HealthEquity®

Arnold
HealthEquity
team member

Heather
HealthEquity
team member

2023

Security Annual Report

Contents

A note from our CEO

Jon Kessler

In 2022, HealthEquity experienced significant growth and transformation. We're continuing to evolve and leverage technology for innovation, while we expand our offerings beyond traditional Health Savings Account (HSA) services. As a healthcare service provider, our commitment to cybersecurity is paramount in our partnership with clients and members.

From the beginning, we set out to establish HealthEquity as a leader in data security, cultivating a security-focused culture across our team. We have undergone organization-wide changes, integrating security into every aspect of our operations, including team member engagement, technology infrastructure, data fabric, and product development. Our dedication has allowed us to align with leading financial services companies, showcasing the maturity of our advanced cybersecurity programs.

Transparency has been a cornerstone of our security program, driving its growth and resilience. We believe that open communication, collaboration, and transparency leads to stronger security. This report serves as a testament to our commitment as we actively share best practices and engage with customers, policymakers, and organizations to address the challenges and opportunities in cybersecurity.

While we take pride in our progress, our journey continues. The upcoming year for HealthEquity security will be marked by continuous evolution and an unwavering dedication to helping our clients, partners, and members enhance their own cybersecurity postures.

As we forge ahead, we remain driven, energized, and steadfast in our mission to strengthen cybersecurity and ensure the trust and protection of our valued partners and clients.

Jon Kessler
President, Chief Executive Officer, and Director

Jon Kessler
HealthEquity
CEO

A note from our CSO

Larry Trittschuh

To set HealthEquity apart from our competitors, we strive to stay ahead of the evolving threat landscape and exceed the best practices in the industry when it comes to security. As a demonstration of our commitment to cybersecurity, we are thrilled to announce the appointment of Kristina Belnap as our new Chief Information Security Officer (CISO). She will lead our efforts in creating a world-class security function.

As we reflect on the global cybersecurity challenges faced in 2022, we acknowledge that the coming year will undoubtedly present us with new challenges. We are committed to embracing cutting-edge technologies, such as cloud computing and generative Artificial Intelligence (AI), leveraging their potential to bolster our security posture while driving business growth.

By harnessing the power of the cloud, we can enhance our security capabilities, streamline operations, and more effectively navigate the evolving threat landscape. Additionally, our utilization of generative AI empowers us to proactively detect and respond to emerging threats, safeguarding our organization and partners from potential harm.

As we continue to evolve and transform, we remain steadfast in our commitment to championing innovation, cultivating secure practices, and fostering a resilient security culture.

Larry Trittschuh
Chief Security Officer

Larry Trittschuh
HealthEquity
CSO

Meet our new CISO

Kristina Belnap

I am truly excited to be the new Chief Information Security Officer here at HealthEquity. I have been part of this amazing company for five years and I am proud of the ongoing advancements we have made in enhancing security and elevating the member experience.

The financial, healthcare, and technology sectors have undergone extensive changes. Our objective is to stay ahead by investing in a talented team and implementing mature cybersecurity practices, ensuring our readiness to tackle emerging challenges.

I am passionate about collaborating with our team members and leveraging technologies that foster business growth, scalability, and enhanced member service, all while prioritizing the protection of their valuable data and information. We are dedicated to instilling confidence in our members and partners, continuously striving to enhance their journey.

Collaboration across our security and technology teams allows us to continually improve our remarkable service.

Kristina Belnap | SVP & CISO

Kristina Belnap
HealthEquity
CISO

2022 HealthEquity Security Highlights

Prioritized Consumer Data Rights

We implemented policies and procedures to meet applicable data privacy laws and regulations. This includes data minimization, providing consumers with the right to access, delete, and port their data, and facilitating their right to opt out of cookies. We have also invested heavily in security controls to protect the confidentiality of consumer information.

Focused on Business Resiliency & Managing Supply Chain Risk

Over the past year, HealthEquity focused on preparing against cyber incidents, especially ransomware, by reducing risk exposure from our supply chain and enhancing our business resiliency program to ensure timely response and quick restoration of services in the event of disruptions. We conducted internal and external tabletop exercises to challenge our existing processes, identify areas for improvement, and compare our efforts to those of our industry peers.

