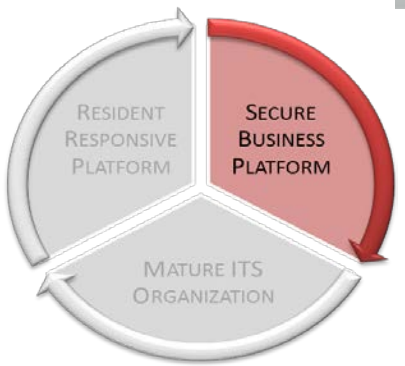
Board of County Commissioners
IT Services Funding Request

April 17, 2018

"Accelerating Speed to Strategic Value
Utilizing Quarterly Governance"

Security First



Secure Business Platforms

- ITS Strategic Business Plan Update
- FY18 Security First Funding Request: $2,307,000

This month I count 20,836,531 records leaked. This figure is likely to grow in the next few days.

Cyber attack

- Atlanta city government systems down due to ransomware attack
- Finger Lakes Health dealing with ransomware attack (Corrected)
- Atrium Hospitality Notifies Hotel Guests of Ransomware Incident
- MVSU Campus Loses Internet After Ransomware Attack
- Ca: JJ Meds was attacked today
- Pinelands Regional School District Computers Hit by Emotet Virus
- County employees targets of malware attack
- Jemison Internal Medicine discloses ransomware event

Data breach

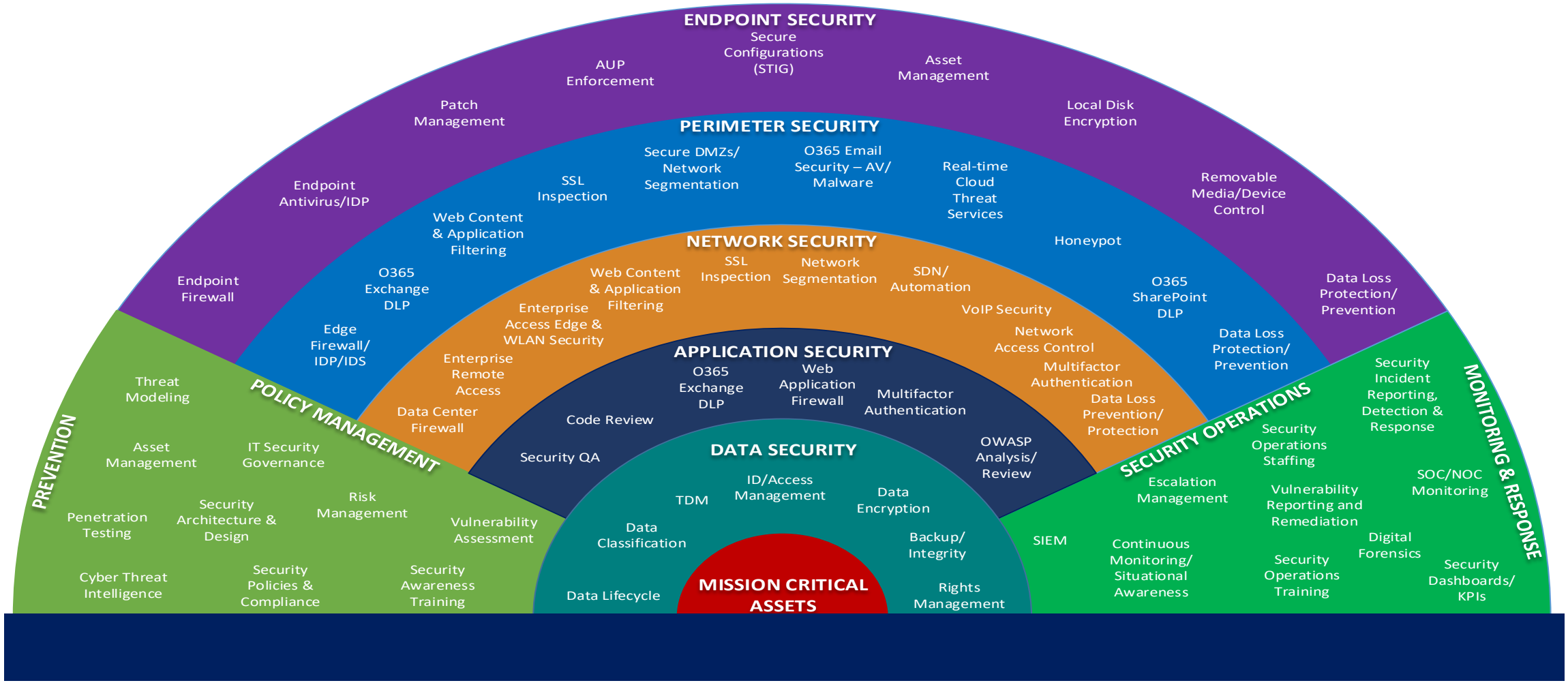
- License, ID data lost in crash: System failure affects 66,500 Hawaii residents
- Revealed! Personal data of 5 million ex-servicemen may have been breached, armed forces veteran calls it chilling
- Kent and Medway NHS and Social Care Partnership apologises for data breach
- Oregon tax agency employee copied personal data of 36,000 people
- SAMBA Federal Employee Benefit Association programming error resulted in mismailed information
- Southeast Clinical Pathology Laboratories Notifies Patients of Stolen Laptop
- Medical records exposed by flaw in Telstra Health's Argus software
- School district reports inadvertent disclosure
- CareMeridian notifies patients after disk goes missing in the mail
- Georgia MENTOR notifies patients after disk with protected health information discovered lost in the mail
- Primary Health Care notifies patients after discovering hack of employee email accounts
- National Lottery hacked: 10.5m players are warned to change their passwords
- The Dutch Data Protection Authority accidentally leaked its employees' data
- Nampa School District investigating cyber security breach
- Svitzer employee details stolen in data breach affecting almost half of its Australian employees
- Walmart jewelry partner exposed 1.3 million customer details
- Luxembourg Chamber of Deputies refers data leak to Prosecutor's Office
- Port of Longview hit with major cyberattack
- ATI Physical Therapy notifies patients of data breach
- FLVS leak affected 50,000 Leon County employees and students
- Used Tesco for your travel cash in the past? Your personal details may have been hit by a data leak at its provider Travelex

