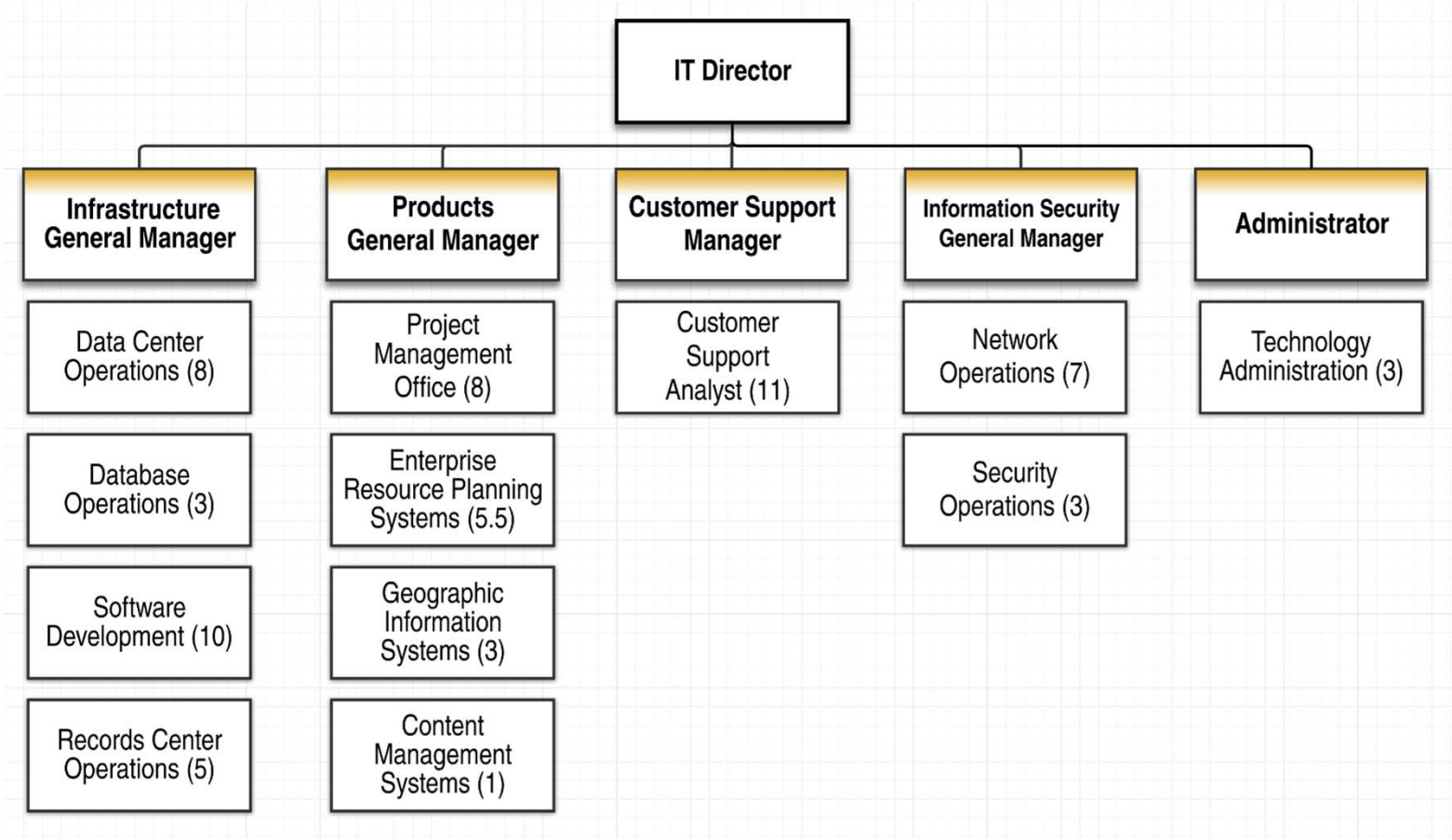
2019 Budget Presentation
Information Technology

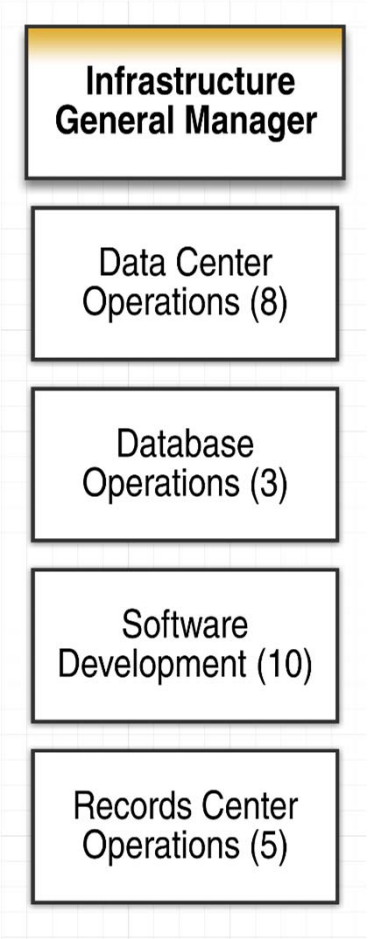
Jeff Eckhart

October 16, 2018

Organizational Chart

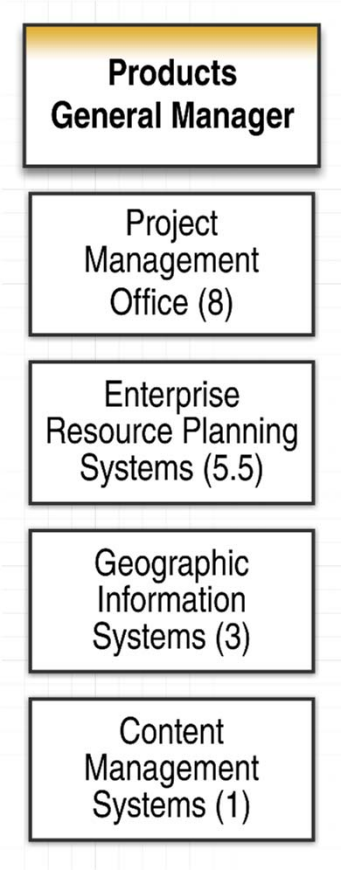


Infrastructure Operations



- Email
- Enterprise Digital Storage
- Enterprise Computing / Application Hosting
- Data Center Virtualization
- Patch Management
- Database Management
- Custom Software Development & Maintenance
- Physical Records Compliance Management

