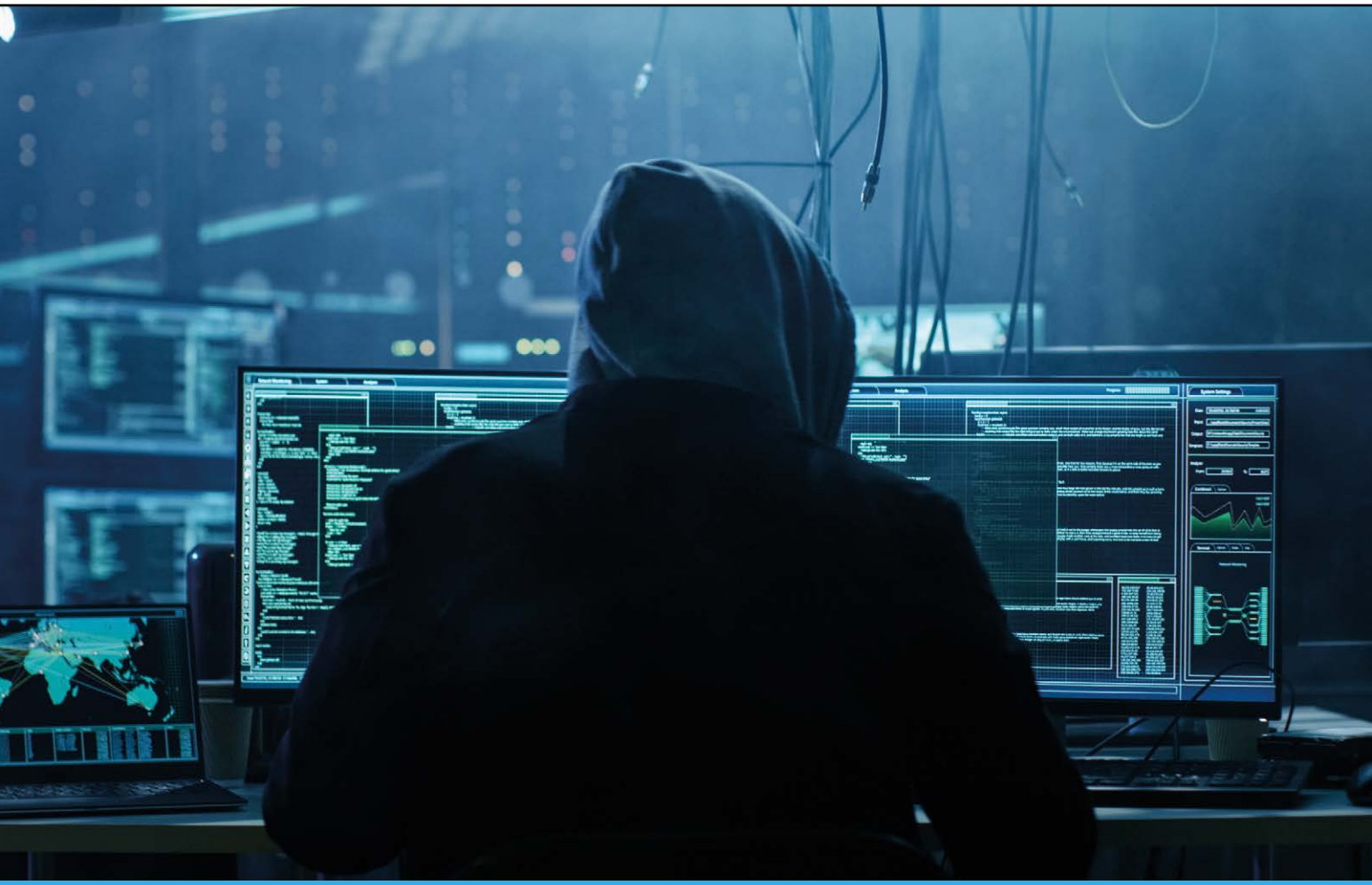
Sponsored by

QBE

CIR
CONTINUITY INSURANCE & RISK



Cyber crime: Are you ready? *Erica Kofie, head of cyber proposition, QBE Europe, outlines the importance of understanding the threat of cyber crime, and of preparing the appropriate responses to protect your business*

Putting your best foot forward *Against a backdrop of rising attacks, Erica Kofie, head of cyber proposition, QBE Europe, outlines five areas for businesses to focus on when making their organisation more attractive to cyber insurers*

Cyber risk and insurance

QBE

Sponsored by

Cyber crime: are you ready?

