ZURICH®
Resilience Solutions

Beyond Compliance: Mastering cyber resilience in a changing world

In this guide...

- **Discover** the 3 reasons for strengthening cyber resilience.
- **Explore** the limitations of compliance-based approaches and discover strategies to strengthen your cyber resilience.
- **Learn** the advantages of a risk-based approach.
- **Find out** how to start your journey with us.

3 reasons for a risk-based approach to cyber resilience

Navigating the cyberthreat horizon can be difficult. Resources are limited and it's hard to know what to prioritise. Often organisations rely on compliance to cyber regulations and certifications to inform their prioritisation.

However, assuming cyber compliance will protect your business can be misleading, because compliance controls may not be tailored to your unique exposures. So a risk-based approach to cyber resilience is more effective for following reasons:

1. Cyber threats are changing.
2. Industry regulations are increasing.
3. Building resilience to support insurability.

1 Cyber threats are changing

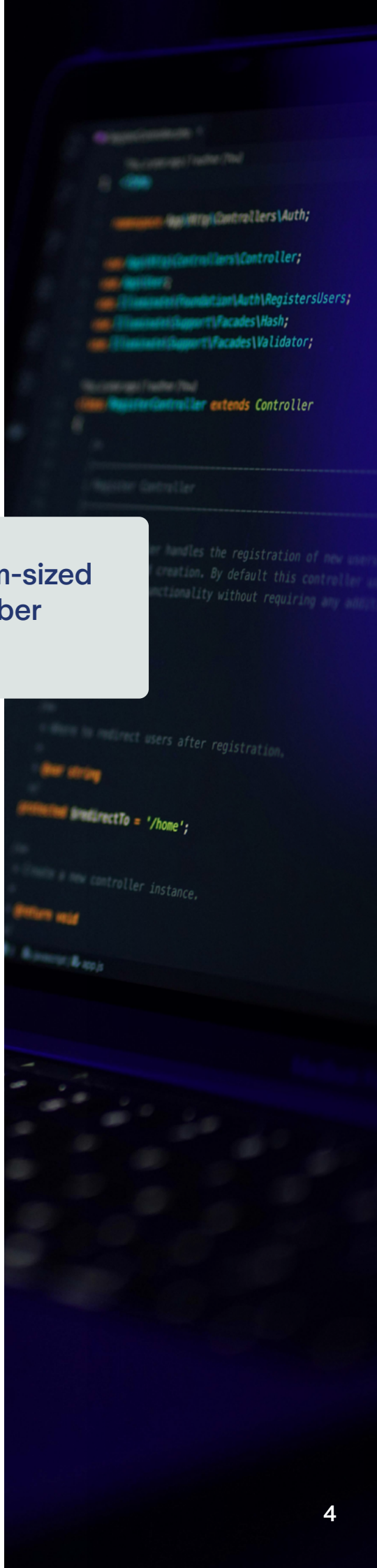
Cyber threats continue to become more sophisticated, with businesses being targeted from different angles.

In the last 12 months, 70% of medium-sized businesses in the UK identified a cyber breach or attack[1].

Are your cyber security measures keeping pace with the growing attack surface?

Organisations may not realise their vulnerabilities. Today's controls and processes may not protect from tomorrow's threats.

Organisations may also underestimate the impact that cyber attacks can have. Operational disruption, reputational damage, fines from the regulator — the fallout can be far-reaching, expensive and the impact can last for months or even years.



1. Source: Cyber security breaches survey 2024

Here are the key factors for a risk-based approach to cybersecurity:

Ransomware

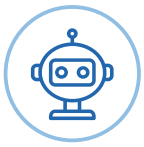
There have been attacks against critical infrastructure, healthcare institutions and large enterprises. But businesses of any size can be a target.

Connected devices

The proliferation of Internet of Things (IoT) devices and network-connected Operational Technology (OT) is creating new vulnerabilities and offering hackers an easy target.

Supply chain attacks

Cybercriminals target trusted vendors and suppliers to gain unauthorised access to networks.



AI vulnerabilities

Increased adoption of Artificial Intelligence (AI) by organisations is creating more vulnerabilities. Also, AI is being used by hackers, with phishing, malware, deepfakes being the biggest concern for approximately half of executives[2].

Against this backdrop of threats, it makes sense to move from a *reactive* cyber security strategy to a *proactive* one.

