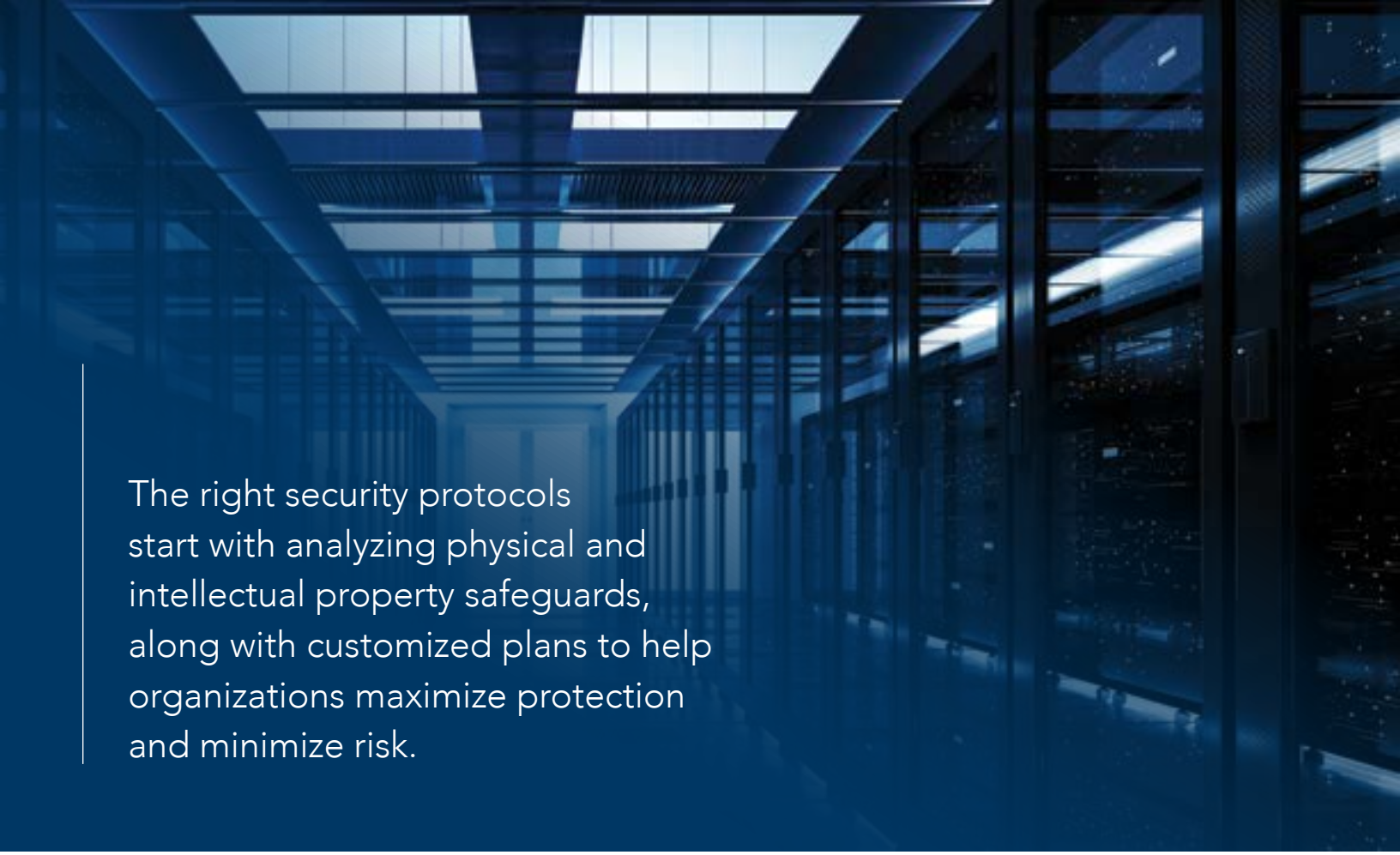
WHITE PAPER

Customer-Specific Solutions to Safeguard Your Business

WHY EXPERT SECURITY PROTOCOLS ARE KEY TO MAINTAINING PROTECTION AND UPTIME

STREAM
CRITICAL ENVIRONMENTS



The right security protocols start with analyzing physical and intellectual property safeguards, along with customized plans to help organizations maximize protection and minimize risk.

