Business Continuity Tabletop Test

Overview

This document outlines a tabletop test for a credit union to assess its business continuity capabilities. The test objectives, scope, participants, roles, agenda, and scenarios are described below.

Test Objectives

- To evaluate the effectiveness of the credit union's business continuity plan and procedures in response to events that affect its IT systems and operations.
- To identify any gaps or weaknesses in the credit union's business continuity plan and procedures that need to be addressed or improved.
- To test the communication and coordination among the credit union's staff, management, and external stakeholders during a business disruption.
- To enhance the awareness and preparedness of the credit union's staff and management for potential business continuity threats and challenges.

Test Scope

The test will cover the following aspects of the credit union's business continuity plan and procedures:

- Incident response and escalation
- Business impact analysis and recovery prioritization
- Backup and restoration of data and systems
- Alternate work arrangements and locations
- Member services and communication
- Regulatory compliance and reporting

The test will simulate an escalating scenario that involves the Incident Response Plan, Business Continuity Plan, Disaster Recovery Plan, Communications Plan, and the Standard Operating Procedures.

Test Participants and Roles

The test will involve the following participants and roles:

- Test Facilitator: The person who will lead the test, present the scenarios, inject additional events, monitor the test progress, and collect feedback from the participants.
- Test Observer(s): The person or persons who will observe the test, record the actions and decisions of the participants, and evaluate the test results and outcomes.
- Business Continuity Team: The group of staff and managers who are responsible for implementing the business continuity plan, procedures, and coordinating the recovery efforts.
- Business Unit Representatives: The representatives of the credit union's various business units, such as operations, finance, marketing, human resources, etc., who will provide input and feedback on the impact and recovery of their respective functions.
- External Stakeholders: The representatives of the credit union's external stakeholders, such as regulators, vendors, partners, media, etc., who will be simulated or consulted during the test.

Test Agenda

The test will follow the agenda below:

- Introduction and briefing: The test facilitator will introduce the test objectives, scope, participants, roles, and rules, and answer any questions from the participants.
- Scenario: The test facilitator will present the scenario. The test facilitator will inject additional events and challenges as the test progresses. The test participants will respond to the scenario according to their roles and responsibilities, and document their actions and decisions.
- Debriefing and feedback: The test facilitator will summarize the test results, outcomes, and solicit feedback from the participants on the strengths and weaknesses of the credit union's Plans and Procedures, and the lessons learned from the test.
- Report and recommendations: The test observer and evaluator will prepare a report that details the test results, outcomes, and provides recommendations for improvement.

Test Scenario

Scenario: Jane is a back-office employee at the credit union. She uses her work computer (VDI) to access the credit union's Core financial system, online banking system, email, and other applications during her normal workday. One day, while browsing the web during her lunch break, she does some quick online research for a new product that caught her eye on Facebook (on her personal phone) earlier. Several hours later, her system starts to behave strangely. It has spurts of being slow and unresponsive, and some of the icons on her desktop disappear. She attempts to reboot the session, but it doesn't seem to want to shut down. After a few hours of dealing with some of these issues, she contacts the IT department, and they suspect that her session might have been infected by malware. Shortly after arriving, the IT department confirms that Jane's computer has been compromised and an unknown process is using significant resources and bogging down her system and producing heavy network traffic. The crack IT department realizes they need to keep this session alive for forensics to know what it might have accessed and isolates Jane's VDI and initiates a security incident response process.

Jane's system did have access to key systems including the Core, the Accounting System, Teams/SharePoint, and other shared folders.

- What teams do you contact internally? Where is this documented?
- How do you validate that the member information is not affected?
- Do you shut down the core and other member services during investigation?
- What does your forensics plan look like?
- Is there an organization you can call on for forensics?
- How do you preserve things for forensic analysis?
- How do you preserve the data in the core for investigation while allowing members to continue to use it?
- What organizations can you call on for support? Where is the list for this documented?
- How do you alert the credit union employees to be on the lookout for related issues?
- How do you alert the fraud team to be on the lookout for related issues?
- How much data do you lose going back to a previous copy of the data?
- What is the Core Service Provider's response to your reporting of a potential breach?
- What will the Core Service Provider do for recovery? Is anything in the contract?
- What are the reporting requirements at this point? Do you have a format for reporting? Do you have a list of who to report to?

