Why Cybersecurity is a Heavy Lift for Governments

PICA Assessing a 21st Century Threat: Cybersecurity in Modern Government

Mark Wheeler

Chief Information Officer, City of Philadelphia

October 8, 2019

Office of Innovation & Technology

Atlanta

Ransomware locked multiple IT systems 2018:

- Suspended water bills + license payments and property sales, loss of some Police camera data
- $1.1M worth of PCs and cell phones replaced

Cause: Weak passwords

Cost: + $17 million

Duration: 3-6 months

Some computer systems and data were not recovered

Baltimore

Ransomware impacted IT systems May 7:

- Lost email
- Suspended water bills, property sales and taxes, license payments and renewals.

Cause: Suspected weak passwords

Cost: + $18.2 million

Duration: On-going

2nd ransomware attack on Baltimore in 15 months

Personal computers stored key data, no backup routine

Allentown

Malware infected central IT systems in 2018:

- Disabled all antivirus allowing more malware
- IT had zero documentation on systems owned by Depts or vendors hampering response

Cause: Phishing email

Cost: + $1.2M

Duration: ~ 6 months

No emergency procurement contracts in place to hire "cyber first responders"

Phila FJD

Malware detected and quarantined at City Hall Courts operations on May 21:

- Suspended FJD emails, website, eFile, eClaims, and impacted property sales
- 200+ workstations; 7 servers infected

Cause and Cost: Unknown

Duration: on-going

Malware similar to versions reportedly found in Baltimore

Security Challenges

Overly complex and intertwined ecosystem of IT applications, operations + owners

Unpatched operating systems and applications

Lack of backup and disaster recovery across entire IT ecosystem

Weak continuity of operations plans (COOP)

