Setting up a security steering committee

Introduction

We frequently encounter companies that have isolated security into its own segment, where it can't bother anybody else too much. Responsibilities are usually split between low-level information technology (IT) staff, who must juggle break/fix scenarios within technology infrastructure along with security tasks. Competing priorities typically mean security best practices are overlooked for the sake of convenience. Any security decisions made by the IT group are usually done in a vacuum with little input from the rest of the organization.

A recent survey of 400 global business and security executives around the world[1] demonstrated a significant disconnect between most businesses and their cybersecurity. In addition, more than half of respondents had not established a steering committee to address cyber-risks or their effect on the business.

For example, in many industries, culture is a leading challenge in implementing proper cybersecurity controls. Yes, culture. How do security decisions affect the everyday lives of employees? Implementing or restructuring a steering committee is a valuable practice to guide security strategies while ensuring alignment with organizational culture. The net results are often positive for all parties involved, but especially for the people responsible for security-related tasks.

80% of respondents did not consult with business users when making cybersecurity purchases or evaluate the business impacts and risks[2]

A steering committee should spend a considerable amount of time discussing the cultural impact cyber-risks have on the business. For instance, it's really easy for a cybersecurity professional to say, "Increase your passwords to 14 characters as a best practice," but companies need to understand the day-to-day impact increased password lengths will have on the business and culture.

Since most cybersecurity professionals focus on risks and not the business, it is critical to gather stakeholders from across the organization to discuss security issues and make joint decisions. That's where the security steering committee comes into play.

What is a security steering committee?

A security steering committee provides an open discussion forum where individuals or departments can raise concerns surrounding existing security policies, or influence the creation of new policies. The security steering committee establishes the corporate IT stance, showing that the company is dedicated to maintaining its systems, and ultimately creating a cost-effective strategy to properly protect systems and data.

Some organizations already have an IT steering committee, which is a great first step. That existing committee could be expanded to address both IT and security initiatives, changing the title to IT/security steering committee. This will provide an effective forum to address some of the frequent resource conflicts that can occur between IT and cybersecurity. (See the sample security steering committee charter in the appendix at the end of this white paper.)

[1] "Failure to Measure Up: The 2017 State of Cybersecurity Metrics Annual Report," Thycotic, accessed Nov. 6, 2018, https://thycotic.com/resources/cybersecurity-metrics-report-2017/.

[2] Ibid.

Vulnerability management is an example of a frequent resource disconnect between IT and security. If security finds 100 extreme vulnerabilities on the internal network, but IT is currently implementing a new business intelligence (BI) tool, guess what happens? Considering that the BI tool is backed by the business, any resources needed to fix the vulnerabilities are usually allocated to the BI implementation. Therefore, the vulnerabilities aren't fixed until resources are available.

Utilizing a security steering committee can help make that conversation and decision occur in an open forum where all business goals are considered. The security steering committee often decides to enlist an outside contractor to fix the vulnerabilities. Thus, the budget and project to reduce the extreme vulnerabilities is approved through the security steering committee.

Who should attend a security steering committee meeting?

Security steering committees should include representatives from across your organization whose responsibilities are adjacent to security concerns. For example:

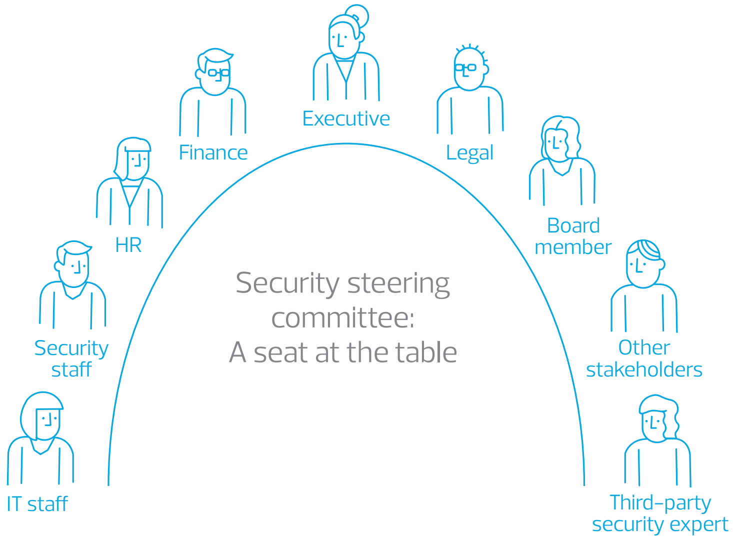
- Legal counsel – To provide regulatory and legal compliance insight
- Human resources – To facilitate communication with personnel or manage training
- Internal audit – To help define security metrics and validate compliance
- Regional directors – To provide information on local concerns that corporate staff may not be aware of
- Project managers – To help ensure the meeting runs smoothly and track action item status between meetings

Many organizations don't consider other key players that should also be a part of the committee. For example, third-party security vendors make excellent committee members because they can communicate changes in security threats, technologies and strategies to your organization.

Inviting a member of the board to attend the meetings is also an effective strategy, as some board members are actively engaged on security matters. A board member can help shape security efforts throughout the year rather than just in the short time that security is usually allotted during regular board meetings.