Product Portfolio Management

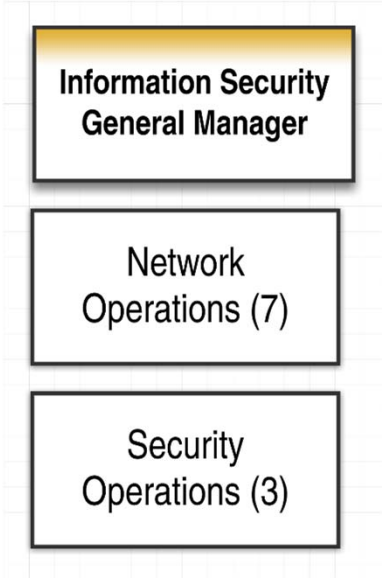


- Project Management Office
  - Project Management
  - Business Analysis
  - Automation
- Enterprise Resource Planning System
  - Financials
  - Human Resources
  - Work Management
- Time & Attendance System
- Geographic Information System
- Citizen Engagement
- Website Management Systems
- Document Management

Customer Support

- Call Center / After Hours Support
- Desktop Computer Support
- Desktop Computer Patch Management
- Mobile Device Management
- PC Replacement Program

Information Security



- Network Operations Center
  - Physical Network Management
  - Firewalls / Intrusion Protection
  - Identity Management / Remote Access Management
  - Cabling / Moves / Adds / Changes
- Compliance
  - Criminal Justice Information Systems (CJIS)
  - Payment Card Industry (PCI)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Personal Identifying Information (HB 18-1128)
- Security Operations Center
  - Vulnerability Management
  - Threat Detection / Prevention
  - Secure Email / Encryption
  - Incident Management / Forensics

Technology Administration

- Technology Finance / Budget
- Volume Purchasing
- Software License Compliance
- Software License Renewal
- Telecommunications Vendor Management
- Inventory Management

Compliance Mandates

- Criminal Justice Information Services (CJIS) Security Policy
  - FBI mandate to protect sensitive information gathered by local, state, and federal criminal justice and law enforcement agencies
- Health Insurance Portability and Accountability Act (HIPAA)
  - Federal mandate for data privacy and security provisions for safeguarding medical information … to ensure the secure passage, maintenance and reception of protected health information
- Personal Identity Information (Colorado HB 18-1128) ***New***
  - Colorado House Bill 18-1128 requires that all covered entities have in place a written policy for the protection, destruction, and proper disposal of paper and electronic documents containing personal identifying information
- Payment Card Industry Data Security Standard (PCI DSS)
  - Security standards designed to ensure that all entities that accept, process, store or transmit credit card information maintain a secure environment

Strategic Plan Goals

Goal 3, Strategy B: provide cooperative general technology services through a secure and modern operating infrastructure, current and sustainable software products, innovation and a qualified professional workforce

1. Develop mobile applications for direct public access to County programs, services and information
2. Implement a 311 type web-based information system
3. **Implement comprehensive technology security program**
4. Expand fiber optic networks to improve operational continuity through redundancy
5. Replaced unsupported analog telephone system with next generation network based phone system

Strategic Plan Goals

Goal 3, Strategy B: provide cooperative general technology services through a secure and modern operating infrastructure, current and sustainable software products, innovation and a qualified professional workforce

6. Define and implement acceptable use policies for technology systems, devices and operations
7. **Retire legacy software products and transition operations to sustainable software architectures**
8. **Design and implement sustainable replacement programs for PCs, software, and technology capital assets**
9. Leverage existing software platforms to enable efficient and interoperable operations

Operational Metrics

35 Business Units

- Public Safety
  - Sheriff
  - District Attorney
  - Coroner
  - Emergency Management
- Elections
- Taxation Management
  - Assessor
  - Treasurer
- Public Works
- Public Health
- Human Services

2,643 County Employees

73 IT Employees

2 Data Centers

3,197 Unique Devices

24,098 Annual Service Requests

- Technical Support
- Moves / Adds / Changes
- Mobile Device Support
- Employee On-boarding
- Employee Exiting
- Security Requests
- Records Center

Operational Initiatives

- Technology Executive Council
  - 4 Elected Officials
  - 4 Department Heads
  - Cooperative Shared Services
- Performance Excellence
  - Continuous Improvement Program
  - Emerging Technology Analysis
  - Voice of the User
- Project Management Office
  - Project Managers
  - Business Analysts
  - Automation
- Data Center Virtualization
- PC Replacement Program
  - 1,000+ out of warranty machines retired over 24 months
- Information Security Risk Reduction Program
  - Patch Management Program
  - Firewall Replacements
  - Email Security
- Legacy System Retirements
  - Oracle Exadata retirements (3)
  - Document Management System consolidation
  - Oracle Identity Management
  - SharePoint 2007

2019 Information Technology Critical Need Requests

Steve Mack

Information Security Manager

Cyber Security Strategy | Security Operations | Network Operations

---

Critical Needs:

Cyber Security Permanent Program Funding

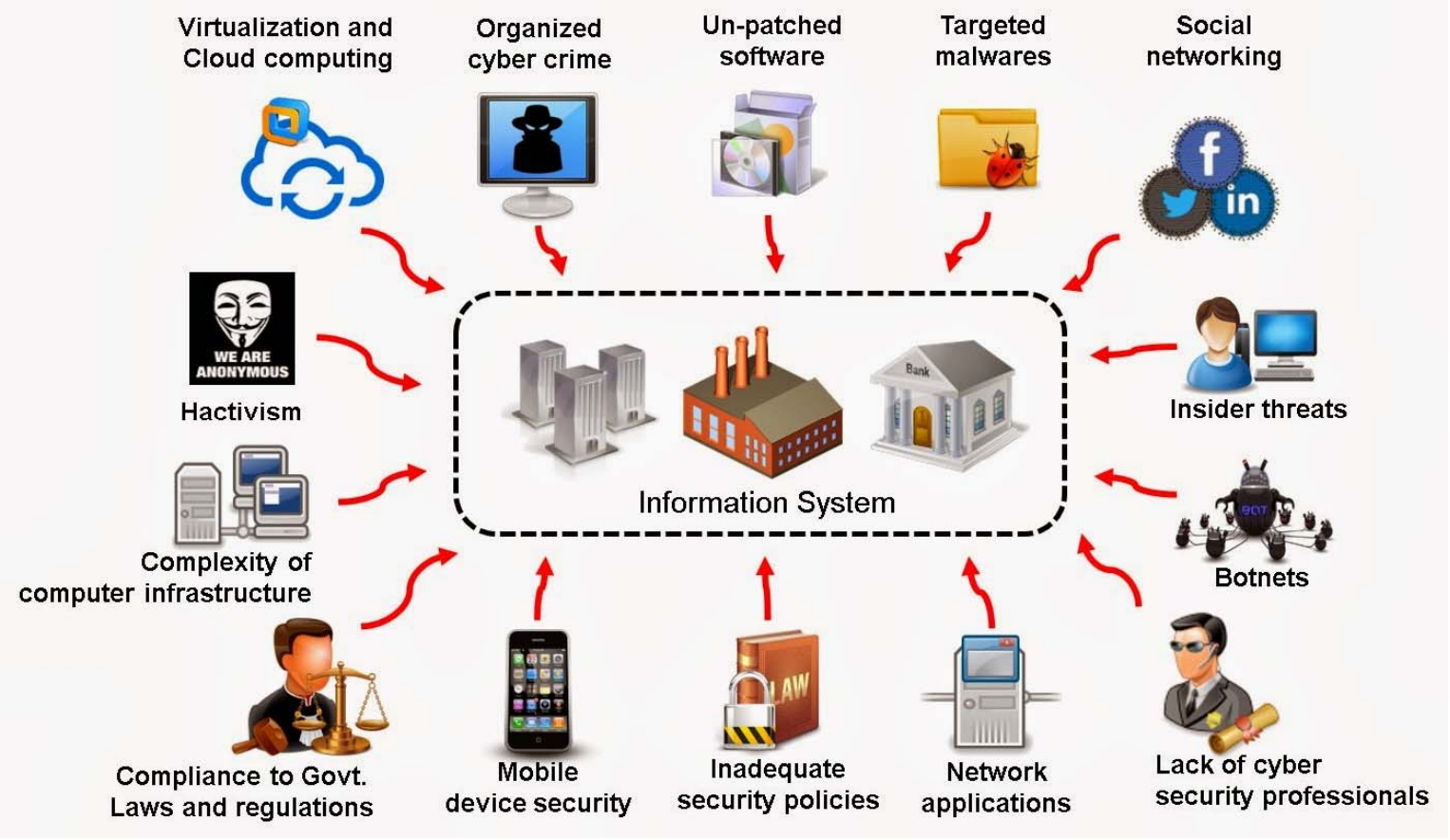
- Ongoing Security Program Funding ($760,000)
- One-time Tools & Technology Purchase ($340,000)

Cyber Security
Critical Need Request

What assets make us vulnerable?

- Election Systems
- Criminal Justice / Public Safety Information Systems
- Property Transactions
- Financial Transactions
- Healthcare Protected Information (Public Health, Employee Benefits, etc.)
- Employee Protected Information
- Public Trust in the Integrity of Local Government

Cyber Security
Critical Need Request



Cyber Security
Critical Need Request

March 22, 2018: large ransomware cyberattack on the city of Atlanta,

- Extensive infection shut down devices at City Hall for five days
- Significantly impacted law enforcement — temporarily returning police to writing incident reports by hand and costing the department access to nearly all its archived in-vehicle video
- Forced the manual processing of cases at Atlanta Municipal Court and stopping online or in-person payment of tickets, water bills, and business licenses and renewals
- $20,000,000 to remediate and rebuild the city network

Source: Theo Davis / Government Technology, October/November 2018

Cyber Security
Critical Need Request

- Colorado Department of Transportation
- City of Atlanta, GA
- Mecklenburg County, NC
- Davidson County, NC
- Adams County, WI
- Baltimore 911
- San Francisco Transit System

https://youtu.be/bQuCgS0DDU0

Cyber Security
Critical Need Request

Q: What is the most secure computer in the world?

A: The most secure computer in the world is turned off, locked in a safe, and guarded by someone with a gun.

