



Print Security Becomes Increasingly Critical with the **Rise of a Work-From-Home Workforce**

An IDC InfoBrief, sponsored by HP

By: **Robert Palmer**, Research Vice President, Imaging, Printing, and Document Solutions, IDC
Keith Kmetz, Program Vice President, Imaging, Printing, and Document Solutions, IDC

September 2020



Security Is a High Priority for All Organizations, But...

IDC has observed a notable difference in the level of priority placed on IT security versus print/document security. IDC's research shows that organizations continue to (falsely) assume that the print environment is adequately protected by network security measures. But security around the network perimeter is crumbling, and every device connected to the network is now a standalone endpoint security risk — printers and MFPs included.

Currently, only 13% of IDC survey respondents¹ believe their company's overall security level is inadequate. The majority believes that existing security measures are fine or even too extreme and sacrifice productivity.

Meanwhile, a new threat has emerged:

Work-from-home (WFH) policies resulting from the COVID-19 pandemic have created new realities. Organizations must consider a holistic approach to security to protect their most business-critical asset: information.

Over 75% of organizations² have either:

- Not recognized print security as an essential element of their IT security strategy
- Taken some basic measures but assume print assets are safe because they are connected to a secured network
- Taken steps to address print security, but mostly limited to device-level actions



One third of the global population is in quarantine or under stay-at-home orders.³

Organizations are only as secure as their most vulnerable endpoint.

¹Source: IDC Generational Print Survey, June 2020

²Source: IDC MaturityScape Benchmark: Print Security in the United States, May 2019

³Source: COVID-19: A Public Safety and National Security Threat — Short-, Medium- and Long-Term Impacts, IDC #46201420, April 2020

WFH Introduces a New Level of Complexity to Security

The COVID-19 pandemic and related lockdown has radically changed the way businesses operate. The initial focus was on putting systems in place to ensure business continuity and provide for the dissemination of trusted information. Companies embraced collaboration technologies and other cloud-based corporate applications to enable employee productivity in a work-from-home environment. But what does this mean from a security perspective?

31% of survey respondents¹ indicate security and privacy as one of the biggest challenges they face when working from home.

Many organizations are unprepared to support the printing needs of remote employees. The complexities associated with print security increase significantly with a largely unmanaged, distributed workforce.

Workforce in Transition²

A recent IDC survey shows that COVID-19-initiated mandates have substantially increased the migration to WFH. The expectation is that some significant portion of this change will be permanently established for work.

63%

of global respondents indicated that some portion of their work occurs at home.

41%

of global respondents indicated that a work location change of working exclusively from home took place in 2020.

COVID-19 ushers in a **“next normal”** where WFH becomes more common. How will organizations address the rising challenges of maintaining the optimal level of security when work is increasingly conducted in home and remote locations beyond their network perimeter?

¹Source: IDC Generational Print Survey, June 2020

²Source: IDC Generational Print Survey, June 2020

Cyber Resiliency Should Be the Ultimate Goal

To accommodate the new work environment, security solutions must support both remote workers as well as those who will eventually return to the office. Organizations must ensure that security offerings remain fluid and oriented to specific user profiles — but managed, controlled, and monitored by the proper IT stakeholders.

The solution involves more than just deploying technology to harden devices and protect from outside threats. The goal should be **cyber resiliency**, which includes a systematic approach to influencing user behavior combined with tools and technologies to ensure proper cyberhygiene.

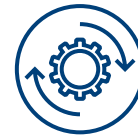
From a device perspective, it's all about protect, detect, and recover while working from home.

Zero-Trust Model

Today's work environment requires organizations to move toward a zero-trust security model, fueled by the need to support remote users, BYOD, and cloud-based assets that may or may not be located within a known network boundary. Implicit trust is no longer granted based on device location.

Top Security Priorities for 2020¹

Reacting to COVID-19 and the challenges of working from home



Automate: Look for ways to ensure that patching, password resets, change control, incident management, and other manual processes are automated wherever and whenever possible.



Deploy multifactor authentication everywhere: It is no longer prudent to rely on passwords for anything, even inside an organization.



Develop a BYOD plan: Even if you normally don't allow BYOD, ensure you have a way for unmanaged devices to access organization resources without compromising on protection.



