Shambliss Guardian

Protecting your critical building infrastructure:

SOLUTIONS HIGHLIGHTS

- Security Advisory and Assessment
- Security Strategy and Roadmap
- Traffic analysis and segmentation
- Asset Identification and Management
- Implementation and Transition
- Monitoring and Management
- Preparation of Due Diligence and Compliance Responses
- Security Posture Validation
- Governance, Risk Management , and Compliance (GRC)

Service Overview

Shambliss Guardian stands at the forefront of securing building automation systems (BAS), offering a robust suite of services tailored to safeguard commercial buildings from the ever-evolving threat of cyber-attacks. Our approach begins with a thorough environmental assessment, cataloging all devices and applications, and meticulously analyzing remote access points. We specialize in the segmentation of BAS devices from the internet, a critical step in fortifying the digital defenses of a building's infrastructure.

Understanding the nuances of Building Automation Systems (BAS) is essential to being able to secure them. These systems encompass a range of devices such as controllers, sensors, door locks, cameras, and HVAC systems. They are distinct from standard enterprise IT equipment. The increasing prevalence of cyber-attacks on these systems highlights their vulnerability and the dire consequences they pose, including loss of control, safety and breaches, as well as potential financial and reputational damage to property owners and tenants.

Shambliss Guardian's methodology is rooted in decades of industry experience, combining deep knowledge of the BAS and office industries to develop customized security solutions for your building. By integrating equipment, networks, firewalls, and operational processes with round-the-clock security monitoring and management, we ensure a resilient security posture that not only protects but also adds value to commercial properties. Demonstrable cybersecurity protections can be another advantage to enhance the desirability of your property.

Why Shambliss Guardian

In today's landscape, where security is paramount, Shambliss Guardian empowers building owners to confidently promote their premises as secure and well-prepared against cyber threats. Partner with us to craft a security strategy that not only defends against current threats but also anticipates and neutralizes future vulnerabilities. Together, we can establish a new standard in building security and tenant safety.

.

Security Advisory and Assessment

Shambliss Guardian starts by collaborating with the business, network, security, and building automation teams to determine the current state of cybersecurity protection. The assessment presents a high-level view of security solutions, processes, documentation, and monitoring. The business drivers, BAS, and communication needs will be incorporated into the definition of requirements. The advisory team will present business, operational, and cybersecurity current state and a recommendation for the outcomes required to meet governmental, compliance, and insurance requirements.

Security Strategy and Roadmap

Shambliss Guardian will work with you to align the initiatives to the desired outcomes. The strategy and roadmap will take a deeper dive into the current state of security. The roadmap is a detailed plan for the resolution of security gaps. It is critical that the roadmap be aligned with the prioritization, budget, and implementation timelines available. We work closely with you to ensure recommendations are actually implemented and your current protection applications are fully deployed.

Implementation and Transition

We coordinate with you to define project responsibilities for the BAS team and any required vendors. Installation and configuration of security solutions can take place without impacting production. The Shambliss Guardian team has decades of experience with strategic migration projects. We understand that uninterrupted operation of the building is critical. Proper planning, expertise, prearranged vendor support, and post-implementation support are all accounted for prior to the transition. We also recommend limiting the number of transition changes to minimize the complexity of troubleshooting.

Monitoring and Management

Cyber criminals do not rest when your team goes home for the night. Shambliss Guardian helps clients incorporate managed cybersecurity monitoring and incidence response services. Our cost-effective monitoring service is considerably lower than investing in equipment, software, and staffing for building security.

Security Breach Case Studies

Threat actors breached Target Corporation and gained network access through an HVAC system. If bad actors can get to your clients' networks though this threat vector, you could have liability to your clients.

Adversaries attacked the Las Vegas MGM casino through a fish tank connected to the internet. Blocking BAS systems from the internet and incorporating multifactor authentication (MFA) is critical to an efficient and demonstrable security posture.

The Lurie Children's Hospital breach rendered many of the network switches useless and unrepairable. The hospital lost ability to use phone, fax and computer networks, then they lost money from system downtime, replacement network switch purchases, and system reimplementation. For many in these situations, there are additional costs for paying ransom for data unencrypting and commitments not to publish private data.

Shambliss Guardian

200 N. Martingale Road
Suite 400
Schaumburg, IL 60173
P: 847-305-4887
E: dan.hansvick@shambliss-guardian.com

About Shambliss Guardian

Shambliss Guardian is a provider of cybersecurity solutions. We offer a complete portfolio of strategic services to help clients define their security programs, identify risks, deploy the right technologies, and ensure operational readiness to respond to threats and breaches. Our extensive hands-on experience enables us to create a comprehensive set of security solutions that target the most pressing information security issues such as Security Assessments, Incident Response, Penetration Testing, Security Awareness, and Tabletop Exercises.