Atkinson, Joel

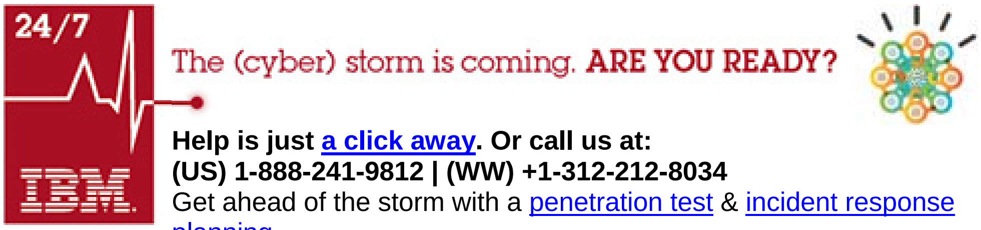
From: Matthew Beard <beardm@us.ibm.com>
Sent: Thursday, November 12, 2015 3:08 PM
To: Atkinson, Joel
Cc: Judy Srail
Subject: RE: IBM Emergency Response Services

Hello Joel

Please see my answers in Red below.

Matthew Beard

Security Services - Business Development
IBM Security Services, NA.
beardm@us.ibm.com
813-388-1725



Help is just a click away. Or call us at:
(US) 1-888-241-9812 | (WW) +1-312-212-8034
Get ahead of the storm with a penetration test & incident response planning

"Atkinson, Joel" ---11/12/2015 02:16:40 PM---Hi Matt: So that I am able to let our Agencies know which services your company provides will you an

From: "Atkinson, Joel" <Joel.Atkinson@dms.myflorida.com>
To: Matthew Beard/Tampa/IBM@IBMUS
Cc: Judy Srail/Cleveland/IBM@IBMUS
Date: 11/12/2015 02:16 PM
Subject: RE: IBM Emergency Response Services

Hi Matt:

So that I am able to let our Agencies know which services your company provides will you answer a yes or no to the following categories:

I. RESPONSE

In order to develop a list of potential vendors that provide cyber-security assessment and remediation services, as well as identity protection, monitoring and protection services, the Department is requesting the following information:

Please indicate whether your company is able to provide any or all of these services:

1) Pre-Incident Services:

a) Incident Response Agreements – Terms and conditions in place ahead of time to allow for quicker response in the event of a cyber-security incident. Yes, we can provide an agreement for 1, 2 or 3 years. This agreement pricing includes hours to supply assessments, preparation guidance, response plan development and training. All the below are included in a full agreement or we can also scope these out individually.

b) Assessments – Evaluate a State Agency's current state of information security and cyber-security incident response capability. Yes, this is included in an ERS Agreement with IBM or can be provided in separate SOW. IBM will Evaluate your current threat and risk level; helps identify malware/botnet activities and other early signs of potential security attacks or advanced persistent threats

c) Preparation – Provide guidance on requirements and best practices. Yes, this is included in an ERS Agreement with IBM or can be provided in separate SOW. IBM provides incident response preparation, enabling you to recover more quickly with simulated attack event scenarios and stress testing

d) Developing Cyber-Security Incident Response Plans – Develop or assist in development of written State Agency plans for incident response in the event of a cyber-security incident. Yes, this is included in an ERS Agreement with IBM or can be provided in separate SOW. IBM Offers an in-depth analysis helps you discover holes in your existing security approach and learn how to remedy them

e) Training – Provide training for State Agency staff from basic user awareness to technical education. Yes, this is included in an ERS Agreement with IBM or can be provided in separate SOW.

2) Post-Incident Services:

a) Breach Services Toll-free Hotline – Provide a scalable, resilient call center for incident response information to State Agencies. Yes, IBM provides a 1-800 hot line for immediate triage due to a breach. 1-888-241-9812 This number can also be called by anyone not under an IBM agreement also.

b) Investigation/Clean-up – Conduct rapid evaluation of incidents, lead investigations and provide remediation services to restore State Agency operations to pre-incident levels. Yes, IBM will provide resources to regain resiliency as quick as possible depending on size and scope of breach.

c) Incident response – Provide guidance or technical staff to assist State Agencies in response to an incident. Yes, IBM Emergency Response Services (ERS) subscription is designed to provide resources to assist you in preparing for, managing, and responding to computer security incidents – including steps for analysis, intelligence gathering, containment, eradication, recovery, and prevention.

