June 8th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining a workforce study that shows just how significantly COVID-19 has shifted the work setting expectations and preferences of younger generations. We outline why organizations should assess how remote work alters the cybersecurity, privacy, and legal risks they face. Next, we take a look at how the changing geopolitical and technological environment may increase the potential for cyberattacks that seek to disrupt an organization by targeting personnel. Welcome back to *Hacking Healthcare*.

1. **Study Highlights Generational Differences in Work Setting Preferences**

   A new research report from Citrix Systems suggests that Millennials and Generation Z, the 'born digital' generations, have distinct preferences for how they want to work. The most significant takeaway might be just how conclusively these generations (and likely those to come after) are averse to returning to full time on-premises office work. These preferences are likely to place pressures on, and increase expectations for, organizations to implement hybrid or fully remote work policies in order to attract new talent and retain existing personnel. With that in mind, it may be time for organizations to consider what these changing expectations could mean for cybersecurity and privacy if hybrid models are to become the new normal.

   Entitled *Work 2035: The Born Digital Effect*, the study set out to examine the "values, career aspirations and working styles" of those born after 1981.[1] The study, which is the product of 3,000 interviews conducted between 2020 and 2021, covered the attitudes of workers and business leaders in France, Germany, the Netherlands, the United Kingdom, Mexico, the United States, the United Arab Emirates, China, India and Japan.[2] It looked primarily at the financial services, healthcare and life sciences, technology, professional services, manufacturing, and retail sectors.[3]

   While the full 46-page study tackles several issue areas and highlights some important differences between workers and business leaders, some of the largest disparities centered on work setting preferences. Significant takeaways in this section from workers in the younger generations include:[4]

   - Only 50% of employees believe they are most productive in the office
   - Only 37% of employees believe they are most creative in the office

- Only 17% of employees believe the office is the best work setting for their wellbeing – as opposed to 60% who selected at home
- Only 25% of employees want to go back to a traditional 9-to-5, five days a week
- Only 10% of employees want to work in an office full time – as opposed to 29% of employees wanting to work at home full time, and another 22% of employees wanting a hybrid model with most of their time at home – these contrast significantly with what business leaders think their employees want (24% office full time, 5% home full time)

Action & Analysis
Included with H-ISAC Membership

2. Non-traditional Cyber Risks

2020 and 2021 have been marked by a concerning array of cyberattacks that have continually pushed back the boundaries of what is considered acceptable behavior in cyberspace. Healthcare networks, water treatment facilities, transportation networks, gas pipelines, and other critical infrastructure sectors have been repeatedly attacked and have dispelled the notion that cybercriminals and nation-state actors would temper their activities to non-critical targets and traditional espionage endeavors.

It is worth considering how this more permissive environment, when paired with increased geopolitical tensions, could lead malicious actors to become more creative and bold in their cyber operations. This could lead to situations where an organization's personnel may be the target of a cyber-enabled physical attack, or an attack designed to disrupt business operations beyond just ransomware and data breach scenarios.

Consider the following examples:

- An organization holding an executive retreat is targeted by a cyberattack that knocks out or severely disrupts transportation and the ability of those executives to leave and return to the office. This leaves the organization with strained access to a large percentage of senior leadership – perhaps it is a resort that relies on a ferry,[5] or has limited internet and communications that suddenly are no longer available.
- An organization's offices are hit by a cyberattack that disables or damages the air conditioning of the building during the height of Summer. The sweltering heat creates difficult to impossible work conditions on-premises.
- An organization in a heavily commuter dependent area finds the local/regional subway/bus system has been disrupted by a cyberattack, and a large

percentage of employees suddenly no longer have a means of transportation to get to work.

This list could go on-and-on and will only get longer as the separation between the physical and digital worlds continues to disappear. For many organizations, these types of situations are addressed as part of business continuity planning and operations, and those policies will need to continue to evolve along with the threats.

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, June 8th:
- Senate – Committee on Homeland Security and Governmental Affairs: Hearings to examine threats to critical infrastructure, focusing on examining the Colonial Pipeline cyberattack

Wednesday, June 9th:
- Senate – Committee on Appropriations: Hearings to examine proposed budget estimates and justification for fiscal year 2022 for the Department of Health and Human Services

- House of Representatives – Committee on Homeland Security: Hearing on Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure

Thursday, June 10th:
- Senate – Committee on Finance: Hearings to examine the President's proposed budget request for fiscal year 2022 for the Department of Health and Human Services.

- Senate – Committee on Homeland Security and Governmental Affairs: Hearings to Examine the nomination of Jen Easterly, to be Director of the Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, and Chris Inglis, to be National Cyber Director.

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/work-2035-the-born-digital-effect.pdf
[2] https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/work-2035-the-born-digital-effect.pdf

[3] https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/work-2035-the-born-digital-effect.pdf
[4] https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/work-2035-the-born-digital-effect.pdf
[5] https://www.nbcboston.com/news/local/mass-steamship-authority-still-impacted-by-cyber-attack/2399217/