10 Tips for the Information Security Officer

Helping you get the most out of what you put into protecting information
The “10 Tips for the Information Security Officer” has been developed and distributed for educational and non-commercial purposes only. Copies and reproductions of this content, in whole or in part, may only be distributed, reproduced or transmitted for educational and non-commercial purposes.

For more information visit: http://www.ocit.saccounty.net/InformationSecurity/default.htm
10 Tips for the
Information Security Officer

About seven years ago, I began to study and test precisely what security management practices work best—what techniques and practices distinguish the best from the mediocre and from those that are horrible.

*10 Tips for the Information Security Officer* resulted from years of research and direct experience with dozens of highly successful (and not-so-successful) habits.

After helping many professionals, including myself, and seeing that even more would greatly benefit from better instruction, my mind was made up… A special report had to come.

My idea was a practical and easy to read report. Down to earth advice on how to improve your performance. One thing I am confident about: with these tips you have the power to make a difference.

Yours for better security more often,

*Jim*
Your Time is Important. How Should You Spend It?

That was my first question when I was appointed the OCIT Information Security Officer in September 2006: “How should I spend my time?”

After some thought I came up with this:

My focus as the OCIT Information Security Officer:
1. Articulate the overall strategy
2. Help my security committee get things done
3. Invest in staff and myself to help with the most important things:
   • Strategizing,
   • Innovating,
   • And marketing information security.

My Approach:
Use a series of 100-day plans as a way of getting things done fast. (http://www.ccisda.org/docs/index.cfm?DocumentScreen=detail&cl=198&ccs=228)

This allows for immediate focus while achieving longer term objectives.

My Challenges:
• Full participation of members of the security committee
• Obtaining executive sponsorship
• Workload balancing

And I have to tell you that the CCISDA Information Security Forum (ISF) has been a part of my career and program development. It keeps me informed, motivated, and connected with others.

Do you want to take your profession to the next level? Yes?

Then I encourage you to be involved with workgroups, associations, and opportunities outside your direct work unit.

Your time is important. How should YOU spend it? Think about it.

Before the next email.
Before the dog barks.
My Favorite Question: “How Do You Know?”

Are you making progress with your project? Are you doing what’s best for your customer? Your career?

How do you know?

Are we making progress with our information security program?

There are many questions like this, but only one answer: “Find out how to better serve your customer.”

I suggest using a proven set of questions designed to get you actionable feedback. Not only find out how you are doing from their perspective, but also find out exactly what you need to do to improve.

Try this.

Use the questions at http://www.baldrige.nist.gov/Progress.htm.

Modify them. Ask questions related to your work. I did this. I asked questions about our security program. It was one of the best things I did in the last couple years.

See how I used this: click this link and then view the booklet titled, “Evaluate your Information Security Program.”

http://www.ocit.saccounty.net/InformationSecurity/default.htm

Find out what the right things are for you to work on... and why.

We used that survey and the ISO 17799 security audit tool to develop our information security plan for the year. Again, one of the best things we've done in years.

www.sans.org/score/checklists/ISO_17799_checklist.pdf

How about you? Any tools or techniques you've used to build and sustain your program? Or your career? I’d be interested…

Yours for better security more often,

Jim
What Exactly DOES “Done” Look Like?

Just what does “DONE” look like?
This is an essential planning question… not just for security, but for every project.

Consider the following:

The goal of County information security is that all information held by the County would be protected from unauthorized use.

So…

What should be in place if we really did protect our information from unauthorized use and provided the highest quality service?

Is just installing new technology or new services or new capabilities enough?

Example: soon we will have the capability to encrypt emails. We have installed a vendor product that can now be used. Are we done?

I’d suggest we get closer to our information security goal IF we think of ‘done’ as the following:

- Technical specs defined
- Contract in place
- A policy for use adopted
- User education available
- Compliance and audit process in place
- Trained IT support staff
- Processes to manage service
- Approval by top management
- Endorsement by IT Governance
- Communication to users

Many of our projects are scoped to focus on the technology aspects only. How is the rest covered?

Don’t stop till the project is really ‘done.’ That way we really do provide the highest quality service.

Yours for better security more often,

Jim
The Most Contentious Issue...

Trend:
According to Gartner, it’s become a chess game.  
IT and the Business at the table, but not sure who makes the next move.

For example,
1. How do we modernize the infrastructure and reduce costs? Who manages the risk to determine what to do?  
2. How do we increase business accountability for security and risk? Can IT force this, or does the business need to lead?  
3. Who takes the lead to resolve turf issues that are obstacles for an enterprise architecture?  
4. How much involvement do you want from the business in the IT project portfolio?

