a big role here.

Vulnerabilities hit a record high.

The number of reported security vulnerabilities across hardware and software is staggering, and growing: over 22,000 reports in 2022, up from 20,000 in 2021. Enterprises are struggling with patch management as a result, making quick remediation and triage more critical than ever, along with appropriate compensatory controls. At HPE, vulnerability management is a trifecta—looking after the vulnerabilities in our enterprise estate, the vulnerabilities in our cloud management platforms, and the vulnerabilities in the products and services we sell to our customers.

Supply fabric complicates security.

As enterprises increasingly partner with other organizations through collaborations, outsourcing, and other arrangements, they must place additional emphasis on third-party security management. HPE's third-party risk management services have extended into supply chain and global procurement security, offering a framework to mitigate logistics disruptions and protect both customers' and our own intellectual property. Additionally, as a supplier to our customers, we recognize the important role that supply chain security plays in customer relationships, and we have grown our capabilities to respond to customer queries accordingly.



A look at the security efforts we've undertaken and their results

Supporting the edge-to-cloud transformation

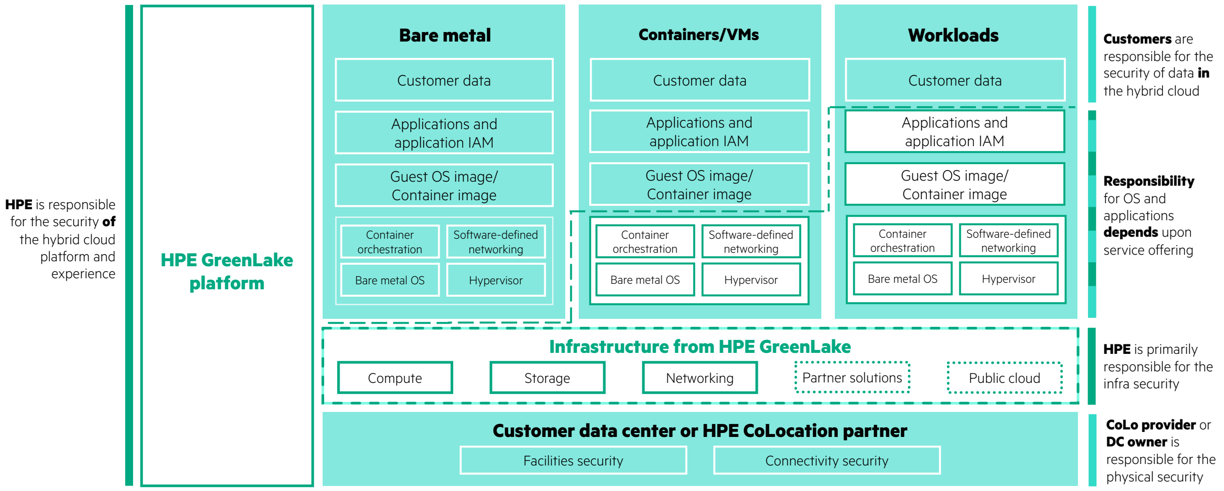
The cloud has proven its value as a resource for reducing infrastructure and support costs and for quickly building applications and services. But well-publicized incidents over the past few years have shown how critical security and compliance are to cloud-based ecosystems.

At HPE, we are well aware of the need for security across edge to cloud and have developed a security architecture that specifically addresses it. We are making security a priority on our cloud platform, HPE GreenLake, and are resolute in both our secure-by-design platform principles and the protection of customer data as a primary design criteria.

Our key tool for accomplishing our security goals is leveraging a risk-based and compliance-driven approach to cyber resilience and data protection, and our platform is fully aligned to industry standards and best practices.

This focus has been crucial as workloads have shifted away from pure public cloud environments, which customers increasingly say is an imperfect solution for all operations for a variety of reasons, including challenges around the confidentiality and sovereignty of data. As the hybrid cloud becomes an increasingly popular and flexible platform choice, HPE is fully prepared to secure these workloads, no matter what the specifics of the customer's operations are.

Along this path, we've learned that questions often arise around where our responsibility ends and the customer's responsibility begins. Any misunderstandings or lack of clarity along these delineating lines can introduce security vulnerabilities and increase exposure to new attack vectors. To mitigate these risks, we developed the HPE GreenLake Security Shared Responsibility Model, which clearly defines the roles of HPE and the consumers of our services, helping to reduce the size of the potential attack surface.


