Proactive vs. Reactive Perimeter Security

Why You Should Implement Integrated Perimeter Security to Lower Costs and Reduce Business Risk







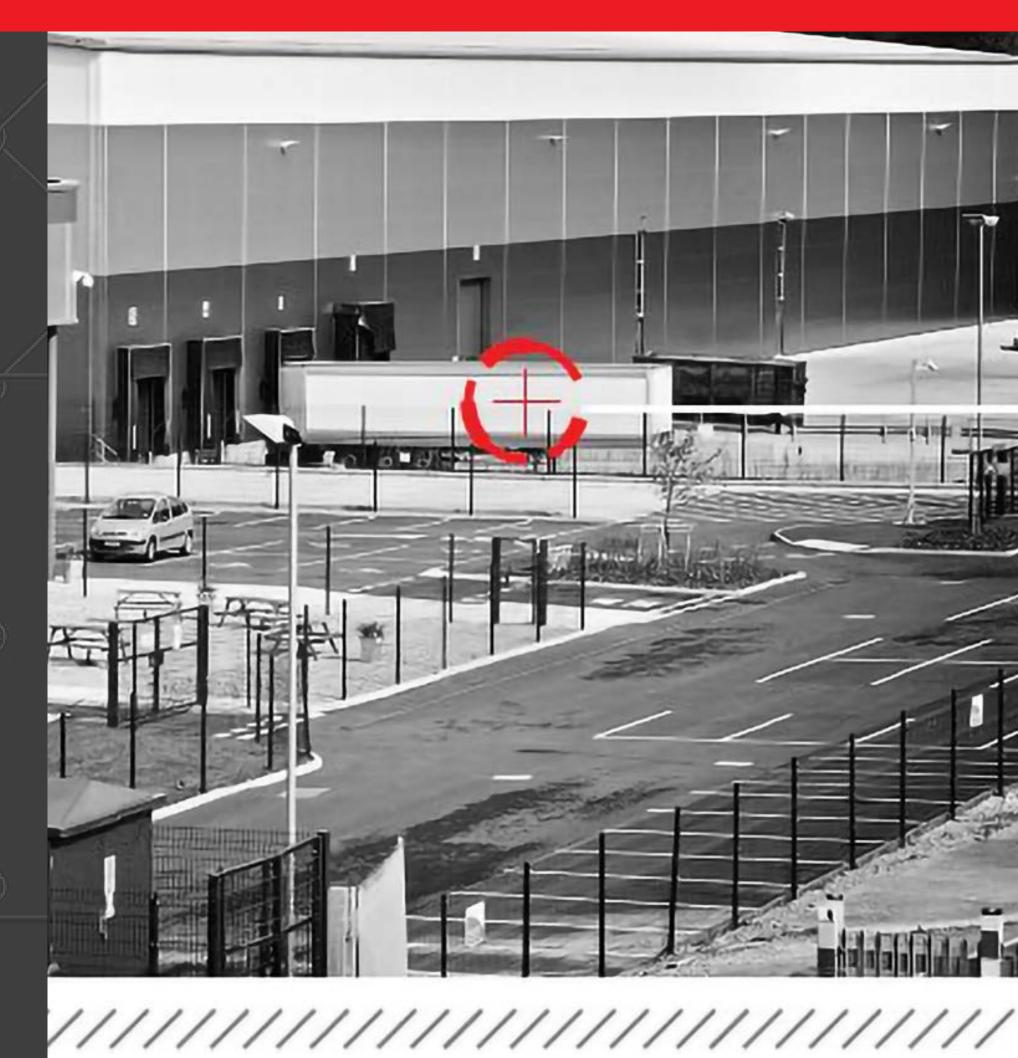












Sponsored by





M Mighty Guides

Table of Contents

Meet Our Experts	
Introduction	
Foreword	
Chapter 1: The Real Cost of Crime is Three Times Greater Than You Think	
Chapter 2: Criminals Only Fear Highly Integrated Perimeter Security Systems	1
Chapter 3: Invest Now vs. Invest Later: All Gain, No Pain	1
Chapter 4: The Consequences of Investing Later	1
Chapter 5: The Benefits of Investing Now	2
Learn More About Our Experts	2

Meet Our Experts

We interviewed eight security experts, from police commissioners to corporate security directors, on what it takes to protect your business from theft. Everyone agrees—theft amounts to more than what was stolen, and it pays to be proactive.

We hope you enjoy their insights!

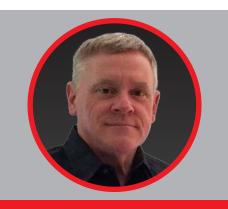


Publisher, Mighty Guides Inc. david@mightyguides.com (516) 788-7886





Michael Dorrington SVP, Sales and Marketing, **AMAROK Security**



Keith James Security Director, Corporate Security, Exela Technologies



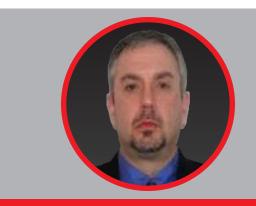
Brock Josephson Sr. Physical **Security Specialist, Burns & McDonnell**



Drew Leppert VP of Enterprise Sales, AMAROK Security



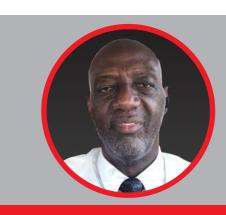
Joe Redmond Sr. Manager, Security, **First Student**



Dr. Christopher Shaffer **Corp. Director, Security** and Safety Compliance, **Valmont Industries**



Brian Stephens Sr. Managing Director, Teneo



Dr. Celvin G. Walwyn **Deputy Commissioner of Police Department**

Introduction

Anybody can be a victim of crime. The level of risk comes down to socioeconomic triggers and local crime rates. However, even commercial properties in low-risk areas can be targeted and, once that happens, every business in the area is at risk.

The problem is that not all criminals can be scared off easily by a single layer of perimeter security. Today's criminals are opportunists who regularly participate in organized crime and are well-informed about what they're up against. You might say, "we're protected by local law enforcement," and while that may be true, police departments today are often underfunded and unable to respond to these types of crimes promptly, or at all for that matter.

When a business becomes the victim of property theft, the loss of physical assets can be considerable and cause significant damage. However, that's just the beginning. The real cost of theft includes

operational downtime, loss of business, reputational damage and more.

