Ace Consulting, Inc.

Chad Nelley

Cyber Management

CSOL 550

December 5, 2016

McCready

Table of Contents

Abstract

As part of any information systems security plan, one of the first concerns of the plan developer is to distinguish and assess the conflicts that exist between optimum cyber security and the productivity, profitability and accessibility of business processes that promote market leadership for the entity. In determining the right balance, management must find the common intersection where costs, risks, profitability and organizational scalability all intersect in harmony. The costs of implementing ultimate security can escalate incredibly fast which will ultimately impact profitability. Further, the risks associated with having a lax set of security controls in place could jeopardize downstream profitability of the organization in the event of a major breach or exploit – the costs of which include but are not limited to brand tarnish-ment, extensive litigation, exfiltration of IP assets or excessive penalties incurred in the event of a non-compliance issue.

Optimal Cybersecurity principles revolve around reducing risk to the organization from exploits derived from the digital realm related to data and information integrity. Cybersecurity at its most basic level is risk management with the primary intent to build technologies, policies, practices and procedures to protect information and networks that are critical to the ongoing vitality of the business or entity. Cybersecurity is an executive and board level imperative and concern and requires full-time attention and constant vigilance. Cybersecurity needs to be a CEO primary concern and organizations need to allocate appropriate resources to the Cyber effort within their organizational structure. Optimal cybersecurity postures will take into account, insider threats, nation-state threats, organized crime threats and competitive espionage threats. The challenge for the entity? To protect against each of these variables and more is an expensive and timely endeavor.

On the other hand, optimal business practice at the highest levels is centered on the principles of profitability, market share expansion and ultimately increasing shareholder value as defined by the Board and in publicly traded entities the shareholders at large. The optimal business practice is to find the best, and most cost effective solutions to problems that impact the business. Until recently, cybersecurity and security in general has been viewed as a highly costly endeavor with almost no perceivable ROI. Why was this? Until the likes of significant recent breaches to major brands (Target, Sony, TJX,

Yahoo, Anthem) and the costs of litigation outcomes has cybersecurity become framed in terms of ROI. Some studies have shown that the cost per record exposed in a breach can be as much as $1500 in legal fees, settlement payouts, restitution, compliance violation fines and the list goes on and on. To put that in perspective, if a company has a 10,000 record database and that database becomes compromised, the expected cost of that breach could be as high as $15,000,000.00. Extrapolate that out to a tier 1 blue chip entity like an Anthem or Yahoo who each house millions of records and the risk impact becomes significantly high. For example, the recent Yahoo breach has already cost Yahoo $1B in market share value as Verizon, who was in the process of acquiring Yahoo when the breach was announced, immediately asked for a $1B concession to continue the transaction to acquire. The $1B ask equates to 25% of the overall deal value.

In the Yahoo example above we see a direct correlation to the conflict between cybersecurity investment and posture and optimum business practice approach. Clearly the executives at Yahoo at some point in the past made a risk assessment call that the investment in Cybersecurity was not as important as other business drivers, subsequently leaving the entity exposed to a higher level of risk – resulting in a one day summary market valuation reduction of 25%. This underscores the need for greater understanding and urgency of Cyber at the Executive and Board levels across all industries.

This ISSP document and plan is intended to be used as the roadmap for the security implements that Ace Consulting will deliver over the next 18-24 months in an effort to harden our Cybersecurity posture and reduce our risk profile. The intent of the security program is to find the appropriate balance between cost & overhead containment and a solid security infrastructure that lends itself to robust security practices that will ensure the organization’s long term viability.

Following this Abstract is a comprehensive outline of the ISSP document that will be developed and fleshed out further as part of our comprehensive approach to security. For purposes of this audience (Executives and Board Members) this is an abbreviated format that will only touch on the Primary headings of sections 1-8. Sub section details, will be available and found in the comprehensive version of this docier that will be published and made fully available in the following business quarter. This document, in its abbreviated state is for purposes of high level review and approval.

Section 1: Company Summary

Ace Consulting is a tier 2 consulting firm that provides management, organizational development, program and project management to a variety of Government and Commercial Entities. ACI employs 150 knowledge workers and trained staff and has a dynamic growth plan over the next 5 years. The company currently generates circa $50MM in annual revenues, with a 3x growth factor expected in the next 5 years. Currently 60% of the company’s revenue base in generated from long-term, long-standing government contracts with the remaining 40% of revenue mix having their root in the commercial sector. A large component of the 60% of government work is indirectly supporting military and DOD contracts and missions.

