Status Update: Cook County Information Security

SENSITIVE AND INFORMATION SECURITY RELATED

August 2020

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 ‘19 to Jul ‘19

EternalBlue Ransomware

EternalRomance Ransomware

Eternal Tools

WannaCry (leveraged EternalBlue and EternalRomance ransomware)

Bad Rabbit Ransomware

Petya/NotPetya Ransomware

Virut Malware

Kraken Malware

FakeAV Exploit Kit

Adobe Acrobat Professional Memory Corruption Vulnerability (CVE-2017-3122)

Adobe Acrobat Professional security bypass vulnerability_CVE-2016-1042

Adobe Acrobat Reader Memory Corruption Remote Code Execution (CVE-2017-11238)

Adobe Acrobat Reader Memory Corruption Vulnerability (CVE-201[illegible]-4195)

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 (Denial of Service)

Adobe Acrobat Reader TIFF File Heap Overflow Vulnerability (CVE-2017-3049)

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 Use After Free Vulnerability(CVE-2016-0932)

Cisco Syslog DoS attacks

Adobe Flash Player – Too many to name individually

Adobe Reader– Too many to name individually

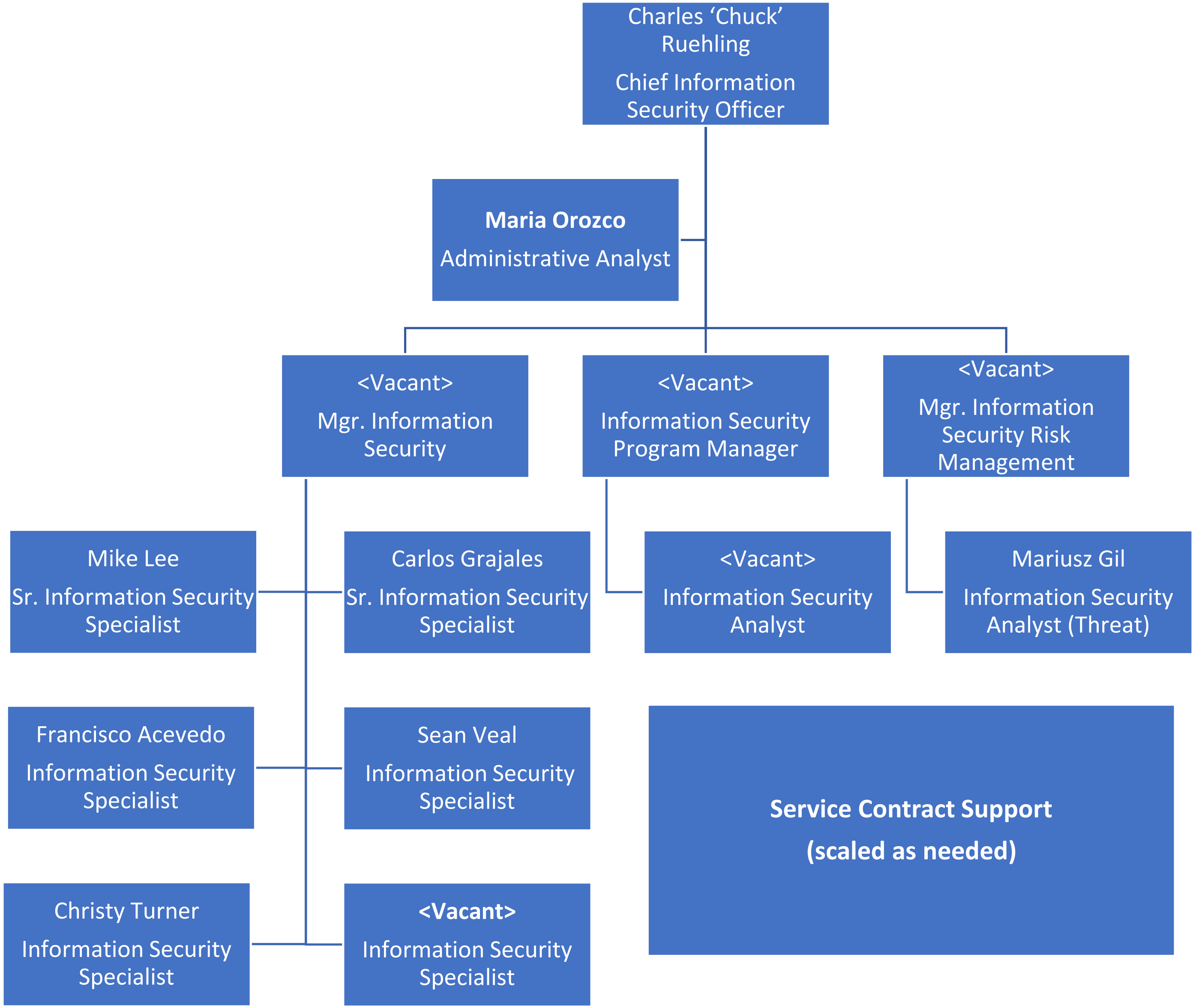
Adobe Shockwave Player – Too many to name individually

