ceocfointerviews.com

Issue: November 16, 2015
The Most Powerful Name in Corporate News

Malware Defense, Incident Response, Risk Management And HIPAA Security Consulting and Solutions

Terry Kurzynski
Founder & Senior Partner
HALOCK Security Labs

CEOCFO: ***Mr. Kurzynski, the tagline on your site is "Purpose Driven Security." Would you tell us how that applies?***
Mr. Kurzynski: Purpose Driven Security® refers to our client's purpose, which includes their mission, objectives and obligations. When we refer to purpose, we are referring to those three drivers for all of our clients. HALOCK's guidance, consulting and solutions are customized for each client's business.

CEOCFO: ***What do you understand about working with people that is unique?***
Mr. Kurzynski: What we are seeing is that risk management, risk assessments and controlling risk to a reasonable and appropriate level has been difficult for organizations. Some of the guidance that may be given or some of the self-driven guidance that they pursue has not been as complete as it could be – some threat vectors are often missed.

Perhaps the guidance they are receiving is exclusively aligned to their obligations, for instance, their company's capacity to cause harm to the public. Or they receive guidance solely on meeting their contractual obligations. Without balance, there's a chance that these companies are overspending on contractual obligations and the harm they could cause the public without balancing the fact that they have a mission and specific objectives to operate as an organization or business. Without balancing the risk to their mission, objectives and obligations, they may cease to exist.

When you look at the regulations, legislation and all of the security standards that have been put in place, for the most part, risk analysis is at the core. Think about the HIPAA security rule, it starts out with performing a risk analysis to ePHI and then applies controls to bring risk down to a reasonable and appropriate level.

The goal of a risk assessment has never been zero risk. If zero risk were the goal, we would not be allowed to drive automobiles on the road. However, because there is an economic benefit to having roads, we accept this level of risk. The same risk framework is true for every organization that is out there because they each have a mission and specific objectives that they are trying to achieve. These organizations might have a profitability objective, or a goal to be number one in their sector, or they might be trying to achieve an annual growth objective. Whatever their objective, they have to meet and balance their obligations and apply appropriate controls or they cease to exist as an organization. Every organization needs to balance the investment in controls to protect their mission and objectives with the investments made in protecting their obligations and harm they can cause the public. And therein lies the missing ingredient for a proper risk assessment. They fail to meet the balance test.

CEOCFO: ***Would you tell us about your new advanced threat diagnostic tool?***
Mr. Kurzynski: The advanced threat diagnostic (ATD) allows us to have a wider view into the organization. The ATD finds the cyber threats that already exist in the environment and indicators of compromise.

If you go to the doctor, your personal health risk assessment might look like this: how are you breathing? Eating? Feeling? Are you working out? The doctor will give advice on some of the risks you have, such as your eating habits, family history, etc. The doctor might examine you at a deeper level by completing some deep diagnostics, perhaps run a MRI, or draw some blood to find out if you have any dangerous abnormalities. The goal of the diagnostic testing is to get a close-up view of what's going on in your body now, before any disease gets out of control.

HALOCK's advanced threat diagnostic helps us find the real and current cyber threats that may exist in the environment so that an organization can direct resources toward the problems as soon as possible. Many times, there's abnormal system use and network traffic occurring right underneath their noses and organizations are unaware of it.

CEOCFO: ***What types of companies are turning to you for services?***
Mr. Kurzynski: Typically, clients that seek out our services have multiple security requirements, be it from legislative, regulatory or contractual obligations that they need to meet. The size of the organization is less relevant. Organizations that are concerned about securing data have legislative requirements like HIPAA or industry standards like the PCI DSS. Organizations that don't have legislative, regulatory or contractual obligations are not an ideal fit. The industries we work with the most include cloud service providers, healthcare providers, legal, financial, retail and educational institutions. The one thing they all have in common is their obligation to secure their sensitive data.

