LOB #133:

CYBER SECURITY

Purpose

The IT/Cyber Security Office (ISO) is responsible for developing and enforcing policy, and defining the security requirements for the protection and operability of the County's IT assets. ISO determines the managerial, administrative, operational, and technical protection requirements and controls and enterprise architecture for the County government to protect County services and the confidentiality of sensitive information as required by Federal and Commonwealth regulation and industry oversight and standards. ISO is a key resource for responding to cyber-events that affect County government functioning and data breaches, as well as conducting and/or assisting in investigations and analysis of unauthorized use issues and cyber-security events. ISO is also responsible for ensuring awareness and knowledge of appropriate use of County IT resources. ISO is the authority for all matters pertaining to IT and Cyber Security and is authorized by the County Executive in carrying out the duties of the Office. Reference CEX PM 70-05 – IT Security Policy.

Description

The Information Security Office (ISO) LOB is a single program with a County-wide mission, housed in the Department of Information Technology. It is administratively managed by the Chief Technology Officer, with authority for compliance and risk through the County Executive. To ensure best practices segregation of duties standard, ISO is organized in teams in specific areas:

- Policy, Governance and Awareness
- Monitoring, Investigations and Compliance
- Security Operations: Engineering and Administration, and Identity Access and Controls
- Security Architecture and Design

IT Security was established as an essential function in the Department of Information Technology at its inception in 1997, and evolved to the current ISO model over the years as the IT industry and security risks dynamically expanded and accelerated.

Ten staff members are assigned to the various areas of the mission. The work is augmented by expert consultants. The County's cyber security program helps ensure that the County's information technology resources secure the confidentiality, integrity, and availability of sensitive information in which the County has been entrusted: this may include, but is not limited to sensitive personally-identifiable information such as social security numbers, HIPAA, credit card data (PCI-DSS), law enforcement and court data. In order to carry out its mission, ISO has developed a policy and management framework for information security, authorized by the County Executive. ISO serves as a catalyst for ensuring that cyber security controls and practices are integrated into planned and ongoing County agencies and DIT operations. The managing position is the Chief Information Security Officer (CISO) who reports to the Chief Technology Officer, receiving authority for compliance activities from the County Executive and risk tolerance guidance from the Senior IT Steering Committee.

ISO works with other technology expert areas in DIT in carrying out its architecture and engineering work. The CISO is standing member of the DIT leadership team, and the position is in the DIT leadership line of succession.

Specific activities of the Information Security Office staff include:

- Exploring and assessing information security risks to business operations. Researching potential threats, vulnerabilities, and control techniques and communicating this information to agencies and senior leadership as necessary;
- Determining what policies, standards, and controls must be implemented to reduce these risks. Developing and adjusting countywide policies and procedures to ensure information systems confidentiality, integrity and availability, and to prevent and defend against unauthorized access to systems, networks and data;
- Participating as an active member in the DIT Architecture Review Board which reviews application and proposed network architecture implementations and changes and recommend enhancements to enhance security posture;
- Implementing and managing malicious code protection platforms. This strategy includes a defense-in-depth architecture with multiple layers of protection, detection, and prevention at the endpoint, network, and application layers (workstation, intrusion detection systems and next-gen firewalls, and email gateways);
- Providing incident response and forensic capabilities in the event of a data breach, exposure, or system/application compromise;
- Facilitating the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes; assisting in the fulfillment of eDiscovery requests as the result of litigation, collecting and fulfilling electronic records requested through Virginia Freedom of Information Act, and providing information as required by agency personnel investigations or audit requests;
- Developing and implementing secure Identity Management Platforms for managing user access to enterprise network and applications as well as customer-facing portals that provide mission essential services;
- Participating in internal and external audits to assure compliance with regulatory requirements (Financial systems, HIPAA);
- Developing and implementing a robust cyber security awareness program to ensure that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures. Current activities include New Employee Orientation, an annual Cyber Security Awareness Day, and a phased deployment of online refresher training to all County agency personnel;
- Conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. Activities include enterprise perimeter and internal vulnerability assessments and penetration testing against endpoints, servers and other supporting infrastructure. This program enables ISO to identify potential weaknesses or exploitable vulnerabilities that could result in unauthorized access or breach to systems or information;
- Developing systems security contingency plans and disaster recovery procedures.

Fairfax County CISO also provides leadership and expertise for cyber security initiatives in the Council of Governments member jurisdictions/ DHS National Capital Region.

Benefits

IT Security is an essential function to the integrity and operation of County government based on:

- Increased dependency upon technology
- Dynamic increase in cyber-attack activity world-wide
- Ensure the confidentiality, integrity and availability of County data and systems that enable County operations and provide essential services to constituents
- Ensure compliance with Federal, Commonwealth, and industry regulation
- Retain confidence of constituents, partners, and other stakeholders in properly handling sensitive information
- Minimize Federal or Commonwealth fines, industry financial penalties, or other revenue losses due to breach of sensitive information such as HIPAA or credit card holder data or unavailability of critical systems
- Safeguard the confidence in and image of County government.

