ways to prevent a data breach

northdoor

◦ Store IT ◦ Protect IT ◦ Use IT ◦

With spending on digital transformation set to hit US$2.8 trillion by 2025, it's clear that business data has never been more important or valuable.

Given the potential for enormous financial, reputational and regulatory damage, all organisations need to think hard about how to keep their data and systems safe and secure.

However, businesses must simultaneously meet growing expectations for fast and convenient access to information and services.

So: how can you balance the demands of cyber security with the need to share information smoothly and efficiently between employees, partners and customers?

Here are ten ways in which some of the world's smartest companies are addressing this challenge and protecting against data breaches.

Take a holistic look at your business and the systems it depends on, work out what you need to protect, and then create the right cross-functional policies and organisational structures to mitigate the risks.

This means setting up: a business-continuity capability that ensures maximum availability for key digital systems; an incident-response plan with well-defined steps, roles and responsibilities; and recurrent training and reminders to help employees stay safe. And remember: cyber security is a moving target, so you need to build these capabilities into your business-as-usual operations.

Understand the risks you're facing, and align your business strategy with your approach to cyber security.

At an absolute minimum, every business must know what its critical assets are, and where they are hosted. After all, if you don't know what assets you have and which ones matter the most, you won't be able to prioritise your investments and properly protect yourself against data breaches.

You need to establish the right mix of measures to protect critical data. Start with an objective assessment of your current state of readiness, compare it to the target future state, then plan a step-wise transformation.

Starting at the core of your infrastructure, determine what key technology resources you have and make plans to protect them.

It's vital to consider data security not just at the level of networks and systems, but at the level of the data itself.

Creating immutable backups and encrypting entire data sets both in flight and at rest should be just the start. You also need to implement access controls on different sets of data within the same systems and databases.

That way, authorised users can get the data they need to do their jobs, while sensitive data remains protected.

Protect data in a granular way that supports business users.

Testing new releases of software depends on sharing access to realistic data sets, raising the risk of data breaches particularly when you are working with external developers who may be located in other countries.

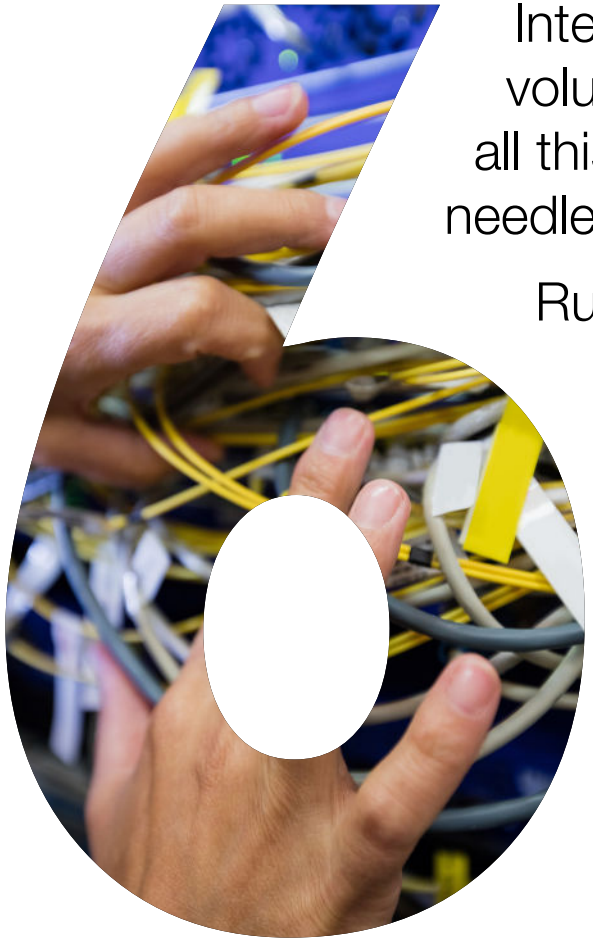
By deploying technology that automatically anonymises data at large scale, you can minimise the effort required to comply with data-privacy regulations while maximising the effectiveness of software testing. These technologies can also make it easier to detect and respond to potential infringements of data-protection regulations, ensuring that you can meet the required audit standards.

Industrialise data privacy with anonymisation and compliance solutions.

A key driver of cyber security risk is the proliferation of new applications, devices, and data sources both inside and outside the organisation. The pandemic has supercharged the adoption of digital technologies and remote working models. As a result, IT teams must maintain security across an attack surface that will continue to grow in both complexity and scale.

You need to make sure you can monitor and protect every point that provides access to your critical data resources.

Set up continuous intelligent monitoring of all endpoints inside and outside of the corporate network.



Internal and external systems generate huge volumes of event logs. How can you keep track of all this activity, weeding out false positives to find the needles in the haystacks?

Rules-based systems tend to produce too much—or too little—information. The latest AI-enriched monitoring tools can provide a clear view of the most important activity, learning typical patterns of system and data usage so that they can alert you when something looks wrong. Targeted attempts to exfiltrate data are often very subtle, and you need powerful tools to detect them.

Automatically detect, filter, triage and respond to emerging cyber security threats.

Email is the single most common vector for the introduction of malware onto the corporate network. Modern email security solutions cut the risk of data breaches by sending real-time alerts to employees the moment they're exposed to advanced phishing threats. These solutions are AI-powered, rather than rules-based, enabling them to adapt to changing threats.

By quarantining suspect messages and teaching users why these messages were flagged, the solutions minimise business disruption while improving the organisation's ability to identify and mitigate against security threats.

Set up comprehensive email security while educating internal users.

A key feature of the modern digital economy is the interconnection between companies. Your organisation needs to open its systems and data to the outside world—but doing so introduces significant risks.

At every point where your corporate network is exposed to public networks, you need to automatically and continuously scan for known and emerging software vulnerabilities. The latest AI-powered tools can also detect changes in behaviour at the network perimeter, potentially helping you identify the movement of protected data before a serious breach occurs.

Run continuous vulnerability assessments and perimeter scans.

It’s no longer just high-profile companies that are targeted in cyber security attacks. The increasing availability of low-cost, highly automated attack kits means that even unsophisticated hackers can take on small organisations with very little effort.

To avoid getting caught in the net, you need to engage external specialists to conduct penetration testing on your network. In addition to technical approaches, this testing should include social engineering attacks, to ensure that key employees understand the risks.

Test your own defences.

A chain is only as strong as its weakest link. In the corporate world, you need to make sure that your partners, vendors and customers are not exposing you to additional cyber security risks. What's more, you need to think about each of their partners, vendors and customers, and the systemic risk inherent in your business network.

A supply chain risk management solution provides real-time visibility of the cyber security stance and status of the third-party organisations you work with, directly or indirectly.

Monitor risks across the extended supply chain.

northdoor

Store IT • Protect IT • Use IT

A uniquely comprehensive approach to cyber security

Truly effective defence comes from a coordinated, holistic approach to cyber security—which can be hard to achieve without dedicated in-house security expertise.

Northdoor's uniquely comprehensive approach to cyber security, backed by expert managed services, helps organisations of all sizes to design, implement, run, and govern the appropriate security policies and technologies—and extend them from their core systems all the way out to their ecosystems of partners and customers.

For more information on how Northdoor can help you tackle cyber security, email, leave us a message or call us on 020 7448 8500 to arrange a free initial consultation.

www.northdoor.co.uk info@northdoor.co.uk +44 207 448 8500

Store IT • Protect IT • Use IT