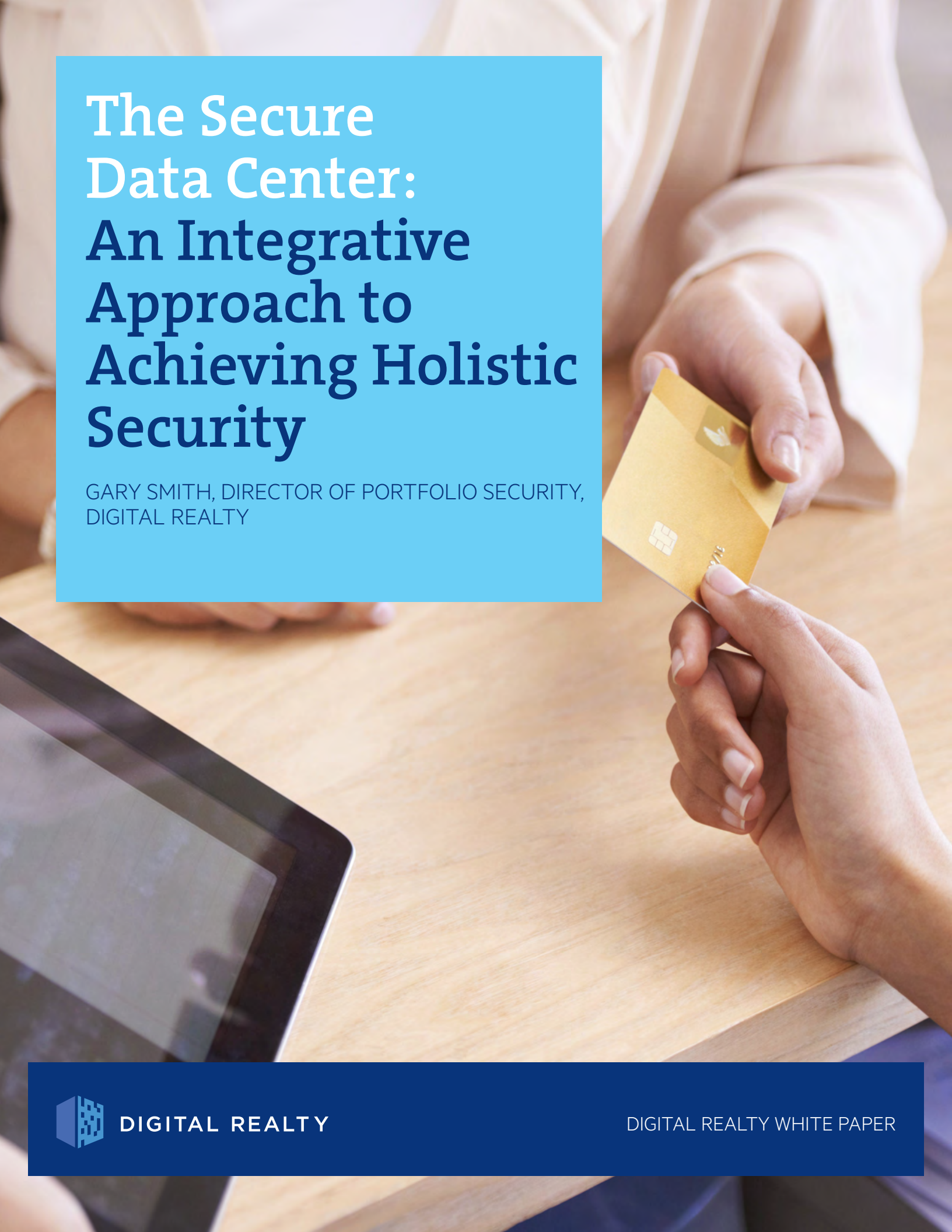

The Secure Data Center: An Integrative Approach to Achieving Holistic Security

GARY SMITH, DIRECTOR OF PORTFOLIO SECURITY, DIGITAL REALTY

DIGITAL REALTY

DIGITAL REALTY WHITE PAPER

Today's headlines are replete with accounts of major corporations that have found themselves **under attack for their enterprise data.**

The threats facing businesses today are arguably the most aggressive and dynamic in history, with data centers' infrastructure comprising a paramount element in the first line of defense for many companies. The advent of mobile and cloud computing has compounded the calculus, driving increased dependence on third parties as significant contributors to a company's enterprise security posture.

