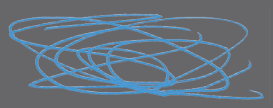
INNOVATION JOURNAL

CYBER-SECURITY SPECIAL EDITION

Keeping our customers, their data and business secure is at the center of everything we do at HP. This special edition of the HP Innovation Journal highlights the growing cybersecurity threats facing businesses and individuals around the world, and the amazing innovations being pioneered by our pan-HP teams to thwart these attacks. We explore the shape-shifting cybersecurity landscape and HP's focus on the frontline—creating robust endpoint device security solutions. From personal computers to printers and mobile phones, connected devices that house valuable data are seeing an increasing amount of cyber attacks and represent a great risk to enterprise security. Through innovation, employee and partner collaboration, and training, HP is at the forefront to stop cyber attacks before they occur.



THIS ISSUE HAS BEEN SPONSORED BY THE HP SECURITY LAB IN COLLABORATION WITH HP'S PERSONAL SYSTEMS, PRINT AND CHANNEL SECURITY TEAMS.

MEI JIANG
Editor-in-Chief

CHANDRAKANT PATEL
Managing Editor

DOUG WARNER
Executive Editor

Contributors
SHIVAUN ALBRIGHT
VALI ALI
BORIS BALACHEFF
LORRI JEFFERSON
THOMAS JENSEN
JIVKO KIROV
JIM MANN
CHRISTOPH SCHELL
SIMON SHIU
GAGAN SINGH

CONTENTS

Innovating in Endpoint Security:

BORIS BALACHEFF
Chief Technologist for Security
Research & Innovation, HP

SIMON SHIU
Head of Security Lab, HP Labs

CYBER RESILIENCE AT THE ENTERPRISE EDGE

One of the greatest challenges to protecting a business against cybercrime is the shape-shifting nature of security threats. Innovation is not the sole domain of the good guys: cyber criminals are constantly finding ingenious new ways to tunnel into consumer, enterprise and institutional IT systems. They are increasingly professional, more aggressively funded, and better-equipped than ever to exploit any weak link in the security chain.

With everything connected and interconnected, security is more important than ever. The rampant rise in cybercrimes—over 1700 significant data breaches[1] in 2016 alone—is driving cybercrime costs in the global economy, with estimates reaching up to $600 billion for 2018[2]. The damage to businesses from theft of intellectual property alone exceeded $160 billion[3] in losses. Cybersecurity is now a truly disruptive force. If you have the security you need, your business runs without incident and stays out of the news. But if not—the damage to your operations and reputation can be devastating.

In order to stay ahead of attackers, we need to always be on the lookout for emerging and future trends in the threat landscape. To this end, we recently announced a new HP Security Advisory Board, a trio of outside experts with unique firsthand expertise in the world of hacking and the latest developments in security technology and strategies.

In fact, business leaders, well-versed in this negative narrative, will spend more than $90 billion[4] on security in 2018 alone to protect their organizations.

In this escalating threat landscape, endpoint devices are on the frontline. From healthcare to manufacturing, from transportation to the home, from agriculture to critical utility infrastructures, endpoint devices are the first line of defense or vulnerability for the data and resources we care about. They are the interface between the physical and digital world, and a prime target for cyber-attacks today, and likely will be for years to come. One example of the worsening threat landscape: we have been seeing a rise in firmware attacks, which are attacks on the software embedded in hardware that can provide an attacker with control over an entire system and which are undetectable by any security software.

Even more worrisome, we are seeing an accelerating trend in destructive attacks that target low-level firmware to disable hardware devices and render them inoperable on a large scale. This is key to understand, as attacker motivations should also drive how we think about defensive strategies. For example, the perpetrators of the biggest attacks of the last year were not just going after information, theft or ransom. They also sought to wreak destructive havoc on infrastructure. Worse still, they sometimes succeeded in both efforts. Last year's suite of so-called ransomware attacks, from WannaCry to NotPetya, were clearly aiming to cause destruction over financial extortion. Most important these attacks created a lot of "collateral damage," hitting organizations indiscriminately, making them truly destructive at scale.

To address this degrading threat environment, and new styles of attacks and attacker motivations, HP has been leading the industry in designing systems and devices with security built-in from the hardware up, to help protect, detect and remediate attacks, with minimal interruption to users.

We call this "design for cyber-resilience:" designing hardware-enforced security from the lowest level of firmware of an endpoint device and working up through the software stack and even management solutions. Design for cyber-resilience is meant to ensure that devices are not only built with protections but that they can reliably detect successful attacks and recover from them. This is the approach that we have been developing at HP Labs, which is guiding us in the design of our business devices, from PCs to printers. The strategy is to not only offer state-of-the-art protections built in from the hardware up, but to include hardware-enforced detection capabilities, and the ability to recover to a good state when successful attacks occur.

Software and network security are not enough anymore to protect endpoints across an organization, we have to start from designing for security from hardware up. This means that today choosing a device is a security decision. Requiring any hardware purchase decision, be it a PC, a printer or any other IoT device, to be recognized as a security decision, ensuring standards are met, and even exceeded with state-of-the-art security that will help address threats over the many years that the hardware will be deployed and in use.

In today's threat landscape, choosing a hardware device is clearly becoming a security decision. For too long, organizations have relied on third-party software security products to protect their devices. With hackers now able to frequently bypass traditional network perimeter security and antivirus programs on endpoints, it's time we consider the security of the hardware we purchase as closely as our software and network security solutions. This means that anyone who makes a hardware purchasing decision—however small or large—will have an influence on the security posture of the business for years to come. The enterprise CISO, who usually looks after the security of operations primarily, needs to start getting involved much earlier at the IT equipment and hardware procurement step: setting security requirements and making sure that security is taken into account as a key parameter of the purchasing decision.

Beyond the security of the devices themselves, the endpoint security challenge for organizations lies with security management. Organizations need to keep all the devices on their network up to date with the latest software and firmware, and in compliance with a good security configuration policy. In addition, they need to deploy, manage and monitor security software that's appropriate to their business needs. To protect the business over the long run, they critically need to have a data and device recovery strategy, ensuring that they can bring the infrastructure and the business back up and running when things go wrong; as they will.

To top the list of challenges organizations are facing, the cybersecurity talent pool is in tension, with a lack of available expertise that is making it difficult for organizations to hire, afford, and retain security talent, let alone specialists in device security, PC firmware, or printer or other IoT configuration management. This has led HP to invest in building up a security practice, to be able to consult with customers with device security assessments, for any device, PC or printer, HP and non-HP, and to help them put in place the right manageability tools and solutions, and ongoing compliance and security management strategies to keep the business a step ahead of the bad guys.

HP has been a leader in endpoint device security for over two decades, pioneering research, driving security standards with industry partners, and raising the bar of personal computer and print security, with many industry firsts. But this is only the beginning. Moving forward, HP will strive to continually deliver the most secure devices, along with the solutions and services to help our customers use them securely. We are committed to leading security innovation and driving the entire industry forward.

LOOKING AHEAD: HP'S APPROACH TO SECURITY RESEARCH

If personal devices and 2D printers are the dominant endpoint devices today, it won't be long before they are joined by technologies that further fuse our physical and digital worlds, like 3D printing, augmented reality, and sensors that monitor everything from the weather to health data and traffic patterns.

As devices sense, actuate, collect data from, and work to change or configure the physical world, the security of endpoints and their ecosystems will only become more critical to any organization's cybersecurity.

The threat landscape will get worse. Nation states and criminal organizations with huge resources are creating increasingly sophisticated attacks, and the efficiencies of the internet and the underground economy means this sophistication is very quickly available to a larger set of attackers with diverse motivations—it is clearly a case of when—not if—you will be attacked.