Erica Kofie, head of cyber proposition, QBE Europe, outlines the importance of understanding the threat of cyber crime, and of preparing the appropriate responses to protect your business

As our reliance on technology, social media, and even artificial intelligence increases, the digital tools and platforms we use in business are essential to maintain market advantage. But as technology continues to develop, so do the methods of cyber criminals, intent on finding more sophisticated routes to exploit weaknesses and launch attacks.

To put the scale of cyber incidents into context, in 2022 a survey showed the UK experienced the highest cyber crime density in the world. That year, there were 18 ransomware incidents that required a nationally coordinated response. And 39 per cent of UK businesses identified cyber attack incidents, with over a third of businesses recording the frequency of attempted attacks as weekly.

Globally, 33 billion electronic records are expected to be stolen in 2023 and cyber damage costs are predicted to increase by 15 per cent each year to an estimated £8.4 trillion by 2025.

With statistics as staggering as these, it is no surprise that cyber security has become a number one priority for businesses of all size. It is essential for organisations to protect their business operations, assets and customers against the constant threat of cyber crime.

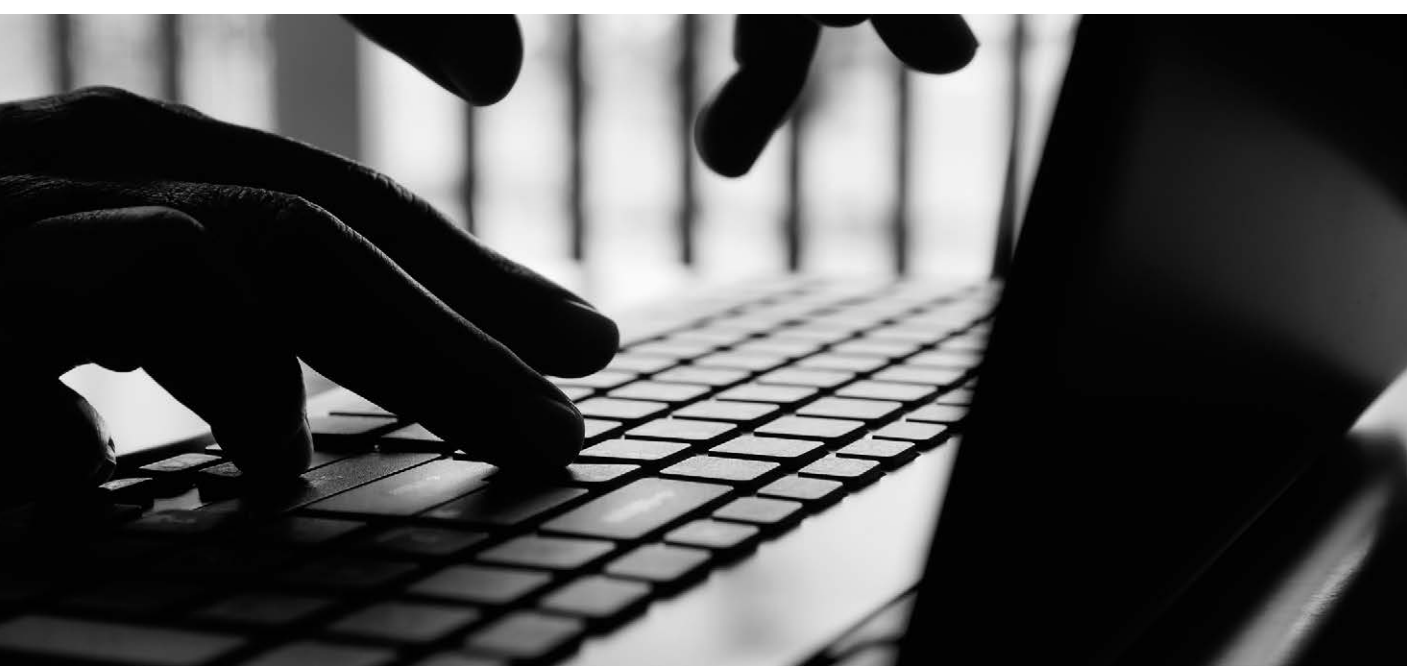
Whether cyber security incidents result from system failure, human error, or an attack by cyber criminals, a breach could cripple your business with potential outcomes including lost revenue, business interruption, damaged reputation, large-scale costs and legal liabilities.

