FEATS OF STRENGTH

PROFILES IN SECURITY

Earning the right to be confident in IT Security

VOLUME 2 / ISSUE 3

K logix

LETTER FROM KEVIN WEST
CEO

DEAR READERS,

In our first "Profile in Confidence," Yalmore Grant, Head of Security at Boston Financial, talks about his "first big win." Some will be surprised that his first big win was not warding off a threat or cyber-attack, rather it was convincing a peer of the value security can have on the business. Yalmore's success at evangelizing security outside of the IT department has earned him the right to be confident in his security program.

How can you earn the right to Be Confident in 2015? We explore that topic and more in this issue of Feats of Strength.

Happy New Year!
Kevin West

Earning the Right to Be Confident

At K logix, we tell our clients to "Be Confident." Confident security organizations impact revenue growth by helping the company manage risk. Where does confidence come from? How can you earn the right to be confident?

First, it is important to understand that your team has the same goal as sales, marketing, finance, and other parts of the company. The mission is to enable business to grow and realize its revenue potential. Security impacts growth by advising and guiding business units on how to effectively manage risk and secure critical information.

Today, most security organizations are mired in reactive response and tactical threat management. When security teams lead with fear tactics, they move themselves away from important business conversations, therefore missing out on opportunities to increase their stature within the company. We believe that every security organization is capable of refocusing their approach to align with business; many need help finding the way forward.

So where to start? Below are important steps, both tactical and strategic, for creating a confident security program.

1. Get to Know the Business

Security teams must be collaborators, communicators, and partners to their peers in other business departments. Security teams must understand how the business makes money, be in-step with overall business goals, and find common ground by aligning security objectives with the key priorities of each department in the company.

Security teams strengthen their relationship with these key business stakeholders by demonstrating an understanding of their goals and challenges. In turn, this opens the door for security to be involved with the development of critical business processes and procedures, ensuring increased security awareness and adoption.

Where to start?

Network and Make Connections – Security teams need to make connections with leaders in other departments. From these meetings, security teams can ascertain partners' key goals, performance drivers, and even their feelings and assumptions about security. Ask them three questions to start What are your goals? How are you incentivized? What do you think of security?

Get an Easy Win – It is important to show that a security-inclusive business approach works. Team with your ally to develop and implement a secure business process that helps them achieve a critical goal. Once you have your first success, use that case study and your ally, to duplicate the process with other departments.

2. Make sure everyone knows security's role (starting with your team)

Keep in mind that the goal of a confident security organization is to enable the business to achieve its revenue growth potential. Successful security teams help the organization manage and alleviate risk. Where to start?

Document your Mission – Make sure that the executives and members of your team understand your mission.

Create and memorize an elevator pitch – An elevator pitch will help keep your team on the same page, and provide your peers outside of IT with a better understanding of security.

Commit to your Framework – Your security framework guides your team, policies, procedures, and technology. To ensure it is successful in helping you achieve your end goals, you must be persistent.

1. Evaluate your team based on their ability to work within the framework
2. Identify critical data and systems
3. Focus on threat and issue detection without sacrificing prevention

3. Be Included in the Boardroom

Once in the boardroom, security leaders need to make the most of their opportunity. It is important to remember your goals and audience and make a game plan for success.

Where to start?

Leverage your allies – Leverage your ally's commitment to security and introduce others in the boardroom to its value.

Speak their language – Effective security leaders discuss security in terms of its positive impact on achieving business goals and increasing revenue. Avoid talk of specific threats, technology standard,s and other items that move the conversation away from business goals.

Provide Proof – Prove that you belong in revenue discussions by providing success stories, reports, and testimonials that show how security impacted the bottom line.

Because of an increased focus from national news, IT security currently has as big a stage. However, business executives need to re-focus away from the fear-based sensationalism that they read and see on the news, and move towards security's ability to impact critical business goals. A confident security organization is well prepared to seize this moment and lead the conversation in the right direction. Are you ready to start?

CREATING A CONFIDENT SECURITY PROGRAM:

1. Get to know the business
2. Make sure everyone knows Security's role (starting with your team)
3. Be Included in the Boardroom

Security impacts growth by advising business units on how to effectively manage risk and secure critical information

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

YALMORE GRANT

Head of Security
Boston Financial

THE START

Yalmore Grant's early career was in the data center at Boston Financial. He describes himself as a "real data center guy. I was about servers and hardware: the big physical stuff. But then, a light bulb went off. I realized that all the data in the data center, which was moving from one company to another, was inherently insecure. I quickly realized that securing that data was the future.

