OHCS Current State Analysis of BC/DRP Strategy

Introduction

OHCS Current State Analysis of BC/DRP Strategy

Robert Dunbar is the chief security officer (CSO) at OHCS, a company that provides healthcare services like healthcare plans, patient services and referrals and management of patient information. He's thinking about the technology disasters and security issues that have been occurring lately. In the past two years, 90 percent of all healthcare organizations have had at least one data breach, with an average cost of $2.2 million.

He decides to schedule a meeting with his executive staff to make sure the company has a current, viable business continuity / disaster recovery plan in place in case of a major disaster.

Meeting with Vice Presidents

The CSO, Robert Dunbar, has scheduled a meeting with his direct reports.

Robert Dunbar, Cheif Security Officer: All right, everyone, it's time for us to take a look at our disaster readiness and security posture. From what I can see, there are so many security incidents happening lately in the healthcare industry. I was just reading another article about a healthcare organization that got slammed with multiple breaches in the past two years. That raises my concerns about our company's business continuity / disaster recovery plan, and our readiness to prevent or reduce potential threats in the future. I want a two-phased project approach to (1) analyze our current state with respect to our readiness and (2) develop a BC/DRP recommendation report with solutions to any identified faults.

Ralph Green, Vice President of Digital Forensics: That's a great idea, Robert. I think we should select someone from each major department: Physical Security, Data Forensics, Healthcare Security, and Network Security. I think Alicia should be the lead.

Robert: Agreed.

Alicia Monroe, Vice President of Network Security: Thanks, Ralph! I'll schedule a meeting with the team ASAP.

Ralph: Thanks, Alicia. Thank you all!

Meet the Team Members

Robert Dunbar, Cheif Security Officer

Robert Dunbar is responsible for the security of the company's physical and digital assets. Responsibilities include regulatory compliance, identifying security initiatives, overseeing the safeguarding of intellectual property, computer systems, and databases, implementation of global security policy, standards and procedures, and overseeing risk assessments and mitigation strategies. Robert has bachelor's and master's degrees in computer science. He is a Certified Information Systems Auditor (CISA) and a Certified Information Security Manager (CISM).

Ralph Green, Vice President of Digital Forensics

Ralph Green is responsible for the investigation of fraudulent incidents relating to patient and system information. He manages a group of six computer forensic analysts, who use forensic tools and techniques to analyze data, data breaches, intrusion detection events, and any evidence of unlawful or unethical employee behavior. Ralph has a bachelor's degree in engineering, a master's in computer science, and a Certified Forensic Computer Examiner (CFCE) certification.

Alicia Monroe, Vice President of Network Security

Alicia Monroe is responsible for risk assessment across departments, ensuring that risk remediation provides audit response planning. She drives both IT and business strategies to ensure delivery of security solutions, and provides expert advice on compliance, risk, privacy and security related matters. Alicia has bachelor's and master's degrees in computer science. She is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM).

Team Meeting for Current State Analysis

Alicia meets with team members to discuss current BC/DRP strategies.

Alicia: Good morning, everyone! Thank you for attending today's meeting. Due to recent natural and man-made disasters that have negatively impacted healthcare companies around the world, our CSO has requested a review of our current BC/DRP strategy (Phase I) and the development and presentation of a recommendation report (Phase II).

As each of you know, you were selected from our major departments to be part of this team to conduct a current state analysis of our BC/DRP strategy. We categorized this analysis into five segments.

Danielle is responsible for analysis of the 24/7 continuous operations of our call center services (CCS). She'll also be analyzing our data recovery strategy.

Jason is in charge of our application and data backup strategy.

Tony has our offsite storage strategy.

Finally, Angela is in charge of our communications strategy.

You were all contacted last week and asked to conduct a current state analysis of your assigned segments. Let's get started with a review. Danielle?

Danielle, Network Defence: Currently, we have a 24-person call center. We have a 90% coverage rate for our 24/7/365 coverage. Our customer service application and data warehouse run on HP servers, and backup is completed nightly. The disks are stored in a room right next to the call center area. There is no fail-over strategy that includes offsite facilities or equipment. Our call

center is located in the basement of the main building. Customer information is stored on the HP servers located in the main computer room on the second floor.