As the trend toward data center outsourcing continues to grow, organizations find themselves relying heavily on the ability of their data center providers to deliver levels of security that meet their own rigorous standards. The provider's security plan is often integral to the foundation for a client's in-house protection mechanisms that support the confidentiality, integrity and availability of its data, and must therefore integrate seamlessly into a client's security plan.

Physical Security, Information Security— Why Not Simply 'Security'?

Ideas and concepts defining security have changed dramatically in the past 10 to 15 years. There was a time when security meant physical security, such as guards, gates and alarm consoles.

With the advent of distributed computing and the rise of the Internet, information security has become a recognized discipline requiring a blend of technical, policy and business acumen, and thoroughly professional practitioners. In the years since, data protection has come to occupy the attention of the C-suite, and savvy information security professionals understand that the foundation for a strong enterprise security program includes physical protection of assets.

But the confluence of physical protection and logical controls is not the only component of a sound security program. Incident management, resiliency and compliance are also critical aspects of any holistic effort to provide best-in-class security. And, of course, the keys to making all of these parts coalesce into a smoothly running, optimized system focused on client success are the people and processes that define its operation.

Please see Figure 1 for a model articulating the holistic, integral approach to security. In the following sections, we will endeavor to break the model down into its component parts.

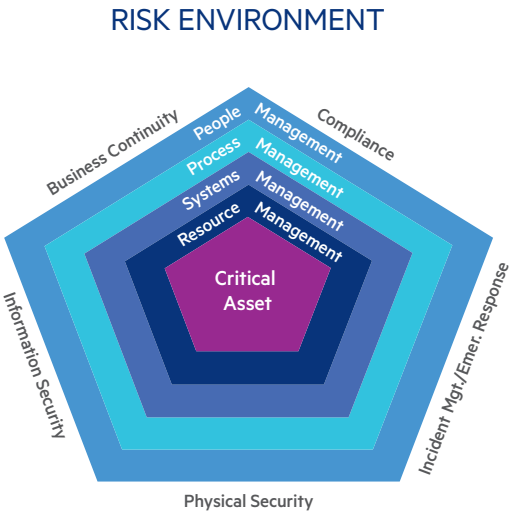

Figure 1

DIGITAL REALTY'S INTEGRATED APPROACH TO PHYSICAL SECURITY COMBINES INDUSTRY-LEADING PLATFORMS WITH PROVEN, TESTED PROCESSES, AND TRAINED, DEDICATED SECURITY PERSONNEL.

