GEORGIA TECHNOLOGY AUTHORITY

IT Issues for Hybrid Work

Jeff Deason
GTA Office of Information Security
Section Director: Governance, Risk and Compliance

OUR VISION

A transparent, integrated enterprise where technology decisions are made with the citizen in mind

—

OUR MISSION

To provide technology leadership to the state of Georgia for sound IT enterprise management

January 25th, 2023

Georgia Technology Authority Mission & Overview

GTA's mission: To provide technology leadership to the state of Georgia for sound IT enterprise management

GTA Overview: The Georgia Technology Authority (GTA) currently manages the delivery of IT infrastructure services to 89 Executive Branch agencies and managed network services to more than 1,200 state and local government entities. IT infrastructure services encompass mainframes, servers, service desk, end user computing, disaster recovery and security. Managed network services include the state's wide and local area networks, voice, cable and wiring, and conferencing services.

GTA is also responsible for enterprise IT governance and planning which is facilitated by establishing statewide technology policies, standards and guidelines based on industry best practices and federal requirements.

Enterprise cybersecurity is a core function of GTA; in this role GTA uses a cybersecurity risk management framework to enhance IT security programs and advance the states ability to protect sensitive information.

Cyber Stats

- Projected Cyber Crime Costs: $10.5 Trillion (2025); $6 Trillion (2021); $3 Trillion (2015)
- Global Ransomware Damage: $265 Billion by 2031
- 2031: A Consumer or Business will suffer a ransomware attack every 2 seconds vs. every 11 seconds in 2021
- There are nearly 5.3 billion unique mobile phone users in the world today (GSMA Intelligence). Mobile security threats are on the rise: Mobile devices now account for more than 60 percent of digital fraud, from phishing attacks to stolen passwords

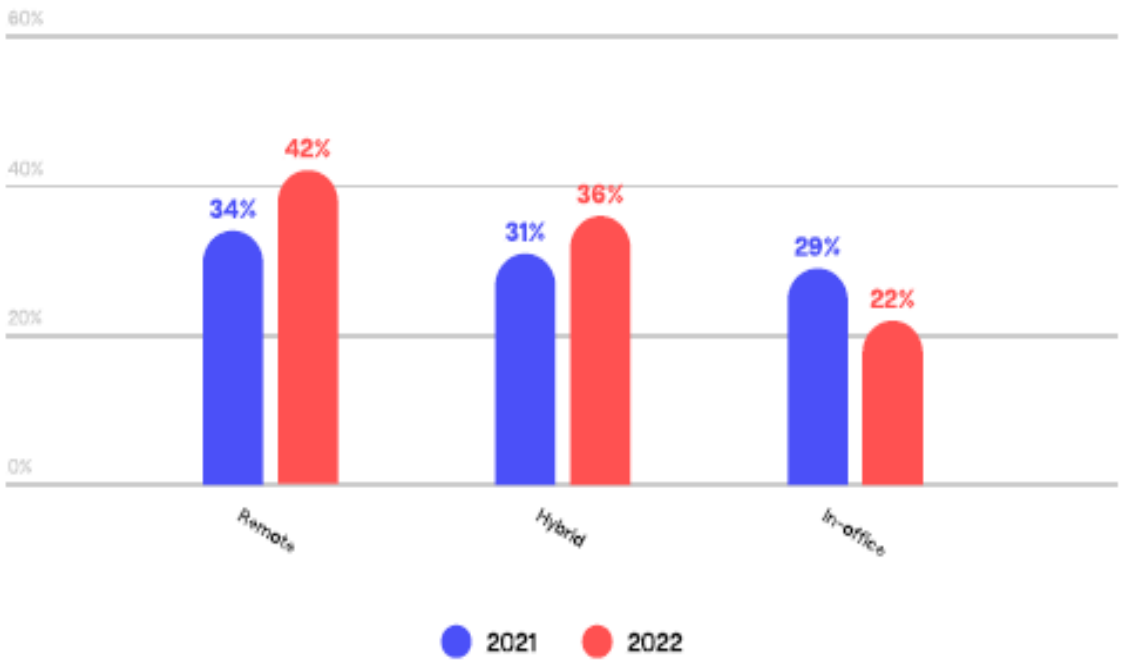
- By 2025, 200 zetabytes of data will need to be protected - 50% of that will be stored in the Cloud
- More than 300 billion passwords were used by humans and machines worldwide in 2021
- The 5 most cyber-attacked industries over the past 7 years: healthcare, manufacturing, financial services, government, and transportation

Sources: CISA.gov; 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics (cybersecurity almanac.com)