SECURITY MANAGEMENT IN THE AGE OF VULNERABILITY

Corporate security is not optional. Scarcely a day passes that we don't see the result of a breach, whether from a physical attack or an information leak. Yet many businesses don't understand the full range of environmental and organizational policies required to mitigate risk. While security technology companies and guard force providers are important elements in prevention and protection from threats, they may not have the experience and perspective to provide broad security solutions. Stream Critical Environments Security Consulting provides proactive analysis of your total security program, offering unbiased solutions that align with your business goals and respect your budget constraints.

ASSESSING YOUR OWN SECURITY

The decision to bring in a security consultant starts with an honest look at your current program. Are your security and safety policies based on an unbiased assessment of risk? Are the policies accompanied by specific procedures to address threats? Are you certain that your employees adhere to those procedures? Do your employees and customers feel safe at your workplace? What threats to security have happened in the past? How did you respond? Do your policies and procedures fit the way you do business?

Knowing the facts about the strengths and weaknesses of your current program enables you to have a realistic and productive discussion with an experienced security consultant to identify possible solutions. Knowing your company's specific needs is crucial in developing a comprehensive security program that checks every box.

BUSINESS CONSIDERATIONS

Operational Impact

Too often, a company brings in security consultants after a breach that has employees feeling vulnerable. Whether the incident was a theft, a break-in or a digital security breach, management understands that they must remedy the situation immediately or risk litigation. Heightened awareness frequently comes from an event that happened elsewhere but is within the realm of possibility at your workplace. Regardless, when employees are fearful, they may be preoccupied with potential threats instead of focusing on job performance.

Audit requirements

For many businesses such as data centers, federal facilities and banking/investment firms, audit compliance requires a threat risk vulnerability assessment. An independent assessor must evaluate risk and present a remediation strategy. A security consultant can complete the process efficiently and cost-effectively — and propose ways to deal with exposed vulnerabilities proactively.

Violence prevention training

Investigations of workplace violence often reveal that signs of a possible incident were evident long before the violent behavior occurred. Managers must understand what to look for and how to report potential problems as well as how to refer the employee to HR for help. Security consultants offer proven training programs that can help prevent a tragic event.

Active-shooter preparation

An unfortunate fact of life is the frequency of workplace shootings, even when managers know how to spot the precursors of such an incident. In the moment, the key is survival, and employees can be trained in the best ways to protect themselves from harm.

Work-related travel security

Your company has a duty of care associated with employees who travel for business. International security alerts are helpful, but too generic to provide protection. A security consultant can train employees in awareness and protection while on the road, demonstrating that your company takes reasonable precautions to ensure the safety of traveling employees.

THE SECURITY ASSESSMENT

A thorough security evaluation must include specific protocols for enterprise protection.

Physical security risk assessment

Environmental considerations are important to ensuring business continuity regardless of location and surroundings. This part of the assessment includes these elements:

- **Threat of natural/industrial disasters -** Is your business in a tornado-prone area or a coast with hurricane potential? Are you on a flood plain? Are nearby businesses at risk of industrial accidents that could damage your workplace?

- **Crime or civil unrest -** Are you located in a high-crime area that could subject your employees and business to increased criminal activity? Is your business safe from the risk of violent outbreaks due to protests against nearby businesses or community incidents? Who monitors the area for potential problems?

- **Existing technologies -** What security technology is in place? Is it up-to-date and functioning properly? Is it monitored? Does your security team stay abreast of anomalies?

- **Policies and procedures -** What written security policies are in place? How is compliance monitored? Are security violations taken seriously and handled appropriately? Are employees and vendors trained in security and emergency procedures?

- **Executive protection assessment -**Are members of your executive management team vulnerable to risk? What protection measures are in place? Are executives and security personnel aware of what to do in case of a threat?

