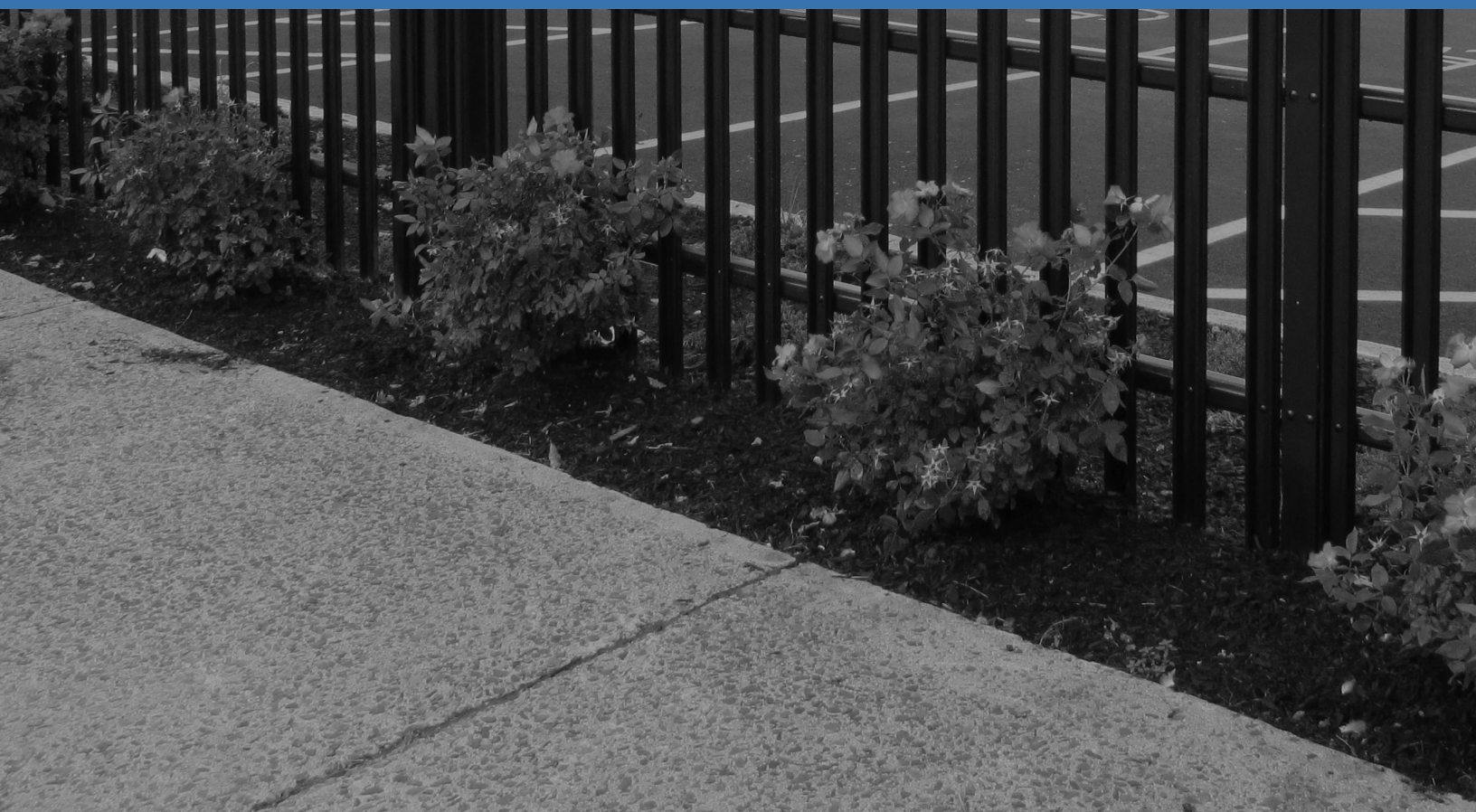
AMERISTAR®

ASSA ABLOY

2019

DEFINING THE VALUE OF PERIMETER FENCE

Justifying the Cost and Design Considerations for Perimeter Security



I. Changing Standards

Increased Threats Demand Heightened Perimeter Security

FOR FACILITY MANAGERS, ENGINEERS, AND SECURITY CONSULTANTS, DEFINING THE VALUE OF A PERIMETER FENCE IS A CRITICAL ROLE.

