Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304

hp.com

HP Policy Position

Cyber Security

Background

The increasing volume of cyber security threats and risks faced by consumers, enterprises, and governments alike has ushered in a new era in which policymakers are increasingly seeking to address the issue through legislation and regulation. Through international standards development, HP is committed to enhancing defenses against the many and evolving cyber threats to governments, individuals, commerce, and critical global infrastructure. HP also invests significant resources in ground-breaking research into cyber threats and the best practices to identify, mitigate, and address such threats.

Security Challenges of the Cloud and Mobile Computing

Cyber threats are evolving in light of the rapid expansion and pervasiveness of cloud, mobile computing, and social media. Cloud-based computing presents new security challenges, as providers and users alike strive to ensure compliance, privacy, and both data and transaction integrity, while using the cloud's many innovative features and efficiencies.

Data is exploding and becoming increasingly mobile, necessitating that laptops, tablets, smartphones, printers, and other devices incorporate data security options. Enterprises and governments are contending with employees accessing work systems from numerous devices and locations, which presents security challenges, including controlling network access, confirming identity, and administering application permissions.

Global Collaboration to Enhance Cyber Security

Cyber security threats, protections, and solutions tend to be global in nature and must be addressed as such in order to ensure a more secure global IT ecosystem. HP participates in a wide range of activities around the world, sponsored by commercial, governmental, and academic institutions, to develop technical standards for IT, in general, and cyber security.

HP signed onto the World Economic Forum's Principles for Cyber Resilience ("WEF Principles"), a multi-stakeholder initiative, derived from dialogue across multiple regions and sectors and intended to help improve systemic resilience to cyber risks. The initiative takes an "act locally, think globally" approach by focusing on the improvement of the local cyber resilience of individual organizations. Through coordination on common principles, these local actions create global benefits by leveraging the effectiveness of individual organizations' actions into a cohesive community of cyber resilience. Through this initiative, HP has joined forces with more than 80 companies and government bodies across 15 sectors and 25 countries, each recognizing the interdependence of private and public sector organizations, mitigating cyber security risks at both the national and global levels, and committing to play a role in providing a resilient digital environment.

The WEF initiative changes the conversation around resilience to cyber risks from a narrow technical specialization to a topic of core strategic concern for chief executives, government leaders, and policymakers worldwide. Widespread adoption of the WEF Principles will help raise business standards associated with hyper-connected information systems across the world. Signatories are particularly keen to link the issue of cyber resilience and the need to provide a trusted online environment for interaction among individuals and organizations with the opportunities that ICT connectivity enables in terms of economic stability, growth, prosperity, and innovation.

HP's Leadership in Cyber Security Research and Technology

HP undertakes and commissions detailed research to understand and assess the cyber risk landscape. Since 2009, HP has issued a bi-annual Cybersecurity Risks Report.[1] The latest report, published in April 2012, reveals a significant increase in the activity of "hacktivist" groups like Anonymous.[2] In addition, HP recently commissioned the Ponemon Institute's 2012 Cost of Cybercrime Study, which found that the average annualized cost of cyber crime incurred by a benchmark sample of U.S. organizations was $8.9 million, which represents 6% and 38% increases from 2011 and 2010, respectively. The study also revealed a 42% increase in the number of cyber attacks, with organizations experiencing an average of 102 successful attacks per week, compared to 72 and 50 attacks per week in 2011 and 2010, respectively. HP has commissioned similar reports on cyber crime – with similar results – in the United Kingdom, Germany, Australia, and Japan.

Information analytics, discerning meaningful information from "big data" sets, hold the potential to unlock key findings and trends in cyber security, as well as financial fraud. Information analytics can provide the tools to detect anomalies such as cyber attack attempts. HP's Security Intelligence and Risk Management platforms, including ArcSight, are protecting cyber infrastructure for business and government clients around the world.

HP Labs – the company's research and develop arm – is leading major new research that addresses how cloud service providers use and protect personal and confidential information in the cloud. HP's TrustCloud project addresses key issues and challenges in achieving a trusted cloud environment. In addition, under the Dynamic Defense research project, HP Labs is also tackling the application security problem by developing technologies that present a constantly changing surface to attackers, thus limiting their ability to detect and exploit vulnerabilities.

