Developing An Effective Security Strategy

Why you need a security strategy

Security is often mistakenly viewed as an IT function, typically delegated to technology leaders. This misconception stems from the fact that most security incidents involve attacks on information assets via technology. However, security is primarily a business function, focused on supporting business objectives. Rooted in risk management, technical controls are simply tools to reduce risks and ensure operational continuity. Many organisations invest heavily in security tools recommended by various vendors, but this approach can be both costly and ineffective.

Developing and implementing a security strategy enables organisations to focus on the specific risks they face. A strategic approach promotes proactive security measures, ensuring preparedness and thoughtfulness rather than reactive, improvised actions that might fail at critical times. A well-planned security strategy identifies where to prioritise security investments, arming the organisation with valuable insights to support business objectives and strategic roadmaps.

Simply put, a security strategy helps business leaders understand the biggest risks to the organisation. It facilitates decisions on controls and safeguards that reduce the likelihood of these risks within an agreed budget and timeframe. This transforms the perception of security from a vague IT expense to a transparent, business-critical function.

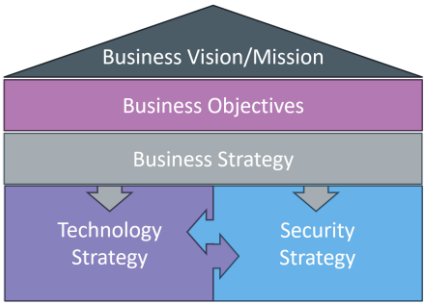
Where to start

Developing a security strategy begins with evaluating the value of both tangible and intangible assets, such as data, platforms, and reputation, using qualitative and/or quantitative methods. A Business Impact Assessment (BIA) identifies the potential impact of disruptions on systems, people, processes, and technology. Organisations must then assess the threat landscape across environments like cloud services, infrastructure, physical locations, and third-party providers to identify risks and attack vectors.

Finally, a Risk Register is created to prioritise high-value assets and associated risks to Confidentially, Integrity, and Availability (CIA), providing a clear roadmap for mitigating threats.

Develop the Strategy…

The security strategy must support the business's overall goals, aligning with the business strategy. It should also complement the technology strategy, as cyber controls need to support technological shifts. For instance, if a business strategy involves migrating to the cloud, the security strategy should align with these milestones, ensuring adequate controls for cloud environments. Understanding the business's primary objectives and how technology supports those goals provides the foundation for the security strategy.

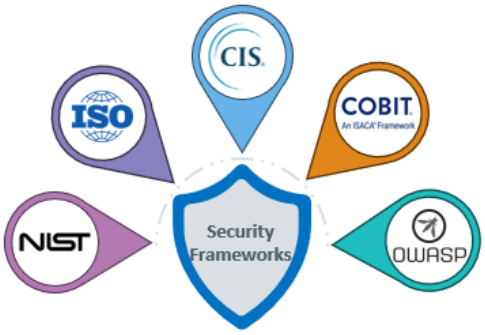


Key factors to consider are the organisations capability maturity against industry benchmarks, risk appetite and any 'quick wins' that can deliver effective improvements at pace and or low cost.

Once these factors are considered, an evaluation of existing security controls should be performed. This identifies where additional investment may be required, either in new or enhanced controls, to deliver 'Defence in Depth'. The evaluation should take a broad approach, considering more than just technical controls. Administrative controls, such as policies and procedures, are crucial to inform physical and technical security measures.

To develop a comprehensive strategy, access the technology estate and catalogue system lifecycles to identify current or future weaknesses. Managing End of Support and End of Life systems is costly and risky; planning upgrades or applying compensating controls can reduce risk, improve efficiency, and support continued operations.

Security evolves rapidly, requiring ongoing awareness of policies, regulations, advancements, and standards. Adopting suitable frameworks provides structure and standardisation, but selecting the right ones depends on organisational needs, regulatory requirements, and business activities. Some frameworks, like PCI-DSS and GDPR, address specific regulations, while others, such as OWASP, focus on particular disciplines. Holistic options like NIST-CSF, ISO 27000, or COBIT support governance and processes but may require tailoring to fully align with business needs, as no single framework offers comprehensive coverage.



Review security policies regularly to ensure alignment with changes in technology, processes, standards, legislation, or regulations, while addressing any gaps. Start with the Security Policy, which defines the organisation's approach to protecting confidentiality, integrity, and availability, and establishes general rules and expectations. This should be supported by specific policies—such as Acceptable Use, Email, Password, Encryption, Remote Access, Data Privacy, Data Classification, Data Retention, and Disaster Recovery—along with standards and guidelines to ensure compliance.

An essential component of any security strategy should include a Risk Management Plan. The plan should include analysis of all the potential risks that could impact the organisation, including operational risk (covering technical and environmental), financial risk, regulatory or compliance risk, and of course, strategic risk. Evaluating these risks, developing a plan, and implementing policies to mitigate or reduce harm from the assessed risks is a vital tool in preparing your business for potentially adverse events.

Implement the Strategy

Once the strategy is developed, with assessment activities and policy plans nearing completion, it will be time to plan delivery. It will be necessary to identify key stakeholders and accountable teams or individuals who will support the prioritised deliverables from the strategy. If your company has a PMO office, then you can enlist them to support the delivery.

Whatever the method, size, and scale of the supporting teams, it will be necessary for the executive team to demonstrate leadership and support throughout delivery, setting realistic goals and deadlines that do not overwhelm the delivery teams. This is also the time to promote the new strategy across the business and to new change initiatives, who should be baking in the strategy to their deliveries.

Continual Evaluation

The Security Strategy represents the response to a point-in-time evaluation. It will therefore need to be reviewed regularly and modified to respond to evolving conditions and threat landscapes. The strategy should be monitored and tested periodically, with key stakeholders held accountable for oversight and reporting.

An annual risk assessment should be performed to help identify any gaps that may need to be remedied in the strategy. This will ensure the strategy remains relevant and continues to support the key business objectives of the organisation.

Engaging with our Team

At Altus Consulting, we have qualified and experienced security consultants who can support your business in developing an effective security strategy.

Our **Security & Risk team** can help you with identifying and categorising risk, setting goals and objectives, assessing technology and security controls, identifying and implementing appropriate frameworks and policies, and all aspects of security strategy development and implementation.

In all engagements, we include the option for ongoing consultation with our team, to give an external perspective to your decision-making and governance processes. To find out more, contact us using the details below.

Find out more:
www.altus.co.uk
+44 (0)1225 438 000
enquiries@altus.co.uk