PRACTICAL CONSIDERATIONS FOR INFORMATION SECURITY MANAGEMENT

Andrew Scharlott

The Big Picture: The Role of Information Security

The primary role of an Information Security function is to support and enable the business.

Information Security is about risk management in the support of business functions. It is not a means to itself, but rather a mechanism to enable management and executive leadership to properly evaluate business options and make risk-based decisions, ultimately leading to a better environment for the business to function. This often includes the implementation of policies and technical components designed to reduce risk to the operating environment and protect critical assets and information.

Given this principle, the primary function of the Information Security Manager and/or Chief Information Security Officer (CISO) is that of communication. This role should be filled by an individual who can work and communicate clearly with senior management as well as “in the trenches” staff across all business units. They should be able to effectively articulate and explain the risks and rewards of various business options. They should be able to take overall management direction and appetite for risk tolerance and convert that to actionable direction to lower level security staff. Additionally, this individual should be able to inform executive decision makers about what security staff are observing in their day to day work, to help improve decision making and resource allocation.

Overall Approach

While numbered in the list below, this isn’t necessarily iterative and is not a one-time action. Instead, this should be considered a list of functional areas that should be reviewed and developed, ideally on a regular and recurring basis.

Important note: none of the ideas outlined in this document should be considered to be a one-time function. An Information Security Manager should be constantly evaluating the state of information security in the organization (including the performance of the team, technologies deployed, management priorities, etc.) in order to determine areas of improvement and changes needed. The adversary is constantly adapting and improving; a security function must as well.

In general, I see the following areas of focus for an information security manager:

1. Security Policy
    a. Need appropriate policies to enable information security function

2. Security Personnel and Team Management
    a. The right team is critical to execute management direction
3. Develop Relationships
    a. Security needs to work well with other IT and business teams to accomplish its directive
4. Functional Priorities
    a. What are the most critical functions the security team should focus on
    b. Evaluate existing security functionality (gap analysis, driven by Functional Priorities)
5. Tools and Technology
    a. Choose the appropriate tools/technology that address the risks
6. Continuous Monitoring, Reporting, and Metrics
    a. Appropriate metrics and reporting are critical to drive informed decisions and to continually improve the information security function
7. Incident Handling and Incident Response (When Needed)

Security Policy

It's important that the overall approach of security policy development (as well as related documents such as plans, procedures, guides, etc.) be focused on risk management. After all, the role of security is to better enable the business functions by appropriately managing risk.

A good security policy needs to be in place to enable the information security function. This should start with an overall governance/organizational approach that empowers the security organization to perform its duties along with outlining responsibilities and scope of the security function. In addition to an overall security policy, additional technical/issue-specific policies will likely be needed in various areas including (but not limited to) items like vulnerability management, access control, and acceptable use.

It's important that all policies, including (and in particular) the overall governance policy, should have executive support. Additionally, policies should be specific enough that they can be enforceable but also take care to ensure that they're workable within the business.

Security Personnel and Team Management

Information security often involves bringing together many disparate pieces of information from numerous heterogeneous sources and trying to make sense of the collected data. Individuals with backgrounds that have exposed them to various areas of information technology and other computer-related tasks often excel in this arena. The focus should be on getting the right people into the right positions on the team. Team fit and personality are just as important as technical ability.

Items of importance to consider:

- The ability to think “outside the box”
- “Jack of all trades”
    - Ability to think beyond one single focus area / can see the “big picture”
- Baseline of ability/skills
    - Other experience in IT can be very helpful
        - System administrators
        - Network engineers
        - Compliance / risk-management
        - Developers
    - Ensure that they have the capability/desire to move beyond that specific skillset
- Demonstrated ability and desire to learn
    - Continuing education and self-driven learning
- Important to consider the individual’s temperament, background, and experience with the specific job function they would fill
- Be careful of limiting job functions only to specific people
    - Cross-training and job rotation are important to ensure backup capability
- Focus on overall ability rather than specific tool knowledge
    - New tools/skills can be taught/learned, but ways of thinking are harder to change/develop
- Manage the team effectively by ensuring they have what they need to do their job
    - Appropriate tools/resources
    - Clear direction and expectations
    - Metrics are useful in determining appropriate workloads and functional distribution/focus

Develop Relationships

Information Security does not exist in a vacuum. While it may ultimately fall on the security team to address and manage, every single person in the company has a role to play. It’s clear then that the security team needs to work very closely with other business and IT units to ensure the overall security posture of the organization. When appropriately implemented, separation of duties and applied least privilege principles often mean the security team can’t always take the action needed, or view the information needed, across every component in the business.

Developing relationships with these other units also allows the security team to be more aware of the overall business environment, including keeping abreast of new initiatives as well as new technologies that can introduce risk. Additionally, having the right working relationships ahead of time enables better cooperation and communication in the event of an incident.

