info security
STRATEGY | INSIGHT | TECHNOLOGY

Infosecurity Magazine Webinar Report

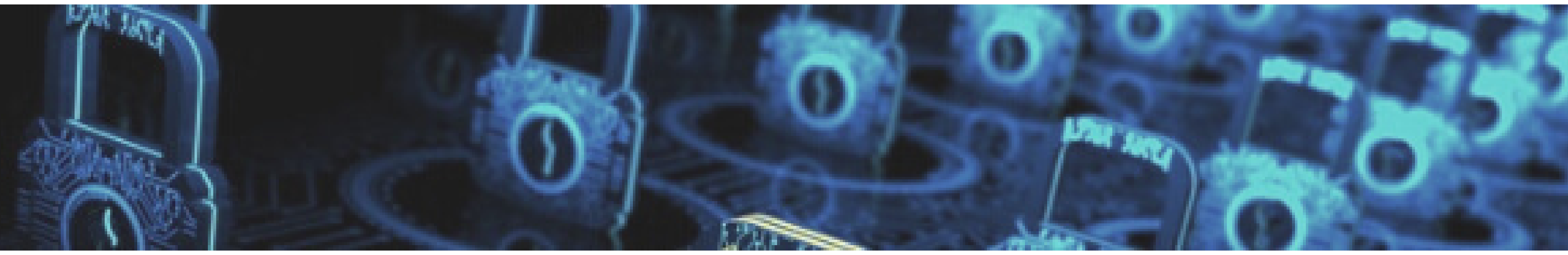
# From Governance to Implementation to Results

BROUGHT TO YOU BY

NETSPI™

#INFOSECWEBINAR

@INFOSECURITYMAG



Within the broad field of information security and the narrower topic of compliance, there exists the subject of governance, which typically encompasses matters such as the governance of people, technology, strategies and policies.

Governance is an important and overarching matter, however, some may question whether it really receives the attention it deserves as a key part of the overall structure of how information security operates.

Well, it was the topic that took center stage on a recent Infosecurity webinar, with a panel of experts discussed featuring NetSPI CEO and founder Deke Georg and 2BSecure consultant Bob Bigman (former CISO of the CIA) discussing the various facets of the governance issue.

The key aim of the webinar was to explore and assess which information security measures today's CISOs should be taking to effectively prevent attacks, and outline the strategies that are worth focusing money and time on.

> "It does involve a step back to understand that the world and associated threats get more severe and with that being the case we need to incorporate risk into what we're doing"

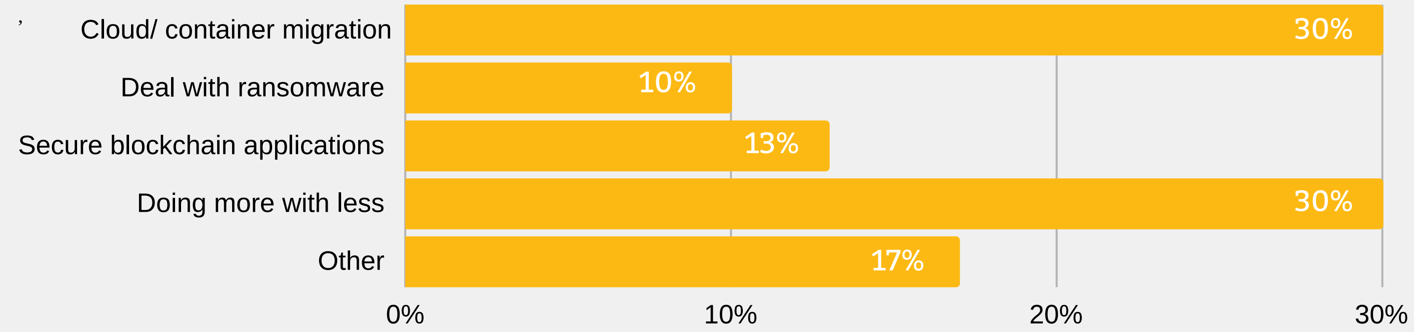
## BUILDING BLOCKS

Opening the discussion by reflecting on the building blocks that can enable a "great security program," Bigman said those who have enabled a great security program have done the following: established a partnership with the IT organization, understood where the systems and sensitive data reside and gained comprehensive visibility into the security status of all systems.

"Basically, they [CISOs] are a partner with the IT organization," he added. "The CIO and the CISO work together, do joint projects together, and the IT organization doesn't move without some sort of approval."

