Status Update: Cook County Information Security

SENSITIVE AND INFORMATION SECURITY RELATED

September 2018

Purpose

The Chief Information Security Officer's (CISO's) semi – annual report shall detail:

- The status of all Agencies' adoption and compliance with the Information Security Framework (ISF); and
- A summary of all advice and recommendations of each Agency regarding their unique considerations.

Addressed Multiple Cyber Threats – Feb '18 to Jul '18

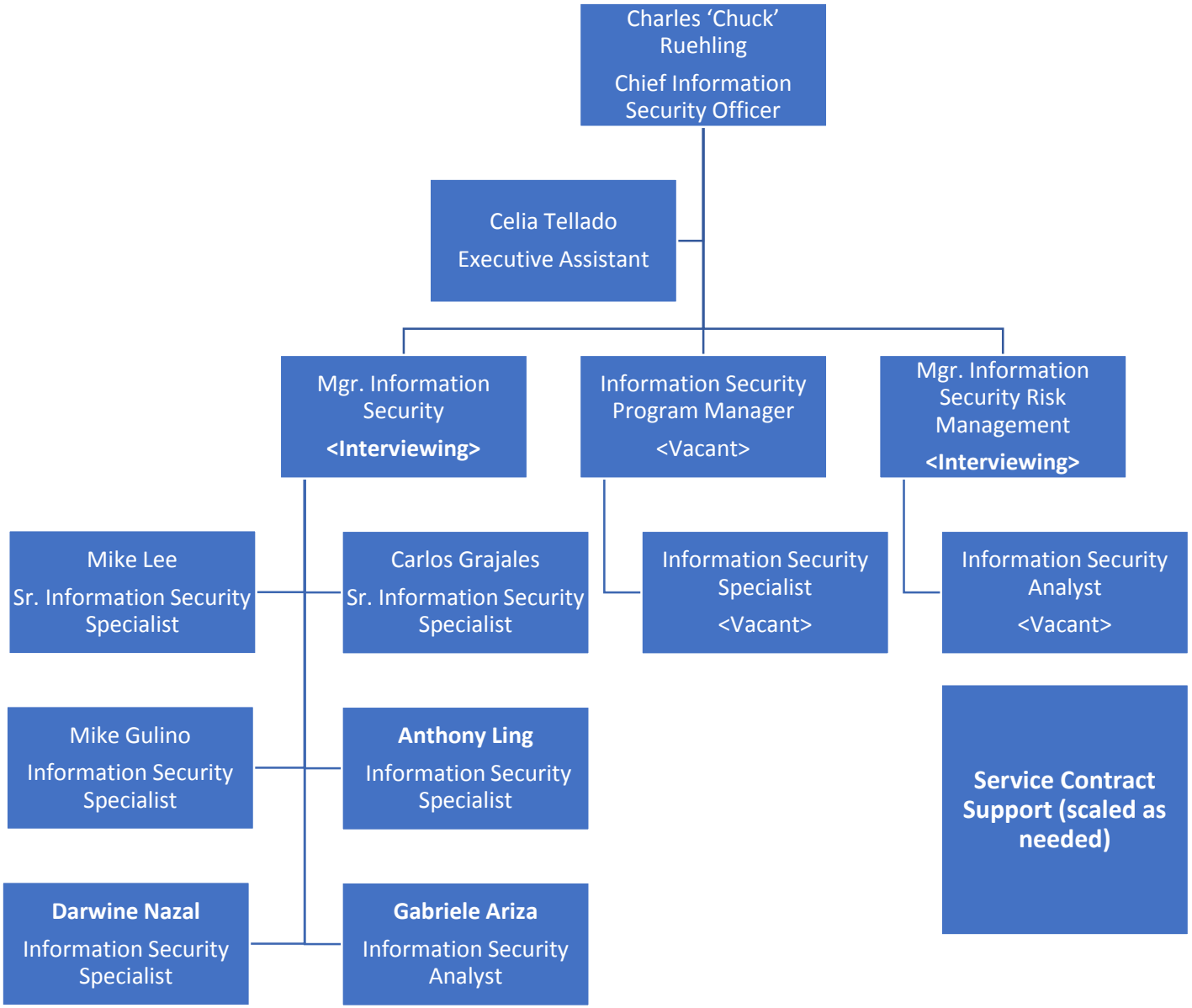
EternalBlue Ransomware	EternalRomance Ransomware	Eternal Tools	WannaCry (leveraged EternalBlue and EternalRomance ransomware)	Bad Rabbit Ransomware
Petya/NotPetya Ransomware	WannaCry Malware			Adobe Acrobat Reader Memory Corruption Vulnerability (CVE-2017-3122)
Adobe Acrobat Professional security bypass vulnerability CVE-2016-1079	Adobe Acrobat Reader Memory Corruption Remote Code Execution (CVE-2017-11238)	Adobe Acrobat Reader Memory Corruption Vulnerability (CVE-2016-4255)	Adobe Acrobat Reader Open Type Font File Format Vulnerability	Adobe Acrobat Reader stack buffer overflow vulnerability (CVE-2017-2948)
Adobe Acrobat Reader Stack Overflow Vulnerability (CVE-2017-2941)	Adobe Acrobat Reader TIFF File Heap Overflow Vulnerability (CVE-2017-2940)	Adobe Acrobat Reader Type Confusion Remote Code Execution (CVE-2017-11221)	Adobe Acrobat Reader Use After Free Vulnerability (CVE-2016-1089)	Adobe Acrobat Type Confusion Vulnerability (CVE-2017-16406)
Adobe Acrobat Reader Use After Free Vulnerability(CVE-2016-0932)	Cross Site Scripting (XSS) Attacks	Adobe Flash Player – Too many to name individually	Adobe Reader– Too many to name individually	Adobe Shockwave Player – Too many to name individually

