Solutions Designation: Success

SECURITY

Solutions Partner for Security Designation

RETAIL

Determine Industry Requirements

Microsoft Solutions Partner
Security

What Are We Assessing?

The first step is to identify which industries are ideal for our Security solution, which we have done using data available to us, as outlined in lesson 2. We will now determine the specific requirements of these solutions by industry. We look at this from three perspectives – partner, customer and the results delivered.

What Is the Information Provided?

- **Partner oriented:** Provides information on the technical outcomes anticipated within this industry and outlines the required functionalities to achieve them.
- **Customer oriented:** Communicates with the customer about achievable outcomes in plain language, providing appropriate context messaging.
- **Outcome oriented:** Communicates to the customer the results or outcomes they will gain after transitioning to your new solution.

Why Is This Information Important to Understand and Use?

To create a successful solution, it is essential to understand the primary priorities of the industry, as they are crucial for meeting customer needs. This step clarifies our solution's goals, allowing us to identify the necessary technical components in our next lesson.

Partner Oriented

Ask Copilot

What are top 10 security priorities faced by the Retail industry in Australia. List the reason and requirement. Visualise in a table. Do not list numbers.

Copilot Outcome

Top 10 Security Priorities in the Australian Retail Industry

Security Priority	**Reason**	**Requirement**
Data Breach Prevention	Retailers manage vast amounts of customer data, making them prime targets for hackers.	Robust encryption, regular security audits, and employee training.
Fraud Detection	Increase in online transactions has led to a rise in fraudulent activities.	Advanced analytics, real-time monitoring, and multi-factor authentication.
Supply Chain Security	Complex supply chains can be vulnerable to cyber-attacks and disruptions.	Continuous monitoring, secure communication protocols, and risk management strategies.
Point of Sale (POS) Security	Cyber-criminals often target POS systems to steal payment information.	Regular software updates, secure payment gateways, and network segmentation.
Customer Privacy Protection	Customers are increasingly concerned about how their personal data is used and stored.	Strict privacy policies, transparent data handling practices, and compliance with regulations.
Physical Security	Physical threats like theft and vandalism still pose significant risks to retail stores.	Surveillance systems, access controls, and incident response plans.
Incident Response	Quick and effective response to security breaches minimises damage.	Established incident response teams, predefined protocols, and regular drills.
Employee Security Awareness	Employees often unknowingly become the weakest link in security chains.	Regular training programs, phishing simulations, and clear security policies.
Regulatory Compliance	Non-compliance with security regulations can lead to hefty fines and damage to reputation.	Regular compliance audits, updated legal knowledge, and comprehensive documentation.

Third-Party Vendor Security	Third-party vendors can introduce vulnerabilities into a retailer’s ecosystem.	Vendor risk assessments, secure contracts, and continuous monitoring.
Employee Training	Prevent security breaches due to human error	Regular cybersecurity awareness and training programs

Customer Oriented

Ask Copilot

What are top 10 security priorities faced by the Healthcare industry in Australia. List the reason and requirement. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.

Copilot Outcome

Top 10 Security Priorities in the Australian Healthcare Industry

Security Priority	**Reason**	**Requirement**
Employee Awareness	Employees can unintentionally cause security breaches.	Regular training, phishing simulations, and clear policies.
Regulatory Compliance	Avoid fines and protect reputation.	Regular audits, updated legal knowledge, and documentation.
Third-Party Vendor Security	Vendors can introduce risks.	Risk assessments, secure contracts, and monitoring.
Customer Data Protection	Protect customer information from being stolen.	Encryption, secure storage, and limited access.
Payment Security	Prevent fraud and theft during transactions.	Secure payment systems, regular checks, and fraud detection.
Cyber Attack Prevention	Defend against hackers and malware.	Firewalls, antivirus software, and strong passwords.
Network Security	Secure internal networks from breaches.	Regular updates, secure Wi-Fi, and monitoring.
Access Control	Ensure only authorised personnel have access.	Strong authentication, role-based access, and regular reviews.

Incident Response	Quickly respond to security incidents.	Clear plans, regular drills, and dedicated teams.
Data Backup and Recovery	Protect against data loss and ensure recovery.	Regular backups, secure storage, and recovery tests.

Outcome Oriented

Ask Copilot

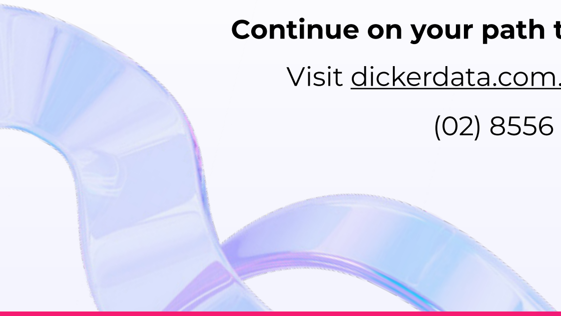
What are top 10 security priorities faced by the Retail industry in Australia. List the reason and security outcomes delivered. Deliver clearly and not using technical terms. Visualise in a table. Do not list numbers.

Copilot Outcome

Top 10 Security Priorities in the Australian Retail Industry

Security Priority	**Reason**	**Security Outcome**
Customer Data Protection	Prevent identity theft and fraud.	Customers' personal information remains safe.
Payment Security	Avoid financial losses and maintain customer trust.	Secure transactions and reduced risk of payment fraud.
Supply Chain Security	Ensure product integrity and availability.	Reliable supply of goods and minimised disruptions.
Physical Store Security	Protect against theft and vandalism.	Safe and secure shopping environment.
Employee Training	Empower staff to recognise and respond to threats.	Informed employees who can prevent and mitigate risks.
Vendor Management	Ensure third-party security practices are robust.	Secure collaborations and reduced risk from partners.
Incident Response	Quickly address any security breaches.	Minimised impact of security incidents.
Data Backup and Recovery	Protect against data loss and ensure quick recovery.	Business continuity and minimal downtime.

Regulatory Compliance	Adhere to laws and regulations.	Avoid legal penalties and maintain market reputation.
Cybersecurity	Prevent online attacks and data breaches.	Secure digital presence and protected online operations.



Continue on your path to achieving a Microsoft Partner for Security designation.

Visit dickerdata.com.au/Microsoft or contact the Dicker Data Microsoft Team

(02) 8556 8061 Microsoft.Sales@DickerData.com.au