HPE is responsible for the security of the hybrid cloud platform and experience
HPE GreenLake platform
Bare metal
Containers/VMs
Workloads
Customer data
Applications and application IAM
Guest OS image/ Container image
Container orchestration
Software-defined networking
Bare metal OS
Hypervisor
Infrastructure from HPE GreenLake
Compute
Storage
Networking
Partner solutions
Public cloud
Customer data center or HPE CoLocation partner
Facilities security
Connectivity security
Customers are responsible for the security of data in the hybrid cloud
Responsibility for OS and applications depends upon service offering
HPE is primarily responsible for the infra security
CoLo provider or DC owner is responsible for the physical security

HPE GreenLake Security Shared Responsibility Model

Meanwhile, we're supporting our cybersecurity initiatives by building a cross-functional security team that supports both our internal business and as-a-service operations, led by our Chief Security Officer Bobby Ford, who is actively challenging the traditional role of the CSO. In Bobby's view, security is a function that the CSO should use to enable the business and not just enforce arbitrary controls, giving everyone in the enterprise the tools they need to make security an inherent part of all operations. Additionally, Bobby has focused on an unconventional approach to talent acquisition, recognizing the high number of cybersecurity vacancies that the industry collectively needs to fill. (See also the section "Rethinking talent" on page 12.) By positioning HPE as a "talent maker," not a "talent taker," he's looking to unexpected places to staff security teams.

Accomplishments and investments

Where we're putting our money and time

Meeting industry expectations around security

U.S. Presidential Executive Order 14028 established new rules to help ensure the security of the supply chain, particularly from a software standpoint. The software bill of materials lays out in detail the components used in building a software application, and HPE has done a significant amount of work to develop processes to gather information to populate SBOMs and provide them for HPE products when needed. As well, our Trusted Supply Chain initiative is now available worldwide. This initiative expands and secures our supply chain offerings, ensuring customers that our products are made with verifiable, authentic parts. Today, we remain the only major server manufacturer to produce industry-standard servers with a U.S. Country of Origin designation.

Taking a layered approach to protection

We've created a chain of trust to protect customers' data (and our own) from cradle to grave. It starts with the lowest levels of silicon, where our unique Silicon Root of Trust gives servers an immutable fingerprint that prevents malicious code from corrupting firmware, and we thoroughly vet suppliers and third parties to reduce the risk of security threats all along the supply chain. Our network devices also use hardware identity and hardware-backed firmware protection to protect device integrity. Our end-of-life program details policies for the safe decommissioning, refurbishing, and recycling of assets. Independent, third-party penetration testing and analysis ensures that all of these programs are highly effective, aligning with National Institute of Security and Technology (NIST) 800-53 controls.

Engaging with customers about security

From a security perspective, we recognize that our relationship with customers is changing as the industry adopts hybrid cloud platforms and that this opens up questions about who is responsible for what. At HPE Discover 2022, our biggest customer and partner event of the year, we addressed these questions head-on, with a session from CSO Bobby Ford. He unveiled HPE's shared responsibility model, stressing the importance of a common language that providers and customers can use to understand the needs of one another. Bobby also led a session with a panel of customers and industry experts to discuss the hype and reality behind zero trust, and how transforming to a security-first culture is critical to improving cyber resilience.

Our newly created CISO Circle brought together top cybersecurity minds across multiple industries to privately share wisdom and best practices with one another. For broader consumption, we produced multiple white papers, webinars, and online articles offering guidance on the latest cybersecurity trends, threats, and solutions. We were also happy to meet customers in our new Houston headquarters, as we hosted tours of our Cyber Fusion Center and discussed best practices for cybersecurity in an edge-to-cloud world.

Team Member Spotlight

Meet **McKaela Doherty, VP, Cybersecurity Center of Excellence**

McKaela has served in various leadership roles at HPE over the past 10 years. As VP of the Cybersecurity COE, McKaela applies her business acumen to building a pan-HPE cyber community, consulting with business teams, and establishing strong security habits among HPE's 60,000 employees. She has pushed the organization to become more externally focused, demonstrating HPE's cyber capabilities and engaging with customers to share ideas and best practices. "But what I'm most passionate about is people," she says. "Our cyber talent programs are all about finding creative ways to recruit, motivate, and upskill team members-and help make HPE a great place to work."

Accomplishments and investments

Where we're putting our money and time

Giving back

HPE strives to be a force for good, giving back to communities around the world through volunteerism, donations, and support from the company's foundation. But one of the most powerful ways we can give back as a tech company is to lend our deep expertise to those who can benefit from it. This year, the HPE team in Galway, Ireland, did just that, partnering with Safe Ireland to build cybersecurity awareness. The team created a billboard campaign—#RedFlagsAreAbuse—and a set of online resources designed to prevent vulnerable groups from becoming victims of technology-facilitated abuse. It launched in October 2022 and received national media attention.

