To: Joint Committee on Information Management and Technology

Senator Aaron Woods, Co-Chair

Rep. Nancy Nathanson, Co-Chair

From: Boris Balacheff, Chief Technologist for System Security Research and Innovation, HP Inc

Dr. Paul Benning, Chief Technologist, Strategy & Incubation, HP Inc

Dr. Kimberlee Brannock, Cyber Security Strategist and Technologist, Professional Services, HP Inc

Date: February 15, 2023

Re: Testimony in support of Oregon HB 2049

Members of the Joint Committee on Information Management and Technology, thank you for the opportunity to submit written testimony in support of HB 2049 on behalf of HP Inc. HP, founded January 1, 1939, is a multinational information technology company headquartered in Palo Alto that continues to innovate and develop personal systems, print devices, including industrial presses and printing solutions, as well as 3D printing solutions, and associated managed and professional services. We have had a substantial presence in Corvallis, Oregon since 1977, with a major research, development, and manufacturing site; and we actively sponsor cybersecurity education in the great state of Oregon, through initiatives like the Oregon Research and Teaching Security Operations Center (ORTSOC) at Oregon State University (OSU)[1].

AN EVOLVING THREAT LANDSCAPE AND SHORTAGE OF CYBERSECURITY SKILLED WORKERS

To the continual advancement of and ever evolving digital technologies there has been a proportional development in their misuse. Daily, organizations face phishing, ransomware, malware, and other forms of cyberattacks and other cyber-events, including inadvertent mistakes and 'insider' threats. Oregon must face these challenges as these cyber events will continue. A few examples, by September 2021, 131 Data Breaches had been reported to the Oregon Department of Justice[2]. In 2022, nefarious actors used the city of Portland's email to trick employees into transferring $1.4M in taxpayer's money[3].

In this context, and due to the COVID-19 pandemic, hundreds of millions of employees around the world started working remotely and from home. What started as a way for organizations to continue to function, IT and cybersecurity teams needed to adapt to manage and secure fleets of endpoint devices, including computers and print devices spread out over geographies without the visibility of devices, how they are being used, nor by whom. This created greater cyber security risk and introduced new vulnerabilities. These vulnerabilities were exploited by attackers resulting in a 238% increase in global cyberattack[4] volume during the early days of the

[1] https://ortsoc.oregonstate.edu/

[2] https://www.doj.state.or.us/media-home/news-media-releases/oregon-data-breaches-rise-in-2021-oregon-ag-settles-with-cpa-firm/

[3] https://www.opb.org/article/2022/08/22/portland-oregon-lost-million-funds-cybersecurity-theft/

[4] https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/wolf-security-and-flexworker/2021_HP_Wolf_Security_Blurred_Lines_Report.pdf

COVID-19 pandemic. This remote work model has continued to evolve into a hybrid work model and is here to stay for the foreseeable future. Many organizations need to adapt to this new hybrid world of IT, where distributed teams are more common, and where agility to support remote and hybrid work is necessary.

The way people, processes and the ever-evolving technologies intersect, only brings about more cyber security challenges. This is because how we work and how we live is becoming all the more interconnected, with the virtual and physical worlds colliding and integrating more and more. In this context, the demand and expectation are growing for more automation, more agility, more scalability, and more ability to have ever-changing, versatility in all we do, and all of it increases the need for more advanced cybersecurity skills and capability to keep our digital infrastructures safe and resilient.

In this new environment the increased rate of cyber-attacks coupled with the behaviors resulting from remote work and hybrid work compound the cyber security risks that governments, companies, and individuals are exposed to every day[5]. Cyber-attacks will continue unabated, and our best path forward is to build for cyber resilience.

Beyond technology itself that has cybersecurity by design, a key component to achieve cyber resilience must be access to a large enough pool of skilled cybersecurity professionals. At this time, the number of cybersecurity related jobs already outpaces the number of people with the qualified cybersecurity skillset to fill the role, and the demand for a skilled cybersecurity workforce continues to grow. According to the (ISC)⍰, a non-profit specializing in training and certifications for cybersecurity professionals, in 2022 there was a global cybersecurity workforce gap of 3.4 million individuals, and a gap of 410,695 in the United States [6]. Per (ISC)^{2,} the cybersecurity workforce gap has grown more than twice as much as the cybersecurity workforce itself with a year-over-year increase of 26.2%[5]. Cybersecurity threats will not be effectively managed if there is not significant investment in growing a skilled cybersecurity workforce.

CYBER EDUCATION THROUGH THE OSU ORTSOC

The Oregon HB 2049 would help to address the noted cybersecurity workforce gap. Programs supported by this Bill, such as the Oregon Cybersecurity Center of Excellence would help oversee, coordinate, and fund cybersecurity education, awareness, and training for public, private, and nonprofit sectors, as well as cybersecurity workforce development which will collectively contribute towards closing the critical cybersecurity workforce and skills gap.

HP is already invested in this mission worldwide, and in Oregon specifically, where we expanded our long-established partnership with Oregon State University (OSU) to sponsoring the OSU ORTSOC .

The OSU ORTSOC aims to address the shortage of trained cybersecurity professionals while serving the cybersecurity needs of underserved entities — such as small local government agencies, K-12 schools, smaller higher education institutions, and nonprofit organizations — who struggle to meet their cybersecurity needs. Studies have shown that to best prepare students for careers in cybersecurity, experiential learning is key. HP believes the OSU ORTSOC is critical to be in a position to accelerate cybersecurity training in order to

[5] https://h20195.www2.hp.com/V2/GetPDF.aspx/4AA8-1111ENW.pdf

[6]https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

create and train a cybersecurity workforce for business and public organizations, including the cybersecurity roles with the great state of Oregon. The OSU ORTSOC can have tremendous positive impact on cybersecurity research and education at Oregon State University, while addressing the cybersecurity workforce and skills shortage in the region.

HP has long been invested in technology and education in Oregon. Another example in the field of cybersecurity is our longtime sponsorship and participation in Oregon's NW Cyber Camp, that you just heard from – a High School camp exposing students to careers in cybersecurity. We believe that this program focused on growing Oregon's cybersecurity workforce greatly deserves the financial support necessary to continue to grow, attract, and support a larger number of students across the great state of Oregon.

We believe in investing in the next generation of skilled cybersecurity workers. HP's investment in Oregon's cybersecurity training efforts to date, as well as our support of HB 2049 are a testament to our commitment to bridging the cybersecurity workforce and skills gap.

The passing of HB 2049 will underline and amplify the impactful activities that are already underway in Oregon and help to maximize our chances of successfully addressing the challenge we all face to build a cyber resilient future, which includes weaving more cybersecurity capability through everything we do in a more holistic end to end manner. Cybersecurity is also an important component to sustainability as outlined in the HP Sustainable Impact Report[7]. Sustainability of the great state of Oregon, sustainability of companies such as HP, of each of us and to our way of life has better odds when we provide cybersecurity education opportunities.

Thank you for the opportunity to submit testimony, on behalf of HP Inc., in support of HB 2049. It is an honor and privilege to do so.

Boris Balacheff

HP Fellow
Chief Technologist for System Security Research and Innovation, HP Inc
Advisory Board Member, ORTSOC, OSU

Dr. Kimberlee Brannock

Cyber Security Strategist and Cyber Security Technologist
Professional Services & WW Security and Analytics Practice, HP Inc
Cyber Security Advisory Board Member CWI & Marymount University

Dr. Paul Benning

HP Senior Fellow
Chief Technologist Strategy & Incubation3, HP Inc
Oregon Venture Fund Advisor

[7] https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=c08228880