In the future, cyber events could compromise millions, or even billions of cyber-physical devices at once, whether to manipulate their behavior or even disable them altogether. As we consider this in the context of digital manufacturing where products are manufactured on the 3D printer nearest the end customer, in the context of computing for personalized healthcare, or more broadly in the context of artificial intelligence and machine learning being built into devices to support autonomous behaviors, we believe that security innovation will be key to address emerging threats and rise to the challenge of assuring the safety of our cyber-physical future.

This is why, at HP, we are investing in long-term research in cyber-security. We are pursuing, for example, the security innovations needed to allow 3D printing technology to revolutionize manufacturing. These range from cybersecurity research for our 3D printers themselves, to researching the design of secure workflow capabilities that ensure key security properties are retained in digital designs until they become physically printed objects. This will be key to ensuring that the physical and mechanical properties of a 3D-printed part can be trusted within a securely digitized distributed manufacturing ecosystem.

Moreover, security will be an enabler for other cyber-physical scenarios such as collaboration in the office of the future, or personalized healthcare. We need to make interactions safe and seamless for users, and manageable for corporations and administrators. A simple example is authentication where we are working to move beyond passwords and allow for seamless but reliable authentication user experiences, with appropriate levels of security and assurance over privacy.

The trustworthiness of tomorrow's infrastructure will critically depend on the resilience of endpoint devices to cyber attacks. After twenty years in device security research leadership we continue to pursue security innovation to help build-in further security assurances into hardware, creating devices that can help detect and isolate breaches, and recover from them, all at considerable scale, and with minimum inconvenience to the user. Critically we pursue research into improving operational security management techniques to allow our customers to maintain control over an increasingly large number of devices, data, and their interactions, at a reasonable cost and with the best security assurances possible.

Importantly, we work hard to keep abreast of the fast-evolving threat environment. We do this in multiple ways, from engaging with other experts across academia, governments, and industry, and with HP's own Security Advisory Board. But we also operate our own Attack and Malware Lab, an isolated environment we use to investigate the state of the art in malicious software and attack capabilities. This allows our teams to experiment with malware in a contained environment, better understand our adversaries, and test our research approaches to detecting, mitigating, or managing infrastructure recovery from real-world attacks.

At HP's Security Lab we pursue long-term research, working closely with HP businesses to ensure we can deliver cybersecurity innovations into HP products, services, and solutions, that will truly help improve security and minimize the cost of operation and ease of use for individuals and corporations alike. Our work takes us beyond HP into global standards organizations and into collaborations with industrial and academic partners, as well as leading customers, with whom we must join forces to advance the cybersecurity state of the art and move our industry forward towards a safer, more resilient future.

1. 2016 Breach Level index, Gemalto 2. "Economic Impact of Cybercrime," McAfee, February 2018 3. CSIS Cybercrime Report, June 2014 4. Forecast Analysis Information Security, Worldwide, 1Q17 Update, Gartner (Elizabeth Kim, Christian Canales, Ruggero Contu, Sid Deshpande, Lawrence Pingree), June 2017

Security Advisory Board Interview

For decades, hackers fell squarely into two camps: "black hats"—initially in it to show off their skills and then later, for money, espionage and data theft—and "white hats," who breached systems to uncover flaws before the bad guys could find them and ensured that companies promptly fixed them.

More recently, destruction for destruction's sake has become a new hallmark of the global cyber-threat landscape. The foremost examples of this were the ransomware and destructive malware attack campaigns we saw in 2017 (Wannacry, Petya, NoPetya...) that rendered computers unusable all over the globe before the devastation was halted. With malicious actors everywhere looking for any vulnerability to exploit, one key to surviving the constant escalation of threats is to keep reinventing how we stay ahead of the game.

This is a challenge to which HP continues to rise, investing in security innovation and research, and leading the industry by constantly raising the state of the art in endpoint security across our portfolio. More recently, we took an extra step by setting up our own Security Advisory Board, bringing a trio of outside security experts inside the company to work with our own security technologists and strategists. The advisory board will help us be the sharpest we can be about what the future holds: understanding the threat landscape today and being able to address the real problems of tomorrow. All three board members have unique first-hand experience in the world of hacking, with a background that spans offensive and defensive security, with a view of both operational and R&D security challenges.

This new board builds on HP's 20 years of leadership in cybersecurity. As the world's largest PC manufacturer and leading maker of printers, HP has driven a slew of security innovations, from technology that provides cryptographically secure updates of a device's BIOS to run-time intrusion detection, which checks for anomalies and automatically reboots when an intrusion is detected.

Today we invited our board members to talk to the *Innovation Journal* about their experience.

> "YOU RECENTLY JOINED OUR NEW SECURITY ADVISORY BOARD, AT A TIME WHEN CYBER SECURITY IS CLEARLY TOP OF MIND FOR OUR CUSTOMERS. WHAT MOTIVATES YOU TO HELP ADVISE HP ON OUR CURRENT AND FUTURE SECURITY STRATEGY AND ON OUR ROLE IN HELPING CUSTOMERS NAVIGATE THE THREAT LANDSCAPE?"

MICHAEL CALCE

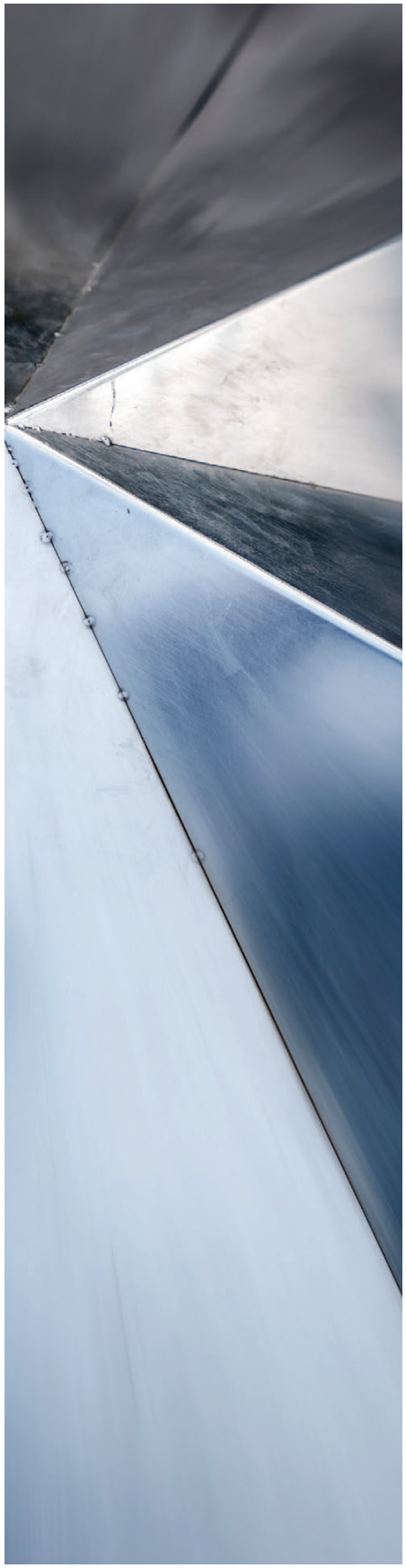
Having worked with HP to consult and educate on the cyber-threat landscape, I was excited to help set up a new HP Security Advisory Board to take things to the next level. I was inspired by HP's commitment to look at different angles to create more secure products. Helping to establish and chair this board was a natural fit for me and enables all of us to team up and advocate how to improve security together. The board is not a symbolic gesture, there is no smoke and mirrors here. The members I assembled are there to offer the best advice and input that we possibly can for HP, to really help develop the most secure products that will impact the world and address a degrading threat landscape.

