Challenges and Keys to Success for Today's CISO from the Former CISO at the CIA

BY ROBERT BIGMAN

Developing the CISO Role at the CIA

When I started as CISO of the CIA, no one really understood the role or what to do with the CISO. The government had mandated that every government agency had to have one, but as the second CISO of the CIA, it was evident when I took the role that there weren't clear guidelines around my responsibilities in the organization. While we were an element in the overall security program with the agency, there was the classic argument about if I reported to the CIO or the Chief of Security. Therefore, initially, I was responsible for defining what the CISO role would be and how I could have the greatest influence and impact on the agency.

Over time, the organization grew, and individuals started to see areas where they could rely on the CISO. For example, as we started to use the Internet more broadly and began to consider taking on perhaps more risky technology or operational choices, people in the organization were asking, "Who do we go to, to find out what the risk is?" And that's when they started to proactively turn to me as the CISO and get me involved.

As CISO, my primary responsibility was defining standards, policies, requirements, and responsibilities, and communicating those throughout the agency. Governance is the not so sexy part of cyber, but it was our primary responsibility to make sure every system we developed and operated met very high levels of security. This included all aspects, from planning, integration, testing, approval, and the standard way you would deliver systems.

The things we were super serious about were critical because we couldn't make a mistake, so that was the easy part. The hard part was that the risks were high. If you made a mistake – and mistakes were made in judgment, in operations, in support, and in the use of certain technologies – you had to be able to recover from, understand them, learn from them and move on. No one's perfect and none of our IT systems are perfect, so we had to deal with that issue.

Every system delivered and deployed was a collection of technology, so a lot of planning and thinking about how best to use technology and what things we needed to do to lower our profile and risks went into each project. In large part, I was trying to help senior managers understand what the risks were and make coaching decisions about cyber risk.

I experienced an interesting evolution of involvement in our own IT life (administrative IT and analytical IT) to also becoming more involved in operational use of IT technologies in the whole agency. Later, I also got more involved in strategic planning – looking into the future and what types of cybersecurity skills people would need and what technology we were going to be using.

Biggest Challenges of Being a CISO Today

1. Most Organizations Don't Do IT Well

The problem in private industries that I see that make a CISO's life most challenging is that they don't do IT very well. If an organization doesn't do IT well, they're not going to do IT security well. I've never seen an organization do IT poorly but do IT security well.

What I mean by "not doing IT well," is they have no central planning, no central governance, no focus, and no strategy. Everyone in the business is out building their own thing, making their own deals, going to the wrong cloud providers, building their own systems, and making connections with their own vendors. It's a free-for-all and the poor CISOs are trying to keep track, keep management, and keep control from a security perspective of all this constant noise and constant change in the environment, which they say has to work at the pace of the business because they're always looking for opportunities to grow the bottom line.

This posture forces CISOs away from good planning and good strategy towards running after the next big opportunity. The business is going to build the application, they're going to deploy the application, or they're going to make the deal with the third-party vendor whether the CISO is with them or not because there's no penalty for not having the CISO with them.

2. The Bulk of a CISO's Time is Spent on Reactive Projects

A second big problem for most CISOs is that they spend 80 percent of their time on reactive projects versus 20 percent on proactive projects. Even in organizations that are better or more centrally managed where there's an IT portfolio of known projects and processes, you still have shadow or ghost IT where there's a risk because of the way most businesses conduct themselves with their IT. The cloud hasn't helped either. Most of these companies have three, four, five different cloud projects going at the same time across their company, making life very difficult for the CISO and forcing them to spend the bulk of their time being reactive.

About Robert Bigman

Robert Bigman is recognized as a pioneer in the field of classified information protection, as he developed technical measures and procedures to manage the nation's most sensitive secrets. Bigman is an information security trailblazer and participated in developing security measures for government computers well before the commercial industry found the Internet. During his 30 years at the CIA, he worked on various cyber security assignments on policy, cryptography, and technology operations support, and was the agency CISO for the last 15 years.

Now an independent consultant, Bigman works with the U.S. Government, foreign governments, and Fortune 50 companies, helping them both build productive cyber security programs and successfully resist attacks from the most sophisticated hackers.

Keys to Being a Successful CISO

1. Instill a Sense of Responsibility in Your IT Organization for Cybersecurity

CISOs should instill some sense of responsibility in their IT organization for cybersecurity.

I was working with a company recently where we finally got an agreement with all the senior IT managers of innovation, digital innovation, application development, and systems deployment that each one of them in their performance appraisal, would now have a rating on how well they implement cybersecurity policy and support the cybersecurity program – and the CISO will write that review. We did that because of the way the organization was continually disregarding cybersecurity policy standards. Many knew what they were supposed to do but were disregarding it, so we knew we had to fix that problem first.

You must make cybersecurity part of IT governance.

2. Don't Focus on Compliance

This is hard, especially for financial services organizations that must comply with various regulations. But when you're chasing the compliance checklist, you're usually not focusing on the sophisticated APT (advanced persistent threat) groups. Too often when I go into organizations and find out what they're doing, they're working on a variety of cybersecurity projects, mostly because an author came down to their office with that direction and then the next month, came with different direction, and so on. And soon, the organization is working on an odd collection of projects.

But, most importantly, what they're not focusing on is the real risk and the real risk is sitting in Russia coming up with better attack payloads and techniques. This is what organizations need to be focusing on, much more so than they are today.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster. Follow us on Facebook, Twitter, and LinkedIn.

Website
www.NetSPI.com

Email
Info@NetSPI.com

Phone
612.465.8880

Ver 03 – 012021