GSRMA
GOLDEN STATE RISK MANAGEMENT AUTHORITY

Cyber Risk Self-Assessment

Introduction

PLEASE READ THIS SECTION CAREFULLY AND COMPLETELY

Purpose

The purpose of this survey is to perform an assessment of your agency's risk of having a significant cyber breach, your readiness to continue agency business during a breach incident, and your agency's ability to fully recover from the incident.

This survey is not a substitute for a full risk assessment or ransomware readiness review.

What are Cyber Risks?

At one level or another, cyber criminals and cyber terrorists are focused on your agency's data and/or systems. Their goals can vary and include such things as collecting money, stealing information, preventing access to information, or planting misinformation.

Thus, there is a wide variety of information and systems that can be leveraged by these organizations. The questions in this survey delve into the potential risks to such things in your agency.

What is a Ransomware attack?

As the name suggests, ransomware attackers hold something valuable to the recipient of an attack and vow to return it in exchange for a ransom (i.e. money). You might not immediately believe that your agency holds information that is valuable (i.e. it is generally public information), but if that information is necessary for your agency to provide services, then it is truly valuable. A ransomware attack can potentially shut down your agency’s services (to the public, other agencies and internally) for weeks or months.

The attacker first penetrates an agency's network and then locates the information and/or systems that they believe are most valuable. In many cases, they just cast a wide net and select all accessible computers and systems. Once ready, they encrypt all systems thereby making them unusable, notify the agency and demand a ransom. In exchange for the ransom payment, they promise to provide the secret key that will decrypt all of the impacted systems.

While the process of encrypting the targeted systems is extremely fast, the decryption process can take days or weeks.

Is my Agency a target?

Yes.

Experts will tell you that very sophisticated criminal organizations go after large companies or government entities with a very tailored approach that involves weeks or even months of planning. However, they will also say that small criminal groups do more of a "spray and pray" method to cast a large net and hopefully find a few easy targets to extract a few thousand dollars in ransom.

That reality makes all organizations a target even if your agency has a very low ability to pay.

Can my Agency prevent an attack?

All systems have vulnerabilities. Thus if the attacker is persistent and patient enough, they will find a way in.

That said, your agency can and must take steps to make entry into your agency very difficult. In addition, your agency should be ready to immediately contain any breach that does occur. Lastly, if and when an attack occurs, your agency must have a plan in place for continuity of services, and ultimate recovery from a “successful” breach.

NEXT STEPS

With all of the above in mind:

1. Complete and submit this assessment to GSRMA
2. Meet with your GSRMA Risk Control Advisor, who will discuss the findings of the assessment and any recommended actions

Potential recommendations include:

- Deployment of active End-point Protection (EDR) software (i.e. advanced Anti-virus solutions)
- Enablement of Multi-factor Authentication (mfa)
- Updating of backup procedures to ensure recoverability
- Password management tools
- On-going security awareness training
- Complete Risk/Ransomware Readiness Assessment

GSRMA
GOLDEN STATE RISK MANAGEMENT AUTHORITY

Cyber Risk Self-Assessment

Contact Information

* 1. Date of Survey

Date / Time

Date

MM/DD/YYYY

* 2. Agency name

* 3. Who is completing this survey

Name	
Title	
Email	
Phone	

Cyber Risk Self-Assessment

Basic Cyber Exposure

* 4. Has your agency had a formal Risk Assessment or Ransomware Readiness Review completed by a 3rd party within the past 12 months? If Yes, please provide a copy of the report to your Risk Control Advisor including a summary of the follow up tasks completed or in progress by your agency to address the deficiencies and exposures identified in the assessment.

Additionally, feel free to refer to your assessment report when responding to the questions in this survey. No need to duplicate the information.

○ Yes

○ No

* 5. Does your agency store any records electronically (regardless of where, how, agency or personal devices, etc.)? Examples include banking records, email, payroll, health benefit and claim forms, other information specific to your district type, ...

○ Yes

○ No

○ I don't know

* 6. Does your agency access any type of information electronically (regardless of where, how, agency or personal devices, etc.)?

○ Yes

○ No

○ I don't know

* 7. Are any computers that are used for agency business (regardless of where, how, agency or personal devices, etc.) connected to the Internet?

○ Yes

○ No

○ I don't know

GSRMA
GOLDEN STATE RISK MANAGEMENT AUTHORITY

Cyber Risk Self-Assessment

IT Landscape

This set of questions provides a picture of the overall scope of computer equipment and devices used by your agency as well as the individuals/organizations responsible for their management.

8. What individual is responsible for "IT functions" in your agency? (Examples of IT functions include computer setup and maintenance, adding/removing programs, set up for new employees, backups, Internet access, etc.)

Name

Title

Email

Phone

* 9. Does your agency have one or more IT staff (i.e. job description is specific to IT)?