Investing in standards

We're investing in standardizing our approach to architecting our own hybrid cloud applications by following and attesting against industry standards. Our services team also helps our customers to align against these same standards with its security-led consulting engagements. This includes developing new security architectures and methodologies that are designed to provide a repeatable, proven approach to protection that aligns with standards including NIST, CSA, and ISO. These have been codified in our Enterprise Security Reference Model, which we demonstrate at strategic security workshops that cover a variety of topics ranging from zero trust to cyber resilience.

Team Member Spotlight

Meet **Ankush Chowdhary, Cloud Services CISO**

Ankush has been part of the cybersecurity world for more than 20 years, but he faces his most critical challenge today as the leader of cloud security transformation for the HPE GreenLake platform. By leveraging his prior experience in building security operations centers, security monitoring programs, incident response, and threat intelligence programs for major public cloud providers, Ankush has brought a much-needed multi-disciplinary approach to HPE's edge-to-cloud security operations. "Data-first modernization is the key to success in today's enterprise," he says, "but enterprises will never succeed without a secure platform on which to work."

Rethinking talent

Changing the way we're investing in team members

Many industries are grappling with severe talent shortages, but this is especially true in cybersecurity. As HPE CSO Bobby Ford notes, reports of a cybersecurity talent shortage aren't exactly on point. He sees it as a shortage of experience. Here are key ways we've worked to create and grow our security professionals in 2022.

Opening doors to overlooked talent

There will be more than 3.5 million cybersecurity jobs open by 2025, but a laundry list of requirements inhibits many of these roles from being filled. The result is an endless tug of war for talent between companies. What if we looked to create talent ourselves by giving opportunities to those who need it? This year, we launched the Cybersecurity Career Reboot Program. which actively seeks out candidates who may be overlooked because they lack the experience required to land entry-level jobs in the field, who are viewing cybersecurity as a new career path, or who may find it difficult to gain corporate employment. What they don't need to have: a college degree or cybersecurity experience. During an intensive, six-month program, participants are paid while learning the nuts and bolts of cybersecurity, embedded within various cyber functions within HPE and taking on project-based work while being mentored by our team members. Our first Career Reboot cohort received national attention. They graduated at the end of 2022, and what was initially a pilot project is now a permanent and growing program.

Giving new graduates a first look at cybersecurity ops

Similarly, our Professional Rotation Experience Program (PREP) is designed to recruit recent graduates into a two-year rotational program that includes global exposure to all our cybersecurity functions. PREP participants gain experience with the foundations of cybersecurity through hands-on project work, exposure to a variety of experiences, and innovative training and development, rotating through the different teams within cybersecurity every six months during the program.

Stressing diversity and mentoring

Through a strong mentoring program and a robust internship program, we're seeing more interest in cybersecurity—from a wider group of workers-than ever. At HPE, we know that people are our greatest strengths, and we consider equity, inclusion. and diversity to be paramount to success in the cybersecurity discipline. We believe that diverse voices improve cybersecurity operations, helping us to overcome inherent biases based on traditional ways of working and to challenge the status quo. This kind of innovative thinking is becoming increasingly critical as attackers adapt their techniques, demanding equally creative responses.

Security outlook: 2023 and beyond

Here's where we believe the industry needs to go

Priorities

Cybersecurity is a strategic business issue that impacts decision-making in every part of the enterprise.

- Define **cyber maturity improvement goals** that align with an industry standard cybersecurity framework, building a common language across cybersecurity teams.
- Establish a **cybersecurity risk framework** by defining criteria to objectively and consistently measure asset criticality in alignment with enterprise risk teams and business leaders.
- Adopt a metrics-based approach to **measuring security controls effectiveness**, enabling leaders to make informed decisions aligned with business priorities and appetite for risk.
- Invest in **talent creation and development** to help address the cybersecurity talent shortage.
- **Protect critical infrastructure** against increasing threats—and the ensuing economic disruption—to ensure national security.
- Manage **geopolitical tensions** and the resulting advanced malware that has now become a commodity, threatening all enterprises.

Security outlook: 2023 and beyond

Predictions

“Cybercriminals will double down on automation as attacks become more procedural and repeatable. Cybercrime marketplaces selling prepackaged malware deployment attacks as a service will increase in popularity, driving more attacks of opportunity and creating an increased capacity drain on cyber operations.”

– Daniel Frye, Enterprise CISO

“We see a risk from distributed supply chains comprising manufacturing and assembly sites in geopolitically adversarial countries or in countries at risk of geopolitical invasion. This can in turn increase the risk of counterfeit or malicious components entering the production lifecycle.”