Total Events: 83,757,498,940

Security Events: 547,851,910

Incidents (Tickets): 704

Information Security Office Organizational Chart



Charles ‘Chuck’ Ruehling

Chief Information Security Officer

Maria Orozco

Administrative Analyst

<Vacant>

Mgr. Information Security

<Vacant>

Information Security Program Manager

<Vacant>

Mgr. Information Security Risk Management

Mike Lee

Sr. Information Security Specialist

Carlos Grajales

Sr. Information Security Specialist

<Vacant>

Information Security Analyst

Mariusz Gil

Information Security Analyst (Threat)

Francisco Acevedo

Information Security Specialist

Sean Veal

Information Security Specialist

Service Contract Support

(scaled as needed)

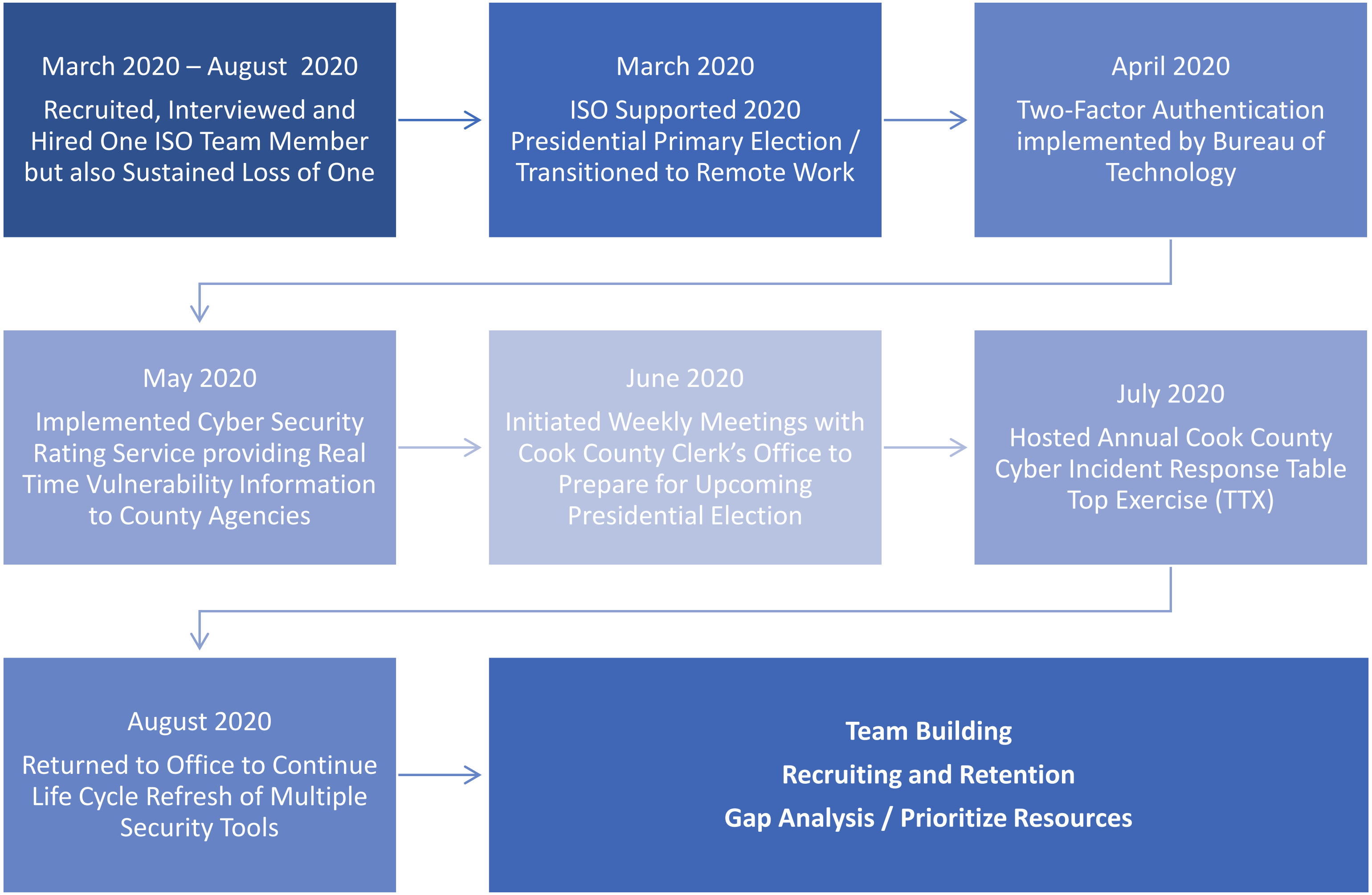
Christy Turner

Information Security Specialist

<Vacant>

Information Security Specialist

Information Security Office (ISO) Major Events



March 2020 – August 2020

Recruited, Interviewed and Hired One ISO Team Member but also Sustained Loss of One

March 2020

ISO Supported 2020 Presidential Primary Election / Transitioned to Remote Work

April 2020

Two-Factor Authentication implemented by Bureau of Technology

May 2020

Implemented Cyber Security Rating Service providing Real Time Vulnerability Information to County Agencies

June 2020

Initiated Weekly Meetings with Cook County Clerk's Office to Prepare for Upcoming Presidential Election

July 2020

Hosted Annual Cook County Cyber Incident Response Table Top Exercise (TTX)

August 2020

Returned to Office to Continue Life Cycle Refresh of Multiple Security Tools

Team Building

Recruiting and Retention

Gap Analysis / Prioritize Resources

Agency Support