Next step: Identify your most contentious issue. Who owns it – IT or the business? Can you link your project to business growth and the IT strategic plan? What can you do to get it moving?

Sacramento County has several security related initiatives that really need attention.

Our approach is to include these in the countywide IT strategic plan which in turn is driven by the business.

To see what we’re doing, click here:
Sacramento County 2008 IT Plan

Or cut and paste this into your browser

Yours for better security more often,

Jim

P.S. Feel free to send me your questions or comments. By the way, I’m also the project coordinator for creating and updating our county’s IT Plan. Let me know if you are interested.
Communicating Your Case: Do You Make These Mistakes?

On January 22, 2008 over 50 security professionals from 30 counties in California met for the 9th semi-annual CCISDA Information Security Forum. The agenda started off with:

How do I better communicate my business case?

Here’s the collective wisdom. It applies not just to communicating the business case for security, but also whenever you are talking with, or writing to, your management or customers.

<table>
<thead>
<tr>
<th>Mistake</th>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act as if you own the data, the application, the business, or the customer served.</td>
<td>Business owns the data. They must make the decisions.</td>
</tr>
<tr>
<td>Use your industry jargon and terminology, acronyms, and vocabulary.</td>
<td>Use terms and concepts the customer or boss is familiar with.</td>
</tr>
<tr>
<td>Drill into too many details you find interesting because you want to describe how it works.</td>
<td>Focus on ‘what’, not ‘how’. Describe what is improved or accomplished.</td>
</tr>
<tr>
<td>Try to give the big picture and all the pieces at once.</td>
<td>Try big picture concepts with bite sized chunks of overall milestones or objectives.</td>
</tr>
</tbody>
</table>

**Bonus:** some suggested that the most important question to ask yourself when trying to present a case, advance your project, or persuade decision makers is, “where can we win?” Be realistic about how much you can get done or get agreement with at one time.

Yours for better security more often,

Jim
What’s holding us back?

Before we can accurately answer this question, we need to ask ourselves: "Back from what?" If you're not sure about this, then nothing in particular is holding you back. That's because you're not heading anywhere in particular.

Success manuals recommend taking inventory of your strengths. That's generally a useless exercise until you know what the inventory is for. The difference between an inventory and clutter is having a specific purpose.

Once we establish a preliminary goal, we're in a position to ask meaningful questions about our plan of action. We can apply and test preliminary answers.

My goal as the OCIT Information Security Officer is that security be viewed as essential to our business growth and success.

I was part of a countywide information privacy and security roundtable on March 30. Twenty four managers and executives from departments around the County participated.

I asked them what drives the need for uniform policies for securing information. Here’s what they said is driving the need for consistent information safeguards countywide:

- Minimize liability
- Maintain customer confidence
- Use best practice
- Public accountability & expectation of transparency
- Take advantage of e-Gov benefits
- Accessibility with sufficient safeguards
- Sensitivity to ID theft notification

Then I asked, “what’s holding us back – what is restraining the County?” They said:

- Selling it – “buy in” at the top
- Time sensitivity – “I don’t have time for this”
- Technological complexities
- Expense – this stuff costs
- Constraints of uniform standards
- Business processes are inconsistent
- Difficulties in focusing on “what it is & what to do”
- It’s overwhelming to us
- Competing priorities

Now that we know the kinds of things holding us back, we’re in a good position to put together a step-by-step plan for progress.

Yours for better security more often,

Jim
The Single Most Persuasive Word In Our Business

Ben Hart tells me that again, contrary to conventional wisdom, the most persuasive words in selling are not “free” and “new.”

The word “BECAUSE” is far more persuasive.

Why?
BECAUSE this word signals to the reader that you have reasons for making the claims you are asserting…
BECAUSE this word instantly lets your reader know that you have facts to back up what you say…
BECAUSE this word shows your reader that you have put thought into your message.
BECAUSE is a great word for building credibility.

Explain the ‘why’ for policy and procedures – “because…”

You will have a much better success rate connecting your ideas with your customers and your employees.

For example:

We each have a responsibility to maintain the privacy and security of all confidential information.
Why?

- Because the public (including you) is trusting us to protect their information from misuse by unscrupulous people.
- Because it is socially irresponsible to violate this trust.
- And because there are civil and criminal penalties for willfully misusing anyone’s personal information.