Are you ready for a cyber event?

Ensuring you have defences in place via technical controls and IT security is the first step to guarding against cyber hackers.

The main types of cyber crime include virus or malicious software infection; phishing; denial of service attacks; unauthorised network access; and confidential data theft. Often the main causes of a breach will be due to a malicious or criminal attack, a system glitch or human error.

Internal cyber security should provide a foundation of measures to protect the technology, systems and



information used in your business operations. Five key management controls to consider include:

- Boundary firewalls and internet gateways – ensuring devices designed to prevent unauthorised access to or from private networks are effective.
- Secure configuration – ensuring that systems are configured in the most secure way.
- Access control – ensuring appropriate system access for people.
- Malware protection – ensuring that virus and malware protection is installed and up to date.
- Patch management – ensuring the latest supported version of applications is used and all necessary patches supplied by the vendor have been applied.

Third parties, contracts risk transfer

Considering that even 'basic' IT securities can form a complex model, it's little wonder that organisations that do not have a dedicated IT department outsource their cyber security to an expert external provider, or a managed service provider.

These third-party firms can cover the essentials before also offering services such as email authentication services, domain-based message authentication, reporting and conformance (DMARC), cloud security and threat intelligence services (such as dark web monitoring) to proactively detect and mitigate risks.

Statistics show that outsourcing IT is now the favoured approach by:

36 per cent of micro businesses (<10 employees)
57 per cent of small businesses (<50 employees)
65 per cent of medium organisations (51-250 employees)
72 per cent of large organisations (250+ employees)

As with all third parties that process data, there is still a risk that external or insider criminals could target them, potentially winning access to multiple business networks as a result.

Because service providers are part of your supply chain, you are within your rights to clarify exactly what the service provider is offering. Assessing the capabilities of the supplier is critical – once the contract is signed (and indeed, there needs to be one for your protection) you're stuck with each other.

Remember: while business owners can transfer part of the risk, as the party contracting out services to a third party, you remain accountable for the consequences of IT and security failures. It is therefore crucial that you ensure that third-party service providers can protect your business and that all parties are adhering to the same set of cyber security protocols.

Securing your supply chain

Risks are intensified where businesses are more integrated with supplier networks: you are only as strong as your weakest link.

Supplier assessments are usually conducted using a tailored supplier questionnaire. These questions can form part of the procurement phase, when trying to identify a good service provider – or if your business already contracts out to a provider, to check they are doing what they say they are.

Asking the right questions will determine which provider is best placed to support your cyber security: Do they understand your business needs, risk profile and strategic direction? What cyber security protocols do they have in place? Will they effectively support you in the event of a breach, IT incident or cyber attack?

Many businesses select based on price rather than ability. Unfortunately, in failing to assess the supplier's capability to deliver a secure service, organisations risk significantly higher financial losses than the annual contract savings.

Even with robust preparation unexpected incidents can still arise, especially in a supply chain that includes vulnerabilities via third parties. This is where the act of preparing for multiple scenarios, rather than simply being reactive, will help organisations develop appropriate responses.

A close working relationship with your insurer before and during a crisis will help ensure that everyone is working together. Steps for preparation can include:

Understand: Mapping and monitoring digital processes in your supply chain can prevent issues before they arise and highlight areas in need of additional security.

Prepare: Scenario planning and preparing playbooks of responses will help prepare for cyber attempts and/or events.

Train: Training teams to respond to crisis situations can prevent or lessen the impact of cyber breaches on the business.