CEOCFO: ***When you speak with a prospective client, how can you know who is ready to take advantage of your services and who just might be picking your brain?***
Mr. Kurzynski: We try to understand their current pain. And as mentioned previously, if they have legal, regulatory or contractual obligations that they are trying to comply with, we are confident we can help them and they are a great prospect that will benefit from our services. When a client is experiencing pain as a result of not being able to meet their obligations, we know they need our help. The pain that these prospects are feeling is real – they lose contracts, are denied cyber insurance policies or are spending countless hours preparing for audits. Many of these prospects are not at the maturity level that they need to be and we can help them get there.

"Every organization needs to balance the investment in controls to protect their mission and objectives with the investments made in protecting their obligations and harm they can cause the public. And therein lies the missing ingredient for a proper risk assessment. They fail to meet the balance test." - Terry Kurzynski

CEOCFO: ***Would you tell us about your flagship services and some of your services that people do not utilize as much as they should?***
Mr. Kurzynski: Risk assessments have been a staple for us. Performing risk assessments usually involves some sort of compliance obligation. We've been doing penetration testing since the nineties; it's a service we have had for over seventeen years and we are best-in-class. Incident response readiness is another area where we excel as well as responding to live incidents/data breaches.

About four years ago, we developed an incident response readiness service. This particular offering is starting to gain a lot of traction because businesses realize that a cyber breach is foreseeable. The Target breach really shined a light on the issue of, and need for, breach preparation. When you examine how Target handled their breach as compared to how Anthem handled their breach eighteen months later, you'll see a night and day difference on their individual responses and their levels of readiness to deal with it. As a consequence of the way their breach was handled, not much is being said about Anthem's breach. By contrast, Target is still in the headlines and continues to have shareholder-derivative lawsuits that are still pending against the officers of the company for not performing their duty of care.

CEOCFO: ***Are you surprised that so many companies still do not understand the need to be prepared?***
Mr. Kurzynski: It's getting better every day. Today there is enhanced awareness and organizations are getting more sophisticated and doing something about it. Every now and again I am surprised when we come across a large and well-established organization that is aware of their obligations, but has failed to invest more in security. Sometimes it comes down to whether or not they have been held accountable for doing something. If there's no accountability, organizations will tend toward inaction. Organizations aren't getting secure for the greater good, but instead because they have had repercussions, many times financial, that have forced them to deal with security. When a company starts experiencing pain we see them wake up and do something about it. The pain can be financial, pressure from third parties, loss of competitive advantage, or experiencing a breach and/or fines.

CEOCFO: ***HALOCK was named in the Inc. 5000. How do you continue the trajectory?***
Mr. Kurzynski: After nineteen years in business, you have to continue innovating and devising new solutions to new or existing problems. Once you stop innovating and evolving, you cease to be compelling as an organization – particularly in this industry. At HALOCK, we embrace the mindset of continuous innovation and we are always looking to improve what we do.

CEOCFO: ***Are you surprised that local seems to be important for your industry?***
Mr. Kurzynski: The information security industry is a game of trust. While HALOCK has deep roots in the Midwest, we still have quite a few clients from all over the country. Local may be one factor that organizations consider when choosing an information security service provider, but ultimately people are buying from people and they want to trust their service provider. When choosing a service provider, prospects want to know that an organization has a solid track record. Next year we are celebrating our 20-year anniversary in this industry – and we could not be more proud of our performance and reputation.

CEOCFO: ***Why choose HALOCK Security Labs?***
Mr. Kurzynski: At the beginning of this interview, we talked about Purpose-Driven Security®. Our aim is to fully understand our client's mission, objectives and obligations and we right-size security for their needs in order to meet those three purpose-driven business considerations. Balancing all of those correctly is exactly what the laws and regulations are requiring of businesses and our purpose-driven approach aligns with that. Organizations choose HALOCK because we can help secure their organization without compromising their mission or business objectives. Under our guidance businesses are able to balance their contractual obligations and their responsibility to prevent harm with their mission and objectives. Ask yourself, is your organization meeting the balance test?

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

HALOCK Security Labs

For more information visit:
www.halock.com

Contact:
Lauren Mieli
847.221.0203
lmieli@halock.com