The

SECURITY MANAGER'S PLAYBOOK

A Leader's Guide to Optimizing Cyber Security for Any Business

STEVE HUNT

Table of Contents

About this eBook

You are a newcomer to security management or an experienced pro who wants a different perspective, either way, this eBook is for you.

Together we will explore successfully demonstrating the health and effectiveness of your company's security and risk management program. We've included examples of documents and lots of suggestions for preparing your own security program document. When you are done, you will have all of the essential information to show executives, large customers or auditors about your company's security program.

The first few chapters of the book lay out the conceptual elements of efficient and effective security. The next few give specific examples of documentation and decisions for better security. The final chapters list the projects and processes essentially to continual improvement.

While this eBook is directed at cyber security professionals, it is equally useful to physical and corporate security directors.

Contact us for document templates, sample policies and other guidance. info@huntbi.com

The Security Alchemist

Sometimes doing security in a business environment feels otherworldly. On one hand, we security professionals have to be technology experts, conforming to the laws of physics and the limits of computer memory and CPU cycles. On the other hand, we are social workers to the business managers who cry when security gets in their way. We hold their hands and explain in our best bedside manner that bad things might happen and we have to help the business to thrive in the midst of risks.

It was Rhonda MacLean, the former global chief information security officer at Bank of America, who first told me the now famous aphorism of security.

“Why do we have brakes on a car?” she asked.

“To stop?” I tentatively offered, suspecting I was walking into a trap.

“To stop?!” she exclaimed, confirming my suspicion. "If our intention were to stop, we simply wouldn't go in the first place."

"No," she continued, "we have brakes on a car so we can drive fast."

I was stunned. The heavens opened. Trumpets sounded. Suddenly everything made sense.

Security is the brakes on the car. It is also the seatbelts and mirrors and other safety equipment. However, my epiphany that day was that none of these devices is in place in order to give me caution, nor to avoid risks, nor to slow me down. Just the opposite. Security exists to allow me to drive fast, even recklessly, zigging and zagging through the racecourse with confidence that my vehicle will perform any way I need it to.

Security exists not to avoid risks, but to thrive in the midst of risks

I tell the epiphany often. I told it recently to officers in the ministry of defense in Oman. I told it previously to oil & gas executives in Rio, and even during a Formula One race in Italy. Around the world, this message rings loud and true.

One person responded in broken English, "You just put the medicine on the cut."

That reaction is common because most people have viscerally negative feelings about security. An annoying layer of cost and inconvenience, they'll say. You yourself, dear reader, have probably been guilty of talking about avoiding risks and getting that blank look from business leaders, haven’t you? The enlightened security professional and the enlightened business executive both realize that actually security is the thing that allows business to grow and to be agile and to--get this--take risks.

Those Buddhas of business therefore do a surprising thing. They purge the word security from their vocabulary. They talk once again about growing the business, out-maneuvering the competition, and racing ahead. In order to win a race, they correctly surmise, they need to put the systems and measures in place to nimbly zoom through traffic.

Every business manager should have the quiet confidence of a Formula One driver, knowing that this awesome screaming machine can do absolutely anything asked of it. Risks, then, become opportunities. Risks become assets. Risks let us thrive and win.

The Four As of Security

The security officer of a European-based financial services company told me that his greatest challenge in building an efficient security infrastructure was knowing where to start. It was apparent to him that launching any single project seemed to have prerequisites. For example, he recently completed the deployment of intrusion detection sensors then discovered how ill equipped his team was to monitor and process all of the event logs, and to determine good behavior from bad. He listed all of the projects which – started beforehand – would have made his intrusion detection deployment more successful. His first wish was that he had better understanding of the authorized users and systems connected to the network. Next, he discovered that having properly configured firewalls and routers would have eliminated a lot of the noise. Finally, he wanted policies as guidelines for differentiating anomalous behavior from normal, and for instructing escalation procedures.

"We simply didn't have our ducks in a row," he said.

CURE THE DISEASE, NOT THE SYMPTOM

So why did a mature company with a global network across several continents not achieve the efficiency and effectiveness it desired? The security officer explained, "The popular wisdom of security architecture design tells us to find out what's happening, then stop the bad things. But that assumes we know a bad thing when we find it – if we find it at all."

According to dozens of conversations during client consulting engagements, I see a disturbing trend: companies apply security fixes simply for the sake of doing so. It is as if the CIO says "We need security, so let's pick a project and do it," without determining if it is the right security measure at the right time.