Review your data governance policy and program: Ensure that owners are identified and any policy issues associated with the content are addressed.



Upgrade the compliance program: Create a program of continuous compliance that does not require site visits. Rely on third-party audits, continuous reporting of activity and controls, and robust architecture for protection.

¹Source: IDC Five Key Cybersecurity Trends for 2020, IDC Doc #US46772720, August 2020

Printers Are a Target for Cyberattacks and Are Often Overlooked

Most organizations fail to recognize the security vulnerabilities of their existing print and document environment. At the heart of this issue is the role of the smart MFP, which has become an intelligent business processing hub that serves as an on- and off-ramp to business information, whether it is stored in the device, on the corporate network, on paper, or in the cloud.

Research shows that cybermiscreants are increasingly leveraging printers and other non-PC-connected devices as gateways into the network or as instruments for injection attacks.



Print Ecosystem Security Vulnerabilities

- **BIOS and firmware:** compromised firmware can open a device and network to attack
- **Management:** undetected security gaps.
- **Network:** print jobs can be intercepted as they travel on the network
- **Control panel:** users can exploit device settings
- **Storage media:** printers store sensitive information on internal hard drives
- **Scan/capture:** documents in motion can be intercepted
- **Input tray:** special media can be tampered with or stolen
- **Output tray:** abandoned print jobs with sensitive information
- **Mobile printing:** on-the-go and remote employees may expose data



Additional Security Factors to Consider for WFH

- Homes were never designed to be cybersecurity perimeters.
- Secure wired and wireless home networks.
- Change the default passwords.
- Restrict access to known or white-listed devices.
- Isolate other IoT devices from corporate devices.
- Unplug Alexa and Google Assistant and keep mobile phones from having active Facebook sessions.
- Refresh security awareness programs.
- Revisit programs for reporting security events and potential threats.
- Use strong authentication.
- Does the employee need a separate work printer and/or shredder?
- Reinforce best security practices with regular and recurring employee training programs.

Securing Print in the WFH Environment Adds New Wrinkle

Organizations have moved quickly to institute work-from-home mandates in response to the COVID-19 pandemic. Newly installed remote employees have scrambled to equip home offices with the IT components needed to perform their daily jobs. Some office equipment, such as laptops and monitors, can be easily transplanted to the home environment. But printers and other devices are a different story. Many organizations have encouraged employees to use their own consumer printing devices, while others have allowed employees to purchase new machines, often with little guidance provided.

