IBM Newsroom

IBM Security Study Finds Employees New to Working from Home Pose Security Risk

X-Force Red Expands Testing Practice to Help Organizations Strengthen Work from Home Security

CAMBRIDGE, Mass., June 22, 2020 /PRNewswire/ -- IBM (NYSE: IBM) Security today released findings from a study focused on the behaviors and security risks of those new to working from home (WFH) during the COVID-19 pandemic. The study shows more than 80% of respondents either rarely worked from home or not at all prior to the pandemic, and, in turn, more than half are now doing so with no new security policies to help guide them. This shift to working from home has exposed new security risks and has left nearly 50% of those employees worried about impending cyber threats in their new home office settings.

Now that **more than half** of the U.S. population is working from home—and a large percentage is expected to continue to do so through the rest of 2020 and beyond—many companies may be playing catch-up as they attempt to manage the security risks of rushed remote-work models. Business activities that were once conducted in protected office environments, and monitored under specific policies, have quickly transitioned to new, and potentially less secure territory. For example, customer service agents who worked in closely managed call centers are now managing sensitive customer data at home.

As a result, IBM X-Force Red has expanded its security testing practice to help companies identify potential blind spots in the work from home world and assist them in designing secure frameworks. The practice will look at key areas including systems that risk exposure of intellectual property, client and employee data, as well as collaboration tools such as video conferencing platforms, and file sharing platforms.

"Organizations need to use a risk-based approach with work-from-home models, then reassess and build from the ground up," said Charles Henderson, Global Partner and Head of IBM X-Force Red. "Working from home is going to be a long-lasting reality within many organizations, and the security assumptions we once relied on in our traditional offices may not be enough as our workforce transitions to new, less controlled surroundings."

No Support for Newbies Creates Opportunity for Cybercriminals

The rapid shift to working from home has also changed the ways many organizations do business from moving face-to-face meetings to video conferencing calls to adding new collaboration tools—yet the survey showed many employees are lacking guidance, direction and policies.

Sponsored by IBM Security and conducted by Morning Consult, the IBM Security Work from Home Survey is comprised of responses from more than 2,000 newly working remotely Americans. Key findings include:

- **Confident, Yet Unprepared:** 93% of those newly working from home are confident in their company's ability to keep personally identifiable information (PII) secure while working remotely, yet 53% are using their personal laptops for work – often with no new tools to secure it, and 45% haven't received any new training.
- **Lacking PII Guidelines:** More than half have not been provided with new guidelines on how to handle highly regulated PII while working from home. This is despite more than 42% of people who manage PII as part of their regular jobs now doing so at home.

- **Policy Awareness:** More than 50% of respondents don't know of any new company policies related to customer data handling, password management and more.
- **Personal (Unprotected) Devices in Use**: More than 50% of new work from home employees are using their own personal computers for business use, however 61% also say their employer hasn't provided tools to properly secure those devices.
- **Passwords Lacking Protection:** 66% have not been provided with new password management guidelines, which could be why 35% are still reusing passwords for business accounts.

Expanded X-Force Red Remote Work Security Testing Practice

X-Force Red has expanded its security testing offerings to help all organizations test and strengthen their security posture and to specifically address those that are new to remote workforces. With more than half of surveyed new work from home employees lacking the training and policies needed to secure critical business operations, this expanded practice can help organizations fill crucial security gaps.

- **Remote Work Adversary Simulation:** leverage X-Force Red's Adversary Simulation services with expanded remote work scenarios designed to test the detection and response effectiveness of remote blue teams and incident response playbooks not originally designed with a dispersed workforce in mind. These simulations can include advanced attacks targeting multi-factor authentication (MFA), VPN, and Single-Sign On (SSO) portals, compromised employee laptops or remote access credentials, ransomware on employee or BYOD devices, or the robustness of remote access controls.
- **WFH Application Penetration Testing:** building on the existing X-Force Red Penetration Testing program, this expanded offering will focus on testing the security and business controls of remote access applications, collaboration tools, and call center management applications for organizations new to work from home models. This includes testing all remote collaboration tools and practices, which will consist of reviewing video conference policies and practices, file sharing controls and default settings, policies to secure sensitive meetings, procedures to help remediate meeting breaches and ensuring that applications that use PII are being deployed securely. This expansion will also include increased remote delivery of these services to address new business demands in today's climate as well as future scenarios that arise.
- **Phishing Exercises:** these exercises will focus on phishing and social engineering to pinpoint remote employees' weaknesses. X-Force Red Social Engineering testing will simulate phishing attacks on employees, conduct social engineering and open source intelligence (OSINT) activities and provide training and recommendations based on the outcomes. Employees will be trained on how to detect and respond to a range of tactics, including email and voice phishing, the use of OSINT data and more.

To download the full report of the survey results, go to:
https://newsroom.ibm.com/image/IBM_Security_Work_From_Home_Study.pdf

For more information on X-Force Red go to: IBM.com/xforcered

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130

countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contact:
Kim Samra
IBM Security
ksamra@ibm.com
510-468-6406

SOURCE IBM
