The Building's on Fire!

Optimizing Procurement & Prioritizing Security

We open our discussion today with a scenario of a phishing attack, that has been plaguing a company for weeks now, let's call them Firetronics. The CISO, CIO, and SOC have had several meetings about this attack, it seems they have an extremely persistent attacker.

The security team has tried everything, including blocking the email address from the initial phishing email, and the attacker simply switched accounts. They attempted blocking the external site that harvests credentials, so the attacker changed sites he was using. They implemented a more diligent education platform to ensure the users could recognize the signs of a phishing attack, the attacker began sending more advanced emails from legitimate companies using standard industry language. The attacker seems to always be ready for their countermeasures, and employee accounts are being continuously compromised, not to mention the time and resources being eaten up by this attack.

> “*They're a sitting duck against attacks that began two quarters ago, and newer attacks that will continue to roll in.*”

It's time Firetronics begins looking for software or security appliances to help mitigate these attacks, and they find a few. So begins the lengthy procurement process, which may take up to a year from demo to implementation.

The analysts begin the Proof of Concept testing, they include the networking and exchange teams to find the best solution that will work for them all. They bring the information to the CISO, however, there is one glaringly large issue, budget. Unfortunately, there is no room in the budget for this new appliance, and won't be until the next fiscal year.

> “*it is an issue plaguing cyber-security teams the world over, and the consequences can be dire.*”

Meanwhile, the attacks persist; the board decides that the security team is being mismanaged and a new CISO takes over. The new CISO has a different appliance he liked using at his former company and suggests this new appliance be vetted and put into place. Here we go again. All the while more attackers have begun targeting Firetronics with several different types of attacks, not just phishing. They're a sitting duck against attacks that began two quarters ago, and newer attacks that will continue to roll in.

......

Unfortunately, this scenario is more realistic than some might think. The process to add security software, and appliances can take several months if not longer. Making sure the right pieces will be put in place is critical and in the best interest of the business. So why are there so many obstacles in front of the trusted chief? How long can a company really wait to add these critical systems when the attacks are constant and ever evolving?

Businesses in today's world need to be agile enough to outmaneuver bad actors. While these might be obvious observations, it is an issue plaguing cyber-security teams the world over, and the consequences can be dire.

However, other aspects of a business are not treated this way, so why treat cyber-security as the proverbial red-headed stepchild?

Companies have all the equipment needed to mitigate physical threats such as fire, power outage, earthquake, flood, etc. It would be baffling to find a sprinkler system is only half of a building, not to mention illegal, and rightly so. If a routine test of a building's fire prevention systems showed them to be faulty, then the business would be responsible for patching up any issues in a timely manner. It's prioritized for the safety of everyone that works within the business's walls.

> *Let us help you sort out the redundant (slapped-on) solutions & make budgets stretch through eliminating needless spending.*

These systems also undergo regular, mandated testing, maintenance and updates, and a digital system full of physical information ought to be treated with the same priority. It is unlikely that we will ever be able to cut down all the red tape surrounding the standard procurement process. So, let's strive to build a supportive community that is effective and collaborative by sharing strategies and resources.

One such strategy is the core of SecureNation, our mission is to make budgets go further by helping our clients be assured they have the right solution, at the right price. We work tirelessly to chip away at manufacturer pricing & make room for shorter road maps by maintaining transparency and treating "Shelf ware" as a four-letter word. Let us help you sort out the redundant (slapped-on) solutions & make budgets stretch through eliminating needless spending.

How do you plan to get the most out of your environment and budgeting complications?