INNOVATING IN ENDPOINT SECURITY

BASED ON EXPERTISE FROM:

Boris Balacheff Chief
Technologist for Security Research and Innovation, HP

Simon Shiu
Head of Security Lab, HP Labs

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

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 has never been more important. The rampant rise in cybercrimes – over 3,800 data breaches in the first half of 2019, up 54% compared to the same time the previous year[1] – is driving up costs. Revealed in Accenture's 2019 Cost of Cybercrime report, the average cost of a breach has reached $13 million, an increase of 12% in the last year.[2] And it doesn't matter which threat has made its way in: the total annual cost of all types of cyberattacks is up – with ransomware seeing the fastest growth year over year.[2]

To stay ahead of attackers, we need to always be on the lookout for emerging and future trends in the threat landscape. That's why we recently announced a new HP Security Advisory Board, a trio of outside experts with unique first-hand expertise in the world of hacking and the latest developments in security technology and strategies.

Cybersecurity is now a truly disruptive force. If you have the multi-layered 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 fact, business leaders, well-versed in this negative narrative, are predicted to spend more than $124 billion in 2019[3] alone to protect their organizations.

Endpoint devices are on the front line

From healthcare to manufacturing, from transportation to the home, from agriculture to critical utility infrastructures, endpoint devices are the first line of vulnerability, and defense, for the data and resources we care about. They are the interface between the physical and digital world, and a prime target for cyberattacks 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. This can give an attacker control over an entire system, undetected 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.

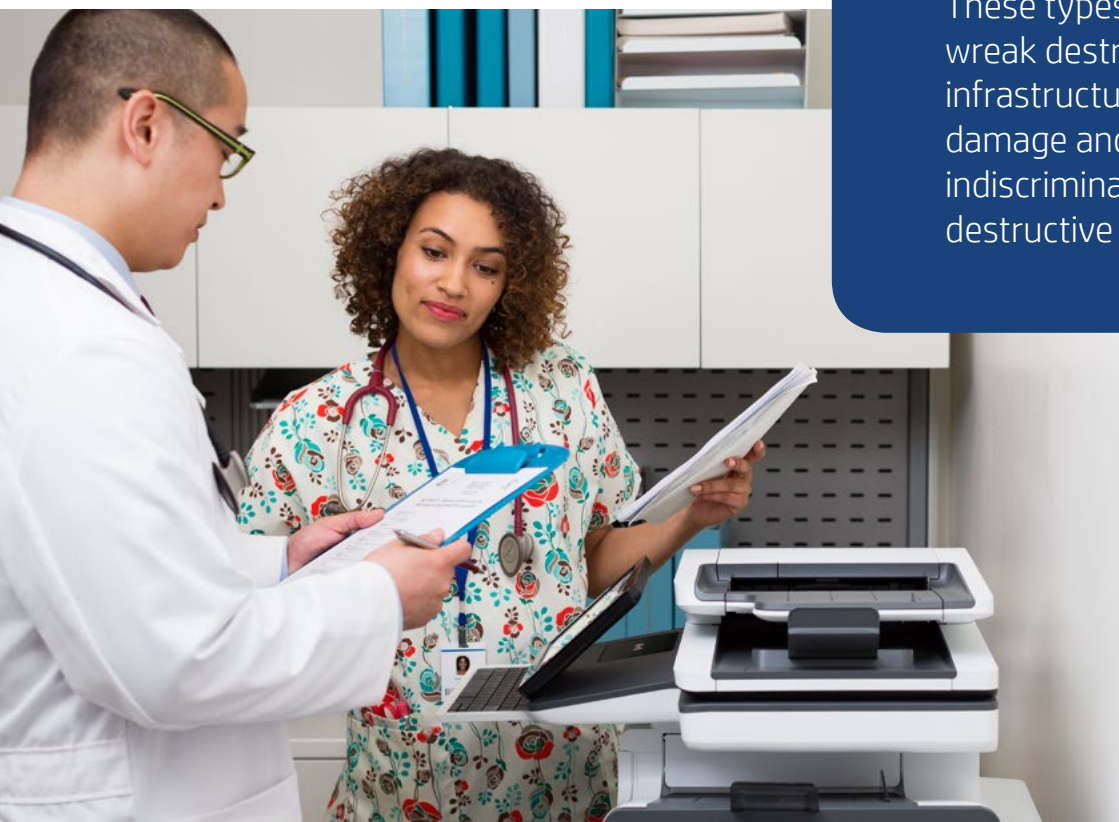
To address this degrading threat environment, and new styles of attacks and attacker motivations, HP has been leading the industry in designing systems and devices with security built-in from the hardware up, to help protect, detect and remediate attacks, with minimal interruption to users.

