CYBERSECURITY FOR CLARK COUNTY, WA GOVERNMENT

May 24, 2017

Technology Services

Introductions

Technology Services Security Team

Sam Kim

Spencer Bauman

Dan Coleman

Marlia Jenkins

Jake McCauley

Jodie Toliver

Work session goal

Update Council on:

- importance of cybersecurity and
- plans to improve the county's security posture

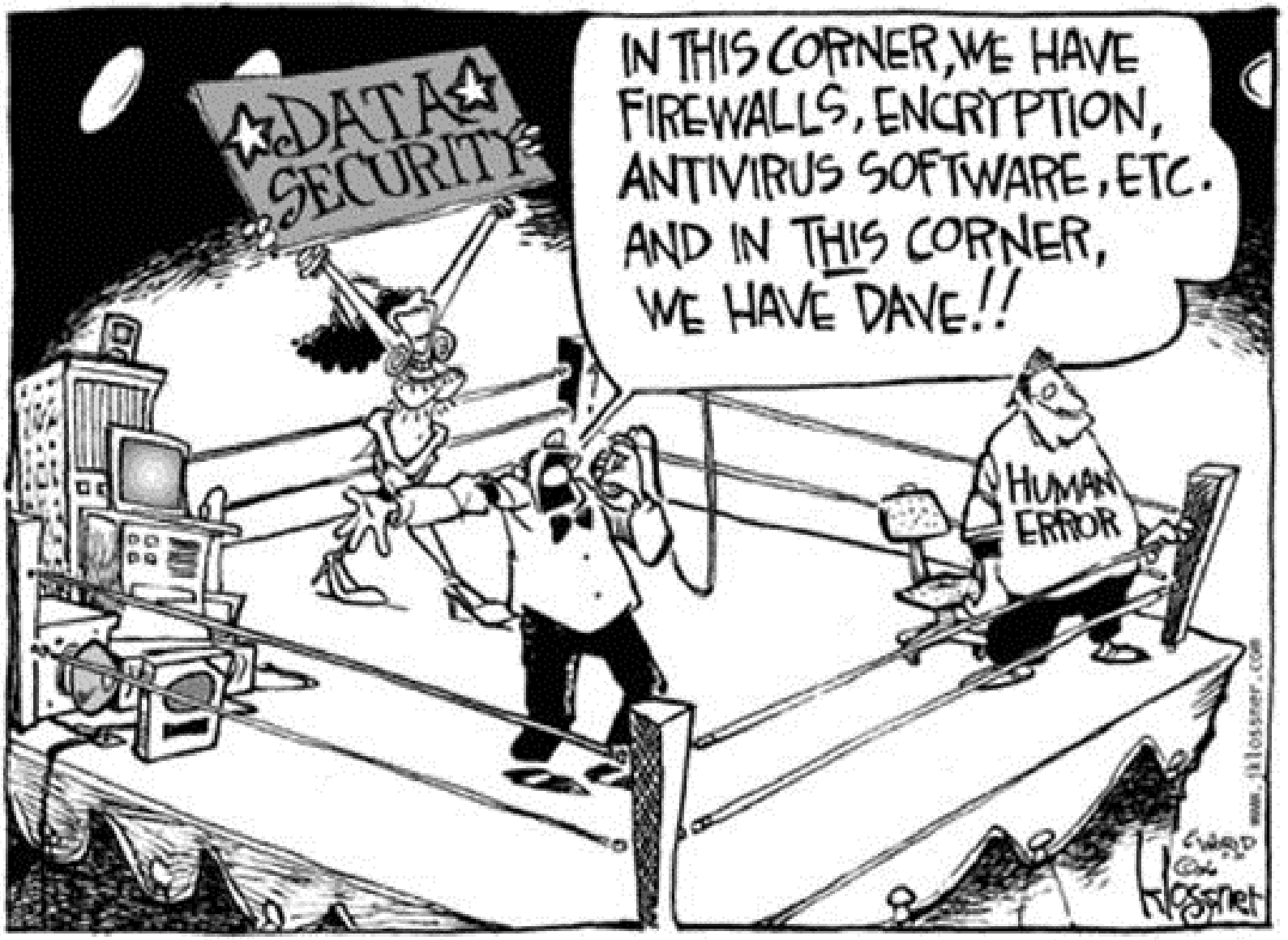
Goals of security

- Protect employee and citizen data
- Protect financial systems
- Retain public records
- Perform the county's mission

Who creates threats

- Attacker with internal or remote access connectivity
- Malicious insider with user-id and password
- Attacker from the internet

- And inattentive or uneducated employees who simply make mistakes


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Attacker need: access

- Access creates value to the attacker
- An individual user might personally have little of value to the attacker
- If access is attained attackers can
  - explore for citizen and employee data for misuse
  - hinder system operation for fun or for profit
  - move from system to system

Risk: Social Engineering\Phishing

- What is likely to go wrong?
- Email based access
  - Lures someone to open an email or email attachment with malicious content

Risk: vendors

- What is likely to go wrong?
- Acquire software with security gaps
- Software updates do not respond to new and emerging threats
- Configure software in a manner that creates security gaps
- Software decommission leaves remnants of old software

Risk: external access

- What is likely to go wrong?
- Configuration allows access to the system
- Factory or default settings are common knowledge
- Failure to change defaults creates risk

Risk: remote access

- What is likely to go wrong?
- Add-on programs to enterprise or niche systems allow access from Point B to enter the county system
- Employee remote access is obtained and misused by others
- Customer interfaces allow entry to databases or the system

Recent horror stories

- Ubiquity
- Port of Vancouver
- Target
- Google

Best practices to control security

- Inventory, detect and remediate
  - authorized devices and software
  - unauthorized devices and software
  - vulnerabilities
- Configure software and hardware to eliminate unauthorized access
- Education

Where local governments can improve

- Standards, policies and procedure
- Personnel engagement
- Training
- Management support
- Access management
- Technology investment

Council role

- Be aware and take awareness training
- Acknowledge your name and role is a desirable target for attackers
  - Name recognition creates a unique access opportunity, be aware of spear phishing
- When necessary, change policy to support a countywide approach to security

2017-2018 focus

- Made possible by decision package approved in 2017-2018 budget

- Build security into everything we do
- 3 project employees dedicated to security assessment and remediation
- Increased awareness and skill building for Technology Services staff and employees countywide
- Best practices