REVIEW OF

VISIBLE OPS SECURITY

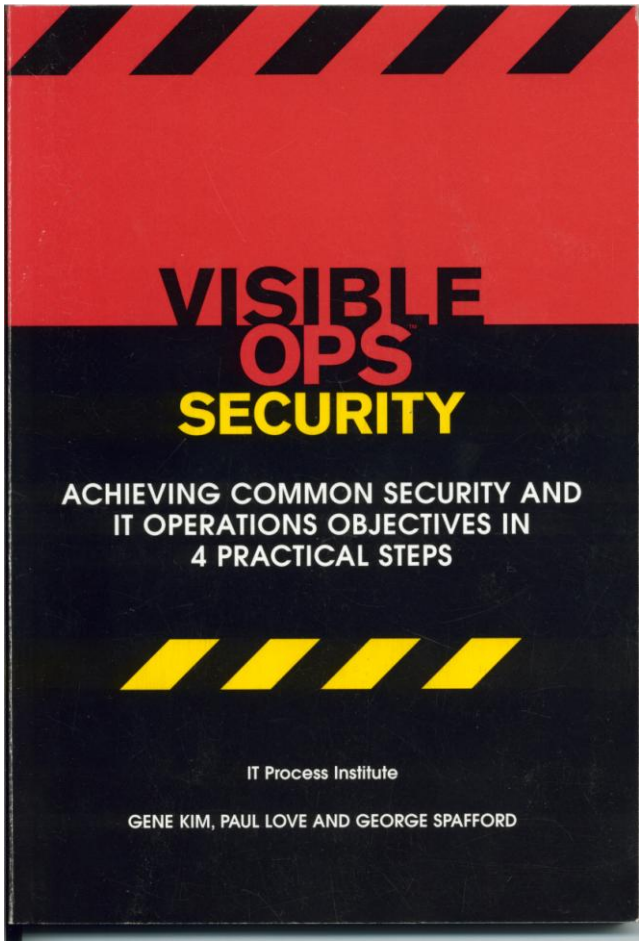
M. E. Kabay, PhD, CISSP-ISSMP

CTO, School of Graduate Studies

Norwich University, Northfield VT

Contents

1. Introduction



In a column for the *Network World Security Strategies*, I wrote about the *Visible Ops Handbook*[1] which I recommend to everyone involved in system and network operations. In this paper, I continue on the same theme by reviewing the newer booklet, *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps*[2] by Gene Kim,[3] Paul Love[4] and George Spafford.[5]

The booklet has only 108 pages and measures 5.5" x 8" – easy to carry around; a PDF version is also available and can be printed in 8.5" x 11" format.

The Introduction discusses the growing concern over security, caused partly by internal perceptions of need and partly by external pressures of government regulation and contractual obligations. The industry consensus is that "the business and IT must integrate sustainable security practices into IT operational and service development processes." Like the *Visible Ops Handbook*, *Visible Ops Security* is "based on the study of the common practices of high-performing IT organizations…. [The ITPI] has studied and benchmarked more than 850 IT organizations to gain deeper insights into what enables high performers to excel."

Two categories of problems confront IT personnel and the authors provide many specific examples of each:

- conflicts between the requirements of normal IT operations or development practices and expectations of security
- interference of security standards and practices with effective and efficient operations.

---

1 http://www.itpi.org/home/visibleops2.php

2 http://www.itpi.org/hZome/visibleopssec.php

3 Gene H. Kim, CISA http://www.tripwire.com/company/management/ is co-founder and Chief Technology officer of Tripwire, Inc. He is also co-founder of the Information Technology Process Institute http://www.itpi.org/home/default.php.

4 Paul Love, MS, CISSP, CISA, CISM, Security+ is a distinguished computer scientists and security expert and author (see for example *Beginning Unix* http://www.amazon.com/Beginning-Unix-Programmer-Paul-Love/dp/0764579940/ref=sr_1_4?ie=UTF8&s=books&qid=1225984912&sr=1-4).

5 George Spaffordmailto:George.Spafford@Pepperweed.com, MBA, CISA, Service Manager http://www.pepperweed.com/ is a principal Consultant with Pepperweed Consulting and is also the author of the popular list "The News" http://www.spaffordconsulting.com/.

Another fundamental problem is that "Although IT supports the business in many different ways, IT has two primary functions:

- Developing new capabilities and functionality to achieve business objectives
- Operating and maintaining existing IT services to safeguard business commitments

The authors write, "*Visible Ops Security* describes how to resolve this core chronic conflict by enabling the business to simultaneously respond more quickly to urgent business needs and provide stable, security and predictable IT services."