To protect your physical assets and reduce business risk, an integrated multilayered approach to perimeter security is *vital*. Through this approach, you can avoid the costs associated with the crime itself, while also protecting your most valuable asset: your employees.

This eBook explores the *real cost of crime* and its impact on businesses. Moreover, it looks at how implementing an integrated security system can ward off potential intruders, reduce the risk of property theft, protect employees and improve business operations.

Mighty Guides

Mighty Guides make you stronger.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Reading a Mighty Guide is kind of like having your own team of experts. These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you.



Foreword

At AMAROK, we believe that taking a proactive approach to deterring theft, instead of reacting to it after the fact, is the best way to prevent catastrophic losses from happening to your commercial property, people, and profits. In this Mighty Guide, we've partnered with eight security professionals who share their perspectives on the benefits of taking a proactive approach as well.

The proactive-reactive distinction matters. It can be easy for businesses to overlook the bigger picture. They focus on potential losses to physical assets while forgetting the importance of deterrence, which can prevent major indirect losses, like service interruptions, delivery failures, product/supply shortages, and personal safety. That bigger picture needs to be incorporated into every company's planning to mitigate the risk of security measures falling short.

AMAROK provides comprehensive Property Security as a Service. Our solar-powered electric fence and other perimeter security solutions, together with our highly trained staff of supportive professionals, form the Ultimate Perimeter Security Solution that stops theft—and its TOTAL costs—before it happens.

We hope these insights are useful as you evaluate your current security plan and that they help you think more broadly about its objectives—like keeping criminals out of your business.



Relentlessly Protecting,

Michael Dorrington

SVP, Sales and Marketing,

AMAROK Security



AMAROK™ is a full-perimeter security company based in Columbia, South Carolina, that provides commercial security services throughout the United States and Canada. We specialize in electric fencing that deters criminals in three ways—a physical deterrent, a shock deterrent, and an alarm deterrent. AMAROK also provides supplemental surveillance solutions, including cameras, lights, and alarms.

AMAROK is the ultimate perimeter security solution because it deters thieves, so there is no need to deal with the aftermath of a crime.

NOBODY STOPS CRIME LIKE AMAROK. PERIOD.





FORTIFEYE™ integrates The Electric Guard Dog™ fence, a formidable physical electric fence, alarms, and ultra-bright lighting, with video cameras and real-time video monitoring. Together, these layers of security deter, detect and detain even the most tenacious criminals to protect your property.

FORTIFEYE YOUR PERIMETER





Deter
with The Electric
Guard Dog™ Fence





Detain
with Remote
Video Monitoring

Learn more at: www.amarok.com/fortifeye I (866) 770-4935

THE REAL COST OF CRIME IS THREE TIMES GREATER THAN YOU THINK

When we think about the cost of theft, the most obvious immediate loss is the value of the stolen assets. However, lost assets are just the beginning of the story and account for only around half of the total losses in most cases.

Sometimes an asset doesn't even have to be stolen to cause damage. If trailers or storage containers are opened, the entire contents can become null and void. This is particularly relevant for industries such as food, pharmaceuticals, and firearms. These assets need to be replaced, which has an obvious up-front cost. However, there's also the cost associated with being without

that asset for a length of time and the effort required to replace it and get it back into circulation.

The indirect costs of crime include production downtime, operational efficiencies, reputational damage, personal safety, and more. These costs can collectively, and sometimes individually, begin to outweigh the cost of the lost asset itself and often compound over time.

Considering this, not being able to service customers and meet service-level agreements can have a huge impact on reputation.



The total cost of property theft can vary greatly based on the type and resell value of assets that a business maintains on the property, but you additionally have to consider indirect costs like potential interruption of service, increased safety risk and damage to brand."



Brock Josephson

Sr. Physical Security Specialist, Burns & McDonnell



Theft or repeated theft can create ripple effects, like employees feeling unsafe and overworked or customers reacting to a negative brand reputation, that generate a cost that is not always associated with the bottom line but is still detrimental to the company's mission."