APPROACH

Coming from the data center, Yalmore admits that in the beginning he was interested in all the shiny new tools of security – the technology. But a conversation with a major client early on in his time as a security leader changed all of that. "Immediately after I was handed the reins of the security department, I received a call from a client. They were coming to Boston to do due diligence, and they wanted to talk about data security. I thought we would talk about proxy servers and firewalls. When we sat down together I quickly learned they had no intentions of discussing anything technical. All they cared about were our processes. What our clients care about is the processes, vision, and strategy. What will happen with their data when they entrust it to us?"

This was a major revelation for Yalmore and would shape his entire approach to running his security organization. "I had to think differently. I would no longer focus on technology, but on the business. I turned my focus to the management of the processes, policy, procedures, and governance."

He continues, "We had policies and processes in place, but they were not communicated well to the employees they impacted. Security is more successful when you have buy in from the people using the systems. When people are aware of security it is easier to implement policy and procedure, and it makes the entire company part of the security team. With the right knowledge, they are essentially another pair of eyes watching out for the safety of our critical data."

THE CRITICAL FIRST WIN

Increasing the company's security awareness required Yalmore to get outside his office and the IT department and make connections one business unit at a time. "I sat down with each of the SVPs of our different business units. I listened to them talk about their business processes and their work. What systems did they use most often? Which ones were most critical to their processes and what would be the impact if those systems fail."

"My first interaction was with a gentleman who runs a major organization within the company. He has a lot of responsibility, and relies on a number of critical systems and 25 servers to ensure the productivity of his team. My challenge was to deliver technical information to him about the security of these systems in a manner that he could relate to as a business mind. We talked about one system in particular that played a large role in the company's ability to reach its revenue goals. He knew if that system went down that it would seriously impact his team and the company. I showed him how the system rated on a Vulnerability Test I had performed. We talked about how a negative incident with the system could impact the end customer. From there he knew I was different. I wasn't asking him to buy a security technology; I was talking about making his team more efficient. We talked about how security awareness could improve the productivity of his team, and our end product."

After that conversation, Yalmore had his first department on board with security. That led to other organizations within the company embracing the approach as well.

COMFORTABLE IN THE BOARDROOM

Since taking over control of the security organization, Yalmore has had several opportunities to meet with the Board of Directors. He comes to these meetings from a position of strength because the Board is largely clued in to his security efforts before the meeting takes place – thanks to constant company-wide communication and education.

"My meetings with the Board are positive because we are not there to discuss fall out from a breach or a catastrophic security failure. In fact, we are not even talking about specific security efforts, because they are covered in company-wide meetings that occur several times a year. Instead we talk about our security posture and how it compares to the industry and to standards. We also talk about our customers and how our security programs can positively impact the services we are delivering to them."

"Security is a series of decisions. That is why it is about the people, more than the technology. Think about it, we are all awareness-oriented people. We make decisions based on awareness and security every day. Lock your car. Dress for the elements. Look both ways before you cross the street. So much of Information Security is about applying this same innate awareness to your business processes. Sure, technology is important as part of the framework, but the most important element is that everyone be aware."

- YALMORE GRANT

FUTURE DIRECTIONS

Yalmore points out that his security program, like all security programs, is constantly evolving and must always adapt to change. He does not get caught up in worries about future attacks, as he knows they are inevitable for every organization.

Instead he says, "Detection and response is just as important as the protection layer of security. We must have good incident response. We must act quickly to remediate issues when they do occur. This will minimize any discomfort we would feel from a malicious attack. That is how we can help drive business forward, and so that is what I focus on when I talk to the Board and the company about our security programs."

Ethical Hacking: Good vs. Evil

In order to be an ethical hacker – a white hat – you have to understand how the unethical hackers – black hats – work.

KEVIN MURPHY

Solutions Architect, Klogix

I am often asked how I became an ethical hacker and can understand why there is so much interest in ethical hacking– it is a classic case of good vs. evil. The topic interests a lot of people, not just security analysts and security professionals. It should be noted that these same tips could help you become an unethical hacker as well, so please use your forces for good!

PRACTICE

As with many other types of skills, there's no substitute for hands-on experience when it comes to becoming a better ethical hacker. There are many great free resources on the net that I've used to improve my skills. Aman Hardikar has pulled together one of the best collections of ethical hacking and pen-testing resources. He provides links to dozens of Capture-the-Flag-type sites where users' skills are tested in progressively more difficult scenarios. He also provides links to virtual machines that can be set up in a practice lab, as well as other great training resources.

READ BOOKS, NOT JUST BLOGS

Books on ethical hacking explore the topic at a deeper level than blog posts. I recommend Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses by Ed Skoudis and Tom Liston. Ed is one of SANS top course authors and instructors, and I personally find his writing smart and engaging. His book is perfect for anyone with security/OS/networking knowledge that wants to understand how hackers do what they do.

