Critical Incident Response Framework

Every financial advisory firm relies on technology, vendors, people, and processes to serve clients and protect sensitive information.

Unfortunately, incidents happen.

Some are caused by malicious actors. Others are the result of human error, outdated systems, vendor failures, or simple bad luck.

Canadian advisory firms have experienced:

- Business email compromise
- Ransomware attacks
- Privacy breaches involving client information
- Lost and stolen devices
- System outages
- Vendor disruptions
- Poor patch management[1] resulting in security vulnerabilities
- Accidental deletion of critical files
- Insider threats and employee misconduct

[1] Patch management is the process of regularly updating software, operating systems, and devices to fix security vulnerabilities, improve performance, and reduce the risk of cyberattacks.

These incidents can be crippling. They can:

- Disrupt client service
- Consume significant advisor time
- Create regulatory obligations
- Result in financial losses
- Damage your firm's reputation
- Most importantly, erode client trust

The purpose of this framework is to help your firm create a simple and practical response plan before an incident occurs.

Your response plan won't prevent every incident. However, it can significantly reduce confusion, delays, and unnecessary damage when something goes wrong.

This document represents the first step.

Once your plan is developed, review it regularly – perhaps every six months – and update it as team members and responsibilities change. Test the plan by walking through imaginary tabletop exercises where you can game out critical incidents to ensure everyone understands their role and can quickly execute the plan under pressure.

Step 1: Identify Critical Incident Scenarios

Consider the incidents most likely to impact your firm.

Examples:

Cybersecurity Incidents

- Business email compromise
- Ransomware attack
- Malware infection
- Unauthorized access to firm systems

Privacy Incidents

- Client information sent to the wrong recipient
- Lost laptop or mobile device
- Unauthorized disclosure of confidential information

Operational Incidents

- CRM outage
- Deletion of critical files
- Phone system failure
- Internet disruption

Vendor Incidents

- Critical vendor outage
- Vendor cybersecurity breach
- Vendor bankruptcy or service disruption

For each scenario, ask:

- What would happen?
- Would impact, if any, would there be to clients?
- How long could we operate before a solution is in place?
- Who would need to be involved?

Step 2: Establish an Incident Response Team

Identify the individuals within your advisor firm who will be responsible for managing an incident.

Every role should have a primary and backup person.

Role	Person Responsible	Back-Up

- Does everyone understand their role?
- Does everyone understand who makes decisions?
- Are backups identified?
- Is authority clearly delegated?

Step 3: Create an Emergency Contact List

Create and maintain a list of critical contacts should your network/CRM be inaccessible.

Include:

Internal Contacts

- Leadership team
- Advisors
- Operations staff
- Compliance personnel

External Contacts

- Dealer/MGA
- Managed IT provider
- Cybersecurity provider
- Software vendors
- Legal counsel
- Cyber insurance provider
- Etc.

Questions:

- Is contact information current?
- Can it be accessed quickly?
- Does more than one person maintain it?

Step 4: Define the First 24 Hours

Many incidents become worse because firms lose valuable time.

For each critical incident type, determine:

Immediate Actions

Examples:

- Pinpoint affected systems
- Contact the IT provider
- Document events
- Preserve evidence

Assessment Questions

- What happened?
- When did it happen?
- What systems are affected?
- What client information may be involved?
- Is the incident ongoing?
- Is there a risk to clients, e.g. unauthorized activities or disclosure of personal information?

Escalation Criteria

- Who decides whether to activate the response plan?
- When should legal counsel be engaged?
- When should your insurers be notified?
- When should your dealer/MGA Compliance be engaged?

Step 5: Develop a Communication Plan

Clear communication is critical during an incident. Determine:

Internal Communications

Who needs updates?

- Advisors
- Operations staff
- Leadership
- Compliance

Client Communications

Who communicates with clients?

What situations require client notification?

How will messages be approved?

If you need to send a message to all clients, how would you do that? For example, do you have a mass email capability associated with your CRM? If your CRM is compromised, what are your fallback options?

External Communications

Who communicates with any necessary external contacts?

- Dealer/MGA
- Vendors
- Legal counsel
- Insurance providers
- Etc.

Questions:

- Is there one designated spokesperson?
- Are approval processes clear?

Step 6: Ensure the Plan Remains Accessible

A response plan is useless if nobody can access it during an incident. Consider:

- Printed copies
- Secure offline copies
- Copies stored outside the primary network
- Copies available to key people

Questions:

- Can the team access the plan if your network is unavailable?
- Can the team access contact information if your CRM/email is down?
- Do people in backup roles know where to find the plan?

Step 7: Assess Team Readiness

A plan only works if people are prepared to execute it.

- Does everyone understand their responsibilities?
- Have backups been identified?
- Do individuals feel confident in their role?
- Have key decision makers reviewed the plan?

Areas requiring additional training:

Role/Name	What Skills & Knowledge are Required?	Target Date(s)

Step 8: Conduct Tabletop Exercises

A tabletop exercise is a structured discussion that walks participants through a hypothetical incident. Each scenario below has happened to advisor firms in Canada.

The purpose of this exercise is to test the plan, identify gaps, and build confidence. Discuss:

- What happened?
- What actions would we take?
- Who would be responsible?
- What challenges might arise?

Record a transcript of the tabletop exercise so you can quickly summarize any gaps in your plan, takeaways and lessons learned.

Example Scenario #1

An advisor's email account is compromised and fraudulent wire instructions are sent to several clients.

Discussion:

- Who discovers the incident?
- Who is notified?
- Who communicates with clients? What do you tell them?
- Is compliance involved?
- Is legal counsel involved?

Example Scenario #2

A ransomware attack locks access to the CRM and your client file management system.

Discussion:

- How does the firm continue operating?
- Who contacts the IT provider?
- What steps do you take to recover?
- How do you service your clients in the meantime?
- What do you say to them?

Example Scenario #3

An advisor laptop containing client information is stolen.

Discussion:

- What information may have been exposed?
- What regulatory obligations exist?
- Who must be notified?
- How do you document the incident?

Tabletop exercises should be conducted at least annually and whenever significant changes occur to systems, vendors, or people in your firm.

Annual Review Checklist

At least once per year:

☐ Review incident response roles and responsibilities, including back-ups

☐ Verify contact information

☐ Update vendor contacts

☐ Review communication procedures

☐ Update critical systems inventory

☐ Conduct a tabletop exercise

☐ Document lessons learned

☐ Update the response plan

Summary

An incident response plan doesn't eliminate risk. It gives you structure and an immediate plan when stress levels are high and decisions must be made quickly. With a solid plan, you will:

- Know who is responsible.
- Know how to communicate.
- Know how to continue serving clients.
- Know how to protect client trust.

The firms that respond best to incidents are rarely the firms who avoid every problem. They are the firms that prepare before a problem occurs.