IT Services Update

Presented to the Mecklenburg Board of County Commissioners
January 2018
Agenda

- ITS 3-Year Strategic Plan Overview

- Securing the Business Platform Update
  - FY18 Security Projects
  - Post- Incident Recovery Recommendations

- Disaster Recovery & Business Continuity Readiness
We are an increasing cybercrime target and we will need to accelerate our strategic plan efforts.

<table>
<thead>
<tr>
<th>Investment Category</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Capabilities Enabled by IT Services</td>
<td>Build Foundation</td>
<td>Scale to More Complex Departments</td>
<td>Extend Across the County</td>
</tr>
<tr>
<td></td>
<td>Connect, Simplify, Improve, Leverage, Architect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stability &amp; Reliability Minimum Standard</td>
<td>Eliminate</td>
<td>Manage</td>
<td>Empower</td>
</tr>
<tr>
<td></td>
<td>Reduce, Streamline, Evergreen, Standardize, Improve</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery &amp; Enterprise IT Security</td>
<td>Protect</td>
<td>Replicate</td>
<td>Seamless</td>
</tr>
<tr>
<td></td>
<td>Protect, Recover, Sustain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Over the last ~2 years, IT Services has had a number of external experts provide analysis and recommendations:

All assessments have noted

- Numerous, material enterprise security and technical risks exist
- Recommendations have been incorporated into our 3-Year plan
Cyber crime damage costs to hit $6 trillion annually by 2021
- Global ransomware damage costs are predicted to exceed $5 billion in 2017 (a 15X increase in two years, and expected to worsen)

- ‘Internet of Things’ attack surfaces are growing exponentially:
  - 50 to 200 Billion connected devices by 2021

- Average time to intrusion discovery has grown by more than one month since 2015

- Cybersecurity spending to exceed $1 trillion from 2017 to 2021
Cybercrime: Third Largest Market Cap (2016 data)
White House Adviser Says North Korea Behind Big Ransomware Attack

Key Facts about WannaCry Ransomware

- WannaCry virus is a malicious program that encrypts files and demands ransom
- WannaCry cyber-attack was launched on 12 May 2017
- WannaCry infected over 230,000 PCs in 150 countries
- Distributed using EternalBlue exploit
- Marks encrypted files by adding .wcry, .wncry or .wncry extension
- Demands $300-$600 in Bitcoins
Bots are responsible for most of the world's internet traffic
Post Recovery: Actions Must Eliminate “Noise” on our Networks Including Unnecessary Traffic

**Good Bots**
- Search Engine Crawling
- Website Health Monitoring
- Vulnerability Scanning

**Bad Bots**
- DDoS
- Site Scraping
- Comment Spam
- SEO Spam
- Fraud
- Vulnerability scanning

---

**6.6% SEARCH ENGINE BOTS**
Bots that collect information for search engine algorithms, which they use to make ranking decisions.

**12.2% FEED FETCHERS**
Bots that ferry website content to mobile and web applications, which they then display to their users.

**24.3% IMPERSONATORS**
Bots that assume false identities to bypass security solutions. They are commonly used for DDoS assaults.

**1.7% SCRAPERS**
Bots used for unauthorized data extraction and the reverse engineering of pricing models.
The Dark Web Dangers

The Deep Web is estimated to be 500X the size of the Surface Web.

Sources: Quora, elixirofknowledge, Silk Road anonymous marketplace
CYBER SECURITY THREATS ARE RISING

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

PHASE 1
PRE-ENGAGEMENT INTERACTIONS
- RULES
- SCOPE
- CONTACT INFO
- PROJECT CHARTER

PHASE 2
INTELLIGENCE GATHERING
- PUBLIC RECORDS
- SOCIAL NETWORKS
- DUMPSTER DIVING

PHASE 3
PRETEXTING
- CREATE BELEEVABLE SCENARIOS
- ATTACK

PHASE 4
EXPLOITATION
- EXECUTE SCENARIOS
- ATTACK

PHASE 5
POST EXPLOITATION
- PILLAGE
- DOCUMENT
- CLEAN-UP

So·cial Eng·ine·e·ring
TYPES OF ATTACKS

PHISHING
SPEAR PHISHING
VISHING

SMISHING
MINING SOCIAL MEDIA
LEARN MORE

www.vasco.com/cronta1ign

Ransomware
2016 in numbers

One in five
SMBs who paid the ransom
never got their data back

statistics were obtained using Kaspersky Security Network (KSN)
© 2016 Kaspersky Lab. All Rights Reserved.
Growth in Ransomware Variants Since December 2015

