SECURITY EXECUTIVE COUNCIL
A research and advisory firm

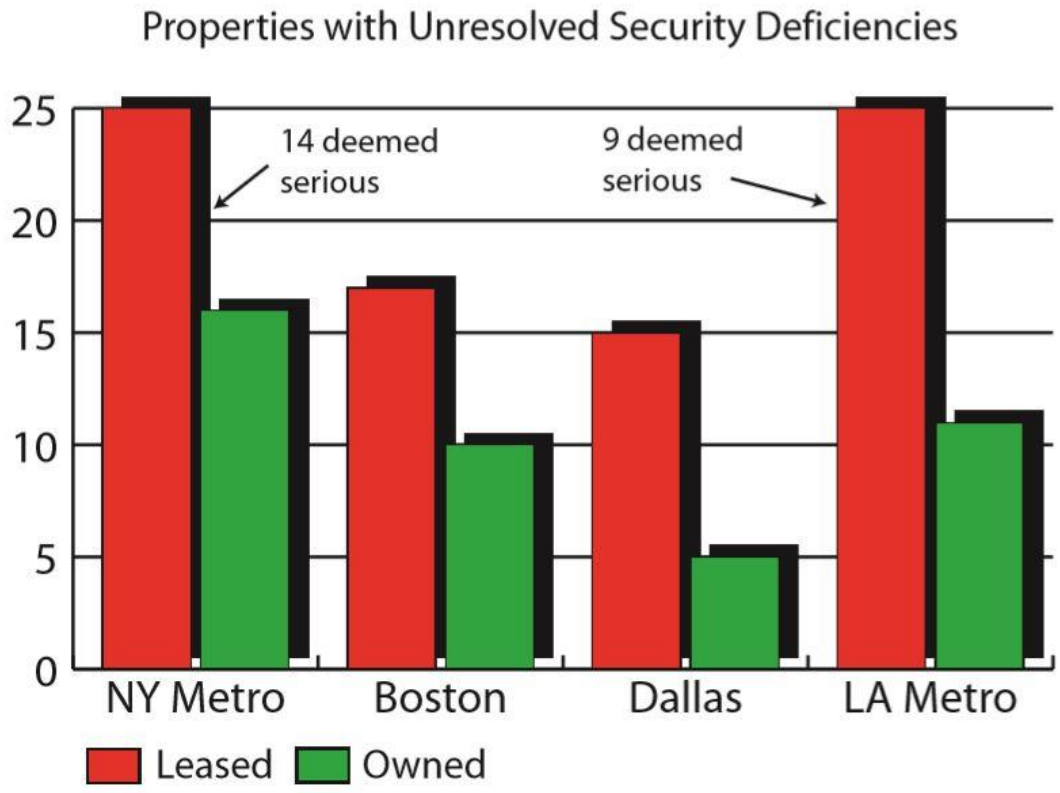
Security Metrics > Specific Examples >

Security Issues in Leased vs. Owned Property

Created by George Campbell, Security Executive Council Emeritus Faculty

A proactive risk management program seeks to identify vulnerabilities that could be exploited and that contribute to a variety of risk exposures. Whether a company owns or leases properties for its various operations often depends on cost and logistics, but risk should also be considered.

In the example from which the following chart is drawn, our CSO wants to make clear that many of the company's leasing arrangements lack risk-based due diligence or lease terms appropriate to a standard of protection enjoyed by owned space. This dichotomy needs to be addressed. The CSO wants to put management on notice that the leasing and fit-up strategy requires significant overhaul, and greater attention needs to be paid to addressing the resolution of security audits in general.



Security has analyzed its properties in four major operational regions and uncovered a number of security deficiencies that run counter to security policy and could be exploited by knowledgeable adversaries. The assessment process ranks each deficiency according to potential consequences to life safety, business interruption and/or financial loss. The risk ranking strategy at work here has identified a total of twice as many deficiencies at leased properties as owned properties and has found a total of 23 serious unresolved deficiencies at two of the leased locations.

Each site has received a briefing and documented survey and is responsible for addressing these deficiencies on a prioritized basis. Follow-up assessments have revealed a number of issues that have not been addressed as required. Security has determined that the continuing non-conformance of leased spaces is due primarily to the absence of pre-site selection risk assessments and directly related remedial requirements in lease agreements.

In the past, the security department has allowed the business units to continue without remedial action for a protracted period before handing the issue off to a more visible process of resolution. The CSO now questions this previous approach. He or she plans to take this information to each site manager before escalating to the senior executive responsible for business operations or to Internal Audit, which requires a far more visible and measured response. The CSO hopes to resolve these issues short of this higher notification.

Security routinely performs security audits at all locations housing company operations to confirm compliance with security policy. The data for this metric is a product of these documented, scheduled, policy-based security assessments. In this case, security also obtained data from the outsourced real estate vendor and Corporate Real Estate that showed lack of communication between the various entities.

Originally published in Security Technology Executive Magazine

Visit the Security Executive Council website for other resources in the Security Metrics > Specific Examples series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/