FRANKLIN COUNTY GOVERNMENT

IT DEPARTMENT BUDGET WORK SESSION

JANUARY 2022

What IT Does Today:

1) Voice Communications (e.g. Voice Over IP).
2) Data Communications (e.g. network connectivity)
3) Wireless Communications (e.g. guest & staff WiFi)
4) Internet Access
5) Help Desk Support
6) Enterprise Application Support (Munis, Energov, PCI)
7) Checks, W2, etc. Printing (Schools & County)
8) IT Inventory & Lifecycle Management
9) Technology Project Management
10) Continuously review expenditures for cost savings
    a) Reduced Internet service contract costs (~$25K/year)
        i. Renewed 1/2022 with another $18K reduction
    b) Reduced Microsoft EA contract costs (~$50K/year)
11) Cybersecurity (see next slide)

Ongoing Security Enhancements:

1) Election workstation enclave
2) Firewalls & Geoblocking
3) User Education
4) IT Policies (internal and external)
5) Stale Account management
6) Antivirus/Antimalware upgrades
7) PC (550) and Server (130) Operating System upgrades
8) Remote Access Controls & Two Factor Authentication
9) Microsoft Advanced Threat Protection & Cloud Application Security
10) Microsoft Azure managed security service
11) Tested Cyber Incident Response Plan
12) State & Federal Partnerships
    1) Malicious Domain Blocking Resource via CIS/MS-ISAC
    2) Annual Vulnerability Assessment via National Guard/Va Defense Force
    3) Monthly Web Application Vulnerability Assessments via DHS/CISA
    4) Weekly Perimeter Scans via DHS/CISA
    5) Real-Time inbound/outbound monitoring & alarming via CIS/MS-ISAC

“New” Support Requirements:

Note: Each requires significant cost and staff time

1) Increasing support needs, especially 24x7 agencies
    a) SRO support calls are double from 10 years ago
2) Election Security
3) Legislation Changes
    a) Ray Baum Act
    b) Minimum security standards compliance
4) Increasing Cybersecurity Threats
    a) This is NOT the only thing we have to worry about

Current Challenges / Obstacles:

1) Staffing Level
   - +1 Staff (2009-2012), No increase in 10 years
   - Increases in support requirements + ~50 IT projects
   - Comp Time is used during normal hours (1 day in 6)
2) Staff Wages (across 6 neighbors & 2 partners)
   - Public Sector Neighbors pays 23%-46% higher
   - Private Sector pays 41%-57% higher
3) Cybersecurity Threats
   - >162,000 Alarms per year = ~445 Alarms per day
   - Public Sector average to detect a breach = 190 days
   - Public Sector average to contain a breach = 57 days
   - Public Sector average cost per capita = $75 ($4.2 Million)
4) Disaster Recovery & Continuity of Operations
   - Close gaps between current & required RTO/RPO.

Cyber Security in the Commonwealth (2019 data):

- 30% percent of all incidents were the result of successful malware attacks via phishing emails containing malicious links or attachments and infected website redirection.
- Most malware attacks are financially motivated. Of the top 10 ten malware infections reported by MS-ISAC, six of these were banking Trojans.
- Information disclosure was the second largest category of incidents for 2019. Things like unencrypted emails containing sensitive data, physical documents were misfiled and sensitive information was mailed to the wrong recipient. Information disclosure incidents accounted for 27% of all incidents experienced.
- The top five countries where attacks against the Commonwealth originated were the United States, Netherlands, United Kingdom, Brazil and France. This likely means more attackers are using compromised U.S.-based infrastructure to conduct attacks, which lowers the value of geoblocking to avoid attacks.
- Approximately 30.5 million attack attempts were detected against Commonwealth systems. This is a rate of one attack every 0.97 seconds.

source: https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/docs/2019-Information-Security-Annual-Report.pdf

QUESTIONS ?