While no other business unit should be ignored, a few of the most critical relationships may include the teams listed here:

- Networking
- Help desk
- Desktop support
- System administrators
- Database administrators
- Backup / Disaster Recovery (DR) / Business Continuity Planning (BCP) Teams
- Compliance / Risk Management / Audit support
- Development teams
- Change Management
- Legal / Human Resources

Functional Priorities

There is an exceptionally long list of functions that might be managed by an information security team. To operate effectively, it is necessary that the information security manager prioritize functional areas. These decisions are not made in isolation, but rather require careful consideration of a number of variables, including (but not limited to) some of the following:

- Organizational risk tolerance
- Budget constraints
- Customer requirements / Business unit requirements
- Security technology
- Security team skillset (personnel)
- Other teams within the organization / internal politics

In general, I believe that the major security-related functions can be broadly grouped into the following categories, keeping in mind that many security technologies may address components of multiple categories and that not all of these functions may be purely security-based in nature (or even managed by the information security team).

Although my thinking is constantly evolving in this space, I generally consider the below functional areas (in rough order of relative importance) to be the most critical components of an effective information security program outside of Incident Response.

Before getting to the list - I have one quick note on the concept of Information Security versus Information Management. For the most part, the function of an Information Security team is just that - protecting ("securing") information, and while technical approaches to that end can vary, the goal is still basically the same. For me, Information Management is a subset of an Information Security function that is focused on the technical or policy directives around the identification and management of information repositories or transfers. Ultimately, protecting a company's critical information (e.g. intellectual property, customer data, etc.) is of the utmost important and should be the focus of information security. However, in practice protecting that information doesn't necessarily mean the specific deployment of Information Management tools like Digital Rights Management (DRM) or Data

Loss Prevention (DLP) products. While those absolutely have their place in a thorough Information Security program, the protection of information can also be (at least partly) accomplished through the appropriate deployment and usage of the other functional areas listed below, especially including things like asset management, configuration management, privilege management, and access controls.

- Network and Asset Management
    - What's actually on the network (and what's authorized versus unknown)
    - Inventory management
    - Network/data flow rules
- Identification/Authentication and Access Control
    - How is IA managed and is it sufficiently secure (multi-factor?)
    - Is access control appropriately implemented and monitored
    - Privileged account considerations (limited deployment, centralized management, monitoring usage, etc.)
- Vulnerability, Patch, and Configuration Management
    - Keeping hosts up to date and in secure configurations
    - Validate settings/patches via scanning or alternative checks
    - Especially critical for public or customer facing functions
- Information Management
    - Identify, manage and monitor access to sensitive information stores
- Malware Prevention and Detection
    - Traditional Security Operations functions (anti-malware, IDS/IPS, etc.)
    - Detection of compromise (and not just attempts at prevention) is critical as well
- Event Logging and Incident Management
    - Log records of what happened
    - Often needed for Incident Response and Investigations

Tools and Technology

It's important to take note of the current security posture of an organization before proposing or implementing any kind of change. Change simply for its own sake isn't a valuable exercise. An evaluation of the current state of the information security function is a necessary first step to determine what changes need to be made.

In particular, when deciding what tools/technologies to pursue, some items to think about include:

- What are the weak links in your network/business and how do I protect against them?
    - This often includes users – so consider website access, email, BYOD policies, lost/stolen equipment (full disk encryption?), etc.
- Where is my most critical information and how do I monitor and protect it?
    - Information is what's truly important, not usually physical items

- What is the actual threat I'm protecting against?
    - Do I know? Can Threat Intelligence help?
- What can an attacker see and get to?
    - Publicly exposed functions
    - Customer exposed functions
- Don't forget about easy wins ("low hanging fruit")
    - Sometimes using existing technology to do the easy things can generate a large benefit (patching is a good example)

When evaluating specific tools and approaches some other concerns come to mind:

- Priorities and allocation of resources/budget
    - Cost/benefit analysis
- Beware of shelfware and underutilized technology
    - Even if a tool is used, you might be able to get a lot more out of it rather than purchasing something new
    - Too many tools can be just as bad as too few tools
        - Need to have enough focus/resources to properly manage entire suite of security tools
- Business justification for every decision
    - This relates back to risk management/tolerance – if it doesn't help support the business and reduce risk it's not a good choice
- Be mindful of the signal/noise ratio
    - Filtering out good information from useless noise is critical
- Beware of letting compliance drive security
    - Except possibly for specific contractual or regulatory requirements, a well thought-out information security program should naturally lead to compliance
    - This can be especially critical and effort-saving for multi-national companies and those with multiple regulatory/compliance requirements (e.g. SOX, PCI, HIPAA, SSAE-18, GDPR, etc.)
- Defense in depth
    - How does this tool/technology help address coverage issues
- Prevention versus Detection
    - You can't only focus on prevention and assume it will work
    - Assume you're compromised and act accordingly (malware hunting, data exfiltration detection, etc.)
- Commercial versus Open-Source Tools
    - There are numerous very good open-source tools that can be very effective at lower cost