Sr. Manager, Security, First Student

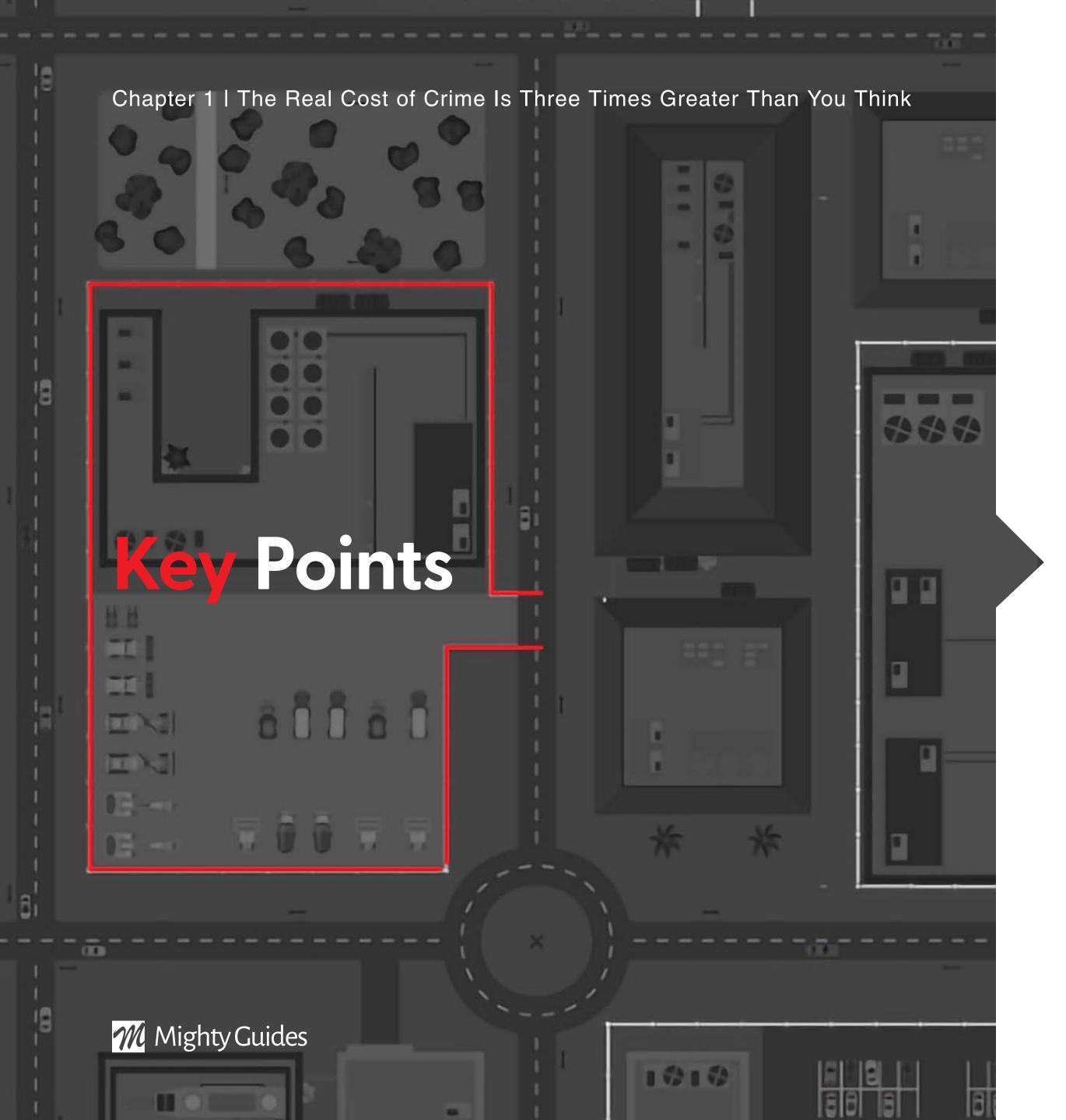


This becomes especially serious if customers' assets are stolen. People don't want to do business with a company that isn't reliable. Property theft can result in lost partnerships and vendors, which is a high-dollar problem, especially in the trucking and logistics industries. There's also the impact on personal safety, which can lead to problems with staff turnover, retention and brand culture.

The biggest mistake we see businesses make is focusing purely on the cost of their physical assets, underestimating the indirect costs of crime, and missing the bigger picture. Without understanding the whole story, they aren't taking the full risk into account, which means prevention and protection measures often fall short.

In addition, insurance premiums generally cover only the physical cost of the stolen asset and, even then, only a percentage of it. Most companies end up being self-insured to account for the potential loss, which involves holding a vast amount of reserves year over year for the worst-case scenario, but even this sometimes isn't enough.

When all the indirect costs are accounted for, the real cost of crime can be three times greater than you think. However, many companies have a hard time seeing past the physical assets and don't understand the real costs until they've been a direct victim, the impact of which can be devastating.



- The cost of a stolen asset accounts only for around half of the total losses; businesses often forget to account for indirect losses.
- Physical assets can generally be replaced, but lost revenue will be gone forever, and reputational damage can be long-lasting.
- Insurance premiums generally cover only the physical cost of the stolen asset and, even then, only a percentage of it.

CRIMINALS ONLY FEAR HIGHLY INTEGRATED PERIMETER SECURITY SYSTEMS

Property crimes accounted for over 60% of criminal offenses in 2021, with under 30% of stolen property being recovered. The actual level of risk comes down to data such as police reports, FBI data, and insurance claims. With this information, you can assess your risk based on a benchmark for the national average. However, even if your business operates in a low-risk area, if it becomes a victim of crime, it becomes high risk, despite what validation scores may show.

What's more, many businesses invest in property close to airports or railroad tracks because space is abundant and costs are lower. The low property prices and fewer eyes drive crime, which in turn, keeps the prices low—a never-ending cycle that enables potential perpetrators.

Thieves can make huge profits from stolen materials, vehicles, and equipment from commercial sites. If you have valuable equipment and assets on your premises, especially visible

assets, strong perimeter security is imperative. Keeping criminals from accessing property should always come first and foremost, but the response is often alarmingly inadequate.

Traditional perimeter defenses, such as chain link fences, are the go-to solution for commercial properties. However, all they do is provide a false sense of security. They aren't intimidating to criminals, they can easily be breached, and they do nothing to alert you of the intrusion.



Visible physical security is a proven deterrent to potential criminals attempting to defeat a hardened target. It comes down to the three L's—locks, lights, and landscape."



Dr. Celvin G. Walwyn

Deputy Commissioner of Police, US Virgin Islands Police Department Chapter 2 | Criminals Only Fear Highly Integrated Perimeter Security Systems



A layered security approach (protection in depth) is essential to a good security plan. Integrated perimeter security is a critical component to ensure the objectives to deter, detect, and delay."

