beazley

Full Spectrum Cyber

Estate Agency Risks

Full Spectrum Cyber: *Estate Agency Risks*

The Key Exposures Facing Estate Agency Risks

Attractive to Cyber Criminals

The estate agency industry is an attractive target for cyber criminals due to the high frequency of transactions, market interconnectivity and regularity of information sharing. These risks are particularly ripe for eCrime attacks such as social engineering, funds transfer fraud, or fraudulent instruction.

Operational Disruptions

Increased reliance on technology leaves the estate agency industry vulnerable to operational disruptions that not only cause significant revenue loss but can have a negative impact on reputation. A system outage may disrupt closings, listings, mortgage processing and title work. This exposure is amplified due to the time sensitive nature of estate agency transactions.

Sensitive Data and Financial Information Stored and Shared Online

Estate agency operations involve the safeguarding and managing of customer financial details in electronic form. If the proper protections are not in place, cyber criminals can access this data online for theft, ransom and financial gain.

How Our Specialist Coverages Respond To The Threats

01 **Specialised Subsidiary Coverage*:** broad scope for Real Estate Investment Trusts (REITs), Joint Ventures (JVs) and other Single Purpose Vehicles or Entities (SPVs/SPEs) established during estate agency transactions.

02 **eCrime:** £/€250,000 sublimit available for Fraudulent Instructions, Funds Transfer Fraud, Telephone Fraud and Invoice Manipulation Coverage.

03 **Artificial Intelligence/Deep Fake Coverage:** enhanced Fraudulent Instruction endorsement clarifies that the policy will cover Fraudulent Instructions that result from some of the innovative ways that criminals are employing AI including deep fakes.

04 **Missed Bid Loss Coverage for Contractors/Developers:** coverage available if new business proposals can't be submitted due to a security breach that interrupts operations.

05 **Broad definition of Dependent Business Interruption:** as a third-party entity that provides necessary products and services to the Insured Organisation pursuant to a written contract.

06 **Money Custodian Coverage:** money custodians are entities responsible for safeguarding and managing financial assets for their customers. Coverage is offered for direct financial loss sustained "solely by the Insured Organisation".

*Available for clients with revenue £35m>

beazley

Reducing risk- Cybersecurity information for the Estate Agency Industry

01 Multi-Factor Authentication: Implement two-factor authentication for all remote access, web-based email access, and for administrator access to key resources. Provide remote access only through secure channels and require strong passwords.

02 Email Security: Properly configuring junk filters, investing in antivirus protection, and adding multi-factor authentication can help employees avoid business email compromises, fraudulent instruction losses, and other cyber claims.

03 Incident Response Planning: Create a plan that is stress tested regularly. Improve upon the issues raised during testing to improve response times to a cyber incident. Testing the plan will help minimise damage by creating the appropriate downtime procedures for the business.

04 Staff Cybersecurity Training: Conduct regular phishing testing for all users to reduce human error. Many cyber incidents happen because someone clicked on something which they shouldn't have.

05 Penetration Testing: Engage a security firm to evaluate your attack surface and assess vulnerabilities: report results to the executive team and recommend future protective actions. Penetration testing can drive down the costs of an incident significantly.

06 Endpoint Protection (EPP) solution and Endpoint Detection and Response (EDR): If your organisation has multiple endpoints, deploy an EPP/EDR solution across enterprise assets, to detect and block common viruses with advanced capabilities of active monitoring.

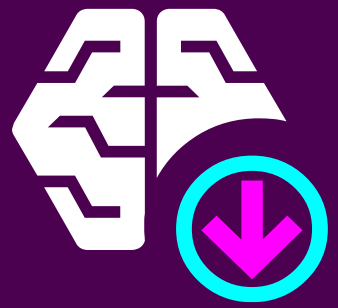
07 Backups: Develop and test backup and recovery plans; keep copies of sensitive or proprietary data in a separate and secure location. Test back-ups regularly to ensure both the technology, and the people, can function during a crisis.

08 Antivirus and Patching: Maintain updated antivirus software and configurations. Enforce a patch management process to address ongoing security updates and defend against critical vulnerabilities.

beazley

Responsive Cyber

How Beazley Security helped estate agency clients get back in the game.



An estate agency brokerage fell victim to a ransomware attack. The policyholder contacted their Beazley Cyber Service Manager who quickly arranged for services from privacy counsel, forensic experts and a ransom negotiator. The payment was negotiated down to £200,000 from the initial demand of £450,000. The **forensic investigation** determined that the threat actor exfiltrated files containing PII from over 2,000 of the policyholder's clients. Privacy counsel assisted with notification services after determining that notification requirements were triggered. Despite having recent backups, the event caused a significant disruption to the policyholder's operations resulting in a reduction in the number of listings. Beazley paid Cyber **Business Interruption** losses and income loss from missed bids in the amount of £275,000 following a review of the policyholder's Proof of Loss submission.

Business Interruption
Missed Bid Coverage

A commercial general contractor reported a widespread encryption event to Beazley. A Cyber Services Manager promptly responded, aligning privacy counsel and digital forensics. Despite the findings that backups were encrypted, the Policyholder did not wish to negotiate, and Cyber Services quickly connected with **data recovery** vendors to assist the internal team in the rebuild. Impacted systems included payroll processing and privacy counsel's analysis determined that exfiltrated data included the National Insurance numbers of more than 400 current and prior employees, resulting in **notification** and **credit monitoring** costs covered under Breach Response. Coverage was further granted under the Policy for significant **Business Interruption** and Data Recovery Expenses.

Data Recovery
Notification Costs

Through RDP (remote desktop protocol), a threat actor was able to infiltrate an estate agency's environment and deploy a crippling ransomware attack. Within hours, a Beazley Cyber Services Manager connected the Policyholder to expert legal, forensic, and negotiation providers. Successful **ransom negotiations** quickly reduced the demand from £350,000 to £280,000. With Beazley's speedy consent, the Policyholder paid the ransom and began **recovery** efforts. Privacy counsel analysed the forensic findings and assisted the organisation in **notifying** hundreds of individuals, all of which was paid under the BBR Policy's separate Breach Response Coverage (outside the limit). An additional £500,000 was covered under the limit for **Business Interruption** income loss and data recovery efforts. Despite significant losses, the remainder of the Policyholder's limit was preserved for use in the event of any future claim during the policy period.

Breach Response

Specialised Ransomware Negotiation Services

beazley

Adaptive Cyber

Our coverage evolution helps your estate agent clients manage risks as they evolve.

Key coverages include:

- **Breach response:** Notifications, Forensics, Public Relations Costs, Legal, Crisis Management
- **First party:** Cyber Extortion, Business Interruption, Dependent Business Interruption, Data Recovery
- **Third party:** Data and Network Liability, Regulatory Defense and Penalties, Payment Card Liability
- **eCrime:** Fraudulent Instruction, Funds Transfer Fraud, Telephone Fraud

Click here for our cyber action plan

Estate Agency Appetite