SPIRE 2.0 CYBERSECURITY ASSESSMENT CRITERIA

Keeping Pace with the Evolving Cybersecurity Landscape

SPIRE 2.0 CYBERSECURITY ASSESSMENT CRITERIA

Keeping Pace with the Evolving Cybersecurity Landscape

CONTRIBUTORS:

David Brearley, HDR
Fred Gordy, Michael Baker International
Monica Kocyk, UL Solutions
Ken Kurz, COPT
Gale Moericke, Crux Solutions
Rebekah Morote, UL Solutions
Mike Regan, TIA
Jason Shaw, AECOM
Sudhi Sinha, UL Solutions
Marta Soncodi, TIA
Osman Saleem, Actimeta
Jon Williamson, JCI

INTRODUCTION

Smart buildings encompass an ever-increasing number of connected operational technology (OT) and information technology (IT) systems and devices that provide actionable insights into building performance. These insights enable data-driven decisions that increase efficiency, optimize operations, mitigate risk, and enhance overall occupant well-being for significant cost savings, improved sustainability, and higher asset value. As OT and IT systems connect more devices and converge via open, interoperable IP-based protocols to support smart building initiatives, they are increasingly at risk for cybersecurity and ransomware attacks that can halt facility operations, require significant remediation costs, and even put lives at risk.

In a coordinated effort with numerous industry experts, the Telecommunications Industry Association (TIA) and UL Solutions launched the SPIRE™ smart building assessment and rating program in September 2020. The SPIRE program consists of an expertly curated, objective, and holistic framework that sets forth technology-agnostic metrics to gauge the ability of a building's systems, processes, and infrastructure to optimize across six major criteria of a facility's function: power and energy, health and well-being, life and property safety, connectivity, cybersecurity, and sustainability. The SPIRE program includes a free online self-assessment for building owners and operators to easily gain insight into their building performance related to the six key aspects. It also has a verified assessment component that results in a rating and detailed recommendations through a performance improvement roadmap.

Since the launch of SPIRE, initial pilot programs, and the development of Version 1.5 assessment criteria, there have been significant changes in industry and market trends. Cybersecurity is a key area of focus for smart buildings due to an expanding threat landscape. Attacks have become more frequent and sophisticated, fueled by geopolitical unrest, global economic uncertainty, and increased digitization that generates more data and increases network entry points.

As industry standards-making bodies, TIA and UL continually evaluate and improve programs and standards to meet real-life business needs in parallel with the latest market trends, technologies, and the global economy. Changes in the cybersecurity landscape, combined with objective feedback from multiple SPIRE Version 1.5 verified assessments and program participant expertise, have called for TIA and UL Solutions to redesign the SPIRE smart building assessment criteria for cybersecurity. This paper overviews cybersecurity market shifts, trends, and global regulations and initiatives impacting today's smart buildings. It also outlines how the new SPIRE Cybersecurity Assessment Criteria Version 2.0 addresses these impacts and provides an improved building-centric and streamlined approach to facilitate a more effective and efficient cybersecurity assessment process.

THE EVOLVING SMART BUILDING CYBERSECURITY LANDSCAPE

Globally, cybercrime has increased drastically over the past four years. This is due in part to geopolitical unrest with fragile international relations, economic uncertainty with high inflation and interest rates, and the COVID-19 pandemic that triggered a rise in e-commerce, remote learning, work-from-home policies, and telemedicine. It also has much to do with increased digitization with more connected devices that are often unprotected. In 2020, the US FBI reported a 300% increase in reported cybercrimes since the onset of the pandemic.[1] 2022 saw a 38% increase in global attacks compared to 2021, with Q1 2023 and Q2 2023 experiencing additional 7% and 8% respective increases in average weekly attacks compared to 2022.[2] The convergence of OT and IT systems and emerging IoT and cloud-based technologies makes smart buildings particularly vulnerable.