○ Yes

○ No

* 10. Are the IT functions for your agency performed solely by internal staff or are there one or more 3rd parties (either another public agency or private company) that perform some/all of these functions?

○ Solely performed by internal IT staff

○ Solely performed by one or more 3rd parties

○ Performed by both internal staff and 3rd parties

○ We have no IT function requirements

11. If there are any 3rd parties, please list them and the functions they provide.

Vendor 1

Vendor 2

Vendor 3

Other

* 12. How many computer "desktop" systems does your agency have?

* 13. How many computer "laptops/notebooks" does your agency have?

* 14. How many computer "tablets" and mobile phones does your agency have?

* 15. How many computer "servers" does your agency have?

* 16. Do you allow personal mobile phones (not owned or managed by your agency) to access agency email, documents, core business systems, or any other data/systems related to your agency?

○ Yes

○ No

* 17. Do you allow personal computers to access agency email, documents, core business systems, or any other data/systems related to your agency?

○ Yes

○ No

Cyber Risk Self-Assessment

Disaster Exposure

Imagine that today, right this minute as you are reading this, all of a sudden all of the computers in your agency were disabled and destroyed. There is no access to anything on your computers; they are as good as dead and are not recoverable. It's as if they were all destroyed in a fire.

18. Given that you have no functioning computer systems and no data from those computers, how severely would your agency's services be impacted? This includes both internal and external processes. For example, performing payroll for your staff, producing records for the public, processing payments, reporting data to other agencies, etc.

○ All services would be shutdown or severely impacted

○ Most services would be shutdown or severely impacted

○ Some services would be shutdown or severely impacted

○ None - we either don't rely on computers or we have manual backup processes

19. Given that in this scenario, you have no internal computer systems, do you have the ability to access your data and/or systems from other computers that are external to your agency (i.e. could you login from a computer at home to a website that stores your data and/or runs an application that your agency uses)?

○ Yes

○ No

○ I don't know

20. If you were to get replacements for all of your computers tomorrow, how many do you have recent backups for?

○ All

○ Most

○ Some

○ None

○ I don't know

21. For those computers that do not have a recent backup, is there data on those computers that will impact your agency and/or your staff if they are permanently lost?

○ Yes

○ No

○ I don't know

22. If you have backups of the data for your computers, what is the latest copy of the data that you have (i.e. 1 day, 1 week, 1 month, a few months, etc.)?

23. If you have backups of the data for your computers, but the backups are not recent, how will you recreate the data that you do not have in your latest backup?

24. How do you know that your backups will actually work when you try to restore them onto your new computers?

○ Backups are verified

○ Backups are periodically tested

○ We don't actually know

25. What happens if one or more of those backups turn out to be faulty and do not provide some/all of the data? How will you recover from that circumstance?

Cyber Risk Self-Assessment

Data Exposure - PCI Data

PCI Data

PCI Data means credit card information within the scope of the Payment Card Industry Data Security Standard.

26. Does your agency store credit card information for your agency and/or 3rd parties (constituents, businesses, etc.) on any desktop, laptop or server, or within a website or computer software used by your agency? This includes credit card numbers, names, expiration dates, and security codes.

○ Yes

○ No

○ I don't know

27. If yes, please describe.

Cyber Risk Self-Assessment

Data Exposure - PII Data

PII Data

The DHS defines personally identifiable information or **PII** as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to your agency.

The DHS defines **Sensitive PII** to include but is not limited to Social Security Numbers, driver's license numbers, Alien Registration numbers, financial or medical records, biometrics, or a criminal history. This data requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

28. Does your agency store any PII or Sensitive PII data on desktop or laptop computers, servers, or cloud storage on the Internet?

○ Yes

○ No

○ I don't know

29. If yes, please describe.

30. Does your agency store any PII or Sensitive PII data via a website or computer software your agency uses?

○ Yes

○ No

○ I don't know

31. If yes, please describe.

32. Does your agency store data (either directly or via a website/computer software) that seems like it might be PII/Sensitive PII data, but is not listed in the definitions above (i.e. you aren't sure, but it might seem to be)?

○ Yes

○ No

○ I don't know

33. If yes, please describe.

GSRMA
GOLDEN STATE RISK MANAGEMENT AUTHORITY

Cyber Risk Self-Assessment

Data Exposure - PHI Data

PHI Data

PHI stands for Protected Health Information.

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.

It is not only past and current health information that is considered PHI under HIPAA Rules, but also future information about medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health information in any form, including physical records, electronic records, or spoken information.

Therefore, PHI includes health records, health histories, lab test results, and medical bills. Essentially, all health information is considered PHI when it includes individual HIPAA identifiers. Demographic information is also considered PHI under HIPAA Rules, as are many common identifiers such as patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, that when they are linked with health information become HIPAA identifiers.

