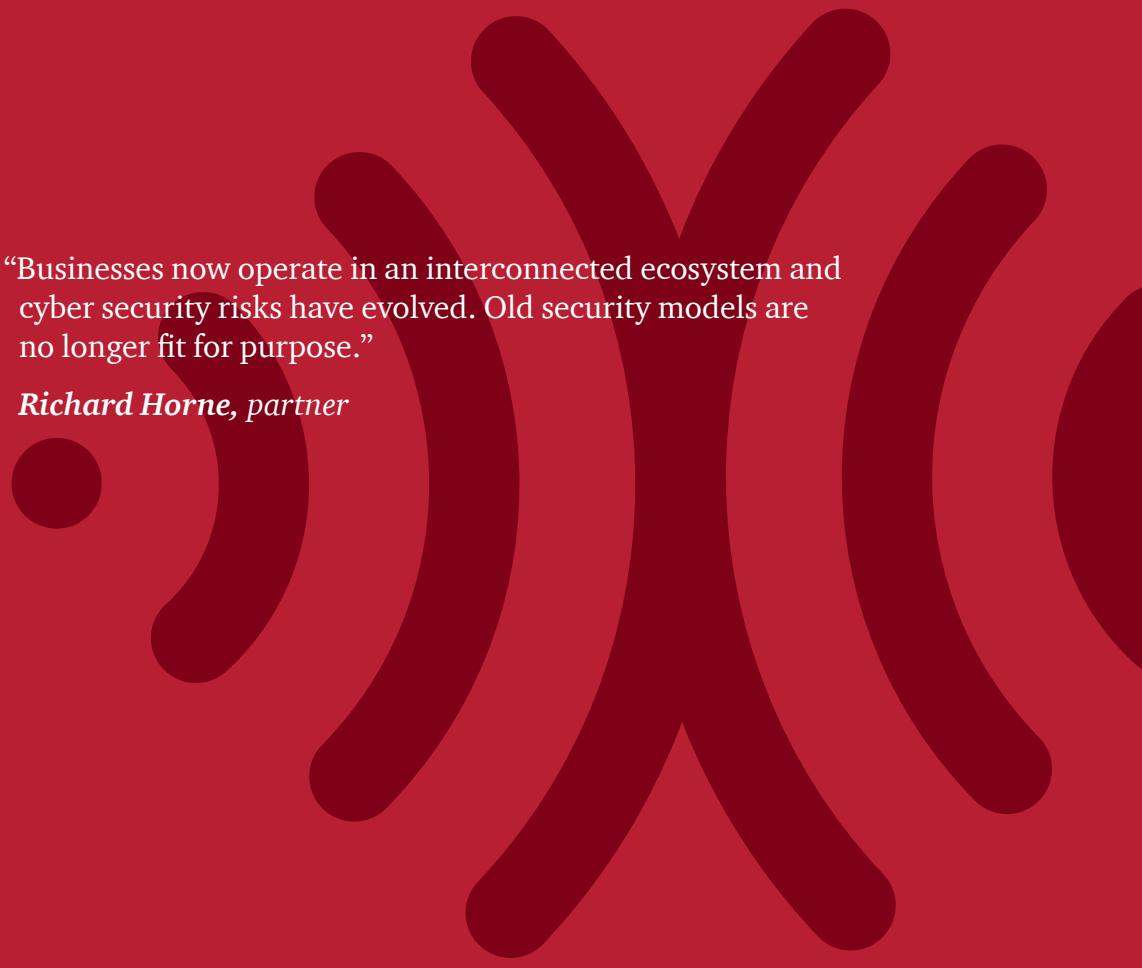
www.pwc.com/riskassurance

Cyber security Confidence in your digital future

The executive summary series – paper No.5

"Businesses now operate in an interconnected ecosystem and cyber security risks have evolved. Old security models are no longer fit for purpose."

Richard Horne, *partner*



pwc

Changing your perspective

We believe that confidence in your digital future is essential to the growth of your organisation.

You need to be aware of your cyber security risks, able to assess which threats could actually affect your business goals and have the agility to deal with new threats as they arise.

At the same time, advances in technology are enabling business ideas to flourish. In considering cyber security and the risks and opportunities it brings, your cyber risk management strategy needs to be at the heart of your business. Old security models are no longer appropriate.

What's on your mind?