Jason, Digital Forensics: This is our current application and data backup strategy: The data center backs up all applications and data warehouse information nightly. The disks are stored in a locked, fireproof cabinet located next to the call center area.

Monday through Saturday, we do incremental backups, and the full backup happens on Sundays. We have a cold site storage facility on the property.

We don't have any warm sites set up with peripherals and software. We also don't have a high availability and fault tolerance strategy.

Tony, Physical Security: As Jason indicated, we don't have a strong offsite storage strategy for our applications and data backups. It was decided awhile back that the costs were too high to invest in offsite facilities. We do have an uninterruptible power supply (UPS) and backup generator equipment, but they haven't been fully tested. Maybe now we can provide evidence of a need to invest in an alternative site for both storage and operations.

Alicia: Thanks, Tony, Jason, and Danielle for your updates. Sounds like we have our work cut out for us! Danielle, can you provide us now with a review of our current data recovery strategy?

Danielle: Well, based on Tony and Jason's update, we know that our data recovery strategy is very weak. I'm concerned about not having an offsite location for parallel or stand-alone running of the call center and data recovery. There was talk about hiring an external company that provided recovery services, including power, communications and technical support. This external company would have been responsible for establishing a secure recovery site, configuring equipment, developing remote services for our call center operations, and securing the confidential data. But again, the costs were too high.

Alicia: Thanks, Danielle, for that update! Angela, last but not least, can you provide us with your analysis of our current communications plan for our BC/DRP process?

Angela, Healthcare Security: Sure! Our current BC/DRP communications strategy consists of a list of contact employees that includes senior management and leaders from the four major organizations. The strategy does include high-level assignments, but not a detailed responsibility matrix. We do have a set of instructions to recover facilities and rebuild our critical applications, including the call center services application, and it's available to all assigned employees. We have a training and testing schedule, but we haven't performed a test this year. We do not have a current corrective action plan for identified issues around the BC/DRP process.

Alicia: Thanks, Angela! So the next steps will be to provide this update to our senior leaders. I will be meeting with them tomorrow. Phase II of the project will include a new team of experts that will review this update and develop a formal BC/DRP strategy recommendation report. It will explain the background, problems, alternative solutions and recommendations for developing and implementing a revised BC/DRP strategy for our organization.

CapraTek™ Headquarters-Ian Walter's Office

Ian Walter is the project manager for a feasibility study to select an ERP vendor. Knowing that Ian has just started work on the project, Rhonda stops by Ian's office to check in with him about how things are going. After talking with Ian, Rhonda finds herself thinking seriously about some of his comments.

Is Ian following PMI ethical guidelines or not?

This question has not been answered yet

Possibly not. Ian's plan to use team members he's previously worked with might be precluding opportunities to other people in the organization.
No. His relationship with the SAP vendor creates a real conflict of interest.
Yes, his plan has the potential to leverage existing relationships in ways that can benefit the organization.

Email to the CSO

To: Robert Dunbar, Cheif Security Officer

From: Alicia Monroe, Vice President of Network Security

Subject: BC/DRP findings

Robert,

My team has completed our current state analysis of our BC/DRP process. Here are some high-level findings. The deficiencies identified include:

- Resource complement for the CCS is 10 percent below minimal level for 100 percent operational coverage.
- Limited data back-up strategy.
- No offsite storage facility.
- No Emergency Operations Center facility.
- No parallel or alternative site operations procedures.
- The following BC/DRP policies and procedures require updating:
    - Call-out listing.
    - Recovery of applications, databases and data warehouses.
    - Equipment configurations.
- Limited testing and training plan.
- Limited communication plan strategy.

Conclusion

OHCS has its work cut out for them to improve their readiness for disaster recovery and security incidents. How will you apply what you've seen to your team's BC/DRP strategy recommendations?

Credits

Subject Matter Expert:
Kathleen Allour
Interactive Design:
Danielle Kaardal Meyer
Interactive Developer:
Matt Taylor
Instructional Design:
Graeme Braithwaite
Media Instructional Design:
Fira Roudenko
Project Management:
Andrea Thompson