34. Does your agency store any PHI data on desktop or laptop computers, servers, or cloud storage on the Internet?

○ Yes

○ No

○ I don't know

35. If yes, please describe.

36. Does your agency store any PHI data via a website or computer software your agency uses?

○ Yes

○ No

○ I don't know

37. If yes, please describe.

38. Does your agency store information (either directly or via a website/computer software) that seems like it might be PHI data, but is not listed in the definitions above (i.e. you aren't sure, but it might seem to be)?

○ Yes

○ No

○ I don't know

39. If yes, please describe.

Cyber Risk Self-Assessment

Critical Business Systems

Critical Business Systems

A critical business system is any application/software/website that your agency uses to conduct its primary business and functions. These functions include but are not limited to providing services to the public and other agencies, providing reporting and data to other public agencies (local, state, and federal), and supporting internal operations of the agency including HR, administration, finance, payroll, etc.

40. What are the critical business systems for your agency?

41. For each of these critical systems, specify below how long your agency can operate without it.

Critical System 1	
Critical System 2	
Critical System 3	
Critical System 4	
Critical System 5	
Critical System 6	
Others	

Cyber Risk Self-Assessment

Data Exposure - Other

42. Does your agency store (desktop, laptop, server, cloud storage) or maintain (via a web site, computer software) any other information that is not accessible to all of your staff and/or the public (i.e. it is either sensitive or confidential)?

○ Yes

○ No

○ I don't know

43. If yes, please describe.

44. Is any PII, PCI, PHI or Other Confidential Information ever stored on an unencrypted USB flash drive (i.e. portable memory/storage device)?

○ Yes

○ No

○ I don't know

45. Taking into consideration all of the above, what are the impacts to public trust and reputation for your agency if any of the data or critical systems become targets of cyber crime?

GSRMA
GOLDEN STATE RISK MANAGEMENT AUTHORITY

Cyber Risk Self-Assessment

Protection

46. What email system does your agency use (i.e. Office 365, Gmail, etc.)?

□

47. Are employees enabled to access email remotely via a web browser?

○ Yes

○ No

○ I don't know

48. If Yes, is Multi-Factor Authentication (mfa) enabled for this access for all employees? (MFA requires a user to enter additional information when accessing a system - typically a numeric code that is sent to the person's mobile device. "Authenticator" apps can also used for this purpose.)

○ Yes

○ No

○ I don't know

49. Does your agency have a virtual private network (VPN) configured?

○ Yes

○ No

○ I don't know

50. If you have a VPN, is Multi-Factor Authentication (mfa) enabled for this access for all employees?

○ Yes

○ No

○ I don't know

51. Does your agency use anti-virus or other end-point protection (EDR) software?

○ Yes

○ No

○ I don't know

52. If Yes, which anti-virus and/or end-point protection (EDR) solutions does your agency use?

53. What percentage of your agency's computers utilize some form of anti-virus or end-point protection solution?

○ 100%

○ 90%-99%

○ 50%-89%

○ 0%-49%

○ I don't know

54. How often are updates/patches applied to your agency computers (i.e. Windows Updates, computer software updates/patches, ...)?

55. How often do you train your employees on the following: Social Engineering, Phishing, General Cyber Security Training, and Training of Account Team Staff on Fraudulent Transactions?

○ Consistently on a monthly basis

○ Once Annually

○ Occasionally

○ We don't currently perform this type of training

Other (please specify)

Cyber Risk Self-Assessment

Readiness

Backups

On any given computer, there are at least two types of information stored on them:

1) The operating system (i.e. Microsoft Windows, Apple MacOS, etc.) and applications (Outlook, Excel, Word, etc.)

2) Agency data/information: internal and public records, saved correspondence, etc.

Information in Category #1 can be reinstalled as needed.
Information in Category #2 needs to be backed up in case of computer failure.

56. For each computer in your agency that has Cat #2 data stored on it, is a backup being performed on that data?

○ Yes

○ No

○ I don't know

57. If yes, how often?

58. If yes, have those backups ever been tested to make sure that they can be read successfully?

○ Yes

○ No

○ I don't know

59. How are these backups being performed (by who and using what software and/or service)?

60. Where are these backups being stored?

61. Who in your agency has access to those backups?

62. Does anyone outside of your agency have access to those backups?

○ Yes

○ No

○ I don't know

63. Is the backup data being encrypted?

○ Yes

○ No

○ I don't know

64. Is the backup data being saved in a read-only fashion such that it cannot ever be modified?

○ Yes

○ No

○ I don't know

65. Does your agency have a Disaster Recovery Plan? If so, when was it last reviewed or tested?

66. Does your agency have a Business Continuity Plan? If so, when was it last reviewed?

67. Does your agency have a Cyber Incident Response Plan? If so, when was it last reviewed?

Cyber Risk Self-Assessment

Additional Information

68. Please provide any additional information regarding your agency's risk and readiness for cyber incidents

69. Do you have any comments or feedback regarding this survey