Recommended incident response actions

Cyber Fact sheet

It is important that you follow a strict process in line with your incident response plan upon identifying a suspected or confirmed cyber security incident. Following a detailed plan will dramatically increase the chance of a positive outcome.

The UK Council for Registered Ethical Security Testers (CREST) has published an extremely thorough guide on all aspects of incident response from preparation to response and post incident actions. We highly recommended their guidance. Links are included in the useful resources section at the end of this document.

The information below summarises the advice and contains digestible practical steps that anyone suffering from an incident can implement.

As soon as you believe you have identified an issue consider the following:

Do:

- If identifiable, remove the affected system(s) from any network by disconnecting network cables or turning off Wi-Fi. If it's a mobile device, enable airplane mode straight away.
- Invoke your incident response plan.
- Contact the Federation of Small Business Cyber Helpline on 03450 727 727.
- Consider engaging professional help – you should think about using a company that has a CREST or NCSC certification for incident response as these have certified and experienced professionals that can handle cyber incidents (see useful resources below).
- Establish a reporting and communication channel with all parties requiring incident details and updates. Nominate someone to be responsible for distributing these details and updates on a regular schedule (for example every two hours).
- Document the incident – this doesn't have to be complicated, just a simple timeline detailing what actions have been performed, and by who, is adequate.
- Secure any potential evidence for investigation purposes – this may include physical media such as USB sticks/CDs or non-physical evidence such as screenshots (or photos of screens).
- Preserve pertinent logs – if you have logging turned on (and you should) these will be vital in understanding what has happened. If you can, keep copies of these.
- Conduct interviews of any involved users immediately and make notes.
- Consider if authorities/customers/staff/insurers need to be informed.

Don't:

- Panic.
- Wait to invoke your incident response plan.
- Probe computers and affected systems.
- Forward any suspicious emails or documents.
- Run any anti-virus or other utilities on affected systems – leave this to the investigation.
- Turn off affected systems – this can damage evidence.
- Reconnect affected systems until you are sure they are safe.

Post-incident actions

Once an incident has been successfully contained and any business impacts have been negated, it is wise to complete some or all of the steps below to reduce future risk, improve company preparedness and maximise customer satisfaction:

- Investigate the incident more thoroughly. Being able to successfully identify an incident's attack methodology may allow you to negate future attacks of this nature.
- Report the incident to relevant stakeholders. This will likely be a more thorough update than those provided during the incident as any impacts affecting the past, present and future should now be known.
- Carry out a post-incident review.
- Communicate and build on lessons learned.
- Update key information, controls and processes.