Continuous Monitoring, Reporting, and Metrics

While the term “Continuous” may be somewhat nebulous when it comes to security management - in effect it really means a regular (even if not real-time) oversight and tracking of information security controls. In other words, it can be thought of as the routine operation of information security systems with special attention paid to the frequency of monitoring and reporting. Depending on the specific details, this can vary from near real-time functions (malware alerts, SIEM incident alerts, etc.) to annual functions (policy reviews/updates). Other timeframes (such as weekly reporting, monthly status reviews, etc.) are common and perfectly reasonable as well.

Once the right tools and technologies are deployed and operational and being adequately maintained and monitored, it's critically important to know what’s working and what’s not working. This means deriving useful metrics from them. After all, if you can’t measure something you can’t really improve it.

A few useful metrics to track and report might include items such as the following:

- Anti-malware coverage and status
- Anti-malware events
- Website accesses (and blocked content)
- Vulnerability scan findings (tracked over time)
- False Positive rates / False Negative rates (if possible to determine)
- Patch status
- Administrative actions
- Capacity/Resource availability
- Critical security alerts
- E-Mail Information (spam, malware found, etc.)

Ideally you would like to see improvement over time (e.g. open vulnerabilities decreasing, patch levels increasing, anti-malware coverage approaching 100%, etc.) in components where that makes sense. If that’s not being demonstrated a determination as to the reasons should be researched.

Incident Handling and Incident Response

To start, it’s important to note the difference between “Incident Handling” (IH) and “Incident Response” (IR). Generally, IR refers to the technical actions surrounding the incident and can includes activities like: log collection and analysis, malware hunting, packet analysis, etc. IH generally refers to the overall management of an incident and might include activities like: communications management, working with law enforcement, regulatory reporting, resource coordination, etc. While these may be handled by the same person or group, in a large incident or complex organization it’s often to the benefit of all involved that these be considered separately but equally important functions.

Basic Incident Response steps include:

1. Preparation
    a. Incident Response Policy and Plan
    b. Communication
        i. Contacts (including outside groups like law enforcement and contract resources)
        ii. Escalation procedures
2. Monitoring/Detection/Identification
    a. Tools/technology
    b. Frequencies
    c. Reporting
3. Containment/Neutralization
    a. Scope of infection/problem (ensure all infections are accounted for)
    b. Business Impact
4. Eradication
    a. Maybe - might be a legal or law enforcement decision
5. Recovery
    a. Regulatory compliance/reporting
    b. Backup/Restoration
6. Lessons Learned
    a. Updated policies/plans as needed

It's critically important for an organization to take care of the "Preparation" items (and test their response plan) before an incident occurs. During a breach or incident response is not the right time to determine something is missing or the right people aren't known.

One other item listed here deserves a special note. I've listed "Maybe" as a note in the *Eradication* step. In some (possibly rare) cases it may not be wise to immediately remove an infection or malicious actor/agent from your network. Prior to doing so it's important that the organization is convinced that they have determined with a high degree of certainty that all compromised locations have been identified. Additionally, in some cases (often at the request of law enforcement or legal advice), leaving a malicious actor in the network without alerting them to your knowledge can serve to increase the collected evidence for prosecution or improve the likelihood of accurate attribution.

Disclaimer / Notes

Although this work is my own, the contents have been heavily influenced by industry standards and published content (see References below). I don't claim that this approach is unique or revolutionary, but it is my attempt to outline my thoughts in how to manage an effective information security program. All content reflects my personal views and not those of my employer (United States Department of the Interior).

This particular document should be considered to be an extremely high-level overview and not anywhere near a complete discussion of the issues presented.

References

Center for Internet Security (CIS) - Critical Security Controls
https://www.cisecurity.org/controls/

Department of Homeland Security (DHS) - Continuous Diagnostics and Mitigation (CDM) Program
https://www.dhs.gov/cdm

ISACA "The Risk IT Framework"
https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity"
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1 "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-55 Revision 1 "Performance Measurement Guide for Information Security"
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 “Computer Security Incident Handling Guide”
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-137 “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

Open Web Application Security Project (OWASP) “Top 10 - 2017 The Ten Most Critical Web Application Security Risks” (Release Candidate)
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Software Engineering Institute “Governing for Enterprise Security (GES) Implementation Guide”
https://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf

SysAdmin, Audit, Network and Security (SANS) Institute - Incident Response Process
https://digital-forensics.sans.org/blog/2010/09/27/digital-forensics-security-incident-cycle/

Most Recent Revision: May 28, 2017