Amphenol Air LB

Cybersecurity Guide

Cybersecurity guidelines for decision-makers

Version : August 2023

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

Table of contents

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

1 Introduction

Cybersecurity is a rapidly evolving field. It is no longer enough to deploy a firewall and encrypt the link between systems. Instead, we need to adopt a defense-in-depth approach, putting in place both preventive and reactive measures to detect and react to any breach of IT security.

Every day, new tools and threat actors emerge to gain unauthorized access to data, disrupt, disable and deny services and systems. Previously, these tools were only available to intelligence services, but increasingly they are available to anyone, including motivated individuals, hacktivists or cybercriminals looking to gain exposure, make money or simply wreak havoc.

In the modern digital world, knowledge is an important differentiator, and the ability of an unauthorized party to access or deny valid users access to critical systems and data, or even to deny access to the owners of these critical systems and data, should be a major concern for any organization.

Frequent articles in the press or notifications of incidents or data breaches received from suppliers prove that this threat is real, and not just a risk with a certain probability.

At every level of the supply chain, a cyberthreat actor has the potential to infiltrate and affect an organization. This threat can come from a disgruntled employee, a partner or software supplier, or even from their compromised components and libraries. It is very difficult to defend a system against all potential attacks, so it can be useful to prioritize security measures based on the actual experience of other victims.

This guidance document has been drawn up for an organization's decision-makers, particularly small and medium-sized enterprises that may be unfamiliar with the field of cybersecurity, or have limited cybersecurity budgets. This guide can help these businesses gain a better understanding of some of the most significant risks they may face, as well as providing additional advice and resources. These tips and resources can deliver quick results and provide insight into areas of focus.

Where an organization has outsourced its IT operations, this guide can also be used to define appropriate cybersecurity requirements as part of a service level agreement.

This document has been structured around the key organizational risks, guidance and additional resources for each of the areas of cybersecurity defense-in-depth ("Identify, Protect, Detect, Respond and Recover").

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

2 Risk management for organizations and decision-makers

2.1 Context

As we explained in the previous chapter, cyber-attacks represent a significant and growing threat to companies operating in specific key sectors, including aerospace and defense technology. These threats can also emanate from the supply chain, as suppliers have access to their customers' information and systems, but may not have the security infrastructure in place to adequately protect these information assets, exposing themselves and their customers to key security risks.

2.2 Main risks

2.2.1 Failure to protect customer data at suppliers' workplaces

This includes unauthorized disclosure or leakage due to inadequate system access control measures, which may lead to a passive breach of agreed non-disclosure agreements.

2.2.2 Exposure of customer information systems

This means that attackers can use inadequate network security in suppliers' systems and use their data connectivity with customers for attacks or espionage.

2.2.3 Legal/regulatory compliance

This amplifies the two risks mentioned above if regulated customer data is affected, such as contracts, intellectual property, export control, personal data (RGPD), classified defense/military data, etc.

2.2.4 Resilience of suppliers' information systems

As a result of a major IT failure due to a physical (fire...) or cyber event (ransomware...) and a lack of appropriate business continuity and crisis management, the company is unable to supply its products or services to its customers, impacting its results and those of its customers.

2.2.5 Exposure of the industrial environment

A cyber attack jeopardizes the integrity of the company's products or those of its customers, for example through the corruption or theft of design data, the electronic sabotage of production machines or the use of counterfeit electronic and physical parts.

3 Areas, advice and resources for in-depth cybersecurity defence

This section is divided into five areas of cybersecurity defense in depth to help readers understand the context and group similar topics together.

Each area is accompanied by tips and tricks, as well as resources and further reading for those interested to consult.

There is some overlap in advice and resources, so it's advisable to consult other areas. For example, certain topics, cybersecurity standards and methodologies often cover several areas (such as the ISO 27000 series or NIST CSF & 800-53B). This guide contains a series of tips and suggestions. It should be noted, however, that these are only a small number of possible measures in a dynamic and changing environment that every company should take into consideration.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

Here are the five cyber-domains:

- **Identify** - Focusing primarily on organizational and governance aspects, every company needs to have an understanding of the systems it controls or interfaces with. A company is not totally isolated, so the context in which it operates, under what legal and regulatory regimes, and with its suppliers and partners, is part of the "Identify" domain. This includes a basic understanding of security risks and controls.
- **Protect** - It's essential to focus primarily on technical measures to ensure that a system is protected at a minimum level, whether it's a customer marketing portal or a business-to-business online interface. Humans remain the most common "weak link" in any system, and the human element needs to be understood when implementing protective measures to safeguard a system against attacks, whether external or internal.
- **Detect** - It's not a question of "if" but "when" something will happen. When it does, an organization needs to be able to detect it and react as quickly as possible to reduce potential damage. Today, it's common to adopt a security posture that assumes a breach. The attack surface is so large that even an erroneous click on a seemingly innocuous website can compromise the entire system. That's why systems and controls to detect any breach are an essential measure in modern IT systems.
- **React** - Once a compromise has occurred, it becomes very important to be able to isolate a problem, minimize the impact on systems and services, and communicate with partners in an efficient and controlled way. Perhaps your expert administrator detects an attack in progress that is gaining a foothold in your users' systems and servers; who do you call for help? Should you immediately disable all user services and network connections? Can you disable the network if you're working in a cloud instance without blocking your own access? It's important to prepare for such events in advance.
- **Recovery** - Even if the breach has been contained and the impact on the business has been minimized, it is necessary to have the processes and systems in place to bring the system and services back to a fully operational state. It's important to understand the company's tolerance for failure during a breach and after it has been contained. Imagine that all the company's data is corrupted, including all online backups, in a matter of minutes. How can the company survive such a scenario? How much tolerance and downtime is an organization prepared to accept before the system is recovered from offline backups (if the backups still work)? Could your business survive if you had to reinstall all servers and network configuration? If so, how long would it be before your customers went elsewhere?