Involve: Involving your supply chain partners in planning and responses is essential – and your insurer should be part of this discussion.

Data breaches

Major breaches are happening all the time, all around the world. One of the biggest concerns is knowing what data you have, and where it is. Securing or

removing connections between data sets is important so that in the event of a breach, if hackers find one window, they don't gain access to everything.

Organisations that carry lots of data can be more of a target, particularly when that information is of a sensitive nature or has financial value, such as credit card details or health insurance records. Equally, businesses that trade online are more prone to attack as they have financial data and a higher web presence.

Data is often stored in the cloud and good cyber security requires the user to take basic steps to ensure the system remains safe and is not compromised. Cloud security questions should include:

- Do you use a strong password to access the system?
- Do you have multifactor authentication in place? This requires the user to have two pieces of information to access the system, so that if one is compromised (eg. the password is guessed), a second step is required (eg. a code sent to a mobile phone or email address, biometric recognition) before access is provided.
- Have you considered both access and authorisations within the system? Who needs access to what? Ensure that access to the ' crown jewels' of your business is restricted.
- Is there a process to administer user access, ensure removal of all leavers from the system or the modification of access if individuals move role?

And if you choose to outsource this service, it is important to assess the security provided and if you choose to end a service, ask providers to confirm the deletion of data.

Incident response plans

Having a tested incident response plan in place has proven to mitigate the impact of a data breach or cyber attack. Planning and preparation are key: being prepared for various scenarios to happen, alongside understanding where your data is and how it can be accessed and by whom.

A good incident response plan will enable you to follow the simple steps of:

- Identification – how did this happen?
- Containment – is it ongoing?
- Eradication – is it happening anywhere else?
- Recovery – is the data in a working state again?

Incident response plans prepare you to respond efficiently and effectively when a breach occurs, whilst also standing up to regulatory scrutiny. Business continuity planning can also support with developing, implementing and/or testing responses.

The crucial part after this is looking at the lessons learnt from the experience and incorporating them into the incident response plan for next time.

For those who need it, compliance software is available from various providers to help manage and mitigate against a range of potential cyber risks via assessments and recommendations. Risk modules include fraud, information security and meeting GDPR responsibilities, in addition to related business risk areas such as health and safety, physical security and HR responsibilities.

Governance and culture

Responding to crisis situations and putting incident responses into action is more than the sum of the information gathered and plans made in advance. Largely, success will be down to how your teams view risk and deal with uncertainty. Building a robust risk culture, with high levels of risk intelligence at all levels will help mitigate the impact of a breach.

Changing staff culture should happen both from the ground up and the top down. While board members perhaps haven't traditionally concerned themselves with IT issues, the more companies realise that their reputation is at stake the more likely their boards are to buy into it. Top-level cyber risk reviews can help generate strategies, promote support and increase buy-in at board level.

As Luke Dembosky, co-chair of the Presidential Task Force on Cyber security, puts it: "It is more important than ever that senior executives and boards of directors engage directly in ensuring their organisations are managing cyber risks effectively.

"The days of leaving that enormous responsibility to the IT team or to privacy compliance to handle are long over, as these are clearly whole company risks to operations, data and brands."

A recent report from the International Bar Association draws on UK sources amongst others to highlight key governance practices for senior managers and boards of directors to protect their organisations against cyber attacks. The report, *Global Perspectives on Protecting against Cyber Risks: Best Governance Practices for Senior Executives and Boards of Directors*, provides insights into both cyber threats and recommendations to strengthen cyber risk governance.

The full report is available at www.ibanet.org.

Training and testing

Understanding cyber risk and

staying compliant is a company-wide endeavour. As human error is documented as one of the leading causes of data breaches, it stands to reason that organisations must highlight the risks and ramifications to their staff – and train them accordingly.

Frequent risk awareness training can drive positive change in both individual and group behaviours, building a responsible risk culture within the workplace. Employers can utilise a range of resources (videos, games, audio stories, webinars, posters and training) on cyber security, data protection, crisis management and risk management to raise security awareness in employees and stakeholders.