We’re all salesmen to some extent. BECAUSE facts and reasons persuade the reader to take action.

Think about it.

Yours for better security more often,

Jim
Don’t overlook the obvious

“With all this money and time we spend on security, how come we still have information security problems?”

Hmmm. Good question. This is what management is asking their security officers. There’s a good answer. It starts out complex, but is really quite simple.

Here’s what a survey of Fortune 500 companies tells us:
• 64% report they have never inventoried where their sensitive data is
• 53% say they’d have no idea what was on a laptop if it were lost or stolen
• 82% of security incidents caused by insiders occurred by accident

And here’s the top security mistakes end users make:
• Failing to install anti-virus and keep it current
• Leaving laptops out in the open unprotected
• Executing games or screen savers from untrusted sources
• Failing to install security patches
• Not making and testing backups
• Being connected to more than one network at a time

What’s the message behind all this?

The security officers from Target, CISCO, Delta Airlines, State of CA, and Johns Hopkins Hospital all came to the same conclusion.

Carelessness.
We don’t do the things we know we should.

The 80/20 rule tells us that 80% of our security protection comes from 20% of our efforts.

Everyone needs to do the easy, simple things.
• Don’t share your password
• Lock up valuable equipment and confidential data when not in use
• Shred paper with confidential or personal information on it
• Don’t let people tailgate through building entrances with badge readers
• Know where your confidential data is
• Keep your computer up to date with virus protection and patches
• Talk to your supervisor or manager if something seems suspicious or not right

Information security is like a chain link fence.
It’s only as strong as the weakest link.
Master This If Security is a MUST for You

Does the life of a security professional appeal to you?

Well, I’m guessing you have an independent streak you like to indulge. Me too.

But here’s something few people talk about in this business. Being independent doesn’t mean you become an island.

**When you work hard all alone you risk getting burnt out and losing momentum.** You have no one to share your successes and challenges. No one to spur you to greater creativity. And no one to help you with a better security program.

It might seem easier to herd cats than to get a bunch of us independent people to work together. But building strong working relationships is crucial.

**Working together with our peers and colleagues is one of the most important skills to develop. I have plenty of examples to prove my theory:**

-- Three years ago, I met Darren. He invited me to an ISSA meeting. Since then we’ve shared ideas for security programs and staff training.

-- Back in 2004 I began HIPAA security compliance for my county. Kevin and Paul helped get me going. And, they helped me stay on track with this effort.

-- And recently I’ve been sharing ideas with colleagues about risk assessments and security awareness.

**My point is this: don’t overlook the importance of building strong relationships along the way.**

Many of us in information security are introverted. And many of us like to be highly independent. This strength helps when we have to work alone or manage the many stresses that come with information security.

But there are other challenges... Staying motivated, sharpening your ideas, and advancing your security program.

**So, don’t be shy about turning to others for support and strength.** You’ll reach your goals twice as fast, and enjoy your success many times more.

Yours for better security more often,

*Jim*
There Are Only 3 Ways To Become A Top Performing ISO...

FREE report is yours for the taking

Every single Information Security Officer started with a dream. Without proper instruction you are closing the doors to the dream.

Continual instruction for your career is critical. And a top performing ISO is made 3 ways.

Within in 30 minutes of getting your hands on this easy to understand 12 page report, you’ll know exactly how to:

1. create and articulate your vision,
2. drive a culture of accountability and execution,
3. and capture executive support for your information security program

If you seriously want to improve your career over the next 2 months, this may be one of the most important things you ever read. (Go to the website to find out more).

Get the ISO Edge with career advancement instruction:

1. Find out if you are making progress
2. Develop a compelling strategy
3. Build and sustain an information security program
4. Develop your information security business plan
5. Organize, prioritize, and evaluate your security program

Find out how to improve your focus, your efforts, and your disciplines – by using and following simple instructions.

You can stop wondering and worrying about all that confusion zapping your goals and strategy, fragmenting your efforts, and ruining your performance as the information security officer.

To access your FREE Report (Guide to Using the Information Security Series), designed to help you be the best ISO you can be – whether you’re new or experienced, just go to

http://www.ocit.saccounty.net/InformationSecurity/default.htm

Yours for better security more often,

Jim
County of Sacramento
Board of Supervisors
2008

Jimmie Yee, Chair, 2nd District
Roger Dickinson, 1st District
Susan Peters, 3rd District
Roberta MacGlashan, 4th District
Don Nottoli, 5th District

Terry Schutten
County Executive

www.SacCounty.net