ROBERT MASSE

When initially approached to join the Security Advisory Board, I immediately saw the potential to assist one of the largest PC and print manufacturers in the world to make a real impact and help reduce the threat surface. As you know, attackers are placing a major emphasis on compromising endpoints as the weakest link in most corporate environments and HP has very interesting technology and a roadmap that will help organizations and individuals really improve their security posture. As an example, HP's focus on helping organizations achieve cyber-resilience with technologies like HP Sure Start definitely resonates with the need I am seeing in the world right now.

JUSTINE BONE

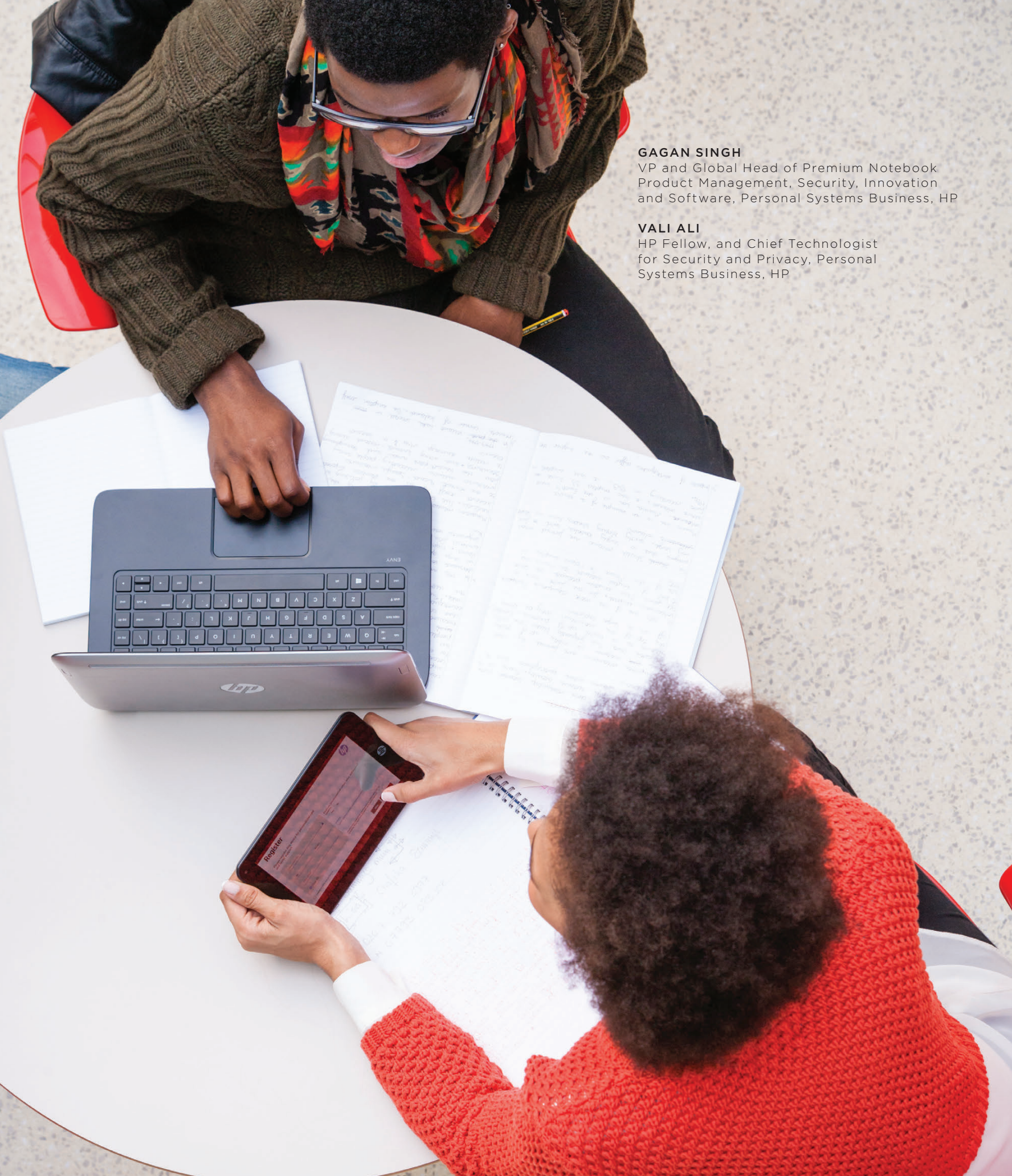
For years, software and hardware makers were able to rely on security by obscurity. There was no upside to building in this quality all the way through the product, because nobody was asking questions. Now, though, people are definitely asking, and it is time for the leadership HP is providing. HP's in-depth investment in security is a testament to the company's ongoing commitment to building quality solutions. It's an honor to be bringing an outside perspective to this initiative as HP continues to assess the threat landscape and prioritize security across product lines.



MICHAEL CALCE, *CEO of Optimal Secure, is HP's Security Advisory Board chairman. Michael became publicly known as "Mafiaboy" when in 2000 at the age of 15 he unleashed a massive cyberattack that brought down Yahoo!, eBay, and Amazon. It led to an FBI manhunt and $1.7 billion in economic fallout. Since then Michael has reformed and has been making a career in cybersecurity consulting and education on the threat landscape. He is the award-winning author of the book Mafiaboy: How I cracked the internet and why it's still broken.*

ROBERT MASSE *is a national partner in the cybersecurity practice. With over 20 years of experience, he's built a reputation as a pragmatic security executive.*

JUSTINE BONE *is the CEO of MedSec, a company specialized in cybersecurity for medical devices and the healthcare domain. She began her career doing reverse engineering and vulnerability research at New Zealand's version of the U.S. National Security Agency before running her own ethical hacking company for a few years. She also has experience as a CISO for companies like Bloomberg L.P. and Dow Jones.*



GAGAN SINGH
VP and Global Head of Premium Notebook Product Management, Security, Innovation and Software, Personal Systems Business, HP

VALI ALI
HP Fellow, and Chief Technologist for Security and Privacy, Personal Systems Business, HP

STAYING A STEP AHEAD OF THE BAD GUYS IN TOMORROW'S WORKPLACE

Today's work/life style is connected, connecting, and converged. With 62 percent[1] of employees working regularly from more than one location. 65 percent[2] of workers say they collaborate multiple times a day. 81 percent[3] report that work activities happen during personal time. And perhaps not surprisingly, entertainment activities on work personal computers (PCs) have doubled. These trends are bound to continue; the workforce will be 50 percent[4] millennials by 2020, and 88 percent[5] of millennials report wanting this work/life integration.

As remote work and collaboration solutions have become more productive and mainstream, physical environments are evolving to maximize the interaction and immediacy an office space can and should provide, including:

- agile workspaces designed for individual productivity
- informal meeting areas encouraging co-creation and conversation
- interactive conference rooms providing efficient and technology-enabled meetings and collaboration.
- integrated communal spaces to encourage socializing, recreation and wellness: the comforts of home migrating into the workplace, perhaps, in our increasingly connected world.

It's clear that traditional boundaries are dissolving, and the "Office of the Future" spans across work and the rest of our lives. Security must evolve and keep pace.

Dramatic changes have taken place in where, when, and how people are working, and those changes will continue to

transform our personal and work environments. The modern office is evolving in keeping with patterns and trends emerging among workers. The physical buildings and firewalls that reliably kept people and assets safely inside, and security threats outside, are being transformed by an altogether more porous and flexible workspace often described as "anytime, anywhere."