d) Mitigation Plans – Assist State Agency staff in development of mitigation plans based on investigation and incident response. Assist State Agency staff with incident mitigation activities. Yes, I BM staff will assist in all mitigation efforts to get back to a steady state. We will also review all mitigation plans for future incidents if they take place.

e) Identity Monitoring, Protection, and Restoration – Provide identity monitoring, protection, and restoration services to any individuals potentially affected by a cyber-security incident. No, IBM does not supply Identity Monitoring, Protection and Restoration Services. This would be a 3rd party that would provide this type of service. IBM will work closely with

State fo FL and the 3rd party Identity Management company chosen.

Joel Atkinson
Associate Category Manager
Bureau of Information Technology & Special Projects
Division of State Purchasing
Florida Department of Management Services
4050 Esplanade Way Suite 360
Tallahassee, Florida 32399
Ph: 850-487-0758
Joel.Atkinson@dms.MyFlorida.com
@FloridaDMS
facebook.com/FLDMS

"We Serve Those Who Serve Florida"

Maintain Process-Oriented Mindset
Challenge the Status Quo
Create Efficiencies
Respect State Employees

From: Matthew Beard [mailto:beardm@us.ibm.com]
Sent: Friday, October 30, 2015 9:09 AM
To: Atkinson, Joel <Joel.Atkinson@dms.myflorida.com>
Cc: Judy Srail <jsrail@us.ibm.com>
Subject: IBM Emergency Response Services

Hello Joel

I am the IBM Security Services Lead for Florida and support all Managed Security Services and Professional Security Services. I am pleased to present you with the attached information to comply with the
Department of Management Services RFI for Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring, and Restoration Services.

IBM leverages the expertise of our industry certified analysts and consultants who have specialized experience in cyber forensics and various other emergency response services. Our robust incident response services leverages security intelligence assimilated from numerous Managed Security Services engagements and IBM X Force Research. IBM uses this information to help revise and enhance your security program. We utilize time tested tools and software to provide customized services based on a subscription model.

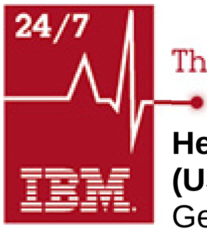
The standard Emergency Response Service is subscription based and agencies can chose to sign up for the subscription. We do have the ability to scope out these services separately on a case by case basis. We can also generate a blanket State Wide Agreement for Florida and I am free to discuss this in more detail.

(See attached file: FL Dept of Management SRV RFI.doc)

(See attached file: IBM Emergency Response Services.pdf)

Matthew Beard

Security Services - Business Development
IBM Security Services, NA.
beardm@us.ibm.com
813-388-1725



Help is just a click away. Or call us at:
(US) 1-888-241-9812 | (WW) +1-312-212-8034
Get ahead of the storm with a penetration test & incident response planning

October 30, 2015

Joel Atkinson
Associate Category Manager
Bureau of Information Technology & Special Projects
Division of State Purchasing
Florida Department of Management Services
4050 Esplanade Way Suite 360

Dear Joel Atkinson:

IBM is pleased to respond to the Florida Department of Management Services RFI for Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring, and Restoration Services. The FL Department of Management Services will reap tremendous benefit from IBM's global leadership in delivering innovation within the Public Sector and our proven security methodology along with worldwide resources and expertise.

IBM requests the opportunity to serve as your trusted cyber security advisor and looks forward to building a long-lasting relationship that will provide ongoing threat protection for your environment. Please do not hesitate to contact us should you have any questions about the information provided. We look forward to working with you on this important project.

Sincerely,

Matt Beard

IBM Security Services Lead
IBM Global Technology Services

beardm@us.ibm.com

Phone: 813-388-1725

Florida Department of Management Services

Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring, and Restoration Services – Request for Information

By Matt Beard
IBM Security Services Specialist
IBM Global Technology Service
1-813-388-1725
beardm@us.ibm.com

October 30, 2015

Executive Summary

A security breach can have devastating consequences for any enterprise, resulting in possible operational disruption, data leakage, reputation dam-age and regulatory complications. The lack of a unified incident management process, coupled with inexperienced staff, can increase the business impact of such incidents. An enterprise wide threat prevention and response strategy can not only help you recover from unforeseen security breaches and downtime more quickly, but can also help prevent future incidents.

