This free survey is powered by QuestionPro Create a Survey

Survey: Cybersecurity Situational Awareness Survey

Cybersecurity Situational Awareness Survey

1.
On May 4, 2017, the outgoing Commander of the 13th Coast Guard District called out cybersecurity resilience as his greatest concern. He called for industry and government to come together and act to remedy the lack of standards for addressing the who, what, how, and when of cyber incident reporting. He spoke of the urgent need for industry and government stakeholders to develop voluntary standards and protocols before the next serious incident like Maersk (which resulted in $1 billion in losses), which could have grave consequences for critical infrastructure in our region.

This survey is designed to help us develop a baseline of current best practices and investments in cybersecurity by organizations in the Puget Sound Region. The first part (31 questions – approximately 15 minutes to complete) is required before our initial workshop in early March, and to ensure the value and efficacy of our efforts to produce a relevant and usable Concept of Operations (CONOPS) based on your input. The second, more detailed section (including first section – total of 52 questions – approximately 30 minutes to complete) is optional but can also provide your organization an opportunity for a self-assessment of the maturity of your current cybersecurity resilience and response capabilities.

Instructions:
Please carefully complete the survey to the best of your knowledge. You may need to consult with or refer some questions to other managers or experts in your organization. At the beginning of each section we note which job functions might be best equipped to answer, listed in order of best choice (with the understanding that many organizations will not have some of the listed resources).

In order to complete the survey most efficiently, we recommend you download the PDF version of the survey HERE, and consult with your colleagues to answer all questions before taking the survey online. That will both give your organization a usable cyber resilience and response assessment and allow you to gather information from the right people in your organization. We invite you to use the comment section at the end of each section to add any other information you deem pertinent. Except for the first section, no questions are required, so please answer only those that you wish to. All answers are non-attributable.

2. Qualifying Questions
(Suggested respondent – CIO; CTO; CSO; CISO; Information Security Management; IT Management; Administrative Manager; Clerk)

3. Describe your sector

-- Select --

4. Under which critical infrastructure sector would you consider your organization?

-- Select --

QuestionPro

5. If applicable, under which of the following categories would you consider your organization?

-- Select --

6. How many full-time employees in your organization?

-- Select --

7. Please indicate the types of high value assets your organization operates and must protect [select all that apply]

- ☐ Finance system/wire transfer (ACH)
- ☐ Traffic management
- ☐ Public safety radio system
- ☐ Human resources database
- ☐ Health information database
- ☐ 911 call center/Public Safety Answering Point (PSAC)
- ☐ Critical Infrastructure control systems/public works
- ☐ SCADA systems
- ☐ Navigation/GPS systems
- ☐ I don't know
- ☐ Other

8. Approximately what percentage of your staff are IT and cybersecurity personnel?

- ○ 100%
- ○ 90%
- ○ 75%
- ○ 50%
- ○ 25%
- ○ 10%

- ○ Other

9. Does your organization have full-time Information Technology (IT) employees?

- ○ Yes
- ○ No

10. If you answered 'No' to the last question, do you outsource any or all of your IT support?

- ○ Yes
- ○ No
- ○ Not applicable
- ○ Other

11. If you do outsource IT support, what percentage of your IT support is outsourced?

- ○ 5-10%
- ○ 10-25%
- ○ 50-75%
- ○ 75%+
- ○ Not applicable

12. Comments

13. Policy
(Suggested respondent: HR Management; CIO; CTO; CSO; CISO; Information Security

Management; IT Management; Administrative Manager; Clerk)

14. Does your organization have documented information security policies in place?

Guidance: Information security policies include any formal document that specifies technology requirements and configurations, as well as acceptable use guidelines or procedures for any computer equipment or data.

- ○ Yes
- ○ No
- ○ Other

---

15. Are your information security policies updated at least yearly?

Guidance: You should have someone specifically tasked with facilitating, documenting and acquiring executive approval/signatures for the updated policy.

- ○ Yes
- ○ No
- ○ Other

---

16. Who in your organization is responsible for cyber security?

- ○ IT Security Manager
- ○ Director of Security
- ○ VP of Security
- ○ IT Operations Manager
- ○ Other

---

17. Are security policies easily accessible to all employees and have they been exposed to the policies through training?