Bigman also explained that an organization may have all the IP addresses of what it is working with, but visibility can often be a key issue, as too many companies don't know where their systems are, how they are connected and where their sensitive data is. "It's hard to have a security program and implement cybersecurity controls if you don't know how your systems are configured or more importantly, where your sensitive data is."

## Q. What is your security team being asked to do in the next 1-3 years?



*Results of audience poll question 1*

# VISIBILITY

Bigman went on to explain that organizations need to have consistent visibility into their networks, systems and applications in order to operate a secure network "have any chance against the hackers."

This element of governance should include knowing where your greatest risks reside, where you should be putting your efforts, energy and money on a day-to-day basis "and, at any one point in time, knowing what the risk level is of your various systems."

So how much is visibility a key part of achieving a strong security program? Bigman cited the use of continuous monitoring, which can be utilized to maintain a consistent visibility of systems and their risk levels and also make an organization immediately aware of any changes.

Was visibility an issue for users? George said it was "as you need IT and security groups to work well together, and that starts with making sure you've got great people being great team players that can work well together and work towards a common vision.

"I think that setting a strong and clear vision and mission is super important and it has got to be all encompassing so it is not just built in a silo."

George acknowledged that is hard to do, but when it works, he said it can be "amazing for what it creates in a work environment as a lot gets accomplished."

> "I think that setting a strong and clear vision and mission is super important and it has got to be all encompassing so it is not just built in a silo"

# SUPPLY CHAIN SECURITY

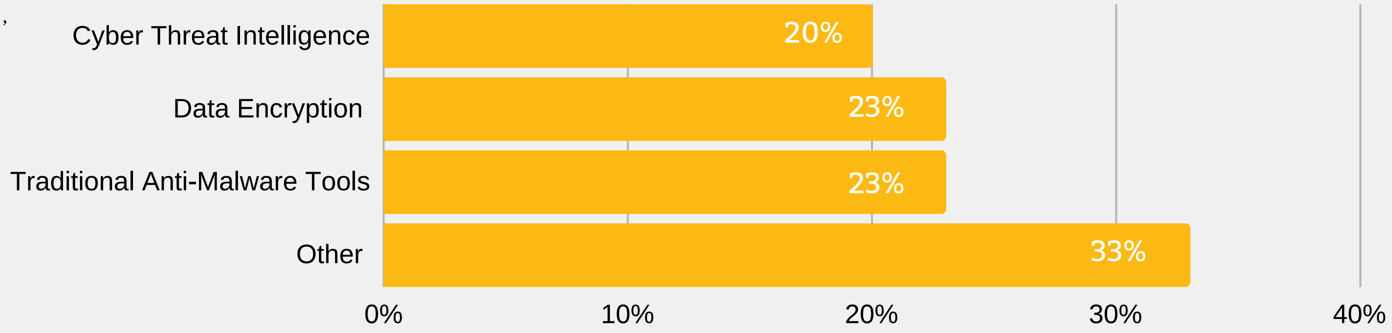
Another issue which is key to successful governance is managing third party risk, which George said many companies are currently tackling with a great deal of risk around assets that are not known about and therefore not prioritized.

"So many organizations are talking [about third party risk] now and there is a ton of risk attached to that," he said. "You may have to apply unique standards and processes to deal with the risk associated with that."

In terms of what works, George said businesses have so many issues and challenges coming at them "and everything has to be done yesterday;" users want to implement the latest and greatest technologies, and he recommended not being too technical beyond your capabilities whilst also avoiding being so rigid that it becomes difficult to evolve the program.

"If you rely on compliance, which can be a rigid standard, you'll find that it is very difficult to advance that component space, so incorporating risk can be difficult and can cause problems." George also recommended doing "the basics right" before attempting anything new or challenging.

