iVendi 10 Point Security Check

1 Check your patching is up to date

Make sure your servers, PCs, laptops and mobile devices are patched and up to date. This should include all applications as well as OS and firmware. It's a good idea to use a patch management solution and turn on automatic updates where possible.

Be sure that web-facing services are patched for known security vulnerabilities. Services of this type that remain unpatched can represent a very high risk and are likely to be targeted by attackers. You should also check the business cases and mitigating factors for known unpatched systems in relation to the increased threat.

2 Check access controls and password policy

Make sure all users are using unique passwords which are not used on other, personal accounts. Ask users to check that their passwords are strong and get them to immediately change any which are not. Password managers are an excellent way to maintain strong and unique passwords. If multi-factor authentication (MFA) is available, make sure it is enabled.

Be sure to review accounts that have privileged or administrative access and remove old, unused or unrecognised accounts. Privileged accounts could be system administrators but could also be accounts that have access to sensitive systems or information.

Following the principle of 'least privilege' is the best policy when managing access controls.

3 Check your defences

Ensure antivirus software is installed on all PCs and laptops, and regularly check that it is active on all systems and that signatures are up to date. Recheck that your firewall rules are as you would expect. In particular, you should check for temporary rules that may have been left in place beyond their expected use.

4 Check logging and monitoring

Review the logging you have in place. Check how logs are protected and how long they are retained. They should be held for a minimum of one month.

For the period of increased risk, you should consider increasing the frequency with which you check security logs on servers and network devices. A log management solution or SIEM will help a great deal with this process.

5 Check your backup and recovery strategy

Confirm that your backups are running correctly and that you have a documented recovery plan. Check that a recovery test has been carried out recently so that you can be confident you will recover from a system loss.

Recovery tests are important as they often reveal incorrect assumptions about how recovery from backup will work. The recovery test should additionally check that critical dependencies, other than data, can also be recovered, such as private keys and access tokens.

6 Check your incident response plan

Review your incident response plan and check it is up to date. Double check that escalation plans and corresponding contact details are all correct. Make sure it is clear who has the authority to make key decisions both during and outside of normal business hours if these individuals are different.

Your incident response plan should be available to all who may need it, whether they are in the office or working remotely.

7 Check your internet connections

Check that records of your internet connections are up to date. This should include factors such as which IP addresses your systems use on the web and which domain names belong to your organisation. Domain registration data should be held securely. Your domain registry account should have a strong password and MFA, if available.

Carry out an external vulnerability scan of all your internet connections and check that everything you need to patch has been patched.

8 Check your phishing response capability

Educating users on how to recognise likely phishing attempts and other forms of social engineering should be a part of your security awareness training plan. Make sure that staff know how to report phishing emails and that you have a process in place to deal with any security incidents that are reported.

9 Check third party access

If you need to let third party organisations have access to your systems, make sure you have a clear understanding of what level of privilege is extended into your systems, and who controls it.

During a time of increased cyber risk, you should be sure to remove any access that is no longer required.

Before allowing connection, you should review the security practices of the third parties in question. Supply chain attacks have been a rapidly increasing threat vector in recent times.

10 Check sources of threat intelligence

Staying up to date with relevant threats during a period of increased cyber risk is critical to avoiding and responding to security risks.

There are many excellent sources of threat intelligence, but a good default source is the National Cyber Security Centre (NCSC) website (https://www.ncsc.gov.uk/). You can go further and sign up for an NCSC CiSP account through which you can access and share information about threats with other organisations, as well as receiving immediate updates.

It is also possible to register for the NCSC Early Warning Service at https://www.ncsc.gov.uk/information/early-warning-service so that the organisation can inform you of any malicious activity originating from your systems.