- ○ Yes
- ○ No

- ○ Other

18. Training should include the following - Please select all that your organization includes:

- ☐ All employees trained as part of their orientation when hired
- ☐ This procedure is documented and kept up to date as part of their HR file
- ☐ Instructions on where to find policies
- ☐ Password, clean-desk, ingress precautions, procedures, etc.
- ☐ Examples of phishing and other cyber threats
- ☐ Information on who to contact with security information or concerns
- ☐ Other

19. How often are employees trained?

- ○ Monthly
- ○ Quarterly
- ○ Twice a year
- ○ Yearly
- ○ At employment
- ○ Not applicable
- ○ Other

20. Comments

21. Physical Security

(Suggested respondent: Facilities Manager; Administrative Manager; Clerk; CIO; CTO; CISO; IT Security Manager; IT Manager)

22.
Are all new hires with access to areas with sensitive or critical data or systems required to pass a background check before employment?

Guidance: Employees who have physical access to computers, servers, network equipment, control systems, etc. that could reveal sensitive data or cause a serious impact if compromised should pass a background check before being employed. The background check should be comprehensive commensurate to the specific criticality of the data or systems in question (e.g. access to basic computer support might require a criminal background only, while access to the financial database might include a credit check).

- ○ Yes
- ○ No
- ○ Other

23. Are there adequate physical security controls to protect your cyber assets?

- ○ Yes
- ○ No
- ○ Other

24. Physical controls should include the following [Select all that apply to your organization]:

- ☐ Secure physical access controls (e.g. card key locks & ID badges) for any rooms, areas or facilities containing cyber assets
- ☐ Documented and audited authentication provisioning for access control systems (e.g. card keys)
- ☐ Regularly audited logging of ingress/egress events and retention of logs for an appropriate amount of time
- ☐ Enhanced authentication (biometric, two-factor, etc.) for critical or sensitive assets
- ☐ Guards, surveillance cameras, fences, “man-trap” doors, locks and/or hardened windows/entrances to prevent unauthorized access for all facilities
- ☐ Policy and regular training for employees on keeping their workplace physically safe, as well as appropriate remote access, physical security at home or on the road and mobile device physical security, etc.
- ☐ Special training for guards on cyber asset protection
- ☐ Other

25. Comments

26. Incident Response and Resilience (Suggested respondent: Incident Response Lead; CTO; CISO; Administrative Manager; Clerk; IT Security Manager; IT Manager)

27. Does your organization have a well-documented, regularly exercised incident response plan? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Incident Response Procedures
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Incident Response Procedures

28. A mature incident response capability will include the following. Which are included in your organization's response plan? [Select all that apply]

- ☐ At least one full-time employee tasked with the documentation, maintenance and overall management of your incident response planning and procedures
- ☐ Regularly scheduled exercises and after-action documentation for each exercise or major incident response
- ☐ Formal project management for remediation of issues or suggested enhancements from after action analyses
- ☐ Regular training for incident response team on event analysis, forensics techniques, etc.
- ☐ Specific training in current threat intelligence and threat information management for Security operations personnel
- ☐ Documented containment procedures and levels of containment including recovery processes
- ☐ Documented procedures including:
  - Defined roles and responsibilities for all responders
  - Alerting and triage procedures
    - Communications and reporting guidelines
    - Specific regulatory sections (e.g. PCI required breach response protocol for Visa, MC, etc.)
    - Signed by executive – highest level possible

☐ Documented response playbook including:

- First on scene response checklist/triage guidance
- Up to date and regularly maintained contact information for executives and incident response team
- Up to date and regularly maintained contact information for all responders or possible stakeholders (e.g. department management; public safety; physical facilities managers; HR; Legal; PIO; Executive Admins; Execs)
- Responsibilities checklist for each of the roles defined in the incident response procedure document
- Full, complete, precise and up to date documentation of all organizational network systems including contact information for the custodians or any third-party vendors tasked with maintenance and monitoring of the network (who should be on your incident response team)
- Specific guidance for responding to a breach of Personally Identifiable Information (PII)
- A detailed communications plan including sample messages to different stakeholders and management, frequency of notification guidance; and sample report templates
- Guidance and contact information on when it is appropriate to contact Law Enforcement or other third parties for assistance (or just to notify), including what should be shared and the secure and safe way to share it
- Up to date documentation and technical instructions on use of response and computer forensics tools and systems

29. Comments

30. Incident Response Plan Specifics (Suggested respondent: Incident Response Lead; CTO; CISO; Administrative Manager)

31. As part of your Incident Response plan do you have a severity matrix in place to internally define a significant cyber incident?