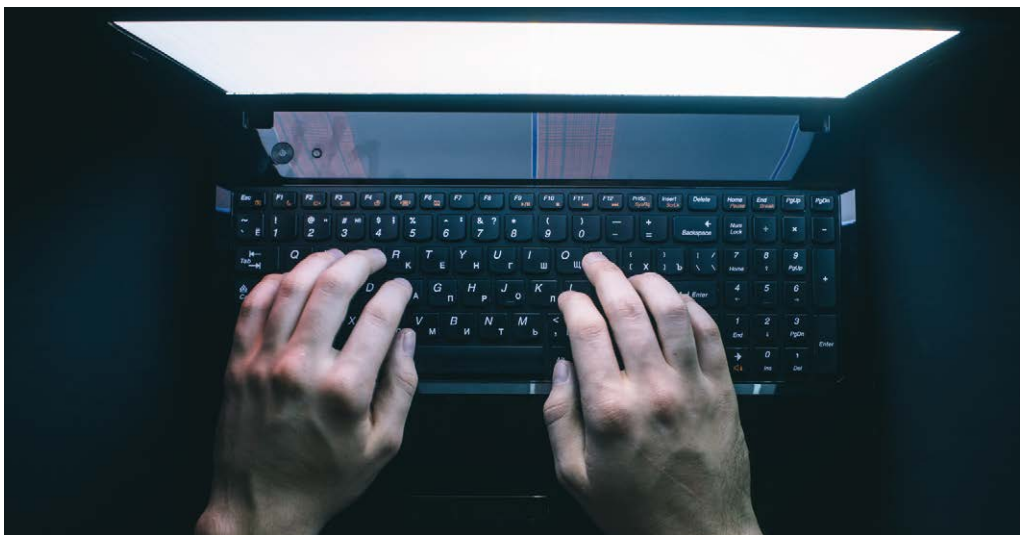
Businesses may also want to consider scenario-based training workshops, courses or tests tailored to your needs. Cyber response testing, tailored breach simulation or phishing exercises highlight the importance of testing response and recovery plans on a regular basis.

Launched by the Bank of England in 2014, CBEST is an approved framework for UK financial services organisations to voluntarily test their cyber and IT defences using AI and attack simulations. The National Cyber Security Centre has launched a specialist certification around cyber exercises for corporates testing their incident response plans using the CBEST framework.

Further details of CBEST-approved cyber threat intelligence service suppliers and penetration testing companies can be found on the CREST website, www.crest-approved.org

Risk management and specialist insurance cover

Even after you have understood cyber risk and built in protections to reduce it where possible, there will always be some exposure. Appropriate risk management can minimise cyber exposure and build resilience by implementing clear strategies and communication plans, alongside a robust cyber risk culture. In addition, cyber insurance protection should be integrated into your overall risk management strategy.



Every business should have cyber insurance. Ensuring that you secure the right coverage is a collaborative effort; you should ask advice from your broker and discuss cover with your insurer.

Further information

The QBE Cyber Risk Profiler can help you understand your risk culture and the actions you can take to improve it. A free self-assessment is available via QRisk, our risk management system, covering everything from leadership and cultural considerations to staff, client and supplier activities that might be impacted by cyber risks.

The QBE Risk Culture Profiling Tool is another tool that can help you analyse and understand the security risks your organisation faces alongside a benchmark against which to measure your processes and risk controls, to ensure appropriate protection.

Complete an online assessment and receive a report and recommendations tailored to your business.

For more information visit: www.qbeeurope.com/risk-solutions/risk-culture

QBE Cyber Insurance

Our underwriters will work closely with you to create cover that suits your specific needs. We take the time to understand your business inside out, so we can provide bespoke cover that protects you against current and emerging cyber risks.

If you have a cyber insurance policy with QBE, you have free access to our cyber risk management portal – the eRiskHub – including key incident response information, cyber news, insights, tools and training videos. Access details are in your cyber insurance policy document.