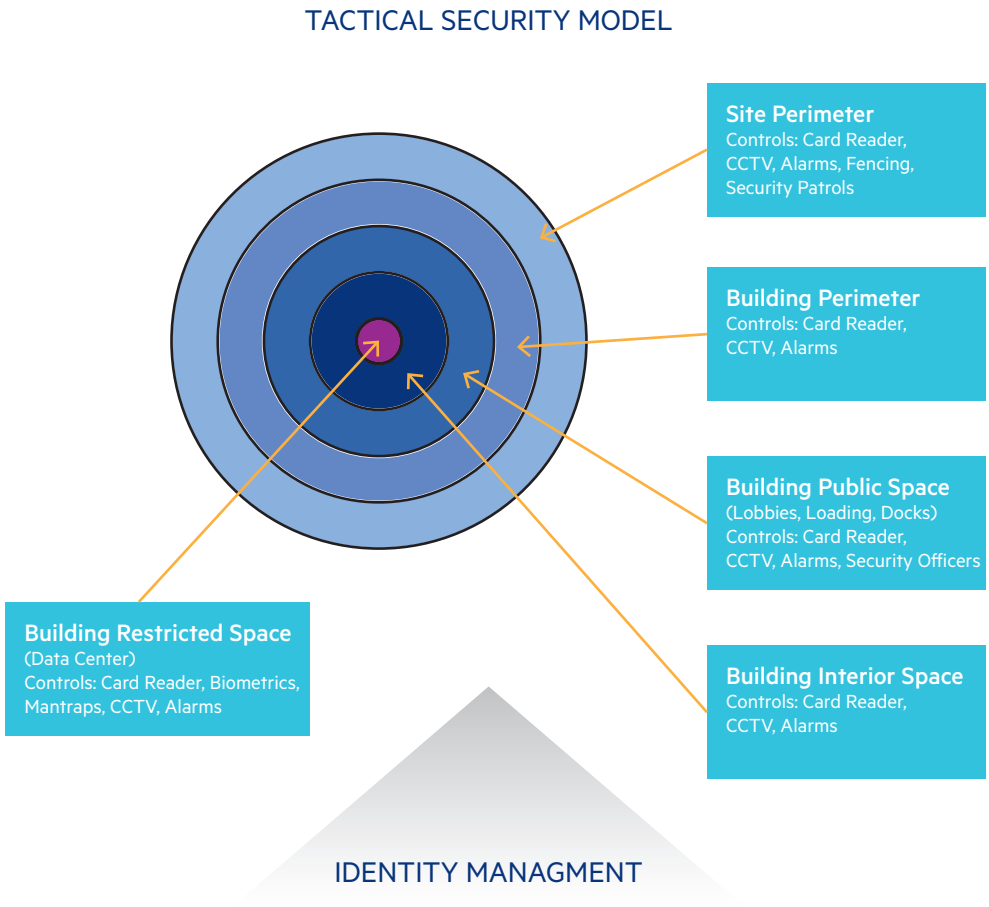

Figure 2

PHYSICAL SECURITY

Unquestionably, the foundation upon which any effective security program is predicated is physical security, which represents the fundamental processes and functions associated with access control and environmental monitoring. Controlling who has access to what, and monitoring the where, when and how that access is then used, constitutes the primary objective for all security professionals. Regardless of how effective other security protocols and systems might be, if access control is compromised, the entire security paradigm becomes moot.

Digital Realty's integrated approach to physical security combines industry-leading platforms with proven, tested processes, and trained, dedicated security personnel to restrict access to your vital data center assets to only those persons whom you decide should be granted that right. Digital Realty's primary physical security platform integrates access control, intrusion detection and video management into a single, unified interface, easing task demands on personnel and presenting essential information in a clear, cohesive format that facilitates rapid response.

Alarm monitoring is integrated with closed-circuit television (CCTV) to provide security officers with real-time video data for optimal situational awareness, resulting in a safer, more appropriate response. In addition, the ability to remotely monitor these data streams provides a powerful collaborative tool in the event that local first response agencies are called to the site to assist with an event, as they can be kept apprised of the changing nature of a dynamic threat in real time. Understanding the nature of the threat is the key to any effective response protocol, and technology has transformed the

INCIDENT MANAGEMENT, INCLUSIVE OF EMERGENCY RESPONSE, IS A FUNDAMENTAL AND CRITICAL COMPONENT OF ANY COMPREHENSIVE SECURITY PROGRAM.

ability to achieve that understanding from safe distances.

Digital Realty employs a multilayered controls methodology providing defense-in-depth protection for its clients' critical assets, as illustrated in Figure 2. Each layer acts as a protective barrier that must be progressively overcome to affect a breach as proximity to the critical asset increases. This not only offers positive protection for a client's critical infrastructure but buys valuable time to allow for the deployment of additional resources that can target the threat.

Perimeter controls may include fencing and manned security stations controlling vehicle access, along with overlapping CCTV and intrusion detection technology. All points of ingress and egress at the building are secured and monitored. Lobbies are staffed with trained security personnel, and standard configurations include card readers, CCTV and anti-tailgating measures. Interior restricted space controls incorporate the above and may also include biometric readers with floor-to-ceiling turnstiles if stipulated by a client's security requirements.

This meticulous approach to access control is further augmented with a comprehensive intrusion detection system integrated with CCTV video monitoring, which quickly identifies any attempt to bypass access protocols, presents actionable intelligence to security responders, and captures the information for later forensic and operational analysis. This not only facilitates an appropriate response to intrusion attempts but allows the lessons learned from such events to be captured and translated into continuous and active improvements.

Identity management is the key that unlocks each layer to provide access to appropriate personnel. Access to restricted areas must be authorized by a designated access area owner, and individual identity must be established using a government-issued ID prior to a badge being issued. These stringent authentication protocols, including multifactor and biometric authentication if required by the client, must be satisfied prior to access being allowed. Subject to emergency access and other requirements, a client can retain control of its space, and authorize who will be granted access. Digital Realty employees have undergone thorough background investigations, providing assurance to clients that staff entering their critical space and performing services for them have been carefully vetted.

Technical controls are important, but their effectiveness can only be optimized by trained, dedicated personnel. Digital Realty's security officers are trained in all aspects of its technical security systems as well as the processes and procedures that comprise an efficient data center operation. This includes response to emergencies, of course, but also to non-security-related events such as mechanical faults, leaks, etc., that might impact a client's critical load. Training is ongoing and updated in order that Digital Realty's security team can meet its clients' expectations under any set of circumstances.