GET INVOLVED WITH ONLINE FORUMS

There are hacking forums for white hats, black hats and even grey hats. I recommend spending time in all of these forums (yes, even the black hat ones). Most of these forums are full of great info and how-to's covering SQL injection, XSS, command injection, reconnaissance/information gathering, scripting and countless others. You can learn a lot about AV-evasion, bot-for-rent services and available hacking tools. You'll be shocked to see how easy it is for low-skilled black hats to get access to these tools and tutorials, so it is important white hats keep up-to-date to combat them. There are many great forums out there, but one in particular I'd recommend is hackcommunity.com.

2015 Security Conferences & Events Schedule

Check out our blog
www.klogixsecurity.com/blog
for updates on security events

JANUARY	• **The International Conference on Cyber Security,** New York • **ShmooCon 2015,** Washington DC
FEBRUARY	• **CIO Summit,** Boston • **SANS 10th ICS Security Summit,** Orlando
MARCH	• **InfoSec World,** Orlando • **Global Privacy Summit,** Washington DC • **Chief Information Officer Leadership Forum,** Boston • **Secureworld Conference,** Boston
APRIL	• **Data Connectors,** Boston • **RSA Conference,** San Francisco
MAY	• **IT Roadmap Conference,** Boston • **iHT2 Health IT Summit,** Boston • **The Security of Things Conference,** Boston
JUNE	• **Gartner Security & Risk Management Conference,** Washington DC • **Data Connectors,** Hartford, CT
AUGUST	• **Black Hat USA,** Las Vegas • **SANS Boston 2015,** Boston • **24th USENIX Security Symposium,** Washington DC
SEPTEMBER	• **IT Security Leaders,** Boston
OCTOBER	• **IANS Boston Information Security Forum,** Boston

SANS CONTROL #11:

Secure Configurations for Network Devices such as Firewalls, Routers and Switches

DON COOK

Senior Solutions Architect, addresses SANS Critical Control #11, Secure Configurations for Network Devices such as Firewalls, Routers and Switches.

Hackers are on the lookout for remotely accessible network services to attack, and regularly scan for them. It is important to make secure ports, protocols and services to limit these types of attacks. Here we break down ports, protocols and services and provide recommendations for securing each.

Our team of security solution architects continue to review each of the 20 SANS Critical Controls and provide advice for addressing each control in a typical enterprise organization.

NETWORK PORTS

To prevent unauthorized access, organizations should:

- Secure network ports in common areas such as conference rooms, lobby, and open offices to prevent unauthorized network access
- Disable ports on the network switch
- Implement a Network Access Control Solution to allow users on specific, limited access VLANs
- Ensure physical security controls, such as locked doors, name badges, and employee awareness, are in place and effective
- Capture all changes to network ports through an effective change control process

NETWORK PROTOCOLS

To ensure security of network protocols, organizations should:

- Ensure that only necessary and secure network ports are enabled on networkable devices such as switches, routers, firewalls, and wireless access points
- Leverage SSH instead of Telnet for network devices, such as switches and routers
- Disable unencrypted web interfaces and discovery protocols on printers unless absolutely necessary
- Implement stateful firewall technology to limit protocol access from trusted hosts only
- Implement remote access protocols on PCs only when necessary and the should be implemented with access lists and encryption-enabled versions of remote access software
- Log all activity to a central location for monitoring and auditing
- Capture all changes to network protocols through an effective change control process
- Conduct quarterly vulnerability assessments to identify previously undiscovered services

NETWORK SERVICES

To ensure the security of Network Services, organizations should:

- Ensure that only necessary services are running on corporate servers
- Ensure that the patch management process is up to date and effective
- Implement a Standard Secure Build plan for all servers that ensures secure implementation of network services
- Log all security related events to a central location for monitoring and auditing
- Capture all changes through an effective change control process
- Conduct quarterly vulnerability assessments to identify previously undiscovered services

SANS CONTROL #12:

Controlled Use of Administrative Privileges

KEVIN MURPHY

Solutions Architect, addresses SANS Critical Control #12, Controlled Use of Administrative Privileges

Curtailing the use of admin privileges is one of the most effective means for reducing exposure to many of today's attacks. To understand why that is, consider the two most common ways an attacker can get a user to execute malicious code:

1. The attacker tricks the user into executing a program that they believe is harmless, but in fact the program secretly performs malicious actions such as sending a command shell to the remote attacker. Depending on how the malware is written, it may require administrative privileges to execute. If you have removed admin rights from the user, you have mitigated that risk. But, what if the malware can run with standard user privileges? You have still reduced your risk by removing admin rights from that user. The reason for this is that when malware executes, it will run with the same limited privileges of that user. This makes it much harder on the attacker to do things such as establish persistent access, dump password hashes, add user accounts, or laterally spread to other machines in the organization.