In the course of counseling hundreds of companies over many years, I have discovered that there is a proper order to security projects. The main point to understand about order is that it naturally breeds efficiency and effectiveness. Therefore, security without order will generally tend toward inefficiency or chaos. This is the leading reason that most companies spend too much money on the wrong security projects.

Optimal Security Follows a Natural Pattern

The proper order of security projects flows from the natural way that the main categories of security rely on and build from one another. The four categories are:

•Authentication, answering the first basic question, "Who are you, who are we"

•Authorization, answering the next question, "What shall we do?"

•Administration, "How do I manage it?"

•Audit, "What happened, or "Is it working?"

To most people, security is an annoying layer of cost and inconvenience – a necessary evil. However, by looking at the course of social history, we see that security is a natural part of every society; it is so natural, in fact, that when done properly, it is hardly an inconvenience at all.

People, organizations, governments, and societies do not want security, they want the benefits of security. That is why throughout history, people have organized themselves and taken steps to secure themselves very naturally. Groups of people adopt security in a repeated, predictable pattern. That pattern is as true today as it was centuries ago – understanding that pattern helps us to understand our point in history, understand society, understand our customer, and understand what the next big technical trend will be.

WE ARE NOT THEM

When people group themselves for social benefit or for their own protection, they first identify themselves. They create a criterion by which they may distinguish "us" from "others." Us from Them. Those people thus create an answer to the first question, "who are you?"

The first authentication measures are simple techniques for remembering who is in and who is out. Early societies gave unique names to members of a clan or region. Later, groups distributed secret handshakes and passwords. Today passwords and tokens are used in similar ways.

WE DO THIS, NOT THAT

The obvious next step is to set boundaries of behavior and property, since the group of "us" are agreeing to act a certain way, or treat ourselves a certain way, and live in a certain geography. We create boundaries (fences, walls, moats, gates, and doors) to allow the community of "us" to live undisturbed from those who would disrupt our life. This answers the second question, "What may you do?"

Buildings today are protected by fences, gates and other barriers, and by guards with guns. In network design, authorization questions like this are answered by firewalls, access control lists,

encryption, and antivirus software. In physical, IT and homeland security the effective use of authorization controls depends on similar authentication capabilities.

THESE ARE OUR LAWS

When we define ourselves, or add new members, we naturally set up systems to administer changes. We may make laws or policies to govern ourselves and to regulate the definition and limits of exposure to others. All of this answers the third question, how do we manage it?

In other words, I have a lot of "you" doing a lot of actions, so I need some way to manage it all. Sometimes an organization will deploy provisioning or user administration in order to improve efficiency of managing authentication or authorization. Sometimes companies find that simply writing policies and standards is the place to start.

The worst policies are the ones dreamed up by a security steering committee as operational ideals: "Here's what we wish people would do." The best policies are those that evolve out of known business requirements, and are enforceable with current states of authentication and authorization technologies and processes. "Of the things we are able to do, these are the ones offering the greatest value to the business."

However, such governing principles are pointless without some degree of confidence that people or systems are who they say they are, and that controls are in place to enforce the policies. Administration is the obvious next step after answering the first questions.

To catch up quickly with the best-run organizations use a jumpstart "accelerator" that gives the basic customizable templates that fill gaps. Imagine having a security program in-a-box. That's the idea behind the Baldrige framework for Excellence. Baldrige is the national standard behind Six Sigma and other quality improvement initiatives. For security managers if can be fairly straightforward. Assess your Security Success Score to identify gaps --> Walk through the Accelerator to fill process gaps-->Modify templates to speed the process --> Continuous Independent Monitoring to ensure process discipline is maintained --> Reassessment, Recognition, and Award improvement and high levels of maturity. To learn more about these concepts, https://www.managehubaccelerator.com/hunt-security/

HOW IS IT WORKING?