Policy and procedure evaluation and development

Most businesses have security procedures in place. But having procedures does not mean that they are sufficient to protect your business. At minimum, these areas must be assessed to determine the best security protocol and the people responsible for enforcement:

- **Guard force standard operating procedures -** If you use a guard force company, what are its minimum requirements for guards? What are the specific responsibilities of your guard force? What training is outlined in your company's security policies and procedures?

- **Mobile device policy -** Do you have a written mobile device policy? Are employees required to sign acknowledgements that they've received the policy? Can employees bring their own devices to work? How do you protect data on mobile devices? Do you have a policy on using mobile devices while driving?

- **Employee email protocols -** Is each employee assigned a company email address? Are they allowed to use that address for personal correspondence? Do you require written acknowledgment that company emails may be monitored?

- **Information protection protocols -** How does your company protect proprietary information and trade secrets? Do you assign access to protected information according to job duties? How do you prevent employees from sharing protected data?

- **Site access and visitor management protocols -** How do you monitor physical access to your business? Do you have secured entrances? Are visitors required to present identification and sign in? Do you verify that visitors have appointments or permission to be on the premises? Are sign-in sheets reviewed?

Security Awareness Training

Employees may understand the basic elements of safety, but they must learn to be aware of their surroundings. Training can help employees develop automatic responses to keep them secure in life-threatening situations. Key topics include:

- **Travel security -** Do you have a written travel safety manual? Do you follow up on international security alerts to determine threat levels to your employees? How do you train employees to travel safely domestically and globally? Do employees know how to prepare luggage, stay safe at the airport, select the safest hotel room and respond appropriately if a violent situation erupts?

- **Active-shooter response and survival -** Do employees know what to do in an active-shooter incident? Does your company conduct active-shooter training and drills to help employees respond appropriately and raise the chance of survival? Do you have discussions of safety precautions in the aftermath of a workplace shooting elsewhere?

- **Tabletop exercises and drills -** Do you have drills or tabletop exercises that simulate emergency scenarios in a classroom setting? Are key personnel with emergency management roles and responsibilities clear about what actions they need to take in an actual incident? Do you have discussions with these individuals that add complexities to allow problem solving?

SECURITY SYSTEM DESIGN

Protection of your premises and employees starts with proper use of a security system that monitors activity and access at all times. An experienced security consultant can help with:

- **Video management system -** Are security cameras visible and operational 24/7? Do they integrate with other security systems? Who monitors the cameras? Is security footage reviewed regularly? Who is responsible for the review?

- **Access control system -** Do employees have ID cards that determine access to secured parts of your business according to job function? Is entry and exit recorded and monitored? Are written procedures in place for issuance and revocation of company access cards? What other access control systems are in place?

- **Integrated systems to monitor triggered events -** What happens when a security breach occurs? Who receives notification? Are employees trained in proper response to a security alert? Is an alert in one area broadcast to other areas?

