

Appendix B PERSONAL QUALIFICATIONS

When interviewing candidates for an Information Security Manager (or information security executive) position, it is important to consider the personality characteristics most relevant to the job. This appendix provides both a ranked list of these characteristics as well as the reasons why these characteristics are important. The most important factors appear at the top of the list. The author suggests that you photocopy this appendix and distribute it to all those who will interview candidates (including a third-party recruiter working on the assignment). These people can then rank the candidates according to these criteria to quickly determine which candidates should proceed to the next step in the recruitment process.

Alternatively you may wish to use the following list as a starting point for an in-house brainstorming session amongst those managers who will need to work with the new Information Security Manager. The session can then be used to develop your organization's own unique list of personal qualifications.

The following list assumes that the job candidate has the necessary technical skills to do the job, as demonstrated through both certifications (see [Appendix D](#)) and prior experience.

Excellent Communication Skills

More than anything else, an Information Security Manager must act as a liaison between many different groups with different world views, different objectives, and different needs. The Manager must be able to attentively listen, just as he or she must be able to clearly state what needs to be done. This Manager must also be able to persuade management to adopt new and possibly unpopular courses of action. The Manager will be required to write top management status report memos, risk analysis reports, security incident post-mortem analyses, vendor request for proposal documents, employee job performance evaluations, and many other documents. This Manager may also be called upon to act as an organizational spokesperson with the news media and professional society standards setting committees. The Manager may additionally be called upon to give presentations at industry and technical conferences. This Manager must therefore have excellent interpersonal skills, including writing and public speaking skills. While an increasing number of organizations are using a bachelor's degree as a quick-and-dirty indicator of

communications skills, organizations recruiting a Manager should go one step further, and look for specific evidence of excellent communication skills such as papers written, conference speeches delivered, industry standards committees served, etc.

Good Relationship Management Skills

In order to get anything done, an Information Security Manager is going to need to work with and through a lot of people. If the Manager is strictly a work-alone technical type, he or she is going to have a lot of trouble in a position as Information Security Manager. The Information Security Manager in most organizations does not have the power that goes along with a top management spot, where he or she could simply order others to follow policies, standards, and other information security requirements. Instead, acting in a staff advisory role, the Information Security Manager must convince and persuade others to follow these same requirements. In this same regard, many people talk about the Manager's role as a salesperson, selling information security. Some people think it's even more difficult, something akin to converting other people to a new religion. Whatever metaphor you prefer, it's clear that an Information Security Manager must have superior people skills, must know how to maintain good working relationships with a wide variety of people, and must be able to maintain the trust and support of these same people.

Ability To Manage Many Important Projects Simultaneously

The Information Security Manager must be an excellent project manager and must be familiar with modern project management tools and techniques. Many information security projects are complex, have a long time horizon, and depend on the participation of a wide variety of people. The successful Manager must be able to delegate work to, and later manage people outside an information security group (these people will typically include consultants and contractors). In an increasing majority of cases, the pressing information security projects that most organizations need to complete simply cannot be accomplished with the limited information security staff on hand. At the same time, the Manager must stay on top of these projects, paying attention to details, and making sure that progress proceeds as top management intended. The successful

Manager must also be able to put together organization-wide status reports that clearly show trends, problems, and areas in need of top management intervention. Separately, the Information Security Manager often has a dotted-line reporting relationship with a variety of staff that have information security related jobs (Systems Developers, Systems Administrators, etc.). The Manager is thus indirectly responsible for obtaining results, but often not in a position where he or she can force compliance with information security requirements. To get results in this environment, the Manager must be both a diplomat and a politician. An Information Security Manager must thus be a team player, a team builder, and a team leader.

Ability To Resolve Conflicts Between Security And Business Objectives

The Information Security Manager must be able to clearly see the pros and cons of certain courses of action, and be able to choose and negotiate a compromise which best serves the organization in the long run. Information security is always a compromise because the only absolutely secure information system is an unusable one. The successful Manager must have a flexible personality, and be comfortable making compromises. He or she must also know about the management tools that can be used to arrive at decisions of this nature (net present value, internal rate of return, payback, Monte Carlo simulation, automated testing tools, etc.). In addition to being familiar with information security technology, the successful Manager must also have business skills, business knowledge, and a business aptitude. The Manager must be able to withstand pressure from various groups with competing objectives, and be willing to take a stand for a course of action that is in the long-run best interests of the organization. The Manager should not be overly concerned about being popular and well-liked; a Manager concerned about popularity will soon be fired for getting nothing done. The Manager must appreciate that, in an organization of significant size, information security takes years of dedicated work before it really starts to become part of the corporate culture.