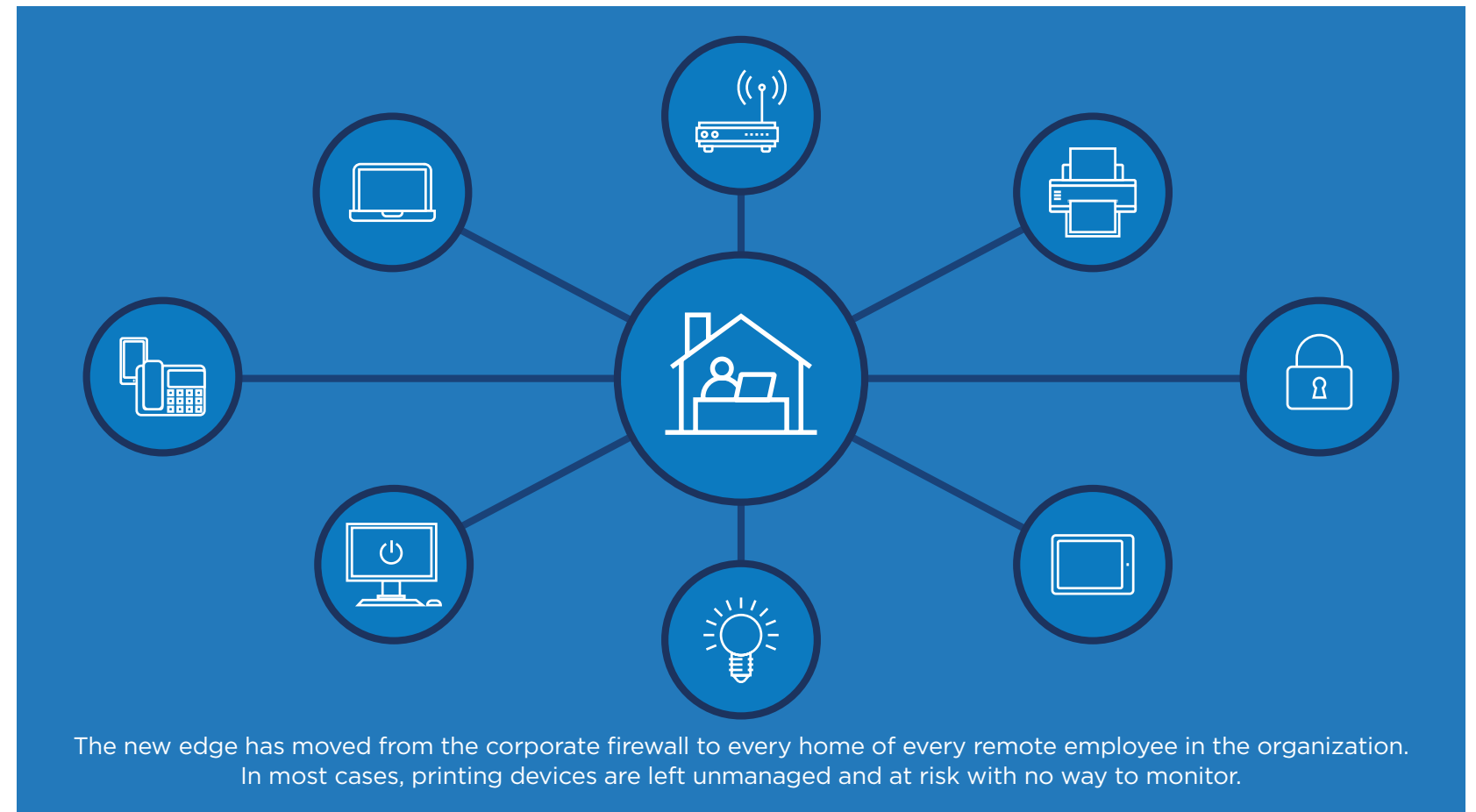
As remotely installed “endpoints” connected to the corporate network, these newly installed home printers pose security threats that most organizations fail to recognize.

By moving quickly to adapt to the evolving workforce, companies have introduced new security risks, losing visibility and control of sensitive customer information and creating data compliance dilemmas. Some employees could be managing customer data in noncompliant ways,

while others might be aware of the risk but decide to print anyway due to lack of options.

Remote workers desire a printing experience similar to what was achieved in the corporate

environment. At the same time, IT needs to ensure that remote printing devices are well aligned with corporate governance and security/compliance policies. Much of this comes down to doing the basics: **cyberhygiene**.



The Vital Steps Toward Print Security

Securing the print environment in both home and office locations becomes a heightened necessity in the “next normal” for business operations. Features designed to provide endpoint security protection for printing devices are important. However, organizations looking to develop a comprehensive print infrastructure security strategy should seek out solutions and services to extend protection well beyond the device.



Solutions Available to Ensure Print Security

IDC believes that the most successful print security initiatives should start with a comprehensive strategy to address the risks of print security wherever work is done — home and/or corporate environments. IDC encourages organizations to leverage expertise from print vendors who understand the unique needs for print-related security.



Device-Level Protection

- Device malware protection
- Detection and automatic system recovery from attacks: Initiate a self-healing device reboot and recovery to secure runtime state without requiring IT or admin intervention
- BIOS, operating system, and firmware updates and password management
- Hard disk and removable storage media protection



Print Management and Content Protection

- User authentication and authorization
- Content security, privacy, and data integrity (hardware and software)
- Remote, BYOD, and mobile printing



Ongoing Monitoring and Management

- Security event management
- Round-the-clock monitoring and management of intrusion detection systems and firewalls
- Overseeing patch management and upgrades
- Performing security assessments and security audits
- Installation, configuration, and usage of equipment
- Remote, BYOD, and mobile printing
- Regular security assessments

The Bottom Line

Print needs to be a critical part of the IT security strategy. At the same time, organizations need to gain better visibility into the print devices installed in remote/home locations. Securing sensitive business information becomes more critical as the line between home and office work continues to blur.

Without the correct control measures in place, attackers can exploit the lack of attention given to printer security in the home environment.