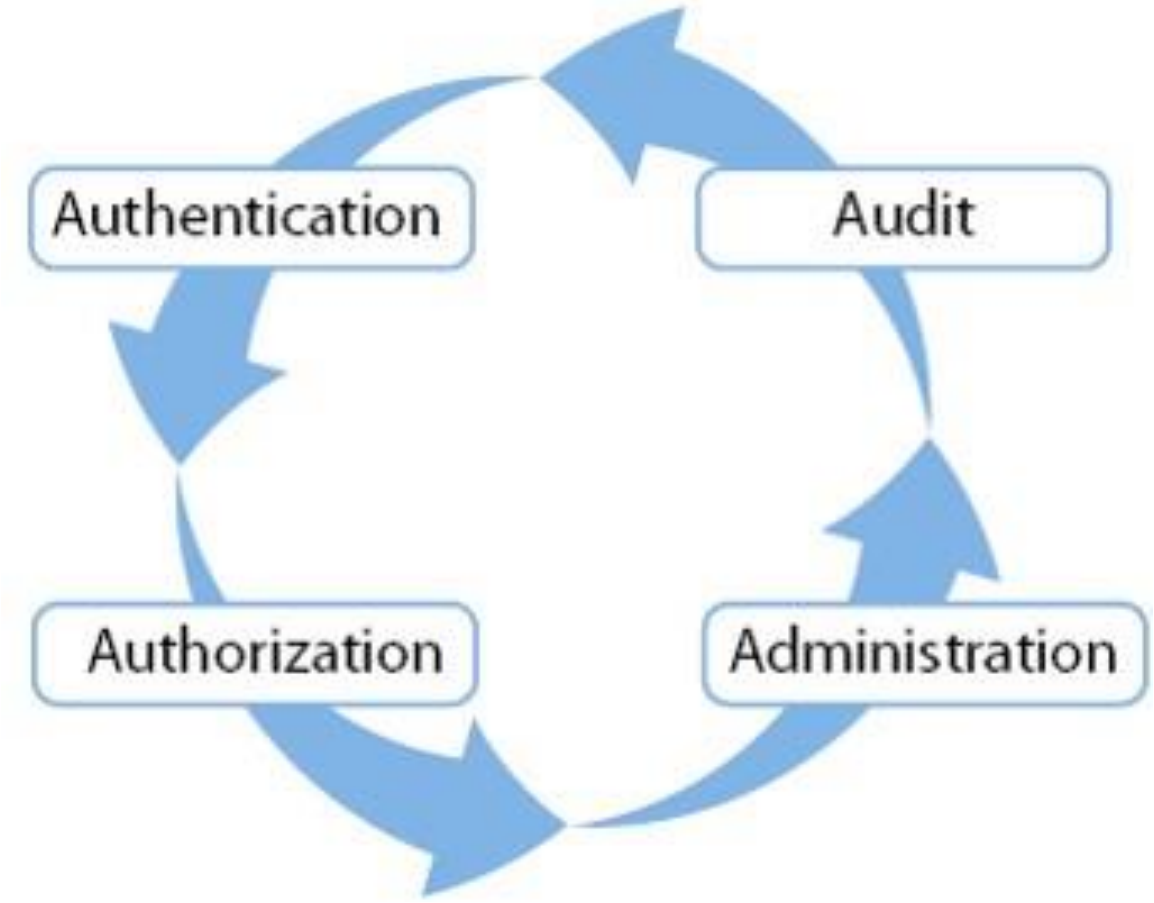
With people and contexts defined, protective controls in place, and policies outlined, the obvious fourth question is "What happened? Or What is happening?" We must know the answer to that question in order to understand whether our people really are who they say they are, they are doing what they ought to be doing, and that our laws and policies are working for the benefit of the group.

Monitoring, surveillance, vulnerability testing, are all methods of seeing how everything is working. One may use these audit technologies and techniques to find weaknesses throughout the security architecture. For example, by monitoring for failed password attempts, one may discover

abuses of authentication credentials. Or, along the same lines, by testing the quality of passwords in light of the policy, you may see that it is time to improve confidence that people are who they claim to be.

It is the same with all vulnerability assessments, monitoring and surveillance tools and projects. They all strive to answer the final fourth natural question as a way of inspiring improvements.

START OVER AND IMPROVE



Once we've answered what happened and what is happening, we have a fairly clear idea how to improve the systems. We start over, improving or refining the contexts for identifying ourselves and others. We go from simply treating all of "us" as the same and all of the others as outsiders, to understanding that even among ourselves there are differences, and among outsiders there are levels of "other-ness." We improve identification and authentication with levels of passwords or secret handshakes.

That causes us to refine and modify the authorization or perimeter controls, allowing outsiders to come in for trade or limited interactions, or alliances. Those actions of course cause us to revisit our policies and systems of administration – now much more complex than before.

Then we audit how well—how efficiently and effectively —our entire system works, make necessary changes in the same order we began, and then do it again - Over and over. Proper security

naturally improves through the repeating process. Who are you? What may you do? How do I manage it? And What happened? These four questions drive the regular, natural, and predictable pattern of natural security adoption.

