Kiteworks

COMPLIANCE BRIEF

Fortifying Legal Cybersecurity With the NCSC Report and Kiteworks

Implement Robust Defenses Against Phishing, Ransomware, and Account Takeover Threats in the UK Legal Sector

The National Cyber Security Centre (NCSC), part of GCHQ and the UK's technical authority for cybersecurity, collaborated with various entities such as the NCSC-sponsored Industry 100 scheme, the Law Society, The Bar Council, the Solicitors Regulation Authority (SRA), Action Fraud (the UK's national fraud and cybercrime reporting center), and the National Crime Agency (NCA) to compile the NCSC Cyber Threat Report. This report serves to aid law firms, lawyers, and legal practices in comprehending existing cybersecurity threats and the specific targeting they face within the legal sector. It also offers practical guidance to enhance organizations' resilience against these threats. The cyber risk applies to law practices of all sizes, including sole practitioners, midsize firms, barristers' chambers, in-house legal departments, and international corporate firms, as cybercriminals show no discrimination in their attacks. Additionally, an extensive body of open-source reporting contributed to its findings. Since its inception in 2016 under the Government's National Cyber Security Strategy, the NCSC has been dedicated to making the UK the safest place for online living and working. The NCSC lists out the main types of cyberattack as phishing, business email compromise (BEC), ransomware and other malware, password attacks, and supply chain attacks. Kiteworks offers a comprehensive solution to support any UK legal business in following the advice laid out in the report. Here's how:

Protect Against Ransomware via Up-to-Date and Supported Software and Built-in Antivirus

The report identifies recommendations to defend against ransomware within a multilayered approach. It is recommended that organizations keep software, and especially operating systems, up to date and have confidence in the provenance of software and ensure that it is suitably supported, including with security patches. Kiteworks provides quarterly software updates and intermediate security, and bug fix roll-ups help with one-click updates to be seamless and quick for businesses. Additionally, Kiteworks development processes regularly check for vulnerabilities and updates for open-source software used in the system. Regular penetration testing and both black box and white box bounty programs are designed to find any system vulnerabilities before the bad actors do. Either way that a vulnerability is discovered, Kiteworks developers rapidly produce a patch and deliver it to customers online so they can apply it with a one-click update. Kiteworks also makes offline patches available for customers whose systems are not on the internet.

Solution Highlights

- **Embedded antivirus**
- **Rapid security updates**
- **Multi-factor authentication**
- **Encrypted communication channels**
- **Robust access controls**

It is also recommended that organizations use antivirus software to detect and isolate infected machines and to scan backups to avoid reinfection, to carefully control what software and applications are allowed into the firm, and to implement strict controls over any means of remote access to the system. The Kiteworks embedded antivirus scanner scans for malware and ransomware during both upload and download to avoid reinfection and prevent the spread within an organization. Kiteworks also integrates with existing data loss prevention, advanced threat prevention, and security information and event management systems to provide additional layers of defense against ransomware. Additionally, Kiteworks servers do not allow the installation of any software, severely limiting what is allowed into a firm. Finally, the Kiteworks system provides remote system access to support personnel for maintenance and support purposes and supports secure, compliant remote access to corporate repositories, such as SharePoint and Windows file shares, as well as the Kiteworks internal repository, further supporting protective controls over remote access to a system.

Secure Your Firm From Phishing by Blocking Phishing From Incoming Emails, Using Anti-spoofing Controls, and Having Well-configured Devices

The report also lays out recommendations to defend against phishing in a few different ways. It is recommended that organizations make it difficult for attackers to reach users by employing anti-spoofing controls DMARC, SPF, and DKIM as well as filtering and blocking incoming phishing emails. Because Kiteworks lays a private email system over your organization's email system, phishing attacks won't have access to your employees since only invited external parties are able to send email to them, effectively blocking incoming phishing emails. Kiteworks supports the report recommended anti-spoofing standards DMARC, SPF, and DKIM, which can be configured through the Domain Name System Server. The report also recommends having well-configured devices and good endpoint defenses to stop malware installation. Kiteworks servers provide endpoint protection to stop malware installation, as they do not allow installation or alteration of software and automatically send security alerts when attempts are made.

Control Business Email Compromise Risk With Strong Passwords and MFA

The report identifies recommendations to defend against business email compromise (BEC) in multiple steps. It is recommended that organizations implement SPF, DKIM, and DMARC email protection for all domains (even if they are not used for email) and ensure that strong and unique passwords are used for email accounts, and that they're additionally protected by multi-factor authentication (MFA). MFA should be enabled, where possible, for all critical business systems. Kiteworks supports the report recommended anti-spoofing standards DMARC, SPF, and DKIM, and supports MFA and grants administrators the ability to set policies for complex password baselines (character, numeric, and special character minimums, as well as uppercase and lowercase alphabet minimums), password expiration timelines, and password history.

Diminish Password Attacks With Strong Passwords, Least Privilege, MFA, and Password Controls

The report identifies recommendations to defend against password attacks by making it hard for criminals to pretend they are legitimate while at the same time keeping it as simple as possible for the legitimate users to access what they need. It is recommended that organizations ensure that staff do not use the same credentials for logging into their work systems as they use for other services, all accounts are protected using strong passwords, when staff forget passwords to make sure they can reset their own passwords easily, restricting users' account permissions and data access to only those that are needed, implementing MFA (or other types of authentication) for all accounts, and changing all default passwords before devices are distributed to staff.

Kiteworks allows administrators to set policies for complex password baselines (character, numeric, and special character minimums, as well as uppercase and lowercase alphabet minimums) and password history to reduce risk that staff are not reusing credentials. Kiteworks supports MFA on all user accounts via RADIUS protocol, PIV/CAC cards, the Kiteworks native email-based OTP and SMS-based OTP as well as time-based OTP. In offering these features, Kiteworks supports MFA and administrators can set policies for complex password baselines, password expiration timelines, and password history. This protects against exploits when a single factor, such as a user credential, is known by the attacker. Additionally, users can easily reset passwords by clicking the login page link and following the password reset link via email.

As administrators have the ability to set up different roles in the Kiteworks system, which are used to define the access and permissions that a user has, access can be removed immediately as well. This feature provides a way to map real-world separation of duties within an organization to the exact set of permissions needed to fulfil the role; this role-based access control is a key requirement in compliance regulations and provides least-privilege default separation of duties out of the box with the possibility to customize exactly for the organization's compliance needs. In addition, Kiteworks offers an easy-to-use setting for administrators to enable, which can force new users to change their password immediately when they log on for the first time, ensuring that default passwords are changed, thus minimizing available avenues for gaining unauthorized access to the system.

The UK National Cyber Security Centre's report provides guidance for law firms to enhance resilience against major threats like phishing, ransomware, and password attacks. Kiteworks delivers comprehensive solutions to help legal businesses follow this advice and strengthen their security posture. Features like embedded antivirus, rapid security updates, multi-factor authentication, anti-spoofing controls, encrypted communication channels, and robust access controls and permissions management allow firms to protect against malware, secure user accounts, control access, and block phishing attempts. Specifically, Kiteworks' private email system blocks incoming phishing, integrated antivirus scans for malware, rapid patch deployment counters ransomware risks, multi-factor authentication secures logins, and role-based access controls enable least-privilege principles. With layered defenses like these, Kiteworks equips legal practices of all sizes, from small firms to large corporate legal departments, with comprehensive solutions to create a more secure IT environment resilient against modern cyber threats.