For decades, the familiar chain-link fence was deemed acceptable for perimeter security at just about any facility that required protection from intruders. Depending on the level of security required, fences were typically six or seven feet high. For an added measure of protection, some had barbed-wire coils atop the fence.

But the standards for perimeter security have changed dramatically. The threats to just about any facility, but particularly those of government, power utility, data centers, and other high-risk properties, have grown. Threats have become more sophisticated, more widespread, and less predictable.

Correspondingly, the stakes have grown higher. The assets, physical and intellectual property, and materials contained in these facilities have increased exponentially in value. So the need to prevent theft and attacks on these facilities with perimeter fences has never been more important.

Responding to these changing conditions, facilities managers, integrators, security consults, and other experts have long recommended robust perimeter fencing as part of comprehensive security strategies and designs.

Fence systems of that caliber carry a significant cost, making them an easy target for budget cuts and reductions. Too often, fences are relegated to afterthought status in a facility's design and construction. They are not specified and installed to be an integral part of the facility and its security plan.

As a result, many perimeter fences don't meet the security needs of the facilities they surround. They may look impressive, but when put to the test, they fail. Sometimes with disastrous consequences.

The security needs of most facilities have outgrown the effectiveness of chain-link fences. New standards of perimeter security reflect threats that are more widespread, sophisticated, and unpredictable.

Communicating the Need and Value

For facility managers, engineers, and security consultants, justifying the expenditure on a perimeter fence – defining its value to company leadership and management – is a critical role. It affects the safety of the assets contained within the facility and the people who live or work in them. That is in addition to the effect a breach might have on the communities outside the facility.

Defining the value of a perimeter fence system can be a challenge. This white paper is designed to provide the information and justification needed to communicate the critical nature of perimeter security systems.

The information that follows will demonstrate how to easily define and explain the threat to a facility in simple terms. Then it will cover the three main areas that help define the value of the perimeter fence: its visual value, its performance value, and its unseen value.

A well-designed fence can visually ward off intrusions while complementing the property's architecture and landscaping.

II. The Threat

Defining the Threat

In order to make the case for a perimeter fence, or any security expenditure, you first need to know what kind of system is best suited to your situation. Begin by defining the threat to your facility.

Not all facilities are the same. Their susceptibility to a breach or an intrusion is affected by a variety of factors. "It comes down to the risk a facility faces," said Brian Zapata, vice president of special projects at ZAPATA, an engineering, architecture and construction company based in Charlotte. "Whether it's from simple theft or an attack by a hostile government, or somewhere in the middle."

The first factor to consider is the type of property the facility is, and the value or sensitivity of the materials or assets contained within it. Those are the two factors that begin to define how attractive a target is for thieves, terrorists, or other intruders.

Its location also can play an important role. A facility located in a remote, rural area might be at a lower risk than one in an urban location for the simple fact that there are fewer people in close proximity. However, a remotely located facility might also be subject to slower response times from police and first responders.

You also have to consider the nature of any threat. One might naturally think of threats as intruders working under cover of darkness, trying to gain access without detection or using a heavy vehicle as a battering ram to breach a fence.

Those are certainly possible threats, but there are other types. The intrusion can simply be visual, with perpetrators gaining information through simple observation from a distance. It can also be ballistic, with vandals attempting to cause damage by shooting at assets within the fence.

Threats can also be accidental, with people unintentionally walking or driving into forbidden areas. Even animals wandering onto a site can cause problems at some facilities.

In assessing the risk to your facility, consider obvious attacks, like vehicles crashing through the fence, and less obvious threats, like animals wandering onto the property.

Risk Equation

There are many different approaches to assessing risk and determining a facility's perimeter security needs. Zapata prefers to use a simple equation:

PROBABILITY x VULNERABILITY x CONSEQUENCES = RISK

Using a scale of one to five, he rates the facility's risk along each of the three criteria. "The greater the number, the higher the need for security measures," Zapata said. "It's a good framework for quickly understanding and methodically justifying a building's needs."