Security Optimized

Let's take all this philosophical thinking about security and apply it now to your business. Security, as you have already figured out, is not a bunch of technology that you bolt on to a business, like screwing a deadbolt on a door. Security is an emotion, an attitude, a culture first and foremost. So we start inside, with a concept called Governance. The first step in optimizing a security program is to create a document that accurate reflects where you are and where you are going. Without it, you will never know if security is making any progress or impact.

GOVERNANCE

What do we mean by Governance, why is it important, and how does it fit into the security program?

You may have heard the word governance – for example in the expression GRC, which stands for Governance, Risk and Compliance – and may even be able to use it in a sentence. However, most people, even security professionals, misunderstand it.

Governance, according to Merriam-Webster's dictionary means

> *noun* | governance | \'gə-vər-nən(t)s\
>
> : the way that a city, company, etc., is controlled by the people who run it

Or, the way it may be plainly used in the context of a security program is simply this:

Say where you are going, who is going to take you there, and how you will know when you've arrived.

Governance of a security program has five essential parts:

- Objective: State the overall purpose of the program
- Organization & Reporting: By what group this program is authorized, at what level in the firm
- Roles and Responsibilities: Who is actively involved, who are the stakeholders, and who is the executive sponsor
- Policy and Guidance: The policies, regulations, or internal mandates driving the program
- Ongoing Monitoring: Describe how "success" of this program will be measured and monitored

Governance is like Management Best Practices

For the last sixty years, the greatest business minds have been exploring, theorizing and fine-tuning a body of knowledge collectively known as "best management practices." You may be familiar with best-practices through the work of thought leaders like W. Edwards Deming and Joseph Juran. You may have read classic management books like "The Goal," "Good to Great" and "E-Myth." You may have even attempted best-practice approaches like U.S. Baldrige Performance Excellence Program, EFQM (The European Foundation for Quality Management), TQM (Total Quality Management), Kaizen, Six-Sigma, ISO (International Standards Organization), or CMMI (Capabilities Maturity Model Integration).

The more you learn about best management practices the more you realize that they share common themes and requirements. Their most fundamental shared requirement is that you create your company's management framework--what we are calling Governance. A management framework automates your company's management processes in the same way accounting software automates bookkeeping, or a CRM automates customer relations. With consistent use, your management framework helps your company become very organized, efficient, and continually improving. Your employees can become empowered, self-motivated, and self-managed. Your company's culture can become more innovative, focused, and collaborative.

In his best-selling book, "Good-to-Great," Jim Collins refers to the concept of a management framework as a "consistent system." The U.S. Baldrige Performance Excellence Program, and EFQM call it a "leadership framework." Other quality management approaches like ISO, Six Sigma, and CMMI fill in the gaps. They emphasize key concepts like process standardization, employee engagement, and continual improvement. They may emphasize different aspects of quality-management, but they all require an overarching, automated management framework.

At Hunt Business Intelligence the automated management framework we recommend is called ManageHub. With ManageHub, a security or IT leader can easily assess his or her Security Success Score daily, in real-time, and correct or improve inefficiencies instantly.

Information security governance provides a framework for establishing and maintaining an information security program that will evolve with the organization it supports. The following list is a summary of good information security governance practices that are critical for ensuring the security of enterprise information assets:

- Information security activities should be governed based on relevant requirements, including laws, regulations, and organizational policies.
- Senior managers should be actively involved in establishing information security governance framework and the act of governing the agency's implementation of information security.
- Information security responsibilities must be assigned and carried out by appropriately trained individuals.
- Individuals responsible for information security within the agency should be held accountable for their actions or lack of actions.
- Information security priorities should be communicated to stakeholders of all levels within an organization to ensure a successful implementation of an information security program.
- Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.
- Information security organization structure should be appropriate for the organization it supports and should evolve with the organization, if the organizati on undergoes change.

- Information security managers should continuously monitor the performance of the security program/effort for which they are responsible, using available tools and information.
- Information discovered through monitoring should be used as an input into management decisions about priorities and funding allocation to effect the improvement of security posture and the overall performance of the organization.

Now, get out your pen and paper. It's time to create your own Security Playbook.

Setting Direction

Imagine getting in the car to go to the office supply store to buy printer toner. Sounds simple. But no sooner have you started the engine and fastened your seatbelt are you faced with a choice: which office supply store should I go to? Staples is closest and has a reliable selection, but the street it's on is under construction. Office Depot is across town, but will take less time on the highway. Choosing direction in this case means thinking about your priorities. Creating a security program is the same.

The priorities to think about may be bad things that the firm is afraid of, or customers crying for you to protect their information better, or some regulation holding its hammer over your head. Consider those priorities and build your security program to address them. This governance statement will set the tone and direction for everything else you do.

If anyone asks why you are bothering with "this security nonsense," you can answer with a mission statement, or some other type description of the Objective. Perhaps you like this one:

"Our Company operates in a challenging environment, putting the Firm's information and brand at risk. The Firm's corporate governance requires an Information Security program that includes careful consideration of security threats, operational quality, and regulatory compliance."

There are many ways to state an objective. I'm particularly fond of mission statements. Consider the culture in your firm. Does senior management prefer a mission statement, or a value statement? Do they like Objectives or Goals? Use the language that your top executives use. For now, I'll use the expression mission statement.

MISSION STATEMENT

A mission statement keeps your eye on the ball. It serves several purposes:

- It is a useful tool for marketing the security program to the rest of the company
- It shows an auditor or customer that your priorities are in order
- And it reminds you what kind of program you are building

Example, "All of the Firm's colleagues and contractors - who create and handle our company's critical information and services - are responsible for executing these missions, especially while interacting with the clients."

If you want to keep it super short and sweet, write something along these lines:

"In order to ensure the Company brand will remain synonymous with customer confidence and industry leadership, the firm will institute a program of continuous improvement and risk management."

Here is a slightly geekier mission statement I wrote for one client.

- Protect the confidentiality of the Firm's information.
- Preserve the integrity of the Firm's critical information

- Ensure the availability of the Firm's systems and information
- Enable colleagues to work from anywhere at any time responsibly
- Encourage protection of sensitive information in spoken or casual form

A friend of mine, and very talented Chief Information Security Officer, wrote this one:

Create Value for the Business

- Enable the business to do everything it needs to do, quickly and responsibly
- Engage the business directly through the risk management program

Respond with Agility

- Embrace change and growth with flexible programs and operations
- Build a security program and framework that allows flexibility and growth

Focus on Solutions

- Create products and services for growing customer trust and enabling our enterprise
- Build infrastructure solutions that provide great functionality in a secure manner

Promote Excellence

- Lead a "best practices culture" centered on quality, customer satisfaction and excellence
- Adopt relevant external standards and build into our DNA

Learn Continuously

- Employees actively participate in protecting and improving the business
- Security is an innovator with relevant knowledge
- Build strong training and development program
- Attend continuing education conferences
- Develop thought leadership

Mission Statements set direction for the security program. Now steal one of ours or write one of your own. The main questions you need to answer in the mission statement are

- What does the security program aim to do?
- How does it aim to do it?

Ok, the Mission Statement is done. Next up, who's in charge?

Organization & Reporting

Now draft a section of your Playbook called Organization and Reporting. This section will clarify which group authorized the creation of a security program, at what level in the firm.

Example, "The security program is managed day-to-day by the security risk management team, consisting of

- The Director of Information Security (or CISO if you have one)
- The Director of Technical Operations (or head of networking, or systems, or whatever you call it in your firm)
- Business unit leaders (Use this simple expression, or be more specific, naming roles such as head of sales, head of manufacturing, heading of HR, head of legal, etc.)
- And is sponsored by the CIO (or CFO, or CEO – or whomever is screaming the loudest to start the program)"

You might like this better.

"Many departments must collaborate in order to create a culture of responsibility and accountability."

Areas of Security	Responsible Departments
Security regarding people and their work activities	HR, Legal, IT, DevOps
Security regarding customers	Marketing, IT, DevOps, General Counsel
Security regarding compliance to laws, standards, and regulations	Legal, IT, Marketing
Security regarding public messaging & disclosures	Marketing, General Counsel
Security regarding disasters and incident response	HR, Legal, Real Estate, IT, Support
Security regarding application development	Application Development
Security regarding computers, servers, networking and devices	IT, DevOps

Now let's get more specific in the roles and responsibilities section.

ROLES AND RESPONSIBILITIES

Who is actively involved, who are the stakeholders, and who is the executive sponsor?

Create a section of your Playbook that accurately reflects responsibility for different parts of security and risk. Be sure to understand that the security director does not own the risk of the company. He or she may be responsible for managing it, but if a torpedo hits the ship, ultimately, it's the captain of the ship, the CEO, who takes the blame. This document should therefore be an accurate representation of roles and responsibilities, so there is no misunderstanding. Here are some examples.

