HM Revenue & Customs

50 Questions to ask your IT provider

Version 5, 3rd July 2019

Many companies use external service providers to look after their IT systems to enable them to focus on their core business. Whilst the day-to-day management can be outsourced, security should be everyone's responsibility as the consequences if it goes wrong can be catastrophic. These questions are to promote conversation between Small to Mid-sized tax agents and their IT providers supporting a strong cyber security culture within the business. Security is a sliding scale that needs to be balanced within a risk management framework; not all of the methods discussed will be appropriate, or even sufficient, for different companies.

Internet connection and your network

1. Do we have firewalls enabled at our network edge and on our devices?
2. Do we let traffic into our network, e.g. remote workers? Is it all necessary? How often do we review the firewall settings?
3. Do we have logging enabled on our perimeter firewall? Are these logs monitored to identify any unexpected or suspicious activity?
4. If staff are able to work remotely, are we using a VPN and reviewing the logs? If we're using Windows Remote Desktop without a VPN, what controls are in place to stop criminals logging in?
5. Does your provider use remote administration tools like LogMeIn or TeamViewer to access computers? Are these products on PCs where it isn't required?
6. Do we use a web proxy[1] or DNS filtering service[2]? Do we use this for content filtering to stop potentially malicious files from being downloaded, or sites visited?
7. Is our Wi-Fi setup with appropriate security and encryption, and limited so that only authorised devices can connect?
8. Are the default passwords on all of our security devices changed to strong alternatives?
9. Do we segment our network, keeping our key systems in separate zones to protect them should our users or internet-facing systems be compromised?
10. Do we conduct regular penetration tests against our external internet connections?

[1] *Web proxies can store frequently-requested files, speeding up the office internet access. They also provide a central log of sites visited by employees, and like firewalls, these can integrate with security products and threat feeds to stop access to known malicious sites.*

[2] *DNS filtering services can help prevent devices on your network from connecting to known-malicious internet domains. There are a number of commercial and free options available, such as quad9.net.*

Secure devices and software

11. What is our vulnerability and patch management policy? Do we apply critical security updates straight away? If not, is the amount of time to test and install them proportionate to the risk they expose? Are we applying this to third party software we use in our website, or other online services too?
12. Do we have any computers running older versions of Windows or other operating systems to support legacy software that we cannot upgrade? What are the additional controls we have in place to protect these?
13. How do we ensure we are using the latest, secure versions of web browsers, browser plugins, operating systems, Office applications, website software, etc.? Are successful updates logged and unsuccessful updates addressed?
14. Do we conduct regular vulnerability assessments to identify out-of-date services and software on our network to verify our patching procedures? If we run a website, do we regularly check for web vulnerabilities, including the OWASP[3] Top 10?
15. If you have Bring Your Own Device to work policy, how do we secure work data on our employee's personal devices? What mobile device management service are we using to ensure control of our data? Can we remotely delete work data should our employee lose the device or their job?
16. Have we got an inventory of all the devices (computers, printers, etc.) allowed to access the network? Have we got controls in place to stop any other devices getting access?
17. Have we got an inventory or authorised software? Have we got controls[4] to identify and prevent unauthorised software from running? Do we have any remote administration tools installed that are unnecessary? Are we sure we installed them?
18. Have we got a secure baseline installation setup for our computers? This includes settings to ensure deployment of software updates, strong password requirements, removal of any unnecessary software and services and limiting user ability to prevent them changing security controls.
19. Do we have encryption on our devices to keep data safe should phones, laptops, USB drives, etc. be lost or stolen? Do we issue removable media (USB devices) to staff and restrict the use of unauthorised USB devices on our network?