- This computer is totally worthless and brings no value to the organization
- *All* computers, information systems, and networks are vulnerable to bad actors and have varying levels of inherent risk of being compromised

Key Strategy: *drive down organizational risk*

Cyber Security
Critical Need Request

Driving Down Risk

2015	⊙ Preliminary Security Audit
2016	⊙ Comprehensive External Assessment
2017	⊙ Program Design
2018	⊙ Contain Highest Risk Vulnerabilities
	⊙ Stand Up Security & Network Monitoring Centers
2019*	⊙ Mature & Operationalize the Program

Cyber Security
Critical Need Request

- Disclosure of Risk
- Awareness & Culture
- Risk Management Training

- Risk Monitoring Strategy & Reporting
- Monitoring Compliance, Effectiveness and Change

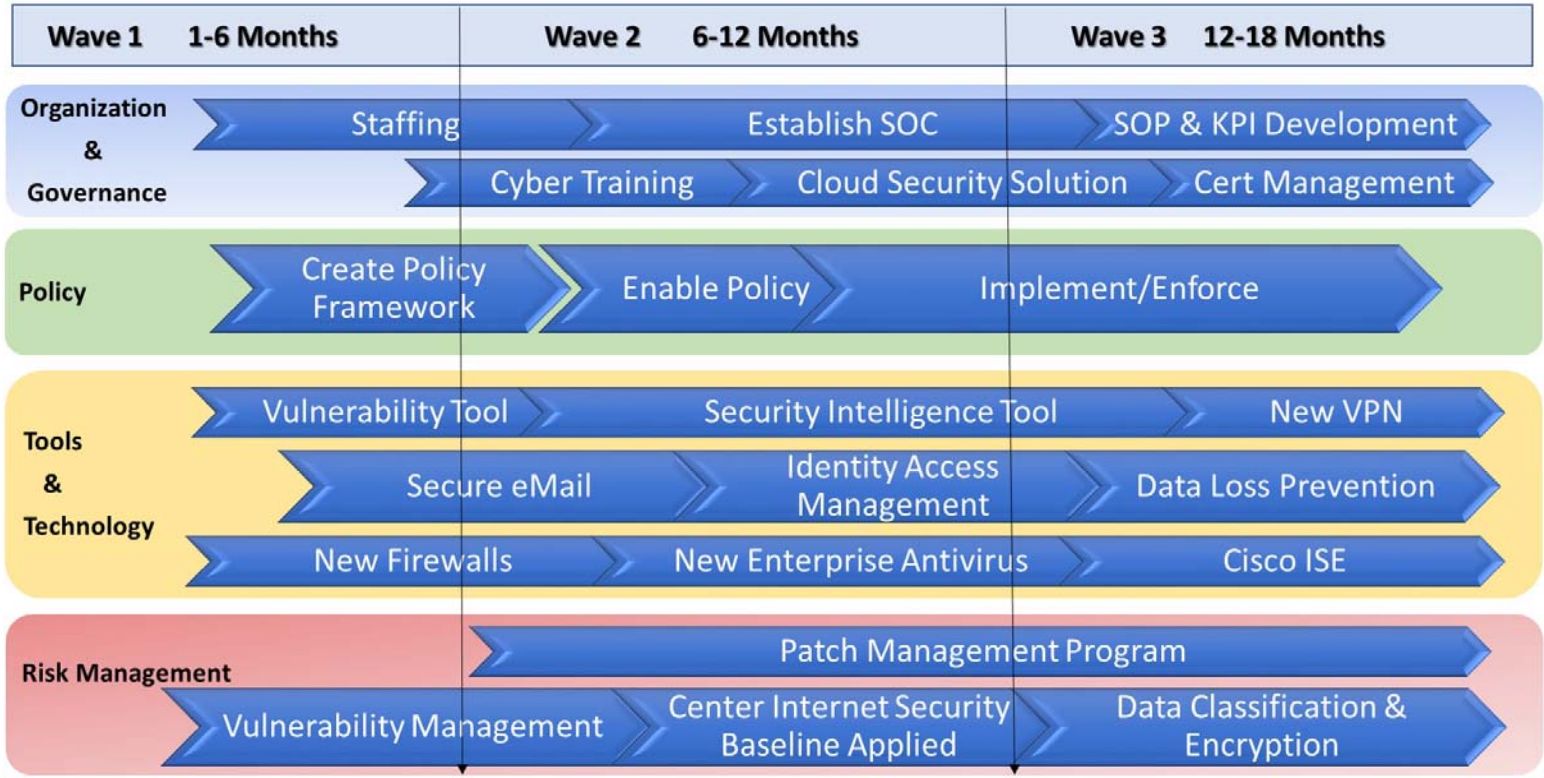
- Strategic Planning
- Operational Planning
- Risk Planning
- Risk Tolerance Planning
- Policy Management
- Compliance Management
- Roles & Responsibilities

- Risk Assessment Methodology
- Risk Hierarchy
- Process & Infrastructure Hierarchy
- Risk Identification
- Risk Treatment
- IT Asset Management