Total Events: 34,165,022,421

Security Events: 1,254,930,523

Incidents (Tickets): 682

Information Security Office Organizational Chart



Information Security Office (ISO)

December 2017

Information Security Office (ISO) realigned under Bureau of Technology

February 2018

Recruit and Hire Chief Information Security Officer (CISO)

March 2018

Define / Update Mission, Vision Statement for CISO

April - May 2018

Outreach / Introductions to System Stakeholder Community

June 2018

Tabletop Exercise & Begin Development of Stakeholder Training

July 2018

Strategic Plan Updates – Budget Defense

June – August 2018

Recruit, Interview and Onboard New Team Members

Policy Reviews

Team Building

Education and Outreach

Gap Analysis / Prioritize Resources

Mission

The Information Security Office (ISO) protects the confidentiality, integrity and availability of **all Cook County information** by leveraging cybersecurity capabilities across the enterprise and informing system stakeholders on cyber risk. The ISO provides enterprise tools, policies, security engineering, training and awareness focused on defeating evolving cybersecurity threats.

In short: Our mission is to help secure yours

Vision

- **Mature the County's implementation of the Information Security Framework**
- **Proactively address threats and enhance the current capabilities**
- **Integrate early into the System Development Life Cycle (SDLC)**
- **Recruit and retain motivated cybersecurity talent**

Maturing of the Information Security Framework (ISF)

- Reasons for NIST over ISO
  - Free! and Readily Available
  - Comprehensive
  - Federal Agencies and DoD have adopted the NIST Risk Management Framework (RMF) as the Standard in Government
  - Intelligence Community and Committee on National Security Systems (CNSS) tie back to the NIST Standards
- Information Security Working Group Approved

Agency Support

- Provided Agencies IT Security Staff Vendor Training on the McAfee Toolset
- Increased Mobile Device Management for County Owned Cell Phones
- Began Weekly Cyber Threat Intelligence Briefings to the IT Community
- Consulted with BoT, CCHHS and Sheriff on Security Requirements for VoIP Deployments
- Worked with Recorder of Deeds to increase Website Availability

2018 Projects / Events

SECURITY INCIDENT RESPONSE TABLETOP EXERCISE

- Conducted a tabletop exercise to prepare for potential cybersecurity threats we may face. We will also conduct executive security awareness training Countywide.

INFORMATION SECURITY STRATEGIC PLANNING

- Produced a Risk Management Framework (RMF) Implementation Plan. The plan outlines all major milestones and resources required to achieve a mature RMF implementation.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RISK ASSESSMENT

- Conducting a risk assessment of our information systems and organizations. Risk assessments, are part of an overall risk management process — providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

CRITICAL APPLICATION CODE REVIEW

- Conducting a code review of County's critical applications. Findings may be vulnerabilities, architectural problems, organization problems, failure to follow best practices or standards or best practices that deserve recognition.

Cyber Security Challenges / Focus

Information security is a continuous process that requires due diligence, expertise and collaboration from all agencies to ensure that Cook County is adequately prepared for cyber security threats.

A modern cybersecurity program must have Board and Executive level visibility, funding and support.

In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters.

QUESTIONS