CTO (or whomever is the top dog governing the security program for the company)

- Provides oversight and approvals
- Authorizes cross-functional project teams
- Appoints business leaders as risk management committee members (The Risk Committee).

CISO (or whatever title you use for the head of security)

- Reports to CTO
- Responsible for
    - Security Strategy
    - Policy and Process
    - Security, Risk Management and Compliance Operations
    - Works closely with CTO, CIO and the Risk Committee to create and execute a firm-wide security and risk management program following accepted standards
    - Hires security personnel and manages a budget
    - Leads activities in the following domains:
    - Governance, Risk Management and Compliance
    - Security Planning, Policies and Processes
    - Security Operations

CIO (or VP Technical Operations, or whatever you call the head of IT)

- Reports to CTO
- Responsible for
    - Secure IT Infrastructure Strategy
    - Secure Network & Systems Implementation and Maintenance
    - Secure IT Operations

    - CIO and CISO coordinate technological and procedural activities.

VP Product (Application) Development

- Reports to CTO
- Responsible for
    - Application development
    - Application security
    - Secure software development lifecycle
    - Customer requirements
    - Ensures that all applications are developed securely
    - Works closely with VP InfoSec, VP Infrastructure, and Risk Committee to meet the firm's risk tolerance

The Risk Committee (if you have one)

- Meets periodically to discuss changes in the firm, its customer needs, or its products, and security or risk ramifications of each
- Determines the acceptable level of risk tolerance for the firm

Policy and Guidance

Now let's look at the policies, regulations, or internal mandates driving the program.

It's time to write a statement about who or what is making security a priority. Here we are not talking about the person who is screaming the loudest (CEO, CIO, etc.). We mean the fire under that person's rear end. Again, this is for future reference, when the security program is under attack, or your job is in question, this should remind everyone why it is so important. Here is an example.

"The firm operates in an environment of constant risk:

- Handling confidential information of clients, some of which is governed by laws and regulations
- Operating in the realm of shared networks and the Internet, which are by nature risky
- Subject to US State breach notification laws and Federal Trade Commission actions governing the legality of business activities and the handling of personally identifiable information

Therefore, the firm seeks to operate with a measured acceptable level of risk."

Ongoing Monitoring

Now we say what "good" looks like. How do we know we are successful? What measurement can we point to later to describe success? Here are some samples.

"The CISO will follow accepted standards in the monitoring of security controls and key performance indicators (KPIs), and will produce periodic reports for the CTO and Risk Committee."

"The CTO conducts an internal audit periodically, perhaps by engaging an outside firm."

"The Risk Committee periodically reviews risk assessments and guides decisions on security controls and projects."

CONFORMANCE TO STANDARDS

If you are ready to think about standards and regulations, then feel free to add a statement about conforming to standards. If you aren't 100% confident, skip it. Example:

The Information Security Program measures the Firm's conformance to

- Specific Customer requirements for trusted third parties
- The Cloud Security Alliance best practices for Cloud Security
- The Health Insurance Portability and Accountability Act (HIPAA)
- International Standards Organization (ISO) 27001
- And the National Institute of Standards and Technology (NIST) Special Publication 800-14 Generally Accepted System Security Principles

Or, more simply

"The security program orients the firm's people, processes and technology to follow common IT security practices, as outlined in NIST 800-14."

Rounding out the Security Program Documentation

Here are the Information Security Policies and Procedures that will be most often requested by auditors and large customers. Prepare each of these documents and keep them in your security program playbook. Like we've said before, contact us if you want templates or examples or assistance fleshing out the rest of these pieces.

- Hiring policies and practices and employment application
- User account administration policy and procedures for all supported platforms where data is processed, including network/LAN access
- Supporting documentation to indicate periodic reviews of user privileges
- Employee non-disclosure agreement or Code of Ethics, or Code of Conduct. This document or set of documents should be something distributed to every employee and signed to indicate that they have read and understood it. Auditors really need to know that employees have been informed of proper behavior
- Information Security Incident Report policy and procedures, including all contract information
- Copy of Visitor Policy and procedures
- Security Log Review Policies and Procedures
- Copy of third party risk management policies and procedures
- Privacy policies (internal, external, web)
- Executive Summary of certificates held. (e.g., PCI, HIPAA, ISO)

WHAT'S NEXT?

You've crossed the chasm. Congratulations. You are on the way to building and maintaining an efficient, effective security program playbook.