– CJ Coppersmith, Director, Product Security

“As organizations embrace digital transformation and IoT, attackers will likely continue to take advantage of the attack surface these create, and destructive attacks could become even more damaging.”

– Sandya Bhoajaraj, Strategic Technical Advisor, Cybersecurity and Digital Risk Management

“As boards come under increasing scrutiny, security will maintain its status as a top concern. Budgetary pressures will require security teams to do more with less and focus on what really matters most to the business.”

– Paul De Luca, Director, Cyber Risk Management

“In light of new regulations and court decisions, CISOs, CSOs, and other security professionals will increasingly be held personally accountable for their failures to provide required breach disclosures or to adequately secure sensitive data.”

– Brian Schmitt, Associate General Counsel, Cybersecurity

Security outlook: 2023 and beyond

Predictions

"The cyber threat landscape continues to grow at an exponential rate. Threat actors such as nation-states and cybercriminals will continue to advance emerging technologies. Security research indicates threat actors are evolving their tradecraft with artificial intelligence and quantum computing. Organizations will need to adopt technologies such as quantum-resistant (or post-quantum) cryptography to secure their data in the near future."

– Travis Murray, Cyber Intelligence Team Lead

"Increasing use of AI/MLOps in cybersecurity will aid in the discovery and remediation of unusual activity in the enterprise."

– Rohini Chavakula, Data Scientist

"Organizations will have an increased focus on building IT architectures that are able to withstand, respond to, and recover from all kinds of IT and cyber-related threats, especially in light of new regulations such as the EU Digital Operational Resilience Act for the financial sector."

– Lois Boliek, Director, Cybersecurity Services

"The enterprise perimeter will expand further and in some cases disappear as organizations invest in edge to cloud and as work from home remains the new way of operating. Technologies such as SASE and SD-WAN, along with zero trust, will play a critical role in the development of effective level controls."

– Tim Ferrell, Distinguished Technologist, Cybersecurity Services

"Cybersecurity insurance will become a standard business requirement in most industries. However, faced with an increasing number of payout requests, brokers will increase premiums exponentially and introduce pre-acceptance criteria around compliance and minimum levels of security."

– Simon Leech, Director, Cybersecurity and Digital Risk Management

Team Member Spotlight

Meet **Carlos Camarillo, Cybersecurity Career Rebooter**

Carlos was born in Mexico City and raised in Southern Mexico. After a stint at Iberoamericana University, he eventually transferred to Ohio's Heidelberg University where he completed his undergraduate studies, moving on to earn an MBA at the nearby University of Findlay. Carlos moved back to Mexico after a family emergency and ran a local restaurant for more than a decade until the pandemic hit, after which he sold the business. Through HPE's Career Reboot Program, Carlos received an employment offer as a cybersecurity analyst in our Houston office, despite a lack of formal cybersecurity training. "I love being back in the corporate world," he says, "and working for a world-class technology leader."

Security outlook: 2023 and beyond

Recommendations

Build resilience and embrace zero trust

Clarify the shared security model of your cloud operations, and understand where your responsibilities begin and your providers' end.

Understand your supply chain in full, and pinpoint locations where third-party cyber risks reside.

Work to connect security teams more closely with the business so they more fully understand the risks to the organization that their work helps to mitigate.

Invest in user behavioral analytics, which model user activities over time and uncover deviations from established patterns, revealing potential attacks underway.

Move from device-based data protection to self-protecting data.

Build a security culture into the organization all the way up to the board level, and commit to a strong cybersecurity awareness training program.

Hire for talent, not necessarily experience. The latter can be developed or earned whereas the former not so much.

Encryption, tokenization, and pseudonymization techniques can protect and mask data in all forms until the point at which it needs to be consumed.

Leverage zero trust and SASE to increase the cybersecurity resilience of your infrastructure—and better prepare the organization against threats.

Security is possible only through the combination of automation and human diligence, ensuring that critical fixes are addressed first and that all impactful vulnerabilities are addressed in an appropriate time frame.

Resources from HPE's Cybersecurity Center of Excellence

HPE reports and online content

- Sharing responsibility for security with HPE GreenLake
- A security practitioner's view of edge-to-cloud cybersecurity
- HPE Annual Living Progress Report
- HPE Critical Product Security Vulnerability Alerts
- HPE Cybersecurity Services
- HPE Cybersecurity Education
- HPE GreenLake Security
- Careers at HPE

External ratings

UpGuard

Feedback

We look forward to your feedback on any security-related topic as our edge-to-cloud world continues to evolve. Please reach us here.

Visit **HPE GreenLake**

Hewlett Packard
Enterprise