

Baxa Corporation

Preventing Cyber Attacks
Technical Paper

This document provides a discussion of Baxa Corporation's policy regarding cyber vulnerability of its products and methods for safeguarding those products from potential attack.



Baxa Corporation
14445 Grasslands Drive
Englewood, CO 80112

tel: 303-690-4204
fax: 303-690-4804
www.baxa.com

Introduction

Baxa Corporation provides several products that may be susceptible to attack by malevolent software if appropriate actions are not taken to properly safeguard them. The following white paper discusses Baxa Corporation's policies relating to product security and safeguarding.

Background

Baxa Corporation distributes multiple products that are hosted on Microsoft®-based operating systems. Our products alone do not perform operations that are suspect, nor do they perform operations that can be taken advantage of by opportunistic software. However, it is common knowledge that Microsoft operating systems, and certain applications that reside within these operating systems, are susceptible to cyber attacks.

Baxa provides applications on two types of computer platforms: desktop personal computers and embedded computing devices. Both platforms have Microsoft operating systems. Baxa does not build or validate our products with cyber security (antivirus) software installed.

It is important to note that the majority of cyber attacks occur through the following means:

- 1) Users copy an infected file from a portable memory device, e.g., CD, magnetic media, solid state media, USB drive.
- 2) Infected files are transmitted via access to the Internet through a Web browser.
- 3) Electronic mail applications may transmit infected files.
- 4) Infected files can be shared through connections between computers on a network.

Policy Regarding Installation of Non-Approved Software on Baxa Products

Baxa products have been verified and validated only with the software that was installed, by Baxa, on that product. Thus, any changes to the original, validated image, including installation of antivirus software, nullifies the validated state and would therefore constitute off-label use of that product.

As an FDA-regulated manufacturer, Baxa Corporation will not/cannot support nor endorse off-label use of its products. Only validated systems are approved by Baxa as being safe and effective for use. Any unauthorized programs installed on a Baxa product will void the manufacturer's warranty.

In addition, Baxa does not regularly install operating system updates or patches, generally published by Microsoft, on our devices. Similar to antivirus software, installing any software, including OS updates, on Baxa devices may change the operating parameters and adversely affect the operation of the device, rendering it unsafe to use. Baxa products have been validated only with the operating system and patches installed by Baxa.

Protecting Baxa Devices from Cyber Attacks

The following precautions, in conjunction with a network security policy, will minimize viruses from infecting any Baxa devices, and the network to which they are attached.

- The device should be used only in accordance with its intended use and not for email, Internet access, file sharing or other non-approved use. No software of any kind should be installed on the device unless approved, in writing, by Baxa.
- Some Baxa devices contain CD-ROM drives or USB ports to permit transfer and capture of data. **Confirm all media is virus-free prior to use.**
- The device should not be connected directly to the facility network, but should be installed behind a firewall that provides a protected subnet for the device. Configuring the firewall to shut down HTTP ports is also recommended.
- The device should not be accessible from the network.

NOTE: The device will only reach out to the facility's network to collect text-based .PAT files, back up device databases or to issue a print job.

Conclusion

Baxa products are provided on platforms that may be subject to cyber vulnerabilities. However, with adequate precautions to protect both the devices and the networks from these vulnerabilities, as noted above and prescribed by individual organizational policies, the devices should remain safe from cyber attacks while maintaining their validated functionality as delivered.