SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Metrics > Specific Examples >

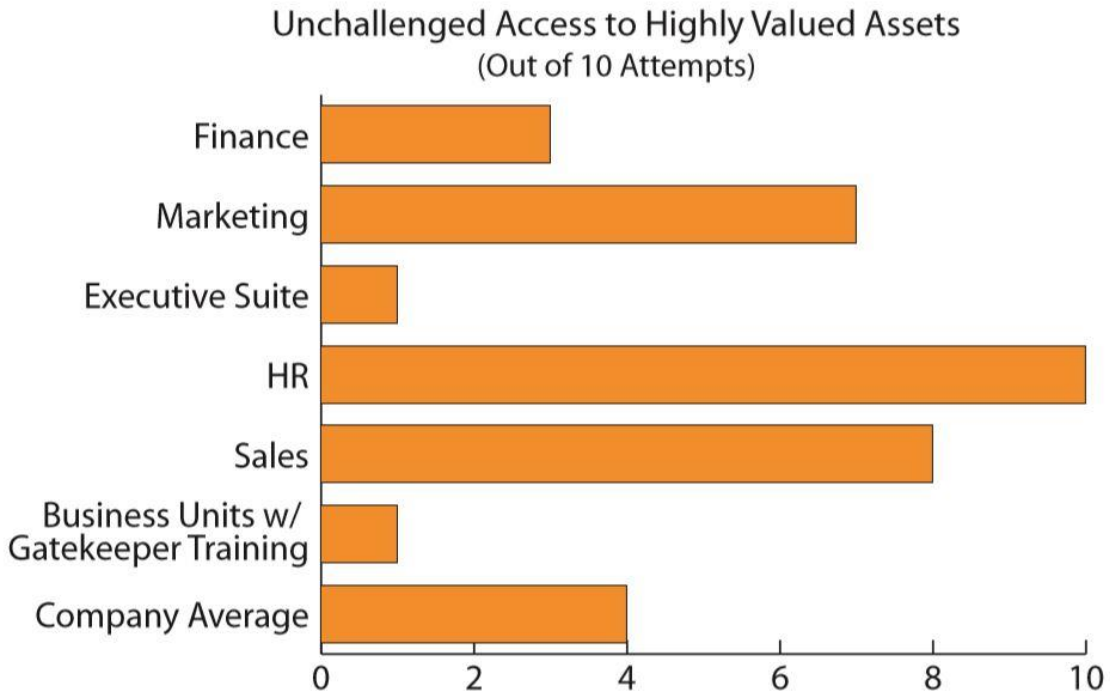
Working with Customers for Better Access Control

Created by George Campbell, Security Executive Council Emeritus Faculty

I have a passion for testing and reporting on the effectiveness of the safeguards we have installed to protect our people and assets. You will not influence anyone with metrics that just count things, but you will with ones that really measure how well you and your customers are meeting your responsibilities to protect the company.

If we are serious about our mission, we test safeguards on a regular basis to measure how well they are working and to find soft spots in our strategy. There is no security manager reading this that has not had to deal with a business unit that pushes back and demands "an inviting space" and "convenience"— in other words, unrestricted access involving disablement of electronic or staffed entry controls. Let's think about this for a minute.

How well have we considered the business culture as we have dealt with this "difficult" client? You can bet that for every person openly complaining about security controls, there are more out there who are simply looking the other way when those controls are purposefully bypassed to make life easier for the employees or residents. Any good patrol plan and a cadre of engaged security officers would have already told you which business functions would be targets of opportunity because of such bypasses. In the example that follows, Security went a step further and conducted 10 unannounced access attempts for each business unit.



If we look at the results of these penetration tests, what might we speculate are the biases of the three bad guys here? Marketing, human resources, and sales. I do not think I'm generalizing when I state that these functions are typically hard sells for the kind of controls we tend to like. They want convenience and freedom, and we either post someone who challenges entry or install things that impose restrictions.

What should we do with these results? First, let's understand that the findings of these tests revealed access to customer lists, an unsecured CFO Laptop, desktop access via posted password and piggybacking into the computer room by unknown individuals, so it is clear that we have to find ways to improve. We could run to the CEO and drop a dime on the top guys of the Freedom Three, or we could approach each of these managers, discuss what we found, and then find solutions that serve a common ground of enterprise risk management.

At the end of the day, these senior managers cannot excuse the potential exposures presented by these findings, nor can we in security escape finding more creative and business-compatible asset protection solutions. The security approach we see here is a one-size-fits-all: You have our solution to access control and that's that! Working with each business unit to direct greater protection around tighter, more internal and focused areas where convenience can agreeably give way to expedience is the middle ground found here. I would add that in this case, HR did agree that their exposure to disgruntled and potentially hostile individuals did demand greater access management and control. The model they adopted reflected the lessons from "gatekeeper" risk

assessment training for receptionists and assistants coupled with duress-related technology.

Summary: Access management is a core safeguard, but there are a variety of ways to achieve that goal and a variety of user perspectives on how it could best work. Understand the range of risks driving this set of safeguards and work with your customers to tailor the protection strategy for results.

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/