HP Policy Position

Security, Privacy and Data Protection

1501 Page Mill Road
Palo Alto, CA 94304
hp.com

HP recognizes the fundamental importance of security, privacy and data protection. As our world becomes ever more connected, cyber attacks target critical and personal data with increasing frequency and sophistication. We design our devices with embedded cyber resilience, offering leading-edge features that enhance security to protect our customers' sensitive information. In addition to these security measures, our practices aim to provide the highest levels of privacy and data protection.

HP's Policy Recommendations

Security

- Even as overall awareness of cyber threats has grown, risks at the device level (computers and printers) are often overlooked. Both the public and private sectors should consider device security as part of their overall cyber risk assessments.

- Public sector procurement practices can mitigate device security risks by developing robust purchasing criteria that explicitly require device security. These security criteria are especially important for critical applications.

- Any cyber security legislation and regulations for commercial products should align with global standards. Geographic restrictions and country-specific technical standards are ineffective approaches to cyber security policies.

Privacy and Data Protection

- HP recognizes the fundamental importance of privacy, security and data protection to our customers and partners worldwide. We strive to go beyond legal minimums, and apply consistent global policies and procedures to safeguard personal information.

- In the EU, we are closely following the Article 29 Working Party (WP29) implementation of the General Data Protection Regulation (GDPR), and look forward to providing our comments and feedback to ensure that requirements align to the daily realities of implementing a successful privacy and data protection program.

- HP has been a long-time proponent of interoperability of various privacy regimes to ensure legal data flows. We are monitoring the review of the Privacy Shield, and encourage data protection authorities to continue working with the private sector to ensure global interoperability.

- Our privacy and government relations teams work with governments around the world to support robust and globally interoperable privacy and data protection regulations. We advocate for accountability-based requirements for both the public and private sectors.

Issue Background

Security

While most organizations are aware of the increased prevalence and risk of cyber attacks, typical response strategies are focused primarily on security software and data center protection, rather than device level security. At the endpoint hardware level (PCs and printers), attacks into a network can exploit low-level system vulnerabilities. Firmware attacks, those that take place in the embedded software (or BIOS) under the operating system, are a fast-growing attack vector. If an attacker penetrates device firmware, they could seize power over most device resources, including administration and control capabilities. Firmware attacks are difficult to detect because firmware is invisible to the operating system and traditional software security applications. In other words, firmware attacks provide the ability to monitor and remotely control all activities on the target device with perfect stealth.

Governments are on the front lines of the cyber threat landscape, and device vulnerabilities potentially could expose national security information and citizen data. To keep government systems and critical infrastructure safe from the most sophisticated attackers, we encourage heightened attention to device level security. Efforts to share cyber threat information between the public and private sectors should encompass the latest intelligence on device security threats, such as firmware attacks.

Establishing procurement requirements for PC/printer security, particularly when used for critical applications, can help mitigate device security risks. Specifically, requirements should include secure boot and update mechanisms for lowest-level firmware and operating systems, firmware intrusion detection, and firmware breach remediation and recovery. Establishing high security standards in public tenders could drive a virtuous circle of private sector investment in device security to compete for these tenders.

HP designs our products with cyber resilience in mind, delivering security protections in endpoint devices, as well as the ability to detect breaches, and recovery from any cyber attacks. Our systemic approach designs security into all layers of the product during development, not as an afterthought addition to a completed design. *HP Sure Start,* which comes at no additional cost in both HP PCs and printers, pushes the boundaries of device security to achieve resilience against cyber attacks on the integrity of low level BIOS firmware. For more information, please see HP's white paper, IT Security in the Public Sector: Strengthening Device Security.

At HP Labs, we conduct leading-edge research to develop new security technologies that help prevent attacks before they happen, detect penetration of existing defenses and ensure swift recovery should an attack occur, even at the lowest hardware or software levels. This allows us to deliver unique security capabilities into PCs and printers, but also to design such capabilities for a world of new technologies across the Internet of Things and emerging cyber-physical systems.

As cyber threats are on the rise around the world, we recognize the interest of policymakers to enact legislation and regulations. Since these cyber threats rapidly evolve and technology must be flexible to anticipate these attacks, we encourage any cyber security measures for commercial products align with global standards, and discourage geographic-based restrictions on components/products and country-specific technical standards as ineffective cyber security policies that do not recognize the global nature of the technology supply chain.

Privacy and Data Protection

Our privacy strategy is based on providing transparency and choice for HP customers worldwide. We follow internationally recognized privacy principles in all of our operations, often exceeding legal minimums. Our privacy guidelines are communicated to our HP employees on an annual basis as part of our mandatory Standards of Business Conduct training and additional privacy training is required depending on employee job function.

HP is one of only a handful of companies to successfully obtain multiple privacy recognitions/certifications, including Privacy Shield, Binding Corporate Rules (BCRs), and APEC Cross Border Privacy Rules (CBPR). We are actively working to implement the EU GDPR requirements to our accountability-based global privacy program. We will share our expertise and experience with the WP29 and the Commission to ensure a smooth implementation of GDPR requirements, as well as interoperability of the review of Privacy Shield.

We work with government agencies, lawmakers, regulators, nongovernmental organizations (NGOs), and industry groups to encourage a more unified and robust approach to privacy and data protection regulations worldwide. Our Privacy Office oversees client customer and employee data protection, and shares best practices with peers, governments, and other stakeholders.

As people start to interact with technology in ever-changing ways, such as through the Internet of Things, wearables, and immersive computing, HP will continue to develop inventive tools that protect people's privacy in these new environments.