Currently the company operates a distributed model with about 90 of the 150 employees reporting into our corporate facilities located in San Diego, Ca. The remainder of our staff are distributed and in the field servicing customers and generating new business opportunities. We expect this mix ratio to remain similar as we advance our growth model over the next 3-5 years.

The company plans to use its existing contacts and customer base to generate both short and long-term consulting contracts. Its long-term profitability will rely on professional contracts obtained through strategic alliances, a comprehensive marketing program and a successful referral program.

Initially, the company will focus on organizational professional development, strategic program and project management engagements, executive and management coaching and special project relationships. Beginning in year two of any engagement, ACI provides a separate and comprehensive management development service which will include facilitated organizational strategy and planning workshops along with vetted growth and industry specific strategies as well as additional networking opportunities. The company has rigorously examined its financial projections and concluded that they are both conservative in profits and generous in expenditures. This was done deliberately to provide for unforeseeable events. The company's CEO believes that cash flow projections are realistic.

It is with this information in mind that ACI has endeavored to boost and enhance its cybersecurity posture and make Risk Management and cyber incident hardening a primary strategic objective over the next 2 years. It is imperative to the ongoing success of ACI and complementary to our ability to scale and grow while simultaneously reducing our attack surface and maximizing our information asset investments.

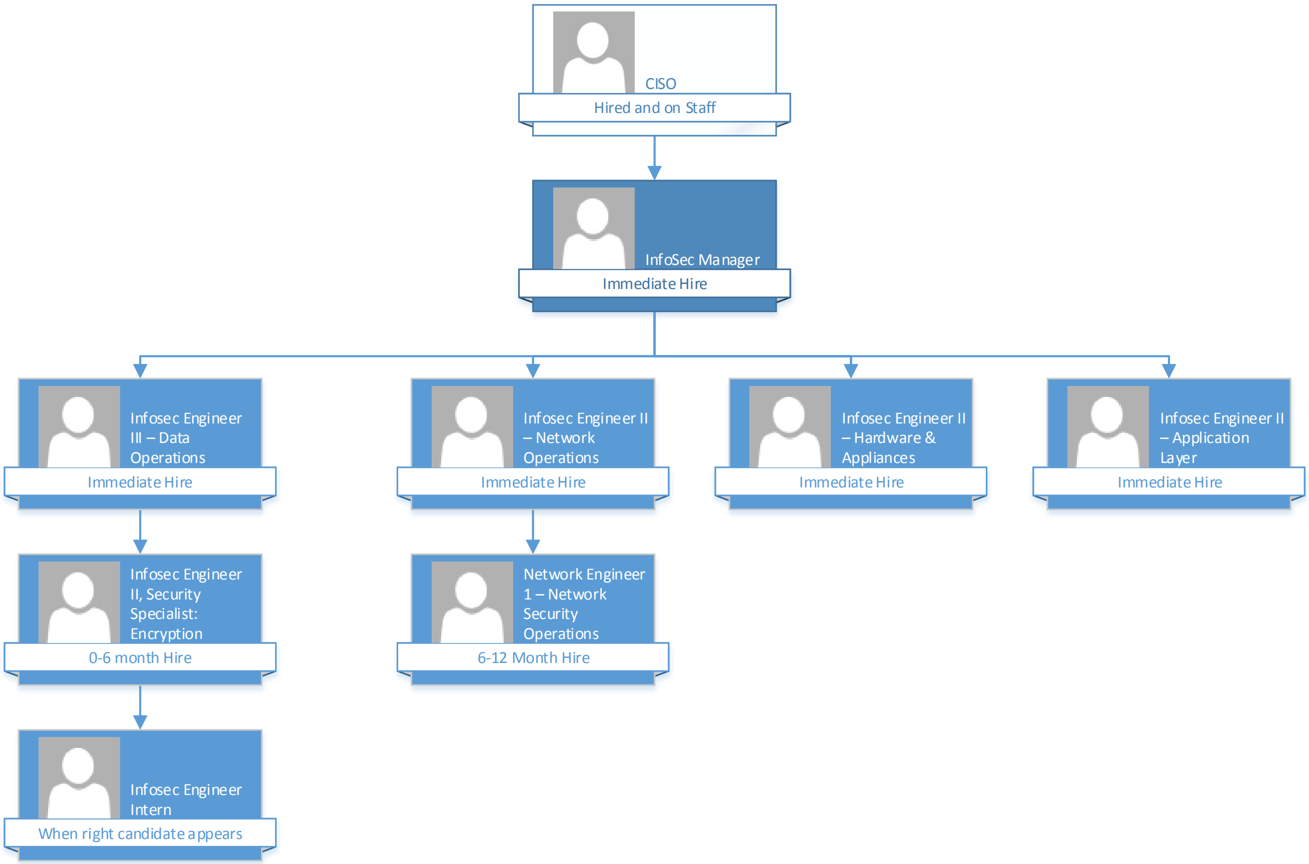
Section 2: Management & Organization

Until recently ACI has taken a more traditional organic and methodical approach to staffing for Management positions. ACI currently has an Executive Team that is comprised of the following roles: CEO, EVP/COO, CFO, CIO, GC, CSMO and subsequent VP and Director roles, rolling up to the C-Level in support of the business. Currently, Management staff overhead HC makes up for 12% of staff and 15% of overall payroll. With this new focus and endeavor on cybersecurity investment, ACI has also completed a comprehensive search and in 2016 has added the new Management role of CISO to the mix above. The CISO will have direct reporting responsibilities to the CEO and Board and will reside at the Executive team level. ACI has made this decision as a further commitment to our approach and philosophy on Risk Management and Security as key differentiators and key mitigation strategies in an effort to secure the long term viability and marketability of the ACI Brand. In the comprehensive version of this document, you will find roles and responsibility matrixes for all management roles, as well as comprehensive overviews for our approach to HR Management, Cost Management, Implementation Management, Project Management and Risk Management. These will be outlined and given comprehensive explanation in the final published document.