For the aerospace industry and its supply chain, the following safety measures are recommended as a baseline:

3.1 Identify

The following safety tips are recommended to help an organization's decision-makers:

- Have a safety policy officially signed by management and made available to all employees.
- Appoint a security manager (who can be part-time for SMEs) with the appropriate resources (budgets, staff, skills and skills maintenance).
- Maintain an inventory of critical data, equipment and software on your network, and allow only authorized assets to be used.
- Establish and apply a risk-based information classification and protection system.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

We recommend that you avoid the terms "RESTRICTED, CONFIDENTIAL or SECRET" in your organization when defining your classification levels for commercially sensitive data, as these terms are generally used for national security/government type information. Consider terms such as "commercially confidential, internal, private, sensitive personal data, limited distribution, publicly accessible" and consider systematically applying the convention in your documents and information systems.

- Know your key suppliers and impose appropriate security requirements on them.

  Understand the nature of shared responsibility between you and your suppliers, and which models (if any) are appropriate for your business and services. Determine whether additional measures are needed to reduce risk and help the company decide which models and suppliers to use (in-house, outsourcing, additional requirements, penalties or monitoring), including suppliers' security maturity, location and service models.

- Check relevant regulations and laws such as export controls and personal data protection.
- Take measures to protect know-how, sensitive data (plans, patents) and intellectual property. These measures apply to the organization and to partner/customer assets that are not patented or subject to export control.

3.2 Protect

The following security tips are recommended to help an organization's decision-makers:

- Ensure the identity and integrity of individuals when recruiting.
- Reduce the risk of human error, theft, fraud or misuse of facilities.

  Ensure that users are aware of information security threats and issues, are equipped and trained to support the company's security policy as part of their normal work, minimize the damage caused by security incidents and malfunctions, and learn from them.

- Prevent unauthorized access, damage and interference with company premises and information.
- Prevent the compromise or theft of information and material assets.
- Implement a fire safety system that takes into account the company's risks.
- Ensure that all users of the network and IT devices have a unique individual identifier and use a strong password.
- Control access to systems and information, particularly for customers, according to user functions.
- Strictly enforce end-to-end lifecycle management of all users and administrators (including access removal/deregistration).
- Use strong authentication (e.g. multi-factor authentication) to connect to clients or remotely from outside the network.
- Crypter tous les appareils mobiles et les connexions réseau qui transportent des données confidentielles ou liées aux clients.
- Ensure that anti-intrusion and anti-virus mechanism templates/signatures are regularly updated on all devices, including mobile devices.
- Ensure that formal change control procedures are in place within the IT organization.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

- Make regular backups of data and software, and store them physically and securely away from production systems.
- Ensure that IT equipment is regularly patched and tested.
- Deploy security patches at regular intervals, monitor critical vulnerabilities and apply mitigation measures.
- Ensure that systems and processes are regularly audited for security effectiveness.

3.3 Detect

The following security tips are recommended to help an organization's decision-makers:

- Have the tools and personnel necessary for security incident prevention, rapid and effective detection and response.
- Control the protection of network infrastructure (Active Directory, firewalls, proxies, intrusion detection, antivirus systems, etc.).
- Monitor and audit critical assets.

3.4 React

The following security tips are recommended to help an organization's decision-makers:

- Establish and test effective procedures for identifying, analyzing and responding rapidly to system vulnerabilities and security incidents.
- Ensure that a crisis management organization and defined procedures for handling major events are in place.
- Ensure ongoing collaboration with customers in the event of security incidents affecting their information or systems, and share information on threats.
- Have "critical contacts" and consider "in principle" or "cooperation" agreements in advance. These agreements enable rapid access to internal and external experts in the event of a breach.

3.5 Recovery

The following security tips are recommended to help an organization's decision-makers:

- Ensure that business continuity management procedures and processes are in place to guarantee a rapid return to a state of normal operation.
- Ensure that adequate disaster recovery planning and procedures are in place to preserve the confidentiality, integrity and availability of systems and information in the event of a major IT disaster.

  Consider scenarios such as a system-wide "cyberpandemic" or ransomware attack.

- Examine the incident after the event, analyze the lessons learned and take appropriate measures to prevent a recurrence.
- Periodically test and verify processes and readiness to deal with a potential incident.

Amphenol Air LB – 2, rue Clément Ader ZAC de WE – 08 110 Carignan – France – Tél. 0324227849 - Fax. 0324227875

Amphenol Air LB

Your Satisfaction. Everyday. Everywhere.