What are the benefits of a security steering committee?

Since security steering committee meetings involve representatives from multiple business units, they allow organizations to receive multiple perspectives on every security issue. For example, the accounting department may bring up the challenges involved in signing into multiple applications every day to do their jobs. In that scenario, the IT department can detail how single sign-on functionality can be implemented to make their jobs easier. Then, a security representative can provide guidance on how to securely implement the solution. Finally, executive leadership can approve the funding necessary to implement the solution.


Executive
Finance
Legal
HR
Board member
Security staff
Other stakeholders
IT staff
Third-party security expert
Security steering committee: A seat at the table

With cybersecurity issues constantly in the news, directors and officers frequently seek updates on the organization's cybersecurity initiatives. Board members are bombarded with cybersecurity concerns, and given their fiduciary responsibilities, they generally bring up items that they have read about or heard from their peers. Aligning security steering committee meetings with board meetings—perhaps offsetting the gatherings by a week or two—can allow the security steering committee to prepare a security brief for board members, in the event that they request an update or have specific concerns.

Recently, for example, a board member shared an article that stated nearly 50 percent[3] of organizations patch their systems within one week following a release, potentially leaving networks exposed. This report was issued in the fallout from the May 2017 WannaCry outbreak. Therefore, during the security steering committee, IT members discussed the cyber-risks involved with patching systems, and business members countered with the operational risks of patching systems that quickly.

While patches will reduce the cyber-risk, the availability of business-critical systems may also be affected. In the end, the security steering committee agreed to implement a 30-day patch window, but made an exception for specific outbreaks, such as WannaCry, that should be patched as soon as possible.

Conclusion

If you believe that your organization is suffering from a security communication breakdown, a security steering committee might be the right solution to bring all involved parties together. Security steering committees will provide buy-in across business units and management levels on security decisions. Ultimately, this will make it easier for the security department to raise issues to executive staff and board members, and also improve cultural adoption of security practices.

[3] "One in Ten U.S. Organizations Hit by WannaCry: Study," Securityweek, accessed Nov. 6, 2018,
http://www.securityweek.com/one-ten-us-organizations-hit-wannacry-study.

Appendix – Sample steering committee charter

Security steering committee charter

This document establishes a formal security steering committee at Watts Refrigeration. This charter is to serve as proof that senior management has granted this group with responsibility for managing security risk issues at Watts.

Purpose

This security steering committee provides leadership in the protection of information assets and technology. The committee members advise on and prioritize the development of information security initiatives, projects and policies as advocates for the stakeholders of Watts. This committee will be charged with resolving security and compliance risk issues that affect Watts.

Sponsorship

Executive sponsor: Stephanie Campbell, CFO

Scope

This security steering committee provides guidance and leadership to maintain and improve the confidentiality, integrity and availability of information across Watts.

Committee members

Committee membership will be approved by the CFO based on the technology vision and enthusiasm that members will bring to the committee. The committee will annually review membership and recommend changes after considering needs for continuity and expertise, as well as the need to encourage change and opportunities to participate. Administrative support will be provided by the (applicable) department.

Committee responsibilities

1. Establish goals for the information security program
2. Coordinate the development and review of system-wide information security policies, procedures and guidelines
3. Recommend, review and prioritize information security projects and initiatives
4. Communicate information security needs and sound practices between departments
5. Facilitate awareness and cooperation between the security program and business units
6. Review the performance and effectiveness of the information security program based on risk measurements

Meeting schedule

Meetings will be held quarterly at the Watts main office.

Decision model

Decisions will be made through member consensus. Disputes will be resolved by the CFO and executive staff members associated with the committee.

Meeting agenda

An agenda will be drafted by the committee chair with consultation from committee members, staff and other stakeholders. The draft agenda will be distributed to committee members on the Friday preceding the meeting. Feedback will be incorporated into the final draft agenda, which will be presented for adoption at the committee meeting. A sample agenda could include plans to:

- Discuss open issues from previous meeting
- Discuss any internal security issues which have emerged since previous meeting
- Discuss any new external security issues which have emerged since previous meeting
- Prioritize the open list of security issues
- Assign responsibility and timelines for remediating security issues

Attendance

All members of this committee are expected to actively participate. Regular attendance for meetings as well as involvement in special activities is important to satisfy the many responsibilities of this committee. Members are expected to RSVP to meeting notices. Due to the nature of the committee work, member consistency is critical. If members are unable to attend, proxy will not be recognized. Committee members may invite additional attendees to participate as appropriate.

Work groups and ad hoc teams

From time to time, the committee may need to involve additional expert resources beyond the committee membership. The chair may designate ad hoc teams to conduct specific work and report back to the committee. Ad hoc teams may include noncommittee members that are subject matter experts. One committee chair will be selected to provide leadership and direction to the ad hoc team(s) while performing assignment(s).

Communication

Meeting notes and action items will be documented at each committee meeting. Following each meeting, the administrative support staff will distribute the documents to the chair for review. The resulting document, and other materials, will be distributed to the committee members prior to the next meeting. During the next meeting, the documents will be approved. Once approved, the documents will be posted to the company's intranet. The committee charter, meeting schedules, membership roster and other documents will also be posted to the intranet.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM