Cyber Crime Checklist for Police Chiefs

This Chief's Checklist 2015 is a quick reference guide designed to support police chiefs in understanding the broad topics of cyber crime, specific action items to be addressed, and resources available to assist in these efforts. In addition to creating an outline of cyber crime fundamentals, the Checklist links to resources which elaborate on these topics in greater detail and connect chiefs to subject matter experts for further collaboration. The information contained in the Checklist is not an exhaustive resource, however, it highlights core information to help law enforcement executives better protect their agencies from cyber threats and better serve their communities.

Step 1: Learn the Fundamentals

1.1 Take Advantage of available materials

- Law Enforcement Cyber Center 101: http://www.iacpcybercenter.org/law-enforcement-cyber-center-101/
- Learn how to get the most out of the Cyber Center: http://www.iacpcybercenter.org/chiefs/how-can- the-cyber-center-help-chiefs/
- Develop an understanding of Cyber Crime: http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/
- Visit the Chiefs Corner often to remain up-to-date on current issues affecting Leaders in Law Enforcement: http://www.iacpcybercenter.org/chiefs-corner/

1.2 Leverage training to build a basic understanding of cybercrime and advanced considerations

- Have all sworn officers and select civilian staff complete one or more of the following free online cyber training courses provided by the National White Collar Crime Center (NW3C):
  - Cyber Investigation 100 – Identifying and Seizing Electronic Equipment: http://www.nw3c.org/training/computer-crime/23
  - Cybercop 101 – Basic Data Recovery and Acquisition: http://www.nw3c.org/training/computer-crime/4
  - Cyber Investigation 120 – Cell Phone Seizure and Acquisition: http://www.nw3c.org/training/computer-crime/119
  - Social Media 101 – What Law Enforcement Needs to Know: http://www.nw3c.org/training/online-training/81
  - Cyberbullying: Our Children, Our Problem: http://www.nw3c.org/training/online-training/105
- For advanced training, complete the Cyber Certification Program Prerequisite Training offered by the FBI's Cyber Shield Alliance. This training consists of five, self-paced class suites (approximately 29 hours), and can be accessed through the Law Enforcement Enterprise Portal at: https://www.cjis.gov
- Additional information on free online training is available on the LECC at: http://www.iacpcybercenter.org/topics/training-2/free-training-for-law-enforcement/

Step 2: Develop a Plan

2.1 Define program goals, objectives, and desired outcomes

- Ensure appropriate staff reviews IT Security and Security Assessments to evaluate an organization's operational resilience and cyber security practices: http://www.iacpcybercenter.org/chiefs/it-security/
    - Cyber Resilience Review (CRR): https://www.us-cert.gov/ccubedvp/self-service-crr
    - National Cybersecurity and Communications Integration Center: http://www.lba.org/files/DHS_NCATS_Fact_Sheet_2014.pdf
    - National Campaign for Cyber Hygiene: http://www.cisecurity.org/about/CyberCampaign2014.cfm
- Promote a greater understanding of cyber crime investigations: http://www.iacpcybercenter.org/chiefs/cyber-crime-investigations/
    - Investigation information for patrol officers: http://www.iacpcybercenter.org/officers/cyber-crime-investigations/
        - Handling digital evidence for the patrol officer: http://www.iacpcybercenter.org/officers/digital-evidence/
        - Common electronic devices that generate digital evidence: http://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/
        - Handling evidence from specific sources: http://www.iacpcybercenter.org/officers/cyber-crime-investigations/handling-evidence-from-specific-sources/
    - Investigation information for cyber crime investigators: http://www.iacpcybercenter.org/investigators/cyber-crime-investigations/
        - Handling digital evidence for the cyber crime investigator: http://www.iacpcybercenter.org/investigators/digital-evidence/
- Legal considerations: http://www.iacpcybercenter.org/topics/legal-issues/
        - Digital search warrants: http://www.iacpcybercenter.org/topics/legal-issues/digital-search-warrants/
        - Relevant federal statutes: http://www.iacpcybercenter.org/topics/legal-issues/8-2relevant-federal-statutes/
- Review training opportunities and resources: http://www.iacpcybercenter.org/chiefs/training/
    - Provide targeted training by subject matter: http://www.iacpcybercenter.org/topics/training-2/
    - Cyber and IT certifications: http://www.iacpcybercenter.org/topics/training-2/cyber-and-it-certifications/
- Personnel development: http://www.iacpcybercenter.org/chiefs/personnel-development/

2.2 Understand program costs and identify next steps

- Review Protection on a budget (SANS Institute Whitepaper: Practical Threat Management and Incident Response, June, 2014): https://www.sans.org/reading- room/whitepapers /analyst/practical-threat-management-incident-response-small-medium- sized-enterprises-35257
- Review PERF Report: Critical Issues in Policing: The Role of Law Enforcement Agencies in Preventing and Investigation Cybercrime: http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf
- Calculating the cost of a cyber attack from Cyber Tab: https://cybertab.boozallen.com/