OT/IT CONVERGENCE IS INCREASING THE THREAT

Building operating systems today are rapidly shifting away from legacy protocols and closed infrastructure with limited data to more open, connected OT systems. Smart building devices collect, transmit, and act upon a wide range of critical and sensitive information, such as personal biometric information used for access control, air quality readings in an HVAC system, or fire suppression settings in life safety systems. Many new smart OT devices and sensors also handle data needed for buildings to meet evolving ESG initiatives and comply with local codes, regulations, and insurance requirements.

The increasing rate at which OT systems are converging with IT networks to transmit information to advanced centralized building management systems and cloud-based platforms for remote operations, data analytics, and reporting is gaining the attention of cybercriminals. The use of new IoT technologies to supplement older legacy OT systems with limited

security controls is especially a concern. The narrowing gap between IT and OT also provides an opportunity for a cyberattack on one to enable a cyberattack on both. According to a 2023 OT Cyber Threats Report, 2022 saw a 140% surge in OT cyberattacks, with most attacks resulting in ransomware that primarily encrypted critical IT network systems.[3]

In addition to vulnerabilities that come with OT/IT convergence, cybercriminals are increasingly targeting OT systems due to how vital they are to maintaining operations and organizations' willingness to pay higher ransomware demands. Skilled workforce shortages in OT security and historical gaps between IT and OT departments that historically operated in silos also often result in IT-centric approaches, lack of team collaboration, and functional differences that can lead to inadequate OT system management and maintenance (e.g., threat detection, software patching, user access, asset visibility, etc.).

OT ATTACKS ARE CAUSING REAL-WORLD CONSEQUENCES

While attacks on IT systems primarily target sensitive data and can result in significant financial losses and damaged reputations, cyberattacks on OT building systems can have physical consequences, such as building shutdowns, outages, leakages, or even explosions. They can even impact the safety and lives of building occupants, which is an enormous liability for building owners and operators. While threats to OT systems were primarily theoretical before 2020, consequential attacks have more than doubled annually.[4]

Attacks on OT systems in a smart building can have more detrimental consequences when the facility is considered part of a critical infrastructure sector whose assets, systems, and networks are vital to national security, the economy, or public health and safety. The US federal government

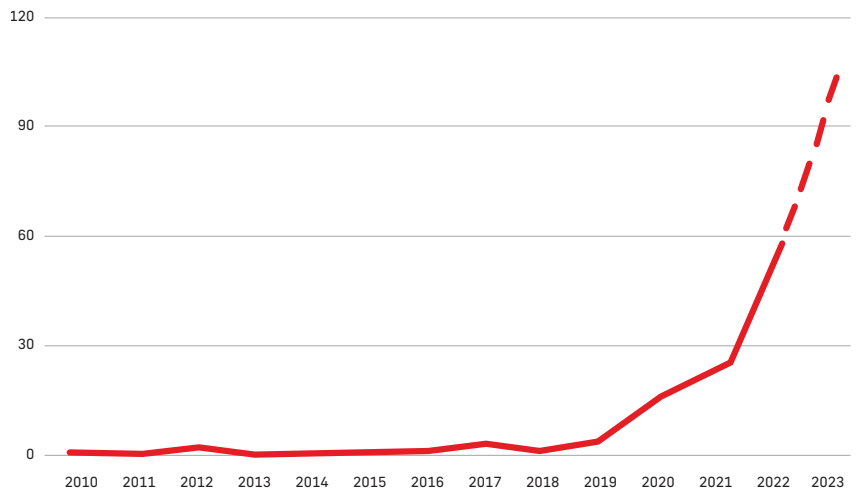

Figure 1: Consequential OT Cyberattacks. Source: Waterfall Security Solutions

defines 16 critical infrastructure sectors, including commercial facilities where people gather (e.g., stadiums, arenas, casinos, retail centers, amusement parks, and hotels.) and commercial real estate (office and apartment buildings, MDUs, and mixed-use facilities). Critical sectors also include healthcare (e.g., hospitals and clinics), financial services (e.g., banking, insurance, and trading), transportation (e.g., airports, railroads, and trucking), energy (e.g., utilities, fuel), water and wastewater, emergency services (e.g., police, fire, and public safety), food and agriculture, and information technology.[5]