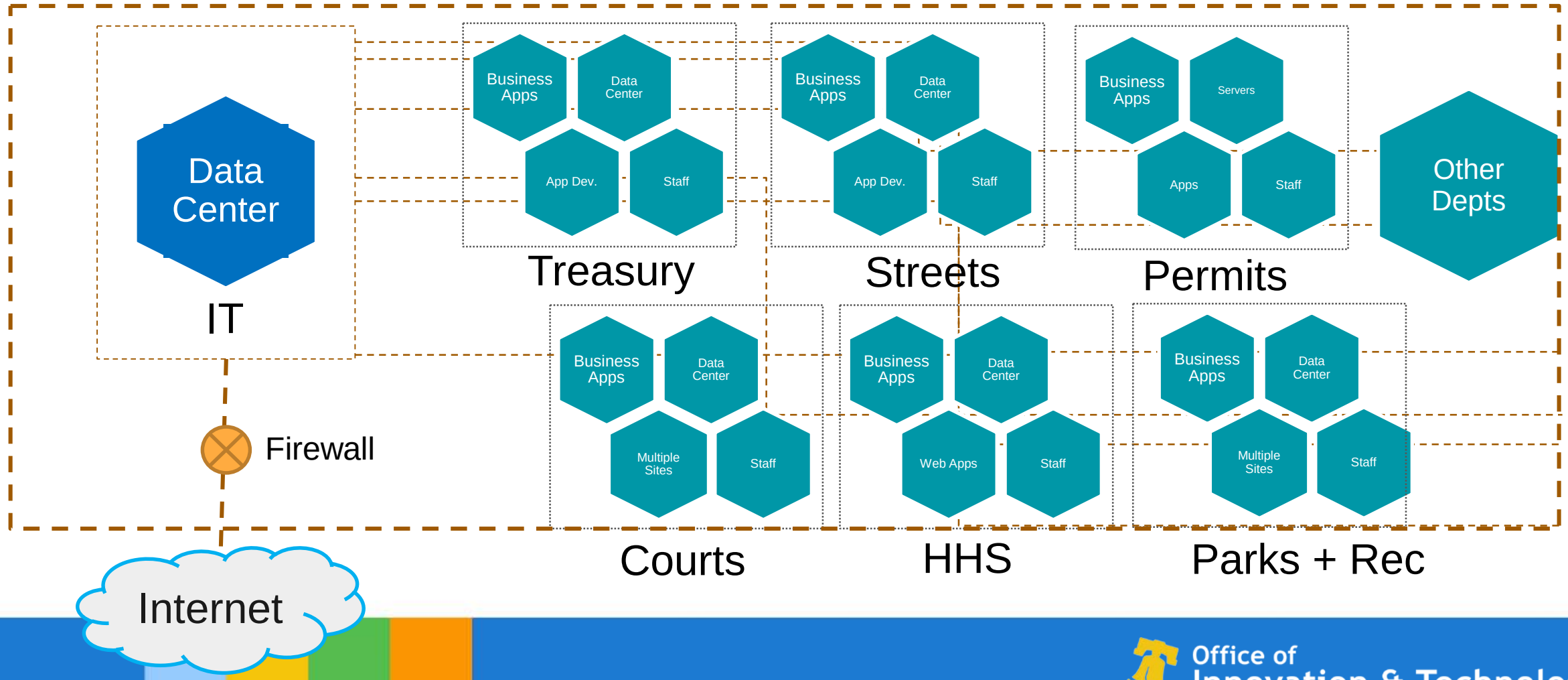
Staffing

Procurement

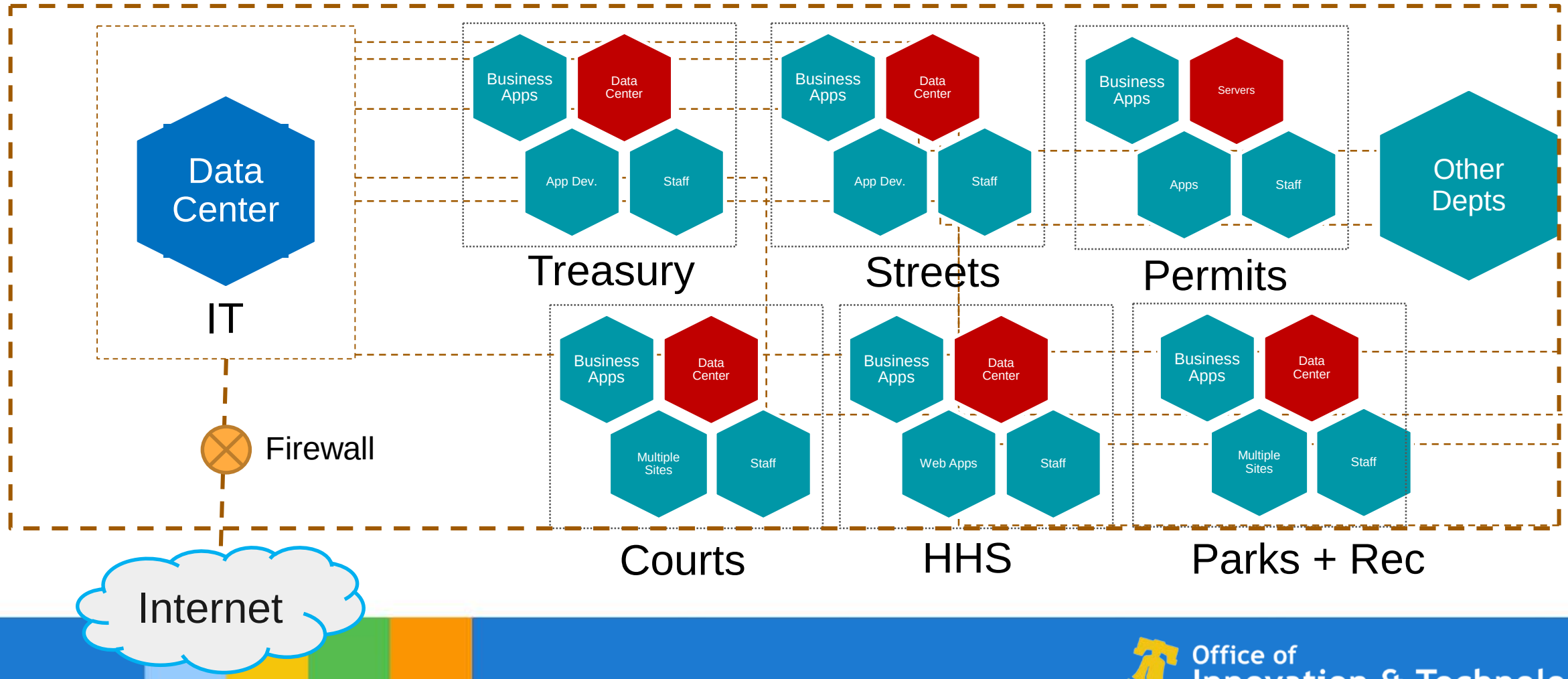
Culture

Budget

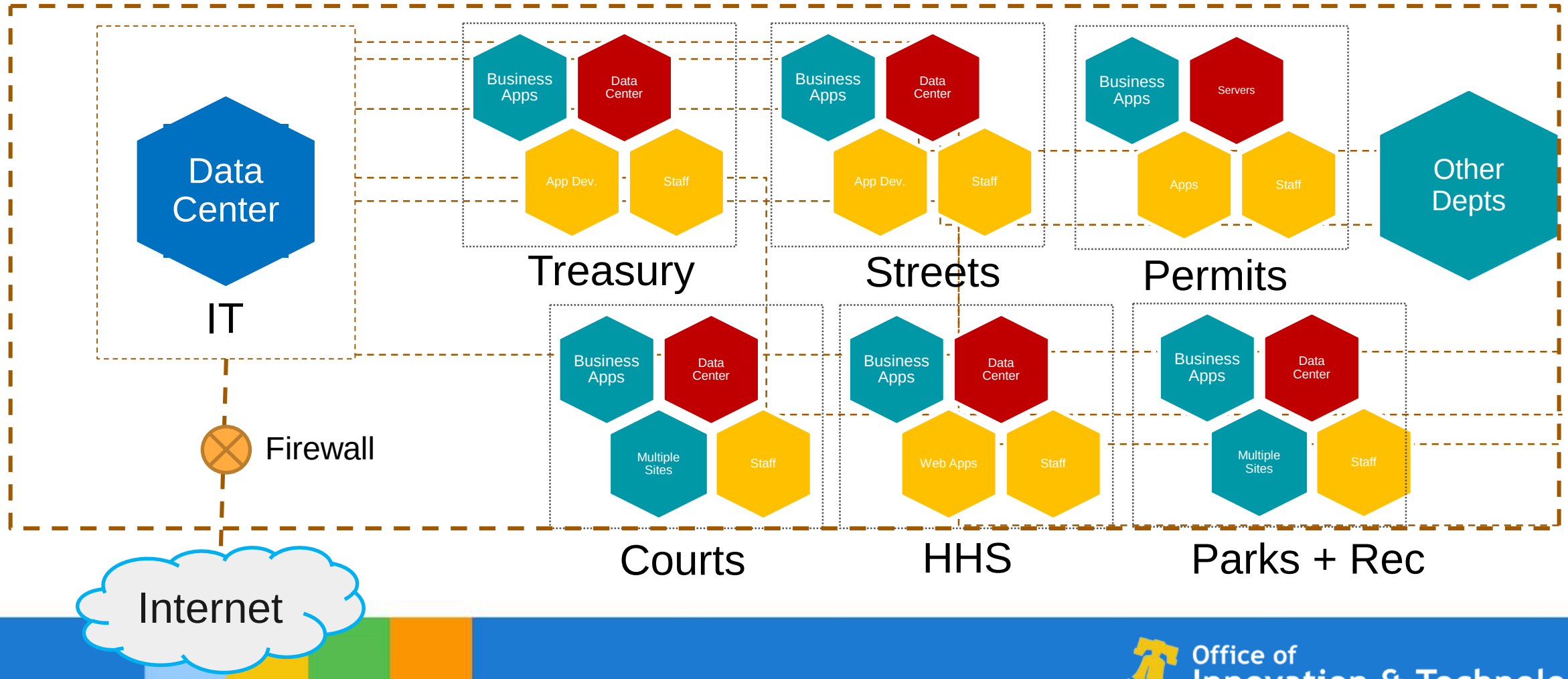
Technical: Federated Network