For purposes of this document, in addition to the roles outlined above we have developed the following primer on how our Infosec team at ACI will be structured moving forward. Building out a Cybersecurity organization is a complex task that requires a myriad of skills, skilled individuals and diverse backgrounds. As we look to build out our Cybersecurity organization, this paper will attempt to identify and isolate the skills and attributes we would look to source and implement across an organization. For purposes of this paper, we will be looking at an org structure for a company in transition (Growth) moving from 125 Employees to 250 Employees over the next 12 months. The company, Ace Consulting, has a legacy security model that has worked till now, but with the onset of new Government contracts and an increased revenue trajectory and a plan to potentially go public in the next 5 years, the Board has recognized and approved the hiring of a CISO and subsequent build out of the team. This paper will set off to establish the 18 month hiring plan and ultimate security organization development required to support the company's aggressive growth strategy.

Ace Consulting has made its initial hire of CISO and will also be outsourcing a large component of the Security Strategy set up and technology implementation. As part of this dissertation, a proposed RFP and tech criteria spec sheet will be included.

So, what will the security organization chart look like in 18 months when we are complete with Phase 1 of the implementation? If we are able to hire to plan, with revenue and growth supporting, here is what our initial organization will look like:


CISO
Hired and on Staff
InfoSec Manager
Immediate Hire
Infosec Engineer III – Data Operations
Immediate Hire
Infosec Engineer II – Network Operations
Immediate Hire
Infosec Engineer II – Hardware & Appliances
Immediate Hire
Infosec Engineer II – Application Layer
Immediate Hire
Infosec Engineer II, Security Specialist: Encryption
0-6 month Hire
Network Engineer 1 – Network Security Operations
6-12 Month Hire
Infosec Engineer Intern
When right candidate appears

This is what our foundational team will look like at the end of our 18 month build out trajectory. We expect that by this time, we will be advancing our Cybersecurity and Risk Management posture and will likely be poised to hire additional lower level engineer to facilitate day-to-day operations. You'll note also that, for at least the initial build out of this team there is no delineated "Director or VP" between the CISO and Infosec line manager. This was done purposely to allow for promotional growth of the hired Infosec

Manager on a 2-3 year trajectory. This approach will insure longevity and build in loyalty at the Infosec Manager level and shows an internal path for career progression to said individuals and other downstream staffers. With this approach we will be looking for mid-long term mid career professionals to cement the early team. As we grow, we will augment with lower level staff and more interns to build a funnel of promotable talent.