Ability To See The Big Picture

The Information Security Manager must not be easily distracted by the fire-fighting that inevitably comes with the job. Taking care of virus problems is certainly important, but this day-to-day work must not crowd out important but not urgent long-run projects such as compiling a network security architecture. The Manager must be able to prioritize resources in a way that satisfies

the organization's urgently pressing needs, but at the same time move the organization in the direction of implementing generally accepted information security solutions. The Manager must also be able to synthesize information from many different sources to come up with a plan for improving information security that is truly responsive to the organization's business needs. A Manager with a narrow technical focus will impede information security progress, because it is only through a broad view of information security that innovative solutions can be conceived. Furthermore, the Manager must be able to read between the lines, identifying the true underlying causes of problems that the organization faces. The Manager must additionally have the guts to tell the truth about these underlying causes.

Basic Familiarity With Information Security Technology

The Information Security Manager must be knowledgeable in information security technical areas such as encryption, smart cards, and system access control. Not only must the Manager not be duped by technical specialists, he or she must know the best technology to apply in response to an organization's information security needs. Without this knowledge the Manager will lose credibility, and thereby jeopardize current and future information security initiatives. Generally a Manager will not have the luxury of learning a great deal about information security technology on the job, so organizations should not hire an inexperienced person and expect that they will be able to pick-up the technology as they go along. Familiarity with the technology does not mean that an Information Security Manager is expected to personally get involved in highly-technical work, for example program a digital certificate user authentication system, but it does mean that the Manager would know when such a technology should be used. In general, a successful Information Security Manager must be familiar with the methods used, the processes employed, and the business reasons cited to justify information security measures. The successful Manager should also be familiar with the successful ways to enforce information security requirements with what is often an uncooperative end-user population.

Real World Hands-On Experience

A successful Information Security Manager is not going to use your organization as the proving ground for untested theories or ideas. This Manager needs to be immediately credible -- your organization can't afford to take the risks that are involved in developing credibility

over time. He or she must have relevant prior experience in the real world of information security, and ideally this would be both as an external consultant and also as an internal Information Security Manager. This will give the Manager a taste for what it's like to work in the information security field, and will allow the Manager to bring that prior experience to bear on the problems your organization is facing. Hands-on experience not only helps prevent the Manager from making stupid mistakes or taking positions which are clearly inconsistent with standard industry practices, it also most importantly buys the Information Security Manager a lot of additional credibility. This credibility will be very important when selling information security to various constituencies such as top management and internal technical staff. One additional benefit to having an Information Security Manager with prior hands-on experience is that he or she knows what they are getting into when they take a job, and will therefore be less likely to quit after several months because the job didn't turn out to be what the Manager hoped it would be.

Commitment To Staying On Top Of The Technology

The Information Security Manager must furthermore keep abreast of recent developments in the information security field. Attending a conference or two each year will generally not constitute sufficient effort. The Manager must read technical magazines, subscribe to online news services, and if he or she is located near a major city, attend an occasional professional society meeting as well. A familiarity with the latest developments is essential if the Manager is going to be able to recommend appropriate responses to recently discovered vulnerabilities. A familiarity with the latest developments is also essential if the Manager is going to be grounded in the information security related standard of due care (this will be an essential reference point for discussions about adjustments to information security controls). If the Manager doesn't possess this current knowledge, and if the Manager hasn't applied this knowledge, the organization runs a high risk that it will learn about its vulnerabilities only when it's victimized. If the Manager doesn't possess and apply this knowledge, it's likely the organization will be using information security solutions that are unnecessarily costly, burdensome, and/or antiquated. If the Manager doesn't possess this knowledge, he or she is not going to effectively present proposals for change to top management. The risk of having a Manager who is not in touch

with the latest developments is greater in large organizations where such an individual may be able to hide because others do the technical work; in a small organization it is unthinkable that the Information Security Manager would not also be able to do extensive hands-on work such as install and fine-tune a firewall.