The print environment is unique because it is leveraged specifically to manage data, documents, and information in both digital and paper format, so business-critical content is exposed and vulnerable in a variety of ways. Neglecting to secure the broader print environment (home and office) as part of an overall IT strategy leaves an organization as vulnerable as if it were taking no IT security measures at all.



Security breaches are costly:

- A security breach will use significant employee time and costs to remediate.
- Revenue-generating opportunities may be delayed or canceled in order to deal with a security breach.
- Financial penalties could be incurred for noncompliance or lawsuits from a breach of client/customer confidentiality.
- An organization's brand or bottom line could suffer financially from a tarnished reputation due to bad publicity.



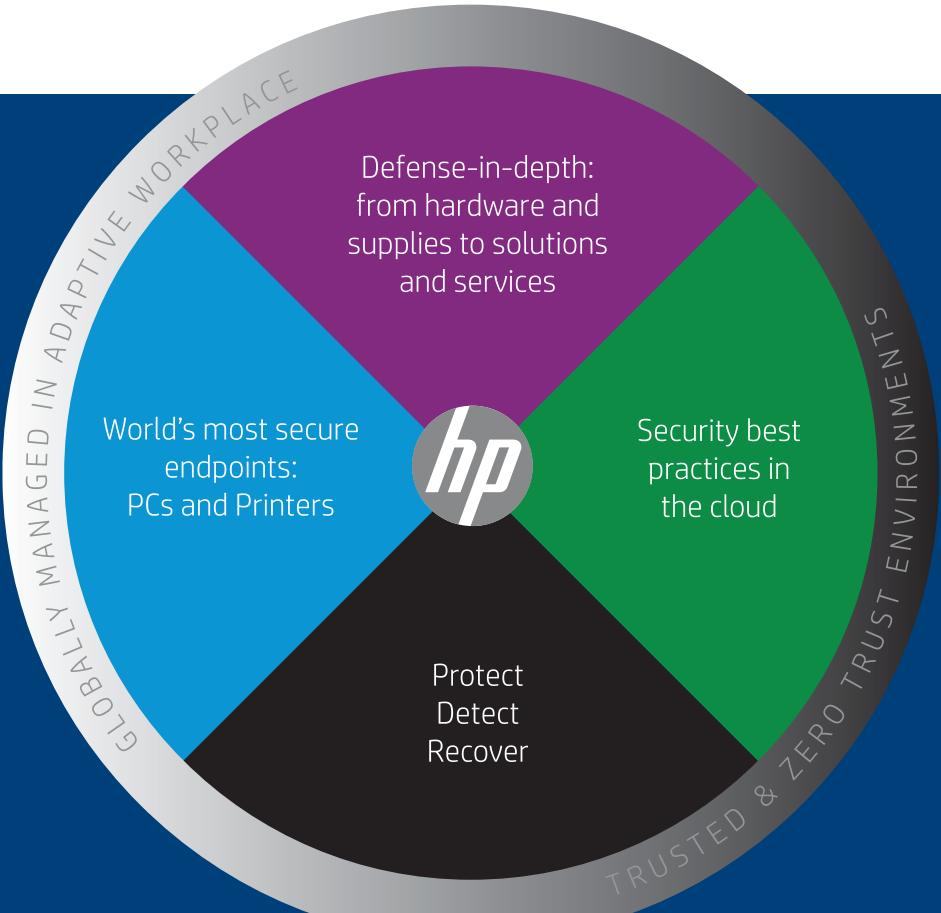
Benefits of a print security program:

- Risk mitigation is addressed with a comprehensive security initiative inclusive of IT and print programs.
- Increased IT efficiency is gained by lowering security breaches and incidents.
- The organization has the assurance of a protective management program for sensitive information.

MESSAGE FROM THE SPONSOR

HP CYBER RESILIENCY FRAMEWORK

Stay ahead of security risks especially with this new distributed workforce — whether your workforce has returned to the office, or continues to work from home, HP can help — detect, protect and recover from security risks. HP has decades-long history of establishing industry security standards and innovations across compute and print. Please consider the following HP Cyber Resiliency framework when evaluating your current security infrastructure.



HP is the only print vendor that has a professional security practice that helps our customers identify, design and implement strong security policies globally. Recognize the risks and contact HP for help.

For more information please visit our print security website, [here](#).