As you can see, we have also put a plan to hire for specific areas of expertise: Data Operations, Network Operations, Hardware & Appliances and Application Layer security. We believe this approach will effectively cover all bases required to move our security posture into the next millennium and set the right foundational mix for building out critical teams.

Section 3: Planning

As our organizational mantra dictates – planning is the most critical element of any engagement. So, it should come as no surprise that Planning will be a paramount undertaking for our Cybersecurity enhancement project. As the ACI experts will tell you – Fail to plan, plan to fail. In the Planning phase of this endeavor to implement an effective ISSP we will layout our comprehensive approach to security implementation management to include but not limited to: Physical Security, Access Controls, Data Security, Encryption Models & Tools, Website Security, Network Security, Device Management Approach, Remote Access, Policy Development, Approach to Training, Mobile, Cloud, BYOD, Vendor requirements and the list goes on and on. Further, in the planning component of our ISSP, we will layout proposed cost models of the variety of solutions we will be seeking to implement beyond the planning phases as well as contingency and business continuity modeling as part of a comprehensive ISSP. The planning component of the project will also consist of specific strategies and methodologies as they pertain to effective ongoing management and maintenance of the systems that are to be implemented – recommendations for which technologies and services will be best utilized for outsourcing and augmenting core efforts as we as outline comprehensive plans for incident management and communication protocols in the event of an incident.

The Planning document will also include staff and hiring recommendations over the next 2 years as well as recommended contract services and the associated costs that will ride along with the project assessment. Further, our security planning phase and subsequent documentation will follow the model prescribed in NIST SP 800-18 and we will develop models that identify Systems, Categorizations, Owners, Authorizing

Officials, Assignment of Security responsibility, adherence to laws, regulations and policies that impact ACI and its customer base. The Plan document will outline minimum security controls, outline completion and approval dates and detail the ongoing system security plan maintenance objectives.

Section 4: Implementation

ACI expects implementation of the comprehensive ISSP approach and model to be a 24 month exercise and process. We expect that the first 6 months will be spent in the primary planning and building phases of the project. In this time we will look to hire 4 downstream roles to the CISO to help secure the core elements of the plan. During this time, the CISO will also be working directly with these new roles to flesh out the plan and approach and fine tune the Risk Management Framework and building an appropriate RFP for procurement of additional augment services from an outside firm to shore up the integrity of the comprehensive approach. Months 7-18 will be spent physically implementing and deploying the inner workings of the new model and approach. Hiring will continue in this period as we seek to further augment staff to deliver core security services, training models and comprehensive security policy development that closely aligns to the business objectives of ACI. In months 18-22 we will being the process of actively testing and auditing all of the security implements we have installed to date and begin refining our day-to-day active monitoring, audit and penetration testing models to ensure that our implements remain relevant. In months 22-24 of the project timeline we will begin to compile a “close down” report that will outline key learnings, takeaways and areas of improvement for additional future phases of the ACI Cybersecurity approach.

As part of the implementation plan, we will be tracking and maintaining a plan v actual budget tracker index. With the recent round of additional funding just completed by the Board and CEO, we have been granted a 2 year initial budget of $2MM to achieve our goal. These monies are comprehensive spend for team and technologies and we plan to track all expenses accordingly throughout the implementation phases of the project. The CISO has established rapport and dialogue with the CFO and are working in tandem to isolate and prepare appropriate budget tracking measures.

Section 5: Risk Management

For purposes of this project, ACI, its CISO and staff will be preparing a comprehensive Risk Management Framework as a ride along and primary supplement to this plan. This Risk Management Framework will outline and detail all of the following elements that will be taken into consideration as we more the cyber agenda forward for ACI. The list of items covered will be as follows:

- **Risk Identification**
- **Risk Assessment**
- **Analysis & Prioritization**
- **Mitigation Planning, Implementation & Monitoring**
- **Risk Tracking**
- **Classification of Risk**
- **Data Driven Risk**
- **Business Driven Risk**
- **Event Driven Risk**
- **Employee Risk**
- **Vendor Risk**
- **Contractor Risk**
- **Customer Risk**
- **Facility/Physical Risk**

Each of these risk categories will be fleshed out in comprehensive format with specific policies, procedures and actions outlined accordingly. The primary deliverable of this component of the ISSP will be a specific playbook that outlines how ACI approaches and handles each of these identified risk categories and how the organization will respond to each.

