

Cyber Incident Response Quick Card

Disclaimer: This material is intended as only an example which you may use in developing your own form. It is not considered legal advice and as always, you will need to do your own research to make your own conclusions regarding the laws and ethical opinions of your jurisdiction. In no event will ALPS be liable for any direct, indirect, or consequential damages resulting from the use of this material.

Meet Mark:

Mark Bassingthwaighte, Esq., serves as Risk Manager at [ALPS](#), a leading provider of insurance and risk management solutions for law firms. Since joining ALPS in 1998, Mark has worked with more than 1200 law firms nationwide, helping attorneys identify vulnerabilities, strengthen firm operations, and reduce professional liability risks.

He has presented over 700 continuing legal education (CLE) seminars across the United States and written extensively on the topics of risk management, legal ethics, and cyber security.

A trusted voice in the legal community, Mark is a member of the State Bar of Montana and the American Bar Association and holds a J.D. from Drake University Law School. His mission is to help attorneys build safer, more resilient practices in a rapidly evolving legal environment.



Contact Information:

Mark Bassingthwaighte, Esq.
ALPS Insurance Agency
111 N. Higgins Ave, Suite 600
Missoula, MT 59802

(T) 800.367.2577 | (D) 406.523.3859

mbass@alpsinsurance.com

www.alpsinsurance.com



What To Do in the First 24 Hours After a Suspected Cyber Incident

Cyber incidents often move quickly. The actions taken in the first hours after discovering a breach can significantly affect the outcome.

Step 1 — Stop the Spread

- Disconnect affected computers or devices from the network and internet.
- Do not immediately shut down systems unless directed by IT or forensic professionals.
- Preserve evidence by avoiding unnecessary changes to affected devices.
- Do not wipe or reimage devices until instructed

Step 2 — Contact the Right People Immediately

- Notify your IT provider or cybersecurity specialist.
- Contact your cyber liability insurance carrier if coverage exists.
- Notify firm leadership or partners.
- Consider contacting outside cybersecurity counsel if appropriate.

Step 3 — Identify What May Be Affected

Work with IT professionals to determine:

- What systems were accessed.
- Whether email accounts were compromised.
- Whether client files or confidential information may have been accessed.
- Whether financial systems or trust accounts were affected.



Step 4 — Secure Financial Accounts

- Alert your bank immediately if there is any risk of wire transfer fraud or trust account compromise.
- Review recent financial transactions for suspicious activity.

Step 5 — Change Credentials

- Reset passwords for compromised accounts.
- Enable multi-factor authentication if it is not already in place.

Step 6 — Evaluate Notification Obligations

Work with appropriate advisors to determine whether you must notify:

- Clients
- Banks or financial institutions
- Law enforcement
- Regulatory authorities or data breach regulators

(Note that notification obligations vary by jurisdiction and circumstances.)

Step 7 — Begin Recovery

- Restore systems from verified clean secure backups if necessary.
- Conduct a security review to determine how the breach occurred.
- Update security controls and procedures to prevent recurrence.