ZEBRA

Best practices for securing **enterprise data and devices**

With security breaches so prevalent today and cyber attacks occurring on a wider variety of devices, enterprises are more vulnerable than ever. This puts them in a vexing situation. As demand for convenient access to data, devices and systems grows, so too does security risk. Fortunately, enterprises can apply best practices to strike a balance between essential enterprise security and workforce productivity.

Increasing connectivity opens the door to opportunity and risk

Today, there is little patience for unconnected, unintelligent devices that don't flex to interact with mobile systems. But modern connectivity, mobile integration and device intelligence capabilities have consequences. Greater connectivity can bring more opportunities for security attacks. The proliferation of intelligent mobile devices can distribute these cyber attack points outside of the enterprise environment, threatening a company's reputation, finances, compliance and legal standing.

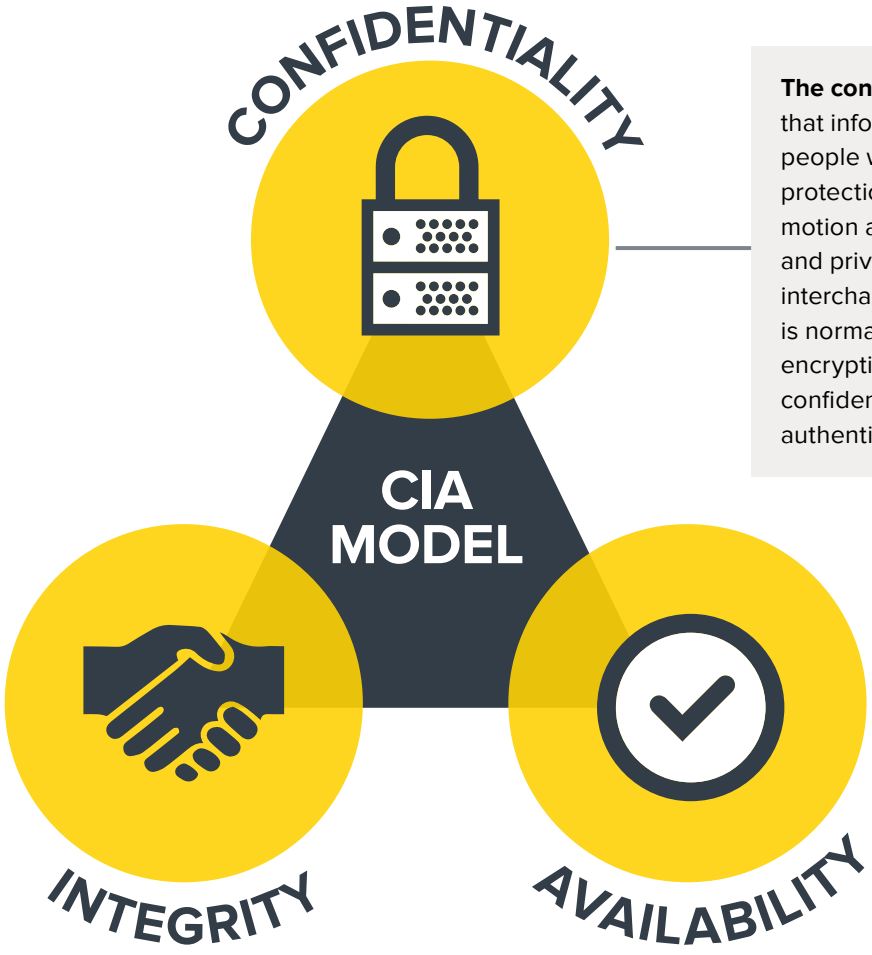
With the spate of data breaches and cyber threats, security is top of mind for enterprises. Companies can harden their security posture and safeguard confidentiality with the best practices found in this document.

Source: *The IDC Worldwide Semiannual Security Spending Guide,* IDC, Oct. 12, 2016

When businesses think of devices that require protection and enhanced security, they usually think of smartphones, laptops, tablets, PCs and IoT devices. They seldom include thermal barcode printers, despite the fact that they are often connected to an IT network and are, undoubtedly, indispensable to the everyday operation of many industries. All enterprise devices, and the data they convey, need to be sent out into the world bound to a well thought out set of enterprise data and device best practices.