[3] *The Open Web Application Security Project (OWASP) aims to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas, and provides guidance on where to go for further information.*
[4] *An example of application whitelisting is AppLocker in Windows 10.*

Control access to your data and services (accounts)

20. Do we have a clear understanding of our most important and sensitive data, with proportionate security controls to protect it, and monitoring to ensure the controls are effective?
21. Have we got end-to-end account management processes? Are accounts removed as employees leave, and their devices revoked from accessing the network? Do you monitor for new accounts being created that aren't authorised?
22. Do our users have the minimum level of system privileges required to do their job?
23. Are our administrators' accounts restricted to a limited number of people, and do we avoid using these accounts for high-risk activity like reading emails and web-browsing? Do we use privileged access management processes to carefully manage the administration of our most critical services?
24. Is access to our audit logs restricted to prevent deletion or modification?
25. Are our audit logs centrally consolidated and monitored in a Security Incident Event Management application for monitoring? Are our privileged accounts monitored to ensure only authorised activity is conducted?
26. Do we have a password policy that prohibits weak passwords? Do our accounts lock-out following repeated failed login attempts? Do our teams use two-factor authentication to log into their accounts? Should we be using a password manager application?
27. If you use Remote Desktop services, is logging enabled for successful and failed logins on your devices? Are these logs reviewed to ensure accesses are legitimate, and is the retention period sufficient to investigate problems? Is there an account lock-out setup for multiple failed logins, especially administrator accounts?
28. Do we have any data loss prevention tools to identify sensitive information leaving our network? Does this include coverage of encrypted data? How would we detect unusual data transfers? Do we record and monitor network flow data to help identify this?
29. Do we protect client data with encryption when stored, whether on devices, cloud storage, backup services, etc? How do we manage access to encrypted material when individual or suppliers no longer require access?
30. Do we protect client data with encryption in transit outside our network? Are data transfer applications, such as web, FTP and email, restricted to only encrypted channels?

Protect yourself from malware

31. What protection do we have from malware on email? Does our email provider reject email that fails sender checks (DMARC)? Do we use threat feeds to reject email from known spam domains? Does our mail provider run anti-virus checks

on our email? Does our desktop AV product run checks too (and is it a different AV product[5])?

32. What protection do we have in place for malware loaded from Office documents and PDF files? Are macros disabled by default on Office documents? Are PDF viewers up-to-date?
33. What protection do we have from web browser-based malware delivery? Do we any controls to prevent our staff from accidentally visiting malicious sites? Do we have riskier services like Java enabled in our browsers for external sites?
34. Can our staff install extensions and plugins on their browsers? How do we ensure these are not malicious and remain up-to-date? Can programs be downloaded and run from the internet by users?
35. Are we running the most up-to-date operating systems with the most current anti-malware capabilities?
36. What restrictions do we have in place to prevent staff from installing software themselves, whether intentionally or not?
37. Do our staff get sufficient awareness training of the techniques criminals are currently employing to deploy malware, and to dupe them into disabling security controls, e.g. enabling macros/content in Office?
38. Do we automatically run virus scans on removable media inserted into our computers? Is the auto-run feature disabled to stop programs automatically running when inserted?
39. How frequently are anti-virus scans run on devices? Are logging successful scans and identifying where scans have failed to run, and investigating why?
40. Do we have any controls that look for indicators of malware on our network, like an Intrusion Detection System? How frequently are the signatures updated? Have we considered Endpoint Detection and Response tools for identifying suspicious behaviours? Who looks at the logs and alerts and what action is taken on detections?

Being prepared

41. Do you use a risk management approach for security? Are you getting sufficient and frequent intelligence from your provider to appropriately assess the risk?
42. How does my IT provider keep their knowledge current about cyber threats?
43. Do we have an incident management plan to deal with likely cyber security scenarios? Are we testing these frequently enough?
44. Are we prepared for a ransomware infection on our network? Are we confident in our backup solution and frequency, and that network-aware ransomware cannot encrypt our backup data too? When did we last perform a test restoration of our backup data?

[5] *Multiple checks can be helpful if conducted at different points in delivery, as different vendors may detect different malware. Running multiple AV products on the same computer isn't a good idea though, as they are likely to interfere with each other's operation.*

45. Are we prepared if our website is compromised and defaced, our corporate email or social media accounts taken over, our HMRC login credentials stolen, etc.
46. Do we have DMARC email controls on our domain to restrict others from pretending to issue emails using our internet domain? This can help defend against external phishing attacks impersonating staff.
47. Are my staff suitably trained and aware of cyber threats and their responsibilities for security? How do we validate this is effective?
48. Have we enabled additional logging on services and devices where appropriate to provide additional information useful for investigating the scope and scale of a network intrusion?
49. Would we benefit from a penetration test and regular vulnerability scanning, internally and externally, to verify where our security controls are effective and where we have gaps?
50. Are we confident in our assurance of our partners and supplier's cyber security, that they apply similar to controls to the data we trust them with, and we understand and manage the risk of the access we grant them to our systems?