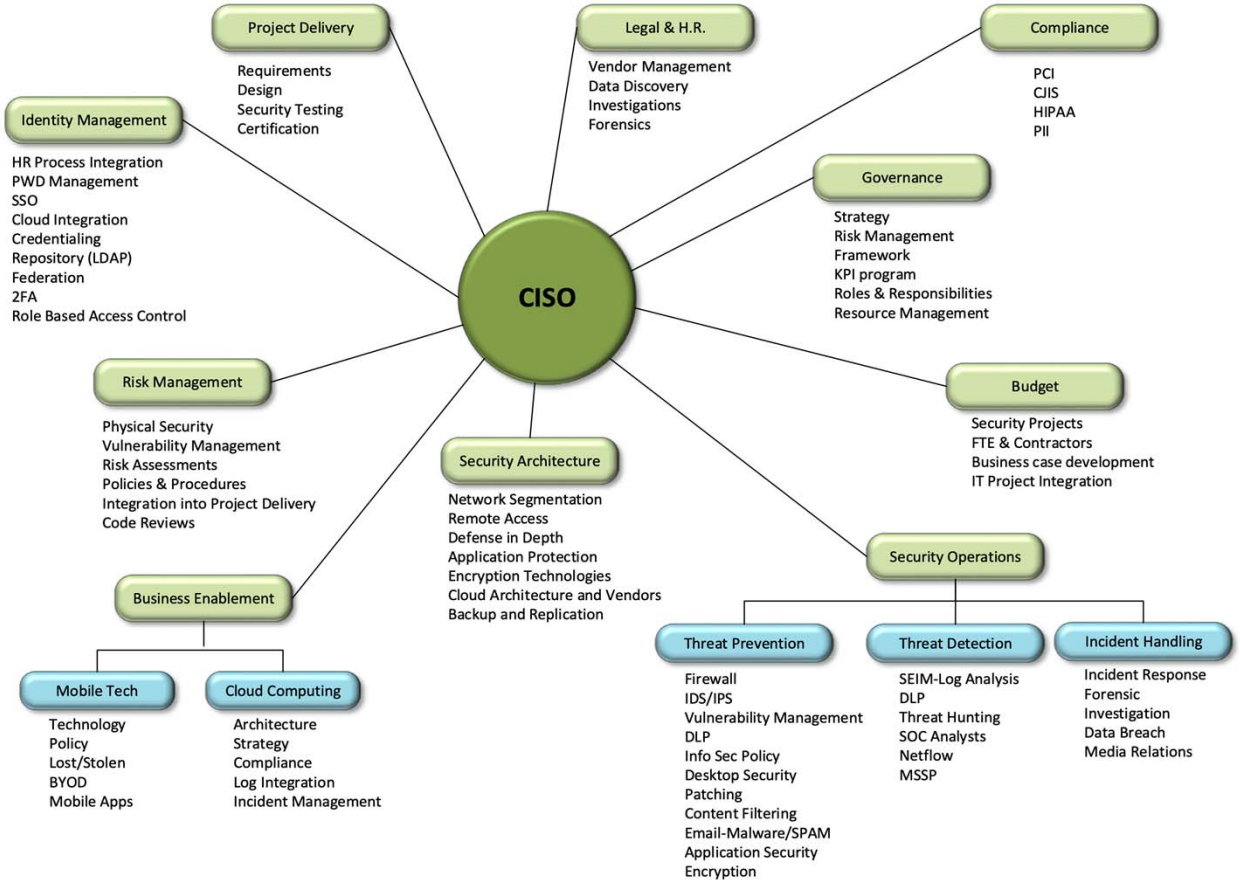
- Event Management & Incident Handling
- Evaluation & Implementation of Response/Course of Action
- Determination & Implementation of Risk Monitoring Triggers
- Security Control Selection & Implementation

Cyber Security
Critical Need Request

High Level Program Road Map 2018



Cyber Security
Critical Need Request



Cyber Security
Critical Need Request

Reducing Risk

IP Address	NetBIOS	DNS	Score	Total	Vulnerabilities
[redacted]	[redacted]	[redacted]	7681	979	616 / 246
[redacted]	[redacted]	[redacted]	7003	851	510
[redacted]	[redacted]	[redacted]	6987	993	546 / 315
[redacted]	[redacted]	[redacted]	6355	835	405
[redacted]	[redacted]	[redacted]	6345	834	460 / 270
[redacted]	[redacted]	[redacted]	6293	855	499
[redacted]	[redacted]	[redacted]	6011	827	484 / 257
[redacted]	[redacted]	[redacted]	5597	740	402 / 268
[redacted]	[redacted]	[redacted]	5573	773	393 / 260
[redacted]	[redacted]	[redacted]	5533	816	458 / 246
[redacted]	[redacted]	[redacted]	5497	783	448
[redacted]	[redacted]	[redacted]	5469	803	442 / 267
[redacted]	[redacted]	[redacted]	5460	739	323
[redacted]	[redacted]	[redacted]	5443	796	446 / 241
[redacted]	[redacted]	[redacted]	5383	783	434 / 257

