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

Network
  Perimeter Defense
  Firewalls
  Intrusion Detection
  Switching/Routing
  Internet Access

Servers

Laptops

Mobile Devices

User Authentication

Printers

Communications
  Voice
  Email
  Messaging

Cybersecurity Policy

I/T Budget and Resources

Cybersecurity Defense Systems/Monitoring

I/T Staff Training

User Training
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
- 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/application
• 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  - Security patching and updates usually out of date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!