○ Yes

○ No

○ Other

32. If you need support during a significant cyber incident does your communications plan include up to date contact information for the appropriate resources, including 3rd party, government, or law enforcement?

○ Yes

○ No

○ Other

33. If those resources are unavailable do you have secondary or tertiary support resources and a plan to contact them?

- ○ Yes
- ○ No
- ○ Other

34.
Do you have a reporting protocol for a significant cyber incident?

Guidance: These might include internal reporting, vertical organizations, regulatory required notice, DHS/NCCIC, Fusion Center, Coast Guard, Local Law Enforcement, Federal Law Enforcement, Private Security Vendor, Other

- ○ Yes
- ○ No
- ○ Other

35. Have you ever reported a cyber incident?

- ○ Yes
- ○ No
- ○ Other

36. If yes, to whom did you report?

37. If yes, what was your experience with intake and feedback?

38. Do you have any information sharing procedures in place with other similar or affected/interdependent organizations?

- ○ Yes
- ○ No
- ○ Other

39. Do you have protocols in place for cyber incident communications with third party supply chain partners?

- ○ Yes
- ○ No
- ○ Other

40. What type of reporting protocol and feedback would be most valuable to your organization? [Select all that apply]

- ☐ Centralized reporting agency
- ☐ Special phone number
- ☐ Online form
- ☐ Other

41. What suggestions do you have regarding reporting protocols for significant cyber incidents?

42. Are you a member of or aware of the following reporting resources/platforms? [Select all that apply]

- ☐ HSIN

- ☐ NWWARN
- ☐ Fusion Center
- ☐ Infragard
- ☐ JHOC
- ☐ ISACs
- ☐ NCCIC
- ☐ FBI
- ☐ CIRCAS
- ☐ Other

43. Comments

44. Business Continuity/Disaster Recovery Plans (Suggested respondent: BC/DR Response Lead; CTO; CISO; Administrative Manager)

45. Do you have an up to date, documented and practiced business continuity and disaster recovery (BC/DR) plan or procedures? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic BC/DR Procedures
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature BC/DR Procedures

46. A mature set of BC/DR procedures would include the following [Please check all that are part of your organization's plan]:

- ☐ All department management as stakeholders
- ☐ Detailed documentation of the specific vital and critical tasks assigned to each department and plans to continue those tasks after a disaster or other incident

- ☐ Defined roles and responsibilities for recovery
- ☐ Alternative work-sites
- ☐ Data and IT specific guidance on secure maintenance of availability of data during and after an event
- ☐ A comprehensive communications plan
- ☐ A regular exercise program including all stakeholders
- ☐ After-action analysis of any exercise or event including a project plan to mitigate any findings
- ☐ Other

47. Do your BC/DR plans include backup plans for operations of critical systems such as navigation/GPS, etc.?

- ☐ Yes
- ☐ No
- ☐ Other

48.
A backup plan should include the following [Select all that apply]:

- ☐ Specific time-frame for deploying backup services
- ☐ Amount of time those backups can be maintained
- ☐ Plan for returning to main production/operations environment
- ☐ Test environment for exercising backup systems
- ☐ Other

49. Comments

50. Third Party/Vendor Management
(Suggested respondent: CFO; Purchasing Managers; CIO; CTO; CISO; Administrative Manager; Clerk; IT Security Manager; IT Manager)

51. Does your organization have a mature vendor cyber security management program in place (this is how Maersk and many others were compromised)? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Vendor Management Program
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Vendor Management Program

52. A mature vendor cyber security management program would include the following [Please check all that are part of your organization's plan]:

- ☐ Specific cyber security qualification requirements in all RFQ's
- ☐ Data security requirements as appropriate in contracts awarded
- ☐ Data security auditing language in any contract with third parties needing access to sensitive data or systems
- ☐ Specific procedures and guidelines for on-site or remote vendor access to any internal systems, applications or data
- ☐ Communications plan for sharing information both to and from supply chain vendors
- ☐ Auditing information from vendors for any next level vendors they contract with.
- ☐ Other

*** 53. This ends the required section. The next section is optional, but will provide us with a more detailed understanding of regional capabilities, and offer you an opportunity to complete a self-assessment of your current cyber security resilience and response capabilities.**

As previously mentioned, we recommend downloading and reviewing the PDF version of the survey HERE. Part 2 is a comprehensive assessment of the maturity of your current cyber security systems. This can be a valuable tool for you to work with your colleagues in addressing some of the questions and issues raised in this self-assessment regardless of whether or not you

choose to submit your answers.