Securing a vibrant, mobilized, distributed workplace is more challenging, and more critical, than ever before. It is a challenge that has consistently driven HP's long history of industry leadership in driving security innovation and standards. We produce some of the world's most secure and manageable personal systems and printers today, and our drive to improve security across the spectrum of devices never rests. We're designing systems and devices for cyber-resilience, with security built in from the ground up, to help protect, detect and remediate attacks—with minimal interruption to users. We keep reinventing security to always better meet the needs of the changing workplace—today's and tomorrow's. This means designing security from the very ground up, right into the hardware of our device: from HP SureStart, the industry's first self-healing BIOS; to HP Sure View, the world's only integrated privacy screen to protect against visual hacking; or HP Sure Click to contain phishing attacks

This year we announced, yet again, industry-leading security innovation. The new HP EliteBook 800 Series G5 features innovations like HP Sure Run, extending hardware-enforced self-healing to critical security software and processes; as well as HP Sure Recover, introducing the first truly hardware-based secure automated network-based recovery of an entire operating system, ensuring robust and reliable recovery at machine speed in the face of modern destructive attacks.

As the saying goes: if you're not moving forward, you're falling behind. Nowhere is this truer than in the work of locking out intruders, locking down data, and delivering a positive and empowering work experience that frees workers to innovate, be curious, and be productive, confident that their business and data remains secure and resilient in the face of growing cyber threats.

Old-school security solutions were designed *by* IT workers, *for* IT workers. Today, security must be designed with the modern workforce in mind. Security solutions are enabled by powerful and complex technology—but they must be easy enough for IT admins to deploy and manage, and for the end user to navigate and embrace.

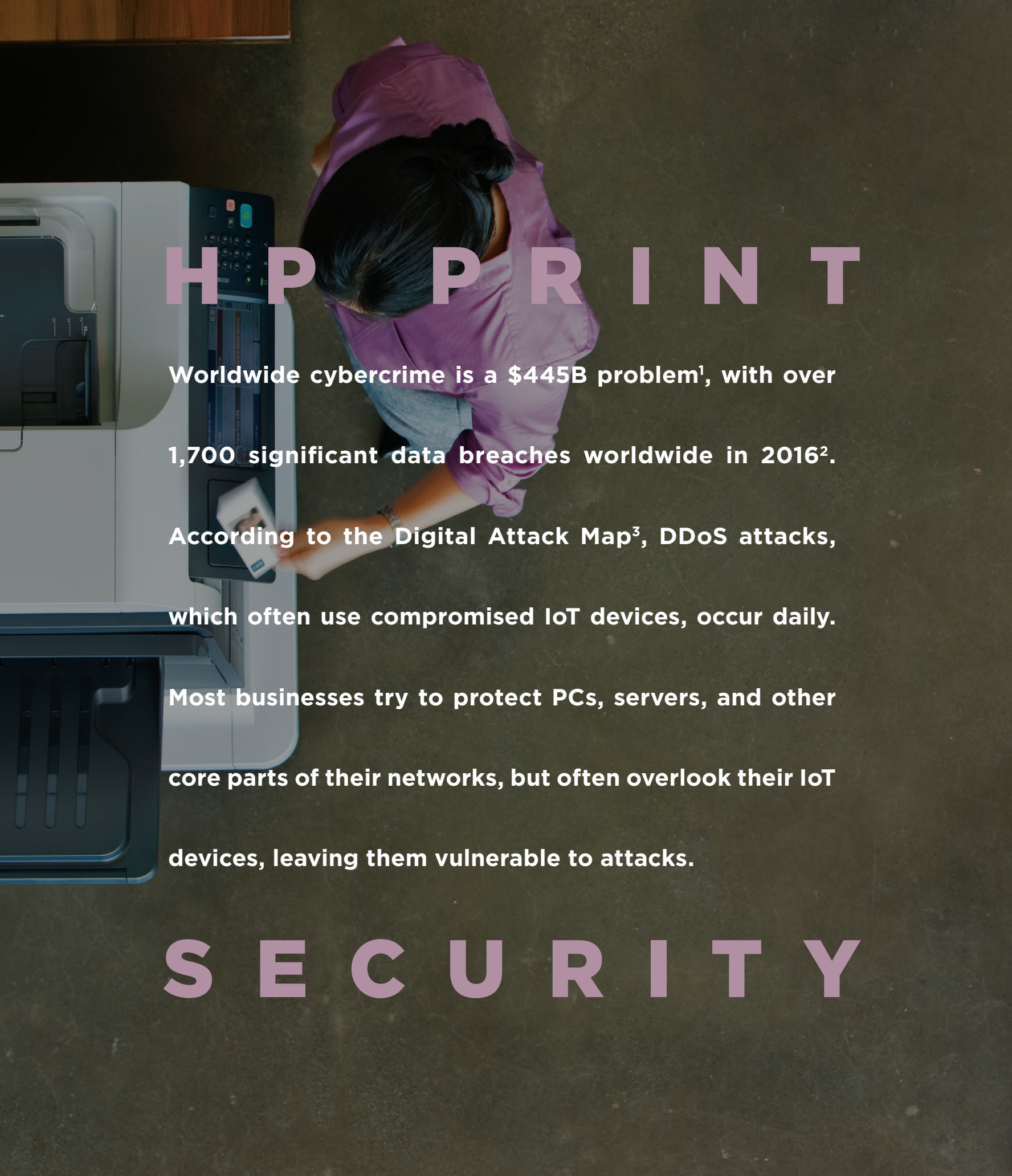
But the need for change in our approach to security goes further. Organizations tend to think about cyber security as an operational problem, which is to be addressed by deploying and managing the right software and network tools in their environment. Yet in today's threat landscape **choosing a device is already a security decision.** Hardware provides the foundation and ground-level security that is increasingly critical to any operating system, software security solutions, and robust recovery on and around endpoints. And endpoint devices are on the frontline of the cyber security battleground, where attackers target both end-user behaviors, and unprotected device hardware and firmware.

In order to stay ahead of attackers, we need to always be on the lookout for emerging and future trends in the threat landscape. To this end, we have been investing in security research at HP Labs for over two decades. Recently we also announced our new HP Security Advisory Board, where a trio of outside experts, with unique firsthand expertise in the world of hacking and the latest developments in security technology and strategies, join our internal chief technologists and lead strategists for cyber security to help us be the smartest we can about the future of the threat landscape. *See the Security Advisory Board story to learn more about this organization and their vision for tackling cyber security.*

At HP, our security strategy is informed by understanding how people work and studying how they use devices. Whether a business's employees are logging in on personal time, working in open office layouts, or collaborating in a conference room, security has to travel with them. We believe that endpoint security is key to knowing your devices are protected, your web browsing is safe, and your private info is secured by multi-factor authentication. The office of the future should be a place where people can move around, be creative and productive inside and outside that office environment, and always know they're protected. It's as simple as that—and it's a powerful vision for security that keeps business a step ahead of threats and lets people focus on the challenges and opportunities we know are ahead.

1. HP, Quantitative Research with WW End Users, 2015 2. Dimensional Research: Collaboration Trends and Technology, A Survey of Knowledge Workers, August 2015 3. C Space Primary Proprietary Research with online communities, 2015 4. PwC, Millennials at work: Reshaping the Workplace, 2011 5. Jamie Gutfreund, What Millennials Want In The Workplace (And Why You Should Start Giving It To Them), Jan 2014


THE OFFICE OF THE
FUTURE SHOULD BE A
PLACE WHERE PEOPLE
CAN MOVE AROUND



HP PRINT SECURITY

Worldwide cybercrime is a $445B problem[1], with over 1,700 significant data breaches worldwide in 2016[2]. According to the Digital Attack Map[3], DDoS attacks, which often use compromised IoT devices, occur daily. Most businesses try to protect PCs, servers, and other core parts of their networks, but often overlook their IoT devices, leaving them vulnerable to attacks.

