tenable network security

Politics of Security Webcast Summary

Working with Stakeholders

January 31, 2013

(Revision 1)

Table of Contents

1 Introduction

While the job of a Chief Information Security Officer (CISO) requires technical and security expertise, the real key to success may lie in relationship management.

Tenable Network Security's ongoing "**Politics of Security**" webinar series convenes panels of past and present CISOs to discuss the political challenges of the job. In late January 2013, a panel discussed the challenges of working with the stakeholders in the security process – identifying allies, gaining alignment and avoiding pitfalls.

The panelists for this discussion were:

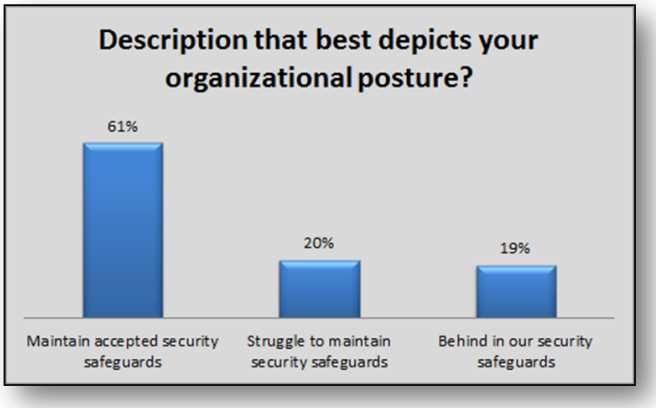
- Larry Brock, former CISO for **DuPont**
- Tom Doughty, Vice President and CISO at **Prudential Financial**
- Bob Hilmer, Director of Information Security and Directory Services at **State Farm Insurance**
- Craig Shumard, Chief Information Security Officer, **CIGNA** Corporation 1999-2010, currently consulting
- Marcus Ranum, Chief Security Officer, **Tenable Network Security**, consultant to industry and government agencies

Key Takeaways:

- **Monitor** what's being said about security and make sure people aren't using it as either a scapegoat or an excuse.
- **Know** how and when to escalate issues – and make sure that you have your facts straight before you escalate.
- **Keep** the business strategy in mind**.** The job of IT is to facilitate business as safely and reliably as possible. When you run into problems, reframe them at this higher, strategic level and often they will resolve themselves.
- **It's your responsibility** to communicate well**.** You need to understand who isn't getting your message. If they're not listening, figure out what they *will* listen to.

2 Know Your Security Posture

While many organizations may feel they are maintaining high security safeguards, the increase in number of threats and successful compromises reported across industries paint a different picture of reality. The audience survey may be indicative of this false sense of security.



Key points:

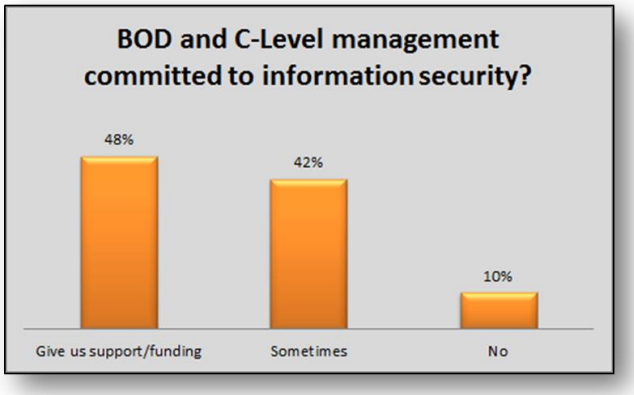
- Security safeguards are challenging with emergence of new technologies such as mobile devices, BYOD, and cloud. Be sure to accurately assess risks associated with these technologies
- Security safeguards must not be treated independently of reliability to ensure network availability
- Be sure to get the buy-in and get resources from executives as needed to ensure accurate security safeguards for your organization.

3 Getting High-Level Buy-in

The success of a CISO's security program depends on whether the CISO can get broad buy-in from key stakeholders – particularly the board and C-suite.

1. **Use business language and avoid technical detail.** All of the panelists agreed on the importance of speaking in business terms, at a strategic level, when engaging with the C-suite and the board. Don't make the discussions about technology and jargon – focus instead on business risk and strategy. And stay tuned into the mood and expectations of the group: were you invited in or did you have to put yourself on the agenda?

- When speaking with the board or C-level, avoid jargon or metaphors that oversimplify the situation and could be seen as 'talking down' to the stakeholders
- If possible, answer the questions they haven't asked yet, which might include any resources you need to address the issue
- Always be prepared to ask for what you need.
  "Don't just answer their questions – finish with by summarizing what you're worried about today and what you're doing. And if there's something you need, ask for it." Tom Doughty



2. **Share multi-year strategies and plans.** Present a multi-year strategy that includes major threats to the business, with strategy described in business terms. Then share the security plans that align with that strategy. This will give the board and C-suite essential visibility into what you are doing and why.