Strengthened Cloud Security

To bolster our cloud security, we established a Cloud Center of Excellence (COE) and improved container security. Our Cloud COE ensures standardized governance, best practices, and expertise across our cloud environments. We fortified container security to mitigate vulnerabilities and unauthorized access, enabling faster application onboarding and improved customer response time. These measures enhance operational efficiency and uphold a secure and resilient cloud infrastructure.

Enhanced Team Member Security Awareness

We have expanded our Security Awareness program with tailored annual training, monthly phishing tests, and educational videos. As a result, our team members exhibit improved cybersecurity awareness, with reduced susceptibility to phishing simulation emails and increased reporting of suspicious emails, including actual phishing attempts. Our proactive approach to employee security awareness strengthens our overall defense against evolving cyber threats and fosters a culture of cybersecurity within our organization.

Modernized Security Tools

We upgraded and integrated our security tools, focusing on cloud and data protection, access management, logging, and image recognition. This initiative has improved governance, reduced risk, and increased operational efficiency. By collaborating with technology providers, we have co-designed solutions that benefit the broader business ecosystem, strengthening overall security. Our enhanced toolset enables proactive threat detection and response, ensuring robust protection for our assets and stakeholders.

Our guiding principles

We operate within a dynamic environment. The way we stay ahead of change is by creating a resilient and adaptive organization that improves through measurable feedback and developing leaders that can execute at all levels of the organization.

Empowerment Culture

HealthEquity team members are our first line of defense against cyber attacks. This is why we invest in tools and training for security awareness, and why we have built a world-class risk and security organization.

Continuous Improvement

Managing cybersecurity, physical security, fraud, and privacy under one team is not just an administrative exercise. It means we combine the decision-making practices and lessons learned from each of these skillsets. And, apply industry best practice maturity frameworks like HIPAA Security, and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

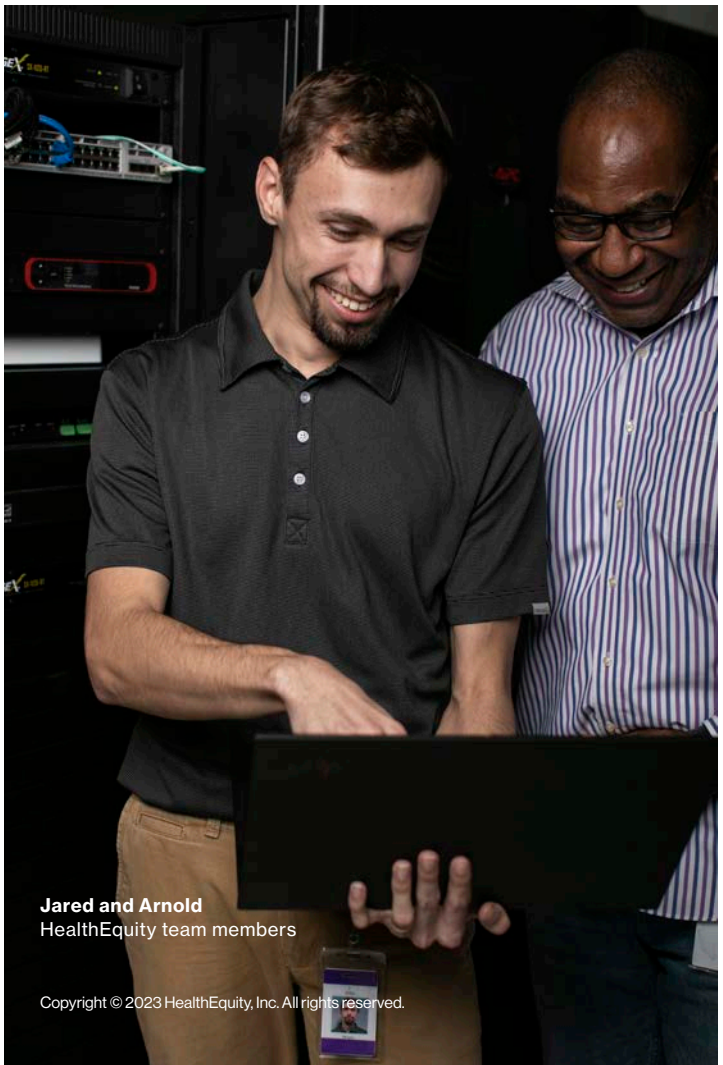
Measurable Operations

Setting targets and benchmarking ourselves against the industry allows us to continuously improve and optimize our efforts. This approach helps us stay ahead of security threats and deliver the best products and services to our customers.