Cyber Security
Critical Need Request

Reducing Risk

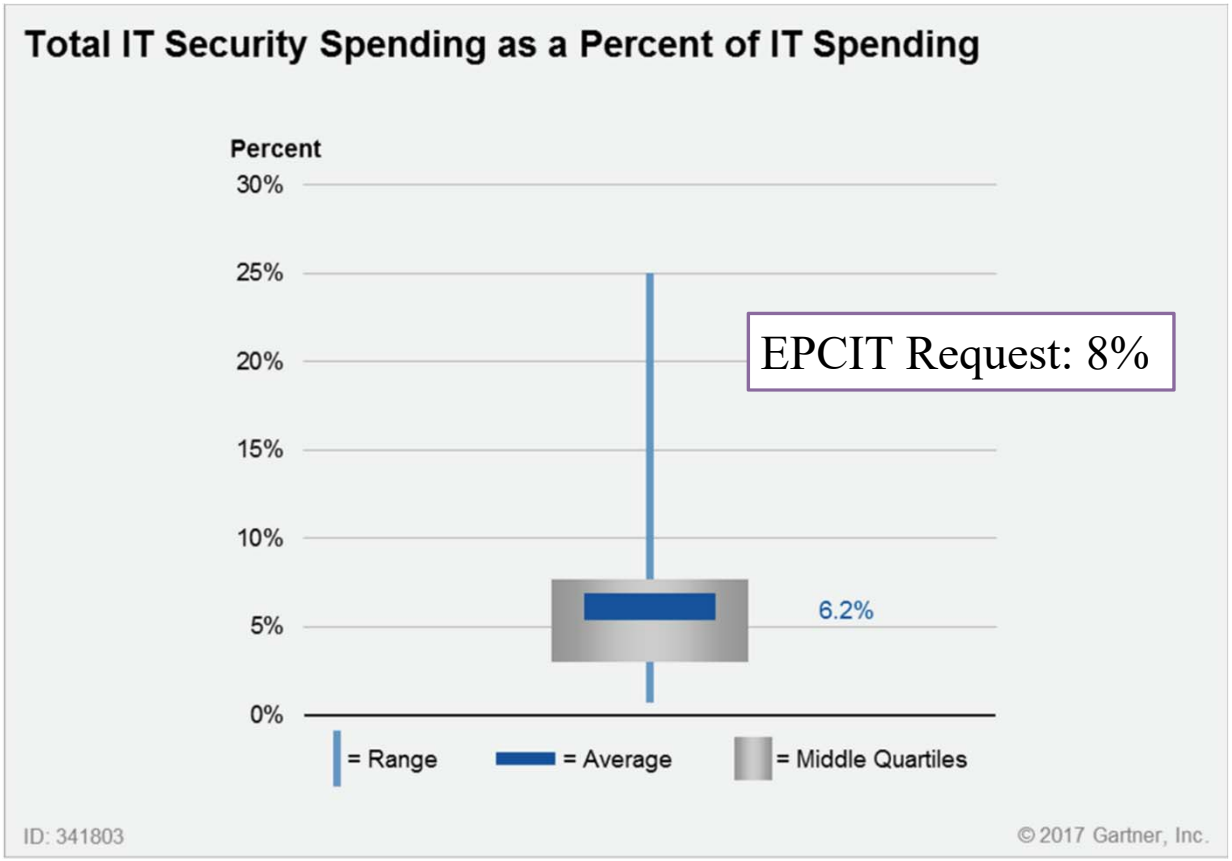
IP Address	DNS	Score	High	Critical	Total	Vulnerabilities
[redacted]	[redacted]	2817	252	0	591	252 / 99 / 240
[redacted]	[redacted]	2793	249	0	595	249 / 101 / 245
[redacted]	[redacted]	2190	219	0	348	219 / 129
[redacted]	[redacted]	2190	219	0	353	219 / 134
[redacted]	[redacted]	2183	218	0	354	218 / 135
[redacted]	[redacted]	2183	218	0	352	218 / 133
[redacted]	[redacted]	2183	218	0	343	218 / 124
[redacted]	[redacted]	2170	217	0	386	217 / 169
[redacted]	[redacted]	2163	216	0	368	216 / 151
[redacted]	[redacted]	2163	216	0	370	216 / 153
[redacted]	[redacted]	2160	216	0	361	216 / 145
[redacted]	[redacted]	2136	207	0	359	207 / 130
[redacted]	[redacted]	2136	207	0	485	207 / 256
[redacted]	[redacted]	2116	205	0	370	205 / 143
[redacted]	[redacted]	2100	210	0	354	210 / 144

Cyber Security
Critical Need Request

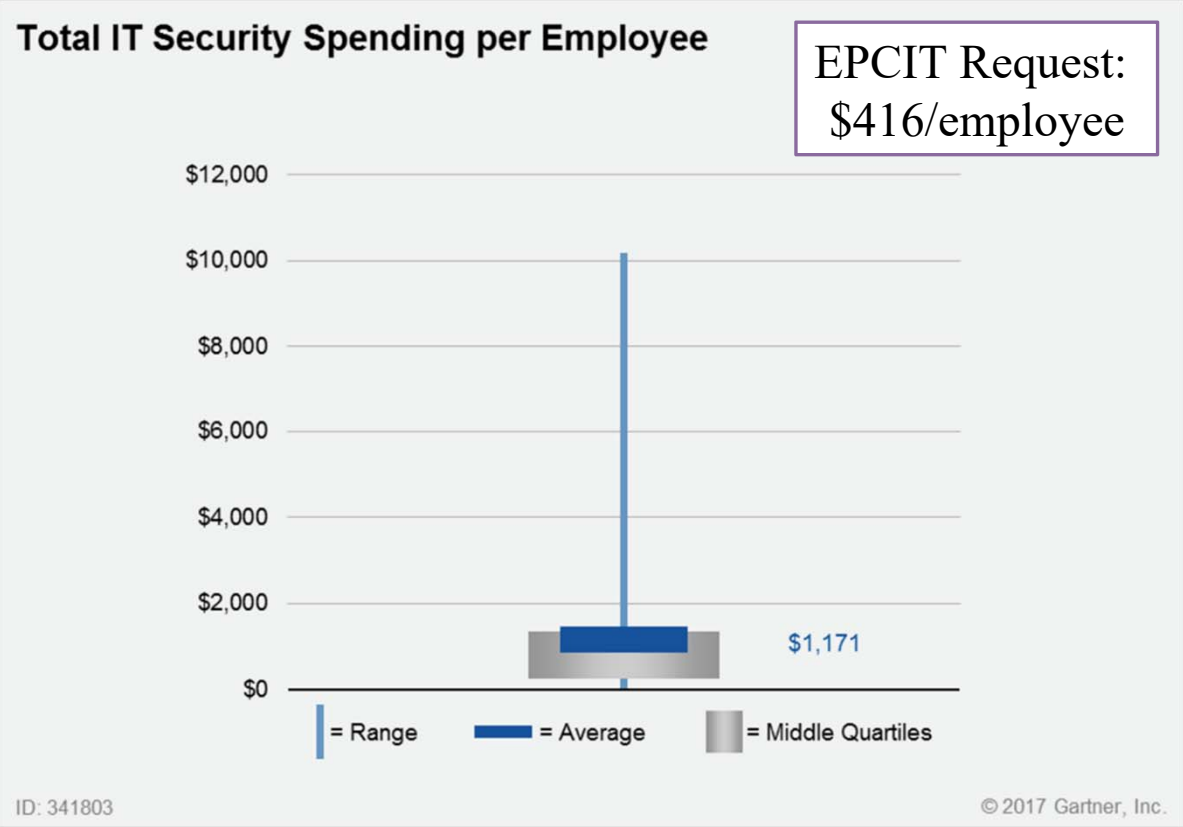
Cost Savings Through Cyber Security Investments