A cybersecurity incident could degrade critical County agencies' services, cause financial damage, harm the County's reputation and ultimately harm citizens and businesses served.

The County's IT Security Program and Policy has been recognized by multiple industry and governmental organizations as a Best Practice, to include National Association of Counties (NACO), Center for Digital Government, Information Security Executive (ISE) conference, Federal government Cyber 7, and the Commonwealth of Virginia. Staff from DIT and ITPAC serve on the Federal Government's Cyber Security Symposium Planning Committee.

Mandates

Cyber security and the protection of sensitive information is a critical aspect of electronic data management and is regulated by multiple applicable compliance requirements throughout Federal law, Virginia Code, Industry oversight and County policy. Included below are links to applicable regulation requiring mandated compliance:

- Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996),
- Code of Virginia §18.2-186.6. Breach of personal information notification
- Code of Virginia § 32.1-127.1:05. Breach of medical information notification
- Payment Card Industry (PCI) Data Security Standard
- Commonwealth Executive Order EO-39: Launching "Cyber Virginia" and the Virginia Cyber Security Commission

Trends and Challenges

There is an increasing trend and frequency of various types of threats conducted as cyber-terrorism, crime and thievery, identity theft and all types of organizations are targets. Critical Infrastructure Protection is also now a concern for IT Security professionals, as well as a key role in Continuity of Operations planning and disaster recovery plans. IT Security also has an instrumental role in the outcome of financial audits and rating agencies' determinations as well as roles on reviewing, assessing and advising on the impact of new regulations and mandates affecting technology services and electronic data. Another related trend for organizations is 'Cyber Insurance'. Other core issues for ISO include balancing data privacy requirements against open-government goals, keeping up with various related federal regulatory churn (federal and state requirements as well as government-to-government,) and government-to-business interoperability.

Also, the landscape of technology opportunities, the WEB and cyber security is dramatically changing with growth in the consumer markets for mobile devices, such as smart phones and tablets, to network-enabled industrial control systems (HVAC, Physical Access Control, lighting systems, supervisory control and data acquisition (SCADA) systems, etc.). 'Clouds' present more complex risk and challenges as these solutions are adopted. As product development transforms the enterprise-enabled landscape, the ISO will need to adapt to evolving threats targeting untraditional endpoints and data repositories. ISO anticipates a 5 percent increase in malicious code detections in FY 2016 and FY 2017 and a continued increase in the collection of electronic records related to agency personnel investigations, legal requests, and Freedom of Information Act requests. Recent changes in Credit Card industry standards will require the County to renew point of sale machines to use the chip technology, and the County to adopt other modern commercial payment apps.

A key challenge for IT Security is balancing ultimate protective measures against reasonable risk, and users understanding of the criticality and consequences of their actions and adopting a cybersecurity mindset.

Resources

Category	FY 2014 Actual	FY 2015 Actual	FY 2016 Adopted
LOB #133: Cybersecurity			
FUNDING			
Expenditures:			
Compensation	$766,478	$811,592	$849,295
Operating Expenses	430,319	744,361	316,783
Total Expenditures	$1,196,797	$1,555,953	$1,166,078
General Fund Revenue	$0	$0	$0
Net Cost/(Savings) to General Fund	$1,196,797	$1,555,953	$1,166,078
POSITIONS			
Authorized Positions/Full-Time Equivalents (FTEs)			
Positions:			
Regular	10 / 10	10 / 10	10 / 10
Total Positions	10 / 10	10 / 10	10 / 10

Metrics

Metric Indicator	FY 2013 Actual	FY 2014 Actual	FY 2015 Actual	FY 2016 Estimate	FY 2017 Estimate
Number of Records Requested for Investigations	42	179	45	92	96
Number of Security Events	103	113	73	100	105
Number of Malware Detections	7,841,131	7,173,155	7,717,330	7,956,416	8,354,236
Cybersecurity Incidents that caused Loss of Production Data	0	0	0	0	0

The number of records requested for investigations are anticipated to rise in FY 2016 and FY 2017 due to the increased requests from Internal Audit, agency personnel, the Police Department, and the County Attorney. It should be noted that in FY 2014, there were an unusual amount of requests for email records related to litigation preservation that caused the substantial spike that fiscal year.

The number of security events held are anticipated to remain in line with prior year experience. These events will focus on stolen/lost devices, information handling, IT security policy violations and other IT security issues.

The number of malware detections are anticipated to rise in FY 2016 and FY 2017 due to the increased number and types of computer viruses.

Cybersecurity incidents that have caused loss of production data has been zero since FY 2002.