OVERVIEW OF INFRASTRUCTURE CYBERSECURITY AND SHADOW I/T

TERRI CLARK

DIRECTOR OF TECHNICAL SERVICES, KS LEGISLATURE

NCSL TASK FORCE ON CYBERSECURITY

APRIL 21, 2017

INFRASTRUCTURE CYBERSECURITY UMBRELLA

Cybersecurity Policy
I/T Budget and Resources
Cybersecurity Defense Systems/Monitoring
I/T Staff Training
User Training

- Network
  - Perimeter Defense
  - Firewalls
  - Intrusion Detection
  - Switching/Routing
  - Internet Access
- Servers
- Laptops
- Mobile Devices
- User Authentication
- Printers

- Communications
  - Voice
  - Email
  - Messaging

SHADOW I/T FALLS OUTSIDE THE UMBRELLA

According to Gartner, by 2020 one third of SUCCESSFUL attacks will be on shadow I/T resources. [1]

WHERE CAN SHADOW SYSTEMS AND DATA LIVE?

- HIGHER ED DEPARTMENTS, FUNDED BY GRANTS
- ELECTED OFFICIAL'S AGENCY
- DEPARTMENT STAFF WITHIN AN AGENCY OR THE LEGISLATURE
- FISCAL STAFF
- LEGISLATIVE AUDITORS
- PERSONAL CLOUD – ONEDRIVE, DROPBOX, GOOGLE
- MOBILE/PERSONAL DEVICES AND FLASH DRIVES
- SOCIAL MEDIA
  - 49 states, DC Council, Puerto Rico, US Virgin Islands using 14 different social media sites[2]
- I/T STAFF (YES, WE ARE GUILTY OF THIS TOO!)

WHY DO SHADOW SYSTEMS AND DATA EXIST?

- LOW CONFIDENCE IN I/T STAFF
- I/T DEPARTMENT FOCUSED ON OTHER USER GROUPS
- LEGACY SYSTEMS/APPLICATIONS
- CONVENIENT FOR USERS
- I/T “EXPERTS” EMBEDDED WITHIN A DEPARTMENT
- PROJECT BUDGET ASSIGNED TO A BUSINESS GROUP, NOT I/T DEPT.
- DECISION TO KEEP DATA SEPARATE FROM ENTERPRISE
- POLITICAL DECISIONS, I.E. ABILITY TO PROVIDE POLITICAL ANALYSIS OF DATA
- TURF WARS

RISKS OF SHADOW I/T

- NON-COMPLIANCE WITH SOFTWARE LICENSING
- OPEN BACKDOOR TO NETWORK, AGENCY SYSTEMS
- VIRUS, MALWARE RISK INCREASED
- RANSOMWARE RISK INCREASED
- DATA LOSS – NO DATA BACKUPS, PERSONAL CLOUD OUTSIDE AGENCY CONTROL
- PERSONAL CLOUD REPOSITORIES MAY NOT MEET AGENCY SECURITY REQUIREMENTS
- USERS ARE UNTRAINED ON TECHNOLOGY THEY'RE USING
- SERVERS, COMPUTERS RUNNING UNSUPPORTED OPERATING SYSTEMS
  - Security patching and updates usually out of date
- LACK OF SECURITY MONITORING
- I/T INHERITS SYSTEMS THEY CAN'T SUPPORT

FINDING SHADOW SYSTEMS AND DATA

- UPDATE CURRENT DOCUMENTATION
  - Map application flows on the network
  - Conduct a software license inventory
- USE NETWORK SCANNING TOOLS – NESSUS, MICROSOFT, ETC.
- CONDUCT 3RD PARTY SECURITY AUDIT
- IMPLEMENT MDM, DATA ENCRYPTION, ETC.
- **TALK TO PEOPLE - GROW TRUST BETWEEN THE USER COMMUNITY AND I/T**

AGENCY HELP DESK STAFF PROBABLY KNOW WHAT'S IN THE SHADOWS

WHAT CAN I/T MANAGEMENT DO?

- SET ASIDE EMOTIONAL RESPONSES (EGO, SURPRISE, OUTRAGE, HURT FEELINGS)
- EVALUATE THE ACTUAL RISKS AND COSTS OF THE SHADOW SYSTEM TO THE ENTERPRISE

  It's probably ok for the fiscal analysts to use Tableau - highly specialized area, niche software, significant training curve

- UNDERSTAND WHY USERS CREATED A SHADOW SYSTEM
- BRING IT OUT OF THE SHADOWS

  Add the shadow system and data repositories to agency app inventory, DR plan, etc.

- RELY ON CYBERSECURITY POLICIES TO INFORM DECISIONS
- ENFORCE CYBERSECURITY POLICIES
  - Defined processes
  - Training
  - Increased service levels
  - Negotiate with end users

IMPROVE THE AGENCY ENVIRONMENT

- PROVIDE POINT-IN-TIME CYBERSECURITY TRAINING TO USERS AT EVERY OPPORTUNITY
  - Reference Cybersecurity policies and processes
  - Get user buy-in on known risks, risk mitigation strategies
- FIND WAYS TO IMPROVE THE SHADOW SYSTEMS – SHARE INFO FROM NCSL, NASCIO, TECH JOURNALS, ETC.
- BE OPEN TO IDEAS FROM THE USER COMMUNITY, COMMUNICATE BUDGETS AND PROJECT SCHEDULES
- BE OPEN TO IDEAS FROM 3RD PARTY VENDORS THE USERS ARE WORKING WITH
- EMPOWER THE USER COMMUNITY TO BRING THEIR PROBLEMS AND NEEDS TO I/T FIRST

WILL SHADOW I/T ALWAYS EXIST?

ENTERPRISE CYBERSECURITY POLICIES ARE THE FIRST TOOL IN THE I/T MANAGER'S TOOLBOX, THEN LOOK FOR CREATIVE WAYS TO:

MANAGE SHADOW I/T WITHIN ORGANIZATION

COMMUNICATE WITH AND TRAIN USERS

BUILD TRUST WITH USERS

CREATE PROCESSES THAT OUTLIVE INDIVIDUALS

Difficult to achieve but critical to an effective cybersecurity strategy!