The confidentiality, integrity and availability (CIA) model

Fortunately, there is a well-established reliable model and best practices that can be easily applied to minimize risks. The CIA model provides a guiding framework when considering how to reasonably and effectively raise the bar on risk mitigation. The model can be applied to all devices that utilize the data protected by enterprise information systems, from the more traditional connected solutions to the new players in the connected environment, such as intelligent thermal barcode printers. It includes three components:



The concept of confidentiality is to ensure that information is only available to the people who are authorized to access it. This protection applies equally to data at rest, in motion and during processing. Confidentiality and privacy are sometimes used interchangeably; however, confidentiality is normally an extension of privacy. Data encryption is a common method of ensuring confidentiality, as are various methods of authentication for authorization.

The concept of data integrity is to ensure consistency, accuracy and trustworthiness of the data over its entire lifecycle. It also means that when a file is stored and then accessed at a later time, there will be certainty that the data has not been directly or indirectly altered by an unauthorized entity while in storage. Access controls can prevent unauthorized access and checksums (CRC), cryptography (hashes) and digital signatures can be used to validate integrity.

The concept of availability is to ensure that the resource/device is available when the user needs it. This can include keeping the resource/device online and rigorously updated to prevent attacks that affect the stability of the device. Some of the responsibility for availability also relies upon the host that the resource/device is connected to and also how it is connected (wired/Wi-Fi™). Business critical resource/devices need to be available when needed; otherwise, a plan needs to be in place to replace the devices and reduce downtime.

Common concerns

Across all device types, there are some common areas and issues to consider when applying these concepts. Creating well protected systems is the goal, but so is moving devices from the “easy target” to “not worth the time” category for someone with bad intentions. Even when the user has good intentions, inadvertent user actions can create havoc with devices that are not adequately protected. Therefore, it is highly advisable for organizations to undertake preemptive measures to increase device protection and prevent data breaches. This certainly includes thermal barcode printers; companies should identify potential threat vectors and apply appropriate protocols as they would to any other device.

Encrypt all connections

How devices will connect should be an early point of planning. Many devices can connect to your network, but how they connect matters. It’s very common to apply password and encryption technology to wirelessly connected devices, but even your wired/Ethernet connected devices may need encrypted or authenticated connections, dependent on what type of information they handle. Long term, it’s expected that most, if not all connected devices, will use an encryption and authentication technology, even if they are not directly handling business critical information. If they’re connected to your network, even the most simplistic devices should be “good network citizens” by applying these confidentiality and availability concepts.

