# Cyber Security and Operational Resilience

## Operational resilience is the capability of organisations to continue to deliver critical services in the face of evolving threats.

**Cyber security is a key mechanism by which organisations achieve this. The range and sophistication of cyber threats, from nation states, hacktivists and organised criminals, was already having a profound effect on how organisations achieve operational resilience - even before Covid-19.**

### Increasing cyber threats

The current pandemic means that companies need to be more vigilant than ever. According to the National Cyber Security Centre, cyber criminals are exploiting coronavirus fears and using the pandemic as bait in phishing attacks. Phishing emails are increasingly citing topical reasons for quick action - such as furlough or home working - to get people to follow instructions in the belief that they have been legitimately requested. Organisations are having to rapidly respond to ensure that their employees and customers remain vigilant to these emerging threats. For example, customer guidance from banks is already being revised in response to this latest surge, and over a dozen NHS organisations have had to respond to ransomware attacks.

### Growing reliance on technology

At the same time, companies are suddenly more reliant on technology than ever before. Working from home has become the norm, leading to an increase in 'shadow IT' as employees eager to collaborate with their colleagues are turning to popular applications and services that may not be approved, or appropriate, for company use. This has the potential to put company data at risk: employees may use home equipment that is less secure – wifi routers with default passwords or no access control; PCs or mobile devices with no endpoint protection; or they may email sensitive HR or financial information to their personal email accounts for convenience, increasing the risk of data leakage. Often organisations have no other option but to sanction the use of technology they have not yet been able to secure, or are only now becoming aware of vulnerabilities because they are being exploited by new threat actors.

*"The most operationally resilient organisations embed good cyber security practices right the way across their operating model - spanning governance, policy, people and process as well as the technology itself."*

Dave Machin
Partner

In addition, some businesses are hastily standing up increased online operations, with the need for speed often meaning security is an afterthought. The change has happened so quickly that few companies have had a chance to adjust their policies or provide any additional training. While speed may be of the essence in the immediate response to the pandemic, there is the risk that many of these new ways of working will stay in place even as lockdown restriction are lifted. The cyber security skills gap may widen as companies are forced to act. However, everyone in the company needs to be aware that they have an important role to play in cyber security – it's not something that can simply be handed to a team of cyber security professionals.

## Responding to the threat

The best response to the growing cyber security threat is not to simply bolt a cyber security function next to existing capabilities. Instead, organisations should use cyber security as a lens through which to improve overall operational resilience. For example, the tools, techniques and cultural responses to cyber security can also be used to strengthen traditional business continuity capabilities.

A pragmatic way of approaching this in our view is a structured review of current cyber strategies and roadmaps to ensure new risks are identified and mitigated, and longer-term changes to ways of working are incorporated into existing business plans. Good cyber security practices should permeate everything technology related in a company and need to span the 'three Ps': policy, people and process, as well as the technology itself. It is important not to forget the supply chain – e.g. assessing third parties for their approach to securing their 'Software as a Service' products. Creating a cyber-aware culture within IT departments themselves is vital but it's important not to forget end-user awareness through communications and training.

Achieving operational resilience requires a broad spectrum of interventions, from initial strategy definition through to delivering change and continuous improvement. Berkeley has worked with clients across this spectrum. We have set a cyber and resilience strategy, conducted health checks of ongoing resilience change projects and helped our clients execute cyber security-driven change initiatives.

# Developing operational resilience

Cyber security fears have bred a proliferation of frameworks and point solutions such as the NIST Cybersecurity Framework provided by the US Department of Commerce and MITRE ATT&CK - a globally accessible knowledge base for tactics and techniques to combat cyber threats. In the UK, the National Cyber Security Centre has provided a Cyber Assessment Framework providing guidance for organisations. Too often, however, these are perceived as silver bullets. Frameworks and technology alone cannot be relied upon to deliver true operational resilience to cyber threats. When providing cyber security consulting to clients, from formulating resilience strategies through to delivering tangible change to their cyber security capabilities, our advice is:

1. **Know the business –** what's important versus what's critical? What are the inherent organisational cyber security strengths and weaknesses?

2. **Don't let great be the enemy of good –** it's easy to be seduced into attempting a leap to the gold standard. Before attempting wholesale organisational change, first ask "How good are we at the basics of cyber security?" It's not glamorous but it's essential.

   For example,
   - Do you understand the estate / what digital assets you have / what may be of value / who might attack and why?
   - Do you have good organisational risk management into which you can integrate cyber security?
   - Do you have plans in place for when things go wrong (incident response)?

3. **Judgement over theory –** with cyber security, it's impossible to analyse your way to success. True operational resilience is achieved by being pragmatic, iterating through focused thinking and delivering meaningful change in manageable steps.

4. **People are as important as machines –** too often cyber security is characterised as a technology arms race, but developing operational resilience relies as much on cultural and behavioural change within your business (see the "three P"s referenced above):

   For example;
   - end-user awareness, to ensure they are less vulnerable to phishing and social engineering, is just as important as latest generation firewalls; but that awareness needs to evolve as the threats evolve. For example, you might spot the email purporting to be from the "finance director", but would you spot the latest deepfake phone call?
   - elaborate information protection solutions are no substitute for a culture in which end users understand what constitutes sensitive or private information and respect how it should be handled;
   - buying extended support for software is of little use if your business stakeholders won't accept the disruption that comes with installing the security patches that come with it.

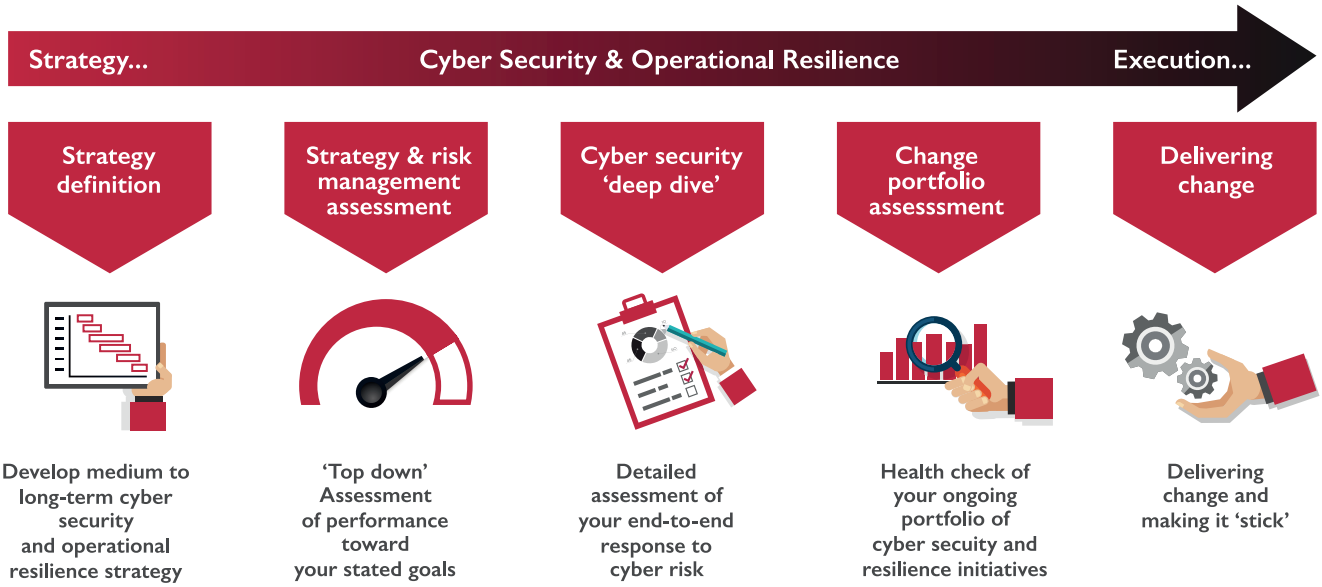
5. **Get in to the heads of the decision makers –** governance, organisation and ownership are everything. Effective operational resilience should come from the top down, not the side in.

**By adopting these principles, which contextualise cyber security interventions, organisations will maximise the value they get from frameworks and point solutions.**

# How we can help?

For the last thirty years, we have been supporting our clients with their most complex, critical and legacy leaving challenges, by deploying small teams of highly experienced people. Over the last five years, an increasing number of our clients have been turning to us to support them with their cyber security and resilience challenges. As a result, we have developed a breadth of experience in the financial services, logistics, consumer goods and media sectors where we have set cyber strategy and delivered associated change programmes.

## We offer our clients a range of services to tackle cyber security and operational resilience challenges:




**Our recent assignments in operational resilience consulting range from upfront strategy and risk management assessments, such as:**

- Developing the recovery and resilience strategy for a central bank operated piece of critical national infrastructure (and mobilising the programme to deliver this).
- Working for a financial services regulator to develop a programme that assessed the operational resilience of firms in a range of sectors.

**Through to existing change portfolio assessments and delivery:**

- Leading significant information security programmes for a global consumer goods company, and a financial services regulator.
- Managing the delivery of a global Cyber Security Programme at a multinational logistics provider, resulting in a successful downgrade of overall cyber risk by the client's corporate risk committee.
- Managing the recovery programmes for a major media and advertising company in response to a ransomware attack, including developing a step change in capabilities for managing future cyber incidents.

**If you'd like to hear more about how we're supporting our clients in this space or if you are interested in learning more about any topics raised in this article, please contact partner Dave Machin. email: Dave.Machin@berkeleypartnership.com**