Inject

The malware is determined to have been by a zero-click malvertisement, which is a type of malicious advertisement that exploits a vulnerability in the browser or the operating system to deliver malware without requiring any user interaction. The malware had access to her machine for approximately 3-4 hours before it was reported and isolated. Firewall logs show that it appears to have been talking to sites on the Internet during that time. After consulting with the Cyber Insurance provider, the CU leadership has determined that because Jane's machine had wide ranging access to member information that the best course of action is to shut down access to everything that could have been affected in order to complete forensics and determine if anything beyond infecting her system had taken place. It could have been possible for someone to access the Core, access different spreadsheets or databases, exfiltrate data, or update information within the Accounts Payable system. This sends the CU into a full-on Business Continuity situation.

- What is available in the Business Continuity Plan to handle a situation where the Core is down, by choice, and could remain so for days?
- How can members access their funds with the core shut down to preserve forensic information?
- How is impact to vital member services minimized?
- What limits are in place? Where is this documented?
- How can those limits be changed with systems shut down?
- How are records of manual transactions kept and recorded?
- Will fees be waived internally?
- Will fees be paid for late payments when members cannot access funds?
- How is the situation communicated internally?
- How is the situation communicated externally?
- If the M365 environment is also shut down, how do you contact everyone? Where are there lists of contact information?
- What are the reporting requirements now?
- How would systems be recovered and brought back up to date? What is the order that services are brought back up?

Debriefing and Feedback

This scenario was based upon real situations that have recently occurred in our industry, some of which are still ongoing today. The questions are meant to help consider and pre-plan our actions should something similar happen. As Gen Dwight D. Eisenhower once said, “I find that in battle, plans are useless, but planning is indispensable.”

This team hopes that this scenario provoked some thoughts on improvements that can be made in systems, processes, and documentation within your area. Please provide feedback to the team on what improvements you would like to make.

Attendance

In attendance on the BCP test on 9/5/2024 were:

Kelli Bartczyszyn

Srigowri Sriram

Amy Primrose

Jackie Templeton

Edwin Plaza

Patty Mitchell

Steve Koinm (External)

Jill Sammons

Megan Kelly

Chuck Smith

Jeanne Richmond

Maggie Vela

Steve Jauregui

Bjorn Larson

Bob Suing

Keaton Messerschmidt

Rubal Sharma

Keith Parris

Shelley Doherty

Bethany Wulf

Brian Millar

Scott Comeau

Kourtney Ross

Steve Elliott

Sri Aravamudan

Cinthya Jaramillo

Chris Pfieffer

Gordon Kenmuir

Jim Block

Mike Valentine

Stephenie Southard

Stacy Bausea

Joe McCarthy

Todd Buersette

Eric Liesener

Nicole Van Leishat

Jonda Rost

Zeke Hellenbrand

Any Auw

Jorge Hurtado

Amanda Jackson

Amanda Jerik

Kimberly Veneziano

Maggie Gargia

Davi Allen

Rob Russeu

Reporting and Recommendations

The following Notes and Action Items were recorded during the session.

What teams are contacted internally?

Contact System Engineering, Security, Vendor(s). Would engage the Business Continuity Team. Would notify the Senior Executive levels and Legal. Notify and spin up the Incident Response Team. If there is information to be shared (very likely), then someone on the Communications Team. General Controls for Incident Management. Templates and drafts for communications. If information needs to be shared with the team, someone like Kourtney Ross would start notifying the employees through SharePoint and other means.

Do you shut down the core to preserve things?

In the triage process they would then start looking to see what communications has happened from the machine. Then go to the cyber insurance provider to start the forensics process if the severity warrants it.

What is the forensics process?

Inside the general controls there is a plan for containment and eradication. Would engage cyber insurance before starting to shut down and contain things.

Can also engage Crowdstrike to look to see running processes and things that happened during that timeframe. Crowdstrike would have seen the odd behavior.

Do you have identified vendors to assist with Forensics?

Would contact Haloc, whom we have worked with before. We have regular engagements with them for other items like Risk Assessments and other items. We have a retainer with them for incident response. If identified at a certain level of severity or criticality then contact Cyber Insurance provider Beazley.

Do you have a process to preserve the information in the core (for forensics) while still allowing for member access to services?

Would contact Jack Henry as the core provider to know about how to maintain the information. Get their input on how to best proceed here. Using EASE to manage the core systems. Use JHA to understand how it might have impacted the core.