HP's Policy Recommendations

HP supports positive efforts by government to enhance defenses against the many and evolving cyber threats to individuals, commerce, and the critical infrastructure that is the underpinning of the global economy. HP participates in global efforts – academic, technical, and governmental – to develop international standards for cyber security policy, legislation, and regulation. HP encourages policymakers, legislators, and regulators to take into account the following basic principles in addressing cyber security:

International Standards Development

- HP supports international cooperation and convergence in standards development because as with the Internet itself, cyber security threats, protections, and solutions tend to be global in nature and must be addressed as such in order to create a more secure global IT ecosystem. Establishing international standards also recognizes the reality of the international operating

[1] Reports *available at* http://www.hpenterprisesecurity.com/news/resource-center/.
[2] Report *available at* http://www.hpenterprisesecurity.com/news/download/2011-top-cyber-security-risks-report.

environment of multinational companies like HP. Governments should avoid imposition of unique technical standards and forced transfer of IP in addressing cybersecurity concerns.

Outcomes-Based Approach to Legislation and Regulation

- HP urges governments to adopt outcomes-based approaches to cyber security legislation and regulation that sets forth clear expectations for what an organization is expected to achieve with respect to cyber security, versus the manner in which the organization should achieve it. HP supports initiatives for business and government to share best practices.

- Governments should reject "one-size-fits-all," legislatively-mandated requirements or best practices for cyber security, particularly since such requirements could be subject to narrow interpretation and codification in agency regulations.

- A flexible, outcomes-based approach will help ensure that, as technology and threats change, organizations can evolve to best address the entity-specific cyber security risks and profile of their particular organization.

Adequate Defenses, Protections, and Immunities

- In crafting cyber security legislation, HP urges policymakers to incorporate adequate defenses, protections, and immunity from liability for regulated or covered entities. HP also advocates for governments to ensure the protection of confidential information shared with government – or industry – as part of cyber security regulation, reporting, threat assessments, or otherwise.

Government-Conducted Risk Assessments to Understand National Cyber Vulnerabilities

- In designing and conducting risk assessments to understand national cyber vulnerabilities, HP advocates for comprehensive risk assessment programs that focus on an organization's overall capacity and its current program for ensuring appropriate cyber security controls, rather than on identifying specific threats. Such a program should include procedures and processes to continually monitor for threats and vulnerabilities, and isolate and resolve issues once identified. In addition, HP urges policymakers to design assessment programs that:

    - Protect the very sensitive information that results from the assessment, as disclosure of such information could provide a roadmap to vulnerabilities in both industry and government;

    - Define how regulators will use the information once a vulnerability is recognized and, in so doing, mitigate further the risk of disclosure of that information; and

    - Provide clarity on whether the risk assessment would be expected to extend beyond the entity being assessed to its sub-contractors, supply chain partners, and others.

Definition of Critical Cyber Infrastructure

- Policymakers should carefully define critical cyber infrastructure for threat assessments, regulation, and reporting requirements, or other purposes. Any such definition should be narrowly crafted to avoid unnecessary assessments at a high cost compared to the benefits, conflicts with privacy protections, and burdensome regulations that could hinder companies like HP that compete in a global marketplace.

- HP urges policymakers to provide clarity on whether critical cyber infrastructure would extend to a covered entity's sub-contractors, supply chain partners, and others. HP encourages policymakers to adopt an outcomes-based approach with respect to assessments and definitions of critical cyber infrastructure.

Reporting of Cyber Breaches/Crimes

- HP advocates for public policies and legislation that encourage – but do not require – the reporting of cyber incidents appearing to have a criminal nature or component to law enforcement authorities. Any such requirements should be coupled with effective and proportionate criminal sanctions that deter the commission of cybercrimes.

- As a necessary prerequisite to mandating reporting requirements, policymakers and legislators should ensure that law enforcement is properly trained and equipped to understand, evaluate, and act upon the information received. Continuous investment in the ability of law enforcement to keep up with technological developments and advancements and changes in the security landscape is crucial for a reporting mechanism to achieve tangible results.