Rotate credentials

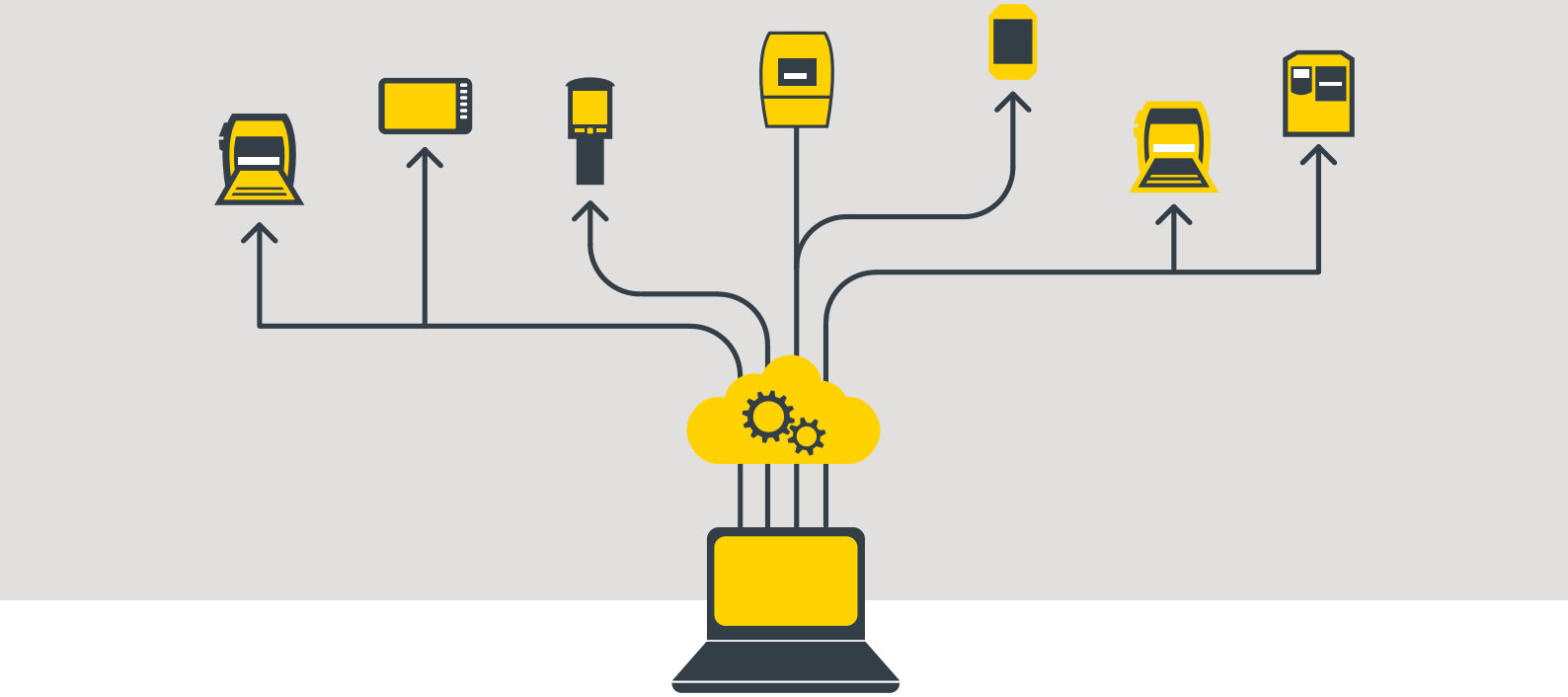
Where possible, organizations should treat devices as you would any person logging into your network. In practice, this means using a credential and authentication system to ensure that the devices that make it onto the network are authorized to be there. Additionally, just as you would rotate user passwords, keys and credentials for your staff, plan to do the same with your devices, including thermal barcode printers. Device credential rotation can be made easier by using a centralized device management system to ensure that updates align with production schedule needs. In this way, both devices and data can be available, but also contribute to overall system confidentiality.

Protect access

Device default settings should be carefully considered. Typically, device designers prioritize ease of use over fortifying device access by default. Many devices sit out in open areas, with access to their settings open for all to use. This can make the device easy to use, but also tempting for misuse. Moving to some form of protected access is an easy first step to consider. Even activating a simple, front panel, password system can make a meaningful difference in both confidentiality and availability.

Monitor communication methods

Many devices offer multiple communication methods. For example, it’s normal for a device to have a web page that administrators can log into and make changes to device settings. Other common network services include FTP, SNMP and SMTP. While these services can enhance the access or manageability of the device, if they aren’t being used, you may want to consider shutting them down. In some cases, it may be possible to control them via a remote device management system.



A closer look at remote device management systems

With connected devices, it is common to use a remote device management system. This can take the form of an application that can connect to and alter settings on one or more devices, or the form of embedded web pages that can control settings. Even simple and single changes to settings can greatly impact production processes—up and down stream. Remote management systems can considerably improve IT productivity, but they should be carefully controlled in terms of access and permissions.

An example of this could be the need to implement a new configuration setting across 5,000 thermal barcode printers. With printers scattered across different sites, IT staff limited and uptime a priority, a centralized and flexible management solution is essential.

Perform regular updates

Access is not the only important consideration when using remote management systems. Timing and scheduling are important areas to consider. Regular updates are a hallmark of a well maintained system, but not everyone needs to know how often those updates are performed. Communication about scheduled updates should be limited to those who need to be aware of them. Many of these updates are associated with device capability changes that should be kept confidential in both scope and content. Users only need to be informed of device availability. How and when devices are updated should be disclosed on a need-to-know basis.

Keep track of your devices

As intelligent devices become more and more geographically distributed in your organization, they are no doubt helping improve your productivity in multiple areas. At the same time, knowing where they are can become a daunting task. Early planning for the later need to keep and maintain an accurate device census can pay off in the long run. Being able to spot devices that are actually still on your network is a core concern. Consider using a device naming scheme, right from the start, that allows you to later easily inventory your widely distributed devices. Use a device management system that allows you to track device “check in” times – so that you can spot devices that are offline for longer than they should be. As you identify devices that have gone missing, withdraw their credentials until their status is determined.