Justin
HealthEquity
team member

Our Roadmap for Security

We take a strategic, risk-based approach to maturing our security program, emphasizing continuous improvement, enabling our business operations, and differentiating our business.



Jared and Arnold
HealthEquity team members

2021

Mastering the Fundamentals

Through 2021, HealthEquity continued modernizing its technology platforms and security program. We invested in security technologies, fraud prevention, and privacy using the NIST CSF as a maturity roadmap.

2022

Security at Scale

The HealthEquity cloud transformation continued with the acquisition of Luum and Further. Nearing our program maturity goals, our security focus evolved toward re-architecting best practices into a more scalable digital environment in multiple cloud environments.

2023+

Preparing for the Cyber Threats of Tomorrow

The threat landscape in 2023 will continue to evolve with an increase in nation-state cyber attacks, an expansion of hacktivism into new areas, and a resurgence of ransomware in new and more dangerous blended forms. To stay ahead, we're using a "Policy as Code" approach to enable more secure automation, collaboration, and faster code deployment while shifting left.

The 2023 Threat Landscape

The evolving threat landscape, driven by geopolitical and economic factors, has led to an increase in cybercrime globally. As worn-out scams lose effectiveness, cybercriminals are becoming more creative in their methods. In 2023, we expect to see a rise in business email attacks, malware and ransomware threats, and the emergence of cybercrime and scamming as a service.

Malware and Ransomware Threats

As the conflict in Ukraine continues and sanctions come into play, the rise in malware and ransomware attacks is expected to impact various sectors. Russian state-sponsored organized crime groups, known for their expertise in ransomware, will likely target not only US government agencies, defense contractors, and organizations supporting Ukraine's defense, but also a wide range of US businesses. The proliferation of ransomware toolkits to cybercrime actors will increase the threat landscape, with potential targets spanning the financial and healthcare sectors, among others.

Business Email Attacks

Scammers will employ business email compromise (BEC) tactics, impersonating trusted sources to manipulate recipients into transferring funds urgently. Payroll diversion scams and sophisticated impersonation techniques targeting mid-level employees are on the rise.

Cybercrime and Scamming as a Service

Underground virtual marketplaces will offer end-to-end services, enabling low-skilled threat actors to purchase stolen credentials, credit card numbers, phishing kits, malware, and other tools for various cybercrimes, leading to an increase in these services in 2023.

Rise of AI-Powered Attacks and Defenses

Cybercriminals will increasingly leverage AI and machine learning (ML) to launch sophisticated attacks. Using generative AI, cybercriminals can automate the first steps of an attack through content generation, improve business intelligence gathering, and speed up the detection rate at which both potential victims and business processes are compromised.

2023 Cyber Initiatives

Broadening our focus from Fraud Detection to Financial Crimes Prevention

In our ongoing commitment to robust security measures, we are expanding our focus to include financial crimes. This involves enhancing transaction monitoring to meet Anti-Money Laundering (AML) requirements, improving identity verification, and strengthening Office of Foreign Assets Control (OFAC) Sanctions screening. By incorporating behavioral telemetry, we gain valuable insights to detect and respond to suspicious activity. These measures aim to safeguard our customers' financial well-being and advance regulatory compliance.

Migrating to Azure Cloud: Unlocking Security and Business Benefits

In our pursuit of operational excellence and heightened security, we are embarking on a transformative journey to migrate our core platforms to the Azure cloud. This strategic move holds tremendous potential for our organization, providing a host of security and business benefits. By leveraging the power and scalability of Azure, a cloud-based platform from Microsoft*, we can enhance the protection of our systems and data and bolster our defense against evolving cyber threats. Additionally, the Azure cloud infrastructure offers robust built-in security features that ensure the confidentiality, integrity, and availability of our critical assets. Simultaneously, this migration will enable us to streamline our operations, optimize resource allocation, and drive cost efficiencies, empowering us to deliver even greater value to our clients and members.

Harnessing the Power of Generative AI: Transforming Enterprise Productivity with Microsoft-Enabled Tools

AI at the enterprise level can unlock new levels of productivity and creativity. With the support of Microsoft-enabled tools like M365 Copilot, coupled with robust built-in security measures and a strong governance framework, we are poised to harness the potential of this bleeding-edge technology while ensuring safety and security. By embracing generative AI, we can revolutionize our workflows, streamline complex tasks, and drive unprecedented levels of efficiency and innovation across our organization. This includes security applications where our analysts will be empowered with AI-enhanced tools to effectively detect and mitigate AI-based threats.

Sharon and Frank
HealthEquity team members

*HealthEquity and Microsoft are separate, unaffiliated companies and are not responsible for each other's policies or services.

The Converged Team

Our cross-functional team is staffed with subject-matter experts and leaders from each of these areas:

Cybersecurity

We follow a defense-in-depth security model with a Joint Security Operations Center (JSOC) and Data Protection team working with security architects and engineers deploying controls designed to prevent or limit the success of an attack.

People Safety and Crisis Management

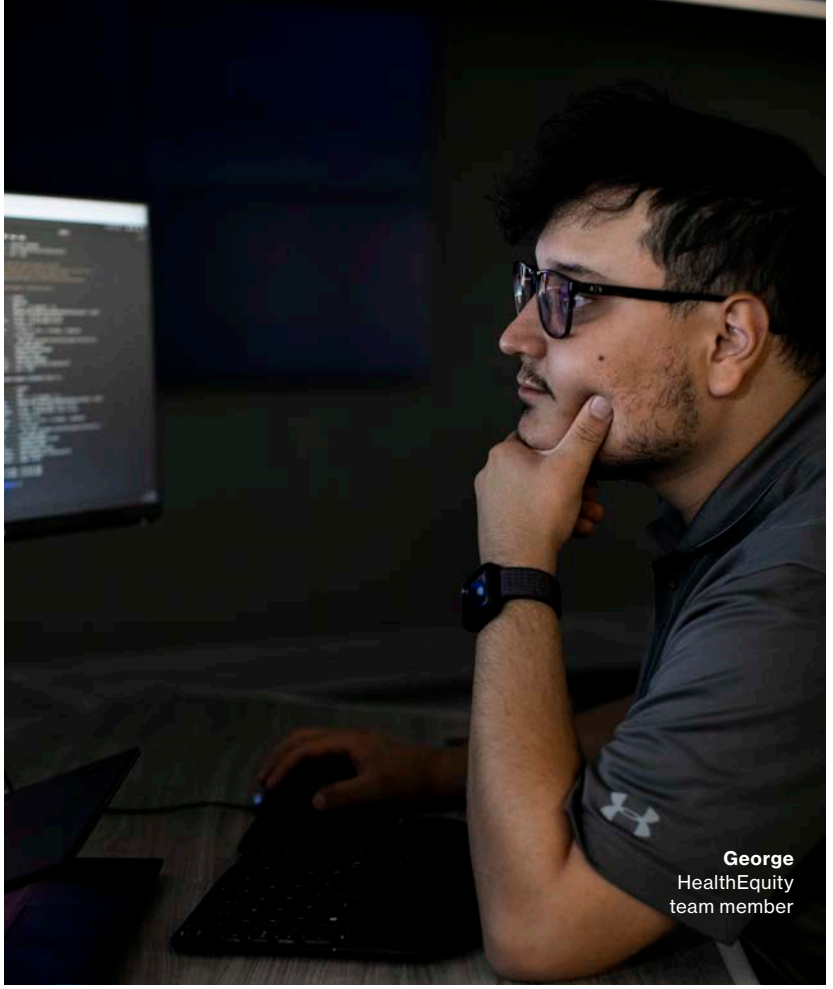
Led by federal law enforcement veterans, our People Safety team is responsible for ensuring the security of our 3,000+ team members across the US. We also conduct regular tabletop exercises to ensure business continuity in the event of a crisis situation.

Privacy

Our Data Privacy and Governance team is integrated with our technology teams to build a lasting roadmap that is focused on creating products, services, and standards with privacy by design, and consumer choice at the forefront.

Fraud Prevention

Our Fraud Strategy and Prevention team is leveraging the best practices of fraud prevention and cybersecurity monitoring to protect the transactions of our members and clients.