Honesty And High-Integrity Character

The Information Security Manager needs to have a squeaky-clean criminal record as well as an open-minded and questioning personality which inspires trust. Some scrupulous organizations go further with additional background checking, for example requiring the Information Security Manager to have a clean credit report. All this makes sense because the Information Security Manager must be a paragon of virtue and honesty, in addition to being an exemplary employee. Above all, this individual must not be a former hacker because this will often cause others within the organization to be untrusting and uncooperative. In the eyes of many, being a hacker is equivalent to being a malicious and irresponsible person who is out to get them. While hackers are often on top of the latest information security vulnerabilities, they frequently lack extensive experience in the business world, and they frequently lack the diplomacy and people skills necessary to do a good job as an Information Security Manager. There are available people with exemplary characters, who are also on top of the latest developments in the information security field, but you may need to pay them well. Just as a well-managed organization would generally not hire an office employee who had previous convictions for violent behavior, so an organization should not hire a "former" hacker who has run afoul of the law. Even if the candidate for an Information Security Manager position has no criminal convictions, any candidate who boasts about being a former hacker should be avoided like the plague. If a newly-hired Information Security Manager were to send confidential internal information to his or her friends in the hacker community, the hiring organization could soon find itself overrun by unwelcome visitors who are using its networks and systems for illegal activities. If you are still intent on hiring a former hacker, think long and hard about the reputation risk that goes along with such a move. Is your firm really prepared for the negative publicity and the loss of customer confidence that goes along with hiring someone who has demonstrated that they have a different set of ethics than most of the others who work at the organization?

Familiarity With Information Security Management

The Information Security Manager must know about the elements of an information security organizational infrastructure. These elements includes responsibilities, policies, standards, procedures, and the like (a list of these is provided in "Current Documents"). The Manager must also be familiar with, and know how to use generally accepted information security management tools such as risk analysis software and contingency planning software. This Manager must additionally be aware of other information systems management tools that can be used to enhance information security; one commonly deployed example is a network management system. If the Manager is not familiar with information security management tools and approaches, he or she will not be able to marshal the limited information security resources to the organization's best advantage. This in turn will lead to problems like unnecessary costs and delays in developing new systems. For example, the Manager may then suggest a manual solution when an automated solution is current available and more cost-effective.

Tolerance For Ambiguity And Uncertainty

Information security is very complex and full of interdependencies. In many instances, a viable solution to various information security problems has not yet been released as a commercial product. This means that the Information Security Manager must be able to make do with the tools and techniques currently at his or her disposal. The Manager must also be able to make defensible decisions when important or even critical pieces of information are unavailable or too costly to obtain. The Manager must have a strong will and a tenacious personality which does not let these problems cause him or her to become overly cynical. At the same time, the Manager must not live in a fantasy land where he or she does not see the realistic and serious nature of the information security issues facing the organization. A patient, relatively-optimistic, well-reasoned, and level-headed Manager who can adjust to a wide variety of situations will do best in this position.

Demonstrated Good Judgment

An Information Security Manager will be called upon to make many judgments which conceivably could have a profound impact on the future of your organization. For example, if the Manager makes a bad call on an architecture decision, your organization could be widely discussed on the front page of the newspapers. This

could cause the organization's reputation to suffer in a very big way. On another note, if the Manager is a former hacker, this background is not convincing evidence of good judgment. It is one thing to know about system penetration tools and techniques, and it is a very different thing to actually use this information to break into a system without the involved organization's formal written consent. A successful Information Security Manager should have a good track record of decision-making in a variety of situations, including those where both management pressure and a quick response were important factors.

Ability To Work Independently

The Information Security Manager must be able to work independently without direct supervision or encouragement. In many cases, top management will not know exactly what he or she is doing. At the same time the Manager must be accountable to top management and the Audit Committee on the Board of Directors. The Manager must be able to stay focused and get things done, even though the resources at his or her disposal are quite limited. The Manager must also be accustomed to taking the lead and not waiting for users or other groups to tell him or her what to do. A deep and abiding commitment to improve the information security status of the organization must carry the Information Security Manager through the inevitable contentious and difficult situations that he or she will encounter. To work independently, the Manager must be creative, proactive, and inspired by a vision of how things could be.

A Certain Amount Of Polish

Although this may at first sound like an unnecessary characteristic of an Information Security Manager, it can be very important when it comes to dealings with both top management and representatives from external organizations. Just as we judge a book by its cover, the Information Security Manager will be judged adversely if he or she does not pay attention to personal grooming, does not take care to dress professionally, and/or does not conduct him- or herself in a professional manner. The Information Security Manager is an important spokesperson who will be a role model and focal point for many people. This person needs to inspire respect and admiration. If the Information Security Manager is disorganized, unfocused, slovenly, and poorly spoken, then people will discount what he or she says, and the projects that he or she promotes will fall on deaf ears. To even mention this point may seem to be an unwarranted

emphasis on external appearance and behavior, but this is the way that the world works, and organizations that ignore it do so at their own peril.