Erica Kofie is head of cyber proposition at QBE Europe

Putting your best foot forward

Against a backdrop of rising attacks, Erica Kofie, head of cyber proposition, QBE Europe, outlines five areas for businesses to focus on when making their organisation more attractive to cyber insurers

Cyber insurance cover is essential for businesses, but not all firms can access the policies they want. Here, we highlight five key areas in which businesses can improve their security profile to access appropriate cyber coverage and build resilience.

Everyone understands what a fire or a flood looks like, and the impact it could have on business operations – but not everybody understands what a cyber event looks like, or what follows.

As part of our ongoing dialogue with customers, we focus on 'being ready', and part of this includes sharing appropriate information on failed attacks, which protections worked, the vulnerabilities that have allowed cyber breaches to happen, and ways to improve security.

A greater level of sharing information both ways helps insurers better understand their customer's business, so we can assess and advise on risk in the most effective way.

It is crucial for businesses to take stock of their cyber security, not only to address any gaps that might let criminals in, but also to meet the criteria required to access full levels of insurance. There are five key areas businesses can focus on.

General IT security

Are you sure all your systems are always kept up to date with necessary security updates?

This doesn't mean simply relying on your anti-virus being up to date. It's important to understand the process for managing software vulnerabilities and updates, even if an external IT provider delivers the service.

Do you have multifactor authentication in place on all remote connections and admin accounts?

This requires the user to have two pieces of information to access the system, so that if one is compromised (eg. the password is guessed), a second step is required (eg. a code

sent to a mobile phone or email address, biometric recognition) before access is provided.

Do you ensure your businesses or employees are not using unsupported systems, and where these are unavoidable, are you sure they are isolated from the internet and the rest of your network?

As new versions of software and programs are released manufacturers stop providing security updates for their older versions creating unsupported systems. These are obviously therefore easy targets for hackers and so extra care must be taken if you plan to still use them.

Do you know the difference between vulnerability scanning and pen testing and how often do you do either?

Simply put, vulnerability testing is designed to scan and evaluate your IT systems for weaknesses. Pen testing is a simulated cyber -attack against those weakness, designed to show how serious the situation could become.

Employees

Your employees can be your weakest link when it comes to cyber security and it is important to have an education programme in place to remind employees about the risks, how to spot suspicious activity and what to do (and what not do).

Sporadic phishing simulations are also recommended to highlight areas of your workforce you might need to spend more time educating about the risks.

Business continuity

Business continuity should be a key focus for all companies, with clearly laid out processes and priorities to help protect your data, reputation, revenue – and if needed, your recovery. Key questions to consider include:

- Do you carry out regular offline backups of critical data?
- Do you segregate IT (information technology) from OT (operational technology, such as machinery) by using for example firewalls or air gapping?
- Do you isolate different locations?
- Do you have a business continuity and/or disaster recovery plan in case of a network outage?
- Have you practiced the application
- of these plans?

Personal sata

It is a myth that small and medium-sized businesses are less at risk. In fact, there's a trend towards targeting those with less robust measures in place and using them to gain access to larger companies.

Encrypting data isn't enough to prevent fraud or misuse. Cyber security encompasses more than just hacking and phishing, and data protection covers everything from email marketing to hanging on to files longer than is necessary.

Business should assess their data protection measures in the following areas:

- How careful are you with the data you hold?
- Is sensitive data adequately secured with appropriate encryption?
- Are you only holding the data you need and disposing of non-essential data properly?
- Do you limit the number of employees with access to sensitive data?

Regulation

Is your business required to be PCI-DSS compliant? Businesses that hold, use, or transmit cardholder data must hold this accreditation.

Are you aware of the privacy and security regulations your business is required to adhere to?

The UK Data Protection Act is not the only regulation most businesses need to adhere to in the event of a cyber incident. There are many specific industry regulations that a lso govern the security of data and IT systems.

Cyber insurance underwriters will take these five focus areas into consideration when deciding whether to offer coverage and at what premium.

Even if your company is not currently looking for cyber cover, taking these security precautions seriously makes business sense, no matter the industry, or size of company.

Erica Kofie is head of cyber proposition at QBE Europe

QBE. Prepared.

How can businesses build resilience in a challenging operating environment?

Visit QBEeurope.com/sector-resilience to find out.

QBE
Business insurance