PSSST... WANNA KEEP A SECRET?

Then call Christine L. Peterson, President of Protus3

protus³

PLAN. PROTECT. PROSPER.

Introducing Christine L. Peterson, CPP, ISP

People often call law enforcement and their lawyers after their business has experienced a loss or their security program has been breached, hacked, compromised, or misappropriated. However, the forward-thinking business executive calls Christine L. Peterson, President of Protus3, well ahead of time to prevent a breach from ever happening.

Chris's journey to business executive and president of a multi-million-dollar security consulting company was neither typical nor expected. She began her career early, eventually accepting an entry level administrative position with Protus3 (formerly known as Risk Management Associates) in 1991. Mike Tucker, the founder of RMA, would later become a mentor, and under his guidance she obtained two university degrees and began her ascent within the company, eventually becoming president and a shareholder.

Now, almost 30 years later, Chris (CPP, ISP) is an industry expert in security consulting—including security assessments, program development, and training. The synergy between her security expertise and her business administration experience is the perfect combination for the fast-paced, ever-changing, and complex world that businesses are faced with every day.

"Protus3 is on the front line of protecting companies' assets," she says, "and we take that responsibility very seriously and with the utmost care and integrity."

To that end, Chris has helped to develop a diverse national and international business portfolio including government agencies, colleges and universities, and private sector firms from the Fortune 500 on down. They even consulted in providing security for a client at the 1996 Atlanta Olympics.

Chris is board certified as a Certified Protection Professional by ASIS International and as an Industrial Security Professional by the National Classification Management Society. As a security consultant she has worked with institutions and businesses to develop the appropriate level of security controls to support their operation and prosper. She believes that security creates the framework that supports a business's stability and prosperity.

As an executive and security professional, Chris is actively engaged in the community, having served on boards and other leadership roles with ASIS International, NCMS, the Greater Raleigh Chamber of Commerce, the RTP CFO Forum, and Triangle Family Services. She also serves on the Business Advisory Boards at Meredith College and Wake STEM Early College High School.

> **When a company is successful, it means jobs, opportunities, satisfied customers, education, homes and so much more. We help companies protect what matters. That gets me excited every day!!**

Still guided by Mike Tucker's core values, Chris is prepared to share some of her knowledge and experience in the following areas.

1

Integrated Security: What is it, and why do you care?
A security program best operates when the business and security processes are working together in harmony. Starting from the ground up, Chris will talk about creating a solid foundation that facilitates your company's mission, while integrating and operating a security program that allows for sustainable growth and profit. Her business and administrative experience lends a deep understanding of the challenges companies face trying to do what they do well, while protecting assets so all that hard work leads to prosperity.

2

Why Background Screening Is Vital For Every Business (one bad apple can spoil the bunch)
In today's business climate, knowing your employees is critical—not only for business success, but also for safety and security of business assets, employees, and intellectual property. Routine background checks may not discover critical information necessary to make an informed decision about whether to hire someone. The buck doesn't stop at the hiring decision. Additional background checks may discover problems that occur years after the routine screening. The fact remains that the single greatest risks for companies are their own employees (whether by clicking on spyware or deliberate espionage or theft). The old adage applies: one bad apple can spoil the bunch.

3

Training: When to intervene… call security… or call the police
Workplace violence has a large impact within the work environment, but a low probability of happening. With this in mind, practiced fire drills and evacuations are not enough. Companies and employees need to first be aware of the external clues of potential threats, and then have options of how to respond appropriately in various critical or violent situations. Leaving this to chance, or reacting with knee-jerk responses, can be dangerous at best—and at worst life-threatening. Creating a culture of "If you see something, say something" ensures all employees are the eyes and ears of the company. In trying to prevent workplace harassment, bullying, and violence, this is vital in responding appropriately to internal or external security risks.

4

Digital Asset Protection: Beyond passwords and firewalls to digital forensics and BYOD.
Computer system breaches all have one thing in common. They are created, operated, and exacerbated by humans. What if that employee hadn't opened the attachment? What if your IT department had installed the latest firewall protection? What if there was an alarm on vital files to prevent theft? Computers are great tools, but training and educating the operators is the key to a winning security system.

5

Low Hanging Fruit: Lights, camera, action!
Security cameras rarely prevent theft or vandalism, because rarely is anyone monitoring the events in real time. Instead they only show you the after-the-fact events. Simple changes in security can have measurable effects in deterring both internal and external security threats. Adequate lighting, access control—limiting access points and limiting who has access to sensitive areas and documents, and rotating passwords or dual authentication can go a long way in creating a culture of security within the company. Integrating the people, processes, and technology is critical to the future of any business. Protus3 is hired by business executives who have assets that are critical to their business and who want to protect them. Passwords, safeguarding sensitive information, light, and signage are the first lines of defense in developing an integrated security system.