State Agency Cybersecurity Survey v 3.4

The purpose of this survey is to identify your agencies current capabilities with respect to information systems/cyber security and any challenges and/or successes you have experienced. The survey follows the five core functions of the NIST Cyber Security Framework for your state agency to self assess its current capabilities. A comment box will follow each question as well, where we request that you provide any further details in terms of successes and challenges you have faced. The purpose of this survey will be to better inform any recommendations made by the Commonwealth Cyber Security Commission to the Governor and Legislature. Responses will be used to identify strengths as well as how current capabilities may be improved. Any recommendations made as a result of your responses will be made as a benefit to your organization and will not seek to reprimand or hinder your capabilities in any way.

General

1. What steps could the Commonwealth take which would have the biggest impact on our cyber security?
2. Within the Commonwealth, how could coordination with the private sector be improved?
3. How can we better leverage the Commonwealth's academic institutions to improve cyber security (e.g. research, workforce development, etc.)?
4. How can we improve the Commonwealth's efforts to fight cyber crime?
5. How could we leverage cyber security to improve the Commonwealth's economy and competitive edge?

Identify

Please evaluate your agency to the best of your ability and in cases

1. What percentage of the physical Information Technology (IT) assets that are owned and managed by your organization have been inventoried?
    a. How often do you update the inventory your physical IT systems?
    b. What process or tools do you use to inventory your physical IT systems?
2. What percentage of the software and application platforms within your organization have been inventoried?
    a. How often do you update the inventory of your software and applications?
    b. What process or tools do you use to inventory your software and applications?

Please indicate how much you agree or disagree with each of the following statements using either Strongly Disagree, Disagree, Neither Disagree or Agree, Agree, or Strongly Agree:

3. My organization and/or service provider has adequate resources to actively inventory physical system assets and software and application platforms (organizational assets only, not third party).
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What resources do you need?

4. My organization and/or service provider has identified and established roles and responsibilities for stakeholders with asset management (software/hardware) responsibilities (e.g. employees, suppliers, and partners).
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - *b.* Comment box: What are some challenges and/or successes your organization has had with respect to this?
5. My organization and/or service provider prioritizes physical system and software application resources for availability and recovery, based on their criticality to business functions and their impact upon the organization if disrupted.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - *b.* Comment box: What are some challenges and/or successes your organization has had with respect to this?
6. My organization has identified and prioritized its objectives and activities (business processes) and has disseminated them throughout the organization.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - *b.* Comment box: What are your organization's priorities? What are some challenges and/or successes your organization has had with respect to this?
7. My organization has identified and understands the IT dependencies and critical functions for the delivery of services.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - *b.* Comment box: What are some challenges and/or successes your organization has had with respect to this?
8. My organization and/or service provider actively discovers and corrects application vulnerabilities within 30 days and keeps records of the vulnerabilities and their corresponding resolutions.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
9. My organization receives threat and vulnerability information from information sharing forums and sources.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - b. Comment box: Name the information sharing forum(s) and source(s). How does your organization make use of the threat and vulnerability information you receive?
10. My organization identifies and documents internal and external threats to the organization's mission.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    - b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
11. My organization analyzes risks to determine their potential impacts to critical services we provide.
    - *a.* *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*

   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
12. My organization develops plans for the risks it identifies and prefers to mitigate.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
13. My organization regularly audits its internal systems.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. What is the frequency of the audits? What are some challenges and/or successes your organization has had with respect to this?
14. My organization has a definition for which of its information systems are considered critical infrastructure assets.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What is the definition/what defines systems as being critical?

Protect

Please indicate how much you agree or disagree with each of the following statements using either Strongly Disagree, Disagree, Neither Disagree or Agree, Agree, or Strongly Agree:

1. My organization and/or service provider manages and protects physical access to these critical systems.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How is physical access controlled to these systems? What are some challenges and/or successes your organization has had with respect to this?
2. My organization manages access permissions, incorporating practices of least privilege and separation of duties, for any systems/applications considered to be critical.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
3. My organization practices network segregation for critical asset systems within its network.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
4. My organization enforces annual security training for all users.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What training methods are used? What are some challenges and/or successes your organization has had with respect to this?
5. My organization has clearly defined and disseminated roles and responsibilities for privileged IT users.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?

6. My organization's physical and information security personnel have clearly defined and understood roles and responsibilities.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
7. My organization designates an adequate amount of resources towards security training.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: Are administrators given additional, specialized training? What does your organization expend on security training? What are some challenges and/or successes your organization has had with respect to this?
8. My organization protects sensitive data at rest.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: How do you protect your sensitive data? Do you encrypt all removable media? What are some challenges and/or successes your organization has had with respect to this?
9. My organization and/or my service provider implements a baseline security configuration of its information technology (IT) and industrial control systems/applications.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
10. My organization implements a systems development life cycle for the management of its systems.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
11. My organization and/or service provider meets or exceeds policies and regulations applicable to the physical operating environment of its critical system assets.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
12. My organization actively improves protection processes and procedures for its critical systems.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: What methods do you employ to improve protection processes and procedures? What are some challenges and/or successes your organization has had with respect to this?
13. My organization shares the effectiveness of protection mechanisms it implements with other partner organizations to contribute to the improvement of their processes.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: How does your organization share this information with partner organizations? How frequently? What could help improve the value of sharing?
14. My organization has developed and manages response plans (incident response and business continuity) and recovery plans (incident and disaster recovery).

  a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
  b. Comment box: What are some challenges and/or successes your organization has had with respect to this?

