MERCER TALENT ALL ACCESS®

The exponential surge in the numbers of employees working from home (WFH) during the COVID-19 pandemic is increasing organizational cyber risk in terms of overall number of potential threats and the potential impact of those threats.

Don't forget your cyber risk sentries

By Mercer's Karen Shellenback

Every home device or wireless connection is a potential cyber risk entry point, yet for many employers maintaining business continuity through secure WFH networks is more important than ever.

Not only has the number of risk vectors increased but unpredictability is creating some chaos in terms of normal IT processes and situational decision making among both WFH employees and cyber risk staff — potentially leading to exposed loopholes. The tsunami of rapid response required of businesses to distribute their all workers, with less than five day's notice, has opened potential holes in the firewall for many organizations — holes that nefarious entities are continuously trying to exploit.

IT, cyber risk staff

The situation is of course, exacerbated by the sheer number of at-home workers but also the stressors placed on IT and cyber risk staff to supply and support new remote modes of working. Cyber and IT staff in normal operating environments are under tremendous stress — their jobs often require monotonous technical work and dedicated attention spans. Under these new conditions, IT and cyber teams are operating on over-drive.

The unprecedented "stay home, work safe" situation has created further strains on over-stretched cyber risk and IT staff that can lead to more compromised risk and security breaches. Malicious actors are aware of and taking advantage of situational weak points.

Pandemic-related cyber challenges:

Normal security protocols and cyber hygiene practices are set aside. Immediate WFH measures can create situations in favor of rapid response setting aside security protocols. New hardware and software systems in these environments may have been deployed with reduced security. Most organizations did not pre-plan, run pandemic contingency scenarios, and stretch-test their technology and protocols for the sheer breadth and depth of the current situation.

Use of personal devices for work/business. While the good news is only 3% of corporate executives report that their organizations reduced security requirements for universal WFH, it seems that in one-quarter of organizations across the globe, IT and procurement could not handle the extra load in terms of buying or renting new laptops and therefore have allowed employees to use their personal technology at home for work. (Mercer COVID-19 survey live results.) This creates a potentially risky security challenge.

Overworked staff due to increased IT tickets/caseload. In addition, the IT team is tasked with immediate tech support resolutions for the hundreds or thousands of staff now using new systems and processes remotely. While everyone is adjusting to new modes of working, the workload for IT and cyber risk teams just became infinitely harder to manage. In this environment, shortcuts executed by overworked and tired IT/cyber risk staff is a concern.

Absences due to sickness or stress. Not only are IT and cyber staff responsible for getting potentially thousands of workers set up to work from home on new laptops and possibly new collaboration tools, but they must execute this work on top of normal cyber and IT responsibilities. A further challenge is absence due to stress and potential sickness of IT/cyber team members. "Organizations should prepare for temporary or permanent loss of key cyber staff and leadership, the evacuation of a Security Operations Center, or a serious attack where only a portion of staff are able to work". (2020, Marsh and McLennan Companies, Cyber Risk Grows as COVID-19 Spreads.)

Financial setbacks may lead to reduced cyber budgets. Everyone is squeezed and budgets are tight or gone. Corporate financial setbacks can negatively affect cyber risk staffing and the prioritization of new effective technologies needed to mitigate the ever-changing risk environment.

Support from third party vendors may be reduced or impacted. Furthermore, third party vendors who supply technology and other SaaS services are also experiencing similar stress among their IT/cyber, customer service, and relationship management teams. Resolution of issues may take longer, patches may not be deployed, and again, some minor security protocols may be ignored in favor of the fastest, most expedited solution. Leadership needs to address these potential liabilities with all vendors.

If an attack occurs, incident response may be impacted. On top of all the above challenges, the impending danger of an imminent attack weighs heavily on the team. Companies are especially vulnerable given that it may take extra time to recognize an attack and/or respond in an optimal timeframe (compared to normal circumstances). Delays in response time creates exponential brand damage and financial loss.