Security Director, Corporate Security, Exela Technologies

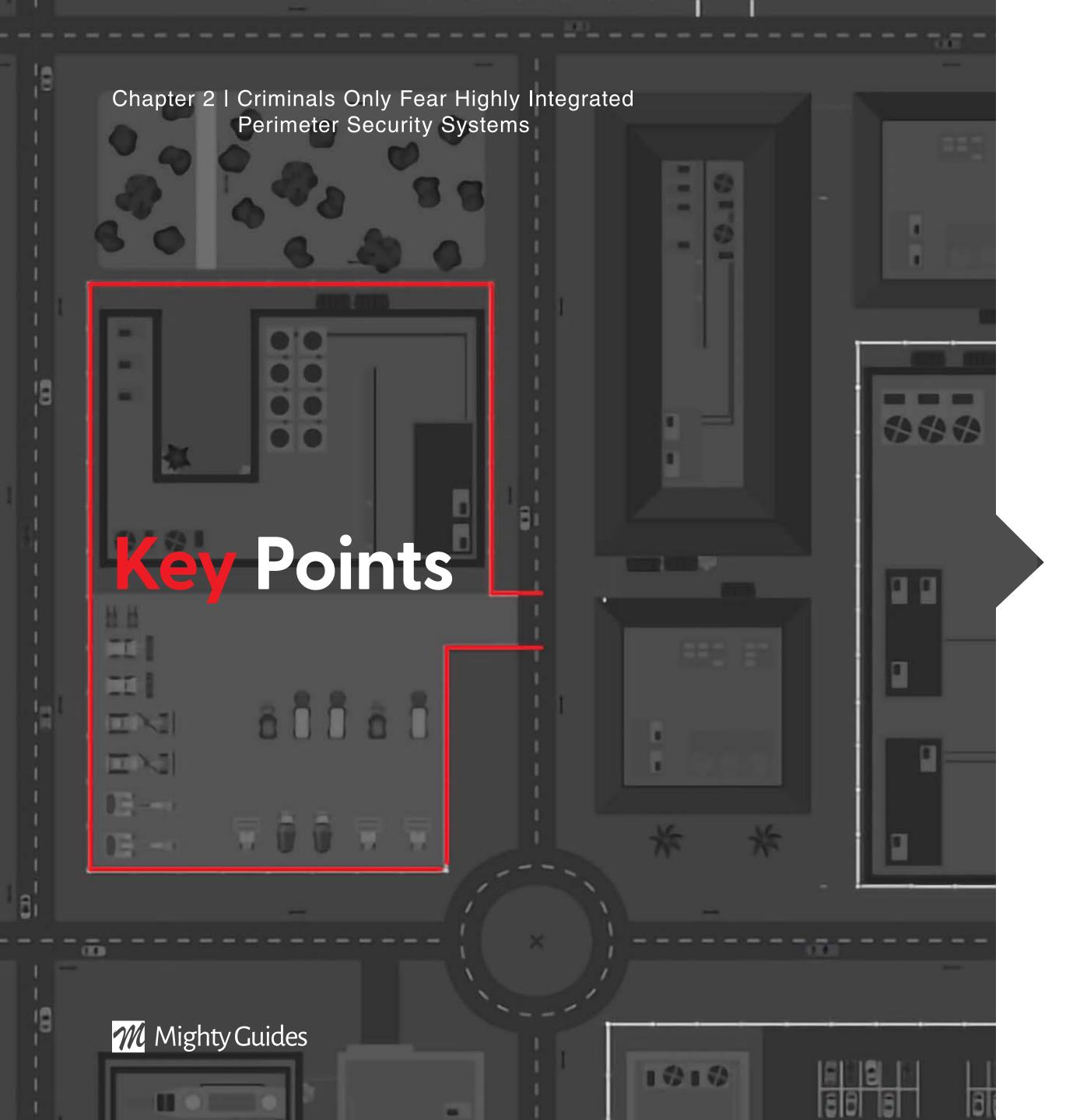


The common response is to then install security cameras. However, unmonitored CCTV systems don't stop criminal activity; they simply record it. Having a recording of the crime after the fact will rarely result in a thief being caught or your goods being returned.

Even when security measures are in place, there's a sliding scale of how criminals will approach a theft and the varying levels of sophistication of any attack. Today's criminals often work as part of crime organizations and are very well informed about what they're up against. They're also highly aware of the capacity of police departments to respond and average response rates.

The reality is that police departments are often unable to respond to property theft in a timely manner, if at all. Resources can be extremely limited and underfunded in many areas. And then there's these case of false alarms that account for almost a quarter of all calls made to police—there's no guarantee your call will be taken seriously.

A multi-layered approach is the only solution effective at deterring criminals. This can include measures such as high fences, wires, steel poles, cameras, lights, alarms, electric fences and physical shock deterrents. While one layer may be defeated, the remaining layers continue to offer protection. Moreover, they work together, providing the dual verification and visual authentication required by law enforcement before acting. The truth is that criminals will be more reluctant to attempt entry into an area protected by an integrated security system, and police will more readily respond if they do.



- While security cameras can capture a crime occurring, they don't necessarily work as a deterrent; reviewing footage after the event is futile.
- Only a multi-layered approach is fully effective at deterring criminals; while one layer may be defeated, the remaining layers continue to offer protection.
- Police are more likely to respond sooner to an integrated verification system combining multiple alarms and video footage.



An integrated system accounts for redundancy. So, if something fails in the system or there's a breach, there's another piece of the system that can continue to offer protection. It's vital to accept that certain parts of a security system will be defeated and to have additional layers to prepare for that."



Drew Leppert

VP of Enterprise Sales, AMAROK Security

INVEST NOW VS. INVEST LATER: ALL GAIN, NO PAIN

Investing sooner rather than later in integrated perimeter security offers considerable business benefits. If no action is taken, your business will remain at substantial risk of becoming a victim of crime. As we've discussed, the cost of crime can be immense, having a lasting financial, operational, and reputational impact on your business. Although it's difficult to measure the efficacy of a security system if it's never been breached, it's important to trust in trends and the cost of typical losses. After all, while it's impossible to predict the future, it *is* possible to prepare for it. The risk level, the number of assets, the value of those assets, and all the other indirect costs need to be weighed against the cost of investing in integrated and layered perimeter security.



Businesses can justify the spend by comparing the number of assets they have on-site, the asset value, the indirect costs associated with losing those assets, and the risk level in that area against the cost of any security system; justification calculators can help them truly understand why they're making the investment."



Michael Dorrington

SVP, Sales and Marketing,

AMAROK Security



The capital approach to perimeter security is a heavy upfront investment into the unknown. You still have to pay for maintenance, upgrades, and refreshes, so costs aren't actually fixed. With the operational expense of security as a service, it's much easier to budget."

VP of Enterprise Sales, **AMAROK Security**



The type of investment you need to make in security has evolved. Traditionally, the only way to account for the expense of perimeter security was to make a large initial capital investment in fencing and video surveillance equipment. However, today perimeter security is offered as a managed service on a subscription basis. This offers distinct advantages.

First, with a managed service, you're investing in the highest quality, most up-to-date product on the market. Second, it will remain current. As thieves constantly work to improve their skills, your provider can do the same to ensure your security measures are always one step ahead. Third, managed security is scalable. You pay for exactly what you need and can then upgrade or expand easily to match company growth without wasting money. Finally, budgeting

becomes much easier. There are no unforeseen costs as maintenance, repairs and replacements become the responsibility of the provider rather than your business. This can reduce downtime and ensure continued operational efficiency.

Coming up with a large amount of capital to buy a new security system can be extremely challenging for any business. However, although spending in the security world is often thought of as a one-time cost through capital expenses, security as a service has changed that. By putting security in the category of operational expenses, the need for a large upfront investment is removed, releasing cash flow into your business. A monthly service fee is often more manageable to budget for than a substantial capital investment.

The total cost of ownership (TCO) can be useful to compare the cost of one-off security to a managed service. Not only are upgrades and maintenance costs included in the latter, but the security measures themselves are more cost-effective than traditional approaches. In addition, by investing in enhanced security, businesses can have more confidence in their ability to protect their business, reduce their insurance reserves and make significant savings.