Additionally, as part of the actual tactical management component of Risk, we will implement strong audit procedures to ensure we are calculating and calibrating our risk accordingly. As we look at setting up optimal cyber audit principles for the organization, first we must look at the operations models for the entity and look to the things we are trying to protect. From here we'll want to establish a set of vulnerability checklists and perform an inventory check on all of our systems in the business environment, examples of a few might be: Computers, Devices, Storage, Internet Access, Peripherals, Read/Write drives, Data Back-ups, offsite storage, data feeds, cloud solutions; and the list goes on and on. Further, as we explore principles for proper cyber auditing what does the threat landscape look like in a given point in time and how, as a organization, are we attacking the problems of hacking, malware, insider threat, competitive threat, ip and data leakage, continuous and regular patching and data protection technologies like encryption. At the end of the day our principles and subsequent practices must serve to mitigate risk.

Simply put, audit is a function of proper governance and lends to the transparency and accountability of the organization for the benefit of everyone that interacts with and benefits from a relationship with the organization. Information governance in the organization is part of the overall management responsibility mix. The information security audit bridges a number of gaps related to mapping information security approach to actual mission/vision outputs and sheds light on the security posture of the organization as it relates to systems implementation, policy approach, separation and securing of data, regulatory standards, legal implications and communication approach as it pertains to Cybersecurity. These audits will augment our approach to risk and at the same time allow us to better understand the gaps in our environment, post ISSP implementation.

And lastly on implementation, ACI will be looking to implement a hybrid staffing and solution model when all is said and done. In this model the most immediate benefit is reduced cost, flexibility and time and resource appropriate application. As we discussed in the previous model, maintaining a staff of folks for tasks and operations that may only occupy a portion of the time required for the task is not a good use of corporate resources. For example, maintaining a team of 4 penetration testers on staff, fully allocated at a fully loaded hourly rate of $65/hr is an annual overhead of $540,800.00. In all actuality though, a team of penetration testers may only be doing actual penetration testing 25% of the time, resulting in an overhead waste of $405,600.00. Chances are that the $135,200 of one internal resource can be applied to an outsourced and trusted service to execute the penetration testing needs and requirements of the organization. This is the more expedient and cost effective way to manage such needs. The cons of this model are the added risk that has now been factored into the equation. By outsourcing services of any nature related to security, the entity is increasing the attack surface and creating new exposures that simply may not exist in a 100% in-house staffed model.

Section 6: Cost Management

For purposes of effective cost management, ACI will incorporate a formal cost management plan template. The CISO will be ultimately responsible for managing and reporting on the project's cost throughout the duration of the project. However, an ACI Project Manager from the IT department will be assigned primary project management duties to include regular cost management and tracking duties. This Project Manager will report costs and cost overruns directly to the CISO throughout the 2 year process of deploying the ISSP model. The Project Manager will meet with management to present and review the project's cost performance for the preceding month. Performance will be measured using earned value against TCO and pre-established project ROI measures. The Project Manager is responsible for accounting for cost deviations and presenting the CISO with options for getting the project back on budget. The CISO has the authority to make changes to the project to bring it back within budget.

Performance of the project will be measured using Earned Value Management. The following four Earned Value metrics will be used to measure to projects cost performance:

- Schedule Variance (SV)
- Cost Variance (CV)
- Schedule Performance Index (SPI)
- Cost Performance Index (CPI)

If the Schedule Performance Index or Cost Performance Index has a variance of between 0.1 and 0.2 the Project Manager must report the reason for the exception. If the SPI or CPI has a variance of greater than 0.2 the Project Manager must report the reason for the exception and provide management a detailed corrective plan to bring the projects performance back to acceptable levels.

The Control Thresholds for this project is a CPI or SPI of less than 0.8 or greater than 1.2. If the project reaches one of these Control Thresholds a Cost Variance Corrective Action Plan is required. The Project Manager will present the CISO with options for corrective actions within five business days from when the cost variance is first reported. Within three business days from when the CISO selects a corrective action option, the Project Manager will present the CISO with a formal Cost Variance Corrective Action Plan. The Cost Variance Corrective Action Plan will detail the actions necessary to bring the project back within budget and the means by which the effectiveness of the actions in the plan will be measured. Upon acceptance of the Cost

Variance Corrective Action Plan it will become a part of the project plan and the project will be updated to reflect the corrective actions.