COVID-19 recommended cyber risk and IT staffing tasks

Your cyber analyst and tech team are on the front lines mitigating the myriad of challenges. During the pandemic, the following are extra cyber risk protocols recommended for a widespread WFH business environment:

- Implement VPN (virtual personal networks) and MFA (multi-factor authentication) for all remote systems on distributed networks
- Include threats from insiders in risk assessments, especially those with WFH set-ups
- Ensure you have the people, processes, products (technology) to detect and respond to threats and risk across the full remote network
- Ensure remote access systems are fully configured, updated, and patched. Maintain the same overall security landscape for WFH networks as the traditional onsite configuration
- Run phishing campaigns to assess the current security landscape and uptake on the remote network
- Use endpoint detection and response (EDR) software to quarantine systems remotely if there is a breach
- Craft a secure remote access plan for privileged users. Track the access and use of highly sensitive/ confidential accounts
- Ensure that the system access provided to employees is the minimum required for each role and function. Monitor access in the event of changes in jobs and locations
- Deactivate sensitive system access following employee termination and after employee role changes
- Use automated auditing software to track employee activity, establishing a baseline of "normal" activity against which unusual attempts at computer or file access can be measured. Monitor and audit employee network activities and suspicious behavior (logging on at odd hours, impossible locations, significantly increased export of reports from internal systems, regular access of unauthorized cloud storage sites, and no collaboration on this workload with others, etc.)
- Use data analytics software to scan email and social media posts to flag "disgruntled" employees. Look for potential malfeasance among "at-risk" employees and discuss scenario planning to address "at-risk" or "on-notice" employees with HR. The equipment of terminated employees may not be returned after termination — focus on terminating access to networks and systems

Supporting IT and cyber risk staff

Awareness of pandemic-related cyber challenges can help organizational leaders support the critical talent and crucial processes within the cyber risk/IT function. Understanding the current talent pool, future capabilities required, current cyber professional stressors and needs, as well as turnover lures are priorities. HR is in the trusted advisor position to help cybersecurity leaders attract, retain, and build a competent and driven cyber workforce.

HR must carefully monitor competitive rewards, benefits, and the overall working environment as cyber staff are highly targeted and can be recruited away if not supported. HR can play an active and critical role in mitigating turnover, absences, sickness, and productivity losses among this crucial operations group by:

- Leveraging strategic workforce planning metrics to understand talent flows, bench strength/skills inventory, and talent pipeline of the IT/cyber risk team(s)
- Planning and executing strategic retention strategies — reviewing competitive salaries per role, and considering "combat" bonuses, retention bonuses, etc. Be aware of dark web brokers (MaaS (Malware-as-a-Service)) positioning potential lucrative opportunities for cyber staff to "go dark"
- Working with cyber-leaders on flexible manager skills to effectively coach, develop, and mentor cyber staff
- Understanding and action planning for current cyber team engagement levels. Monitoring stress, burnout, and unhealthy work practices to mitigate these challenges
- Supporting certification, recertification, and online training for security professionals
- Deploying enticing career path trajectories for all levels of cyber staff. Focus on creative career growth opportunities that align with career goals, passions, and personal aspirations
- Providing mentorship, sponsorship and/or and "visibility" opportunities for underrepresented cyber talent
- Developing innovative community collaboration techniques, design challenges, relevant games, hackathons, or crowd-sourced approaches that can be deployed after the immediate crisis is over to engage cyber staff in new learning and skill development opportunities
- Building line of business experience by providing opportunities for cyber staff in areas such as business strategy, pragmatic negotiations, legal considerations, delivering impactful, and strategic presentations — that again, can be deployed after the immediate crisis is over to help analysts learn leadership skills and enable their advancement

What can corporate leaders and HR do to reduce internal and external cyber-threat vectors during the pandemic? Beyond revision of cyber-governance practices among the executive leadership team, HR plays a significant role in supporting cyber risk and IT staff.

Cybercrime is growing at a furious pace, costing organizations trillions globally and this cost is expected to increase to $6 trillion annually by 2021 (Cybersecurity Ventures). The chance of avoiding an attempted breach is almost nonexistent, but the odds of preventing a successful breach will increase with executive and HR leadership attention to the areas discussed in this article (and the complementary Mercer TAAP+ article on Insider Risk). HR can demonstrably contribute to corporate security through the development of a specific WFH risk mitigation plan (in partnership with the cyber risk leadership team), educating employees on cyber risk, hiring the best and dedicated cyber talent, and fostering the healthy engagement and development of cyber staff.