Beazley Security Requirements for Cyber Coverage

Beazley require the following requirements/standards to be complied with in order to obtain Beazley Breach Response (BBR) Cyber terms.

4 critical security requirements*	Supplementary information to provide guidance on Beazley's requirements	Practical examples of how you or your IT services provider might implement this requirement	Further information
 You regularly back-up critical data to a "cold" or "offline" location that would be unaffected by an issue with your live environment, and you test to ensure those backups are recoverable.	• All organisations should take regular back-ups of their critical/important data and make sure that these back-ups are recent and can be restored. By doing this you can ensure your organisation can still function following the impact of a cyber attack, accidental deletion, physical damage, or theft of data. Furthermore, if you have back-ups of your data that you can quickly recover, you are much less likely to be successfully blackmailed by ransomware attackers. • The more regularly you change your files and data which are critical to your business, the more regularly you need to back-up. If you make lots of changes to critical data each day, then you should consider daily back-ups. If you have little critical data and make few changes then it is possible monthly back-ups may be regular enough.	• Many platforms have built in back-up functionality. Explore what options you already have. • Alternatively, you can explore either a third-party back-up solution (e.g. cloud backup platforms) or perform your own back-ups to external drives that you keep securely, disconnected from your live environment.	ncsc.gov.uk 
 You use multi-factor authentication (MFA) for cloud based services (such as cloud based email account access) and for all remote access to your network.	• Passwords no longer provide enough security especially for services available via the cloud (e.g. Microsoft 365, Google Workspace, etc). • Users might choose passwords that can be easily guessed and/or be susceptible to accidentally sharing their password via social engineering. • MFA is important as it makes stealing your organisation's information much harder for the average criminal.	• MFA doesn't eliminate usernames or passwords, but adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone or mobile app. MFA is built in to most cloud/internet based services so please enable it. • Alternatively, there are third-party suppliers that offer MFA utility through the use of SMS codes, unique codes and even hardware tokens.	ncsc.gov.uk 
 You do not allow remote access into your environment without a virtual private network (VPN).	• Attackers are regularly "port scanning" the entire internet for visible remote-access services such as Microsoft's Remote Desktop Protocol (RDP). Any open RDP services will be constantly probed for weaknesses so hiding your remote-access services behind a VPN will afford a good level of protection against these attacks.	• Like MFA, there are many third-party providers that offer VPN services and your own networking infrastructure (e.g. routers) may also have this functionality built in, so may just need enabling. • This requirement for a VPN is not relevant for any cloud-based services.	ncsc.gov.uk 
 You regularly (at least annually) provide cyber security awareness training, including anti-phishing, to all individuals who have access to your organisation's network or confidential/personal data.	• Your staff are at the frontline of your organisation. They are constantly exposed to electronic communications with third-parties that may leave them open to attack. Even though technical security measures like email gateways and endpoint detection and response (EDR) software may afford some level of protection, it is still essential for them to be aware of the risks. • Training will help them identify cyber risks and hopefully prevent them from impacting your organisation in the first place.	• The National Cyber Security Centre (NCSC) offers free cyber security training for staff, which has an anti-phishing module within it. There are also third-party providers that offer a range of cyber security training services, such as our partner provider, KnowBe4. Beazley cyber policyholders receive discounted rates.	ncsc.gov.uk 

*Required pre-bind

3 important security standards**	Supplementary information to provide guidance on Beazley's requirements	Practical examples of how you or your IT services provider might implement this requirement	Further information
 You implement critical patches and update systems as soon as practicable, and do not use any unsupported/end of life (EOL) software.	• All software platforms receive updates in the form of "patches". Some of these add new features to the software and/or they may be focused on fixing issues such as instability or unintended operations that can be leveraged by attackers (vulnerabilities). Since vulnerabilities are constantly being discovered and corrected, applying software vendors' patches are a routine security task that should be at the core of any organisation's basic cyber security posture.	• Most operating systems make updating/patching very straight-forward. For other software please review the relevant provider's website or other channels to ensure you keep up-to-date with critical patches and releases. Providers will typically announce when their software becomes unsupported/EOL and it is imperative that you take notice of these communications as to remediate your systems.	ncsc.gov.uk 
 You scan incoming emails for malicious attachments and/or links.	• Email remains the top form of electronic communication for most organisations and it is therefore no surprise that it is also a prime target for attackers to effectively reach your staff. Email gateways protect staff from email threats like spam, viruses and phishing attacks by filtering potentially malicious messages from reaching them in the first place.	• By placing malicious emails into quarantine or blocking those emails or their senders, an email gateway should materially reduce the number of successful compromises of user credentials and reduce the chance of exposing sensitive data. Most email platforms offer basic filtering and quarantining. Make sure this is enabled. Ideally also look to specialist mail gateway providers for solutions.	ncsc.gov.uk 
 You protect all of your devices with anti-virus, anti-malware, and/or endpoint protection software.	• Anti-virus, anti-malware and EDR are types of software that attempt to detect, block and/or remove malicious software from running on devices. Modern EDR tools also frequently integrate into a logging platform so organisations can look across their estate and see emerging patterns or trends that might signal an attacker is in their environment. • These tools are an essential part of any organisation's cyber security tools because they aim to proactively remove malicious software which tools like firewalls cannot do.	• There are many tools available in this regard, and the following link from the NCSC offers advice on the selection, configuration and use of antivirus and other security software on smartphones, tablets, laptops and desktop PCs.	ncsc.gov.uk 

**not required pre-bind, but the Retention for Breach Response Services cover under the Policy is removed if all 3 standards are implemented

beazley