Cybersecurity Advisory

Ensure that your security posture meets evolving business needs

With our Cybersecurity Advisory, we assess your security posture, identify gaps, and deliver recommendations for improvement.

Business outcomes

- Identify opportunities to reduce operating costs, improve efficiencies and meet compliance obligations.
- Identify gaps in your security architecture and security management practices.
- Balance the need between the solutions to meet business outcomes versus best-of-breed technologies.
- Recommendations to make informed decisions about immediate security priorities.

Challenges

Security boundaries have moved, no longer can you rely solely on traditional networks to provide adequate protection for your most valuable business assets. Threats continue to evolve rapidly and your IT landscape changes driven by new business demands that include: more mobile access, more web-based applications, and hybrid IT environments. You need to think strategically about planning, designing, and operating your enterprise security.

A review of the current state of your security architecture is required as part of your ongoing security improvement initiatives. A security architecture includes the unified and integrated design, implementation, and operation of security practices across your organisation. This will enable you to formulate a plan to manage risks, maintain compliance with external regulations and contractual mandates, and align to industry best practice.

Solution

Our Cybersecurity Advisory covers the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimising existing environments, to designing your next-generation enterprise security architecture. Insight gained from assessments allow you to apply your resources and controls in the most effective way to protect key assets.

With our Cybersecurity Advisory, we undertake detailed assessments of your security architecture, from policies, processes to technical controls. Our flexible approach enables you to select key areas of focus and our more detailed assessments help you validate and support assumptions based on your current and desired to be states.

Based on strategic conversations in the information-gathering phase and the optional assessments chosen as part of the engagement, we deliver specific recommendations that allow you to apply your resources and controls in the most effective way to protect key assets. Combined with a remediation roadmap, these recommendations can be used to build a budget and resource plan, or simply align to an existing strategy for confirmation and reassurance.

The engagement includes:

- An information gathering phase which may involve interactive workshops and interviews to assess your current and desired state.
- The option to choose from a selection of security assessments to assess your security landscape.
- Recommendations for improvement.
- A security roadmap aligned to your business and technology initiatives.

> **‘Security is no longer seen as merely a technical issue. As business leaders continue to be challenged by the growing demands of today’s competitive digital landscape, security has become a central focus at the highest level for many organisations and governments.’**
>
> *The Executive’s Guide to the 2017 Global Threat Intelligence Report*

Document Code © Copyright Dimension Data 2017

Our consulting approach and methodology

Our engagement starts with an information-gathering phase with a representative audience from your team, facilitated by one of our experienced consultants.

Following the information-gathering phase, the optional security assessments are executed. Optional assessments may include, but not limited to:

- Review of documentation, policies, and technical controls to assess operational effectiveness.
- Firewall assurance assessment to review the firewall policy rule base and design to ensure it provides adequate security.
- Network visibility security assessment to determine if users are browsing risky websites that host malicious content and to identify malware infected systems, as well as, incidents of potential data loss.
- Tailored attack and penetration testing across web application, network infrastructure, corporate information systems to determine readiness to identify and protect against a targeted and focused actor scenario.

Speak to your local representative about our optional assessments.

Using the outcomes of the workshop and the selected assessments, we'll define your current state, review the internal and external security influences, determine the desired / required state, and make recommendations for improvement to achieve your goals in a mutually agreed timeframe.

We'll also create a dashboard that shows your current state as rated by our maturity scale, along with a future state, based on your objectives and aligned to a proposed remediation roadmap.