EMERGING TECHNOLOGIES ARE EXPANDING THE CYBERATTACK SURFACE

An ever-increasing range of connected IoT devices and sensors deployed in smart buildings enable everything from energy and resource metering, space optimization, and predictive maintenance to environmental monitoring and control, asset tracking, life and property safety, and more. These devices create more entry points into OT and IT systems, expanding the cyberattack surface.

IoT devices are typically customized for specific functions with limited computational ability that can technically and financially inhibit incorporating adequate security measures. They also comprise many software and hardware components from a wide range of vendors across a vast global supply chain that rely heavily on third-party open-source software at greater risk for gaps in poorly written or undermanaged code. Due to these vulnerabilities, cybercriminals increasingly regard IoT devices as low-hanging fruit to access and exploit. High-risk vulnerabilities in IoT-related code bases jumped 130% over the past five years, with the first two months of 2023 alone seeing a 41% increase in attacks targeting IoT devices compared to 2022.[6]

With more IoT devices and sensors come various cloud-based solutions leveraging open-source code to enable integration across diverse workloads. Open-source software vulnerabilities,

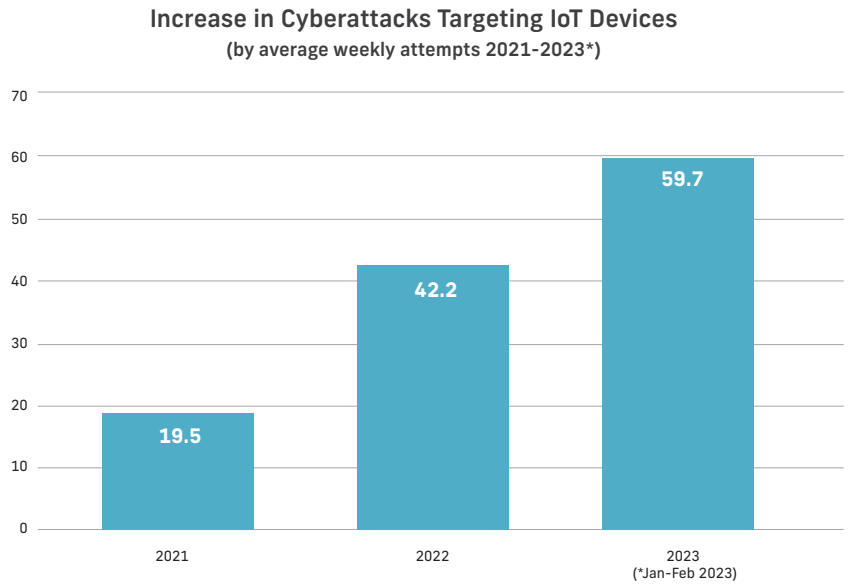

Figure 2: IoT devices are increasingly being targeted by cybercriminals

misconfigurations, storage of large data sets, and lack of access restrictions are giving rise to more cloud-based security threats. Cloud exploitation cases grew by 95%, and nearly 40% of businesses experienced data breaches in their cloud environments in 2022.[7] While cloud providers are using emerging technologies like artificial intelligence (AI) and machine learning (ML) to help identify anomalies to detect malicious activity and software-related weaknesses, cybercriminals are also now leveraging these technologies to scan for vulnerabilities, automate malware, crack passwords, analyze stolen data, and formulate content used in social engineering attacks.

