Cyber Threat Incidents/Trends Overview June 14, 2018

Table of Contents

Section 1	Background About CRA	2
Section 2	Key Team Members	4
Section 3	Current Attack Trends	6
Section 4	Incident Response Process	9
Section 5	Risk Mitigation	12



Section 1 Background About CRA



About CRA

Charles River Associates is a leading global consulting firm that provides independent economic and financial analysis of litigation matters; delivers independent forensic and cyber investigation services; guides businesses through critical strategy and operational issues to become more profitable; and advises governments and regulatory agencies on the economic impact of policies and regulations. We are headquartered in Boston with over 650 professionals located in seven countries around the world and are able to respond nimbly to events on a global scale. CRA has served major law firms, corporations, and governments around the world for the past fifty years, and has worked with over 90% of Am Law 100 law firms and over 65% of Fortune 100 companies.





Section 2

Key Members of our Team



Team Member Bios

Name

Andy Obuchowski / Boston Office

Experience



Andy leads high-profile cybercrime and data breach investigations and provides digital forensics and incidence response services. His experience includes managing teams responsible for data breach investigations, complex digital forensic collections, network vulnerability and rapid security assessments. Mr. Obuchowski has substantial experience providing testimony a deposition, hearings, and bench and jury trials. As a former law enforcement officer and Special US Marshall with the Regional Electronic & Computer Crime Task Force (REACCT), he managed digital-related investigations on all types of media, ensured compliance with accepted computer forensic protocols, and presented testimony for numerous criminal cases. Mr. Obuchowski holds numerous certifications and has earned his Master's in National Security. He is also an adjunct professor at Anna Maria College.

Email: aobuchowski@crai.com | **Office:** 617.425.3549 | **Mobile:** 508.922.4770

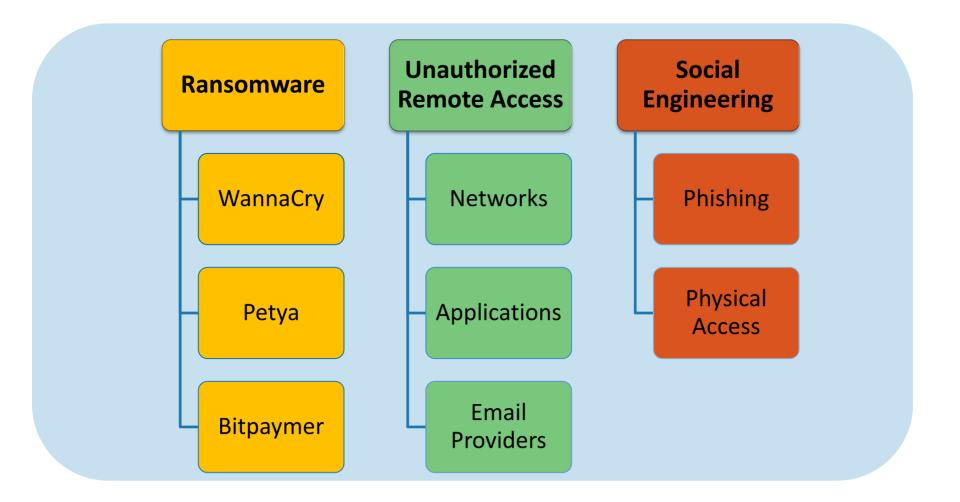


Section 3 Current Attack Trends











Section 4 Incident Response Process



Incident Scoping & Evidence Preservation

Collect information surrounding the incident to identify and preserve all potential sources of evidence

Define Period of Compromise

Establish timeline of events for the incident and when was it contained

Production of Data for Review

Compile clean data set that may require further analysis and action











Forensic Analysis

Analyze relevant sources of evidence for malicious activity or unauthorized access to electronic data

Evaluate Risk of Harm to Information

Determine the type of electronic data that could have been accessed during the period of compromise



Process Summary

Containment

- Threat
 Identification
- Threat Hunting
- Configuration Changes
- Vulnerability Testing
- Patch Management
- Batch Scripting
- Evidence Preservation

Analysis

- Malware Analysis
- Collection Scripts
- Dark Web
 Threat Intel
- Event Timeline
- Structured and Unstructured Data Triage
- Data Processing & Review

Reporting

- Executive Summary
- Detailed Reports
- Under Counsel Direction
- Acronyms to Short Stories
- Qualified Experts

Remediation



Section 5

Risk Mitigation



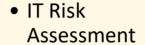
Administrative Tasks

Organizational Programs



- Written Information Security Programs
- Vendor management
- Business
 Continuity and disaster recovery

Preparation Tasks



- Incident response plan
- Mock incident response drills
- Security awareness training

Response

- Documentation
- Trained resources
- Qualified vendors



Technical Tasks

- Data segregation
 - Data classification/identification program
- Network and application patch management
- Backup and archiving solutions
 - Access to data backup and offsite facilities
 - Test archiving solutions (email, data vaults)
 - Speed of exports, change in file properties, search functionality
- Network vulnerability testing
- Enterprise monitoring solutions
 - Event logging (VPN, file audit, network access, building access)
 - Data Loss Prevention (DLP) solutions

