CLIENTFIRST TECHNOLOGY CONSULTING

Disaster Recovery Workshop

IASBO 2025 Annual Conference

Presented by

Paul Miller - Director - Cybersecurity Practice
Craig Williams - Director Infrastructure Consulting Practice

Paul Miller - Speaker
- Director Cyber Security Practice
- ClientFirst Technology Consulting
pmiller@clientfirstcg.com
(847) 598-0345 x6300

Craig Williams - Speaker
- Director Infrastructure Consulting Practice
- ClientFirst Technology Consulting
cwilliams@clientfirstcg.com
(630) 656-7366

Lee Pietrowski – Moderator
Partner
Imagetek
lpietrowski@IMAGETEC.com
(630) -717-3772

Disaster Recovery Overview

Disaster Recovery Planning (DRP)

- The technical complement to the business-focused BCP
- Technical controls that prevent disruptions and facilitate the restoration of service

Business Continuity Planning (BCP)

- Assessing the risk to organizational processes
- Creation of polices, plans and procedures to minimize impact
- Maintains continuous operation in the event of an emergency

Incident Response Planning (IRP)

The scope of today's presentation will cover Disaster Recovery.
You are the CSBO, charged with creating an after-action report about lessons learned from a building and IT outage.

District Overview

K-8 District

- 3 Grade Center Schools (K-2, 3-5, 6-8)
- 750 Students, 160 Staff Members
- Aging Heating, Ventilating, and Air Conditioning systems
- Technology Data Center is located in the Junior High Building
- Main Internet access is also in the Junior High

Staff

Department
Superintendent's Office
Business Office
Technology
Facilities
Teachers
Community
3rd Party Vendors

Scenario

It is one week after winter break…

Sunday afternoon

- An outside group is renting the lunchroom for an event.
- They call to say the heat is not on.
- Facilities checks and they cannot access the HVAC system remotely
- They come to the school and find they are not able to log into the HVAC control system, which is in the Maintenance Office. They place a call via cell phone to their temperature control vendor, who creates a dispatch ticket for Monday morning.
- Facilities calls the Technology Director about the HVAC server being down. They also notice that wireless is not working. They cannot reach the Technology Director, who is on vacation without cell phone access. They have no other numbers for Technology contacts, so they decide to wait until Monday.

Scenario

Monday Morning

- Faculty arrive onsite. Temperature in classrooms and offices is tolerable. However, Internet, wireless, telephones, and printing are not working.
- Other buildings also report that the Internet, wireless, and telephones are not working.
- Technology discovers that the Data Center has not had cooling all weekend. The temperature is 120 degrees. The core internet switch, firewall, and all virtual servers have overheated.
- Technology opens door into the Data Center and brings in portable cooling units. They manage to get the Data Center cooled down to 80 degrees.
- The core switch, firewall, and virtual servers do not respond. They have all failed and will need to be replaced.
- The decision is made to send all students home at Noon and declare
- an e-learning day for the following day.

Scenario

Tuesday – Friday

- The e-learning days continue while Technology scrambles to purchase, install, and configure new equipment.
- Parents are upset about the sudden e-learning days. They are demanding alternate arrangements, and a return to service immediately. Many cannot arrange daycare on short notice.
- The incident makes the local, online newspaper. With the Superintendent out of town, the Assistant Superintendent schedules a press conference. He is ill-prepared. The session does not go well.
- The temperature control vendor determines that the HVAC server was the victim of a cyberattack and orders a new server. Facilities staff balance the temperature controls within the building.
- Cybersecurity forensics firm works with the District to collect evidence of the attack and help find the perpetrator.

Key Takeaways

Disaster Recovery Planning and Preparation

- Create a planning and recovery team
- Perform a business impact assessment (BIA)
  - Critical business functions
  - Consequences of disruption
  - Prioritizing recovery strategies (RTOs, RPOs)
- Identify critical data
- Document policies
- Put resources in place for backup, response, and recovery
- Create a DR playbook

Example - System Prioritization

Applications/Systems	Max Down Time	Priority
Telephone System	2 Hours	1
Internet Access	2 Hours	2
Network Access	8 Hours	2
System Backups	2 Days	5
Outbound Community Communication Platform	4 Hours	2
Temperature Control Systems	4-8 Hours	1
Physical Security/Door Entry/Cameras (changes)	2 weeks	7
Student Information Systems	8 Hours	4
Student Transportation Systems (changes)	1 week	6
Web Server	8 Hours	3
Remote Access	2 Days	5
HR System	8 Hours	3
Payroll System	8 Hours	3

Example – Planning & Recovery Team

Department	Responsibilities
Superintendent's Office	Communication with Board, Parents, and Community
Business Office	Liaison to insurance and operations
Technology	Performs recovery actions and restores systems
Facilities	Building Operations
Teachers	Validate E-Learning Set Up
3rd Party Vendors	Help with Disaster Recovery, Contingency Planning & Resources

Questions and Answers

Paul Miller - Speaker
- Director Cyber Security Practice
- ClientFirst Technology Consulting
pmiller@clientfirstcg.com
(847) 598-0345 x6300

Craig Williams - Speaker
- Director Infrastructure Consulting Practice
- ClientFirst Technology Consulting
cwilliams@clientfirstcg.com
(630) 656-7366

Lee Pietrowski – Moderator
Partner
Imagetek
lpietrowski@IMAGETEC.com
(630) -717-3772