2. Source: Global Cybersecurity Outlook 2024 — World Economic Forum

Recent research shows

54%

of organisations fail to understand cyber vulnerability in their supply chain sufficiently[2].

2. Source: Global Cybersecurity Outlook 2024 — World Economic Forum

2 Industry regulations are increasing

As technology continues to evolve, governments worldwide are passing ever-more stringent cyber security laws and regulations.

Cyber resilience legislation in the UK

In the UK, the Department of Telecommunications and Information Services (DTIS) has issued a call for views for a 'Cyber Governance Code of Practice'[3]. This code would bring together the critical governance areas that directors need to take ownership of in one place. It would also formalise the government's expectations of directors for governing cyber risk.

The Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) increased the requirement for operational resilience across the financial sector within the European Union (EU).

Under DORA, from 17 January 2025[4], financial organisations must:

- Follow rules for the protection, detection, containment, recovery and repair capabilities against Information and Communications Technology-related incidents.
- Identify potential threats and vulnerabilities to their digital infrastructure, systems and services.
- Implement effective measures to mitigate these risks.

3. Source: Cyber Governance Code of Practice: call for views

4. Source: The Digital Operational Resilience Act (DORA)

Directive on measures for a high common level of cyber security across the Union (NIS2 Directive)

The NIS2 Directive[5] came into force in 2023. It expands the scope of the cyber security rules with the aim of improving the resilience and incident response capacities of organisations across the EU.

Reporting on 'material' risks in the US

The SEC (US Security and Exchange Commission) has enhanced their requirements for disclosing and managing cyber security risks[6]. This includes reporting on 'material' risks, which means organisations need a way to translate traditional risk scenarios that could cause losses into tangible, financial information.

5. Source: Shaping Europe's digital future
6. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

3 Build resilience to support insurability

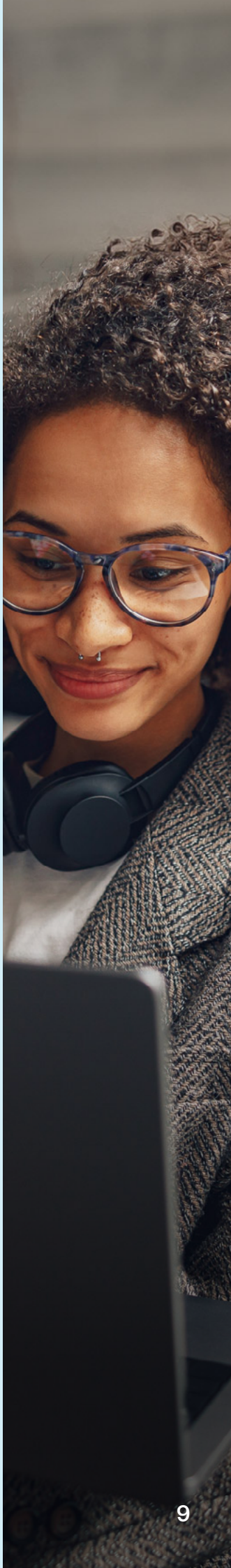
Cyber insurance offers financial protection and support in the event of cyber attacks or data breaches.

With the increasing threat of cyber attacks, more organisations are recognising the need for cyber insurance. In the Cyber Security Breaches Survey 2024, 62% of medium businesses report being insured against cyber security risks[7]. As more organisations seek cyber insurance, they will have to prove cyber resilience to insurers.

Navigating the complexities of cyber insurance

Securing cyber insurance can be an involved process. There are stringent requirements, forms to complete and security controls that need to be in place.

Organisations also need to demonstrate their dedication to understanding cyber risk at renewal. Insurers want evidence that the organisation can not only respond and recover from cyber attacks, but also anticipate new threats on the horizon and adapt.



7. Source: Cyber security breaches survey 2024

Do you have the right measures in place?

- Cyber underwriters look beyond compliance.
  For example, they also expect you to have Multi-Factor Authentication (MFA), well-tested backups and a disaster recovering strategy.
- Appropriate privileged access management controls and procedures.
- Vulnerability and patch management processes.
- Monitoring and detection tools.
  For example, SOC, SIEM, EDR.
- Incident response planning and testing.
- Evidence of a robust and regularly tested backup solution.

Our risk insights can help improve your cyber resilience and support your insurance journey.

Can you quantify your risks?

Organisations can find it a challenge to understand the potential cost of complex cyber risks. Clearer metrics can also help organisations secure the right level of insurance. But that requires the ability to calculate and report on material risk for your organisation and supply chain.