IBM Cyber Security Assessment and Response Services provide access to highly skilled security consultants who can conduct preemptive incident preparation, data preservation, in-depth data analysis and response and management functions in the event of an incident. Designed to provide a preventive and proactive approach, we can facilitate greater visibility into threats and enable a more rapid remediation while supporting complex infrastructures and industry specific operations.

IBM IT emergency response services (ERS) can provide real-time onsite support should a security breach occur. Our solution helps you:

- Manage incident response more efficiently across stages including prevention, intelligence gathering, containment, eradication, recovery and compliance management
- Resolve issues more quickly by delivering faster response times
- Access deep technical skills in real-time
- Be proactive through preemptive incident preparation, data preservation and in-depth data analysis

Objectives

The Department is seeking to identify vendors that are able to provide assessment and remediation services in the event of a cyber-security incident and provide identity protection, identity monitoring and identity restoration services to any affected individuals under GSA Schedule 70.

The Department provides centralized statewide contracts for use by all state agencies. This RFI requests information to help the Department determine which vendors under GSA Schedule 70 are able to perform the services described in this RFI.

Service Overview

IBM Emergency Response Service subscription provides access to real-time, on-site and remote support. The subscription retains expert security consultants to help your organization better prepare, manage and respond to security incidents. The subscription encompasses:

- Incident Response
- Incident Management
- Data Acquisition
- In-depth Data Analysis / Computer Forensics

The included activities are intended to support end-to-end incident response

- Prevention
- Intelligence gathering
- Containment
- Eradication
- Recovery
- Compliance

IBM Delivery Model

IBM Emergency Response Services is based off of a subscription model and all 5 steps are included in the service. These services can be scoped out separately to better meet client objectives.

1. **Kick Off**

   The initial workshop to gather information, review current incident response plan & declaration process, collaborate on staff hours usage plan, and establish procedures for incident data exchange

   - Identifies authorized primary & alternate Incident Declarers
   - Strategizes Subscription Staff Hours usage
   - Schedules Quarterly Checkpoints
   - Setup XFTAS Seats (2)
   - Discusses Incident Data Exchange

- Complete ERS Subscription Customer Questionnaire

2. Readiness Services

The utilization of subscription hours for CSIRP gap assessments, incident response scenario exercises, and/or an assessment of existing hidden threats, including the use of penetration testing.

At your discretion, IBM will perform one or multiple preemptive incident preparation services.

Active Threat Assessment

- Evaluate the current threat and risk level of your enterprise.
- Perform tool-based scanning and analysis to attempt to discover any potential malware and/or botnet activities in the current environment.
- Identify and document security exposures that may be used to infiltrate Customer's network.
- Assess the vulnerability of critical external facing assets by conducting network technical testing across Customer-specified Internet-facing IP network addresses.
- Exploit key identified vulnerabilities and target specific systems and attempt to gain direct access to confidential data and administrator or elevated access privileges on vulnerable systems.
- Attempt to compromise internal networks and systems by leveraging limited external access.
- Demonstrate specific or systematic security weaknesses, if present.
- As applicable, analyze and document its findings and recommendations to be included in the Final Report.

Security Incident Response Plan (CSIRP) Gap Assessment

- Identify the business units and processes in your enterprise with which your current computer security incident response plan interfaces.
- Determine how the current computer security incident process impacts these business units and processes.
- Identify the current computer security incident response team, including its roles, responsibilities, organization, and reporting hierarchy.

- Review the current computer security incident response plan, based on industry best practices, for your enterprise.

- Discuss telephonically your current state with the client computer security incident response team.

- If warranted, work with your computer security incident response plan development team, conduct telephonic interviews with representatives of your key business units, including, but not limited to, I/T system administration, I/T network administration, I/T security, corporate security, business continuity, legal, human resources, and public relations.

- Based on the information gathered during the aforementioned interviews, industry best practices, and other specific requirements you provide, update the current computer security incident response policy for your enterprise.

- Provide you with the opportunity to review each draft and make comments and suggestions as its development progresses. Up to three iterations of the write/review/comment/modify cycle will be provided at no additional charge.

- Provide you, within ten business days of the conclusion of the draft cycle, with a list of suggested next steps for you to follow to continue the maintenance of your computer security incident response plan.

Incident Response Training and Incident Simulation

- Conduct one half-day or full-day workshop to provide first responder type training, for up to 12 attendees.