SHIVAUN ALBRIGHT
Distinguished Technologist, HP

For today's hackers, the massive profit potential drives innovation and creativity. Among the greatest threats are botnets—automated tools built out of thousands of hacked IoT devices that are used to execute a coordinated attack. To create a botnet, hackers hijack the processors of unsecured devices, then use these compromised devices to mine bitcoin, or they rent their botnet to others to launch ransom-seeking DDoS attacks. The Mirai botnet attack in October of 2016, used as many as 1.2 million compromised devices to wage a DDoS attack, preventing access to popular websites such as Amazon, Netflix, and PayPal. The Mirai malware targeted IoT devices such as DVRs, security cameras, and printers.

HP's Printing and Imaging devices have evolved to become just as sophisticated as PCs containing a powerful processor running Windows or Linux, with storage, displays, scanners, network access, and email capabilities. With the ability to print, copy, scan-to-network destinations and send-to-email attachments, these print

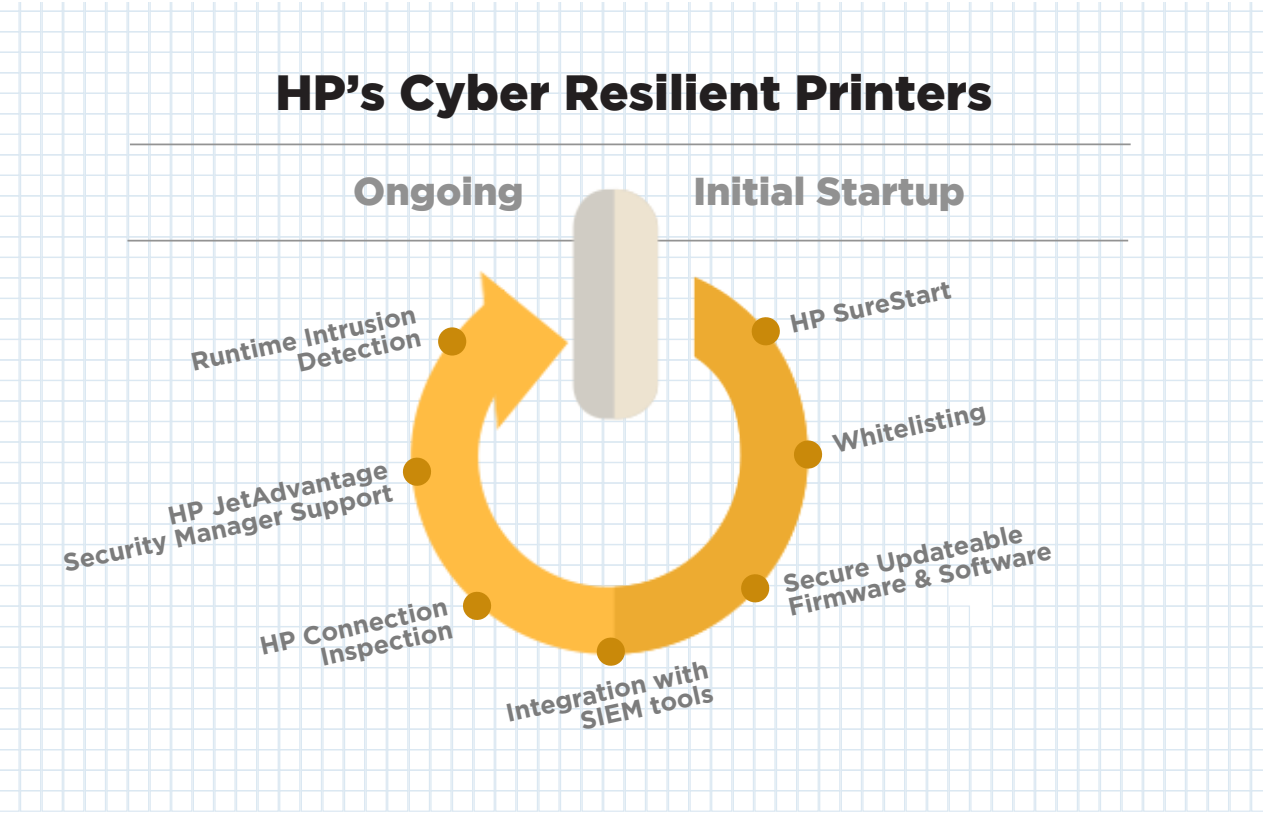


Figure 1: Device Lifecycle Initial Startup HP SureStart

devices come equipped with hard disk drives and run internal web servers. Hackers are becoming more sophisticated, with the availability of commercial tools designed by and for cyber criminals (e.g., Metasploit, IdaPro) that make it easy to reverse engineer code and craft new exploits. HP Printers must protect against these increasingly sophisticated attacks.

Malicious attacks can occur from inside or outside the organization. Here are some of the ways potential print-related security breaches can occur:

- Access via unsecured network ports/protocols are an entry point to the company network and information assets.
- The interception of print/scan data in transmission can expose a company's sensitive data.
- Injection attacks into the memory of printers can compromise an entire network.

HP's printers provide multiple layers of defense to protect the device and the customer's data. HP's printers have device protection features to ensure a root of trust at boot time and intrusion detection features to guard against runtime injection attacks.

Device vendors need to ensure that they reduce their exposure points (attack surface) by locking down the device as much as possible. Products also need to be developed with security requirements from the beginning. This means that devices need to be developed using secure coding methodologies, designing for security, performing a threat analysis early in the development cycle, and finishing with thorough penetration testing. HP follows these best practices using a security-in-design process to reduce potential exposure points and vulnerabilities on their printers.

Figure 2: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017[4]

HP was recently recognized as the market leader, ahead of the competitors in security capabilities and strategies. Some quotes from IDC MarketScape:

- "HP Inc. is a leader in our IDC MarketScape for print and document security solutions and services worldwide."
- "HP Inc.'s approach to security takes the entire print and document infrastructure into account beginning with locking down the device and extending into all aspects of devices usage and content protection."

In order to protect HP devices from the sophisticated security attacks occurring in the industry, HP's enterprise LaserJet and PageWide Enterprise printers have multiple layers of defenses. The following figure groups these defenses into two categories: Initial Startup functions and Ongoing operations.

INITIAL STARTUP

HP SureStart

Figure 1 highlights the initial startup process for FutureSmart Devices. The first step of the startup lifecycle is to load the BIOS which performs hardware initialization during the boot process. It is essential that this code be protected since it is the "Root of Trust." All other device-hardening measures depend on a safe and secure BIOS. Any malware in this layer would not be detectable by other layers. HP's innovative SureStart technology validates the integrity of the BIOS code and provides a self-healing capability if the BIOS becomes compromised. HP uses hardware to isolate and protect the "Golden Copy" of the BIOS which prevents access during normal run-time execution on the device. This

protected section of Flash contains a "Golden Copy" of the BIOS in the event of any BIOS compromise. The BIOS is hashed and signed with a cryptographic signature which is verified during boot. The device can revert to the "BIOS Golden Copy" in the event the BIOS becomes compromised.

WHITELISTING

The second step in the startup lifecycle is to ensure that the device only loads HP-authentic code. HP provides a dynamic whitelisting technology that ensures only authentic, untampered, executable code can run on HP's Printers. To clarify the terminology, a blacklist is used by antivirus scanners today which rely on identifying fingerprints of known malware. The problem with a blacklist is that it typically takes about 4 days or more to isolate a new virus during a zero-day attack and publish an update that needs to be downloaded to the antivirus software. Embedded devices, such as printers being a closed system, have the luxury of knowing the code that should be loaded and only allowing "known good files" to execute on a system. HP supports the whitelist feature by only loading known software into memory and calculating the hash of the code that is compared against the known "good" signed hash value to verify its integrity.