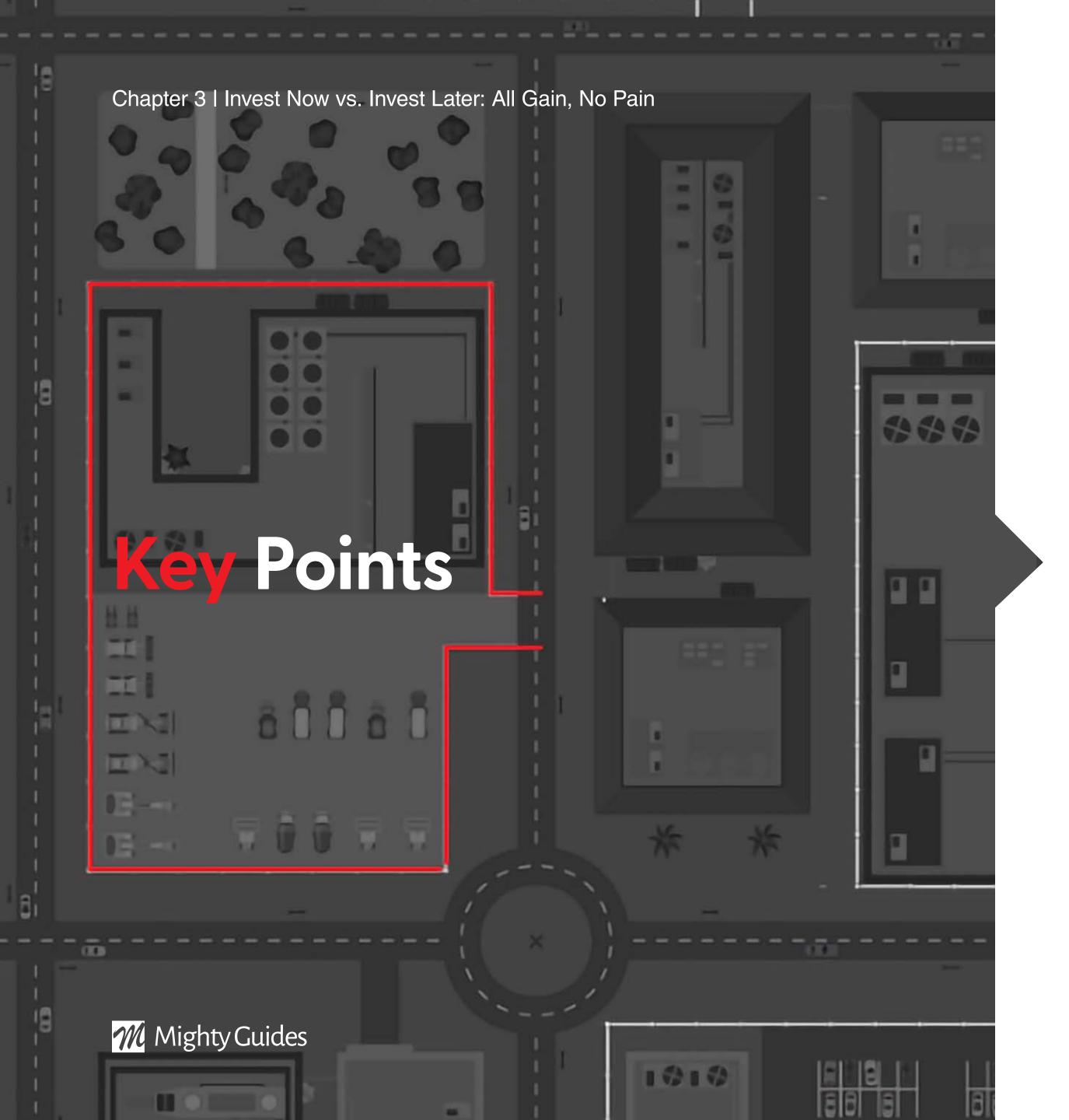


When thinking about perimeter security, you need to take into account unforeseen events, such as severe weather (e.g., hurricanes, floods) and extended shutdowns (e.g., holidays, pandemic). Are you protected in these circumstances?"



Dr. Christopher Shaffer

Corp. Director, Security and Safety Compliance, Valmont Industries



- To justify the cost of investing now in perimeter security, businesses need to weigh the risk level versus the total cost of a breach.
- With security as a managed service, upgrades and maintenance costs are covered and businesses can make significant savings.
- Investing in security as an operational expense is often more manageable than a substantial capital investment.

THE CONSEQUENCES OF INVESTING LATER

By waiting to invest in perimeter security until a crime has taken place, you're putting your business at significant risk. Ultimately, once there's a break-in, it's too late. The costs of crime can easily mount up in terms of the cost of assets stolen, downtime, reduced production and operational efficiency, loss of revenue, reputational damage, and more. Although you can replace assets, you can't recoup their costs and that can have a significant and far-reaching impact.

Not only do victims of property theft have the direct and indirect costs of the initial crime to account for, but they're at a much higher risk of being targeted again. The problem is that the successful attack highlights your business as an easy target to other criminals. Not only do they know that you're suffering the damages of the first incident, but you're likely in a state of panic. With your guard down and the time required to put improved security in place, you can inadvertently create further opportunities for your adversaries.



The Equation: Risk = (Likelihood a negative event will occur) x (Potential cost) can help you quantify a security risk to your business. Then you can consider the cost of the risk against the cost of the solution and how much that solution reduces the likelihood of that risk from happening."



Brock Josephson

Sr. Physical Security Specialist, Burns & McDonnell

Chapter 4 | The Consequences of Investing Later

Another significant downfall of waiting until an incident takes place before investing in perimeter security is that you don't allow yourself enough time to assess your options. There are many different types of perimeter security and several options to consider with a managed security offering. You're much more likely to make a well-considered, educated decision with time on your hands. If you're in a panic to rectify a gap in security, it can easily result in siloed solutions being put in place that don't work together effectively. When this happens, you're essentially losing more money and increasing the overall cost to your business.

It's no good waiting for something to happen and then assessing the risk. You should constantly audit the risk level of your business and put the appropriate measures in place to effectively manage that risk. The alternative is investing too late, investing in the wrong solutions and increasing business risk.