3. **Share benchmarks and reports.** Use a benchmarking tool to assess security strengths and weaknesses and highlight potential risks. Share the results with the board on a regular basis to give them high-level visibility into whether or not you are making progress towards security objectives and risk reduction.

4. **Highlight your customers' requirements where possible.** If you have RFIs or RFPs from customers, highlight the security trends that your customers see as important and use that information to support requirements at the C-level.

5. **Leverage C-level steering committee.** Include C-level individuals on the security steering committee to provide direction for the program. This takes away some of the mystery around security and provides important transparency.

   "Meet with your steering committee on a quarterly basis. As you go into a committee or to the board, having this C-level commitment to your plans is invaluable." Larry Brock

4 Working with Natural Allies

In a well-functioning organization, the CISO has a number of 'natural' allies that can help them get buy-in and alignment. But sometimes these natural allies do not work well together. For example, a survey of webinar attendees found that for almost half of respondents, the relationship with the Audit group was sometimes problematic.

"When you see compliance and risk management used to 'club' IT, that's a sign of a dysfunctional relationship. It's almost always due to a lack of board-level commitment to information security." Marcus Ranum

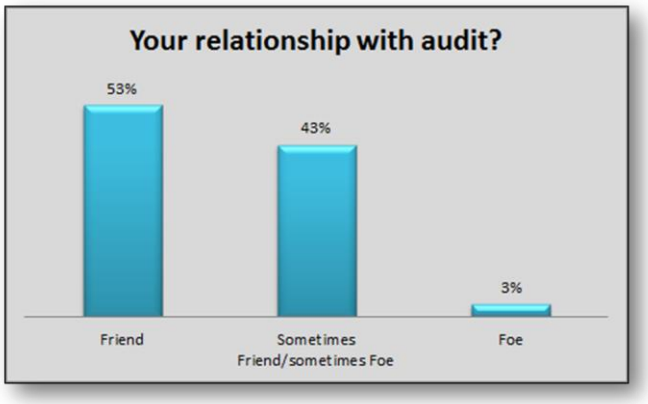
In 'dysfunctional' organizations, the CISO's role will be more difficult. Establishing and maintaining good relationships with these allies is critical, and communication is almost always the key.

- **Compliance:** Compliance is a natural ally. However, the panelists warn that the CSO must be careful about equating security with compliance and using compliance as a baseline justification for security measures.
  "If our stakeholders are accustomed to supporting security for compliance reasons only, then it may be more difficult to take actions on a risk-driven basis without a compliance driver." Tom Doughty
- **Privacy:** Security and privacy are also natural allies.
- **Audit (internal and external):** Foster your relationships with senior auditors. Audit observations are critical and can be useful for communicating with the board. As with compliance, the panelists warn about letting audit findings dominate the security program focus. As the designers and maintainers of controls, security can see things that auditors do not.
- **Enterprise Risk Management:** Information security should be a participant in the enterprise risk discussion. For the CISO, participating in enterprise risk discussions provides a broader view of risk.
- **Legal:** The legal team is involved in any litigation exposure due to lack of policies or internal controls, and can provide important guidance and counsel on what not to do. They can also serve as a safety net, identifying contracts that haven't gone through appropriate due diligence for security.

- **Human Resources:** Make friends with the VP of Human Resources, who has the opportunity to support security programs through education and awareness, exit interviews, new employee onboarding, etc.

5 Are you Friend or Foe?

Some groups can be both friends and foes at different times – even among natural allies. The panel shared some of its suggestions for dealing with the two relationships that have the greatest potential for becoming adversarial…



- **IT:** The CISO is often a part of IT, so there should be a natural alliance. The CISO depends on IT to make sure things happen, so every individual in the CISO organization must work closely with IT. However, individual groups within IT have different priorities and may be measured and incentivized on different measures. In some situations, IT can be more of a 'foe' than a friend.
- **Business units**: Depending on your business model, the business units may essentially be funding security initiatives and controls. You need bi-directional transparency into what is happening, where resources are being allocated, and why.

"Your worst foe is a business partner who conceals their efforts without letting you learn of them until they are about ready to put it into place." – Bob Hilmer

"You don't have to win every battle, but you want to win the war. Sometimes you will make concessions or put in countermeasures. Understand how and when you need to escalate issues, and make sure you have your facts straight first." Craig Shumard

6 Summary

To listen to the full discussion of this webinar or access the past sessions, visit www.tenable.com/webcasts. Additional webinars, in this series, include

- The Politics of Risk Tolerance
- The CISO Job: Getting It and Keeping It (2 parts)
- The Politics of Security: Getting What You Want (and Avoiding What You Don't)

You can find more white papers, webinars and videos in the Resources section at www.tenable.com.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com

tenable network security