Every 10 seconds, a consumer gets hit with ransomware.
(up from every 20 seconds in Q1 2016)

Every 40 seconds, a company gets hit with ransomware.
(up from every 2 minutes in Q1 2016)
Identify “New Normal” Security Practices

Such as:

- Implemented extended password length **COMPLETE**
- Significantly restrict international emails **COMPLETE**
- Dec. 20th: Policy & Perimeter Security changes: **COMPLETE**
  - External email alerting
  - Non-County web-based email elimination
  - Eliminate email auto-forwarding
Policy & Perimeter Security Layer

- All emails coming to county mailboxes from external email address will have [External] in the subject line (see example below):

- All emails coming to county mailboxes from an external email address will have the following within the body of the email at the top of the message:

  ![Example Email]

  **CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

- Employees will no longer be able to access non-county email via county systems. This includes web-based email such as Hotmail, Gmail, AOL, Yahoo, Live, etc.

- All County Email users will no longer be allowed to set up email rules to automatically forward their Mecklenburg County email to any other account. For example, you cannot set up a rule that automatically sends all Employee News Now email messages to your home Gmail or Yahoo accounts. This allows us to protect sensitive information from inadvertently leaving the County network.

- Policies & Procedures can be found on MeckWeb under the Forms and Policies tab. [https://mecktech.sharepoint.com/Forms-and-Policies/Pages/default.aspx](https://mecktech.sharepoint.com/Forms-and-Policies/Pages/default.aspx)
Identify additional “New Normal” standard operating practices such as:

- Reaffirm that One-Drive for Business is the sanctioned County cloud storage solution
- Eliminate utilization of unsanctioned cloud storage solutions such as:
  - Google Docs
  - Drop Box
  - Others
- Eliminate unnecessary network traffic (block non-County business centric URL’s)
- Broader utilization of two factor authentications *(Recommended list forthcoming)*
  - County staff access to externally facing solutions when staff are not on County network
    - PeopleSoft
    - Office 365 (Email, MeckWeb, VPN)
    - More to Come
- Implementation of new technology tools:
  - Advance Thread Protection
  - More to come
Post Recovery “New Normal” Recommendation

Eliminate Utilization of All Unsanctioned Cloud Storage Solutions by January 30, 2018

- Personal applications and storage locations present Mecklenburg County with the largest security risks because we have no visibility, enforcement or access to them.

- All of these applications are in use by employees today. We have limited visibility into most.

Where is our information stored? How is it shared? How can we protect County data?
Effective Risk Management Requires a Secure Business Platform

- **Business Capability**
  - Develop application and IT infrastructure recovery plans on a common understanding of essential functions supporting county services.

- **Tools and Process**
  - Secure data and system operations from malicious intrusion and unauthorized use.

- **Disaster Recovery**
  - Establish executable disaster recovery capabilities.

- **Infrastructure**
  - ‘Harden’ the IT infrastructure against malicious attack, catastrophic mistakes or natural disasters.
IT Security utilizes a layered model to address security concerns across the enterprise. Due to the highly dynamic nature of information security, specific items on this diagram are frequently updated; however, security initiatives should align with one or more of these layers as an area of focus.