- **Probability.** Has an intrusion happened at the facility in the past? Has it ever happened to any facility like it?
- **Vulnerability.** Given the location of the property and the value of its contents, how easy would an attack or an intrusion be?
- **Consequences.** If an attack or a breach were to happen, how significant would the consequences be?

Zapata urges anyone using this equation to give each question serious consideration. The answers and scenarios aren't always obvious.

To illustrate his point, Zapata used the example of a typical warehouse. Though not a high-value target, it might be attractive to small-time thieves and vandals. In that case, while the probability and vulnerability factors might be low, the consequences might be higher than a few stolen items or some damaged property.

"Let's say someone gets hurt or dies inside a facility," he speculated. "The family will almost certainly sue that company for damages."

The bottom line is that nearly every facility should consider perimeter security to some extent. "If you want to stay in business, you should pay attention to security," Zapata warned.

But for certain types of facilities – utilities, data centers, government, military – perimeter fencing has increased value.

A well-designed fence can visually ward off intrusions while complementing the property's architecture and landscaping.

III. Visual

Visual Value

At its most basic level, every fence is a visual deterrent to trespassers and intruders. Even the humble white picket fence surrounding the yard of a small-town home sends a subtle message to neighbors that the property should not be accessed without permission.

When dealing with vandals, criminals, and especially terrorists, the message should not be so subtle. It needs to be a clear and strong indication that any efforts to breach the fence and access the facility will be difficult and time-consuming.

In other words, a perimeter fence is a show of strength. Through its sheer visual presence, it communicates to would-be intruders that it's designed and built to keep them out. "The first thing a fence should do is cause an intruder to move on and choose a different facility to target," said Edward Ankers, director of corporate security at RagingWire Data Centers.

A perimeter fence can send that message in a variety of ways.

Anti-Climb

There are two basic ways to breach a fence. The first, and most common, is to climb over it. A perimeter fence's design can serve as a warning to would-be intruders that climbing is no easy task and not worth trying.

Fences send the "do not climb" message with pales spaced at 1.5 inches, which prevents anyone from being able to gain a foothold. Tridents atop each pale show that getting over the fence would be a perilous endeavor. Other fences are designed with wire mesh fabric – with openings far too small for hands or feet – between the posts.

Anti-Cut

The other way to breach a fence is to go through it by cutting the material, something that can be done easily to chain-link fences.

But fences with heavy, steel pales send the message that cutting through will take considerable time, using tools that are not easily carried. Similarly, the wire mesh fences have minimal space for cutting implements to fit.

FENCES SEND A MESSAGE TO EMPLOYEES, TENANTS, OR CUSTOMERS THAT THE PROPERTY IS SAFE.

Anti-Ram

If a fence can't be climbed over or cut through, the last option for an intruder is to smash through it using a vehicle.

Again, the robust design of a fence, especially when reinforced with steel bollards and anti-ram cabling , tell intruders that a vehicle will be disabled in the process of ramming through the fence.

Positive Messages

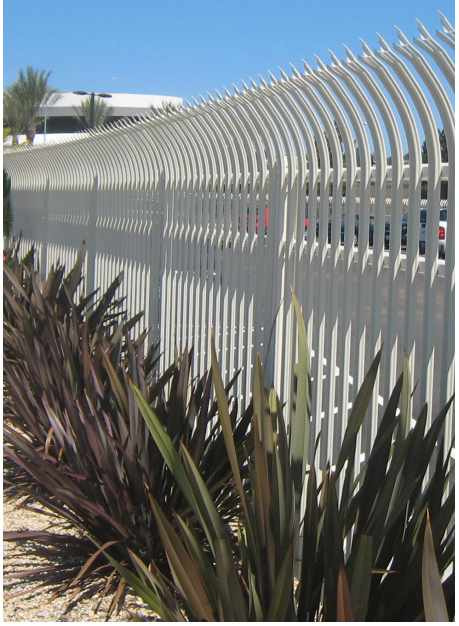
If a fence is designed to send the right message, it stops all breaching attempts before they even reach the planning phase.