Taken together, the technical, operational and administrative controls that comprise Digital Realty's physical security program provide clients with the peace of mind that comes from knowing their critical business operations are protected by a security team that is among the best in the industry.

INFORMATION SECURITY

Digital Realty understands that the confidentiality, integrity and availability of its clients' data are uppermost in their minds when it comes to securing this most critical of enterprise assets. While Digital Realty does not manage its clients' data, it does take very seriously its responsibility to protect the equipment within the facilities on which that data resides. This is the reason Digital Realty puts so much time and effort into the physical environment housing its clients' information systems.

But the company also goes to great lengths to safeguard its own information and building management systems (BMS), recognizing that they are critical to the services Digital Realty provides to its clients. These systems are protected by industry-standard network and configuration protocols designed to ensure the integrity of the network environment and systems.

Digital Realty's network is monitored and tested for vulnerabilities based on an ongoing assessment of risk. This allows the company to be able to implement a risk-based security framework that goes beyond just compliance. BMS and security systems operate on a dedicated critical facilities network segregated from Digital Realty's administrative network, and remote access sessions are encrypted and secure via IPSec protocols through VPNs.

In addition, policies and education are designed to make employees aware of their responsibilities to protect both Digital Realty's and its clients' confidential and proprietary information, and underscore the importance of information security as the responsibility of all its employees and suppliers.

Periodic reviews of security are provided to senior management, and incident-handling procedures are well-established to provide early detection, intervention and mitigation of any attempted breach. A dedicated team of information technology professionals oversees every aspect of the program and is on call 24/7 to guarantee that response to incidents is appropriate and consistent with the best interests of clients.

Collectively, Digital Realty's security team holds a number of information security certifications, including the Certified Information Systems Security Professional (CISSP) designation, the Systems Security Certified Practitioner (SSCP), Certified Chief Information Security Officer (CCISO), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), Member of the Business Continuity Institute (MBCI) and the GIAC Security Essentials Certification (GSEC), attesting to its expertise in this important discipline.