**Goal:** Reduce an Attacker’s Chance of Success While Increasing an Attacker’s Risk of Detection
Disaster Recovery & Business Continuity Readiness

October 2nd 2017 – Cybersecurity Table Top Exercise: Complete

October 30th 2017 – Disaster Recovery Table Top Exercise: Complete

FY19 – Continue County-wide & IT Team specific Table Top Exercises integrating Cybersecurity and Mecklenburg County Cybersecurity Command Center

Disaster Recovery: Primary Decision Drivers and KPI’s

Disaster recovery, like all risk mitigation strategies, is an insurance policy where risk tolerance must be balanced with cost tolerance. The Business Impact Analysis and prioritization ensures you are weighing these considerations appropriately, establishing key tracking and performance metrics, and reporting to stakeholders on a regular basis.

Emergency Operations Center
1770 Shopton Road
Charlotte, NC

Safety Preparedness & DR Update
Summary: Strategic Actions in FY18 Plan

- **Secure End Point Devices** *(Work-In-Progress)*
  - Trust by Exception rather than Trust by Default
  - Windows 10 and Workspace1
  - Eliminate Local Admin Rights
  - End-user Computing Evergreen

- **Streamline and Simplify Datacenter Infrastructure** *(Work-In-Progress)*
  - Mecklenburg County’s “second datacenter” will be Microsoft Azure Cloud
  - Leverage Oracle Data Appliance to provide increased ‘High Availability’
  - Hyperconvergence (Migration to VXRail)
  - Flash Array & File Server Migration
  - Consolidation of Data Environments
  - Data Center Segmentation Architecture & Design
  - Data Backup & Recovery Appliance