15. My organization includes cyber/information security in regular Human Resource activities (e.g. credential revocation, screening of personnel, etc.).
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: Are these practices written, understood, and followed in Human Resources operations? What are some challenges and/or successes your organization has had with respect to this?

Detect

Please indicate how much you agree or disagree with each of the following statements using either Strongly Disagree, Disagree, Neither Disagree or Agree, Agree, or Strongly Agree:

1. My organization has identified and manages a baseline of normal network operations and expected data flows for users and systems.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
2. My organization analyzes the information pertaining to an event to determine attack methods and targets.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How do you analyze and use this information? Do you share detection information with partner organizations? What are some challenges and/or successes your organization has had with respect to this?
3. My organization and/or my service provider monitors its networks to detect potential cyber events.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What network monitoring is performed by your organization? What are some challenges and/or successes your organization has had with respect to this?
4. My organization's physical environment is monitored to detect potential cyber events (physical threats).
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?
5. Personnel activity within my organization is monitored to detect potential unauthorized access.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What methods are used to monitor personnel? What perceived threats do personnel create for your organization? What are some challenges and/or successes your organization has had with respect to this?
6. My organization monitors for unauthorized users, connections, devices, and software.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*

   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?

7. My organization actively scans for vulnerabilities on its systems.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How does your organization identify and manage system vulnerabilities? Do you report vulnerabilities to another organization? What are some challenges and/or successes your organization has had with respect to this?
8. My organization's continuous monitoring and detection practices comply with all applicable policies and regulations.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How does your organization ensure continuous monitoring compliance?
9. My organization's continuous monitoring and detection practices are regularly tested and reviewed.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How often are they tested and reviewed? How does your organization use this information? What are some challenges and/or successes your organization has had with respect to this?
10. My organization has established a threshold for internal/external alerting on an incident to executive leadership (e.g. agency head or equivalent).
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: Please describe how your organization triages incidents to determine which require alerts. What are some challenges and/or successes your organization has had with respect to this?
11. My organization has a formal means of reporting event information to specifically identified parties.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: Which parties does your organization formally share information with? Could the sharing of information be improved and if so, how? What are some challenges and/or successes your organization has had with respect to this?

Respond

Please indicate how much you agree or disagree with each of the following statements using either Strongly Disagree, Disagree, Neither Disagree or Agree, Agree, or Strongly Agree:

1. Following an event, my organization has a means of determining the impact of the event.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: If you determining the impact of an event, what do you do with the results? What are some challenges and/or successes your organization has had with respect to this?
2. My organization maintains a response plan to execute during or after a cyber or physical event.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are some challenges and/or successes your organization has had with respect to this?

3. In my organization, all personnel are aware of their roles and responsibilities when a response is needed.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How does your organization communicate the response plan to personnel? Are all personnel included in the testing of response plans? What are some challenges and/or successes your organization has had with respect to this?
4. My organization reports events to authorities in accordance with response plans.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: If so, to which authorities do you report events? How soon are events reported after they occur? What are some challenges and/or successes your organization has had with respect to this?
5. In accordance with our response plan, my organization coordinates with stakeholder organizations during or after an event.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What is your coordination and notification process? What are some challenges and/or successes your organization has had with respect to this?
6. My organization investigates event notifications produced by its detection systems.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How long after events are detected does your organization investigate? What are some challenges and/or successes your organization has had with respect to this?
7. My organization seeks to understand both the direct and cascading impacts of an incident.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: Are these impacts assessed and do they inform decision making? What are some challenges and/or successes your organization has had with respect to this?
8. My organization has access to a forensic analysis capability.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What is your organization's capability? Or what forensic analysis capability can you obtain from a partner organization?
9. My organization's response plans incorporate lessons learned.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How are lessons learned used? Does your organization account for lessons learned from events and exercises? What are some examples of lessons learned? What are some challenges and/or successes your organization has had with respect to this?
10. My organization's response plans and strategies are exercised and updated regularly from lessons learned.
    a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
    b. Comment box: How often are these plans and strategies reviewed and updated? What are some challenges and/or successes your organization has had with respect to this?

Recover

Please indicate how much you agree or disagree with each of the following statements using either Strongly Disagree, Disagree, Neither Disagree or Agree, Agree, or Strongly Agree:

1. My organization maintains a recovery plan to execute during or after a cybersecurity event.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How often does your organization review and revise the recovery plan? Does your organization exercise its recovery plan and if so, how often? What are some challenges and/or successes your organization has had with respect to this?
2. My organization communicates recovery plans to personnel within the organization.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How do you communicate plans to personnel? How do you ensure personnel have reviewed and understood your recovery plans?
3. My organization incorporates lessons learned in its recovery plans.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: If so, what are some examples of lessons learned? What are some challenges and/or successes your organization has had with respect to this?
4. My organization regularly exercises and updates its recovery plans.
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: How often does your organization exercise its recovery plan? What are some challenges and/or successes your organization has had with respect to this?
5. My organization seeks means of restoring and/or maintaining its reputation post event (e.g. public relations).
   a. *Strongly Disagree/Disagree/Neither Disagree or Agree/Agree/Strongly Agree*
   b. Comment box: What are your organization's methods for communicating with the public? Describe the means your organization plans to use or would like to use to maintain its reputation.