The remainder of the Introduction provides an overview of the four phases of the systematic approach to resolving fundamental problems in the operations and security sectors:

1. Stabilize the patient and get plugged into production
2. Find business risks and fix fragile artifacts
3. Implement development and release controls
4. Continual improvement

2. Phase 1: Stabilize the Patient and Get Plugged Into Production

Phase 1 provides a chilling reminder of how badly information assurance implementation can go wrong. A table lists many typical issues (and narrative examples, some of which are hilarious) which security experts encounter all the time in our assessments and audits; examples include (quoting directly)

- Inadequate situational awareness (I came into the information security job full of high hopes, but I started to realize that I was dropped into the desert, with no idea what I was supposed to start walking in. Worse, I didn't know how big the desert was, but I did know that I had no food or water. / I also started to notice that everyone seemed to be avoiding me, often running in the opposite direction when they saw me.)
- Information security ineffective as an afterthought (We couldn't believe they just deployed the application over our objections. I'm literally losing sleep at night because of the potential risk of loss of confidential information. I said, "Look, you can't put private health information out on the public Internet." They just don't seem to understand, and the all say I'm being hysterical, paranoid, and an obstacle.)
- Information security disrupts IT operations and IT operations gets in information security's way (…. And half the time, when we do get the patches in, I almost wish we hadn't. At the end of last year, we did a database patch that broke seven of our top business applications. . . .)

Step 1 of Phase 1 is "Gain Situational Awareness." The authors urge practitioners to know exactly (again, quoting)

- What senior management and the business wants from information security.
- How the business units are organized and operate.
- What the IT process and technology landscapes are.
- What the high-level risk indicators from the past are.

In good, clear English, the authors then expand on each of the four tasks above with some practical examples and excellent suggestions and examples that readers can use in formulating their own responses for their own organizations.

Step 2 of Phase 1 is "Integrate into Change Management." The key tasks (again, well developed and explained in the text) are as follows:

2.1 Get invited to change advisory board (CAB) meetings (i.e., learn what has to be changed in the production environment before it gets changed behind the security team's back – and be cooperative and supportive instead of obstructive)

2.2 Build and electrify the fence (i.e., develop automated measures to detect changes in the production code, processes and infrastructure)

2.3 Ensure tone from the top and define the consequences (i.e., use top management's explicit support to change the corporate culture – and develop a finely-graded scale of consequences for violating security rules)

2.4 Substantiate that the electric fence is working (i.e., audit your own change-control procedures to verify that people are actually following them)

2.5 Look for red flags (i.e., analyze service interruptions and look for evidence that change-control procedures were violated)

2.6 Address failed changes (i.e., perform root-cause analysis on problems)

The chapter continues with equally germane and practical recommendations in the steps called

Step 3: Reduce and Control Access

Step 4: Codify Information Security Incident Handling Procedures and Modify First Response

The authors finish this section with thoughtful analyses of

- The Spectrum of Situational Awareness and Information Security Integration (a good scale for evaluating the degree of maturity of situational awareness and security integration in the organization)
- What We Have Built and What We Are Likely to Hear (a concise summary of the observable changes one should look for as we implement the recommendations of Phase 1).

3. Visible Ops Security Phase 2: Find Business Risks and Fix Fragile Artifacts

The chapter begins with a summary explaining that with infinite risks and finite resources and time, we have to focus our attention on securing critical areas of the business. As with the Phase 1 chapter, this one also includes a succinct and sometimes amusing chart of common issues. Some of the highlights (or lowlights, depending on your perspective) that had me chuckling with recognition include the following (quoting):

- Information security often can't focus its efforts on the top risk areas (We hundreds of business applications that we need to secure and support. . . . There is just no way that our information security team can stay on top of it all. We are spread way too thin. I figure that each one of us is covering hundreds of systems and thousands of controls. . . ."
- Must repeat audit work year after year (We are repeating a lot of documentation and substantiation work for IT controls. . . . Last year we spent thousands of hours on this. And we're going to do it all over again this year. / Why? Because instead of building controls into daily IT operations, we substantiate the presence of controls after the fact. . . .
- Top-down risk-based processes never finish (There's some hope that the new Enterprise Risk Management [ERM] task force will address some of these issues. . . . The problem is that they've been at it for three years, and there are no indications that the consultants they're using are ever going to leave. In fact, the only certain thing is their next invoice, and another one of their horrible half-day workshops. . . .)

The authors explain, "…we extend the focus of Phase 2 beyond just operational risks, to those risks relevant to information security, compliance, and financial reporting. To make sure that we focus on what really matters, we go through an explicit scoping step for IT services and systems to ensure that we can explicitly link information security controls to risks that can affect the achievement of business objectives or requirements."