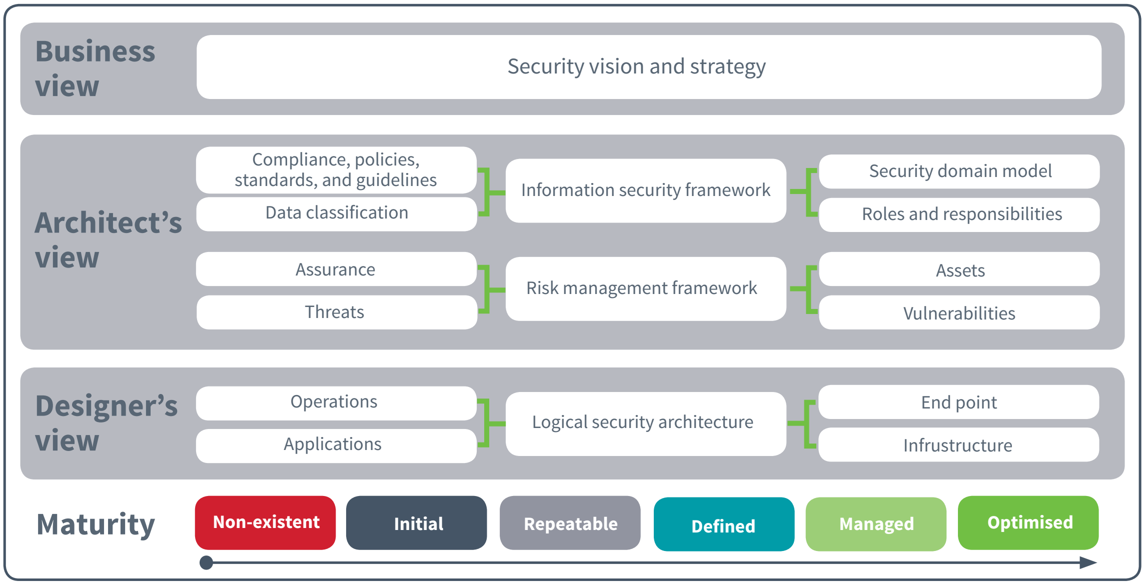

Figure 1: Dimension Data information secuty dashboard

Information security dashboard

As part of our assessment approach, we've developed an information security dashboard which summarises the assessment outcomes, based on our security maturity level model.

Figure 1 represents a holistic information security framework of our architecture model. Concepts of the framework have been inspired by SABSA (Sherwood Applied Business Security Architecture) to assist in developing architectures based on business-driven objectives.

The dashboard can be used to illustrate maturity across an organisation, a business unit, system or simply a business application. At the end of the engagement, each element of the dashboard is colour coded to your current security maturity level (an illustrated example is depicted in Figure 1).

Determining where you are, and where you want to be

As part of any organisation's ongoing security improvement initiatives, it's always recommended, and in most cases a requirement, to review the current (as-is) security architecture and understand the need for improvement, based on the agreed future to be state.

Not all organisations aspire to achieve the same level of maturity. Many factors influence this objective including business goals, an appetite for risk, security culture, budget, industry, regulatory compliance, and competition.

Our maturity model is based on the Carnegie-Mellon University Capability Maturity Model, using stages 0 to 5 to determine the level of maturity across people, process, and technology.

> **'As organizations explore innovative ways to tap into the power of data to create business value, effective risk management will underpin every business decision.'**
>
> *The Executive's Guide to the 2017 Global Threat Intelligence Report*

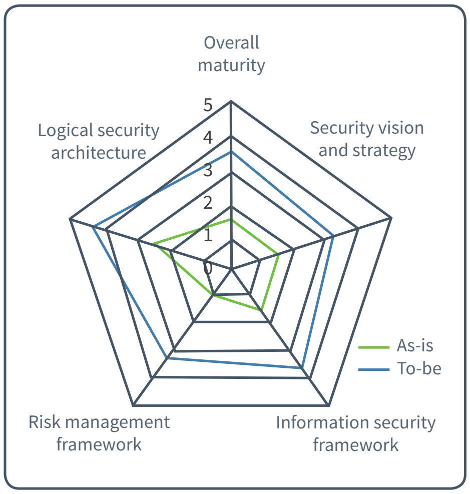

Figure 2: Illustrating current and future state

Dimension Data advantage

Our proven methodologies present solid security architectures to protect against the latest, most advanced threats, while providing flexible, agile environments that enable and support business initiatives. Our methodologies deliver adaptive and dynamic security that supports and enables all business initiatives including cloud, mobility, and Bring Your Own Device.

Dimension Data offers

Global experience

More than 15,000 security engagements with clients spanning 49 countries across multiple industries.

Track record

Decades of experience in providing professional, support, managed, and fully outsourced security services to over 6,000 clients.

Expert skills

Highly-certified security consultants with expertise across various infrastructures, systems, and application technologies.

Proven approach

Client-centric, pragmatic approach using proven assessments, methodologies, frameworks, and best practices to deliver consistent, high-quality engagements.

> **‘The expansion of the Internet enabled through mobility, cloud adoption, and the proliferation of the Internet of Things, has exposed new attack surfaces. Vulnerabilities are rife, data is exponentially increasing, privacy is being eroded, and the cost of breaches is becoming ever more debilitating.’**
>
> *The Executive’s Guide to the 2017 Global Threat Intelligence Report*

Document Code © Copyright Dimension Data 2017