Please select the "Submit answers and exit survey" button if you would like to stop here. If you would like to save your answers and continue at a later time, select "Save Page and Continue Later" at the bottom of the page. Otherwise, select "Continue to next section".

- ○ Submit answers and exit survey
- ○ Continue on to next section

54. General Cyber-Security Management (Suggested respondent: CIO; CTO; CSO; CISO; Information Security Management; IT Management; Administrative Manager; Clerk)

55. If you have full-time IT employees, how many are dedicated to IT support and administration per 1000 users? [Please type in the answer]

Guidance: IT support can include network administrators; desktop support; application developers; telephone/communications administrators; email administrators; web or social media administrators or developers; information security staff; etc.

56. What percentage of your total IT budget is allocated to security? [Provide a percentage, if applicable]

Guidance: When calculating this answer, include

- **Costs for security hardware and software – this might include:**
- **Firewalls, routers, switches and other network equipment**
- **Desktop antivirus products**
- **Any other preventative controls e.g. IPS/IDS, spam filtering tools, web site filtering, etc.**
- **Remember to include costs for purchasing, licensing, operations and maintenance).**
- **Also include any actual personnel costs (salary plus benefits) for dedicated staff (or percentages for staff not specifically assigned to security).**
- **Finally, if you outsource any of your IT support, consider what percentage of their time is taken with advice, deployment, management or maintenance of any of the security hardware and software; access control (password setting, user management, etc.); incident response; monitoring of your systems; policy creation or assistance. You may be able to contact your vendor for assistance or their response to this question.**

57. To what extent is your organization's leadership committed to supporting information security practices? [Rate on a scale of 1-5]

- ○ 1 - Not committed
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Extremely committed

---

58. The following are indications of executive buy-in [Check all that apply to your organization]:

- ☐ The IT Security Policy has been signed by the highest executive level of your organization
- ☐ There are staff dedicated to information security practice
- ☐ There is a planned and documented information security risk management procedure
- ☐ There is awareness at the executive level of security regulatory compliance requirements such as PCI, HIPAA or CJIS, and are there personnel dedicated to meeting those requirements
- ☐ Other

---

59. Do your cyber-security policies meet best practice standards as defined by NIST by addressing all areas of importance? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Security Policies
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Security Policies

---

60. Are your security policies compliant with or modeled on industry standards, such as NIST?

- ○ Yes
- ○ No
- ○ Other

61. If you answered yes to the last question, please indicate which standard you are following.

62. Optimized/mature security policies should, at minimum, address all of the following [Check all that apply to your organization]:

- ☐ Business continuity procedures related to security controls
- ☐ Change control and patch management
- ☐ Security risk management and
- ☐ Regulatory compliance
- ☐ Access control procedures (password management, etc.)
- ☐ Email use and protection guidelines
- ☐ Classification of data and information assets
- ☐ Levels of response based on classification/priority of data
- ☐ Encryption of sensitive data
- ☐ Network and systems monitoring/detection tools, policies and procedures
- ☐ Incident response procedures
- ☐ Acceptable use policies
- ☐ Physical security guidelines
- ☐ Privacy and confidentiality policies and guidance
- ☐ Remote access procedures and policy
- ☐ Virus protection standards
- ☐ Secure development standards of practice (if you are developing applications in house)
- ☐ Vendor/3rd Party management and procurement guidance
- ☐ Web application security
- ☐ Network systems security hardening guidelines
- ☐ Wireless device management, policies and standards
- ☐ Desktop and mobile device policy, procedures and standards
- ☐ Social media policy and standards
- ☐ Other

63. Comments

64. Risk Management (Suggested respondent: CFO, Risk Manager, CIO, CTO, CISO, IT Manager, Administrative Manager, Clerk)

65. Does your organization actively assess cyber security risk within a regular and sustained program? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Risk Management Process
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Risk Management Process

66. A mature cyber risk management assessment process would include the following [Check all that apply to your organization]:

- ☐ There are personnel specifically tasked with facilitating, documenting and acquiring executive approval/signatures for a regularly scheduled cyber risk assessment
- ☐ Those assessments include penetration testing both from inside and outside the firewall(s)
- ☐ They include a thorough review of critical cyber assets and their associated vulnerabilities
- ☐ A risk prioritization formula is used that takes into account the level of impact/cost if an asset is compromised, the likelihood that a vulnerability will be exploited against that asset, and the cost/time required to mitigate the vulnerability
- ☐ Other

67. Does your organization invest in cyber security insurance?

- ○ Yes
- ○ No
- ○ Other

68. Do you contractually require vendors and 3rd party service or product providers to demonstrate their use of a mature cyber risk management program?