CYBERSECURITY REGULATIONS AND STANDARDS ARE BECOMING MANDATORY

Increasing cyberattacks and an expanding attack surface have given rise to several government, corporate, and industry initiatives based on various international cybersecurity standards and frameworks. Several of these initiatives call out the need to comply with the latest National Institute of Standards and Technology (NIST) standards, including NIST Cybersecurity Framework (CSF), NIST 800-82 Guide to Industrial Control Systems (ICS) Security, and NIST 800-53 Security and Privacy Controls for Information Systems and Organizations. Others may require compliance with standards from International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), UL Solutions, TIA, or others.

Many new initiatives are becoming mandatory, with several now adopted as legislation and required by law. According to the UN Conference on Trade and Development (UNCTAD), over 80% of countries have enacted cybercrime legislation, with another 5% having draft legislation.[8] In the US, at least 40 states introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity, with 24 states enacting 41 bills in 2022 alone.[9] Examples of key federal legislation include the following, with several more on the horizon:

- **US IoT Cybersecurity Improvement Act** of 2022 sets minimum security standards for IoT devices procured and used by the federal government
- **In July 2023, the Securities and Exchange Commission (SEC)** mandated all public companies to report cybersecurity incidents and disclose corporate governance and risk management
- **EU Cybersecurity Act** established a mandated certification framework for all information and communications technology (ICT) products, services, and processes.
- **EU NIS2 Directive** requires essential entities to manage cybersecurity risk, minimize the impact of potential incidents, and disclose vulnerabilities
- **EU Cyber Resilience Act (CRA)** sets requirements to protect consumers and businesses purchasing or using any products or software with a digital component

Cybersecurity is also becoming a key component of corporate governance under environmental, social, and governance (ESG) frameworks, requiring policies and procedures with oversight and reporting related to procurement, risk assessments, incident management, response, and disaster recovery. Complying with growing legislation and governance requirements places more pressure on smart building owners and operators.

At the same time, industry standards addressing cybersecurity are expanding their scopes to include coverage for emerging technologies, supply chain risk management, and governance. In 2020, UL released the Methodology for Marketing Claim Verification 1376 with a security verification and labeling solution for IoT products. The 2023 release of the NIST CSF 2.0 added the function of governance to its historical five main pillars of identify, protect, detect, respond, and recover. It also added 10 specific requirements for supply chain security risk management. TIA recently released the latest version of its SCS 9001 Supply Chain Security Management standard with expanded coverage for any technology and improved support for government policy and legislative requirements.

SPIRE 2.0 CYBERSECURITY ASSESSMENT CRITERIA RESPONDS

Based on the evolving cybersecurity landscape and feedback from multiple SPIRE Version 1.5 verified smart building assessments and program participant expertise, TIA and UL Solutions have significantly redesigned the SPIRE smart building assessment criteria for cybersecurity. SPIRE Cybersecurity Assessment Criteria Version 2.0 provides an improved building-centric approach to more closely address requirements and performance related to the built environment, including expanding OT exposure and the vulnerabilities that come with OT/IT convergence. The updated criteria also consider growing governance requirements from a global perspective with support for international standards and frameworks while adding clarification and context to streamline the assessment process.

SPIRE Version 2.0 cybersecurity assessment criteria are structured as question-and-answer sets, grouped by category into the following sections that provide a high-level yet straightforward framework that is technology and standards agnostic:

- **Governance:** Policies, procedures, and oversight to ensure effective smart building cybersecurity
- **Assets:** Identification and protection of critical assets, including data, networks, devices, hardware, and software
- **Architecture:** Design and configuration of cybersecurity infrastructure, networks, systems, and technologies
- **Access:** Management of access controls for users and systems, including authentication, permissions, account management, and authorized access

The following are examples of how SPIRE Cybersecurity Assessment Criteria Version 2.0 responds to the evolving cybersecurity landscape within each criteria category.

GOVERNANCE

SPIRE Cybersecurity Assessment Criteria Version 2.0 considers governance by documenting roles, policies, and procedures, including risk assessments for critical systems, change control, training, and incident response. The criteria address the vulnerabilities that come with gaps between IT and OT roles by considering users, assets, and policies related to smart building systems across IT and OT environments.