The digital age is bringing rapid change: new customer connections, tighter supply chain integration, new sourcing models; new ways of exploiting bulk data; faster R&D processes; mobility and much more.

Your digital world just got bigger
Businesses now operate in an interconnected ecosystem. As a result, securing critical data, transactions and operations means working beyond the walls of your enterprise. Businesses are completely dependent on digital business processes. This amplifies the impact of cyber attacks on every area of your business.

It's not if, but when
Scarcely a day goes by without mention of a new cyber crime in the newsfeeds. Businesses face a wide range of threats. Adversaries range from nation states and organised crime to hacktivists and insiders. It's understandable why you may feel fearful – by the time you've strengthened your defences, you are probably already under attack. Would you know what to do if you are compromised? Are you prepared?

How do you survive and thrive?
Cyber security is not just about protection – it's exploiting the opportunities that the digital way of working brings. New technology such as cloud computing brings more efficiency, lower costs and greater consumer productivity, but it's fraught with risks. If your cyber security is inadequate you won't have the confidence to take risks that allow you to get ahead of the competition. Cyber breaches damage reputations and destroy trust – both are vital ingredients for success in the digital age.

"According to the Global CEO Survey, one third of CEOs don't think a cyber attack would negatively impact their business. Yet 61% of consumers would stop using a company's product or services if an attack resulted in a known breach."

2012 PwC Consumer Intelligence Series

Our point of view

Old security models are no longer adequate
While cyber security risks have evolved, the traditional information security model – one that is technology-focused, compliance-based, perimeter-oriented and aimed at securing the back office – is no longer fit for purpose. Not only that, your cyber capability needs to provide continual insights and intelligence on the threats your business faces. Armed with this insight, you can anticipate and react dynamically to changes in your cyber threat profile.

Cyber security at the heart of your business
When looking beyond enterprise boundaries, you need to protect what matters most and ensure investment is allocated correctly. Cyber risk management in the business ecosystem is a complex issue, requiring your board and managers to engage, and sophisticated techniques, new skills and capabilities to be embedded in your people. It's better to assume you will be attacked, ensure you can respond effectively and prepare for the worst. You cannot afford to be complacent – cyber security should be 'front and centre in your business'.

Build trust into the fabric of your digital operation
Your reputation is key. You need confidence in your operations and environment to allow you to unlock and prioritise opportunities and protect what matters most to you and your business.

Develop a clear risk appetite
Cyber security should be treated as an enterprise-wide risk for which you need to develop a clear risk appetite to suit your specific business circumstances and associated action plan; and you need to see frequent assurance that risks are appropriately managed.

What good looks like

Successful security models have the following characteristics.

- You continually monitor your risk profile. You understand what matters to the success of your business. You realise this changes as you move forward with your business.
- You understand in real time, the new threats within the digital landscape. You are fully aware of the risks you're exposing the organisation to as you execute your strategic plan.
- You understand how digital is changing the fabric of your business, introducing new threats and changing your risk profile.
- Your eyes are fully open to digital threats.
- You recognise boundaries have shifted: your business architecture has changed, so have the risks within your digital supply chain. You are aware that threats can come from within your organisation as well as from outside it.

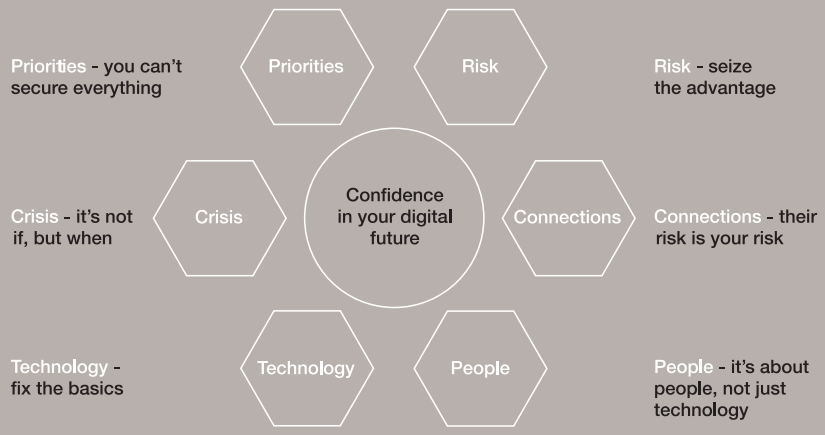
When to act

There are logical triggers in your business activities that prompt action. These will almost always be times when you should talk to us. Here are some examples.

- By involving us as early as possible in your strategic business planning cycle rather than waiting until an issue becomes a problem.
- Changes to regulation or legislation that will affect your business.
- Change in the form of new suppliers, new technology, acquisitions, new markets or a change in leadership.
- Trends or developments in your market that are likely to affect your business and where it's better to respond proactively.

How we can help

We can help you shape a broader strategic response to cyber risk by helping you understand your current capability and putting in place a focused plan to target investment in the right places. To do this, we focus on six key areas:



Four-stage process

Assess – understanding your capabilities and maturity to help you prioritise your investment.

Build – designing and delivering cyber security improvement programmes.

Manage – managing and maintaining control of your business, enabling you to focus on strategic priorities.

Respond – rapid, global access to leading cyber incident containment, investigation and crisis management expertise.

What you gain

Below are the six confidences that will help you apply cyber security to the heart of your business.

Confidence in your people
Fostering secure behaviours by designing processes, systems and roles with human vulnerability in mind.

Confidence in your technology
Understanding the inherent risks of your technology and how to mitigate them.

Confidence in your connections
Building an agile risk management framework, adept at keeping pace as your collaborative networks evolve.

Confidence to take risks
Considering your interactions within the digital world and assessing where and how they impact your past, present and future.

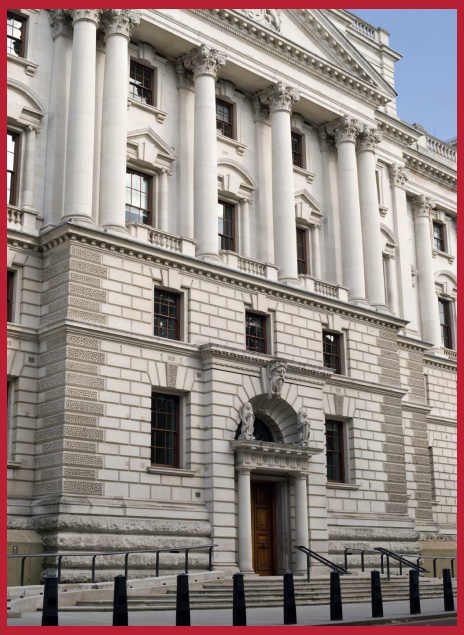
Confidence during a crisis
Protecting what's important, detecting intruders and minimising your exposure when you are compromised.

Confidence in your priorities
Recognising where key assets are, which are often intangible, and aligning them with your priorities.

Delivering value

After losing a significant amount of cash via online banking transfers to one-off foreign suppliers, our international engineering and service company suspected they had experienced a cyber security breach rather than fraud. With malicious software ruled out, they suspected that insider threat was the root cause.

We identified how the cyber criminals were able carry out the eCrime. Using a combination of activity timeline analysis, file recovery and reverse engineering, we diagnosed the nature of the crime, the chain of events leading to the breach and how they were able to manipulate a secure online banking payment process.



We were asked to review two service suppliers who were providing security control services to a major central government department. Our role was to undertake a compliance review against the Cabinet Office Security Policy Framework, CESG IA policy, Good Practice Guides and ISO27001, to assess their level of compliance.

We also reviewed the complete risk management and security culture of both suppliers, providing the department with recommendations to improve control.

Our global shipping conglomerate engaged us to create and deploy a large-scale information security programme including the development of a business case for creating a security operations centre (SOC).

We reviewed and assessed their current security services, processes and controls across the business including IT functions.

We provided recommendations and clarity on what a SOC does; the business need and benefits; scope of activities, roles, responsibilities and skill sets; implementation requirements, costs and timelines and developed an SOC operating model and deployment options (insourced vs outsourced).

This telecommunications provider was keen to understand the effectiveness of their privacy strategy, especially against their competitors. We were asked to review how it had been implemented within the UK business and other business units across their global network.

To gain a broad overview, we benchmarked information about how a number of global clients approached the implementation of their privacy programmes.

Contact:

Richard Horne
richard.horne@uk.pwc.com
+44(0) 7775 553373

Grant Waterfall
grant.waterfall@uk.pwc.com
+44(0) 7711 445396

www.pwc.com