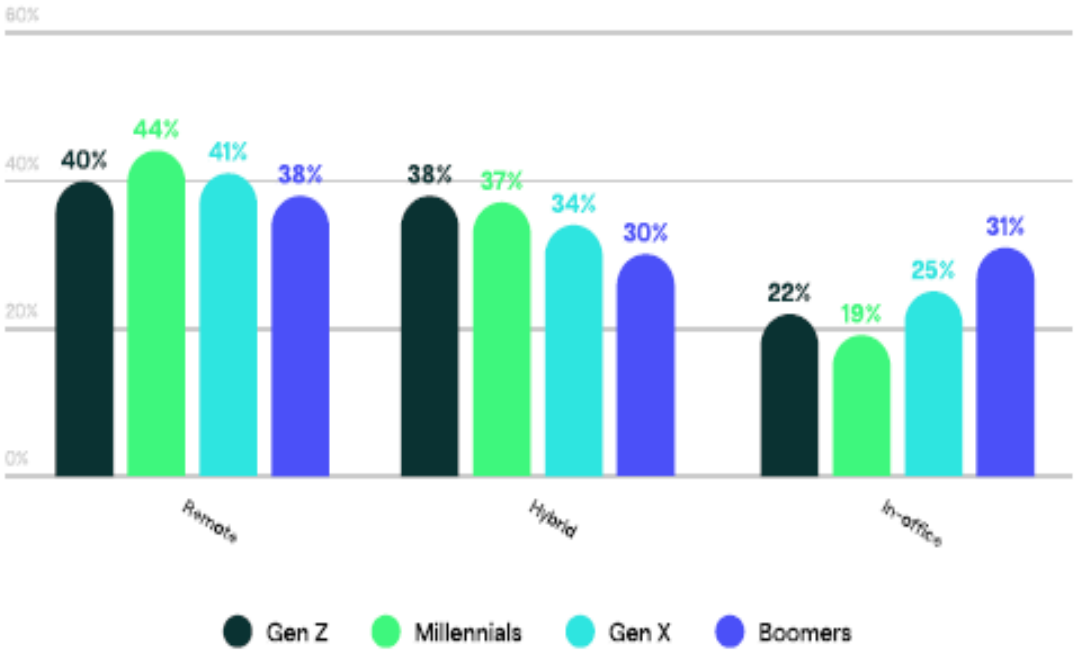
Employee Preferences

- Hybrid work is **a flexible work model that supports a blend of in-office, remote, and on-the-go workers**. It offers employees the autonomy to choose to work wherever and however they are most productive.

Preferred working style year-over-year:



Preferred working style by age:



Sources: State of Remote Work 2022; www.owlabs.com ; Global Workplace Analytics

Challenges of Hybrid Work

- Expanding network boundary and environments introduce new attack vectors and creates a vast attack surface, posing challenges in enforcing security policies and assuring proper authentication.
- Issues with VPNs have become apparent relating to cost, scaling and visibility. Home or off-site networks can be sketchy.
- Workers need to connect to a secure cloud or system. Security measures must have minimal impact on user experience and productivity.
- Detection and mitigation of threats, attacks and anomalies are complicated.
- Lack of visibility and control over remote endpoints can hinder efforts toward cyberresiliency that allow the infrastructure to recover quickly whenever threats and attacks arise.
- Losing data, due to ransomware, malicious internal actors or human error.

Recommendations - to secure an organizations hybrid workforce

- **Update security polices** to reflect employees working remotely to keep data secure no matter where they are working (i.e., implement and enforce policy that requires two-factor authentication; utilize non-disclosure agreements to deter employees from sharing company information).
- **Prioritize security awareness** to provide employee training and awareness on how to protect themselves while working from home or other off-site locations; keep abreast of information security threats, policies and procedures for addressing them.
- **Incorporate Mobile Device Management (MDM)** that secures, monitors and manages end-user mobile devices.
- **Implement Multifactor Authentication (MFA)** so every employee provides two pieces of information to authenticate to the company network rather than asking for only the username and password.
- **Implement data leakage prevention (DLP)** solution as a control against leakage of business-critical information.
- **Virtual Private Network (VPN) Access** to allow secure access for employees working remotely. Should be a secure VPN tunnel between the organization's local network and the employee.
- **Virtual Desktop Infrastructure (VDI)** to run a user's desktop inside a virtual machine that lives on a server in a datacenter (profile settings, installed applications and operating system are stored and managed centrally).
- **Zero Trust network access (ZTNA)** operates based on never trust, always verify; user or device that attempts to connect to the network and resources is automatically untrusted and must be authenticated before access is granted.

Resources

Center for Internet Security

- www.cisecurity.org

Cybersecurity and Infrastructure Security Agency

- www.CISA.gov

NIST – National CyberSecurity Center of Excellence

- www.nist.gov/cybersecurity
- www.nccoe.nist.gov

Jeff Deason, *CISSP, PMP, CRISC, SP, ITIL, ZTX-I*
Office of Information Security
Section Director, Governance, Risk & Compliance
(470) 270-1892 | Jeff.Deason@gta.ga.gov

Georgia Technology Authority
47 Trinity Avenue SW
Atlanta, GA 30334

gta.georgia.gov

Appendix

User Cybersecurity Tips Beyond Office

- When utilizing Wi-Fi, ensure you only connect to known and secured networks. If use of public wi-fi becomes a necessity for connectivity, ensure that you explicitly ask the hosting organization (e.g., library, coffee shop) for the correct network to join. Be mindful of shoulder surfing and do not leave printed documents on public printers where they can be seen by unauthorized individuals.
- Use strong passwords, passphrases, and multi factor authentication when accessing sensitive data
- Be aware of suspicious emails and activity
  - Report suspicious emails and activity to the appropriate person or organization
  - If you ” See something, Say something “
- Properly destroy unwanted data
- Keep security software up to date and devices patched
- Never leave devices unattended
- When traveling with your portable device, ensure that you always keep it in your physical possession.
- Explicitly log out of all browser and VDI sessions when not actively in-use, do not just 'X' out of the active window. If you do not log out, others with physical access to your device could gain unauthorized access to agency data.