Reactive cyber-security measures are much more expensive and less effective than a proactive approach

February 2025

Stefanie Graf, Sandra Cramer

Cyber security involves a difficult balance between controlling the risk of successful cyber attacks, and keeping costs to a minimum, while also not losing focus on core operations. The best return on cyber-security investments can be achieved through a continuous proactive approach that is tailored to the organisation's individual risk appetite.

Many companies get caught in a reactive cycle

For too many companies, investment in cyber-security measures follow a repeated pattern. Initially, cyber security is a low investment priority; there are no incidents, and the business is 'getting away with' a limited cyber-security budget.

This underinvestment eventually allows a successful cyber attack, after which cyber security is suddenly the company's top priority. The second stage of the cycle sees a huge increase in budget and resources leading to a transformational improvement in security. Initially, intentions to maintain high cyber-security standards are declared, but often not adhered to, which leads to the third stage.

In the third stage of the cycle, there is a slow erosion of focus and investment. Eventually, the trauma of the cyber attack recedes, cyber-security measures slip down the priority list and the cycle begins again.

In behavioural economics, this pattern is known as the 'Rebound Effect'. However, this approach is neither efficient nor sustainable. Companies that maintain a constant focus on cyber security, backed up with consistent (proactive) investments, are typically more effective in reducing breaches and ultimately incur much lower overall cyber-security costs.

Cyber attacks cause damage in several ways

Many companies are reluctant to divulge detailed information about cyber attacks, but the negative consequences are varied and substantial. They include immediate impacts in service disruption, knock-on costs of repairing and recovering data and systems, regulatory fines, as well as the persistent but more nebulous effect of reputational damage.

The costs vary substantially according to context: the size of company, the industry, the nature of the attack and the location all have a bearing. The average direct cost per data breach globally was USD4.88 million in 2024.

How are the costs constituted?

A cyber attack typically triggers direct, measurable costs, as well as indirect impacts that are harder to quantify.

The direct costs of a cyber attack relate to incident response, system downtime, regulatory fees and ransoms. Forensic investigation alone can reach USD100 000; revenue losses due to system downtime and missed opportunities typically equate to around 9% of the company's annual revenue, as well as a 2.5% drop in stock valuation; regulatory fines and fees can be applied in addition, which in the EU can be up to EUR20 million or 4% of a company's annual global turnover (whichever is higher), depending on the policy affected.

These direct costs can be substantial, but they are only incurred for a limited period. The indirect costs (especially reputational damage) are more persistent and can derail attempts to implement carefully designed business plans.

Companies that have fallen victim to a cyber attack have difficulties both attracting new customers (reported by 20% of companies in 2023 and 47% in 2024) and retaining existing customers (reported by 20% of companies in 2023 and 43% in 2024).

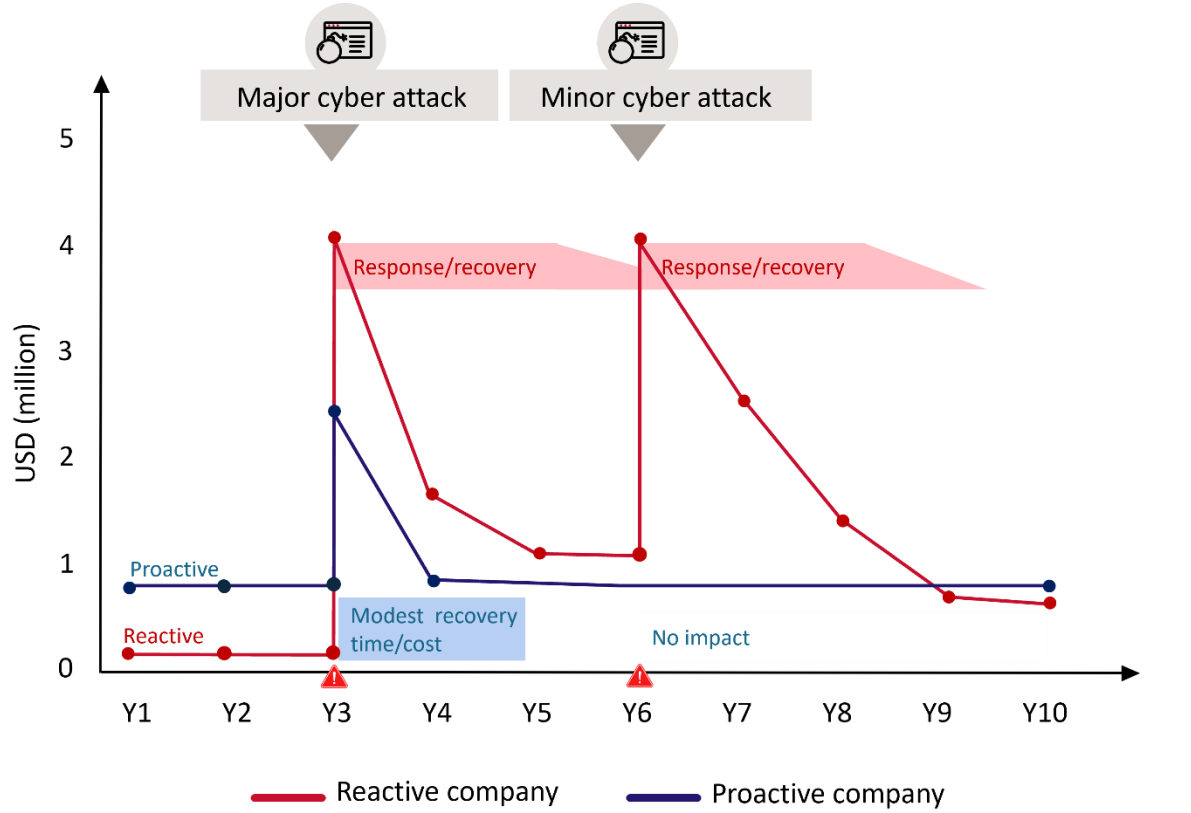
Optimising cyber-security investment and outcomes