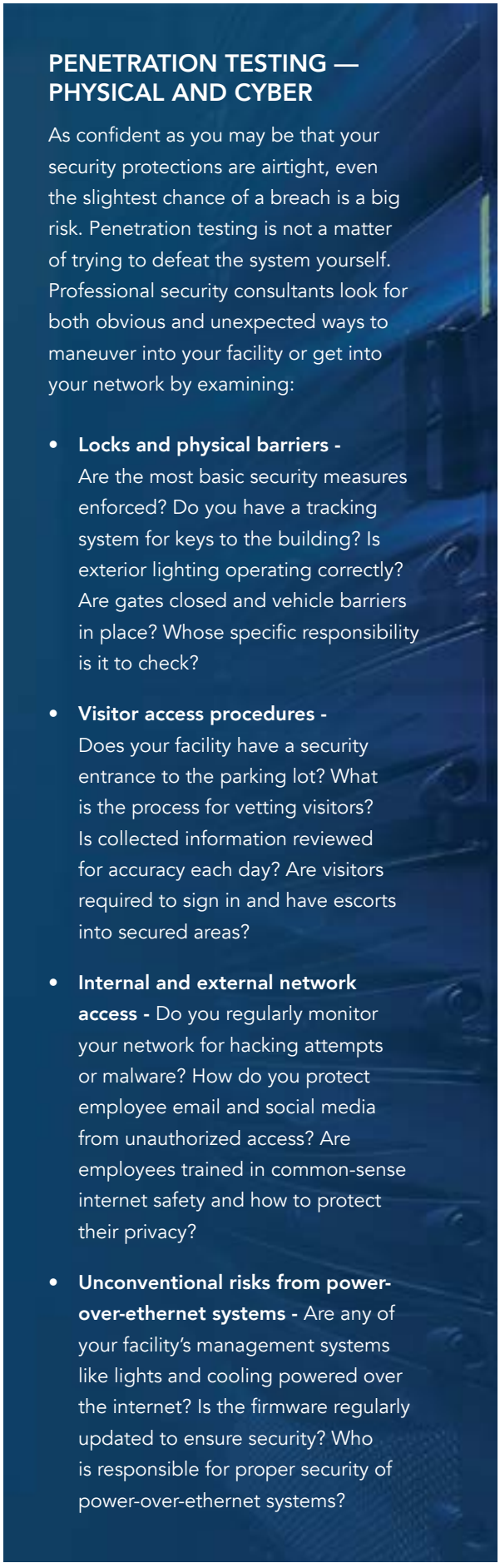
SECURITY VENDOR MANAGEMENT

Evaluating business security includes an objective evaluation of your current security and/or guard force company. An objective security consultant is not connected to a particular vendor and will provide the pros and cons of different security companies to assist you in vendor selection. Security management can even involve day-to-day supervision of your security protocol, allowing dedicated monitoring of security. Security vendor consulting may include:

- **Due diligence on security firms -** Has your current security company been reviewed in light of your current business goals and practices? Has the security company been under scrutiny for incidents at companies other than yours?

- **Oversight of policies and performance -** Are members of the security staff trained in your company policies and procedures? Do they have written copies of their scope of responsibilities and how they are expected to meet them? What is the process for handling employee complaints against specific security staff members?

- **Guard force provider contract bid/award/oversight -** Do you periodically ask for competitive bids from guard force vendors? Do you know if your current provider's contract provides the best value for its services? Would you benefit from an objective party handling the bidding process, including meetings, discussions and even contract negotiating? Once you have selected a guard force, who is responsible for ensuring that they adhere to your policies and procedures?



PENETRATION TESTING — PHYSICAL AND CYBER

As confident as you may be that your security protections are airtight, even the slightest chance of a breach is a big risk. Penetration testing is not a matter of trying to defeat the system yourself. Professional security consultants look for both obvious and unexpected ways to maneuver into your facility or get into your network by examining:

- **Locks and physical barriers -** Are the most basic security measures enforced? Do you have a tracking system for keys to the building? Is exterior lighting operating correctly? Are gates closed and vehicle barriers in place? Whose specific responsibility is it to check?

- **Visitor access procedures -** Does your facility have a security entrance to the parking lot? What is the process for vetting visitors? Is collected information reviewed for accuracy each day? Are visitors required to sign in and have escorts into secured areas?

- **Internal and external network access -** Do you regularly monitor your network for hacking attempts or malware? How do you protect employee email and social media from unauthorized access? Are employees trained in common-sense internet safety and how to protect their privacy?

- **Unconventional risks from power-over-ethernet systems -** Are any of your facility's management systems like lights and cooling powered over the internet? Is the firmware regularly updated to ensure security? Who is responsible for proper security of power-over-ethernet systems?

CHOOSING A SECURITY CONSULTANT

While business security needs have changed over the past decade, the goals have not. Security consultants still focus on creating barriers between critical assets and outside access.