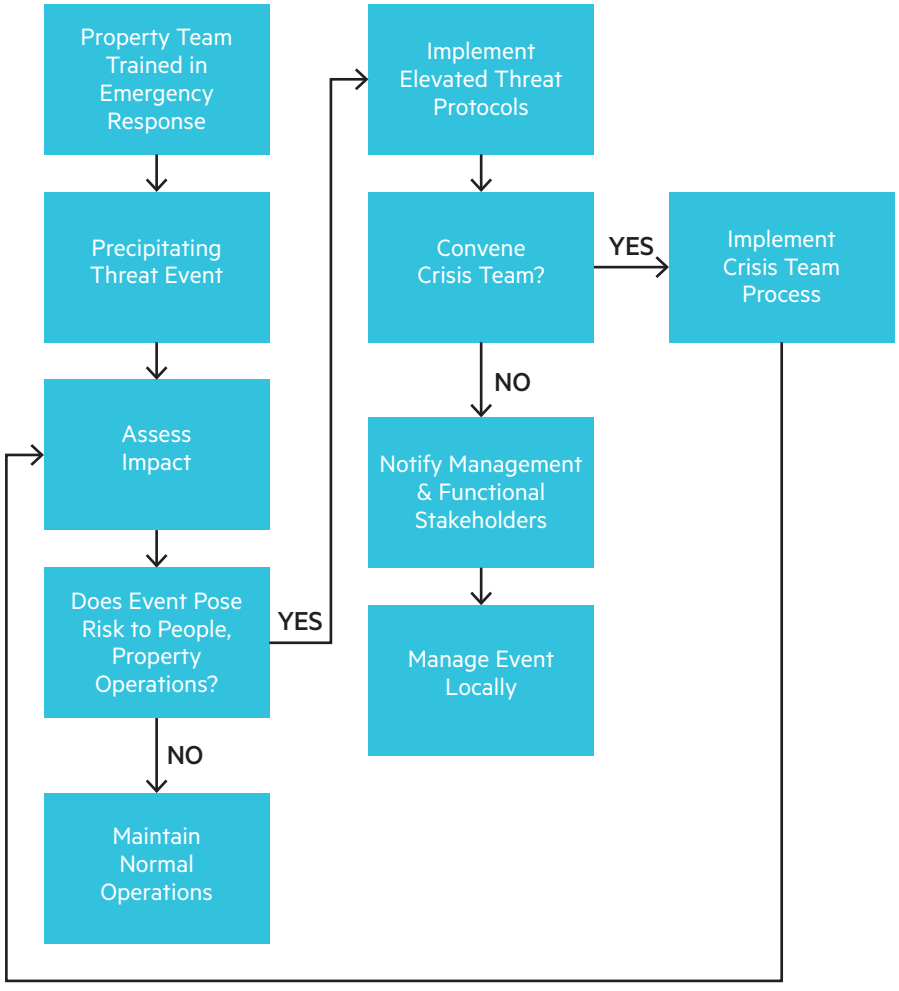

Figure 3

INCIDENT MANAGEMENT/ EMERGENCY RESPONSE

Incident management, inclusive of emergency response, is a fundamental and critical component of any comprehensive security program. An improper first response, particularly if aggravated by a lack of foresight and planning, can make recovery of the business after a serious event problematic, or even impossible. For this reason, Digital Realty focuses strongly on emergency planning and crisis management as key aspects of its overall incident management process.

When disaster strikes, being prepared is the difference between managing the event and succumbing to it. Every one of Digital Realty's data center locations maintains a comprehensive emergency response plan that is reviewed and tested annually. In addition, its portfolio security team conducts annual training for property managers in emergency response and threat assessment, focusing on the ability of local teams to respond properly and in a timely fashion to any emergency. The corporate crisis team provides guidance and oversight to ensure the local teams—those closest to and most familiar with the event and its impact—have the resources they need to properly manage the event and provide best-in-class support to clients, enabling them to focus on the continuing operations of their businesses.

Digital Realty's emergency response plans include contingencies for reasonably foreseeable risks or threats that may impact its clients, from earthquakes to tornadoes and bomb threats to terrorist events. The company employs a hierarchical set of threat protocols based upon the severity of the incident, with a decision-making process designed to provide a local response that is both appropriate and timely, as shown in Figure 3.

As illustrated, the process is predicated on continuous assessment of the event and its probable impact, integration of response protocols with support from the corporate crisis team, and effective management of the incident at the local level until the threat has passed and resources can be directed to contingency management and recovery.

The results of Digital Realty's overall emergency preparedness speak for themselves. On Sunday, October 28, 2012, Hurricane Sandy began its devastating march up the United States' Eastern Seaboard, beginning in North Carolina and ploughing through the New England states over the course of the next two days. In all, some 15 Digital Realty properties in eight states felt the impact. But thanks to the company's forward-thinking property teams and their commitment to emergency preparedness, Digital Realty met the challenge and provided continuity of operations for its clients.

The end result was that, despite widespread utility outages, Digital Realty's operations teams successfully supported 9.2 megawatts of critical load for more than 165 hours without utility service. Due to the strength of the company's supplier partnerships, it was able to ensure the continuity of its data center operations during this period, utilizing some 176,000 gallons of fuel and enabling clients to maintain their own operations. Ultimately, of 152 clients impacted, only one sustained any outage, and that was due to equipment for which Digital Realty had no operational or maintenance responsibility.

These results are not uncommon. In the latest round of severe winter storms to hit the East Coast and Northeastern United States during 2014, Digital Realty once again proved it was up to the challenge, with all affected sites reporting continuous operation during these events.

SWEEPING STATEMENTS ON THE EFFECTIVENESS OF SECURITY IN A DATA CENTER MEAN NOTHING IF THE DATA CENTER OPERATOR CANNOT DEMONSTRATE THAT VALUE PROPOSITION TO CLIENTS THROUGH A RECOGNIZED ATTESTATION METHODOLOGY.

PREPARATORY ACTIVITIES PRIOR TO THE ONSET OF THE STORM INCLUDED:

- Thorough internal and external inspections of each property
- Storage of emergency supplies and critical spares
- Staging of strategic partners in support of Digital Realty's operations, including fuel suppliers and disaster remediation services
- Increasing on-site staffing 24/7 for the duration of the event
- Development of a redundant internal communications capability in the event that internal phone and computer systems became unavailable
- Development of a client communications plan to ensure clients would be kept informed of the status of the storm and activities at the site

Regardless of the event, Digital Realty has a proven track record of successfully managing the risks that threaten its clients' business operations, allowing them to focus on their core businesses and their own imperatives. With excellence in planning, training and preparation, coupled with sound management and unparalleled experience in the operation of critical facilities, the company continues to be an industry leader when it comes to incident management and emergency response.