2.3 Indentify stakeholders and resources to inform policy

- Determine strategic partnerships: http://www.iacpcybercenter.org/about-the-cyber-center/partners/
- Review cyber threat bulletins: http://www.iacpcybercenter.org/resource-center/cyber-threat-bulletins/
- FBI's Cyber Shield Alliance available through the LEEP Portal: https://www.cjis.gov /CJISEAI/EAIController
- National White Collar Crime Center (NW3C): http://www.nw3c.org/

2.4 Develop appropriate cyber policy for agency

- MS-ISAC State Cyber and Information Security Policies: http://msisac.cisecurity.org/resources/state-cyber-policies.cfm
- MS-ISAC Local Government Cyber and Information Security Policies: http://msisac.cisecurity.org/resources/local-cyber-policies.cfm
- Cybersecurity Handbook for Cities and Counties: http://msisac.cisecurity.org/resources/guides/documents/DC_Mag_Dec12.pdf

Step 3: Identify Working Groups and Leverage Opportunities

3.1 Identify regional resources that offer economy of scale and program support

- Consult Regional Capabilities List to search for resources available in your area (including state, federal, and private sector entities). Link coming soon!
- Utilize proven Strategic Partnerships: http://www.iacpcybercenter.org/about-the-cyber-center/partners/
- FBI Cyber Crimes Task Forces: https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1
- Secret Service Electronic Crimes Task Force and Working Groups: http://www.secretservice.gov/ectf.shtml

Step 4: Develop Appropriate Policies and Key Protocols

4.1 Understand local and state laws affecting cyber crime

- Understanding Cybercrime Legislation: http://www.brighthub.com/internet/security-privacy/articles/68442.aspx
- The following reference guide provides a description of all types of cyber crime: http://msisac.cisecurity.org/resources/toolkit/oct13/documents/Cyber_Crime.pdf
- Cybercrime in the Future: http://www.brighthub.com/internet/security-privacy/articles/68548.aspx

4.2 Review available resources

- Cyberspace Policy Review: http://msisac.cisecurity.org/resources/reports/documents/CyberspacePolicyReviewMay2009.pdf
- Combating Cyber Crime: http://www.dhs.gov/topic/combating-cyber-crime

4.3 Develop appropriate written policies for specific topics, such as:

- IT Security
- Cyber Crime Investigations
- Forensics
- Training
- Stakeholder Engagement

Step 5: Identify Outreach Resources

5.1 Cyber Crime Community Resources; Protecting Family and Friends

- Information on how to protect yourself online through Stop. Think. Connect: http://www.dhs.gov/stopthinkconnect
- Project iGuardian helps kids, teens and parents to be smart about online safety and stay safe from online sexual predators: http://www.ice.gov/cyber-crimes/iguardian
- US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world: https://www.us-cert.gov/
- Internet Crimes Against Children Task Force (ICAC): https://www.icactaskforce.org/Pages/Home.aspx

5.2 Cyber Crime Resources for Law Enforcement

- Department of Homeland Security Fusion Centers: http://www.dhs.gov/fusion-center-locations-and-contact-information
- FBI Field Offices: https://www.fbi.gov/contact-us/field
- Infraguard: https://www.infragard.org/
- The FBI's Cyber Action Team – Rapidly Responding to Major Computer Intrusions: https://www.fbi.gov/news/stories/2015/march/the-cyber-action-team
- Multi-State Information Sharing and Analysis Center (MS-ISAC): http://msisac.cisecurity.org/

5.3 High Technology Crime Assistance for Law Enforcement

- International Association of Crime Analysts: http://www.iacis.com/
- Regional Computer Forensics Laboratories (RCFLs): https://www.rcfl.gov/
- High Technology Crime Investigation Association (HTCIA): https://www.htcia.org/

Step 6: Work with Agency Providers and Cyber Subject Matter Experts (SMEs) regarding Technology Solutions

6.1 Define hardware and software requirements

- Securing Federal Networks: http://www.dhs.gov/topic/securing-federal-networks
- Protecting Critical Infrastructure: http://www.dhs.gov/topic/protecting-critical-infrastructure
- Information Sharing: http://www.dhs.gov/topic/cybersecurity-information-sharing

6.2 Assess current capabilities and identify needed areas of improvement

The following guides are useful in assessing the current state of preparedness and determining areas of improvement of your department's internal cyber security system:

- Cyber Security Getting Started: A Non-Technical Guide: http://msisac.cisecurity.org/resources/guides/documents/Getting_Started_Print.pdf
- Internet and Acceptable Use Policy: http://msisac.cisecurity.org/resources/guides/documents/Acceptable%20Use%20Guide.pdf
- Erasing Information and Disposing of Electronic Media: http://its.ny.gov/sites/default/files/documents/Erasing-Information-and-Disposal-of-Electronic-Media-2012.pdf
- Guidelines for Backing Up Information: http://msisac.cisecurity.org/resources/guides/documents/Backing-Up-Information-Guide.pdf
- Risk Management Guide: http://msisac.cisecurity.org/resources/guides/documents/Risk- Management-Guide.pdf
- Cyber Research and Development: http://www.dhs.gov/science-and-technology/csd-projects