

Cybersecurity guidelines for building automation systems.

Cybersecurity threats present a challenge to the normal functioning of critical infrastructure both nationally and globally. Staying up to date on cybersecurity best practices and taking proactive steps to prevent breaches can help your company avoid incidents or at least minimize their impact. At Trane, we align our approach to cybersecurity with National Institute of Standards and Technology's (NIST[®]) "Framework for Improving Critical Infrastructure Cybersecurity" ¹Although every company and industry is different, following these general guidelines and steps can help your organization better position itself to prevent or recover from cyberattacks.

¹NIST site <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-1.1-its-popular-cybersecurity-framework>



5 steps to improving organizational cybersecurity.

Identify:

Identify all the assets in your building (building automations systems /IoT devices equipped in the network). Assess your risks. Understand your organizations cybersecurity strengths and weaknesses. Identify where risks and opportunities to improve may lie.

Protect:

Proactively act on your assessment and protect your assets. Implement safeguards to reduce risks such as preventative procedures, equipment/ technology updates, staff training, etc.

Detect:

Enact activities such as continuous asset and network monitoring to detect the occurrence of cybersecurity events as early as possible.

Respond:

Develop a set of response planning and mitigation strategies. These might include efforts to contain or minimize impact, analysis, and assessment of the incident and its impact on the organization.

Recover:

Outline recovery processes, business continuity procedures and best practices to ensure timely restoration of building systems or assets affected by cybersecurity events to return to normal operation as quickly as possible.

For more information, read the NIST Framework [here](#).