This is where Cyber Risk Quantification (CRQ) can help. CRQ is a useful technique to translate traditional risk scenarios that could cause losses, into tangible financial information.

Compliance doesn't go far enough

Cyber compliance is a necessary aspect of cyber security, but it doesn't give you a complete picture of your organisation's risk posture. In fact, it can give you a false sense of security. To effectively manage cyber risk and build resilience, it helps to move beyond a compliance-based approach for the following reasons.

Cyber essentials has limitations

While cyber essentials addresses technical controls and basic cyber hygiene, it lacks continuous monitoring and doesn't put emphasis on people and process.

Overlooking significant risks

Cyber essentials doesn't require organisations to conduct comprehensive risk assessments. Without these, risks may be overlooked.

A tickbox mentality

Compliance provides a baseline for minimum security standards. A tickbox approach that satisfies the regulator may mean organisations fall short on managing their risk exposure.

Frameworks are a minimum standard

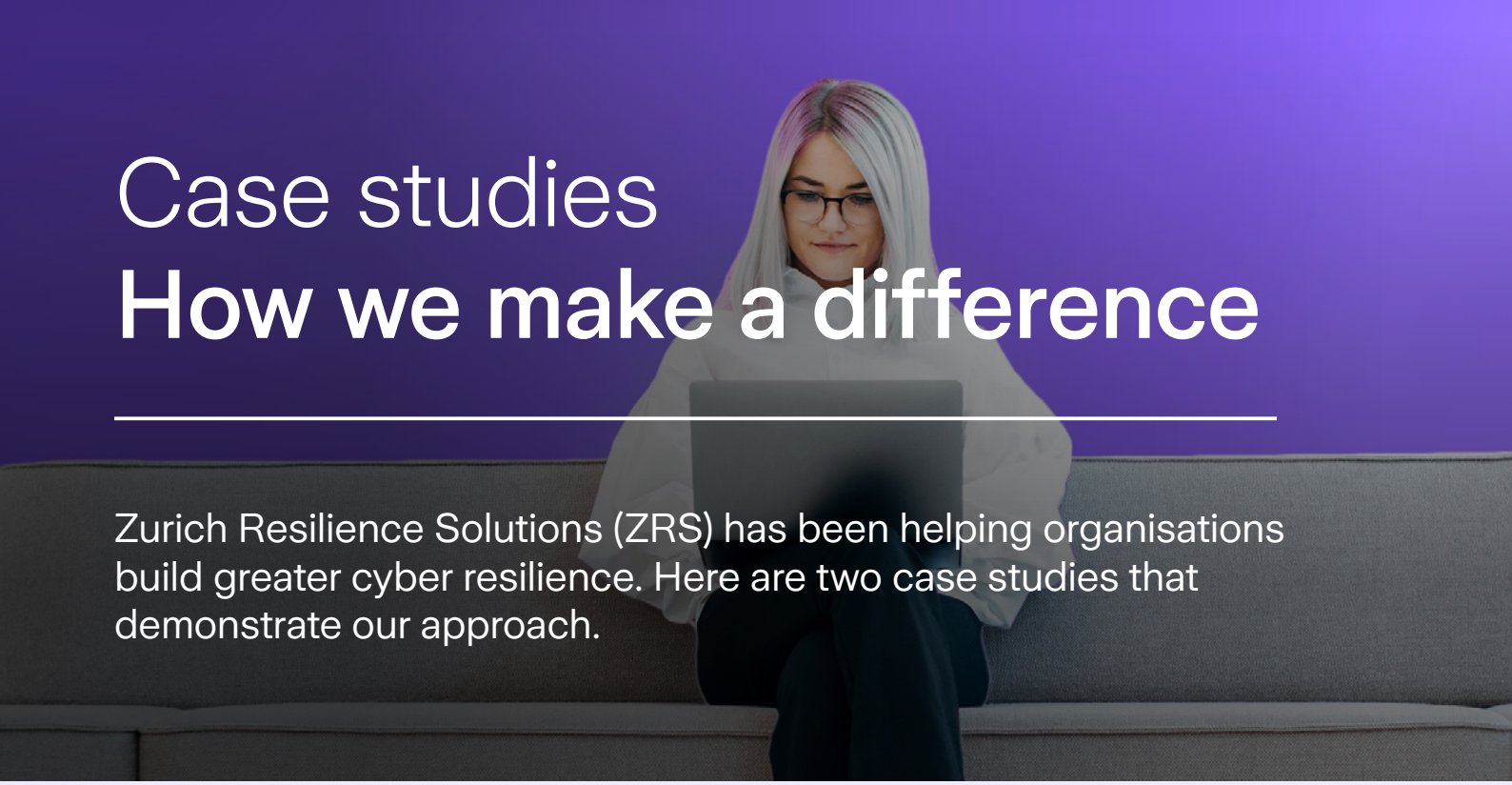
Cyber compliance focuses on meeting regulations, standards and guidelines set by industry bodies and governing authorities.