Device lifecycle

CONSUMER-GRADE MOBILE DEVICES

ENTERPRISE-GRADE MOBILE DEVICES

ENTERPRISE-GRADE PRINTERS

Extend the value of long lifecycles

Consider the long life of some industrial devices. While some may last just a couple of years, others might be on your network much longer; this is frequently the case with thermal barcode printers. During that time, your network standards are likely going to change. Pick devices that have the ability to be updated over time, so that they can be kept current with changing standards. Choose a supplier of thermal barcode printers who can deliver intelligent printers that are easy to update during the course of their lifecycle. A device OS update can bring with it significant device enhancements and new capabilities, extending and expanding the unit's value. At the same time, OS updates also represent a moment when integrity must be carefully considered. Device update methods should use some form of digital signature or checksum to ensure that the OS file(s) being applied to the device contains what it is meant to contain.

Ensure safe device retirement

One last item to plan for – device retirement. Even the most dependable devices someday reach that moment when it's time to remove them from the production system. They may be resold, turned in as part of a trade-in program or kept for their parts – but they should not be allowed to retain entrprise information they used during their time in production. As devices retire, it's time to apply all aspects of the CIA model. Keep your information confidential by deleting any files or settings that might be stored on the unit. Maintain overall system integrity by withdrawing any credentials or user accounts you might have created for them. And, finally, check that none of your systems are hardcoded to continually search for or attempt to use the retired devices, so that no one can simulate the older device for inappropriate purposes.

Common sense best practices

These considerations and common concerns are part and parcel of today's connected device world. Being aware of them is the first step. Applying both common sense best practices and the CIA model to all your devices—without forgetting thermal barcode printers—are the next steps. Use this checklist as a planning guide:

1	Start early. Plan for incoming devices and how you'll protect them.
2	Use encrypted and authenticated connections where possible.
3	Plan to rotate access passwords, access keys and authentication credentials.
4	Defaults typically represent documented methods to access a device. Activate user interface passwords and consider turning off the device services that you don't plan to use.
5	Leverage a remote management system to allow you to quickly update settings and standards. The longer devices are using out-of-date settings, the longer they become an easier target.
6	Keep update schedules and plans only in the hands of those who need to have them. Knowing when updates are planned can inadvertently encourage inappropriate actions.
7	Plan for a method to continuously monitor your system for "out of touch" devices. Where you suspect a device has been taken out of your environment, withdraw its credentials until the device status is determined.
8	Choose devices that can be updated across their long service lives, so they keep current with new standards. Verify that the updated system uses a method to ensure the updated file hasn't been tampered with.
9	Plan for device retirement by removing enterprise system settings, deleting device user accounts/credentials, and checking to make sure the existing system isn't hardcoded to look for retired devices.
10	Consider confidentiality, integrity and availability during all stages of the devices lifecycle.

Why Zebra

Zebra has been giving physical objects a digital voice for over 40 years, interconnecting systems and solutions to offer real-time, actionable insight. With a commitment to an enterprise asset intelligence (EAI) strategy that brings IoT opportunities to reality, companies gain deep visibility into the performance—and security—of their data, devices and operations.

What is essential in protecting data and infrastructure is equally vital in protecting thermal printers. They are not only a portal to an enterprise's network and data, but also an industry workhorse that handles an enormous range and number of transactions each day. With every label, tag, receipt or card printed, core business processes move forward, as data is collected, sorted, and transported throughout enterprise systems.

That is certainly true of Zebra's thermal printers. Users depend on our printers' reliability, performance and precision for millions of transactional events each day. They also look to our printers to actively ensure the integrity and protection of their data and infrastructure.

That's why we build our printers on a secure foundation of Print DNA—a suite of tools that carefully control each connection and data exchange to safeguard information and grant access to only authorized users.

Our latest printer operating system, Link-OS® v5, features PrintSecure. With PrintSecure, companies can encrypt connections, allow only permitted access and regularly update their thermal printers to address new threats. Now, they can leverage the data that flows through their thermal printers for decisive insight.

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
+1 847 955 2283
la.contactme@zebra.com