- **Encrypt All Microsoft SQL Data at Rest and in Motion**

- **Securely Store and Manage All Encryption Keys**

- **Security Information and Event Management (SIEM) Replacement**

- **3rd Party Application Patching Solution**

- **Begin Data Classification and Discovery**
<table>
<thead>
<tr>
<th>Layer</th>
<th>FY18</th>
<th>FY19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies &amp; Prevention (Training)</td>
<td>- Continue County Wide &amp; Dept. Privacy &amp; Security Training</td>
<td>- Continue County Wide &amp; Dept. Privacy &amp; Security Training</td>
</tr>
<tr>
<td></td>
<td>- HIPAA Security &amp; Privacy Assessment (Agio Contract)</td>
<td>- Leverage 3-Year Strategic Infrastructure and Security Plan</td>
</tr>
<tr>
<td></td>
<td>- NEW: Implement “NEW NORMAL” SOP’s &amp; Business Practices</td>
<td>- Operationalize and Optimize Asset Management</td>
</tr>
<tr>
<td></td>
<td>- 3-Year Strategic Infrastructure and Security Plan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- NEW: Implement “NEW NORMAL” SOP’s &amp; Business Practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Install Asset Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Install Email Gateway (Trendmicro)</td>
<td></td>
</tr>
<tr>
<td>Security Operations Monitoring Response</td>
<td>- eDiscovery RFP &amp; Tool Selection</td>
<td>- Continue County-wide &amp; IT Team Specific Table Top Exercises</td>
</tr>
<tr>
<td></td>
<td>- NEW: Cybersecurity Operations Command Center funding</td>
<td>- Integrating Cybersecurity &amp; County Cybersecurity Command Center</td>
</tr>
<tr>
<td></td>
<td>- NEW: Solarwinds Across Application Portfolio</td>
<td>- NEW: Cybersecurity Operations Command Center Go-Live</td>
</tr>
<tr>
<td></td>
<td>- NEW: Security Awareness Training w/Compliance (KnowBe4)</td>
<td>- Implement &amp; Operationalize eDiscovery Tool &amp; Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-Point</td>
<td>- County-wide deployment Windows 10 / BitLocker</td>
<td>- Continue Evergreen Refresh (1/4 devices annually)</td>
</tr>
<tr>
<td></td>
<td>- Deploy Trend Micro Antivirus/Malware/Data Loss Prevention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- NEW: System Center Configuration Mgr. Re-engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- NEW: Configuration Mgmt.</td>
<td></td>
</tr>
<tr>
<td>Perimeter</td>
<td>- SIEM Tool Replacement</td>
<td>- SIEM Tool Replacement Utilization &amp; Optimization</td>
</tr>
<tr>
<td></td>
<td>- NEW: Eliminate Utilization of All Unsanctioned Cloud Storage</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>- NEW: CISCO Wireless Access (replace Aerohive)</td>
<td>- NEW: CISCO Wireless Access (replace Aerohive)</td>
</tr>
<tr>
<td></td>
<td>- NEW: NAC - Identity Services Engine</td>
<td>- Continue Data Center Segmentation Implementation</td>
</tr>
<tr>
<td></td>
<td>- NEW: Expand Two Factor Authentication</td>
<td>- Redesign County Enterprise Network for Security, Reliability, Failover</td>
</tr>
<tr>
<td></td>
<td>- Data Center Segmentation Architecture &amp; Design</td>
<td>- Begin rolling 5 year Network Devices Evergreen Refresh replacement</td>
</tr>
<tr>
<td></td>
<td>- NEW: Begin Enterprise Network Redesign &amp; Evergreen</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>- Leverage Oracle Data Appliance for High-Availability</td>
<td>- Expand “Second Datacenter” (Azure Cloud) Utilization for Application Development, Secure Data Storage as well as DR / BC</td>
</tr>
<tr>
<td></td>
<td>- HR (PeopleSoft) Complete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Financials (Advantage) Q3 &amp; LUESA Permitting (POSSB) Q4</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>- Continue to make progress addressing Vulnerability Scanning</td>
<td>- Continue to make progress addressing Vulnerability Scanning across ALL of Mecklenburg County Systems</td>
</tr>
<tr>
<td></td>
<td>- NEW: Expand Vulnerability Scanning Licenses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- NEW: Replace Web Application Firewalls</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>- Meck. County Second Datacenter (Azure Cloud) Data Lake</td>
<td>- Continue County-wide Data Classification / Discovery</td>
</tr>
<tr>
<td></td>
<td>- Datacenter Rationalization / Simplification</td>
<td>- NEW: Data Backup &amp; Recovery Appliances</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Database Consolidation &amp; Encryption</td>
<td>- NEW: Oracle Encryption</td>
</tr>
<tr>
<td></td>
<td>- Data Backup &amp; Recovery Appliances</td>
<td>- NEW: Oracle Data Guard Real-Time Protection &amp; Availability Complete</td>
</tr>
<tr>
<td></td>
<td>- NEW: Oracle Encryption</td>
<td>- NEW: Privileged Account Management (PAM)</td>
</tr>
<tr>
<td></td>
<td>- NEW: Oracle Data Guard Real-Time Protection &amp; Availability</td>
<td>- NEW: Data-Centric Audit and Protection</td>
</tr>
<tr>
<td></td>
<td>- NEW: Privileged Account Management (PAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- NEW: Data-Centric Audit and Protection</td>
<td></td>
</tr>
</tbody>
</table>
Mecklenburg County utilizes numerous technologies to protect the enterprise from malicious intrusion as well as phishing / spamming attacks. One of those solutions is Microsoft Advanced Threat Protection solution. We are migrating to Trend Micro’s Smart Protection Suite (conceptional process flow below).
Anticipated New Functionality:
- Data Loss Protection/Prevention for local, removable & cloud storage locations
- Removable media encryption
- User behavior analytics
- Enhanced end point protection utilizing local firewalls

Eliminate Security Gaps with Superior Protection

Smart Protection Suites protect all user activities, reducing the risk of sensitive information loss. You'll get advanced protection with endpoint security, email and collaboration security, web security, and mobile security. The result is a protective shield that is extremely difficult for cyber criminals to penetrate.