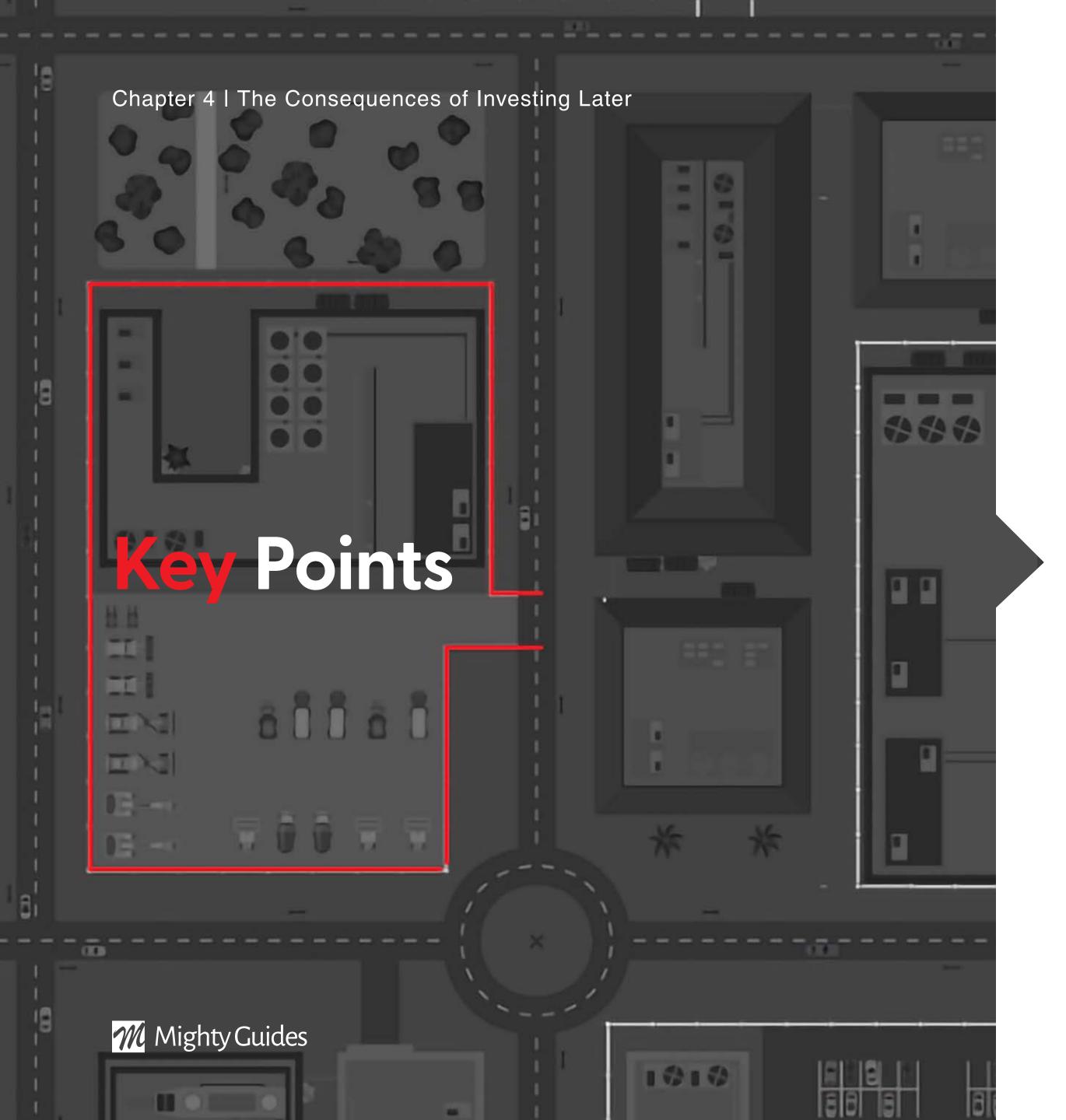


Security is more about preventing crime than reacting to it. Putting in the appropriate security controls and taking a risk management approach will save time and money."



Keith James

Security Director, Corporate Security, Exela Technologies



- Implementing security measures after a break-in is too little, too late; the damage is done and the costs will easily mount up.
- Once a company becomes a victim of crime, it's much more likely to be targeted again, increasing business risk considerably.
- Implementing reactive security measures can easily result in siloed solutions being put in place that don't work together to improve security.



Reactive security is often too little too late because companies are starting from absolute zero. Once a crime has taken place, they're in a state of panic to rectify the problem; they have no idea what the market is like and what solutions are available and can easily throw good money in the wrong direction."



Michael Dorrington

SVP, Sales and Marketing, AMAROK Security

THE BENEFITS OF INVESTING NOW

The most obvious benefit of investing now in integrated perimeter security is that it reduces the risks of the direct and indirect costs associated with crime. As such, it can deliver a quick return on investment. However, there are also many intangible benefits of investing; after all, there's no way to put a number on peace of mind.

By investing now and demonstrating a commitment to security, you can increase staff retention, boost employee morale, and improve company culture. When an employer shows they care for their employee's well-being, they are much more

likely to be dedicated to your success. However, when it comes to physical security, it's more than that. Companies have a duty to keep their employees safe. If the police don't respond to a security incident, an employee usually has to step up to try to defend the company premises and its assets. Although the human experience of feeling safe at work isn't completely tangible, nobody should have to go to work feeling at risk. If security and safety aren't priorities, staff retention will fall, and the costs of recruitment and training can easily mount up.



Businesses can link a one-time investment in perimeter security with a Business Impact Assessment of an operation disrupted or shut down for set periods of time. Perimeter security is the first layer of a multi-layered approach to avoiding disruption caused by unauthorized outside parties/hostile intruders."



Brian Stephens

Sr. Managing Director, Teneo Risk Advisory, Teneo



In the K-12 school bus industry, the bus yard contains two of our most valuable assets—our employees and our buses. How we approach perimeter security helps us reduce incidents and set the tone for our company security culture."

