PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHRIS DUNNING

CSO, **AFFINION GROUP**

HEADQUARTERS: STAMFORD, CT

EMPLOYEES: 3,700

“There are two camps when it comes to employees and security. Some believe that people are the biggest threat, and others believe that people are the best security asset. I say to the workforce, ‘raise your right-hand and be deputized.’ I would rather have 3,700 security deputies than just my security team members tasked with making sure that 3,700 people do not make a mistake that exposes the company.”

WHAT IS IN A TITLE? THE DIFFERENCE BETWEEN A **CSO & CISO**

Christopher Dunning holds the title Chief Security Officer, instead of the more common Chief Information Security Officer, at Affinion Group, one of the largest providers of customer loyalty programs. He explains the difference between the two roles, “A CISO lives in the IT department, whereas a CSO influences all aspects of security – from information security, to privacy and physical security. A CSO is a peer to the CIO, while typically a CISO reports into the CIO.” It makes sense to Dunning that Information Protection or Security is run outside of the IT department, he states, “security is not just a technical problem, it is also a business challenge. It cannot be solved with just a technical solution. You have to also take a business-centric approach.”

With that being said, Dunning has a strong working relationship with the CIO and other leaders in the company. “Without good communication between the C level executives, it may become a battle of command and control. In my first days here, I sat down with many of the leaders and asked about their risks and concerns. I established myself as their consultant, and made sure to include legal, HR, and Internal Audit .”

The Future: Security Takes the Lead

"I think that five or ten years from now, CISOs will be much more involved with the actual defining and development of business solutions, instead of being at the tail end of the development process, where we often are today. It all comes down to how quickly businesses need to move in order to be successful." Dunning has some experience in this type of security-led development. In an earlier role as Director of Information Security for a Fortune 500 retailer, his team worked with the development team to create a security-aware development process.

FINDING THE RIGHT BALANCE IN **REPORTING**

Dunning's goals are to protect the brand and shareholder value, right-size the security efforts to provide appropriate defenses, provide a security program that meets the needs of the business, and protect critical data, applications, and systems. The organizational structure matters when it comes time to gain executive level mindshare and buy-in to help him achieve these goals. "As CSO, I report into the COO and participate in monthly status meetings with the CEO," he says.

Dunning states that many CSOs are challenged with reporting and presenting metrics that resonate in these executive meetings. Over a number of years spent in several security leadership roles, and with input from mentors, Dunning has fine-tuned his status reports for leadership. However, he believes that even his current reports provide more information than the executives are able to digest. "The bottom line is to keep it simple. There are so many granular issues with risk management it can be like boiling the ocean. I take a very simplistic view when reporting at the senior level. I ask, 'Are you solving a business problem or just reporting on results?'"

Dunning reports on four categories: Security Incidents, Compliance, Vulnerabilities, and People. Brevity and clarity are keys to his presentation. "My goal is to produce a one-page status for each that could be understood by anyone." His one-pagers include:

- Security Incident Response 'The First 48' - a monthly security incident report that documents all security incidents that have been reported, evaluated, and responded to following the first 48 hour process.

- Compliance Tracker - an overview on the company's status with PCI, SOX, and other compliance mandates.

- Vulnerabilities Quadrant - a method for tracking existing and remediated vulnerabilities and risk.

- Security Awareness Calendar – a high-level view of on-going employee security training and awareness activities.

NO BOARD VISIBILITY, **NO PROBLEM**

Dunning reports he does not meet regularly with Affinion Group's Board of Directors. "Is there a strong interest in security from the Board? Yes, it is a very strong interest," he says. Even with this interest, Dunning does not have an annual meeting on the calendar, although he does meet as needed with the Audit Committee and speaks regularly with the CEO. "There is a process in place for the Board to be updated on security through the Audit Committee and the CEO. I think it makes sense to have this reporting structure. If they need me, then I am here as their consultant," says Dunning.

Advice from a Veteran CSO

Because he has almost 30 years in the security industry, and two CSO roles under his belt, we asked Dunning for his advice to newer CSOs. He states, "First, establish the behavior of yourself and your team. A successful security organization is not just comprised of engineers and architects, but consultants. You will have engineers and architects on your team, but everyone should be acting in the role of a consultant. The security team has to be available to help their peers solve business problems with security solutions. Getting involved in these discussions as early as possible is always a plus!"