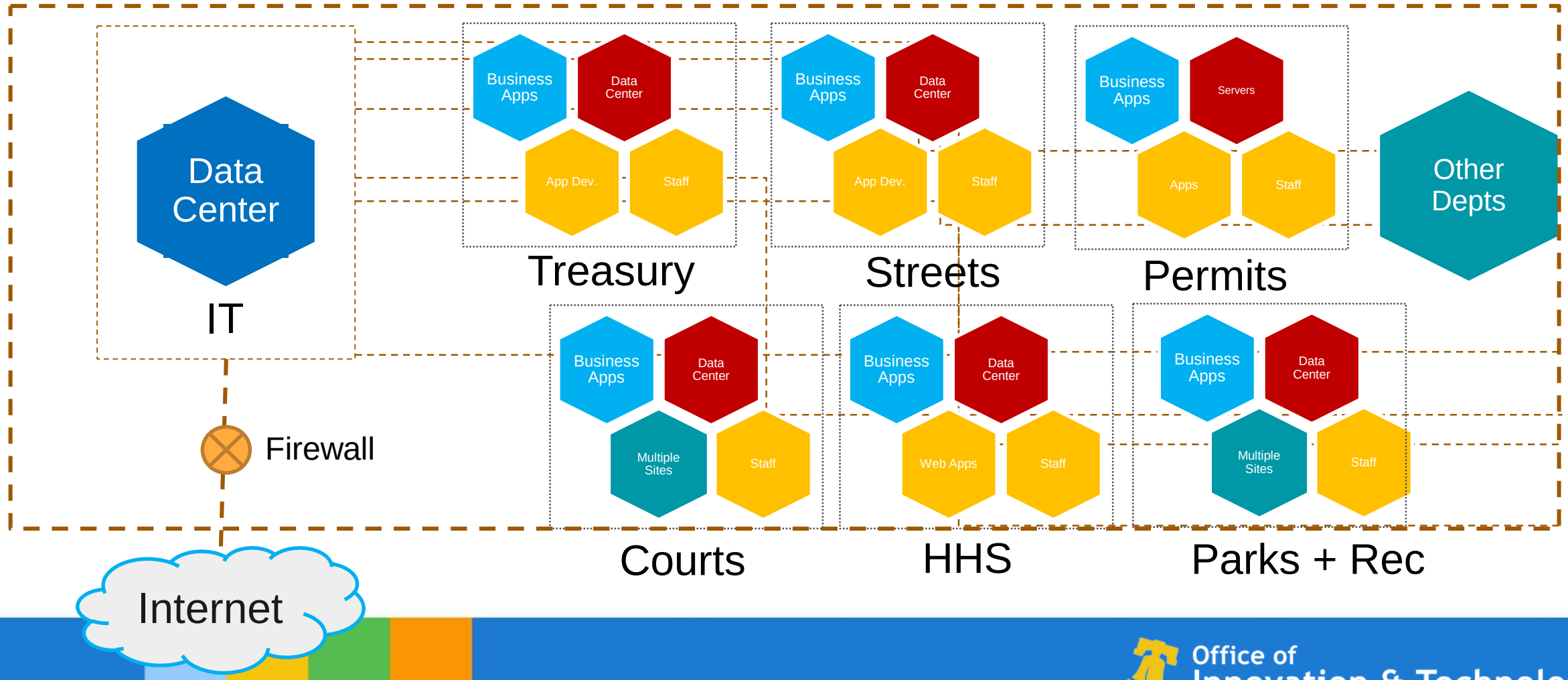
Federated Network = Increased Complexity



