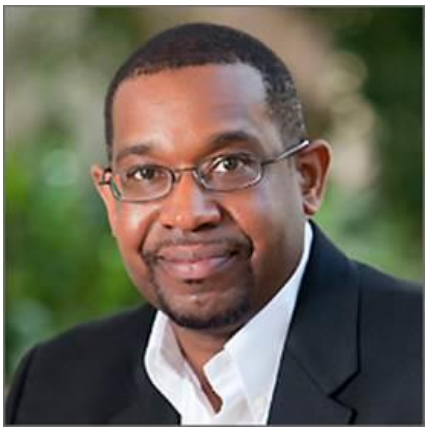
CyberPro
Keeping Cyberspace Professionals Informed
Volume 7, Edition 18
September 4, 2014

Senior Leader Perspective: Lamont Orange, Information Security and Strategy Officer, Websense Inc.



NSCI recently had the opportunity to interview Lamont Orange, Information Security and Strategy Officer, Websense, Inc. In this role, Orange is responsible for developing, maintaining and socializing the company's internal security program. He also serves as a trusted security resource for Websense customers worldwide.

Orange has more than 15 years of experience in the information security industry. For more than 10 years, Orange was vice president of enterprise security for Charter Communications. During his tenure, he was responsible for safeguarding enterprise information, computing assets, intellectual property and customer privacy, while providing data retention and compliance oversight.

Prior to Charter Communications, Orange served as senior manager for security and technology services at Ernst & Young. As the information security senior manager, he directed technical infrastructure diagnostics, and oversaw the assessment, design and implementation of security and information technology solutions.

Orange received his bachelor's degree in computer science from the Missouri University of Science and Technology in Rolla, Missouri.

NSCI: First off, can you tell us a little bit about Websense and what it offers in the cybersecurity market?

Orange: Cyber attacks can severely cripple or completely incapacitate a business through financial loss and brand erosion. We enable businesses to focus on what they do best, because they know that we are protecting their most critical assets from cyber threats and data-stealing attacks.

Websense, Inc. is a global leader in protecting organizations from advanced cyber attacks and data theft. Our comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) to prevent data breaches and intellectual property theft.

More than 11,000 enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware.

NSCI: What key components would you say should be addressed in an organization's information security strategy?

Orange: There are several key components that should be addressed in an organization's security strategy, which include the following:

1. **Align Security Strategy to Business and Risk** – First and foremost, organizations need to align their security strategy to the business and the potential risk of the business. They should not do security simply for security's sake.

2. **Focus on the Data, Not the Devices** – Organizations also need to focus on the data, not the devices. It doesn't make sense to try to lock down every device in a connected world where BYOD is king and data is often stored offsite, and in the cloud.

3. **Understand Your Connections and the Flow of Information to the Cloud** – The Internet of Things is changing the enterprise technology landscape and we need new controls in place to protect the deluge of data. In addition, businesses need to have a fundamental understanding of how they will be willing to connect and accept connection to and from the cloud.

NSCI: Can you tell us a little bit about how cybersecurity training and education play in Websense's internal security program?

Orange: Websense takes a different approach than most organizations. Most companies have an annual check-the-box training, where there is little to no retention or change in employee behavior. We want to show our employees what's in it for them and make them a partner in the internal security process.

For example, we reward Websense employees for finding anomalies in the environment such as spam, a phishing email or even finding a USB in the parking lot that they opted not to use. We encourage them to report these anomalies and we reward them with gift cards or cash. We also started an internal campaign around tagging important data. We then challenged the various business units within Websense to tag or fingerprint their own important data. This exercise became a fun competition which fostered camaraderie and had everyone aiming for the same goal – while also greatly benefiting our business as a whole.

We also continually educate our employees on the types of malicious cyber threats that exist today, whether on the web or in email, because these threats are ever evolving.

This comprehensive strategy allows our employees to be part of the solution rather than be categorized as part of the problem.

NSCI: How do you measure the effectiveness of your internal security program?

Orange: We measure the success of our training programs through random testing. For example, we'll send our employees a test email with a malicious link to see how many employees click the link. We conduct this test throughout the year and consistently see the numbers drop following our training and incentive plans. Ongoing testing also allows us to observe and track our risk trend line and continue to reduce our employee exposure to threats.

We continue to see a reduction in the number of security incidents across our organization as we make our employees a true partner in our quest to combat cybercrime within our own organization.

NSCI: There have been some fairly significant data breaches in the news recently and Congress seems to be struggling to determine how best to proceed on policy and law to address them. Any thoughts on what the key pieces of any legislation should (or should not) address?

Orange: We are seeing attempts at legislation that lack reach and teeth. For example, the US recently tried to pass legislation treating cyber espionage as a diplomatic issue. For example, if we have diplomatic sanctions, do we have the rights and privileges to try those individuals in a US justice system? What are the real penalties? Will other countries bring their own people to justice? And, are we prepared to stop being an ally with a country over cyber espionage? These are a few of the discussions that need to occur if it is our desire to legislate security.

In addition, bills are often written that can be limited in focus. Let's take the Cyber Economic Espionage Accountability Act HR 2281 for example. The bill, as written, is singularly focused in some areas. It only highlights the loss of manufacturing jobs, but manufacturing is not the only industry affected by intellectual property theft. This bill may also be perceived as antagonistic to some given it calls out China and Russia specifically. It is also dubious to think elevating the issue to diplomatic/WTO levels of discussion would be effective as the majority of cyber espionage by state sponsored organizations are classified, and thus "do not exist" at a negotiation discussion level.

It's also important to consider that national security priorities are usually defined and managed at the executive levels, and are very fluid, changing frequently. Since cybercrime can change in its methodology and targets in very short time frames, any published law definitions may become obsolete very quickly.

This leaves a business and/or an individual with a lack of understanding of what they need to do to be in compliance. We need to be more clear and prescriptive with our policies and legislation.

In the interim, it is absolutely necessary for each organization to act now to protect their information and the sensitive information of their customers, partners and vendors. The risk is real and present today. Even if introduced and passed, legislation will not remove that risk, so we must not wait to integrate strong security policies into our day-to-day business.

NSCI: There's been some discussion on turning cable companies into public utilities. Having some background in that industry, what do you see as the pros and cons of this?

Orange: If a cable company becomes a public utility, it will be considered critical infrastructure and now will have access to the superhighway of communications. Right now, a cable company has the choice to protect or not to protect with no real governing programs. This move will add a new level of protection by requiring these organizations to comply with regulatory and security issues that are mandated for other critical infrastructure elements.

On the flip side, someone has to pay for this. This may increase rates or consumer and/or business contributions to the organization.

NSCI: Thank you very much for taking the time to visit with us.