But the visual presence of a fence isn't just to ward off potential intruders. It can also send a message to employees, tenants, or customers of the facility that the operators take security seriously, and that the property is safe.

For many facilities, especially data centers, this is an important message to send. Ankers said that a perimeter fence sends a strong message of assurance to current and potential clients that their data is being protected. "There is no way you can be successful without perimeter security," he said. "Clients won't even consider a facility without it."

Finally, just because a fence serves as a visual deterrent to intruders doesn't mean it can't be beautiful, as well. A well-designed fence can complement a building's architecture and design, or blend in naturally with the landscaping.

For many facilities, aesthetics and being a good neighbor is almost as important as security.



IV. Performance

Performance Value

Because of the visual presence of a perimeter fence, its ability to actually prevent a breach might never be tested. Silently, it will do its job, warding off anyone with thoughts of gaining unauthorized access.

However in the unlikely event of an attempted breach, the perimeter fence has to do what it was designed to do. It has to perform.

THE RIGHT PERIMETER FENCE WILL ALLOW FOR DETECTION, PROVIDE DETERRENCE AND DELAY INTRUDERS.

After deterrence, a perimeter fence has two main functions: to allow for the detection of an attempted breach, and to delay the intruders long enough for a response by the police or security personnel.

Detecting a Breach

By itself, a fence does little to actually detect an intruder. To do that, a facility might have an array of cameras, lighting, motion detectors, and other technologies to identify intrusions in progress.

The best perimeter fences have the added value of being able to easily accommodate these technologies. Zapata said that makes installing and upgrading the systems and equipment easier. “All of that technology requires wires and need to be mounted somewhere,” he said. A fence that integrates with security technology eliminates the need for trenching and boring. “That has tremendous value.”

Perimeter security should be the first consideration for any site.

For a perimeter fence to perform properly, it needs to be incorporated into the overall design of the facility.

Slowing an Intrusion

For many facilities, the job of delaying an intruder from gaining quick access to the property is critical.

"The vast majority of facilities are not guarded by a dedicated response force," said Zapata. "If a breach occurs, the only response force is the local police, which might take 45 minutes to arrive."

A perimeter fence might be the only thing keeping an intruder occupied for the first hour of the event. That is where the anti-climb and cut-resistant designs of high security fences show their real value.

According to Ankers, a motivated individual will find a way to breach a fence. "Ideally, the fence's design will cause them to choose a different target," he said. "But if they do attempt to get in, the fence should make it as slow-going as possible."

Not an Afterthought

For a perimeter fence to perform properly in the event of an attempted breach, it is crucial that it's incorporated into overall design of the facility. It can't be an afterthought.

In fact, it should really be the first consideration, according to Ankers. "Security engineering begins at the outer perimeter," he said, adding that he starts thinking of fencing at new facilities before construction even begins. "When I see a green field, my first thought is fencing. I want that before the building is even there."

Zapata agreed, adding that when perimeter fencing is not engineered into the property correctly, the result can be gaps and other areas intruders can exploit easily. He gave the example of a driveway not being graded properly, leaving a large gaps underneath the fence and gate.

"If you're going to do it, a perimeter fence has to be part of the design from the beginning," he said. "The building, the landscaping, the fence all have to accommodate perimeter security."

A perimeter fence can limit the facility owner's exposure to liability, helping to keep insurance premiums low.

V. Unseen Value

The Unseen Value

While the visual presence and the performance of a perimeter fence are critical to its overall value, companies and facility owners and operators will experience its value in other ways that are less obvious.

A perimeter fence's value can be measured in the operations and maintenance of a facility and in terms of liability.

Operations and Maintenance

For all of the potential threats to a facility, whether they are intentional or unintentional, human beings or wildlife, they all pale in comparison to a fence's greatest enemy. One that is relentless and over time can wear any fence down: the weather.

For any facility, the ravages of wind, rain, and sun are a constant threat. For properties in locations with desert heat and sand, or coastal moisture and salt, the value of a perimeter fence can lie in its durable construction.

Zapata said that maintenance is a critical factor when determining the value of a perimeter fence. "You have to look at if the fence will last and if it's going to require maintenance," he said.

Two factors that indicate a perimeter fence's durability are its construction and warranty. Well-made fences are manufactured with a multi-step finishing process that prevents corrosion. Pre-galvanized steel components are meticulously prepped and coated with an epoxy powder coat and polyester powder. This not only resists weathering and corrosion, but also prevents scratches during shipping and installation.

With this level of construction and finishing, manufacturers will also offer warranties of up to 15 years, so facility owners and operators can be sure the fence will last.

The value of a perimeter fence is then reflected in minimized maintenance costs.

Liability

The value of a perimeter fence can also be seen in limiting the facility owner's exposure to liability, and helping to keep insurance premiums low.

To illustrate this value, Zapata referred back to the example of thieves being hurt or killed while trespassing in a warehouse. Despite the fact that they were on the property without permission, their families would certainly sue the facility for damages.

Such a lawsuit would likely be groundless, but litigating it would be expensive. "You do some basic math on the consequences," he said. "The cost of litigation would be more than just putting up a better fence."

In the event of a terrorist attack, some perimeter fences offer another level of liability protection to facility owners. Fences that are certified by the U.S. Department of Homeland Security as meeting SAFETY Act standards can significantly reduce liability exposure from lawsuits in the wake of a terrorist attack.

This protection also extends to the security integrators, architects and engineers who specify the fence, and the contractors who install them.

VI. Conclusion

Defining the Value

FOR ENGINEERS, INTEGRATORS, AND SECURITY CONSULTANTS, THE CHALLENGE IS DEMONSTRATING THE VALUE OF A PERIMETER FENCE.

For engineers, integrators, and security consultants, the value of a perimeter fence is no mystery. The challenge is to justify the cost, and demonstrate the value to facility owners and managers who are not familiar with the nuances of security design.

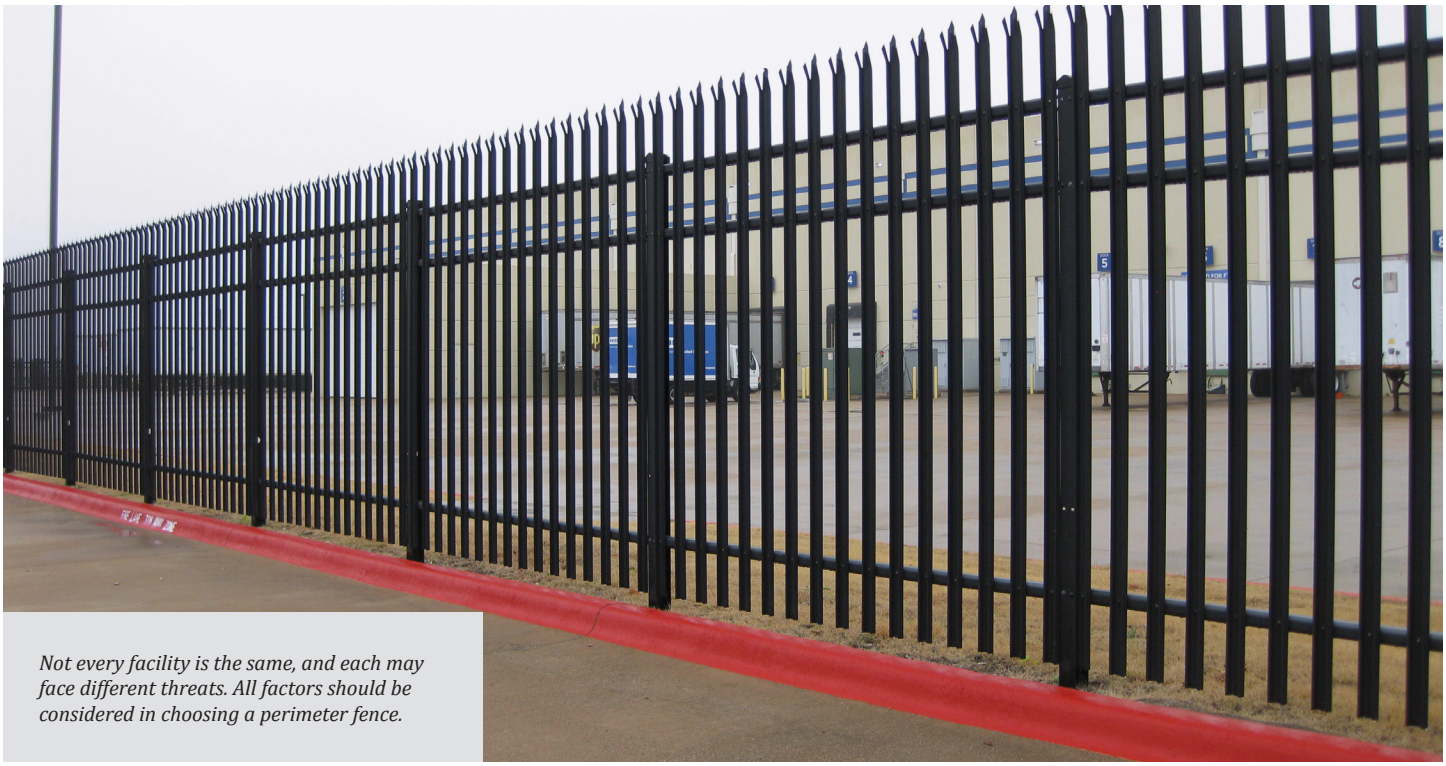
Meeting this challenge starts with assessing the risk and defining the threat to a facility. Not every facility is the same, and depending on a variety of factors, each may face different threats, whether intentional intrusions, accidental breaches, or by wildlife.

Once the threat a facility faces is determined and the perimeter security requirements defined, the value of a perimeter fence can be defined in three main ways.

- **Visual Presence.** The fence's ability to visually deter would-be intruders, as well as assure employees, tenants, and clients of its security.
- **Performance.** The fence's ability to help detect an active intrusion in progress, and delay the perpetrators long enough for a response by authorities.
- **Unseen Value.** The reduction in maintenance costs, insurance premiums, and liability exposure as a result of the fence being in place.

The value of a perimeter fence is demonstrably significant, but only if it is given proper consideration from the beginning of the facility's design process. Otherwise, even the best fences might be susceptible to intrusion through gaps caused by poor security system design and installation.

For more information about perimeter fence design and integration, contact Ameristar today, or visit them online at ***AmeristarFence.com***.



Not every facility is the same, and each may face different threats. All factors should be considered in choosing a perimeter fence.

VII. Bios

Featured Expert Contributors

Brian Zapata, PhD, PE, SE has over 15 years of professional experience in structural, security, blast, and forensic engineering. He serves as Vice President of Special Projects at ZAPATA responsible for managerial and technical aspects of unique projects across ZAPATA's portfolio.

He has experience in the analysis, design, and renovation of commercial and industrial structures including office buildings, warehouse and distribution centers, manufacturing facilities, fossil power facilities, nuclear power facilities, and high voltage transmission infrastructure.

Dr. Zapata also has experience in explosives and blast testing, structural vibration monitoring, finite element analysis, materials investigations, building condition surveys, nondestructive testing, and structural monitoring. Currently, he manages ZAPATA's ongoing portfolio of utility work in the southeast.

Edward Ankers is the Director of Corporate Security for RagingWire Data Centers. In his role, he partners with industry peers, state and federal emergency personnel, and security providers to ensure security of 1.5 million square feet of infrastructure across ten data centers in Sacramento and Santa Clara, California; Ashburn, Virginia; and Dallas, Texas.

Ankers spent 20 years in law enforcement roles, knows the importance of building and campus security. He has been heavily involved in community security, assisted in the design of correctional institutions, and designed the security plan for several data centers.

Ankers has been instrumental in spearheading a partnership with the Department of Homeland Security, which will be funded and given training support through the Regional Resiliency Assessment Program (RRAP). This program also acknowledged that data centers should be categorized as critical infrastructure.

This white paper was authored by **Draper DNA**, a marketing strategy, content and design consultancy based in Raleigh, N.C. The company has a long history in the building products category, and combines that industry expertise with an innovative approach to marketing. Whether it's using traditional tactics, new ideas, or most likely a combination of the two, Draper DNA is focused on helping their clients disrupt their industries, build their brands, and generate demand.