HP WOLF SECURITY LEADERS SHARE 2023 SECURITY PREDICTIONS

Joanna Burkey, CISO, HP Inc.

The cybersecurity onus for 2023 is going to be on intentional investing

"There won't be an unlimited treasure chest of money to devote to cybersecurity in 2023, so it's important to be intentional about where to invest. Good governance is about more than just compliance – it's about appropriately handling your company's resources, including budgets. There is an ocean of security issues to boil, so understanding which areas expose the company to the most risk will be essential.

"If you're in charge of security spending, you need to think about your organization's value proposition – what makes you unique – as well as understanding risk appetite and position on the business curve – whether you're gearing up for sale, in hyper-growth, or pivoting into a new market. These factors will inform the business priorities and help you contextualize which assets to focus on and where new risks may emerge. Then you can figure out the best areas to prioritize and what investments are needed.

"It's important to consider how you can group certain risks. For example, if you are a service business where your workers are your most valuable 'assets', then applying technologies like isolation can help defend against the most common attacks targeting those workers – such as phishing and social engineering. Equally, supply chain might be a big area of risk. It may be that there are gaps in basic cyber hygiene within your supply chain footprint that need addressing.

"In a nutshell, know the highest risk areas throughout the business, know where is most likely to be targeted, and know how much you can afford to invest. With a solid cybersecurity foundation, you can ensure maximum resiliency for anything that gets through."

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

In 2023, sophisticated firmware attacks will become more widespread, and cybercriminals will continue to invest in attacks that leverage physical access to endpoint devices

"In 2023, organizations should take control of firmware security. Firmware attacks were once only used by sophisticated APT (Advanced Persistent Threat) groups and nation states. But over the last year, we've seen signs of increased development and trading of capabilities in the cybercrime community – from tools to hack BIOS passwords, to rootkits and trojans targeting device BIOS (Basic Input/Output System) and UEFI (Unified Extensible Firmware Interface). We now see firmware rootkits advertised for a few thousand dollars on cybercrime marketplaces.

"Affordable prices for sophisticated attack capabilities go hand in hand with growing demand. We should expect to see more listings of this kind on sale in the cybercrime underground, and in turn more firmware attacks.

"Beyond software designed to attack firmware, there's also growing concern around physical attacks. These seek to exploit physical access to a machine to tamper with devices and inject malware locally into firmware or software.

"Access to the firmware level enables attackers to gain persistent control and hide below the device Operating System, making them very hard to detect – let alone remove and take back control. Organizations should ensure they understand industry best practice and standards in

device hardware and firmware security. They should also understand and evaluate state of the art technology that is available to protect, detect, and recover from such attacks like HP Sure Start, Sure Recover, Sure Admin, or Tamper Lock.

"It is key that organizations start asking the right questions about how devices are designed with security and resilience in mind down to the hardware and firmware levels, and consider this during procurement to underpin their endpoint infrastructure for years to come."

Shivaun Albright, Chief Technologist for Printing Security at HP Inc.

2023 could be print security's WannaCry moment, as Nation State trickle down increases prospect of cybercrime groups exploiting printers for financial gain

"In 2023, we could see print security's WannaCry moment as Nation State techniques exploiting printers trickle down to the wider cybercrime economy – just as we saw with the EternalBlue leak. This will lead to cybercrime groups exploiting printers for financial gain. There's plenty of motivation for doing so. Accessing printers could allow attackers to capture confidential documents and data for ransomware purposes or use the printer as a launch point to other devices on corporate networks.

"Aiding attackers in these efforts is a plethora of exposed and unsecured print devices, handling sensitive information and even connecting to corporate devices. Picking off these machines and hijacking them will be like taking candy from a baby, as no one really sees their printer as an attack vector.

"To defend against attacks on printers, organizations must improve cyber security hygiene. Printer security can no longer be overlooked. Updates must be applied regularly, and devices should be regularly monitored and analyzed to see if they are in a breach state. Overlooking print security leaves a gaping hole in cybersecurity posture, one attackers will gladly walk through on their way to your organizations crown jewels."

Dr. Ian Pratt, Global Head of Security for Personal Systems at HP Inc.

Rise in hijacking remote access sessions could result in high-value domain servers and cloud admin portals – or even physical OT environments – being breached

"Session hijacking – where an attacker will commandeer a remote access session to access sensitive data and systems – will grow in popularity in 2023. Increased use of features like Windows Defender Credential Guard are forcing attackers to pivot – either capturing users' passwords to enable lateral movement, or hi-jacking the remote session itself to access sensitive data and systems. The latter is particularly powerful.

"By targeting users with elevated rights to data and systems – such as domain, IT, cloud, and system administrators – these attacks are more potent, harder to detect, and more difficult to remove. The user is typically unaware that anything has happened. It takes just milliseconds to inject key sequences and issue commands that create a backdoor for persistent access. And it works even if Privileged Access Management (PAM) systems are being used to employ Multi Factor Authentication (MFA), such as smart cards.

"If such an attack connects to Operational Technology (OT) and Industrial Control Systems (ICS) running factories and industrial plants, there could also be a physical impact on

operational availability and safety – potentially cutting off access to energy or water for entire areas.
"Session hijacking does not rely on exploiting a fixable vulnerability; it is about abusing legitimate and necessary functionality of remote session protocols – like Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA), and Secure Shell (SSH). Strong isolation is the only way of avoiding these kinds of attacks and break the attack chain. This can be done either through using a physically separate system, like a Privileged Access Workstation (PAW), or virtual separation, via hypervisor-based approaches like HP Sure Access Enterprise."

Alex Holland, Senior Malware Analyst at HP Inc.

People may turn to 'cyber hustling' in the cybercrime gig economy to make quick cash during the economic downturn

"The 2009 recession saw surges in malware and online fraud. Since then, we've seen the rise of the cybercrime gig economy, where the shift to platform-based business models has made cybercrime easier, cheaper and more profitable. Cybercrime tools and mentoring services are readily available at low costs, enticing cyber hustlers – opportunists with relatively low levels of technical skill – to access what they need to turn a profit. As we face another global downturn, easy access to cybercrime tools and know-how could increase the number of attacks we see – especially attacks against home users by opportunistic cyber hustlers.

"Home users may get caught in the firing line, as they are easier to compromise than enterprises. Cyber hustlers are likely to use simpler techniques, like scams and phishing – potentially capitalizing on the economic downturn by offering people fast ways to make money, like cryptocurrency and investment scams. The interconnected nature of the cybercrime gig economy means threat actors can easily monetize attacks. And if they strike gold and compromise a corporate device, they can also sell that access to bigger players, like ransomware gangs. This all feeds into the cybercrime engine, giving organized groups even more reach.

"As attacks against users increase, having security baked into people's PCs from the hardware up – so they can easily prevent, detect and recover from attacks using tools like HP Sure Recover – will be essential. Our research shows that email is the most common attack vector, particularly for opportunists like cyber hustlers. Isolating risky activities is an effective way of eliminating entire classes of threats without relying on detection. Threat containment technology like HP Sure Click Enterprise ensures that if a user opens a link or attachment and something nasty comes through, the malware can't infect anything. This way organizations can reduce their attack surface and protect employees without hindering their workflows."