The "Concentric Rings" Model, an Industry Standard, is a Visual Representation of this Multilayered Approach

DETER, DELAY, DETECT

While the number of layers may vary depending on the business, each ring represents a security barrier geared toward deterrence, delay and detection. Deterrence, for example, could be visible barriers like fences, cameras and security guards. A criminal will likely see those things and keep going. If not, the next set of barriers, whether a person, a vehicle barrier or a sensor, will delay entry. Next is detection of the threat, which triggers action to counter the particular type of security breach. Optimally, these three barrier levels are integrated so that triggering one level heightens security at the next.

BUSINESS CONTINUITY PLANNING

Even when your security system is at its best, smart businesses prepare for the worst. A security consultant will tap into these and other areas to help you develop a plan that will ensure business continuity in the case of a crisis:

- **Key stakeholder insights -** What tools and resources do key operations employees need to keep their areas functioning during a crisis event? Do you know that they have those things?

- **Pinpointing mission-critical functions -** What specific departments and functions are essential to keeping your business open? Do the managers and personnel of these areas know what to do in crisis situations? Have you brought those people together to help develop a contingency plan?

- **Clear protocols for staff and systems -** Do you have a written crisis management plan? Are specific employees informed of their responsibilities and standards of operations to maintain business continuity? How will you ensure that your systems and information continue operating in the aftermath of a crisis?

THE IMPORTANCE OF EXPERIENCE

The challenge of security program development is that while security systems and methods continually improve, new threats are not far behind. That's why your security consulting team must have extensive experience in integrating all aspects of protection, from global security management to executive protection to cybersecurity. Securing the network without appropriate access controls or software updates, for example, leaves you vulnerable.

Stream Critical Environments Security Consulting has the expertise and perspective to view all layers of security and build barriers that mitigate risk proactively. Our team sees beyond current threats to what you may encounter as your business expands. We propose scalable solutions that align with how you work today and your goals for the future.

Our services go beyond those of many security consultants, and we are vendor-neutral in our assessment process. If you need an evaluation of security policies and procedures to meet audit requirements or want a comprehensive review to determine the safety of your business and employees, Stream offers an objective analysis with solid recommendations for a multilayered security program. From there, you can opt to have us manage your security program using the providers you choose, or you can implement the program yourself. Whatever the scope, you can count on Stream to listen to your needs and propose a tailor-made solution that protects your business at every level.

CHRISTOPHER D. MILLER, CPP

Stream Critical Environments Services, Director of Corporate Security

Chris draws upon the insights gained over his 25 years of experience in global security management, investigations, executive protection and incident management to provide Stream customers with comprehensive strategies and tightly targeted tactics to protect their assets. Over the course of his career, Chris has been instrumental in security operational management, vulnerability assessments and remediation for such high-profile customers as AIG worldwide, Equinix, T5 Data Centers, Dyson Technologies, Tyson Foods, city and college police departments and many more.

As both a licensed security consultant and a private investigator, Chris is well-versed in a broad range of security assessment and operational issues, including security management, site security vulnerability assessment, and executive protection at home and abroad. His professional affiliations include ASIS International, InfraGard and the North Texas Crime Commission.

ABOUT STREAM DATA CENTERS

Stream Data Centers has been providing premium data center solutions to Fortune 500 companies since 1999. Product offerings include Hyperscale Data Centers, Private Data Centers™and Suites, Ready-to-Fit™ Powered Shells, Retail Colocation and Build-to-Suit Data Centers — all with immediate connection to network carriers and public cloud providers.

Above all, Stream is dedicated to improving the data center experience through exceptional people and service. Services supporting critical environments and energy procurement leverage the combined skill sets and resources of Stream's technical real estate professionals with fine-tuned data center and energy management expertise, to deliver an end-to-end solution for all mission-critical infrastructure needs.

Stream Data Centers is a subsidiary of Stream Realty Partners, L.P., a full-service commercial real estate investment, development and services company. Founded in 1996, Stream Realty employs hundreds of real estate professionals, managing commercial properties across the nation.

Contact us for a consultative review of your security needs:
sales@streamdatacenters.com

STREAM
CRITICAL ENVIRONMENTS

2001 ROSS AVENUE, SUITE 400 | DALLAS, TX 75201

214-267-0400

STREAMDATACENTERS.COM