ASSETS

SPIRE Cybersecurity Assessment Criteria Version 2.0 addresses cybersecurity for all building assets, including the procurement, management, and maintenance of devices and systems. This includes supply chain security considerations to ensure that smart buildings are protected from cybersecurity risks from external vendors, such as open-source software used in IoT devices, systems, and platforms. The criteria respond to vulnerabilities that come with IT/OT convergence by addressing the need for proper firmware updates, obsolescence monitoring, backups, and compliance with standards, legislation, and corporate requirements. The criteria don't just address those deploying and operating smart building systems and devices but also the vendors that supply them.

ARCHITECTURE

SPIRE Cybersecurity Assessment Criteria Version 2.0 addresses the configuration, documentation, and protection of building systems, networks, and data via encryption, regular vulnerability scanning, and conformance to recognized industry standards and best practices. The criteria explicitly address

the segmentation of various IT and OT functions to prevent an attack on one from impacting the other.

ACCESS

SPIRE Cybersecurity Assessment Criteria Version 2.0 addresses secure access to building systems and devices by ensuring that only individuals who need to have access are authorized to do so via user management policies and procedures such as multifactor authentication, policies regarding remote access, and thorough documentation that logs what asset is accessed, when, and by whom.

GET STARTED PROTECTING YOUR SMART BUILDING

As the cybersecurity landscape continues to evolve and grow, cyberattacks will become more frequent, sophisticated, and expensive. The global average cost of a single data breach in 2023 hit $4.45 million, with the total global cost anticipated to reach nearly $13 trillion by 2028.[10,11] Smart buildings are increasingly becoming the norm across all sectors, with OT/IT convergence and emerging technologies that offer significant advantages but also increase vulnerability and make ensuring proper cybersecurity more complex.

As a straightforward, agnostic, and streamlined framework for the built environment, SPIRE Cybersecurity Assessment Criteria Version 2.0 is an ideal tool for smart buildings to assess their risk and identify steps to bridge the gap between OT and IT that will help them address current and future vulnerabilities and comply with evolving government, industry, and corporate requirements. The enhanced cybersecurity assessment criteria, along with the other five assessment criteria of SPIRE—power and energy, health and well-being, life and property safety, connectivity, and sustainability—empowers smart building owners and operators to identify, prioritize, and optimize performance from a holistic perspective that results in significant cost savings, improved sustainability, and higher asset value.

SPIRE 2.0 with updated cybersecurity, connectivity, and sustainability assessment criteria is now available. Get started on the journey today with a quick, easy, and FREE of cost SPIRE Self-Assessment or contact us to learn more about how a SPIRE Verified Assessment can improve and optimize the performance and value of your building.

Interested in participating in TIA's Smart Building Program to help develop SPIRE holistic assessment criteria and shape the future of smart buildings? Contact us today at membership@tiaonline.org.

REFERENCES

1 FBI Internet Crime Complain Center (IC3), April 20, 2020.

2 Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks, January 2023

3 2023 Threat Report, ISSSTRIVE and Waterfall Security Solutions

4 2023 Threat Report, ISSSTRIVE and Waterfall Security Solutions

5 Critical Infrastructure Sectors, Cybersecurity & Infrastructure Security Agency (CISA)

6 The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally,Check Point Research, 2023

7 2023 Thales Cloud Security Study, Thales

8 UN Conference on Trade and Development (UNCTAD), Cybercrime Legislation Worldwide, 2021

9 Cybersecurity Legislation 2022, National Conference of State Legislatures

10 Cost of a Data Breach Report 2023, IBM

11 Estimated cost of cybercrime worldwide 2017-2028, Statista

TO LEARN MORE ABOUT SPIRE 2.0 CYBERSECURITY ASSESSMENT CRITERIA

CONTACT

membership@tiaonline.org

SBPWP1004