Guidance: This may require checking with your procurement staff – you should review all contracts to see if there is any language regarding cyber security and risk programs and if your organization has the right to audit, or if you only require attestation or documentation of compliance.

- ○ Yes
- ○ No
- ○ Other

69. Security Architecture and Design/Asset Management (Suggested respondent: CIO; CTO; CSO; CISO; Information Security Management; IT Management; Administrative Manager; Clerk)

70. Do you have network and systems design documentation specifically to indicate security controls?

- ○ Yes
- ○ No
- ○ Other

71. If you selected 'Yes' for the last question, you should have personnel specifically tasked with the maintenance and updating of a current network and systems diagram that includes all of the following listed items. Please select all that apply to your organization:

- ☐ Network devices, sharing relationships and data transport paths – with details available on their configuration
- ☐ Databases and storage classified by sensitivity level – critical assets clearly indicated
- ☐ Preventative or Detective control systems – with details available on their configuration
- ☐ Network segmentation and redundancies
- ☐ IP addresses & device IDs indicated for all internal and external devices – specific asset details available

72. Do you keep a current database or record of all computer assets?

Guidance: To answer yes, there should be someone tasked with the maintenance of an asset management record. This record should include the following:

- **A dynamically updated list of the model information and/or Asset ID of all computers, mobile devices, databases, network devices, printers, scanners, etc.**
- **A current and updated list of the owners' of all listed devices including their name, location and contact information**
- **A record of the de-provisioning and disposal of all assets**

- ○ Yes
- ○ No
- ○ Other

73.
Do you have a mature and documented configuration management policy and procedure? [Rate on a scale of 1-5]

Guidance: An optimized configuration management would require someone tasked with maintaining and documenting up to date configuration standards for all of your cyber assets, including,

- **All network devices**
- **Any preventative or detective control systems e.g. antivirus, firewall(s), Intrusion Prevention or Detection Systems (IPS/IDS)**
- **Desktops & laptops**
- **Mobile devices**
- **Databases**

- ○ 1 - Ad Hoc/Basic Configuration Management
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Configuration Management

74. Do you have a formal patch management procedure in place? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Patch Management Process
- ○ 2
- ○ 3

- ○ 4
- ○ 5 - Optimized/Mature Patch Management Process

75.
An optimized/mature process would require someone tasked with maintaining and documenting a formal patch management process including all of the following. Please check all that apply to your organization's patch management procedure:

- ☐ The upgrading and updating of all software and hardware to the most recent patch level as soon as possible
- ☐ A risk management approach to patching the most critical systems according to the level of possible impact weighed against the business impact and resources needed to update/upgrade
- ☐ A testing procedure and test environment to assess possible impacts to business processes or the performance and compatibility of integrated systems or software before comprehensive patching
- ☐ A formal patch assessment, testing and deployment schedule
- ☐ A communications process to inform owners and users of patching strategies and schedules
- ☐ Other

---

76. Do you have an automated and tested backup system in place? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Backup Process
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Backup Process

77.
An optimized backup system should include the following. Please select all that apply to your organization's backup system:

- ☐ Policy on when, how and what is backed up that is signed by the highest executive in the organization
- ☐ Procedural and standards documentation on the devices and systems used to do the backups
- ☐ Documented configuration, storage and retention standards for backup media including encryption standards where appropriate
- ☐ Documented and audited backup schedules

☐ Tested and documented recovery procedures scheduled at least once per year

78. If you have a backup system, do you have off-site or Internet-based backup systems?

○ Yes

○ No

○ Other

79. Comments:

80. Authentication and Access Control (Suggested respondent: CIO; CTO; CSO; CISO; HR Management; Information Security Management; IT Management; Administrative Manager; Clerk)

81. Is there a documented process for creating network accounts and granting network access? [Rate on a scale of 1-5]

○ 1 - Ad Hoc/Basic Asset Management Process

○ 2

○ 3

○ 4

○ 5 - Optimized/Mature Asset Management Process

82.
An optimized process would require dedicated personnel to document, maintain, and manage access and authentication provisioning. This should include all of the following. Please select all that apply to your organization:

- ☐ Procedures for activating, monitoring and auditing all network authentication & connections
- ☐ Procedures for provisioning new user accounts, including least privilege standards (only grant privileges to systems and shares that are required for their job)
- ☐ A regularly scheduled review of all accounts and purging of cancelled, stale or unused accounts
- ☐ Current contact information for all account owners or managers
- ☐ Vendor and 3rd party access procedures and standards
- ☐ Remote access procedures and standards
- ☐ De-provisioning standards and documentation

---

83. Comments

84. Monitoring and Auditing
(Suggested respondent: CIO; CTO; CSO; CISO; HR Management; Information Security Management; IT Management; Administrative Manager; Clerk)

85.
Do you have network and desktop monitoring controls in place that are regularly assessed and documented? [Rate on a scale of 1-5]

Guidance: A mature monitoring system and process would require dedicated personnel responsible for the following,

- **Research and acquisitioning assistance for optimum network and desktop monitoring solutions**
- **Development and deployment of monitoring hardware and software**
- **Documented configuration and deployment procedures and standards**
- **Maintenance and updating procedures**
- **Configuration and ongoing refinement of alerting and response procedures**

- ○ 1 - Ad Hoc/Basic Monitoring Process
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Monitoring Process

---

86. Comments

87. Security Awareness
(Suggested respondent: HR Manager; CIO; CTO; CISO; Administrative Manager; Clerk; IT Security Manager; IT Manager)

88. Does your organization have a cyber security awareness program in place? [Rate on a scale of 1-5]

- ○ 1 - Ad Hoc/Basic Cyber Awareness Program
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Cyber Awareness Program

89.
A mature awareness program will require dedicated personnel to document, manage, deliver, and maintain the program and will include documented training for employees and vendors on all of the items below. Please select all that apply to your organization.

- ☐ Acceptable use of all of the organization's cyber assets
- ☐ Email security guidelines and phishing prevention/awareness
- ☐ Password and antivirus policy
- ☐ Remote access policies, standards and procedures
- ☐ Mobile device policies and standards
- ☐ Server and desktop security control and configuration standards (e.g. antivirus, firewall(s))
- ☐ Wireless device standards and procedures
- ☐ Personal device standards and policy
- ☐ Social media acceptable use and policy
- ☐ Indications of virus or other compromises
- ☐ Appropriate responses to issues or problems
- ☐ Up to date and maintained contact information to report issues or ask for assistance

90. Comments

91. Secure Application Development (Suggested respondent: Applications Manager; Lead Developer; CTO; CISO; Administrative Manager; Clerk; IT Security Manager; IT Manager)

92.
Does your organization develop applications in house?

Guidance: Do you have employees whose jobs include the development or revision of business applications?

- ○ Yes
- ○ No
- ○ Other

93.
Does your organization contract with 3rd party vendors to develop applications?

Guidance: Do you purchase business applications developed outside your organization or off the shelf tools?

- ○ Yes
- ○ No
- ○ Other

94.
Do you (or your vendors) have a mature and well defined Secure Development Lifecycle (SDLC) program or require one of your vendors? [Rate on a scale of 1-5]

Guidance: A mature program will include specific guidance, documentation, testing and auditing of all application development during the entire lifecycle of the application. It will also include ongoing training and testing of your or your vendor's developers in secure application development techniques and protocols.

- ○ 1 - Ad Hoc/Basic SDLC Program

- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature SDLC Program

95. Comments

96. Regulatory Compliance (Suggested respondent: Compliance Manager; CIO; CTO; CISO; Administrative Manager; Clerk; IT Security Manager; IT Manager)

97.
Does your organization have an employee specifically tasked with management of a mature regulatory compliance program? [Rate on a scale of 1-5]

Guidance: A mature regulatory compliance program would include:

- **A complete understanding of which regulations apply to your organization (e.g. PCI, HIPAA, CJIS; FERPA; FACTA, applicable USCG CFRs and the latest NAVC)**
- **Documented and up-to-date regulatory requirements for each of the above that apply**
- **A consistent and documented compliance assessment program including project management for mitigating issues**

- ○ 1 - Ad Hoc/Basic Compliance Program
- ○ 2
- ○ 3
- ○ 4
- ○ 5 - Optimized/Mature Compliance Program

98. Who is responsible for compliance management?

- ○ IT staff
- ○ Legal staff
- ○ Administrative staff

- ○ Third party vendor
- ○ Not applicable
- ○ Other

99. Comments

100. Thank you for taking the time to complete the survey. If you have any additional comments before submitting your answers, please provide them below.