UPDATEABLE FIRMWARE/SOFTWARE

One of the key technological improvements for modern consumer and enterprise electronics has been updateable firmware via the Internet. From phones to smart TVs, to network switches, to VOIP phones, it is the expectation that the firmware will be updated regularly. Often the manufacturer relies on firmware updates for security patches and bug-fix issues as well as adding new features. Although updateable firmware has been a positive breakthrough, the firmware update capability has introduced the possibility of rogue code being installed, and printers are no exception.

HP ensures that only "known good firmware" is updated on the device. This requires the firmware to be hashed, ensuring that the firmware has not been tampered with and signing the hash using an HP-protected Private Key to ensure that the updated code is HP authentic code.

ONGOING OPERATION

Runtime Intrusion Detection

Recognizing that a device cannot protect against all current and future malware attacks, it needs to be able to look for and detect anomalous behavior while running. HP provides an innovative feature called Runtime Intrusion Detection to monitor memory for potential injection attacks. A buffer overflow is a typical example of an exposure point that a hacker could use to inject malware into a running device. Runtime Intrusion Detection performs continual checks in memory to identify, detect and highlight any anomalies. If an anomaly occurs, the device performs a reboot, flushing memory of any potential malware and booting to a secure state. If this happens, a security event is generated and can be monitored by various security monitoring tools (e.g., Security Information and Event Management (SIEM) tools).

CONNECTION INSPECTOR

HP Connection Inspector is an HP Labs patented technology to help printers stay one step ahead of malware attacks. The technology inspects outbound network connections to determine what is normal and stop any suspicious activity. On initial infection, malware commonly contacts its command-and-control server for additional instructions. This behavior can be detected by an increase in DNS traffic. If the printer detects this type of network anomaly, it automatically triggers a reboot to initiate HP SureStart self-healing procedures, and if configured, sends security events to SIEM tools, all without any intervention.

EASIEST TO SECURE AND MANAGE

HP JetAdvantage Security Manager

An often-overlooked area of device hardening is configuration control, which is perhaps one of the most important security areas.

Security can be complex for companies to understand and implement. Printer security requires an Administrator understand the dependencies between various protocols on printing devices; MFPs have over 200 security settings. JetAdvantage Security Manager is a policy-based security compliance tool that makes it easy to secure a customer's fleet of printers. Security Manager applies an easy-to-understand security policy to the fleet, handling printer differences effectively, and periodically assessing compliance and automatically remediating a

printer, if needed. JetAdvantage Security Manager provides a default "Best Practices Policy" based on current industry best practices and HP security recommendations. A customer can customize the security policy to meet their specific needs. A single instance of JetAdvantage Security Manager can manage up to 10,000 printers with daily monitoring.

Utilizing a network-based self-announcement protocol designed into HP Printers, JetAdvantage Security Manager is able to provide an Instant-On security feature which automatically applies the customer's security policy to a printer as soon as it is connected to the network.

JetAdvantage Security Manager can also be used to apply and renew Certificate Authority (CA) signed certificates to the

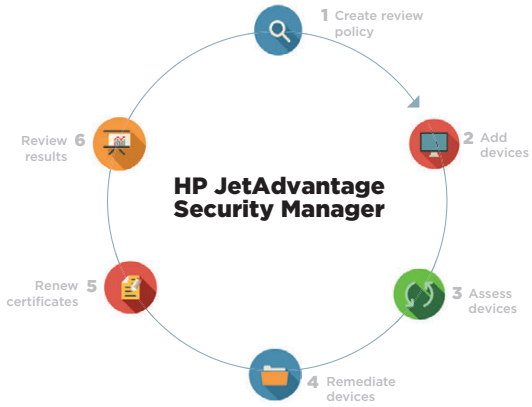


Figure 3: Device Lifecycle

printer to ensure secure and authenticated connections to the printer for browsing to the printer's Embedded Web Server as well as securely printing using the Internet Printing Protocol (IPP) over HTTPS.

By applying a security policy to a customer's fleet of devices, the customer can reduce the attack surface of their devices and ensure that those devices remain in compliance by periodically assessing the fleet.

SIEM TOOL SUPPORT

Security Information and Event Management (SIEM) tools aggregate event data produced by devices, network infrastructure, systems, and applications. HP, recognizing that many of our customers use SIEM tools, has added HP Printers as an additional device type that can be seamlessly integrated into ArcSight, SIEMonster, Splunk, and McAfee.

SECURE MPS AND SECURITY ADVISORY SERVICES

To help protect corporate print environments against cyberattacks, HP offers a service to our customers, called HP Secure Managed Print Services (Secure MPS). With Secure MPS, HP manages your print security from device hardening to advanced security solutions that address people, processes and compliance requirements. HP provides the following benefits to our customers as part of this service:

- Customers can outsource the management of the printer fleet to HP and HP will ensure that the fleet is kept up-to-date with the latest security measures.
- HP will address any potential security vulnerabilities of the printer fleet and handle the evolving security threats and changing compliance requirements.

Customers can add HP Print Security Professional Services to their Secure MPS contract to get further layers of protection. Credentialed security advisors can help co-develop and deploy a custom plan to advance print security.

- HP Print Security Advisory Services can help assess the customer's risks, develop a custom print security policy, and make process and technology recommendations for improved security.
- HP Print Security Implementation Services can help customers execute their security action plan—deploying security settings, adding security enhancements like device certificates, and integrating printers into SIEM tools such as ArcSight, Splunk, SIEMonster or McAfee.
- HP Print Security Advisory Retainer Service provides ongoing access to advisors to evaluate your security plans on a regular basis, plus ad hoc support for compliance audits.
- HP Print Security Governance and Compliance Service provides trained experts to monitor and manage print security compliance.

CONCLUSION

Protecting HP Printers from cyberattacks is important to HP. We will continue to provide industry-leading, innovative security features, and security services to protect our customers from the sophisticated attacks occurring in the industry.

1. McAfee & CSIS. Net losses: estimating the global cost of cybercrime, 2014 2. Gemalto. Breach Level Index, 2016 3. Digital Attack Map 4. IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment

JIVKO KIROV
Director, Worldwide Sales & Partner Training, HP

THOMAS JENSEN
Worldwide Head of Channel Sales Strategy, HP

HP UNIVERSITY SERVES CHANNEL PARTNERS AND CUSTOMERS WITH THE ENDPOINT SECURITY TRAINING AND CERTIFICATION PROGRAM

Cyber security attacks are increasing every year, with some of the most prolific cases ever occurring in 2017. You don't have to search far to find a large, well-known corporation that has been hit hard financially and had their reputation tarnished by a cyber breach.

IT security spend needs to shift from prevent and protect to detect and respond.

The concept of a network needs to change. The idea of the network as a fence around a collection of devices doesn't apply anymore. It's time to recognize the reality that the "network" emerges from connected devices—each an endpoint. Securing the network means securing the endpoints. Each endpoint consists of two elements: the device and the data, both of which need to be considered.

The challenge is formidable. And with time—with the explosion of devices in the IoT era, and the increasing sophistication of cybercrime—this challenge will only become more daunting. But with the right technology, the right strategy, and the right resources, we can defend our endpoints. We can keep our data safe.

At HP University, we believe **every endpoint purchase decision is a security decision.** That's why we are preparing our salesforce and technical consultants to confidently engage and educate customers with security in their sales conversations.

WITH 87%* OF BOARD AND C-LEVEL EXECS LACKING CONFIDENCE IN THEIR LEVEL OF CYBER SECURITY, HEREIN LIES AN OPPORTUNITY!