The National Cyber Security Centre (NCSC) provides clear, practical advice and guidance for a range of audiences, including a dedicated section for small and mid-size businesses.
https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

Cyber Essentials is a scheme developed by Government and industry to help business get the basics right to defend against cyberattacks. A self-assessment questionnaire can be completed to certify your business, reassuring your customers about your security and may attract new business. If you're not Cyber Essentials certified already, consider working with your IT supplier to achieve it. For more information, visit:
https://www.cyberessentials.ncsc.gov.uk/

What does 'Good' look like?

You have identified the data and services that are most critical to the successful running of your business, and the likely costs to your business should these be compromised. You are aware of the risks to these assets and you have invested proportionately to mitigate them to an acceptable level – your level of risk tolerance.

Internet connection and your network

Perimeter and host firewalls, configured to your businesses requirements. Remote access is via VPN and RDP services are not directly exposed to the internet. Gateway controls block access to high-risk websites and IP addresses. Your network is segmented with key assets such as databases held within separate zones with firewall rules (not set to any<>any) and monitoring of traffic between zones. Wi-Fi networks are encrypted. Logs are fed into your SIEM tool and monitored for anomalies. Regular scans of your IP addresses provide part of your assurance processes to identify any misconfiguration and unnecessary services visible to other internet users.

Secure devices and software

You have a patching policy that ensure updates are applied promptly, proportionate to the security risk that the update addresses, prioritised and fixed within defined timescales. Audit logs and vulnerability assessments are used to verify successful installation of updates, both on systems on your network, and on internet-facing services[6]. You have an inventory of authorised devices on your network, and the authorised applications installed, with means to identify any unauthorised items. Logs are fed into your SIEM tool and monitored for anomalies. You have a baseline build for your computers providing consistency, ease of management and easier for security staff to identify anomalies. This includes full disk encryption, and encryption of removable media.

Control access to your data and services (accounts)

User accounts are provisioned and removed to an agreed process, and a minimal number of accounts have Administrator privileges on a just in time basis, which are solely used for system administration tasks.
Logs are fed into your SIEM tool and monitored for anomalies. Two-factor authentication is used where available. Staff have the option of password managers to promote the use of unique, strong passwords across accounts. Remote Desktop access is not permitted without connecting via a VPN. Data loss prevention tools look for important data (client financial details, etc.) or unusually large volumes of traffic leaving your network. Secure (encryption) options are used for data transfers and external storage.

[6] *For example, this could include checking for updates for the software used on your website, like Wordpress.*

Protect yourself from malware

Incoming and outgoing email is scanned by anti-virus tools. Our email service checks the validity of incoming email using DMARC and anti-spam threat feeds. Office macros are disabled and staff aware of the risks of enabling them. Applications and browser plugins can only be installed administrators, not users. Anti-virus scans run regularly and any incomplete or positive scans are reviewed. Intrusion Detection Systems scan our network traffic for indicators of malware, using a frequently update signature set. If we are still using Windows 7 or prior we are conscious of the reduced protections in these older operating systems, and apply other layers of security to compensate.

Being prepared

Current cyber threats are monitored to help evaluate the effectiveness of our controls. We have an incident management plan and 'playbook' for several likely scenarios, and these are tested in simulations to validate their effectiveness and ensure staff are familiar with procedures. We run phishing simulations to raise staff awareness of techniques used by criminals. We have two-factor authentication on our corporate online accounts (our internet domain, cloud services, email admin, company Twitter account, etc.). Logging across all of our devices and cloud environments is centralised and monitored; we have an incident management process to address any issues identified. We validate our security controls and detection capability, and identify any gaps through regular vulnerability scanning and penetration testing of our systems.