SELF-RUN TABLETOP EXERCISE · FOR BANKS AND CREDIT UNIONS

# The Breach That Starts With Someone Else's Software

A 90-minute incident response rehearsal your team can run in a conference room. No software, no consultants, no preparation beyond printing this. Adapted from OPERATION DANGER CLOSE, a facilitated exercise built from a real 2023 event.

## WHY THIS SCENARIO

Most institutions rehearse their own failure: ransomware on their own network, an outage in their own data center. Far fewer rehearse the morning a trusted third-party product becomes the way in, when the vendor controls the fix and you control none of it.

That is also where examiners press. Not whether you have a plan, but whether you tested it.

**Hold this in mind.**

Your first priority is not stopping the attacker. It is keeping the business running while you stay in control.

| WHO SHOULD BE THERE | RUN TIME | GROUP SIZE |
|---|---|---|
| Anyone you would call on a real Saturday: IT, risk, legal, ops. | 60 to 90 minutes. Five phases, same rhythm each time. | 5 to 30. Break into teams of four so everyone holds a role. |
| **WHAT YOU NEED** | **FORMAT** | **WHAT YOU LEAVE WITH** |
| A room, a whiteboard, a timer, someone to read aloud. | Discussion-based. No laptops, no simulation, no technical setup. | A documented test, a list of gaps, and named owners. |

## HOW IT RUNS

1. **Read.** Facilitator reads the phase aloud. One minute, no slides.
2. **Huddle.** Teams work the questions and commit to a move. Four minutes.
3. **Share.** Two teams report back. Disagreement is the point.

## FOUR RULES THAT HOLD THROUGHOUT

1. Protect people first.
2. Keep the business running.
3. Stay in control of facts, timeline, message.
4. Paying a ransom is the last resort.

## THE SETUP · READ THIS ALOUD FIRST

You work at **Harbor Point Bank & Trust**, a regional institution serving 1.5 million customers. Every day it moves loan documents, wire instructions, payroll batches and regulatory reports through **FileBridge**, a file transfer product from a vendor called **Vantage Software**. Boring. Trusted. Everywhere. It is also about to ruin a holiday weekend.

## THE FOUR SEATS

*The executive approves the plan and sets the tone, but does not run the response.*

| | | |
|---|---|---|
| **Chief Executive** | Owns final approval and outside stakeholders. | Give decisions, not instructions. |
| **Incident Commander** | Owns execution and keeping the bank open. | Define the incident in one sentence. |
| **CISO** | Owns the security program. | Turn the technical picture into a risk decision. |
| **Legal & Comms** | Owns obligations, clocks, regulators. | Track what is reported, to whom, by when. |

## 1 Panic

SATURDAY, 6:00 AM

Vantage announces a flaw in FileBridge being exploited worldwide. No patch exists. Your on-call analyst is at home, rumors are spreading, and the CEO is awake and asking what is happening.

- Define the incident in one sentence.
- What do you know, and what are you afraid of? Say which is which out loud.
- Who makes the first call, and what does calm sound like right now?

## 2 Control

SATURDAY, NOON

Still no evidence Harbor Point was hit. Someone proposes pulling FileBridge offline now. That freezes loan closings and Tuesday's payroll.

- Are you overreacting or under-reacting? Argue both.
- What does shutting down cost if you are wrong, against what waiting costs if you are right?
- What should already have been in place: policy, contract terms, training?

## 3 Confirmed

SUNDAY INTO MONDAY · BANK CLOSED

Forensics finds unauthorized software on your FileBridge server and evidence files were copied out Friday night. Scope unknown, and people are tired.

- What changes now that this is confirmed as yours?
- How do you preserve evidence while operations keep running?
- How does leadership steady a tired team on day three?

## 4 Obligations

TUESDAY

Copied files held names, addresses and account numbers for roughly 95,000 customers. A criminal group posts Harbor Point on its leak site demanding $3 million. A reporter emails.

- **What clocks just started, and who must be told?** Banks notify their primary federal regulator no later than 36 hours after determining a notification incident occurred. Credit unions notify NCUA within 72 hours of reasonable belief, including when a third party is the one who tells them. NYDFS Part 500 sets 72 hours, and that clock covers incidents at a service provider too. Public registrants have four business days on Form 8-K for a material incident. Argue whether stolen files with the doors still open even meets the federal threshold. Confirm your own.
- **Do you pay?** Who decides, and is law enforcement getting a call at all? Under Part 500, paying starts a 24-hour notice to NYDFS and a 30-day written account of why it was necessary and what alternatives you weighed. Decide now who writes that.
- What do those 95,000 people receive from you, and when?

## 5 Recovery

THE FOLLOWING WEEK

A patch ships and the server is rebuilt. Forensics runs for months, but leadership wants a preliminary report now.

- Would replacing the tool actually prevent this? Any vendor can be breached.
- Which single control would have shrunk the damage most?
- What can you honestly put in writing while the investigation is open?

### CAPTURE BEFORE THE ROOM EMPTIES

*Undocumented means it did not happen, to an examiner.*

- ☐ Who attended, in what role, on what date.
- ☐ Every decision the room could not make, and why it stalled.
- ☐ Each gap, with a named owner and a date. A person, not a department.
- ☐ Anything in the written plan that failed under pressure.

### FACILITATOR NOTES

THE REVEAL · SAVE THIS FOR THE END

## Harbor Point is invented. The rest is drawn from the public record.

| IN THE EXERCISE | WHAT ACTUALLY HAPPENED |
|---|---|
| **Harbor Point Bank** | M&T Bank |
| **FileBridge, from Vantage Software** | MOVEit Transfer, from Progress Software |
| **An unknown flaw, exploited before anyone knew** | CVE-2023-34362, exploited by the CL0P extortion group |
| **Roughly 95,000 customers** | At least 95,261 Massachusetts residents, per M&T's filing with the state Attorney General. Exposure in other states was not disclosed. |
| **One bank in the story** | 2,773 organizations and more than 95 million people, per Emsisoft's final tally in June 2024 |
| **A ransom demand on a leak site** | CL0P extorted MOVEit victims broadly and most refused to pay. There is no public record of M&T paying. |
| **A compromised server inside the bank** | M&T stated its own systems were not compromised. The exposed files sat with third-party service providers running MOVEit. The exercise puts the server inside your building so every decision stays on your side of the table. In the real version, you would be waiting on someone else's forensics too. |

**WHERE THE EXERCISE STRETCHES THE TIMELINE**

Progress disclosed the flaw and shipped a patch on the same day, May 31, 2023. The theft had already happened days earlier, over the Memorial Day weekend, before anyone knew to look. The exercise holds that window open so the room has to make the Phase 2 decision with no patch in hand, which is exactly the position the earliest victims were in.

No PINs, passwords, Social Security numbers, dates of birth or payment card numbers were reported exposed, and no funds were confirmed stolen from accounts. The damage was fraud exposure, class action litigation, and the cost of proving care. Illustrative only. This is not legal advice and not a determination of your obligations. Every deadline above is summarized, not quoted, and thresholds turn on facts. Confirm your own against your charter, your primary regulator and your counsel.

## The facilitated version goes further.

Live injects, a scenario rewritten around your actual vendors and charter, and a written after-action report your board and your examiners can read.

Built by a former OCC and NYDFS IT examiner, from the perspective of the person who eventually asks how you tested this.

To scope a session: contact@blackknightrm.com · blackknightrm.com