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 including management solutions. This is the approach that we have been developing at HP Labs, to ensure that devices, from PCs to printers, are not only built with protections, but can reliably detect successful attacks and recover from them.

Stories of high-profile data breaches are becoming more and more prevalent in the media – and the perpetrators of the biggest attacks are going after information, theft, ransom and disruption.

In May 2019, the US city of Baltimore, Maryland, was hit by a ransomware attack,[4] infecting around 10,000 government devices with a new strain of ransomware called RobbinHood, blocking city services such as the payment of water bills and property taxes. As well as the financial impact – which resulted in costs worth millions of dollars – the attack left city employees without access to their emails and impeded on the city's real estate and water billing for the months following.

These types of attacks seek to wreak destructive havoc on infrastructure, creating collateral damage and hitting organizations indiscriminately, making them truly destructive at scale.



A hardware purchase is a security decision

Software and network security are no longer enough to protect endpoints across an organization. This means that, today, choosing a device is a security decision. Whether a PC, printer or any other IoT device, ensuring that standards are met, and exceeded, with state-of-the-art security, will help address threats over the years that the hardware is in use.

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.

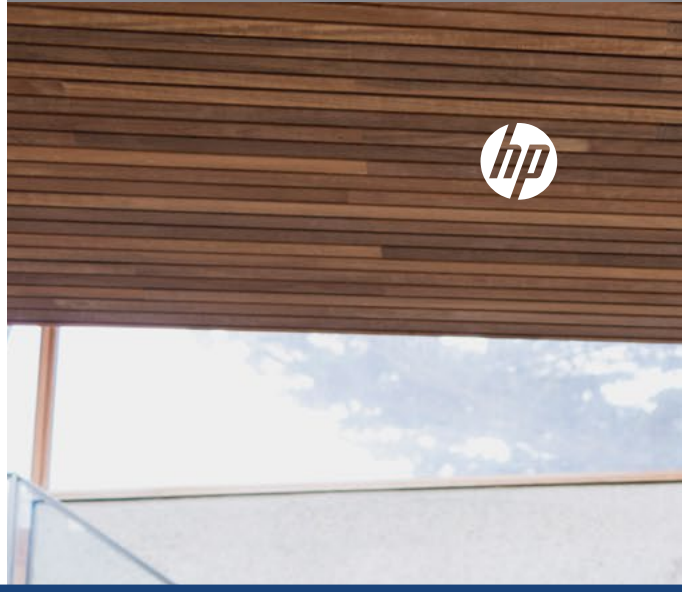
Anyone who makes a hardware purchasing decision – however small or large – will have an influence on the security posture of the business for years to come. The enterprise CISO, who usually looks after the security of operations, needs to get involved much earlier at the IT equipment and hardware procurement step: setting security requirements and making sure that security is a key parameter of the purchasing decision.

Considerations for security

Beyond the security of the devices themselves, the endpoint security challenge for organizations lies with security management.