Smart - The Right Technique At The Right Time (XGen™)
## Secure and Manage Network Access

<table>
<thead>
<tr>
<th>BENEFITS</th>
<th>Q3</th>
<th>Q4</th>
<th>FY19 Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>FY20 Q1</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standardize &amp; simplify the delivery of consistent, highly secure access control across wired, wireless, and VPN connections</td>
<td></td>
<td>NEW: CISCO Wireless Access (replace Aerohive County-wide)</td>
<td>HHS CRC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Require utilization of secure access method to externally facing solutions when staff are not on County network</td>
<td>NEW: Network Access Control - Identity Services Engine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Network redundancy and high-availability architecture</td>
<td>NEW: Active Directory Redesign Completion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Replace EOL network infrastructure</td>
<td>NEW: Expand Two Factor Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Center Network Segmentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NEW: Redesign County Enterprise Network for Security, Reliability, Failover &amp; Automation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NEW: Begin rolling 5 year Network Devices Evergreen Refresh replacement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Layer: Two Factor Authentication

- In-place today for remote Virtual Private Network access
- Expand adoption mandate and utilization
Goal: Reduce an Attacker’s Chance of Success While Increasing an Attacker’s Risk of Detection

- Web Application Firewalls
- API Management Systems

- Database Audit and Protection
- Encryption and Data Masking
Secure and Manage Data as an Enterprise Asset

Consolidation & rationalization of fragmented enterprise data and siloed, department centric data warehouses

Delivers secure, highly available enterprise analytics and dashboards via Mecklenburg County’s second datacenter (Azure Cloud)
## Secure and Manage Data as an Enterprise Asset

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Moves data off legacy SAN and fiber-channel network</td>
<td>Hyperconvergence (Migration to VXRail)</td>
<td>Complete</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reduces datacenter footprint</td>
<td>Flash Array &amp; File Server Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Increases performance (New flash array)</td>
<td>Microsoft SQL DB Consolidate &amp; Encrypt (Store / Manage Keys)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reduces complexity</td>
<td>Data Backup &amp; Recovery Appliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reduces licensing costs</td>
<td>NEW: Encryption of Oracle Data Bases (Store &amp; Manage Keys)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Real-Time Protection &amp; Availability</td>
<td>NEW: Oracle Data Guard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Principle of Minimal Privilege</td>
<td>Begin County-wide Data Classification / Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Data Privileged Account Mgmt. (PAM)</td>
<td>NEW: Data Centrix Audit and Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Secure and Manage Data as an Enterprise Asset**

- **Benefits**
  - Moves data off legacy SAN and fiber-channel network
  - Reduces datacenter footprint
  - Increases performance (New flash array)
  - Reduces complexity
  - Reduces licensing costs
  - Real-Time Protection & Availability
  - Principle of Minimal Privilege

- **Q1**
- **Q2**
- **Q3**
- **Q4**
# Data Layer: Consolidation & Rationalization of Data Environments

<table>
<thead>
<tr>
<th>Current State</th>
<th>Target State</th>
<th>Benefits Summary</th>
</tr>
</thead>
</table>
| 916 Databases | ~400         | • Approaches industry standards of DB’s per DBA and/or TB’s managed per DBA  
• Reduced support needs of DBA’s freeing them up to focus on development efforts and innovations |
| 75 Servers    | ~12          | • Reduced man-hours needed in server support (related to SQL Server).  
• Lowered licensing costs (both OS and DB licensing) |
| ~6 Different Product Versions | Target 1  
Realistically: ~2 | • Less customization in support scripts, automations, and know-how on day to day support needed |

### Diagram:

- **Oracle Data Appliance (ODA)**: Production/Reporting  
- **Oracle Data Appliance (ODA)**: Development/Test/QA/Demo
1. Encrypt all sensitive data at rest and in motion
2. Securely store and manage all of your encryption keys
3. Control access and authentication of users
### Current State

<table>
<thead>
<tr>
<th>System</th>
<th>Use</th>
<th>Platform</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantage</td>
<td>PROD</td>
<td>Win 2012</td>
<td>12.1.0.1</td>
</tr>
<tr>
<td>Advantage</td>
<td>PROD</td>
<td>Win 2012</td>
<td>12.1.0.1</td>
</tr>
<tr>
<td>Advantage</td>
<td>NON</td>
<td>Win 2012</td>
<td>12.1.0.1</td>
</tr>
<tr>
<td>POSSE</td>
<td>PROD</td>
<td>Win 2012 R2</td>
<td>11.2.0.3</td>
</tr>
<tr>
<td>POSSE</td>
<td>NON</td>
<td>Win 2012 R2</td>
<td>11.2.0.3</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>PROD</td>
<td>Win 2008 R2</td>
<td>11.2.0.1</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>NON</td>
<td>Win 2008 R2</td>
<td>11.2.0.1</td>
</tr>
</tbody>
</table>