- EPC experiences 1.5 Phishing attacks per week
- Recent EPC Phishing Attack:
  - 726 copies of a phishing email were identified in this attack
  - 280 copies (39%) were automatically rejected by recent investment in secure email product Mimecast
  - 240 copies (33%) were placed in the held queue and later manually rejected
  - 112 copies (15%) were accepted by email server
  - 94 copies (13%)were bounced by exchange for some reason such as invalid email address (13%)
- Total time to resolve using Mimecast was 6 hours costing **$300**
- Before Mimecast we would average 24 hours of cyber time, 30 hours of service desk time, and 8 hours of enterprise time on an attack of this type with 32 hours of user productivity impact. A grand total of 94 hours to respond and rebuild all the PC's that were infected with a simple cost calculation of **$4,700** ($366,600 annually)

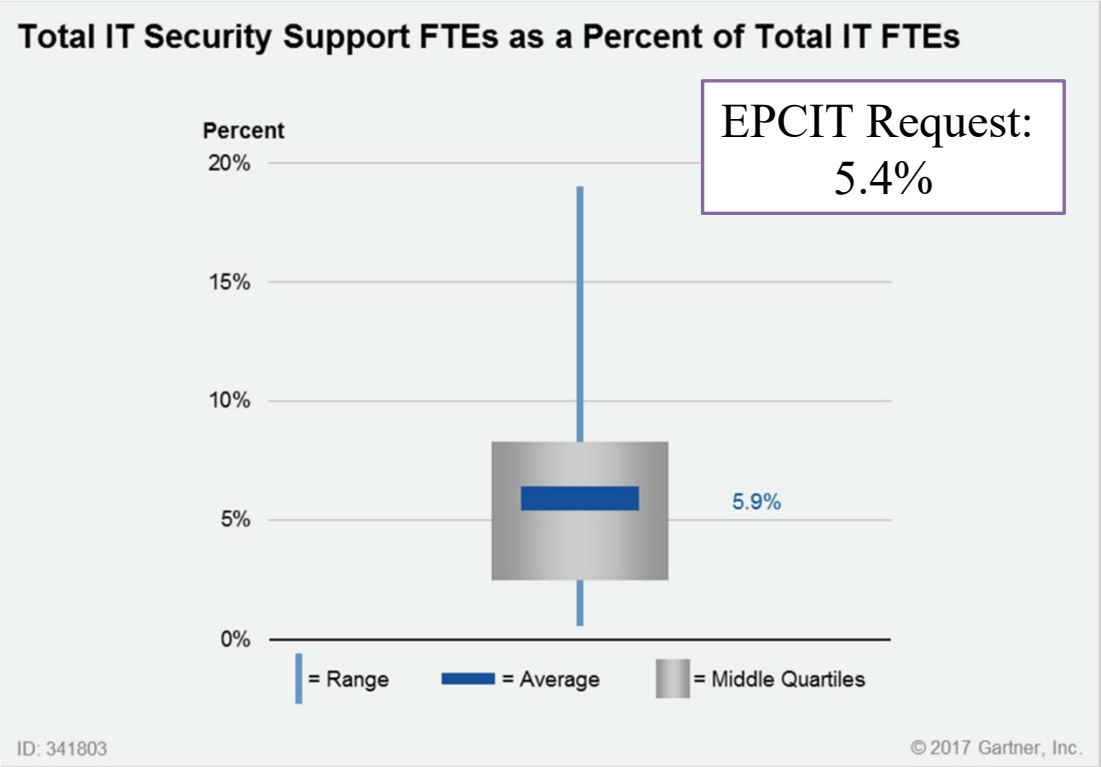
Cyber Security
Critical Need Request



Cyber Security
Critical Need Request



Cyber Security
Critical Need Request



Cyber Security
Critical Need Request

Information Security Program

Ongoing Funding ($760k)

- Permanent Cyber Security Positions (4)
- Security Operations Systems
  - Email Security
  - Advanced Firewalls
  - Network Monitoring
  - Identity Management

Information Security Program

One Time Funding ($340k)

- Network Segmentation
- Data Loss Prevention
- Certificate Management
- Virtual Private Network
- Data Classification & Encryption

2019 Information Technology Critical Need Requests

Kelly Mundell

Customer Support Manager

Call Center | Desktop Computing | Communications

Critical Need:

Microsoft Office Lifecycle Replacement Program

- Office 365 Cloud Subscription ($600,000)

Office Replacement Program
Critical Need Request

Microsoft Office Desktop Software					
Version	In Use	Support Status	Security Patches	Replacement Total	One Time Upgrade to Office 2019
Office 2003	440	No (2005)	No (2005)	119	$43,613
Office 2007	826	No (2009)	No (2009)	825	$302,362
Office 2010	948	No (2015)	No (2015)	879	$322,153
Office 2013	611	Extended (2023)	Yes (2023)	0	$0
Office 2016	834	Yes	Yes	0	$0
Microsoft Exchange On-Premise Email Server					
Exchange 2010		Mainstream Support (2015) / Extended Support (2020)			$450,000
One-Time Upgrade Microsoft Office Environment					$1,118,128

Office Replacement Program
Critical Need Request

Current Office Replacement Model:
Office and Department Discretion

- 77% of Microsoft Office versions on the network unsupported (no security patching, etc.)
  - 440 Office 2003
  - 826 Office 2007
  - 948 Office 2010
  - 611 Office 2013
  - 834 Office 2016

