Resources

Is your industry at risk from cyber crime?

QMTCOMMERCIAL
INSURANCE BROKERS

Retail & wholesale

The risk

The rise in online shopping makes customer data vulnerable. Prioritising ease over security, like multi-factor authentication, risks data breaches. Criminals can exploit stolen info to access accounts and make unauthorised purchases.

The impact

Failure to meet payment card industry security standards | Temporary disruption in card payment processing | Damage to reputation | Loss of customers

Manufacturing & industry

The risk

The sector's dependence on rapidly advancing technology exposes it to ongoing cyber threats. This can lead to the theft of valuable intellectual property and significant disruptions to operations if system software is compromised.

The impact

Production delays may lead to possible contractual penalties | Production interruptions leading to decreased revenue | Risk of losing valuable intellectual assets | Damage to reputation

Professional & consultancy

The risk

Professional services face significant risks from cyber attacks due to their management of sensitive data and client funds. Recently, there has been an increase in cybercriminals targeting law firms' property teams, employing tactics like social engineering and compromised emails to misappropriate funds.

The impact

Data breaches | Loss of customer funds | Damage to reputation | Loss of customers

Business services

The risk

Business services increasingly depend on technology to operate efficiently. Whether it's managing customer data or offering essential outsourced services, the reliance on remote access to client systems can expose vulnerabilities to cyber threats. A single security breach can impact multiple clients.

The impact

Contractual penalties for disclosure of sensitive business data | Business disruptions to services | Contracts not renewed due to quality concerns | Service providers can serve as entry points for cybercriminals to infiltrate third-party systems, increasing their vulnerability

Construction & building

The risk

Construction firms manage confidential information, such as staff records, tenders, property proposals, plans and client data. Unauthorised access can lead to financial losses. The use of software by multiple users, including architects, contractors and planners, increases the number of access points and vulnerabilities.

The impact

The frequent transfer of funds along the supply chain increases the risk of social engineering or fraud | A breach of bid data can result in losing a competitive edge | Delays in work may lead to contractual penalties | Reputational harm could result in loss of contracts

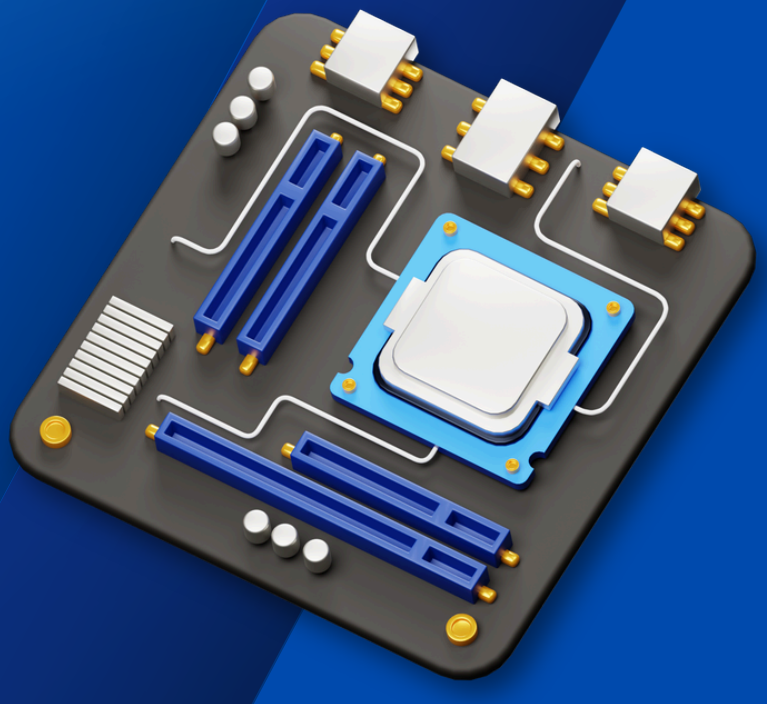
Owners & landlords

The risk

Online exchanges of personal information, contracts, and payments make agents, landlords and tenants prime targets. Criminals can commit identity theft, forge documents, and engage in property or mortgage fraud. Financial fraud is rampant due to large online money transfers.

The impact

Risks of social engineering fraud from frequent large transactions | Harm to company reputation | Data breaches may result in regulatory scrutiny and legal consequences



Technology & IT

The risk

The sector's reliance on digital solutions increases its exposure to cyber threats, such as device hacking and ransomware, which can lead to significant financial losses.

The impact

Breaches in customer data may attract regulatory scrutiny | Production stoppages could incur contractual fines | Risk of losing intellectual property | Potential harm to reputation

Motor & vehicles

The risk

Motor traders manage extensive personal data from their clients, particularly when financial arrangements are involved in sales. Cybercriminals exploit this by selling stolen data, locking computer files for ransom, or executing scams to siphon funds from bank accounts.

The impact

A data breach may prompt regulatory action |
Social engineering scams can cause major financial setbacks

Charities & non-profit

The risk

This sector encompasses a range of organisations, from faith groups to healthcare providers and retail. These entities depend on volunteers and often lack centralised IT infrastructure. Charities face vulnerabilities due to the sensitive data they manage, including information on donors, beneficiaries, volunteers and staff.

The impact

The impact of cybercrime on charity funds is significant, leading to donor hesitation | Data breaches are being exploited through social engineering tactics

Education & schools

The risk

Educational institutions are dependent on technology for tasks ranging from tracking performance to facilitating staff-student collaboration. This involves handling sensitive information. Students connecting personal devices can unintentionally introduce malware into the network. Additionally, lapses in protocol adherence by staff may result in data breaches.

The impact

Data breach and legal action risks increase with the volume of student records | The timing of events, e.g. exam results, can influence outcomes | Social engineering tactics, e.g. targeting school fees, pose a serious threat | Negative publicity can affect enrolment

Health & public services

The risk

This sector is particularly vulnerable to threats. They handle sensitive data and operate open systems that can be an easy target. Suppliers with poor cybersecurity but access to healthcare systems are a gateway for hackers to gain patient data. Breaches can lead to significant fines and penalties.

The impact

Release of patient data causes harm | Healthcare data is a valuable target on the dark web | Regulatory scrutiny is high due to the sensitivity of the data | Inaccessibility of files can have severe human impacts e.g. in hospital emergencies | Breaches expose healthcare providers to fines and legal penalties

Arts & culture

The risk

In this industry, staying at the forefront of technological advancements is crucial. From implementing recommendation and review features to utilising booking apps, live chat and loyalty programs, companies must also prioritise the secure and efficient management of customer data.

The impact

Experiencing business disruptions and increased liability due to decreased contributions from donors | Facing media-related risks, including defamation and intellectual property issues | Encountering challenges with credit card data security and PCI compliance | Revenue affected by booking limitations

Need help with your insurance?

Our team of friendly advisors are here to support you, whether you need a quote or have a query.

01227 285 540
HEAD OFFICE

01233 222 562
ASHFORD BRANCH

Find more tips and resources:
www.qmtcommercial.co.uk/hub