Law Enforcement Cyber Center

Cyber Report Card - **Police Executives**

1.1 Account & Password Management

#	Question	Yes	No	Comments
1	Are passwords used throughout your agency secure, i.e., not easy to guess, regularly changed, not set to temporary or default passwords, and securely stored? This applies to both end user passwords, as well as those used by software applications.			*Weak passwords make it easy for unauthorized users to access critical information resources. Your agency should require users to establish and regularly update strong passwords.* *The resources below will assist you with proper password hygiene:* *Choosing and Protecting Passwords* *Tricks for Creating a Strong Password*
2	Do you know who has access to your computing systems (laptops, desktops and servers, email and business applications, confidential information, report management systems, informant and investigative files)? Do you know who has administrative rights to your computing systems?			*It's important to know who has access to the critical systems, which contain personally identifiable information, confidential data, financial records, etc. Agency administrators should have procedures in place to regularly monitor who has access to all information system resources. Mechanisms should be in place to verify and authenticate the credentials for authorized users and administrators.*
3	Do you remove computer access rights immediately when employees, contractors, and volunteers leave your agency?			*Agencies should have policies and procedures in place to immediately terminate access rights to all information systems when employees, contractors, volunteers and others leave the agency. The procedures should include mechanisms for release notification and confirmation that system access has been terminated.*

1.2 Confidentiality

#	Question	Yes	No	Comments
4	Do you classify your data, distinguishing between sensitive versus non-sensitive, according to the potential impact should the information become unavailable, corrupted, or stolen?			*Some data simply does not require a high level of protection because its value is low, or it is public information. Focus time and effort on the information that must be protected such as Personally Identifiable Information.*

				The resources below will assist you in protecting your personal identifiable information: *Protection of Personal Identifiable Information* and *NIST-Guide to Protecting Personal Identifiable Information*
5	Is the most valuable or sensitive data encrypted?			*In many cases, storing data in an encrypted format will prevent unauthorized access to the computer system. Encryption, however, must be properly managed to ensure your organization has the encryption key and others don't.* *The resource below will assist you in understanding encryption:* *Understanding Encryption*
6	Are any of your vendor's networks connected to yours? If so, has their information security posture been evaluated and audited, and do they subscribe to appropriate security awareness procedures? In addition, are vendors granted access to any of your networks or applications?			*At times it is necessary to allow your vendors to access to your systems for upgrades or to solve problems. Have procedures in place to log and limit their access only to necessary applications or network, and ensure that access is terminated when their work is completed.*

1.3 Software & Hardware Law Enforcement Cyber Center IT Security

#	Question	Yes	No	Comments
7	Do you follow a regular process for identifying software vulnerabilities and applying updates?			*Many security incidents are caused by exploiting software vulnerabilities for which updates already exist. Therefore, it is crucial that processes are created to regularly scan for, and update, all software applications, including operating systems, web, email, and database servers.* *The resources below will assist in evaluating your organization's cyber security posture:* *Cyber Security Evaluation Tool* *Understanding Patches* *Guide to Enterprise Patch Management Technologies*

8	Do you store data on a cloud service?			*Storing data in the cloud **can** be as secure as storing it locally. Before any cloud services are used, investigate and ensure that their security policies and practices conform to your requirements.* *The resources below will assist in understanding cloud computing:* *Basic Cloud Computing and IACP Cloud Computing Guiding Principles*
9	Is there dedicated staff to monitor network and application access?			*Identify someone to monitor your agency's network. Continuous vigilance is needed to ensure that only authorized, authenticated users have access to your systems.*
10	Do you limit access to software applications and information based on data sensitivity and user need?			*Any user should only have access to systems and information resources that are specifically relevant to their work assignments. Structuring access to information and systems requires segregation of computing systems, networks, and information. Critical information should be categorized as "Need to Know."*

1.4 Education & Training Law Enforcement Cyber Center Training

#	Question	Yes	No	Comments
11	Do you provide basic information security training to your staff, including free online training courses provided by organizations such as the FBI, NW3C, SEARCH, US Secret Service, and DHS?			*Train staff on common threats to security such as phishing (i.e., fraudulent emails that solicit personal information, or contain dangerous programs), and social engineering (e.g., a call from someone, apparently in IT, asking you to provide information).* *The resources below will assist with identifying training resources for information systems security:* *Free Training for LE and Introductory Courses*
12	Are your employees able to properly identify and protect sensitive data, including paper documents, removable media, and electronic documents?			*Establish policies and provide training to ensure that employees are able to protect critical information (i.e., personally identifiable information, confidential data, financial records, etc.) internally and when transporting it outside of your secure facility.* *The resources below will assist in securing and disposing of devices safely:* *Disposing of Devices Safely and Safeguarding Your Data*

1.5 Policy & Procedures

#	Question	Yes	No	Comments
13	Do you have a disaster recovery or (DR) or business continuity plan (BCP) that includes a process for reliable back-up and recovery of all data?			*Backing up critical data becomes necessary in the event of damage or loss of availability or integrity of information. If possible, store backups in a controlled, offsite facility. Test the recovery process to ensure files can be recovered. Some agencies that were victims of ransomware were able to recover their data by relying on backup systems.* *The resources below will assist with properly establishing a back-up system:* *Cyber Resilience and Guidelines for Backing Up Information*
14	Conduct appropriate background checks on any personnel who will be responsible for maintaining your information systems?			*When hiring internally or externally, examine the security status to ensure there is no obvious risk in having them work on your systems.*
15	Do you regularly update and audit your IT policies?			*As technology evolves, regularly update your policies to reflect new risks, vulnerabilities, and threats.*
16	Do you make use of third party security professionals to audit your network, applications, and procedures?			*Have a qualified third party test the security controls of your network, software applications, and policies.*
17	Do you have a Cyber Threat Action Plan (aka incident response plan) that defines actions to be taken in the event of a cyber-attack?			*Every agency should have a plan to guide them if/when they become the target of a cyber attack. Don't wait until an incident happens to act. Develop a Cyber Threat Action Plan and train to it. NIST has an excellent outline Computer Security Incident Handling Guide. It highlights the considerations that need to be decided before an attack occurs.*
18	Do you have a comprehensive data security policy than includes each of the processes described in this Report Card?			*Every agency should have a security policy which is regularly updated and enforced. Refer to the NIST Framework for Improving Critical Infrastructure Cybersecurity when creating or updating your policy.*