We have listed several critical vendors here. Is there a list managed somewhere?

The list of critical vendors is in the Business Continuity Plan. This plan is hosted by LogicGate on the network.

How would information be communicated to internal team members?

There are many methods of internal Communications. Email, Texting, building workers, remote workers, and updates feed on the Intranet. Security also has a SharePoint site. Security will notify about awareness things. That site might also get some information shared to broadcast information about what has happened. The communications would include information about keeping the information within the circles where it needs to be kept. Have regular classes to remind people to never speak to the press. Would immediately remind employees not to communicate this information any further. Also have social media guidelines about what you can post personally.

How would the Fraud Team be notified?

Fraud would be notified during the incident response process to start looking for things that look suspicious or different.

If there is the potential of compromised data within the core, how much data would you lose if you go back to previous backups? How do you restore/recover the core?

We have the conversation with JHA. We currently do a backup every night and then start running through the T-logs (Transaction Logs).

Would you expect any type of negative reaction from Jack Henry? Something akin to cutting you off to make sure you don't infect some other client?

JHA has been a fantastic partner. They will get things back to production ready. Legal being part of the biz continuity members would be looking through the contracts to see what happens.

Would you need to declare an incident with JHA?

We would work with Jack Henry to understand the risk and evaluate next steps.

What about reporting requirements at this stage?

With this being suspected, start drafting up a communication to the NCUA. We have members in many different states so we will need to start reaching in respect to state privacy laws and letting them know. There is a Beazley agreement to draft up the communications. Have a general controls incident list in the appendix of the Incident Response Plan for whom to contact.

With the situation escalating, the leadership and the cyber insurance providers have determined that the Core and member services need to be shut down for a period of time in order to investigate more fully. What does the plan say for a situation including a voluntary shutdown of the Core?

Would pull together the command team. They would work with the rest of the management team to handle how to deal with vendors and managers. Put together workarounds for the core being down. This scenario is not currently in an incident response plan right now.

How do you get ready for this to happen and provide members with access to funds?

Would start up a duplicate version of the core and bring that online as quickly as possible up to the point of where the situation arose. When the potential of this occurring would be thought, we would start to get this ready.

We would start posting things on socials, get communications together. Taking a page from Patelco's event, document everything into a new landing page for a security event.

If the core is down, then the branches have limits set up for offline transactions to be completed. Can document the transactions off the core for a period of time.

If we are going to bring down the Core, we are going to ask the whole organization to look at their backup procedures. Start working with the lenders to know how they can still provide with this. Start working with Online Banking to review limits, etc.

If the core is only taken down from a VPN perspective (back to BCU) then Online Banking could remain up. We could potentially get OLB back up with another version of the core while the CU remains disconnected.

What would happen with ATMs?

ATMs would go into offline mode. ATMs are not connected to the Core; they are connected to PSCU and Fiserv. Debit cards have established daily limits for each card. PSCU disconnects would mean that the ATM's would go out of service. Not sure how that would work if they disconnected. Either the core or the service provider would need to authorize a

transaction. Credit card team says that the authorization would come through Visa but that would not work if PSCU were disconnected.

The limits we have discussed are for the short term. What if this was going to become a longer-term outage?

Established limits are in place for offline limits. If this is going to go on for more time, need to change those limits. Can roll that out to the teams. There is risk if they are unable to validate the funds with members. What is the process to establish what their last available funds might have been. Money movement outside of cash would be down. Not a way to look at last available to determine risk levels. Would OLB show a balance for when the connection was last severed? If we took the core down through the VPN then things like micro-services would go down but other things might stay up and running.

If lumen still had connection to the core, they have the admin connection so maybe they have the possibility to see balance information.

If the core is not responding, would Credit Cards still be usable?

Yes, we have microservices with lumen/pscu. That could still allow for things to work for the Credit Cards.

Start assessing the risk of changing offline limits. If PSCU is still up, then they could change the limits at PSCU. Have a branch operations communications system. Would write up a procedure and communicate it out in that system. They would communicate that they received that.

What is the process to log and manage offline transactions?

Did a short trial run when the world went down with CrowdStrike. If they are going to log a deposit or debit they run through and keep the transactions in their daily work. Those tickets are then processed in the branch to get that back up to date. The bigger impact would be the OLB side of things.