ACI maintains the following initiating budget parameters for the ISSP project:

HR & Overhead Costs: $1,200,000
Capital & Equipment Costs: $650,000
Contractor Costs: $150,000
Total Project Cost: $2,000,000
Management Reserve: $200,000

Total Allocated Spend: $2.2MM

Further, as part of the overall cost elements of this plan, the CISO is expected to deliver models that show the following cost/benefit analysis as part of the overall benefit of the ISSP Program. Those include but are not limited to:

- **Provide security infrastructure that reduces development costs**
- **Reduce operational costs**
- **Reducing development costs**
- **Cost of Security**
- **Planned costs (Ongoing Security Operations)**
- **Potential costs**
- **Comparative costs with industry**

And finally, we'll look at ROI from a cost perspective. From a management perspective, it is imperative that ACI begin to weave in cyber risk models and incorporate the outputs of various ROI calculators. Cyber value at risk models consider 3 primary components of an entity. Specifically: Vulnerability, Assets and Attacker Profile. The prevailing assumption being that the number of attacks an entity might experience is likely directly dependent on the perceived value of an entity's assets and the ability for the black hat actor to exploit and monetize those assets for their own benefit. One calculator in particular will be used to ascertain ROI of our ISSP implements as we move through the project – it is known as the FSSCC tool and uses a number of input criteria to help assess risk. This tool combined with the IT Initiative ROI Spreadsheet will help us identify the TCO and ROI elements of this project.

Section 7: Analysis & Recommendation Management

As part of the final components & deliverables, the CISO will also formulate a final Analysis & Recommendation document to ride along with this analysis. The format of this analysis will be the traditional SWOT with a specific comparison to the pre-project SWOT that was compiled by the incoming CISO to assess the pre-project environment in the process of establishing a baseline for improvements. As each component pf technology is layered into the new environment, a comprehensive report outlining the technology advances and environmental impact will be provided to upper management for review. These reports and outcomes will come with associated log files and comprehensive explanation of the technology that has been deployed. These reports will be developed by the line security staff and pushed up through the CISO on a monthly and quarterly basis. Further, as new technologies come online, we will develop comprehensive dashboards to provide deeper insights to the secure/insecure nature of our environment and what the potential attack surface may look like at any given snapshot in time.

From these outputs and reports, we, as a Security & Service bureau within ACI, will make informed recommendations for new technology sets, enhanced operating policies and cost effective outsource solutions that are not core to the ACI mission and objective. We will make these reports and dashboards available to C-Level staff and approved Board Members for further scrutiny and investigation.

Section 8: Student Assessment of ISSP to Cyber Management

Hi professor – I am guessing that this section is an add-in by you as it relates to the ISSP and our topic. If upon grading, I have misunderstood this section, I will be happy to resubmit for full grading consideration.

As for my assessment of the ISSP as it relates to Cyber Management – I think it is one of the most critical elements of a comprehensive Cyber Management Approach. Each entity and organization that is looking to take their cyber posture to the next level needs to have a formal approach and plan as to how they intend to move forward. Much like the Risk Management Framework and so many of the other valuable NIST Documents, the ISSP gives Executive Management a clear understanding of how the organization interprets strategic drivers into specific information security approaches. It is imperative for all entities that are conducting business online in the Cyber realm to be thinking about, discussing and implementing a comprehensive ISSP that examines all of the things we have covered in this particular course. From people dynamics, teaming dynamics, budget considerations, outsourcing vs. in-housing….All of these are significant Management concerns and play a role in the effective management of a cyber posture. The ISSP, when executed effectively and carried out in the spirit it is intended, provides every organization an effective and useful roadmap for securing their most valuable information assets.

References

www.projectmanagementdocs.com

www.sentekglobal.com

http://nvlpubs.nist.gov

http://smallbusiness.chron.com/swot-analysis-recommendations-identified-opportunities-24571.html

portal.hud.gov/hudportal/documents/huddoc?id=DOC_15139.doc

https://www.sans.org/projects/systemsecurity.php

Touhill and Touhill, ***Cybersecurity for Executives***, Wiley, Hoboken, NJ, 2014

Schneier, ***Secrets & Lies***, Wiley, Hoboken, NJ, 2000