Your systems will fail.

So, what can you do about it?

How to protect your customers through operational resilience

What's it all about?

You're going to have a cyber-attack. Your systems will fail. You will have a data breach.

We paint a bleak picture, but the reality is a critical event is inevitable for most businesses.

Prevention should form a key part of your operational resilience strategy, but it is even more important to quickly respond to, recover from, and learn from critical events.

Click to jump to:

Why now?

Operational disruption and cyber-crime are not only a pain for your business, causing outages and breaches you need to fix on the fly. These things are also very likely to harm your customers. Service continuity when the worst happens is all your customers care about. Can they access their funds, money and cash? Can they pay their bills? Will they end up in arrears with a poor credit score?

If these incidents are not managed well, if you don't learn your lessons for next time (and there will be a next time), you may lose the confidence and loyalty of your clients, directly impacting your bottom line.

We've found that clients tend to look at operational resilience from an internal and cyber perspective, forgetting that it's the end-customer they should ultimately be protecting. In this guide we take you through the key tactics you can employ to enhance operational resilience, while focusing on ensuring business continuity for customers.

This is why you should care

Reported critical failures increased more than three-fold between 2018 and 2019!

Several high-profile systems outages have harmed customers, as have increasingly common data breaches in the industry.

Regulatory bodies plan to take a more joined-up approach to supervision. They will assess the effectiveness of firms' governance and risk management framework for managing operational resilience.

Given the risk operational failure poses to the financial markets, scrutiny from regulators is only going to increase.

How can customers be impacted?

The FCA has highlighted that, unbelievably, many businesses have not considered the impact of cybercrime on their customers. Systems weaknesses and cyber-attacks can lead to considerable consumer detriment.

- **Data breaches** can result in the loss of customer data which could be used for cyber-crime and identity theft.
- **Systems failures** and service outages can lead to missed payments, sending customers into arrears. This can result in fines and detrimentally impact customers' credit ratings, which may make it difficult for them to access financial services in the future.
- **Cyber-attacks** can result in the theft of data and money, and can cause systems outages.

Foster a security culture

Whether through intent or negligence, your staff are a key entry point for cyber-breaches and attacks. Fostering a security culture that informs effective training and monitoring sets the groundwork for robust operational resilience.

26%

of firms do not have a board-approved IT security strategy

53%

of firms identify staff in high-risk roles do not provide additional training on cyber-crime

Enhance your culture
Firms tend to view cyber-security as an add-on to technology rather than embedded within the culture. This means they're often on the back foot when a breach or failing occurs, resulting in quick-fix measures that are sure to lead to customer detriment, and neglect the opportunity to learn from mistakes.

With the increase in the number and sophistication of cyber-criminal offences, a security-conscious culture, driven at board level, is the best protection for business continuity and sustainability. A customer-centric culture will naturally align with cyber-security to focus on ensuring positive outcomes for customers.

Embed through training
Most firms report having difficulty managing staff that are in high risk roles or who deal with critical and sensitive data. This includes executives and their assistants, HR and finance personnel, as well as staff that have privileged system access.

SMCR will play a role in apportioning and aligning responsibilities for cyber-security and operational resilience. However, training is often overlooked with only 47% of firms providing, at best, ad hoc and inconsistent additional training for high-risk staff. Education and training on the necessity of cyber-security, and how staff can be exploited to gain access to data and systems, empowers them to deal with the cyber-crime risks they are exposed to in their role. Staff training should complement the technical control environment.

Monitor key risks
The prevalence of social engineering and phishing attacks as a means of cyber-attack presents a significant weakness. This is often exacerbated by failure to monitor staff activity. We're not saying you need to implement big brother-style surveillance! Carefully planned and consistent monitoring of the key risks will make it easier to identify discrepancies in your staff behaviour, as well as activity that should be further investigated.

"Technology can help you monitor risks more effectively and efficiently."

Get your house in order

Cyber-criminals will be able to easily exploit vulnerabilities in your systems – vulnerabilities caused by a lack of understanding, and a failure to record key assets, services and third-parties. So it's essential to truly get to the bottom of the systems you use and how they impact business resilience, service continuity and customer outcomes.

80%

of firms struggle to maintain a view of the information assets and third-parties they hold

15%

of operational incidents are due to third-party operational failures

Know your assets
It's likely that you have a general understanding of the information assets your organisation holds. You probably have a vague knowledge of the third-parties you use. But this all changes frequently, often without adequate assessment of the vulnerabilities of the systems, networks and assets.

Conduct an audit, and log the data in an all-encompassing register making sure this information is up-to-date and complete. In particular, you should identify who within the third-parties has access to your systems and data and how this could be restricted.

Appreciate the business impact
Plenty of firms do not fully appreciate the sensitivity of their information assets, and just how critical these are to the continuity of business services.

Your audit should cover how these assets and systems are used within business services and the impact of failure if they aren't adequately protected.

Assess your customer impact
Are you assessing the risk that failure could have on your clients? Your audit should include an assessment of how systems outages and breaches will influence your clients' ability to access and use your services.

Develop protective measures
Organisations can neglect to upgrade or replace their information assets in good time, particularly at the end of their usable life. They also often fail to carry out any added risk management practices while assets are replaced.

Cyber-criminals often access systems by exploiting unaddressed vulnerabilities in unsupported assets. You need to understand the impact of cyber-crime and systems failures on both your operations and your customers, responding with effective, risk-based preventative measures.

This should include scenario planning, penetration testing and stress testing to ensure the measures you put in place are as robust as possible.

20%

of operational incidents are caused by IT changes

Regularly review
Although some firms regularly review their assets, networks, systems and third-parties to identify those reaching the end of their life, they often don't carry out a complete or continuous review. In some cases, the review may only be done periodically on a manual basis.

You should review periodically with an annual audit and also put processes in place that ensure the record is kept continually updated as assets change over time.

So, now might be time for a spring clean. For many firms this will be a long and complex pro-cess combining people from across the business. We're here to make that process easier.

Implement an effective operational resilience framework

While most firms operate a 'three lines of defence' governance model, operational resilience is often not widely considered. You can ensure you are prepared by implementing an effective operational resilience framework, considering the wider context as well as monitoring the cyber perimeter.

When implementing an operational resilience framework, don't just focus on the challenges you'd face internally. In looking at continuity and disruption issues, also consider it through the lens of conduct and customer outcomes.

The way in which you manage and respond to operational disruption will go a long way in assuring both the regulators and your customers that appropriate controls are in place. In particular, demonstrating you have considered the fair treatment of affected customers and communicating effectively with those impacted will illustrate that customers are at the forefront of your business. This could make all the difference for gaining valuable loyal customers.

You don't have to go it alone!
Enhancing your operational resilience is not an easy task – it'll require expertise, preparation, coordination, proactive prevention, and let's not forget accountability.

We're here to make it easy for you.

Come to us for operational resilience frameworks where customers are the core focus and your business is protected as a result.

Get the latest insight and regulatory analysis, straight to youar inbox.

Subscribe