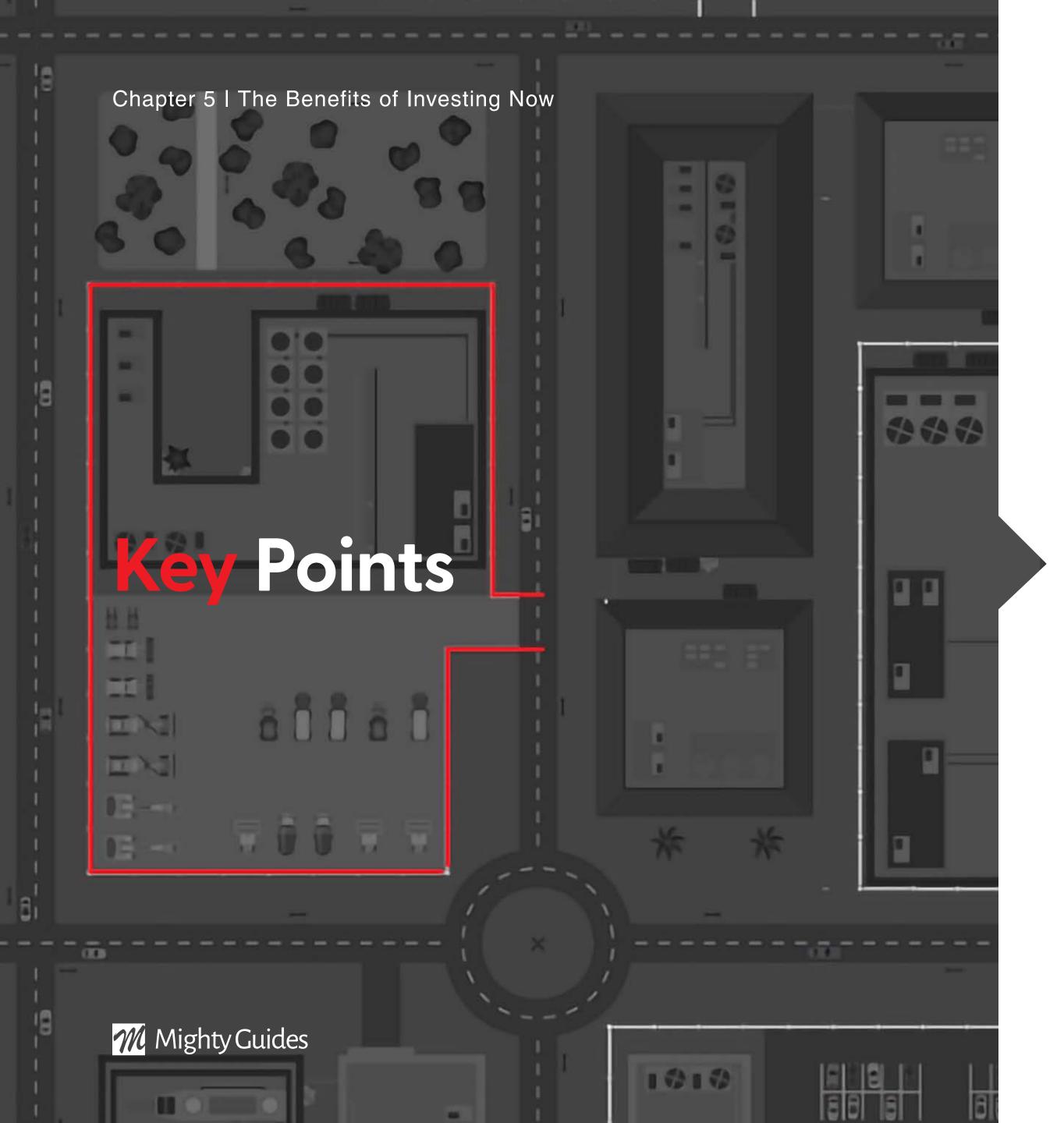
> Sr. Manager, Security, First Student



Besides needing to know that their employees are safe, every business must uphold its promises to suppliers and stakeholders. That means being able to deliver goods and services on time. Ultimately, by demonstrating a commitment to security, a company becomes a more attractive business partner. Security has a place in the business case for suppliers and customers alike; it's proof of a commitment to protect the supply chain and everyone involved. After all, people want to work with and buy from people they trust, who will be reliable, and who can show they know what they're doing. By showing that security is a top priority, companies can lower the risk of doing business with them and gain a significant competitive advantage.

Also, although physical security and cybersecurity have been discrete functions, there's now a need to bring them together with an effective risk-based security policy.

Security standards for all devices should be on par with corporate computers and servers. Because the security risk is real for both, companies need to think about physical security audits, policies and standards in the same way as they approach cybersecurity. As the integration of physical security devices, such as security cameras and alarms, into the business network continues to rise, having an advanced, up-to-date perimeter security solution will pay dividends.



- Companies need to know that their employees are safe and that they'll be able to uphold their promises to suppliers and stakeholders.
- By demonstrating a commitment to security, companies can lower the risk of doing business with them and gain a significant competitive advantage.
- Businesses should approach physical security audits, policies, and standards in the same way as cybersecurity; the risk is very real for both.

Learn More About Our Experts



Michael Dorrington SVP, Sales and Marketing, **AMAROK Security**

in

Michael is active in the cargo security and theft prevention community. He is a member of SWTSC, SETSC, MWTSC, and CargoNet and works closely with these agencies and AMAROK's enterprise customers to stay on top of security trends and ensure theft prevention is front and center. Michael holds a BA in Communications/ Public Relations from Michigan State University with formal sales training in Challenger and Requirements Based Selling methods.



Keith James

Security Director, Corporate Security, Exela Technologies

in

Keith James is the Senior Director of Corporate Security at Exela Technologies. He has more than 15 years of experience securing facilities, protecting assets, and mitigating risk. He's partnered with government, law enforcement, and private sector counterparts to implement strategies for physical security, emergency preparedness, crisis management, and business continuity.



Brock Josephson

Sr. Physical Security Specialist, Burns & McDonnell

Brock Josephson is a Senior Physical Security Specialist at Burns & McDonnell. He specializes in electronic security system design including electronic access control, intrusion detection, and video surveillance. Brock has over 10 years of experience in security design and implementation for critical infrastructure, government, military, and commercial industries and is an ASIS Board Certified Physical Security Professional (PSP®).



Drew Leppert VP of Enterprise Sales, **AMAROK Security**

in

Drew is responsible for developing strategic security plans, educating customers, and sustaining loyalty for AMAROK's enterprise customers. He is a member at ASIS and a member/ speaker at SIA, ATA, and CargoNet. Drew is a merit graduate of the United States Naval Academy and served as Captain in the United States Marine Corps for five years. He also holds a Master's in Business Administration (MBA) from Emory University.