2. The other way for an attacker to get their code to execute on a system is for the user to browse to a site hosting malicious exploit code, very often this is a compromised legitimate website. Much like in the previous example, the risk is greatly reduced if the user is running with limited, non admin privileges. Any exploit code encountered by the user will execute with limited user privileges.

It is important to maintain as few administrative accounts as possible, and log and monitor all use of these accounts. An attacker will eventually need administrative privileges in nearly all attack scenarios. The more tightly controlled the use of these admin accounts, the easier it will be to detect an intrusion.

In today's environment, there is little reason to give admin privileges to most users. Newer operating systems have made it easier than ever for the majority of users to perform their day-to-day work without admin privileges. Windows features such as User Account Control (UAC) provide a convenient way for admin rights to be temporarily granted to specific processes only when necessary.

Is Your Security Environment Optimized to Its Full Potential?

QUESTIONS TO HELP YOU DECIDE

We talk a lot about how important it is to "Be Confident" in your security posture, but it takes work to get there. A committed security program provides a secure foundation in which business can achieve its revenue and growth objectives. To maintain this strategic level of security, the program must include constant evaluation, updating, refreshing, analyzing, and review of compliance mandates, security controls, and the critical systems they protect.

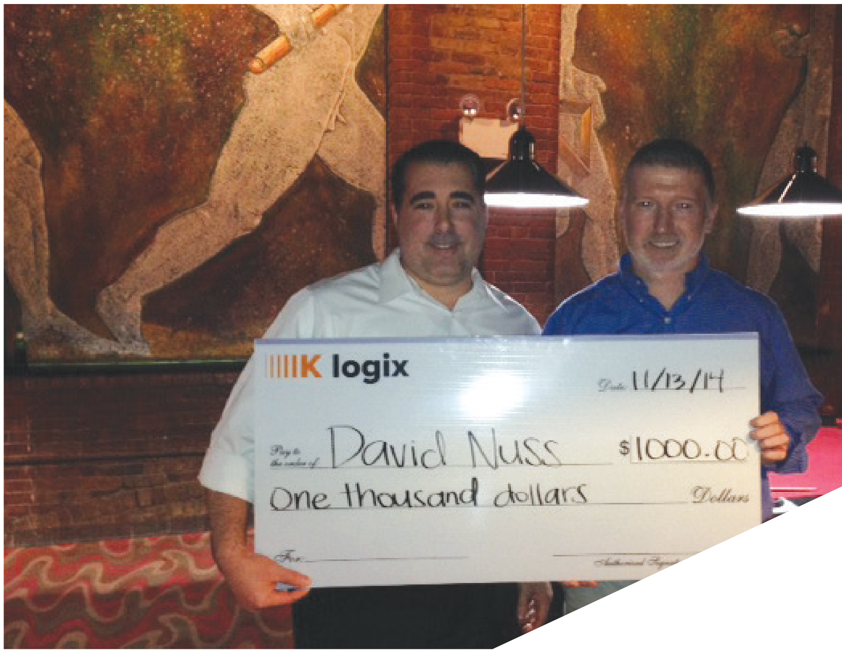
A big part of any security program is technology, why it is also important to be vigilant about keeping technology up-to-date. Here are a few questions to ask yourself as you consider whether you are utilizing your security products to the best of their ability:

- What are your business goals, and the objectives of each department in the company? Is the technology working to support these objectives? What can be done to bring the technology in-line with goals?
- Are you up-to-date on patches and upgrades of the product? Do you have a process in place for reviewing and installing them?
- Are your policies up-to-date and are all users aware and trained on them?
- Has your team remained certified in the product, even with turnover or re-organization?
- Have you considered how new services, products, or users have impacted the integrity of each specific security solution?
- Are you leveraging the reporting features to maximize detection and prevention?
- Have you considered how the security product impacts compliance requirements?

Security teams are busy and typically under-staffed. As a result, security products are sometimes neglected or even un-managed post-implementation. This may have a negative impact on business goals and compliance reviews, as well as the security team's ability to prevent and detect security issues. If you regularly review each security product against this check list of questions, you will be better positioned and more confident in your security posture.

BILLIARDS & BLUES

Over 80 security professionals joined us at our second annual Billiards & Blues for a night of live music, great company, and a high-stakes billiards tournmanet. The winner was David Nuss from Cresa, who donated all of his winnings to the South End Community Health Center, the event's featured charity.



K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

FEATS OF STRENGTH

PROFILES IN SECURITY

VOLUME 2 / ISSUE 3

K logix