Chad Ballay

**Week 4 - Effective Implementation of Security Policy**

Security best practices is to have multiple different roles with an interlocking web of checks and balances. This overlapping of stakeholder responsibilities is a feature that ensures defense in depth and that no single point of failure should go unnoticed.

**Compliance Liaison**

This role will often be the primary mechanism for ensuring that a directed communication channel exists between the security area to the individual departments and individual contributors outside of the security area. Proactively raising awareness as well as championing alignment early within the project lifecycle within the various departments. (Rollauer)

**Security Administration Team**

This team is a specialization of the larger System Administration team. They will work at the infrastructure and operational layer of installing, maintaining, monitoring of systems. Heavy consideration must be given for ensuring process audits and implementation reviews to meet the significant ethical and compliance dimensions of this role. (Watts)

**Incident Response Team**

The organized process for triaging the demands on an organization during or after a security breech will fall upon this class of team. The reactionary nature of their duties requires a unique mix of dogmatic adherence to preparation and training that also allows for a flexibility and autonomy in response. (What Skills Are Needed When Staffing Your CSIRT)

**Security (Outsourced Firm)**

Externally sourced team for an internal facing role is not an uncommon pattern. The role that teams like this one play could be sourced internally. Existing teams may also share duplicated functions individually, but no single team will wholly duplicate the sum of the externally sourced team. The benefit is that the transactional nature of explicitly contracted relationships coupled with the clearly defined lines of communication will often serve as a virtuous feedback loop. Being beholden only to the upper echelon of the administration tier of the organization is also a contributing factor for the success. (Outsourcing Business IT Security Pros & Cons)

Much of these delineations depend on the specific organization’s size and maturity. For a relatively small organization budgetary constraints will keep the security area to a limited number of employees. In those cases, you will often see teams have broadly defined domains and individual contributors will focus on being generalists instead of specialists. None of this is surprising. Security is often seen as a cost center and thusly the staffing numbers relative to total company size and balance sheet will inevitably reflect this. (Tipton and Krause)

**Large Organizations and Lines of Communication**

A close up of a logo

Description automatically generated

1-Illustration of the geometric growth in lines of communication vs number of people involved.

The calculus for specialization is driven by the organization’s size. As witnessed by the brutal math of , the lines of communication grow exponential. This increased number of communication channels will be the driving force. (Nocolette)

**Security Area Environmental Response**

Org chart alignments can reduce the communication channels to curated pathways. Weekly newsletters being an ideal example. A scannable collection of distilled information presented as a one communication to a large audience. Thoughtful and intentional growth of a shared sense of community to increase the buy in for non-security area teams when presented with security area requests or requirements.

**Compliance Liaison pt 2**

The role of Compliance Liaison is a first-class example of this. For the non-security areas this represents a single interface that reduce the cognitive load of compliance efforts. The established communication channel provides the security area with a mechanism to get in front of the right eyes at the right times. This role requires a high degree of trust and acceptance. If perceived as an outsider or as not a core competency to the organization, this role will fail. For large organizations this role should not be outsourced.

**Security Administration Team pt 2**

The high degree of technical proficiency will often require this to not be outsourced. Dollars spent here have a high likelihood of ongoing payback. Business needs will precipitate changes being introduced to existing systems. Speed of implementation and execution success requires this to be a core competency.

**Incident Response pt 2**

This team will often require a high degree of technical proficiency, but the work intake variability shifts the value proposition closer to being outsource friendly. Maintaining a large enough team to handle the highwater mark of the historical max number of crises is very large budgetary spend. By the time that the organization reaches capacity it is because a new incident has been discovered. Due to the skillset needed and the reaction time for capacity growth an established vendor partner relationship makes this a potentially outsourced area.

**Security (Outsourced Firm) pt 2**

In the case of a defined initiative where the engagement criteria is defined a self-contained security team can be outsourced. Transformational and onetime initiatives will often require that a security area maintain existing services provided while the additional effort proceeds in parallel. Some examples would be SOX compliance, GDPR impact analysis, on-premise migration to cloud infrastructure, or tech debt removal like AIX to Linux. Initiatives like this are focused and require parallel progress to be made while existing security services are maintained. The nature of these initiatives lends itself to the creation of SLA’s which will have an additive affect on existing process documentation. The organization size budgets of these initiatives require that senior level administration is tightly involved. This will often bypass unacknowledged communication roadblocks. Fiefdoms that have been established that otherwise are tolerated or not even acknowledged. Finally, these initiatives are never without resistance. Large scale changes are risky and complicated. An external third party can often be used to communicate the breaking of existing patterns without engendering the long-term damage to the culture that reactionary resistance will do.

**Conclusion**

If you are a small organization, these roles won’t be implemented at the team level or if they are, they’ll be done by teams with too large of a portfolio to cost effectively outsource without a great degree of care. If you are a large organization, you can only outsource these roles when you understand the inertia involved as well as the core competencies needed.

# Works Cited

Nocolette, Dave. *Applying Brooks' Law*. n.d. <https://www.leadingagile.com/2018/02/applying-brooks-law/>.

*Outsourcing Business IT Security Pros & Cons*. n.d. <https://www.bradenonline.com/blog/outsourcing-business-it-security/>.

Rollauer, Tom. "How Regulatory Liaison Offices Can Help Manage Risk." n.d. *The Wall Street Journal.* <https://deloitte.wsj.com/riskandcompliance/2014/03/11/how-regulatory-liaison-offices-can-help-manage-risk/>.

Tipton, Harold F and Micki Krause. *Information Security Management Handbook*. CRC Press, 2007.

Watts, Stephen. "System Administrator vs Security Administrator: What’s the Difference?" n.d. *BMC.* <https://www.bmc.com/blogs/system-administrator-vs-security-administrator-whats-the-difference/>.

"What Skills Are Needed When Staffing Your CSIRT." n.d. *Carnegie Mellon University.* <https://resources.sei.cmu.edu/asset\_files/WhitePaper/2017\_019\_001\_485684.pdf>.