Learn More About Our Experts



Joe Redmond Sr. Manager, Security, First Student

in

Joe Redmond is currently the Senior Security Manager in the Enterprise Security Department, supporting First Student. After proudly serving his country, Joe pursued a career in law enforcement. He joined First Student in 2019 where he has led several initiatives to secure vetted security vendors, reduce costs, and increase efficiency by reevaluating physical security and the security culture at various locations. Joe is a Certified Protection Professional (CPP) through ASIS international.



Dr. Christopher Shaffer

Corp. Director, Security and Safety Compliance, Valmont Industries

in

Dr. Christopher Shaffer is the Corporate Director of Global Security at Valmont Industries. He specializes in global security and executive / dignitary protection. Chris is former military and law enforcement. He is also certified in Homeland Security, tactical medicine, and other areas specific to global security.



Brian Stephens

Sr. Managing Director, Teneo Risk Advisory, Teneo

Brian Stephens is a global security executive focused on security technology, crisis and event response, and security as a service. He is currently serving as the Senior Manager Director, Teneo Risk Advisory at Teneo. He is also the Co-Director of the Policing, Security Technology & Private Security Research and Policy Institute at Florida State University College of Criminology and Criminal Justice.



Dr. Celvin G. Walwyn

Deputy Commissioner of Police, US Virgin Islands Police Department

Dr. Celvin G. Walwyn is the Deputy Commissioner of territorial police operations for the police department of the Virgin Islands of the United States. He has 35 years of experience in investigations on the local, state, and federal level and has served as chief, deputy police commissioner, and police commissioner. Dr. Walwyn has been married to his wife Antoinette for over 30 years and has four daughters and one son.

DO YOU KNOW WHAT YOUR PROPERTY THREAT RISK LEVEL IS?

SCHEDULE AN ASSESSMENT

AMAROK knows how difficult securing a commercial site or property can be. With theft and vandalism on the rise, we can transform your business perimeter from an easy target to one that criminals will not want to mess with.

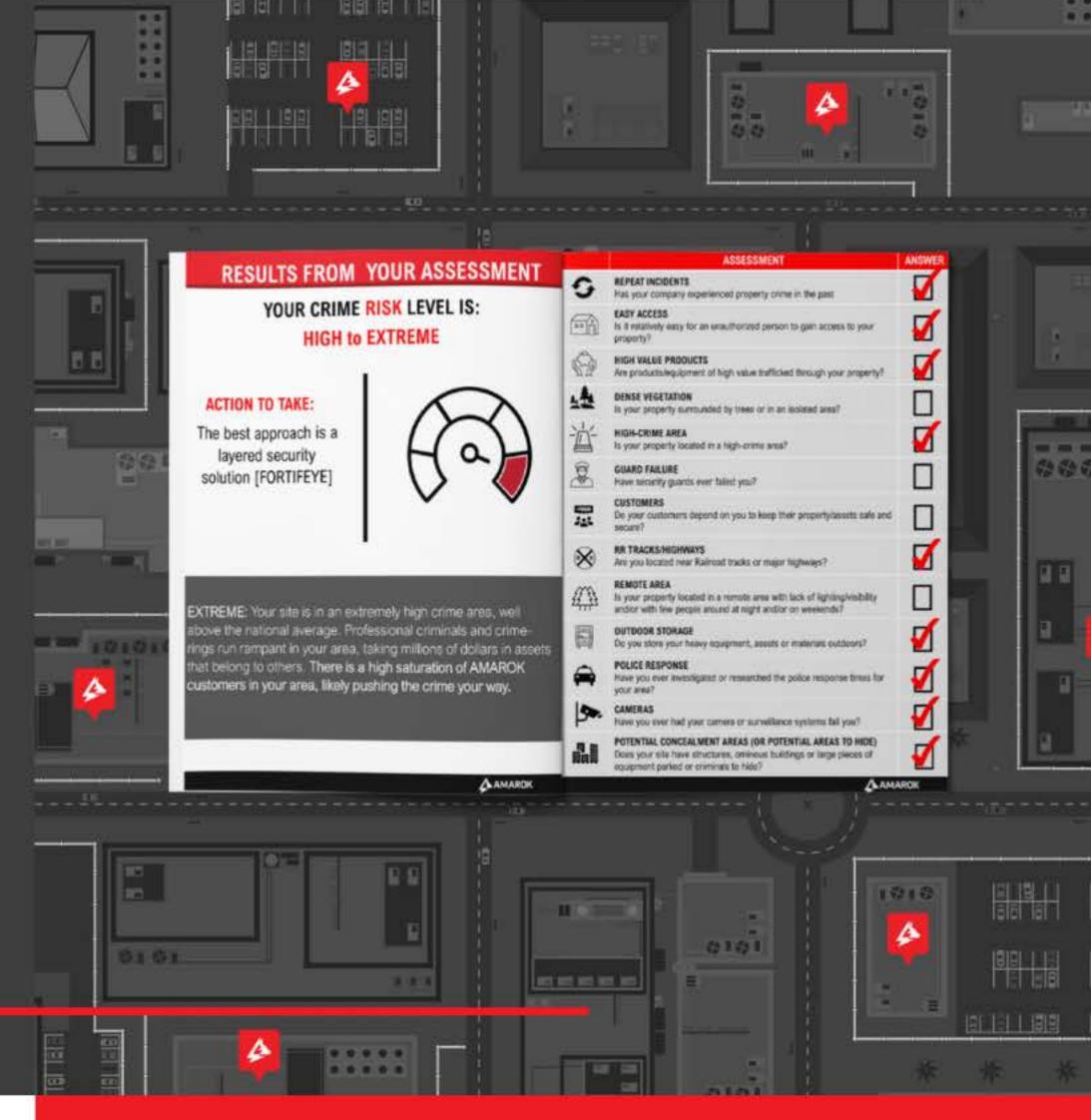
We help businesses like yours stop crime before it happens. PERIOD.

FIND OUT YOUR THEFT RISK

Set up your FREE property assessment at:

www.amarok.com/threat-assessment

(866) 770-4935





500 Assembly Street I 5th Floor Columbia I South Carolina I 29201