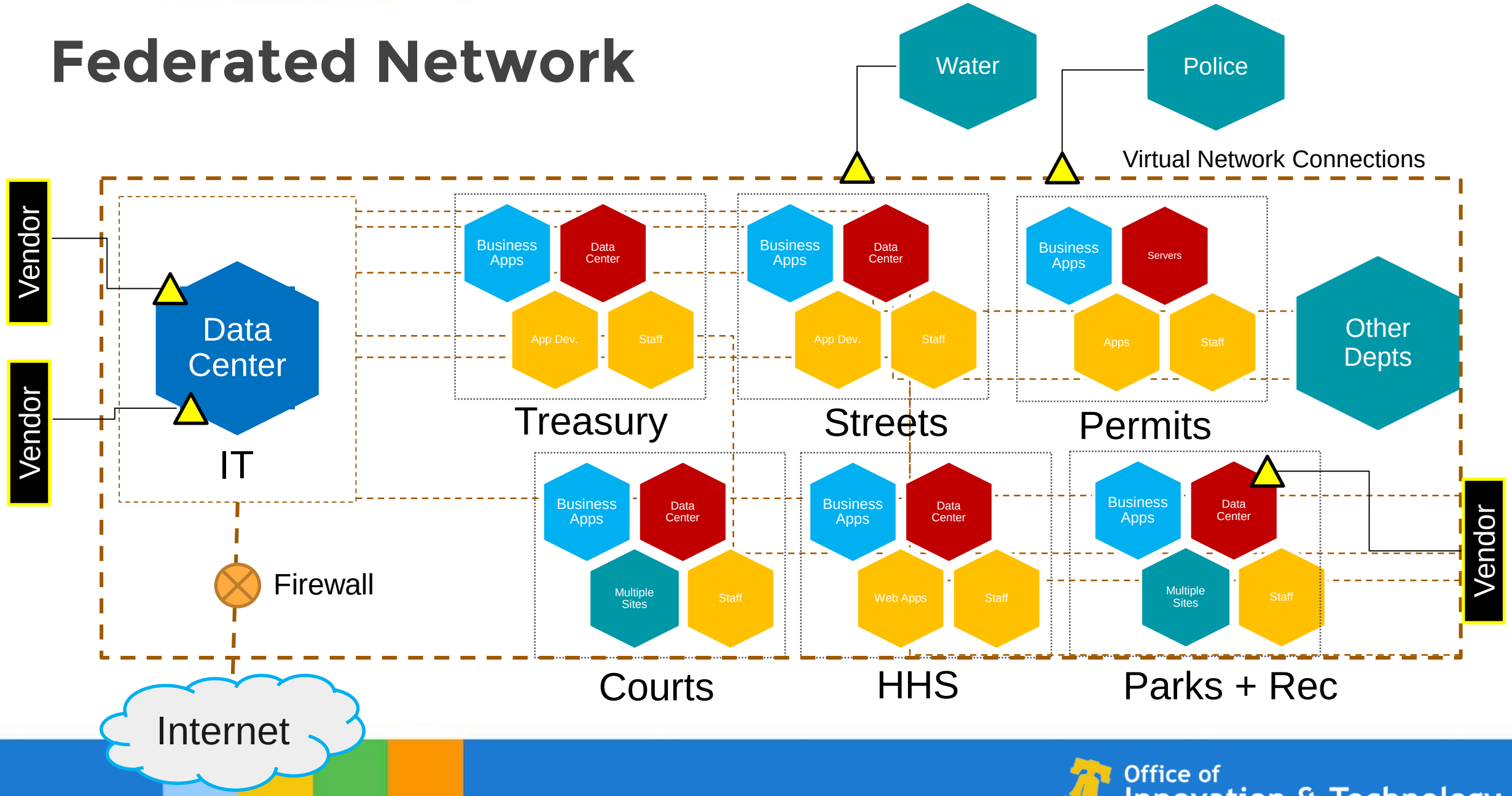
Federated Network = Increased Complexity



