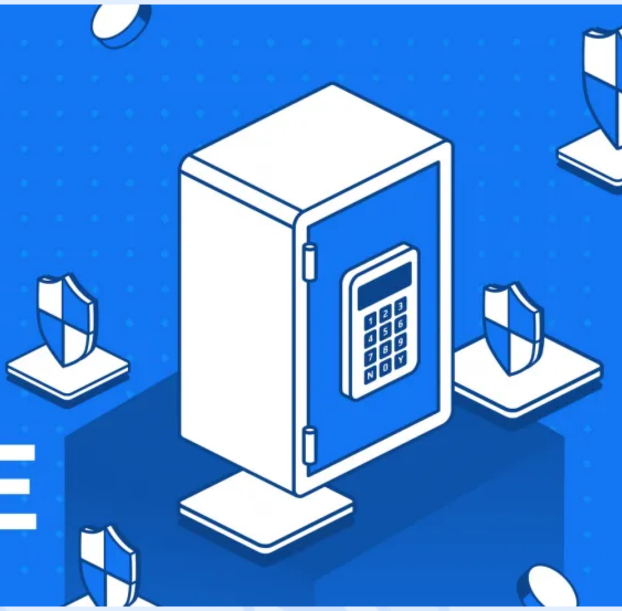
CYBER SECURITY AND RESILIENCE



Safe as the Bank of England: Improving resilience and cybersecurity

We always say that in the technology age, in order to stay competitive, it is necessary to let digitalization into the process of business improvement. Nevertheless, there are two sides to every coin. The more people and organizations use the Internet and devices for essential data storage, the more cases of cyberattacks we hear about in the news. The number is constantly growing (plus 50% year-to-year) and the main issue is that cyberattacks change and develop. The average company suffers from 925 attacks in a week. That’s why it is not enough to wait for the cat to jump, but on a regular basis to monitor vulnerabilities and constantly upgrade the security system. Companies need both plans against cyberattacks and scenarios for mitigating damage later. Here we come to the resilience term. Cybersecurity and resilience are in perfect step, but let’s have a closer look at their peculiarities.

Cybersecurity vs. Cyber resilience

Cybersecurity implies all actions, technologies, and policies aimed at providing the company’s protection of essential data and system networks against cybercrime and growing cyber risk. Meanwhile, life always throws you a curve, and when one of the company’s elements is hacked, it is time to go to a cyber resilience plan. As you can see, cyber resilience is a company's ability to face attacks and recover after, maintaining productivity and minimizing harm done. It is a flexible strategy of doing business that accepts risks and chooses the path of fewer ill effects. Complementary to one another, these two tools will help save the business and keep it afloat, avoiding financial and reputational losses as well as legal liability.

Steps to achieve cybersecurity and resilience

Just 14% of small companies are ready to protect themselves against cybercrime. By complying with the following rules, your company will improve your odds of success.

1. Make connections with a team of IT experts to consult with and to maintain the technical side of the security questions.
2. Regularly train your employees how to recognize danger and suspicious data, how to act in these cases.
3. Use a strong, unique password and regularly change it.
4. Set up a multi-factor authentication (MFA) on apps and software.
5. Install the latest software updates.
6. Do not download from unverified sources or link to unsecured devices.
7. Use firewalls and antivirus solutions.
8. Provide scheduled audits for system vulnerabilities.

That is not the whole list of the security measures. Elaborating on a tailor-made service in order to prevent and minimize the number of cyberattacks, Magora works in close coordination with your company. Based on your business characteristics, we will undertake a thorough assessment and will generate a route plan to pursue your goals.

However, after a while, cybercriminals can find new loopholes, and resilience must not be neglected. Some of the necessary steps that we advise you to take:

1. Be proactive and ensure that the offline backup operates properly.
2. Develop a substantive business continuity and disaster recovery policy.
3. Build a PR strategy to minimize the spread of negative chatter and keep customers’ trust.
4. Bring up the cybersecurity issues to the level of the company’s management to improve overall engagement.
5. Cooperate with or hire talented IT experts.
6. Maintain the level of readiness through regular simulations and tests.

Unfortunately, there is no single solution to the numerous scams, ransomware and malware in the evolving cybercrime world. Moreover, human error plays an important role, and sometimes it complicates the whole process of defensive shield building.

Magora always takes a responsible approach to bespoke software development and is ready to create a powerful defensive system in order for your company to be as safe as houses.