Their methodology includes the following approaches, each step of which is fully explained in the text (in the unquoted sections, I am merely summarizing highlights):

- "Establish an initial scope of the business process and IT services and systems that really matter by using a top-down, risk-based approach."
- "Cover the periphery" (identify "externally facing systems" whose compromise could cause catastrophic consequences)
- "Zoom out to rule out" (ensure that we are focusing on business issues, not noodling around interesting technical issues regardless of whether they matter in real-world consequences)
- "Find and fix IT control issues" (identify the business functions where controls are inadequate to reduce risk and mitigate damage from breaches of security)
- "Streamline IT controls for regulatory compliance" (build reusable controls that can save time and money for all sectors of the enterprise in meeting security standards)

Their discussion continues with excellent examples drawn from cases involving Sarbanes-Oxley compliance and then turns to principles enunciated by the Institute of Internal Auditors (IIA) Research Foundation called the "Guide to the Assessment of IT General Controls Scope Based on

Risk" or "GAIT."[6] The IIA makes four documents freely available for download about this methodology:

- The Gait Methodology ("GAIT-1")[7]
- GAIT for IT General Control Deficiency Assessment ("GAIT-2")[8]
- Gait for Business and IT Risk ("GAIT-R")[9]
- Case Studies of Using GAIT-R to Scope PCI Compliance[10]

I am grateful to the authors of *Visible Ops Security* for introducing me to the GAIT methodology.

6 http://www.theiia.org/guidance/technology/gait/

7 http://www.theiia.org/guidance/technology/gait/gait-methodology/

8 http://www.theiia.org/guidance/technology/gait/gait2/

9 http://www.theiia.org/guidance/technology/gait/gait-r/

10 http://www.theiia.org/download.cfm?file=24876

4. Visible Ops Security Phase 3: Implement Development and Release Controls

The authors introduce Phase 3 as follows: "…we move upstream to the development and release management processes, as well as to the internal audit and project management processes. We will involve stakeholders from development, project management, and release management so they get involved earlier with projects and we will also work with change management, purchasing, and accounting to maintain accurate situational awareness. We will define the model for engaging with individual project groups when there are information security relevant tasks that we can help with."

As in the other chapters, the authors provide a table of issues and narrative examples that will resonate with anyone who's been in the security field for a while. For example (quoting),

- Information security and audit do not work together (This afternoon, I had a pretty awful meeting with the internal IT auditor. Several things bothered me. First off, he blindsided me with a whole bunch of deficiencies on password controls for some random systems buried in some business processes that shouldn't even warrant being audited. To make matters worse, he even did a penetration test and hit us with findings from that. And then we ended up getting into a heated debate about IT controls instead of talking about the risks we are trying to mitigate. / I guess the thing that bothers me most is that we don't appear to be on the same page with respect to what the top business risks are. . . .)
- Project teams that do not involve information security risk building services contrary to the needs of the organization (For example, let's talk about the last application that the developers put into production. Instead of using the libraries we created to do authentication, they created their own nonstandard libraries, made worse because they haven't been trained on secure programming practices. Now we have to create another piece of complicated middleware to adequately control access. / The unique authentication method now becomes yet another one-off that we need to support. We keep making the mistake of favoring the project goals over the enterprise's goals – over and over again. It has slowly consumed all the air in the room and is killing us.)

The steps and tasks detailed in this chapter are a challenging agenda for anyone in the real world. The prescribed methodology (amply discussed in the text) has the following framework:

Step 1: Integrate with Internal Audit

Task 1: Formalize the relationship with audit

Task 2: Demonstrate value

Step 2: Integrate into Project Management

Task 1: Participate in PMO approval meetings

Task 2: Determine information security relevance

Task 3: Integrate into project review and approval

Task 4: Leverage detective controls in change management

Task 5: Link to detective controls in purchasing and accounting

Step 3: Integrate into the Development Life Cycle

Task 1: Begin a dialog with development

Task 2: Establish requirements definition and secure coding practices

Task 3: Establish secure testing practices

Step 4: Integrate into Release Management

Task 1: Formalize the relationship with release management

Task 2: Ensure standards for secure builds

Task 3: Integrate with release testing protocols

Task 4: Integrate into production acceptance

Task 5: Ensure adherence to release implementation instructions

Task 6: Ensure production matches known and trusted states

I don't think anyone can view this agenda as anything less than daunting, but the case for integrating security thoroughly into audit, project management, development and implementation (release) is so strong that I fully support the authors' views.