Completed Drafts on Five Information Security Framework Policies in an 18 to 24 Month Effort Culminating in a Risk Management Framework

Began Request for Proposal Process for expiring Managed Security Service Provider (MSSP) contract that will end in July 2021

Continued Working with Enterprise Business Services (EBS) Cloud Migration Initiative to Ensure Integration of Security Controls in New Cloud Environment

Working with Several Agencies to Integrate ISO Tool Sets more Comprehensively into IT Environments

2020 Projects / Events

RISK MANAGEMENT FRAMEWORK TRAINING DEVELOPMENT

- In 2021, the Information Security Office (ISO) will develop Risk Management role-based training that aligns with updated Security Policy. This role-based training will be available for the Executive level and below.

INFRASTRUCTURE REFRESH OF THE SECURITY TOOL STACK

- In 2021, the ISO will continue the refresh of information technology in the security tool stack that is at end of life for vendor support while evaluating capabilities.

SECURITY INCIDENT RESPONSE TABLETOP EXERCISE (TTX)

- Building on the After Action Report (AAR) and lessons learned from the July 2020 TTX will continue to mature the Incident Response TTX for 2021

INFORMATION SECURITY OFFICE STAFFING

- Recruit and retain motivated cybersecurity talent that is technically proficient, team-oriented and service-minded. Leverage contract resources to enhance capabilities where appropriate.

Cyber Security Challenges

Evolving Adversaries & Threats

Talent Recruitment & Retention

Team Building

Mature Capabilities

Cyber Hygiene

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.

Questions