- Work with key members of your staff to develop a computer security incident simulation exercise that will test your updated computer security incident response plan and procedures, with focus on the areas that may need to be updated or improved.

- Conduct and referee the incident simulation exercise on-site for one day at your location, paying particular attention to:

    a. whether your computer security incident response team is properly notified of the incident, and how long notification takes.

    b. how well the members of your computer security incident response team work with each other and members of higher management.

    c. how well your computer security incident response team performs in the five phases of incident response (analysis, containment, eradication, recovery, and prevention).

d. how well your computer security incident response team interfaces with external entities (Internet service providers, administrators of other sites, other response teams, law enforcement entities, etc.)

e. how well your computer security incident response team communicates with customers, external users, employees, and the press.

- Document findings in final report

Sample Incident Response Training and Incident Simulations

- Advanced Persistent Threats (APT)
- Zero Day Exploits
- Phishing (Spear/Whale)
- Social Engineering
- Denial of Service Attacks
- DNS Hijacking
- Network and Appliance Hijacking
- Identity Theft
- Network Intrusions (Rogue or Sustained Hackers)
- PHI/PII/PCI Data Compromise
- Network Abuse (Internal)
- Significant Employee Departures
- Due Diligence
- Significant Malware Outbreaks
- Cyber Stalking
- Theft of Intellectual Property/Services

3. Ongoing Checkpoints

The “open line” to an account manager for incident advice or assistance, a quarterly checkpoint to review subscription service usage, and updates on the current threat landscape.

Your Open Line to ERS

- Reach out to your account manager with questions
- 8 Hours a quarter are available for telephonic support
- Usually used for incident discussions/questions
- Also used for triage in the event of an incident
- Call the ERS Incident Hotline for Declarations

Quarterly Checkpoints

- Typically a 30-45 minute teleconference each quarter
- Discuss any ongoing incident support needs
- Share updates on current threat landscape
- Review current subscription staff hours plan
- Q&A

4 Emergency Response

The emergency response service can be activated with an incident declaration to ERS via the hotline, which is staffed 24x7x365 by ERS analysts who will coordinate the initial triage and work to initiate emergency response

Incident Declarations 24x7x365:

- Any time, call the ERS Incident Hotline for Declarations
- An Analyst will coordinate a Triage call to understand the current threat and determine the scope of response efforts

US Hotline: 888-241-9812

Global: (+001) 312-212-8034

What to Expect:

- ERS will provide remote or on-site response and analysis within 24 Hours*

- Data Acquisition will likely require support from your IT department (e.g. access, credentials, etc)

- Significant findings during the analysis process will be provided daily or as per your requirements

- A formal final report will include recommendations for future prevention as well as observations for enhancing security

5. Predictive Threat Intelligance

The department with get direct access to IBM X-Force Threat Analysis Service (XFTAS), which evaluates global online threat conditions and provides analysis for proactive security management.

XFTAS provides customized security intelligence about a wide array of threats with global insight

- Offers detailed analyses of global online threat conditions and includes:
    - Up-to-the minute, customized security information about threats and vulnerabilities
    - Expert analysis and correlation of global security threats
    - Actionable data and recommendations that help clients maintain their network security

Conclusion

IBM is position perfectly to assist you with assessment and remediation services in the event of a cyber-security incident. It is no longer IF you will be attached, it's when. Minimize the impact of security incidents with an enterprise-wide prevention and response strategy that not only assists you in recovering from unforeseen security breaches and downtime more quickly, but can also prevent incidents before they occur

Emergency Response Services Subscription

Resources to assist in preparing for, managing, and responding to computer security incidents, including steps for analysis, intelligence gathering, containment, eradication, recovery, and prevention

Incident Response Program Development

Create an effective plan that allows you to almost immediately react and reduce the impact of a security breach

CSIRP Gap Assessment

In-depth analysis helps you discover holes in your existing security approach and learn how to remedy them.

Incident Response Training and Simulated Exercise

Incident response preparation enables you to recover quickly with simulated attack event scenarios and stress testing

Active Threat Assessment

Evaluate your current threat and risk level; helps identify malware/botnet activities and other early signs of potential security attacks or advanced persistent threats

Forensics solution implementation

Deploy the right forensic investigation tools to help you improve defense and automate the incident response and forensic analysis process