### Q. Which "shiny object" has your organization used that did not work?



*Results of audience poll question 2*

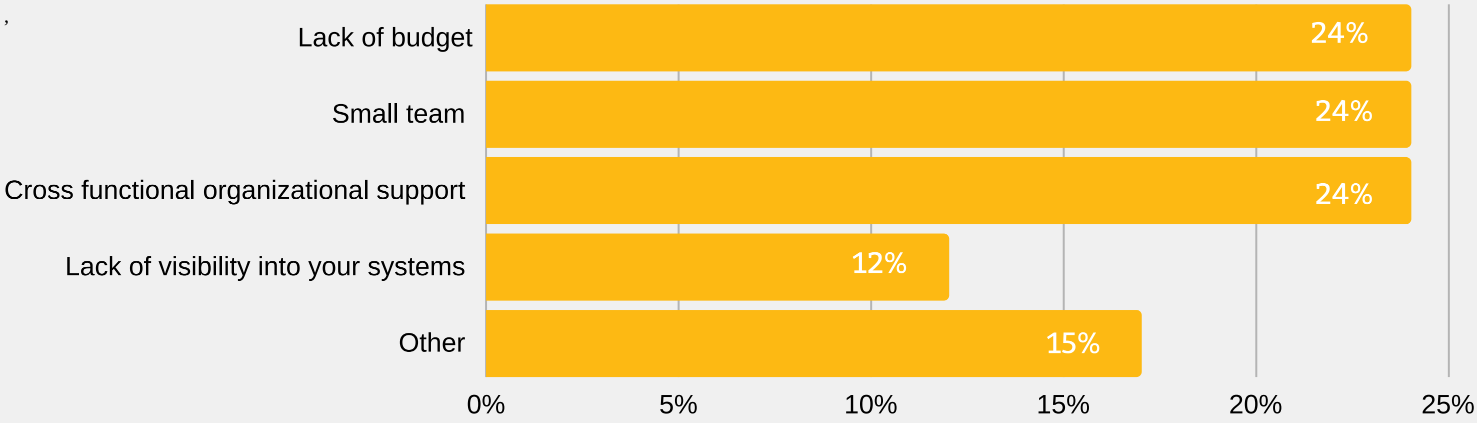
# HIRING CHALLENGES

Another factor of governance is building the right team. Asked where he commonly saw governance being done incorrectly in this regard, Bigman explained that when you're building a system you need to know what the necessities are for security to meet requirements. "It is not just cyber-governance, it is cyber-governance as part of IT governance, and it is very important that the teams who are doing the IT projects understand the governance responsibilities." Bigman added that this involves being given ownership responsibilities, to be made to feel a part of the team and understanding security requirements and compliance.

So what leads to that end goal? Bigman said it begins with a strong CIO, and with a strong CIO, there is a better chance "and the best organizations have a central focus." He said governance is achieved where there is a strong security focus, where people know where their responsibilities are and how to support security.

George agreed, stating that it comes back to great people and building a great team as well as corporate IT governance, and combining the two to create a core vision of where you are going. "The greatest organizations in the world have done this, which is interesting as there is a lot going on and there could be a lot of things to look at – but to hit a balance of not being verbose enough so they are not overwhelmed, that is key as you've got to give teams ownership and clear responsibility for what they need to do."

**Q. What are the biggest roadblocks to your organization's security program?**



*Results of audience poll question 3*

# INCORPORATING RISK

Another point that was raised in the debate was around what leading organizations are doing to both comply with governance requirements and incorporate risk into their programs. The three points raised were: still satisfying governance and compliance, hiring great people to understand what's working (and what's not); and incorporating risk by driving risk-based approach initiatives.

George said governance should drive a governance, risk and compliance (GRC) strategy, but governance is the easiest factor to achieve of the three. As businesses mature, they need to change their risk strategy as appropriate, "but risk is a cultural shift and you need to begin thinking about conversations about what your mission is and what you are trying to accomplish."

George said the evolution of programs to be more risk-based will have risk incorporating compliance, but most organizations are not at that stage yet. “I do think that having good people on the team is really important for having that shift, as good people can understand that step from compliance to risk, but it does involve a step back to understand that the world and associated threats get more severe and with that being the case we need to incorporate risk into what we’re doing.”

This therefore leads back to the conversation about how visibility, corporate governance and an engaged team are key to achieving that level of governance. If you want to remain ahead both competitively and defensively, governance should be at the core of your strategy.

## SPEAKERS

**Bob Bigman**,
Cybersecurity Consultant,
2BSecure, and former CISO,
CIA

**Deke George**
CEO and Founder,
NetSPI

**Dan Raywood**
Deputy Editor,
Infosecurity Magazine

## BROUGHT TO YOU BY:

NETSPI™

NetSPI is an expert in Penetration Testing and Vulnerability Management. Clients trust their clear and actionable remediation advice. With NetSPI you get an experienced team with consistent and proven testing playbooks.

This live webinar was broadcast on
Infosecurity Magazine’s Webinar Channel
23rd July, 2020 and is now available on demand
https://www.infosecurity-magazine.com/webinars/governance-implementation-results/