**Ernst & Young. Global Economic Crime Survey 2016*

With a comprehensive security program, HP University provides a strong foundation within the latest security landscape, enabling sales professionals to drive higher awareness of security risks, recognize opportunity triggers, and effectively identify HP security solutions tailored to their customers' needs.

HP channel partners are critical to extending our security leadership to customers. HP University offers channel partners comprehensive training on HP endpoint security offerings and teaches them how to engage and educate customers on security challenges and solutions, thus helping them to become strategic advisors to their clients.

SECURITY TRAINING STRUCTURE

The security training and associated certification program features different tracks, tailored to different roles, from pan-HP security fundamentals for sales professionals to advanced and technical training tailored to print and PC specialists and technical consultants.

A BRIEF OVERVIEW OF EACH CERTIFICATION:

Endpoint Security Training and Certification

This is the most fundamental training of the series, delivering a strong foundation of security knowledge to tell the HP security story. The format is made up of short, online, self-paced training and includes an online assessment that will lead to the HP Sales Certified–Endpoint Security certification.

Advanced Endpoint Security Training and Certification

The two-day classroom-based training focuses on building a salesperson's confidence and competence to engage in an effective, security-led conversation with a customer.

Technical Security Training and Certification

This program may differ by region, typically focused on improving the presales technical consultant's ability to progress an opportunity through to building the right security solution. There are two tracks, one for Print and one for PC. An optional Security Primer may precede this training.

How are we rolling this out?

The online training, exams, and classroom trainings are rolling out in every region. It's part of HP's ongoing commitment to industry leadership, educating partners and customers on endpoint security and enabling them to successfully detect and respond to any security concern.


EXIT

BY CHRISTOPH SCHELL
President and Managing Director, Americas, HP

HP'S BATTLE AGAINST CYBERCRIME

Keeping data safe in an increasingly mobile world

The number and sophistication of cyberattacks is set to rise again this year. Successful hacks are causing lasting damage to privacy, trust and corporate reputation—three prerequisites of connected commerce.

There are several reasons for this escalation in cybercrime. Firstly, as more data is digitized, it becomes more susceptible to hacking. The expanding ecosystem of connected devices has increased the number of access points to this data and into networks. Finally, and most maliciously, cybercriminals of various motivations are inventing new ways and tools to expose private and sensitive information.

Many cybercriminals have turned their attention to "endpoints"—connected devices at the periphery of a network, like printers, laptops, and phones. They house valuable data and their usage and portability make them vulnerable to external threats, often yo-yoing in and out of the protection of corporate firewalls.

As depicted by our excellent miniseries *The Wolf* and *The Fixer*, networked printers have become a particularly popular target for endpoint attacks. Data thieves have learned to bypass network security controls and copy sensitive documents straight from a printer's memory, revealing closely-guarded corporate secrets.

Endpoint security has already become a critical battleground in the fight for privacy. The Ponemon Institute's 2017 State of Endpoint Security Risk report stated 69% of organizations believe the endpoint security risk has significantly increased.

In this escalating war between those protecting privacy and those wishing to profit from its demise, I am proud to say HP is taking a leading role. We are developing transformative digital technologies providing safeguards against data intrusions. HP is fighting back against cyber thieves on three fronts:

1. ENDPOINT SECURITY

When we think of hacking, we often imagine quickly-typed code, supercharged computer towers and ominous aliases. But that's only part of the story. Endpoints are susceptible to a variety of threats. For example, "visual hacks" require only for a third party to read secret information over an employee's shoulder.

The solution is Endpoint Security: a range of cutting-edge defenses built for, and into, the endpoint device itself. Without interfering in a device's normal functionality, endpoint security software protects vital functions from malicious interference, authenticates software loaded onto the device and vigilantly monitors for external attacks. Further precautions, like screen shields and print queue management, negate other vulnerabilities.

2. DEVICE-AS-A-SERVICE (DAAS)

In appreciation of worsening cybersecurity threats, DaaS providers like HP are making cybersecurity protection a core part of their offering. There are many benefits to the DaaS model, in which companies lease productivity hardware from a specialist device provider. It ensures faster device upgrade cycles for hardware and software, meaning office hardware is equipped with the latest cybersecurity defenses.

By allowing standardization across device fleets, DaaS also helps companies better manage their IT environment. DaaS solutions allow IT leaders to monitor an entire fleet of devices, empowering them to spot and address anomalous activity and ultimately thwart emerging cyberattacks.

3. MANAGED PRINT SERVICES (MPS)

In a Managed Print Services arrangement, a company's print operations are managed by an external provider. Armed with print-specific expertise, MPS providers such as HP are best suited to protect a company's print fleet from cyberattacks.

Today, with the help of expert cloud analytics partners, HP has transformed the MPS value proposition from that of a basic service to a strategic business tool. Companies can now gain powerful insights into print costs, printing behaviors, and printer utilization to drive efficiencies and streamline business processes to enhance productivity.

The threats posed by cyberattacks are worsening, but HP is rising to the challenge by building technologies and solutions ready to tackle and repel the next wave of cyber threats.

For more insight on HP's endpoint security strategy, read 'Innovating in Endpoint Security: Cyber Resilence at the Enterprise Edge,' pg. 4.


ENDPOINT
SECURITY HAS
ALREADY BECOME
A CRITICAL
BATTLEGROUND
IN THE
FIGHT FOR PRIVACY

AON AND HP ARE WORKING TOGETHER TO HELP MITIGATE THESE RISKS BY DELIVERING AN INTEGRATED SET OF RISK MANAGEMENT SOLUTIONS

LORRI JEFFERSON
VP and Head of Services and Software Product Management, Emerging Compute Solutions, HP

Aon and HP Join Forces to Combat Cyber Risk

HP is collaborating with Aon Cyber Solutions, part of Aon P.L.C., to provide enhanced, integrated cybersecurity coverage tailored to meet the growing needs in today's businesses.

The two companies are launching a holistic solution for customers that includes hardware-level security protection, comprehensive risk assessment and remediation, rapid incident response, and options for enhanced cyber insurance coverage. The solution will be available through the HP Device as a Service (DaaS) offering, which provides multi-OS device management support and advanced analytics and proactive management capabilities.

The cyber threat landscape is rapidly evolving, with business leaders increasingly concerned about the disruptive impact of cyber risk.[1] At the same time, the number of devices and operating systems used by enterprises is skyrocketing. While providing increased productivity and efficiency, this explosion of endpoints can significantly increase cyber risk exposures. HP estimates that by 2020 there will be 9 billion commercial devices worldwide,[2] with an average of four devices per user[3]—creating added costs and complexity for businesses.

According to Michael Park General Manager and Global Head, Emerging Compute Solutions, at HP, "The vast majority, 82% of IT teams with whom HP works say they are challenged on securing data and devices in their environment.[4] Adding that more than 70% of data breaches now occur through endpoints such as PCs and handheld devices."[5]

Aon and HP are working together to help mitigate these risks by delivering an integrated set of risk management solutions that include:

- Aon Cyber Resilience Evaluation: Aon's cybersecurity professionals will use Aon's proprietary assessment tool to evaluate a company's cybersecurity posture and provide recommendations to improve defenses.
- HP DaaS: HP DaaS makes it easier for businesses to equip their employees with the right hardware, accessories, and lifecycle services to get the job done. Businesses benefit from HP's analytics and proactive management service that provides actionable analytics and fleet insight to uncover potential device health and security risks, so they can be proactively addressed before they impact user performance.
- Aon Premier Cyber Insurance Panel: Deploying HP's DaaS and conducting Aon's Cyber Resilience Evaluation will enable companies to qualify for enhanced cyber insurance coverage through access to Aon's comprehensive booking resources with a view towards best-in-class pricing and deductibles to mitigate financial risk.
- Aon Incident Response Services: Organizations will have access to Aon's incident response team in the event of an attack, including incident response retainers.

