HOW TO BUY CYBERSECURITY SOLUTIONS

So, you want to buy a Cybersecurity solution. What is the problem you are trying to solve? Is it a point problem or a more significant issue? How did you decide this “problem” is the priority? Most organizations remain mired in tactical warfare – reactively managing tools, putting out fires, and this is their Cybersecurity program. They decide what “problem” to budget for when a tool loses utility or an expert tells them they need something to fix a problem. But if you don’t adopt and implement a Framework to support your Cybersecurity strategy, then all you have is a mission statement. You will remain stuck in tactical warfare, reacting to the latest industry and internal noise, buying more tools to solve problems when what you need is a strategy.

Organizations of all sizes continue to get breached. Millions of dollars get paid in ransomware per incident, nation-states keep the upper hand, and organized crime gets away with cash and a laugh. What can we really learn? That we need to adopt a mindset of resiliency. A resilient enterprise accepts the reality of a breach and builds “solutions” to rapidly detect, respond to, eradicate, and recover from a compromise. Containment is key. Detection is the lynchpin. If you stay down in the weeds, managing the firewalls and other security infrastructure, chasing vulnerabilities, and patching, then you are going to remain in reactive mode, missing the real Threat Actors.

Let’s get out of the weeds and get serious. The real problems to solve are a lack of time and a lack of focus. Frameworks deliver both. Be proactive and choose a Framework carefully, ensuring it matches the context and culture of the organization. CIS Security Controls, SANS Top 20, NIST, ISO, and others are excellent choices, but for the right environment! Choose wisely, start simple, establish the basics, and then you have a baseline to measure from and build upon. Implement a continuous improvement mindset, and the Cybersecurity program becomes a resilient, dynamic, adaptive ecosystem to keep pace with the evolving threat landscape. Exceptional brainpower is required to select a Framework and deploy the right “solutions” to build this capability. This is the right use of your team’s time, not managing security tools.

Stop paying organized crime and instead pay the good guys, increase security budgets, and invest in your own army to defend and defeat the bad Actors. Be realistic that you and your teams can’t do it alone. It’s not practical, feasible, or even attainable. Leverage Service Providers to get scale and efficiency and act as your force multiplier. For a fraction of the cost of more security staff, you’re getting consistent, SLA-bound performance and a dependable function from a 24×7 operation of dedicated experts. Of course, you must choose a vendor carefully, but when you do – what you’re buying is Time – precious time for your team.

The best use of a Cybersecurity professional's talents are deep-thinking projects on business and IT initiatives, not managing tools. These include a focus on Cloud adoption, Data protection, advanced Threat Hunting, establishing reference architectures, evaluating emerging technologies, design reviews, and improving the Cybersecurity program. Keep Service Providers accountable for routine cybersecurity functions traditionally delivered by tools, but now consumed as a service. The output of those services is refined feedback for your Security experts to make more informed decisions about the overall effectiveness of the Cybersecurity program, through direct and inferential knowledge. This shifts the organization into a proactive, resilient mode with risk, strategy, and continuous improvement driving the priorities.

Buying Cybersecurity the right way means you start with a risk analysis. Ideally, this includes current, informed, and mature Threat modeling. Only the beginning, this process ought to be an iterative process. Risks change over time, so should the analysis. This process defines the strategy, and then a Framework should be chosen, championed, and deployed, which puts the strategy in motion. Choose carefully! It will be the foundation for your Cybersecurity program, and early success is vital to adoption and continued support. Being overly ambitious, draconian, or failing to consider the culture of the enterprise is the perfect recipe for failure. But establishing a proactive, adaptive program built upon a Framework delivers resilience to the 21st-century enterprise.

The recent FireEye and SolarWinds storylines give all of us a serious wake-up call to the reality of 21st-century cyber warfare, as it is much more than a "yet another breach" story. Your enterprise depends on IT to deliver services, orders, goods, obtain revenue, and you are connected to the Internet. Accept that you are a breach soon to happen because this is the new reality. Adopt a Framework to deliver a risk-informed, adaptive Cybersecurity posture.

That's the essence of Cyber resilience. Adopt a Framework for uniformity, confidence, and a structure to allow adaptability over time. Focus on better Threat Hunting, data protection, Incident Response, and continuous improvement. Let experts manage the tools and buy services instead, thereby enabling your experts to focus on the tools' information. Rely on your experts to model the output of those services within the context of your environment, making more informed, effective, and wise Cybersecurity decisions of where to spend time.

Think holistically across the enterprise and silos. Establish a reference architecture built upon a Framework. Increase budgets to shift from a reactive to proactive posture using the scale and expertise of Service Providers for all the basics. Focus your team's efforts towards more advanced, sorely needed areas where you can best use their excellent brainpower.

Buy time for your team. That's the solution to your Cybersecurity problem.