ZEBRA CAPTURE YOUR EDGE

Security Best Practices

These considerations and common concerns are inherent in today's connected device world. Being aware of them is the first step. Applying these common-sense best practices to all your connected devices is next. Use this checklist as a planning guide.

1. Start Early

Plan for incoming technology, and how you'll protect it.

2. Protect Data

Use encrypted and authenticated connections where possible.

3. Control Services

Consider turning off the technology services that you don't plan to use.

4. Change Passwords

Using default passwords makes it easy for hackers to access devices. Activate User Interface Passwords.

5. Remote Management

Leverage a secure remote management system to allow you to quickly update settings. The longer devices, solutions and systems use out-of-date settings, the easier targets they become.

6. Enable Activity Logging

Use activity and audit logs when available to detect bad behavior.

7. Need To Know

Keep update schedules and plans only in the hands of those who need them. When too many employees know about update plans, the odds of security breaches increase.

8. Monitor OOT Devices

Develop a method to continuously monitor your system for "out-of-touch" devices. When you suspect a device has been removed, withdraw its credentials until you can confirm its location.

9. Updateability

Choose devices that can be updated across their long service lives to keep current with new standards. Make sure update systems can prevent update file tampering.

10. Device Retirement

Plan for device retirement by removing enterprise system settings, deleting device user accounts/credentials, and checking that existing systems aren't hardcoded to look for retired units.

11. C.I.A.

Consider "Confidentiality," "Integrity" and "Availability" during all stages of the device's life cycle.

12. Continous Planning

Updates to security practices should be an ongoing priority. Security planning is not a one-time event.

Did You Know?

$360,000

Encryption minimizes data breach costs by an average of **$360,000**, making it the most effective hacking countermeasure.[1]

81%

The use of stolen or weak passwords accounted for **81%** of hacking-related data breaches.[2]

$1.2 Million

Companies that have data breach incident response teams and test response plans reduce the cost of a breach by more than **$1.2 million.**[3]

38%

of firms reported security incidents involving enterprise devices.[4]

40%

say cyber attacks are a factor increasing the importance of securing mobile devices.

197 Days

It takes an organization an average of 197 days to realize that a data breach has occurred.[5]

[1] Cost of a Data Breach Report 2019, IBM Security • [2] 2017 Verizon Data Breach Investigations Report, IBM Security • [3] Cost of a Data Breach Report 2019 • [4] Carbon Black Incident Response Threat Report, November 2018 • [5] 2018 and 2019 Cost of Data Breach, Ponemon Institute