When you are ready for more, Hunt Business Intelligence is standing by ready to help you assess, create, improve and optimize your security program in these areas:

Risk Management

Threat & Vulnerability Management

Incident Response

Network Security

- Network configuration diagrams for internal and external networks. (Note: Sanitized versions of the network diagram are always acceptable)

- System and network configuration standards
- System backup policy and procedures
- Offsite storage policy and procedures

Change Management

- Application security policy
- Change control policy/procedures
- Problem management policy/procedures

Secure Application Development

- Software development and lifecycle (SDLC) process document

Physical Security policy and procedures

- Building and/or restricted access)

Business Continuity

- Business continuity plan (BCP) and / or Disaster recovery plan
- Most recent BCP/DR test dates and results

Vendor Risk Management

- Legal clauses and confidentiality templates for third parties

Security Awareness

- Topics covered in the security training program

Becoming a better security director

- Everything you need to know about
    - Security strategy
    - Security staffing, budgeting
    - Security outsourcing
    - Selecting technology products

The Framework for Day-to-Day Operational Excellence

Following is a framework of specific tasks and continuing activities of the Information Security Program organized in four sections and modified from NIST 800 (www.nist.gov)

The first, Governance, Risk and Compliance details the processes and techniques to align all of the company's security efforts with current business objectives. We've already gone over most of these.

Next, Security Planning, lays out the security program office and day-to-day-management of security.

Finally, General Attributes of Security, describes standards and goals for protecting the information and assets of the Firm.

1. Governance, Risk, and Compliance

Formulate Security's Mission, Values, and Organization

- Draft Mission and Values statements
- Assign Leadership and delegation of risk and compliance responsibilities
- Assign a Risk or Security Committee
- Appoint Chief Security Officer (permanent or interim)
- Empowered by executives and Board of Directors to affect change
- Recommends success factors in management performance reviews
- Meets requirements of CISOs by *Company* guidelines (see below)
- Assign departmental liaisons
- Assign roles and responsibilities
- Determine with business leaders the reasonable and responsible level of risk to be achieved
- CISO work closely with Executives and Departments to ascertain
- Use Legal department's language of impact and likelihood as found in the Risk Register
- Calculate a risk goal for the Firm where the responsible level of risk is less than or equal to impact of a breach multiplied by its likelihood $R \leq I \times L$

Determine a reasonable and responsible level of cyber insurance

- CISO work with Legal to ascertain
- Insure against damages
- Insure against notification costs

Identify regulations and laws related to the business

- Assess compliance
- Manage compliance

Perform risk management

- CISO institute processes for continual improvement
- Track and manage vulnerabilities
- Identify & research emerging threats relevant to the Firm
- Enter into risk register and incident management program
- Maintain a risk register
- Remediate high risks urgently

- Remediate other risks
- Update the risk register continually
- Involve a risk committee for oversight
- Perform periodic risk assessments
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Risk Mitigation
- Evaluation and Assessment

2. Security Planning

Awareness and Training

- Awareness and Training Policy
- Components: Awareness, Training, Education, and Certification
- Designing, Developing, and Implementing an Awareness and Training Program
- Managing Change
- Program Success Indicators

Capital Planning and Investment Control

- Integrating Information Security into Business Process
- Capital Planning and Investment Control Roles and Responsibilities

Performance Measures

- Metrics for Measuring Success and Performance
- Metrics Development and Implementation Approach
- Metrics Development Process
- Metrics Program Implementation

Strategic Planning

- Major Applications, General Support Systems, and Minor Applications
- Security Planning Roles and Responsibilities
- Rules of Behavior
- System Security Plan Approval
- Security Control Selection
- Completion and Approval Dates
- Ongoing System Security Plan Maintenance

Information Technology Contingency Planning

- Develop Contingency Planning Policy Statement
- Conduct Business Impact Analysis
- Identify Preventive Controls
- Develop Recovery Strategies
- Develop IT Contingency Plan
- Plan Testing, Training, and Exercises
- Plan Maintenance

Security Services and Products Acquisition

- Information Security Services Life Cycle
- Selecting Information Security Services
- Selecting Information Security Products
- Organizational Conflict of Interest

Incident Response

- Preparation
- Preparing for Incident Response
- Preparing to Collect Incident Data
- Preventing Incidents
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity
- Response and disclosure
- Design standards and processes for responding to serious incidents and major information breaches.
- Identify a single individual or role who will serve as the Firm's spokesperson when a breach occurs. A quick and professional disclosure may mitigate many lawsuits.