Do we cut off calls transferred to CCSS since they will not be able to help?

Via the ticketing system they could still help them.

Would Bill Pay work?

PSCU services the platform but it is hosted through Lumen. If they can get to the portal. That is still money movement. It would come to a halt.

If the core is down, not processing Fedline files. That would limit everything with ACH, Drafts, Zelle, etc. Still have information where the information could be done manually by

logging into the Fed. But the money would not actually come out of the member's account. So there is a big risk there. Money Movement is stopped. Wires could happen but we couldn't manage that back to the core. You could manually do the loan and log it, and then perform the transaction. That is less risky. Not going to be receiving funds. Won't be able to sell Zelle. Can we disengage during the downtime?

The members could still access BillPay through Lumen and PSCU if they are up. But the transactions could not post to their account.

Would fees be waived?

In general, the command team will determine whether fees are going to be waived. They have done that in the past where fees are waived for days for bigger events.

If we cannot talk to Fedline, how can we order cash for the branches?

If they can get to Fedline they can order cash for the branches. In the process to get another cash-in-transit provider. Would have some redundancy to get the cash to the branches.

Update on OLB access from Sri.

If Lumen is up and the core is down then they go into Stand-In mode. They will have the sync'd transactions so they can show the previous balance. From the Lumen admin tool can the employees see the same balance? Can use the view-as-user mode and be able to see the balance. But they have been cutting that access back recently. But it could be changed back in an emergency.

BillPay is an SSO. Capture the info through the first time they log into Lumen. Billpay is risk based and not balance based. Just the reconciliation phase is where the funds flow through.

Discontinued share branching. How do they turn something on in the case this occurs? Offline processes and limits for shared branching.

Following up on Communications. How would things be further communicated?

Have an Intranet called Search where they can really show a lot of what is happening internally. They can create an FAQ internally. Lots of internal meetings and videos to make sure that everyone knows. Search if the knowledge base product from Salesforce. Is there a way to connect for more information within that.

Internal push notifications and Text messages can get out to users. Would have overheads and emergency broadcast system. Different IVR methods. Without SharePoint they could

put a hidden site or page that can just be accessed by the employees and send out a text message. Also have communicator line through everyone's badge. They can call in to that number.

Note about the SMS Messaging system!

Everyone needs to opt-in to the SMS message system! Employees cannot be automatically added. They have the ability to use the SMS service (Day Force) and convert it into an emergency conference call. But it can only notify everyone that has taken the time to opt-in.

Noted that everyone's badge will have a phone number on it for emergency updates.

Turns out that not everyone's badges seem to have a phone number on them at this point.

DayForce has home pages that something can be posted on. If an employee is using the DayForce app, can you push notifications through that? DayForce has emergency broadcast processes.

Need to make sure that employee account coding is up to date in Symitar.

If Teams is down, SharePoint is down. Where are the procedures?

Some are in Search/SalesForce. Critical communications library is offline on the desktop for Kourtney.

Where does everyone keep those procedures?

Will document where those are.

If we now need to report, what do we need to report and how?

We have hit the 72 hour rule, state rules, privacy laws, vendors, employees, members, Boards, etc. Could be via different ways that those happen.

How are systems restored and brought back up to date?

As soon as the core came up they would start going through the transactions and run them forward. The old core that was used for forensics would go away. The backup core would become the new core. Recovery Matrix in the DR Plan. They have a BIA that is put together on a regular basis. RTO and RPO's are put together with MTD. The core, communications with vendors, network access will be top of the list. Tier 2 is the 24 hour or less item. Tools to make things work, etc.

Could people do their jobs without SalesForce and Temenos?

In the branch world they could do a lot in the core directly. They could do primary member servicing. Have a lot that would work but may things would really be a struggle. There used to be life without Temenos.

Most of the work does happen in the core. But new employees are not trained on how to do things in the core directly. Do we have knowledge in-house to do that? Would have to spread out the tenured agents. The workarounds are probably not documented at this point. The back-office probably knows how to do some of the things but there would be no processes for the frontline. Offline limits are now a SalesForce workflow. Can we make those changes in the core? Yes, but how?

Does it make sense to prioritize necessary transactions and document how to complete those transactions directly in the core?

Does the Backup call center have its own connection to the Core?

Backup call center uses the BCU connection, they are in the process of getting their own direct connection. So if that connection were down, both primary and backup call centers are down.