Proposed Office Replacement Model:
Lifecycle Replacement Program
$600,000 Ongoing

- Lower organizational risk of unsupported software
- Increase compatibility with operational systems and security software
- Maintain compliance (CJIS, etc.)
- Retire or isolate unsupported versions
- Implement 3-year replacement cycle
- Cloud-based email
- Two-tier implementation model to save on licensing costs

2019 Information Technology Critical Need Requests

Eric Blakesley

Technology Administration

Finances | Purchasing | Asset Management

Critical Need:

Software Maintenance Contracts ($350,000)

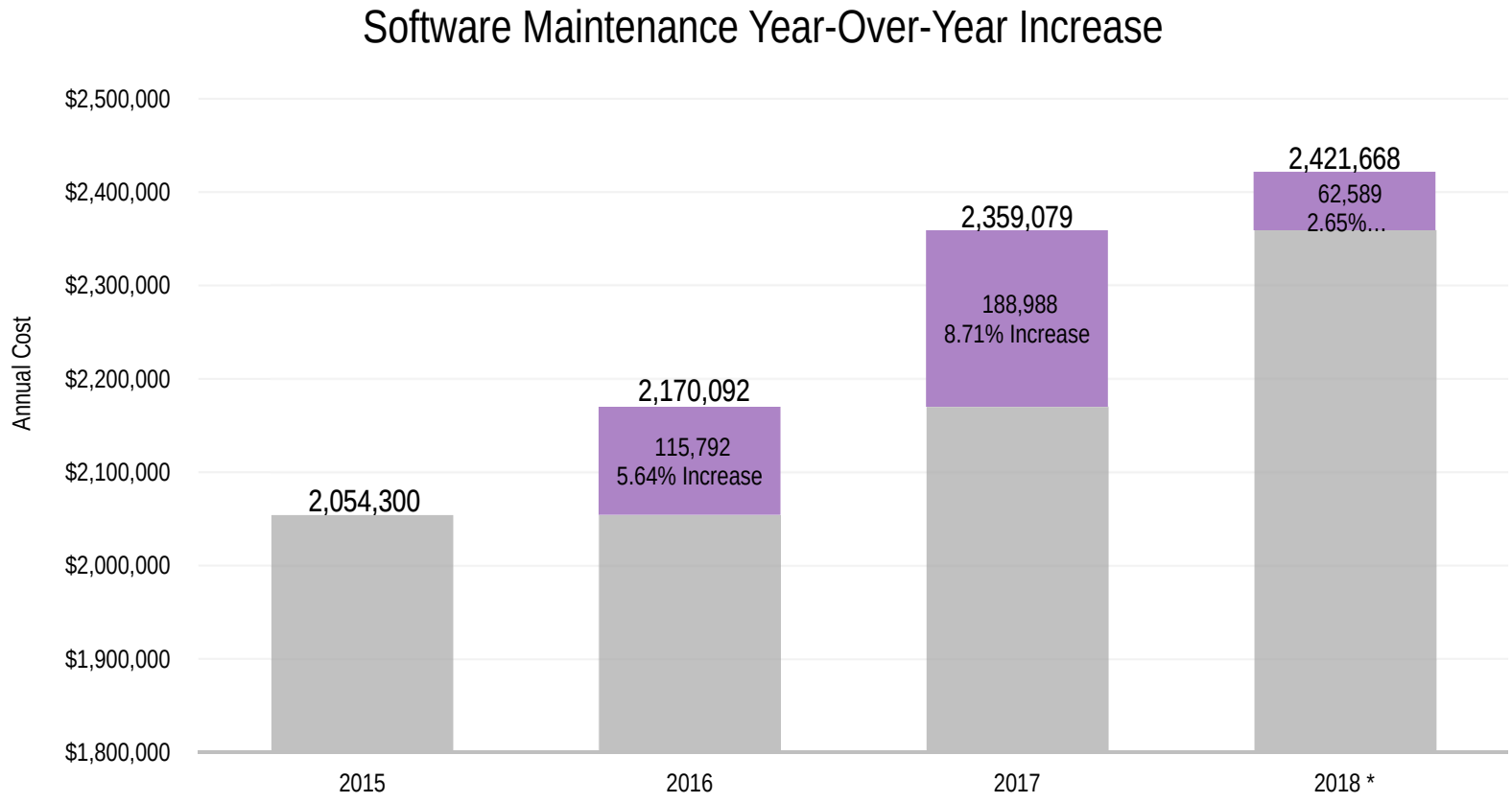
Software Maintenance Contracts
Critical Need Request

- Primary Technology Supplier Maintenance Contracts

  - Microsoft - Cisco - Veritas - VMWare
  - Oracle - NetApp - ESRI - Kronos

- Maintains current functionality and is a ***sole source of security patches***
- Costs increase 5% year over year and now consume 21% of the IT budget
- The increases in software maintenance costs diminish ability to fund capital replacement programs for network and data center infrastructure
- On Financial Roadmap Since 2016

Software Maintenance Contracts
Critical Need Request



2019 Information Technology Critical Need Requests Summary

Description	2018 Budget - OAB	2018 One-Time Funding	Other Internal changes	On-going Base Budget	2019 Critical Needs	2019 Requested Budget
Information Technology	11,610,561	0	0	11,610,561	2,050,000	13,660,561

1. Cyber Security Permanent Program Funding
   - Ongoing Security Program Funding ($760,000)
   - One-Time Tools & Technology Purchase ($340,000)
2. Office Replacement Program ($600,000)
3. Software Maintenance Contract Increases ($350,000)

Questions?

Add department/office name here