Buncombe County IT Security and Standards Program

Presented By

Eric Grau – IT Director

Mark Goodwin – Chief Information Security Officer

4/5/2022

Bottom Line Up Front

- Opportunities to improve our IT Security posture
  - Engaging with a Managed Security Service Provider – 24/7/365 coverage
  - Dark Web Monitoring – protecting users / account information
- General Program information
  - History
  - Introductions
  - Threat Landscape and Program Approach
  - Management and Security Philosophy

History

In FY19

- Created dedicated Security Division within IT
  - Separation of duties
  - Repurposed 5 IT positions (Network Engineer, Operations Engineer, IT Trainer, Service Desk Manager, SharePoint Developer) and 1 HHS position
  - No new positions

- Chief Information Security Officer (CISO) position established

Investments since FY19

AVG annual cost: $266,000

- Next-Gen Anti-Virus Software
- Log capturing Software
- Email Security Software
- Security Training Platform
- Threat Detection Software
- Governance, Risk, and Compliance Software
- Vendor Security Rating Tool

Milestones/Accomplishments

- 3rd Party Audit
- HIPAA Audit
- National Guard Assessment x2
- Multifactor Authentication
- Role Based Provisioning
- Separation of Duties and Accounts
- Professional Development and Certificates
- Third-Party Risk Management

Who Am I?

Mark Goodwin, MBA, PMP, CISSP, ITIL

Led and Supported IT and Security Programs since 1994

- Buncombe County Government
- National Institutes of Health
- US Department of Veterans Affairs
- US Department of Justice
- US Patent and Trademark Office
- Celera Genomics
- General Electric Information Systems

Threat Landscape

- Who/where are the threats?
- What can we learn from other successful attacks?
- Motivation – What drives the need for IT Security?
- A typical day at Buncombe County.

Our Approach – A Team Effort

Management – Operations - Technology

Focus Area	Primary
IT Security Management – Policy, Operations, and Projects	Mark Goodwin
Information Assurance / Risk – Operations and Projects	Monica Stewart
IT Security Operations – Incidents and Tickets	Mark Romine (and Everyone)
Technical Architecture and Solutions - Projects	
Security Training/Awareness	David Anderson
Network Security Engineering	Kevin McCall
Host Security Engineering	Adam Scarboro
Microsoft Security	David Anderson

Management and Security Philosophy

- **Management Philosophy**
  - Servant Leadership
  - Four Agreements
    - Be impeccable with your word
    - Don't take anything personally
    - Don't make assumptions
    - Always do your best
- **Security Philosophy**
  - Defense in Depth
  - Regulatory Compliance
  - Paranoia – attacks can come from anywhere at anytime
  - Appropriate and rapid Incident Response
  - Effective Communication
  - Automation and Accuracy

Request for Board Action

(Budget Amendment | | +$225,197)

- **Managed Security Service Provider – 24/7/365 coverage**
  - Complement and enhance skills of IT Security team
  - Better tuned tools and awareness of attacks
  - Extend coverage beyond daylight / standard business hours
  - Replaces existing toolset ($25k)
  - $189,783 / year
- **Dark Web Monitoring – protecting users / account information**
  - Finding compromised BC accounts before they can be exploited
  - Resetting the comprised passwords quickly
  - Avoiding a compromise of user information
  - $35,414 / year