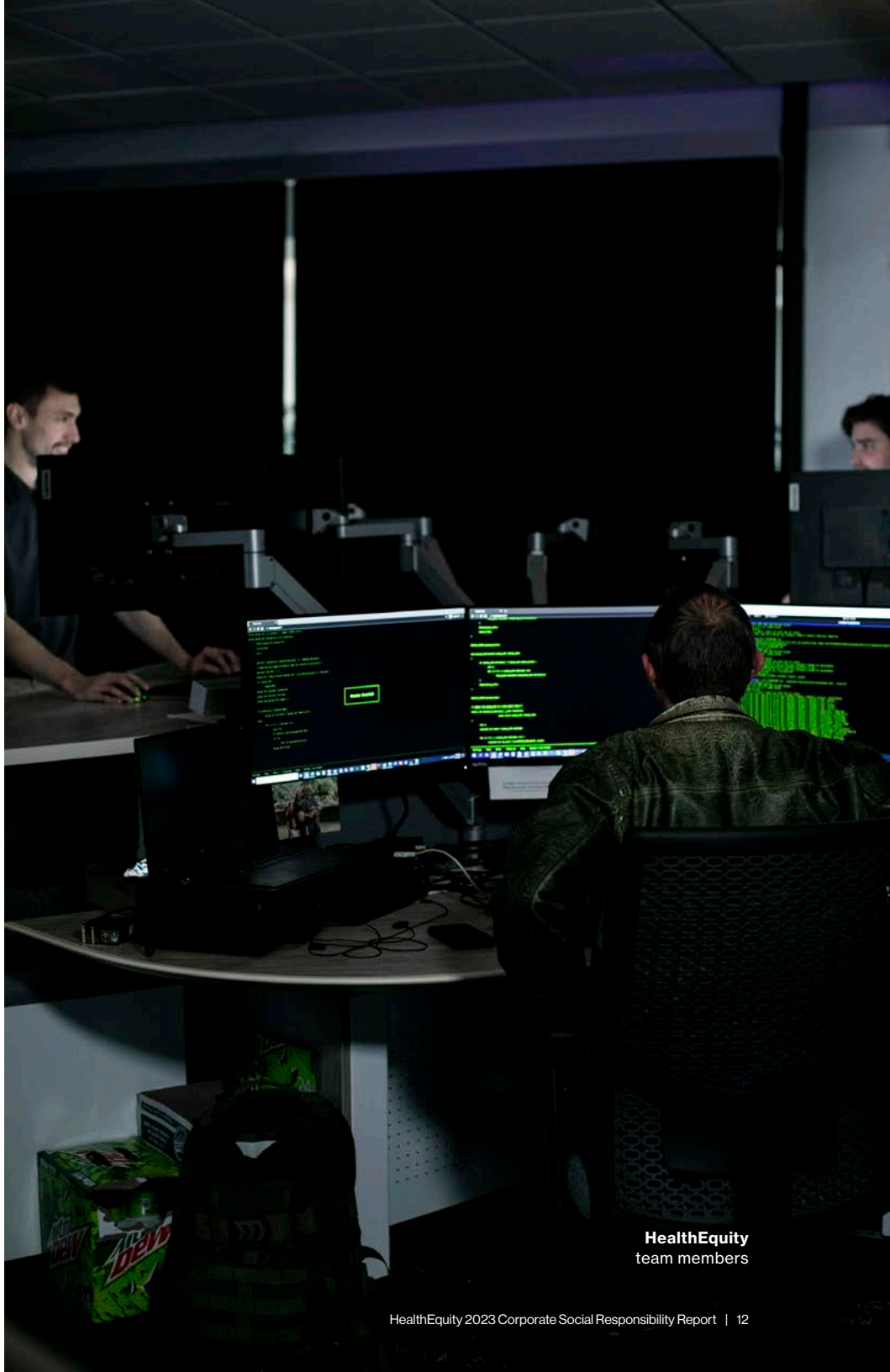
George
HealthEquity
team member

Three Lines of Defense

We have implemented the Three Lines of Defense model to effectively mitigate organizational risk. Our Security team serves as a first line of defense, closely working with our Enterprise Compliance function as a second line of defense, and Internal Audit as the third line of defense to guarantee that our members' data is secure and that we adhere to the highest industry standards.

Detailed Capabilities

- Statement on Standards for Attestation Engagements 18 (SSAE-18) and Service and Organization Controls (SOC 1 and 2) reports
- Encryption of sensitive data in transit and at rest
- Regular security audits by independent third parties
- Compliance with relevant industry regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Gramm-Leach-Bliley Act (GLBA)
- Cybersecurity insurance to protect against losses resulting from cyber attacks
- Robust incident response plan in place to handle security breaches
- State-of-the-art Joint Security Operations Center to detect and prevent unauthorized access
- Regular testing of disaster recovery and business continuity plans
- All employees complete Security and Awareness training annually
- Employment verification and criminal checks for US employees



HealthEquity
team members

HealthEquity®

Connecting health and wealth