DATA BREACH

PREVENTION AND RESPONSE

Many computer attacks and data breaches go completely unnoticed until it's too late, with only the largest and costliest breaches ever making the news.
Here are some practical steps to take when responding to a cyber-attack:

Triage

Determine the level of compromise, set realistic expectations and determine whether there are any reporting and regulatory issues that need to be dealt with.

Containment

The primary purpose of this phase is to quickly limit the initial damage and prevent any further damage from happening.

Eradication or Remediation

This phase deals with the actual removal and restoration of affected systems. As with each of the prior phases of incident response, all actions taken will be thoroughly documented and can be used to determine the cost, in manpower and other resources, to determine the overall impact on the organization. It is important that the necessary steps are taken to completely remove malicious and/or other illicit content from the affected systems, which may also be beneficial toward satisfying regulatory compliance requirements.

Recovery

The purpose of this phase is to bring affected systems back into the production environment carefully, as to ensure that no further incidents occur. This may also be an appropriate time in hardening (securing) the systems to significantly reduce the organisation's vulnerability to further cyber-attacks.

Post-mortem and Lessons Learned

The purpose of this phase is to complete any documentation that was not done during the incident, as well as any additional documentation that may be beneficial in future incidents. This report should provide a play-by-play review of the entire incident, and will also be invaluable in determining the answers to the big questions – Who, What, Where, When, Why, and How.

Source Global Digital Forensics