Configuration Management

- Configuration Management in the System Development Life Cycle
- Configuration Management Roles and Responsibilities
- Configuration Management Process

3. General Attributes of Security

Information Confidentiality

- Draft a statement describing goal and mission related to confidentiality. How does confidentiality apply to this particular application?
- Address topics such as Access, Encryption, Terms & Conditions

Information Integrity

- Draft a mission statement related to Integrity for workplace, systems and information
- Address topics such as Access, Data modification, Storage

System and Workplace Availability

- Draft a mission statement related to system and information availability. How often is it acceptable for the system to be down (inoperable)?
- Address topics such as Failover, Backup, Recovery

Resources

The security program for any enterprise shouldprotect people, information and assets, but most ofall it should protect quality of life and work experience. Our approach at HUNT is holistic. We do not artificially segregate aspects of security such asnetwork security, building security, data security,personnel safety, operational risk management,business continuity and privacy. We advocateapplying security principles to create value for any organization.

SECURITY FROM THE GROUND UP

Hunt is standing by to provide you with a best practicesapproach to creating an efficient and effective security program. We will detail the processes,procedures and planning needed to achieve yoursecurity and operational goals. Hunt will assistyou by ferreting out risks and gaps in youroperation from a security point of view and makerecommendations as to how to close those gapsand mitigate the risks.

- Are you unclear about where your major weaknesses are?
- Do you collaborate with customers who feel the need to protect their data?
- Do you have a sense you are spending a lot of money on security, but are unsure if you are getting the value you expect?
- Knowing your security infrastructure hasn't been evaluated in years, do you fear there are emerging requirements or threats you've likely missed?

A QUICKSTART ACCELERATOR IS AVAILABLE

Earlier, we mentioned ManageHub as a useful tool for coordinating process improvement for your entire security program. The easiest way to start with it is to join the ManageHub Accelerator. You will learn the four steps to Security Maturity and receive you own Security Success Score. You also receive all the basic customizable templates needed to fill operational gaps.

Revisit your Security Success Score frequently—like checking your Credit score—and watch your security operations improve.

The Security Success Score™ is also a useful metric to show your superiors, so they have independent industry-stander verification that you are doing a great job.

https://www.managehubaccelerator.com/hunt-security/

BENEFITS OF WORKING WITH HUNT

Hunt will help you create value, preserve your corporate culture, and ensure that technical architecture, maintenance, and staff meet industry standards and best practices in network, data and physical security. Your security program will be influenced by our "Synthesi s of Best Practices" research, applying standards and emerging legislation frameworks such as COBIT, ISO, HIPAA and others when suitable.

Hunt offices and partners operate in North America, South America, Europe, Middle East and Asia.

After all, it's not your job to secure the network. It's your job to secure the business.

About the Author

Steve Hunt is an executive strategist with expertise in information security, physical security, confidential information protection, critical infrastructure protection, technology, risk management and regulatory compliance. He was inducted into the ISSA Hall of Fame for his achievements in information security and, CSO [Chief Security Officer] Magazine presented him with the "Industry Visionary" Compass Award.

For over 20 years Steve has been helping organizations to create value from security and technology investments. His clients are diverse, in industries such as banking, health care, oil & gas, software, and retail. With each client, Steve helps to create a strategic vision, then maps out its execution including business justification, technical architecture, governance, risk management, compliance, technology selection, and training. His favorite projects are those business-critical initiatives that touch both employee behavior and the IT infrastructure.

From 1998 to 2005 he was Vice President and Director of Security and Risk Management at the think-tank Forrester Research where he served as adviser to business leaders globally. Previously Steve served as technical director, traveling the world helping large companies understand how to build efficient and effective security architecture. Earlier, Steve worked as a consultant to Chicago's financial community.

His clients have included the United Nations, JPMorgan Chase, Lockheed Martin, Bank of Montreal, Allstate Insurance, AXA Group, Société Générale, Dexia, Pfizer, British Petroleum, Exxon Mobil, Microsoft and IBM.

Steve is a regular keynote speaker at business and security conferences around the world. He also appeared as a homeland security analyst on CNBC, Fox News, CNN, and other news programs. His analysis has appeared in the Financial Times, Wall Street Journal, The New York Times, Business Week, and other global publications and trade magazines.

Steve attended Elizabethtown College and was a graduate fellow at University of Chicago. He is an adjunct professor at DePaul University, and is certified CPP and CISSP. Steve's diverse background lends a fresh perspective on security.

HUNT
BUSINESS
INTELLIGENCE