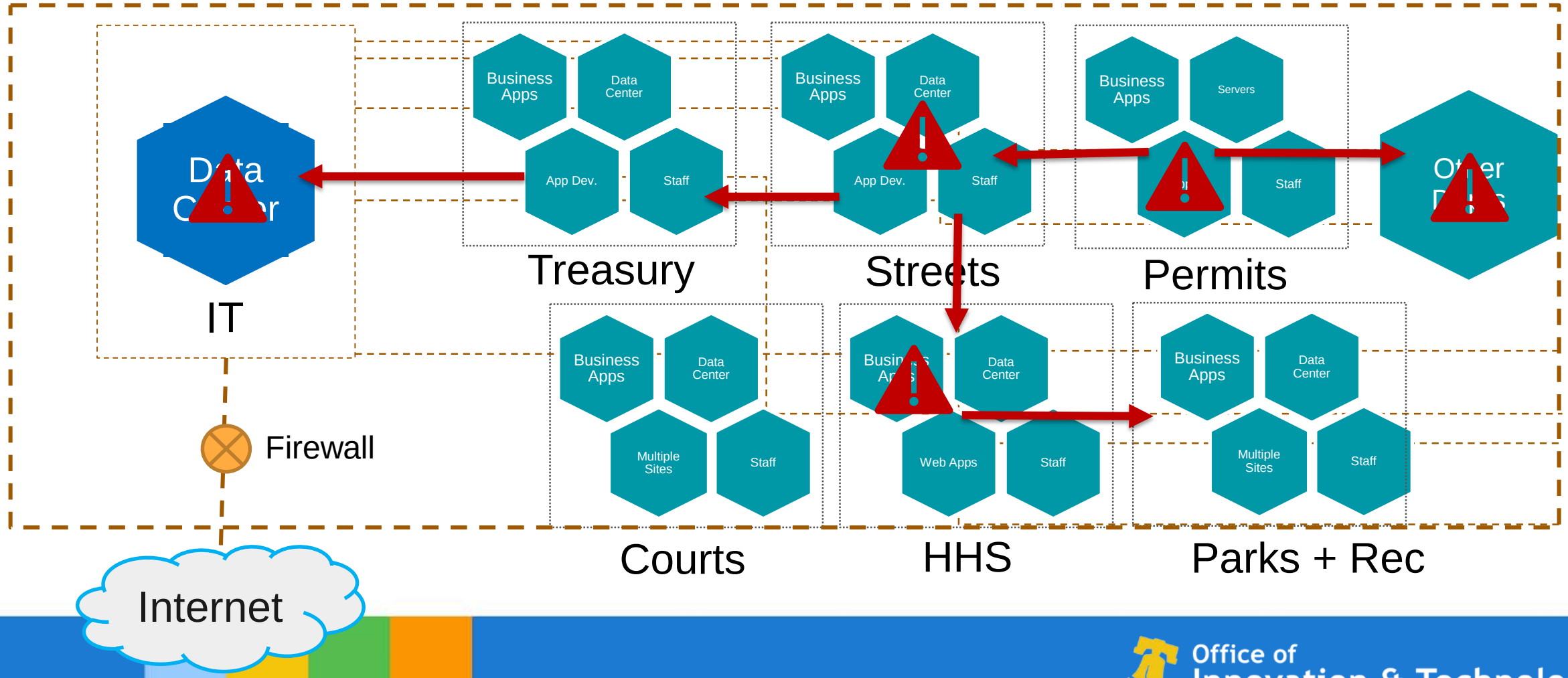
Federated Network = Increased Complexity



Federated Network



Shared Risks



Staffing

- Governments cannot match market rate salaries
- Needed expertise for strategy and execution is not at the entry level
- Residency requirements
- Civil Service rules for hiring may be antiquated and misaligned to nature of IT workforce and operations
- Lack of investment in training, certifications and overall professional development is typical within governments

Culture

- Siloed and political nature of government makes it difficult to enforce IT security standards + controls uniformly or consistently
- Resistance to change is very high
- Civil service and union rules can elevate barriers to the ability to act with urgency and pivot quickly in both strategy and operations
- IT is not seen as strategic to operations = undersized budgets and resourcing
- Functions of Human Resources, Procurement or Law departments are not viewed as key to enabling high-performing IT + cybersecurity operations

Procurement

- Open and competitive procurement is a necessity in government
- Ability to respond quickly to a cyber threat requires forethought and pre-planning to have procurement vehicles at the ready
- Local procurement rules may require changing to allow for time + materials contracting or unitary contracts for professional services
- Care has to be taken to craft RFPs that do not divulge cybersecurity weaknesses when openly procuring services – counter to practice

Budget

- Fiscal year budgets are set months in advance, subject to public hearings and balancing among many competing priorities, then locked-in
- Process + organizational change management are critical to success of IT and security projects, but rarely if ever included in budgets
- Inability to hire full time IT staff can strain budgets for contractors to fill void as budget classes may not be interchangeable
- Cybersecurity is the cost of network ops, backups, disaster recovery solutions, COOP planning and drills, training…not just firewalls and antivirus