Why a risk-based approach is essential to strengthen cyber resilience?

Effective management of cyber risks requires organisations to adopt a risk-based approach. This allows organisations to identify and mitigate risks to a level accepted by the organisation.

What does a risk-based approach consider?

A risk-based approach will consider the likelihood of an attack occurring and the impact it can have on an organisation through financial loss, reputational damage, operational disruption, data breaches, and the impact on critical assets. It also enables organisations to make informed decisions about the allocation of resources too.



Case studies
How we make a difference

Zurich Resilience Solutions (ZRS) has been helping organisations build greater cyber resilience. Here are two case studies that demonstrate our approach.

1. Orbit Housing

Orbit Group is a leading UK housing association.

The ZRS team has worked with Orbit since 2021 to improve cyber resilience, starting with a cyber health check.

The health check recommendations:

- **Suggested enhancements to IT security policies** to improve resilience by laying requirements for users and increasing cyber security awareness.
- **Improve incident response capability** by running regular tabletop exercises to ensure Orbit is prepared in case of a real incident.
- **Recommendations to improve incident and business continuity response** following the results of the tabletop exercises.

Customer outcomes
Orbit is able to:

- **Deliver** an ongoing cyber improvement programme.
- **Demonstrate tangible cyber security improvements** to stakeholders.
- **Undertake regular cyber incident and business continuity exercises** to help senior leaders understand the technical and operational responses to a major incident.

2. LondonEnergy

LondonEnergy is a waste management company that supports environmental sustainability. The organisation asked ZRS for support in building and maintaining its cyber resilience.

ZRS assessed LondonEnergy's environment to understand their risk exposure. They then created an action plan for developing resilience.

LondonEnergy
Powering the Circular Economy

The health check recommendations:

- **The implementation of proactive tools** to improve cyber detection capability.
- **Development of the incident response capability** through regular tabletop exercises to ensure the company is prepared for real incidents.
- **Creation of a cyber risk management policy** that describes the requirements and coverage of regular risk assessments, including a defined risk appetite.

Customer outcomes
LondonEnergy now benefits from:

- **Improved cyber maturity** thanks to the implementation of a cyber risk management policy.
- **Assurance for senior leaders and stakeholders** due to the organisation's improved ability to respond to cyber incidents.
- **The implementation of a proactive detection tool** that has improved the organisation's ability to detect and respond to events.

How Zurich Resilience Solutions can help you

Zurich Resilience Solutions specialist cyber risk consultants can support your organisation's cyber resilience journey.

Who's it for?

We're a trusted partner to a range of organisations, from SMEs to global enterprises. Your organisation doesn't have to be insured with Zurich.

How can we help you?

We provide end-to-end cyber risk services tailored to your organisations needs. These include cyber risk assessment, cyber response preparation plus technical services such as penetration testing.

A connection to insights and data

We have exposure into how organisations prioritise their cyber risk management. We can use this insight to help your organisation.

Sharing information for industry benchmarking

We benchmark the cyber maturity of our customers. You can learn how your organisation compares, and implement strategies to improve.

Helping support insurability

We can help support your insurability journey because we know what underwriters expect and can help you meet these standards.

Start your journey with a cyber risk assessment

A risk assessment is the starting point for a risk-based approach. Think of it as an MOT, where we assess the strengths and weaknesses of your current approach.

We can identify improvements and give you a starting point to strengthen your cyber resilience.

How Zurich Resilience Solutions can help you

Ready to get started?

If you're ready to start your journey with us today, book a 30 minute consultation call with one of our cyber resilience experts.

Book a call today:

www.zurich.co.uk/business/cyber-resilience/book-a-call

52553_CYBER-RESILIENCE_0524

ZURICH®
Resilience Solutions