To avoid the risk and expense of cyber attacks, organisations need to adopt a more proactive stance. This means a structured programme of investment in infrastructure, tools and maintenance (covering security tools, encryption, threat detection etc.).

It also requires an active programme of employee training to raise security awareness. Even the best systems can fail if a human unwittingly facilitates a cyber attack (exemplified by the USD100-million attack on MGM Grand).

Figure 1 below provides indicative costs for a European company of 200 employees and offers a comparison of the cost profile for that company under two different scenarios: one in which cyber-security measures follow a reactive approach, and one in which a proactive approach is taken. These indicative direct costs are the outcome of a simulation based on our experience of supporting clients of different sizes and sectors.

Figure 1: Indicative direct cyber-security costs for a proactive and reactive business



Source: Analysys Mason, 2025

In the reactive scenario, the company's security investments constitute a bare minimum. The measures are not tailored to the company's specific needs and are not underpinned by a coherent security strategy. In the proactive scenario, a defined security strategy is tailored to the company's specific needs.

A major cyber attack is launched in Year 3. In the reactive scenario, this leads to a severe security incident including a data breach. Substantial data loss leads to substantial fines. The lack of skilled staff and trained incident response plans prolongs the remediation significantly. The proactive approach leads to a better outcome. Trained security staff implementing practised incident response plans allow for an accelerated recovery, incurring smaller operational losses and less effort for reputational repair, as well as more modest regulatory fines.

In our experience, recovery from a severe attack can take years for companies that are not well prepared. In the months and years following a breach, the company must simultaneously regain operational capabilities, find skilled security staff and implement further security measures.

In our simulation, a second attack is launched in Year 6. The reactive company has not yet fully recovered from the earlier breach, and is vulnerable, making the second attack very significant. The proactive company is able to defend itself on the basis of the security strategy it has followed.

In our illustrative example, the direct costs in the reactive scenario are USD17 million, compared to USD8 million in the proactive scenario over the 10-year period.

The proactive approach holds additional advantages. As well as much lower direct costs (shown in Figure 1), the indirect costs to repair reputation are also lower (or zero). A security strategy can be implemented slowly and

carefully, aligning and evolving with the business goals of the company. It improves the company's standing in terms of governance and risk management, as well as staff morale. It allows for better long-term financial planning.

Making the transition from reactivity to proactivity

To avoid the punishingly high costs of a successful cyber attack, there is a clear path:

To establish a strong cyber-security framework, organisations should first assess their risks and identify critical assets. Then they should develop a comprehensive cyber-security strategy that reflects their specific business needs and set up an appropriate security structure within the company. Next, a realistic roadmap for security initiatives or a security programme needs to be designed to address the identified gaps and guide prioritisation of security measures. This includes implementing essential security technologies as well as organisational measures. Employee training is vital to raise awareness and protect the organisation. During and after implementation, the effectiveness of the defined measures needs to be monitored with appropriate reporting.

Analysys Mason has a proven track record building up risk management capabilities and identifying and assessing the cyber-security risks and vulnerabilities that could affect value and operations. Based on impact evaluations, we help our clients understand organisational risk appetite and security strategies. We work within our clients' operational teams to identify tools and vendors and manage budgets for cyber-security programmes. We help build customised reporting to track the progress and effectiveness of security measures. We are committed to helping our clients protect themselves from the financial and reputational disruption that cyber attacks can cause.

To find out more on how we can help you manage risks, gain a better understanding on your vulnerabilities, or define your own security strategy, please contact Annika Nitschke, Stefanie Graf or Sandra Cramer.