- Different OS versions, builds, & configurations
- Different Oracle versions
- Non-standard OS for Oracle deployment

### Future State

- Establish executable disaster recovery capabilities
- ‘Harden’ the IT infrastructure against malicious attack, catastrophic mistakes or natural disasters

**PeopleSoft migrated to ODA**

**Oracle Real Application Clusters (RAC)**
Oracle Encryption and Data Guard (Co-location of data)

Mecklenburg County’s Primary Data Center (Peak10)

Mecklenburg County’s Second Data Center (Azure Cloud)
Begin Data Classification / Discovery:
• Work County-wide to inventory, classify and secure data (multi-year).

Privileged Account Management (PAM):
• Enterprise and cloud data security software for data-centric encryption and tokenization to protect sensitive data while maintaining usability.

**Principle of Minimal Privilege**
The principle means giving a user account only those privileges which are essential to perform its intended function.
Data Layer: Database Activity Monitoring and Audit

- Databases typically contain the most important and sensitive information in an organization.
- Compliance standards (HIPAA, PCI DSS, others) mandate monitoring of database activity.
- Close monitoring helps to ensure changes to the system are authorized, information isn’t leaking, and operations can be tracked back to the originating users.
Enterprise backup is among the most critical tasks for infrastructure and operations professionals!

Need to Implement a standardized, robust, secure, scalable solution

- Deliver quicker Recovery Time Objective (less downtime)
- Dramatically improve staff efficiencies and productivity
Perimeter Layer: Replace SIEM (Tool Selection then Implementation)

Network Breach Prevention Strategy (Remains a Focus for FY2018)

(SIEM: Security information event management)

SIEM Replacement

- Negotiate & procure new tool Q3 – Q4
- Implement, train staff & operationalize FY19
Security Operations & Monitoring Layer

Security Awareness Training with Compliance Management

Social Engineering
The clever manipulation of the natural human tendency to trust.

KnowBe4
Human error. Conquered.

Oops! You clicked on a phishing email.
Remember these three ‘Rules To Stay Safe Online’

✓ RULE NUMBER ONE:
  • Stop, Look, Think!
  • Use that delete key.

✓ RULE NUMBER TWO:
  • Do I spot a Red Flag?
  • Verify suspicious email with the sender via a different medium.

✓ RULE NUMBER THREE:
  • “When in doubt, throw it out”. There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: Stay alert as YOU are the last line of defense!
Implement a Cybersecurity Command Center

• Move from siloed engineering monitoring tools to proactive network and device monitoring

• Strengthen collaboration and partnership with Departments which have & manage IT functions with technology infrastructure

Requires physical floor space and funding to implement.
(Can groups that are scheduled to move downtown do so sooner than planned?)
Significantly Expand:

- Consistent adoption of QS standards (Testing is the new normal)
- Work closely with planning & strategy to adapt consistent “Shift Left Thinking”
- Accelerate Test Data Mgmt. initiative
- Stringent governance of the lower level environments
- Regular cadence of patch releases
- Expand utilization of automation
- Significantly expand non-functional testing

Communities of Practice:
- Mature Quality Services to drive and ensure customer quality and improved internal controls / compliance
- Predictable / engineered outcomes that meet business expectations
- “Shift Left Thinking” (Lean Manufacturing) - Accelerate Speed to Value
Address County-wide Risks & Improve Cost Management by strengthening collaboration and partnership with Departments which have & manage IT functions while dramatically accelerating:

- IT Asset Management
- Vendor Risk Management (i.e. IT Contracts, Source Code Escrow, Data Protection, COOP/DR, etc.)
Questions?