Readers interested in seeing my own perspective on these issues might like to look at my MS-PowerPoint lecture slides on operations security and production controls,[11] monitoring and control systems,[12] and application controls.[13,14]

11 http://www.mekabay.com/courses/academic/norwich/is342/lectures/32_Operations_Security.ppt

12 http://www.mekabay.com/courses/academic/norwich/is342/lectures/38_Monitoring_Control.ppt

13 http://www.mekabay.com/courses/academic/norwich/is342/lectures/39_Application_Controls.ppt

14 The same links with ".pdf" instead of ".ppt" will download the lecture handouts instead of the slide files.

5. Visible Ops Security Phase 4: Continual Improvement

Before reviewing Phase 4, here is a little historical digression.

William Edwards Deming was born in 1900 in Sioux City, Iowa; he graduated from University of Wyoming in 1921 as an engineer. By the 1930s, he had become fascinated by the applications of statistical analysis to practical problems and he increasingly focused on improving production processes by identifying and applying metrics.[15] He was invited to Japan in the early 1950s to help rebuild Japanese industry; his philosophy of management, which became known as Total Quality Management (TQM) and which was enunciated in his text *Out of the Crisis*[16] included the following Fourteen Points:[17]

1. Create constancy of purpose for improvement of product and service (Organizations must allocate resources for long-term planning, research, and education, and for the constant improvement of the design of their products and services)
2. Adopt the new philosophy (government regulations representing obstacles must be removed, transformation of companies is needed)
3. Cease dependence on mass inspections (quality must be designed and built into the processes, preventing defects rather than attempting to detect and fix them after they have occurred)
4. End the practice of awarding business on the basis of price tags alone (organizations should establish long-term relationships with [single] suppliers)
5. Improve constantly and forever the system of production and service (management and employees must search continuously for ways to improve quality and productivity)
6. Institute training (training at all levels is a necessity, not optional)
7. Adopt and institute leadership (managers should lead, not supervise)
8. Drive out fear (make employees feel secure enough to express ideas and ask questions)
9. Break down barriers between staff areas (working in teams will solve many problems and will improve quality and productivity)
10. Eliminate slogans, exhortations, and targets for the work force (problems with quality and productivity are caused by the system, not by individuals. Posters and slogans generate frustration and resentment)
11. Eliminate numerical quotas for the work force and numerical goals for people in management (in order to meet quotas, people will produce defective products and reports)
12. Remove barriers that rob people of pride of workmanship (individual performance reviews are a great barrier to pride of achievement)
13. Encourage education and self-improvement for everyone (continuous learning for everyone)

---

15 http://www.amstat.org/about/statisticians/index.cfm?fuseaction=biosinfo&BioID=4

16 http://www.amazon.com/Out-Crisis-W-Edwards-Deming/dp/0262541157/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1226253949&sr=8-1

17 http://www.valuebasedmanagement.net/methods_deming_14_points_management.html

14. Take action to accomplish the transformation (commitment on the part of both [top] management and employees is required).

In *Visible Ops Security*, Kim, Love and Spafford exemplify the principles of TQM as applied to integrating security into all business processes. In Phase 4, they start by recommending the formation of an Information Security Oversight Committee (ISOC) which focuses on "whether information security is meeting the needs of the business." In my own lectures to students at the undergraduate and graduate level, I never fail to emphasize how important it is that security must *serve* the strategic goals of the organization: we don't run the show!

The chapter has a good discussion of security metrics, which the authors define simply as "measures that indicate the success of our interactions with various groups." Their examples include the following (parenthetical explanations are my own):

- Customer satisfaction
- Percent of target operational process integration (how many of the identified processes are now including security considerations)
- Number of challenged integrations (how many processes still have conflicts and problems relating to security)
- Percent of codified process integrations (how many of the processes include formal documentation for the security components)

In addition, say the authors, "There are additional indicators of increasing success that are simple but effective measures of progress:

- Invitations to meetings….
- Soliciting of information security input….
- Reduction in frequency of audits, audit preparation effort, and remediation efforts associated with audit findings…."

The authors then systematically present detailed, concrete suggestions for metrics relating to each of the phases enunciated in the *Visible Ops Security* framework. By the end of the chapter, they sketch out what a mature organization should be seeing once the recommendations are implemented and continuous process improvement has become part of the culture: "We are now more integrated with foundational-level activities within the organization, allowing us to target more advanced activities and processes, such as automating some of the processes we have built. For example, through our involvement with SDLC [System Development Life Cycle] we can create automated components (such as MS Project tasks) to give to project managers that are rebuilt on adaptive self assessments."

Finally, they write, they hope that readers will hear this kind of summary: "Information security is no longer thought of as an outside entity nor does information security have to fight for involvement. We find we are becoming involved in more project and strategic discussions instead of being involved only when problems are discovered. When information security is automatically and without a second thought included in future operations planning, we know we have become part of the team."

Go forth and read this book. Then start implementing its methodology! And may the Authors be with you.