The Aon-HP joint offering is expected to launch in fall 2018. Initially, the offering will be available directly from HP and through channel partners in the U.S. only, becoming available outside of the U.S. over the next year.

1. Aon 2016 Cyber Captive Survey 2. HP Proprietary Research, 2017 3. Strategy Analytics Global Internet Device Forecast Report, 2014 4. IDC, Transforming Device Lifecycle Management with Device as a Service 5. IDC


SECURITY FOR
EVERY
ONE

JIM MANN
Distinguished Technologist,
Office of the Chief Engineer, HP

The digital revolution and hyper-connectivity which has taken shape over the last several decades has resulted in tremendous benefits for those fortunate enough to be able to participate. However, there are people who actively seek to take advantage of vulnerabilities in the systems built with this technology. They do this for reasons including personal gain, promotion of ideology, espionage, geopolitical influence, or sometimes just for fun. The actions of these bad actors have consequences ranging from minor inconvenience to devastating personal impacts and even personal injury.

All of us have likely been impacted by a cybersecurity event, so we understand the pain our customers feel when they are impacted. During 2016, Symantec reported 1,209 confirmed breaches which exposed more than one billion user identities. PWC reported 32% of companies disclosed an incident of cybercrime. According to the Ponemon Institute the average cost of a breach is roughly $9.5M. These are alarming numbers, yet they still underestimate the total impact because it is hard to put numbers to cybersecurity incidents for individual consumers. Importantly for HP and our customers, it is estimated that 71% of breaches start from an endpoint device, such as a PC or printer, putting our products at the forefront of protecting customers' data.

For many years, HP has been at the forefront of endpoint device security, as demonstrated both through active participation and leadership in industry consortia and standards bodies, and our market-leading innovations such as HP SureStart. This has resulted in new marketing statements such as "World's Most Secure Printers", and "World's Most Secure and Manageable PCs", as well as *The Wolf* and *The Fixer* video series.

Because security is such a key element of our promise to customers, and the impacts can be so severe, we continually strive to push the envelope in delivering the best security technology (the what), with a process methodology that ensures HP products and services are developed securely (the how). This tandem of what and how was succinctly captured by HP's Chief Information Security Officer, Jack Clark, as "secure products, built securely" and serves as a guiding principle for HP's product security strategy.

To solidify HP's position into the future, we must have a culture of security throughout the company. Security is a team sport which benefits by everyone—not just security professionals—being knowledgeable and invested in the security of the products and services we deliver to our customers.

But security is an expansive topic, uses terminology which can be daunting to those new to the subject, and makes use of a broad array of often complex technologies. To make this more accessible to the non-security professional, our team champions various efforts across HP to engage and enrich not only professionals in the security community, but also others with interest in the topic or who just need education in the basics of security. This includes co-leading the Security and Privacy Affinity Group, sponsoring security summits and topical webinars, hosting business-challenge workshops, curating, sourcing and developing training materials, creating development learning paths, and working with HR on security talent management.

At HP we know the security landscape continues to evolve rapidly, threats increase each year, and attackers only get better and more creative. Continuous learning is critical in ensuring HP can continue to put the most secure products in the market to help our customers maintain their businesses and missions.

To learn more about this video series or suggest ideas for specific topics to be covered, please contact Jim Mann at mann@hp.com.

SHIVAUN ALBRIGHT is the Chief Technologist for Printing Security responsible for defining the security strategy for HP's Printing and Imaging fleet which includes all facets of enterprise printing and imaging security.

BORIS BALACHEFF is an HP Fellow and Chief Technologist for Security Research and Innovation. Boris leads the HP Security Lab research strategy and is responsible for driving security technology innovation strategy with HP businesses.

MEI JIANG is Head of Pan-HP Innovation Strategy. Her focus is on HP's future growth, capitalizing on disruptive technologies and business model innovation. **@MeiJiangHPMaker**

LORRI JEFFERSON leads the services portfolio strategy, product management and analytics and machine learning for HP Personal Systems. Her team drives innovation for multi-OS device management, security services and modern IT management services. Lorri is recognized for bringing innovative products to market featuring grounds up designs as well as with strategic partnerships.

THOMAS JENSEN is Worldwide Head of Channel Sales Strategy at HP. Thomas leads the development of the channel strategy and partner program that cover 87% of HP's revenue. **@tjensen1973**

JIVKO KIROV is a seasoned HP sales and business strategy manager with extensive experience in global business transformation. He maintains a proven track record in leading country-based and regional teams of sales professionals; and a strong cross-cultural background and outlook. Jivko drives strategic projects with critical business impact.

JIM MANN is an HP Distinguished Technologist and Security Strategist in the Office of the Chief Engineer. He works pan-HP on security technology, governance, and education, as well as externally in industry consortia.

CHRISTOPH SCHELL is President of the Americas Region for HP. In this role, Christoph is responsible for the go-to-market strategy and overall financial performance of the Americas' business products and services across all markets. **@ChristophSchel**

SIMON SHIU is Director of the Security Lab. With twenty years of security research and industry experience, Simon manages security research for HP, from dealing with today's growing cybersecurity challenge to delivering security innovation.

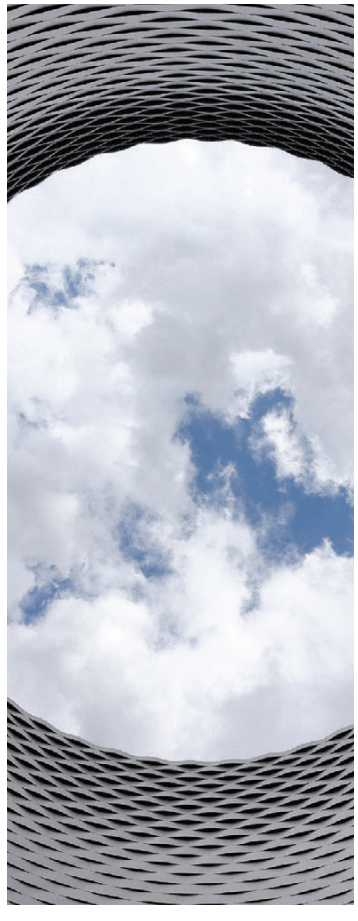
GAGAN SINGH is head of product management for HP's Premium (1000 series) notebook product line, security and Innovation for Commercial PC's. This team is responsible for driving market-leading solutions that will allow HP commercial PCs to continuously claim world's most secure and manageable PCs.

DOUG WARNER is VP and Global Head of Tech Vision & Strategy at HP. He began his career at HP as the Director of Strategic Development, Digital Imaging. **@dougwarner**

SHANE WALL is Chief Technology Officer, HP and Global Head, HP Labs. Shane drives the company's technology vision and strategy, new business incubation and the overall technical and innovation community. **@ShaneWallCTO**

CHANDRAKANT D. PATEL is a distinguished Senior Fellow and Chief Engineer at HP. In 2014, he was inducted into the Silicon Valley Engineering Hall of fame. **@joulespatel**

VALI ALI is an HP Fellow, and the Chief Technologist for Security and Privacy for Personal Systems group. He drives vision, architecture, technology, and evangelization for all security, privacy, and platform enabling hardware, software, and firmware for HP's Business Client PCs.



Visit the Garage by HP, our new digital storytelling destination, where you'll find inspiration and information about innovation, reinvention and how technology is changing the world.

keep reinventing

keep reinventing

JUNE 2018

THIS PUBLICATION WAS PRINTED USING AN HP T230 COLOR INKJET WEB PRESS AND HP INDIGO 7600 DIGITAL PRESS