- Used Tesco for your travel cash in the past? Your personal details may have been hit by a data leak at its provider Travelex

- Owner says North Battleford store receiving private medical records via fax
- Personal data of 3,000 South Carolina college scholarship recipients exposed for nearly a year
- Approx. 9,000 Penn students affected by security breach that released their private information
- Medical and personal information on 33,420 BJC HealthCare patients left exposed on Internet
- Statistics Canada loses, mishandles hundreds of sensitive census, employment files
- Security breach affects 46 employees, family members at Columbia College Chicago
- Data Breach Left Millions of Israeli Kids' Pictures Vulnerable to Hacking
- Leon County Schools vendor's data leak exposed 368,000 current and former FLVS students' details, LCS teacher data, and more
- LA talent agency burglarized of three computers with private data
- Front Range Dermatology Associates suffers a breach of medical records
- Waltham Forest Council has breached data protection laws
- Officials: 2 ex-Florida Hospital employees stole, sold patient records
- Flexible Benefit Service Corporation notifies 5,123 of phishing incident
- Kansas Department for Aging and Disability Services Notifies 11,000 Consumers About Breach of Protected Health Information
- QuadMed health records system issue affected onsite clinics of three clients
- Tufts Health Plan notifies 70,320 members after vendor error exposes information in envelope window
- French news site L'Express exposed reader data online, failed to promptly secure it when notified
- Memorial Hospital at Gulfport Discloses Email Gaffe

CONTINUE & ACCELERATE OUR 3 YEAR STATEGIC PLAN: Layered Security Approach

Updates to ITS' 3-Year Strategic Plan represent an escalation of our strategic goals to support our "new normal" of security first practices and address security risks at multiple layers.



STRATEGIC BUSINESS PLAN IMPACT: FY18 Funding Request

Security Layer	#	Project	Justification	Amount
Policies & Prevention	1	eDiscovery	Enables a formalized process for eDiscovery or public information requests utilizing software that assist with the organization, redaction and publication of requested information. Current manual processes increases the risk of accidently providing sensitive information in public information request; this is a compliance and regulatory risk.	$ 456,000
	2	Text Message Archiving	Enables a formalized process for public information requests of text messaging data. Current manual processes increases the risk of accidently providing sensitive information in public information request; this is a compliance and regulatory risk.	$ 60,000
Security Operations & Monitoring Response	3	SIEM Replacement	Provides real-time analysis of security alerts generated by applications and network hardware. This piece of equipment collects security logs from all the devices connected to it and aggregates the information to look for threats inside our network. With this tool, we can view the activity on the network and respond faster.	$ 600,000
	4	KnowB4: Phishing Alert & Training Tool	Increased training and awareness will decrease the County's exposure to phishing attacks. This project will enable a security training and phishing alert platform for county staff and will also enable staff to safely and efficiently report suspicious emails to IT Security.	$ 106,000
	5	Vulnerability Scanning Licenses	This software will limit the level of vulnerabilities and unknown presence inside our network. HIPAA and PCI compliance require that we scan our entire network for vulnerabilities.	$ 100,000
	6	Network Monitoring Licenses	Provides real-time network performance monitoring. Having this visibility into the network's performance allows us to be proactive rather than reactive to network outages.	$ 125,000
Network	7	Network Access Controllers	This project will enables us to apply and enforce access policies across all access points to the County's network. Specifically, the tool validates and grants the level of access the device and/or user is authorized to have on our network. This product allows us to limit access to our network for everyone unless we grant them explicit permission.	$ 235,000
Application	8	Multifactor Authentication	Multifactor authentication is a security system that requires more than one method of authentication of credentials to verify the user's identity for a login or other transaction before gaining access to the County's network. This is best practice for organizations that offer hosted solutions to their staff outside of their internal network.	$ 100,000
Data	9	Backup & Recovery Appliance	The current backup device is at end of life and only allows us to recover one server at a time. Without a new solution, we have significant delays in restoring from major outages.	$ 500,000
	10	Active Directory Hardening	Active Directory (AD) controls who has access to applications and servers across the network. There are a significant number of improvements needed for our AD to be effective in managing user access.	$ 25,000
TOTAL				$2,307,000

Questions?