RESILIENCY AND CONTINGENCY PLANNING

Business continuity management (BCM) draws on the other components of an integrated security program and on Digital Realty's extensive technical operations expertise to properly protect business operations from disruption in the event of a disastrous event.

At Digital Realty, resilience is the watchword, and the company goes to great lengths to build redundancy and fault tolerance into its operations and services. For, unlike more traditional business models, one cannot simply relocate the infrastructure required to run a top-tier data center. Resiliency must be baked into the DNA of the data center to ensure it will continue to operate as designed and supply the solutions on which clients depend. Technical operations excellence, physical security redundancy, information security—including associated disaster recovery protocols and effective emergency response—all play a role in ensuring the delivery of best-in-class continuous operational performance.

Digital Realty takes a two-pronged approach to resiliency and contingency planning. At the property level, the company constructs its data centers and trains its teams to ensure that contingencies can be met and managed in the most effective manner possible. In the event of utility outage, multiple power feeds at the power distribution unit provide reserve power; if utility is completely lost, uninterruptable power supply systems provide continuous power until backup generators come on line, while redundant chillers provide cooling levels at all times.

With smart technology incorporated into physical security systems, badge readers will continue to function in the event network connectivity is disrupted, and power supplies supporting door locks are equipped with backup power as well, resulting in no loss of security for client infrastructure. Property teams are thoroughly trained and tested in potential threat scenarios that might disrupt operations, and contingency plans are reviewed and updated annually. Digital Realty has seen the effectiveness and professionalism of its property teams time and again as catastrophic events have occurred. As a result of this planning, preparation and professionalism, the company believes its approach to continuity of operations at the property level is unmatched in the industry.

The second aspect of BCM involves the assurance that executives and corporate functions can recover and maintain efficiency if an event impacts their ability to operate in their normal business environment. To that end, Digital Realty uses technology to make secure, encrypted communications available to senior leadership to enable them to operate remotely, and the company conducts rigorous disaster recovery exercises, ensuring critical corporate data are backed up and can be recovered at a designated off-site facility in the event of system loss or compromise.

COMPLIANCE

Perhaps the most important aspect of any security program in the eyes of clients who depend upon it for their businesses is the assurance that the program is actually performing as advertised. Sweeping statements on the effectiveness of security in a data center mean nothing if the data center operator cannot demonstrate that value proposition to clients through a recognized attestation methodology. A client may trust its data center provider, but it may also want an impartial third party with a reputation for accuracy and reliability to verify the services it receives.

Digital Realty has embraced a standards-based approach to earning its clients' trust by adopting the Service Organization Controls 2 (SOC2) reporting standard as the cornerstone of its compliance efforts. Data centers in the U.S., Europe and Asia Pacific are scheduled for a SOC2, Type 2 examination in 2014, the fourth year in which the company has conducted such examinations through its third-party auditing partners. Such attestations provide trusted assurance to clients that Digital Realty's services in physical and environmental security are, in fact, meeting a world-recognized standard for control efficiency and validity by a service organization. These reports are made freely available to clients.

In addition, exciting new plans are in the works to expand compliance to include PCI-DSS and ISO 27001 attestations at a number of Digital Realty locations in 2014. Once complete, the company expects to field the most comprehensive and in-depth compliance program in the data center industry, one that directly reflects the diverse needs and requirements of its valued clients.

SUMMARY

A comprehensive approach to security requires much more than simply installing locks and hiring security officers. While these remain important aspects of an effective security plan, they are part of a broader, more integrative approach to security in today's dynamic environment. For data center operators, ensuring the security and continuity of their clients' business operations is a key and compelling imperative.

This paper has examined the elements and organization of a holistic approach to security. Digital Realty views security as an integrated process, consisting of the subprocesses of physical security, information security, incident management, business continuity and compliance, enabled by the systems, processes and people providing quality of delivery and reliability of performance. Absent any of these elements, security becomes a series of loosely related tasks lacking in cohesive effectiveness.

Digital Realty embraces the entirety of security and what it means for its clients. The company focuses on all elements and their interrelationships to deliver the highest-quality, most reliable security services in the data center industry. Its security team is on call around the clock to address any security concerns a client may have, and the company prides itself on the transparency afforded by a robust compliance program.

ABOUT THE AUTHOR

Gary Smith, CISSP, is the director of Portfolio Security at Digital Realty, responsible for physical security, emergency planning and compliance across the company's global portfolio of properties. He has more than 30 years of experience in the law enforcement and security communities. Gary holds a Master of Engineering in systems engineering from Stevens Institute of Technology.