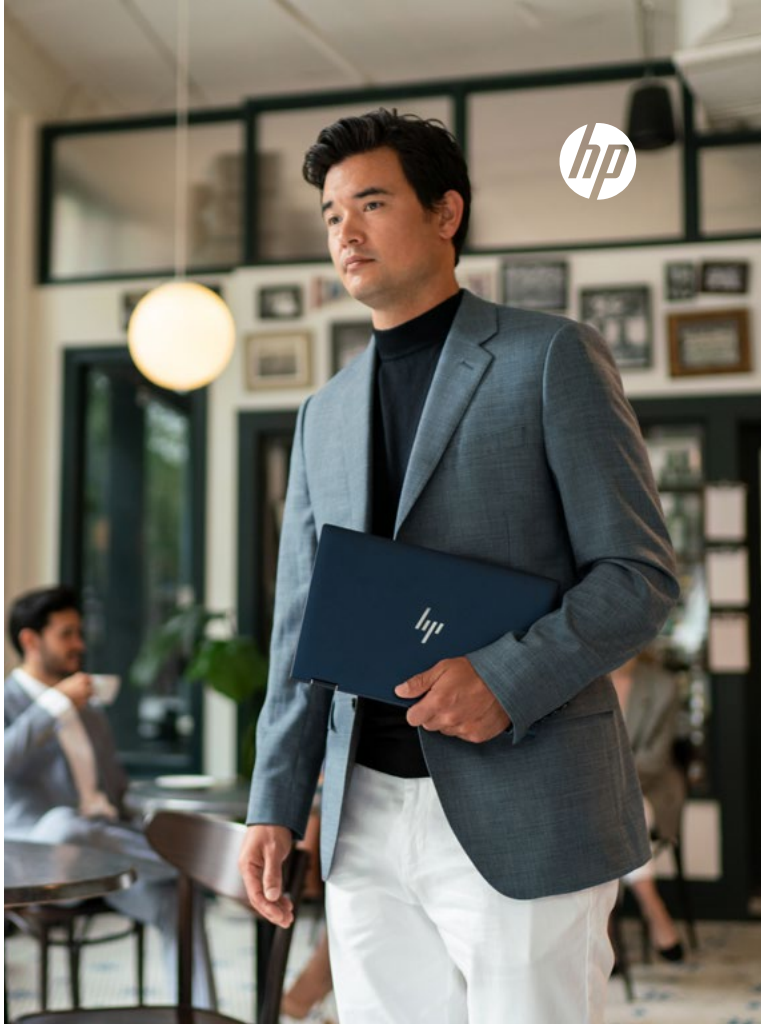
- **Organizations need to keep all the devices on their network up to date with the latest software and firmware, and in compliance with a good security configuration policy.**
- **In addition, they need to deploy, manage and monitor security software that's appropriate to their business needs.**
- **To 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.**

To top the list of challenges organizations are facing: the cybersecurity talent pool is in tension. A lack of available expertise 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. This can 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.



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. Consider this in the context of digital manufacturing where products are manufactured on the 3D printer nearest the end customer. Or consider this in the context of computing for personalized healthcare, or, more broadly, of artificial intelligence and machine learning being built into devices to support autonomous behaviors. We believe that security innovation will be key to addressing emerging threats and to rising to the challenge of assuring the safety of our cyber-physical future.

Investing in the long term

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 user experiences, with appropriate levels of security and assurance over privacy.

The trustworthiness of tomorrow's infrastructure will depend on the resilience of endpoint devices to cyberattacks. We continue to pursue security innovation to help build 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. This, while allowing 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: from engaging with other experts across academia, governments and industry, and with HP's own Security Advisory Board. We also operate our own Attack and Malware Lab, an isolated environment to investigate the most sophisticated 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 work 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 cybersecurity and move our industry forward towards a safer, more resilient future.

Meet the HP Security Advisory Board

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, ensuring that companies promptly fixed them.

More recently, destruction for destruction’s sake has become a new hallmark of the global cyberthreat landscape. 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. We took an extra step by setting up our own Security Advisory Board, bring¬ing 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 land¬scape 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 cryptographi¬cally secure updates of a device’s BIOS to run-time intrusion detection, which checks for anomalies and automatically reboots when an intrusion is detected.

Ask the experts

"You recently joined our new Security Advisory Board, at a time when cybersecurity 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 cyberthreat 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 compro¬mising 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 technol¬ogies 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.

Sources

1 TechRepublic, August 2019, Data breaches increased 54% in 2019 so far. https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/

2 Ponemon, 2019, The cost of cybercrime. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

3 RSA Conference, June 2019, The future of companies and cybersecurity spending. https://www.rsaconference.com/industry-topics/blog/the-future-of-companies-and-cybersecurity-spending

4 Ciso Mag, June 2019, Baltimore hackers leak data on Twitter after no ransom was paid. https://www.cisomag.com/baltimore-hackers-leak-data-on-twitter-after-no-ransom-was-paid/