68 Great Ideas for Running a Security Program

LOOKING FOR INSPIRATION? Want to learn a few new ways to elevate your security game? Can you spare five minutes to think strategically and long-term instead of just putting out another fire?

Then look no further. We've combed through our archives and come up with 67 of the best, most useful, most interesting ideas for running a great security program. Some are big ideas; some are very small. These tidbits come from security practitioners, industry experts, and some other all-around smart folks, covering new trends and age-old dilemmas. We present them to you here in bite-sized pieces, with topics intentionally intermingled to help get your creative juices flowing.

Tip: Get your highlighter. Read this document until you hit an idea you like. Flag it. Then go try it. Come back again when you're ready for another idea. We'll be here.

< 1 >

Nurture dissent. "I solicit people to challenge management. That is so critical. It creates much better decisions when people can respectfully and openly challenge assumptions, thinking and decisions," said Tim Williams, global security director for Caterpillar.

www.csoonline.com/article/688812/?source=greatideas1

< 2 >

Decide to be a better listener. To hone your negotiation skills, start with your ears. "Active listening is a bunch of relatively simple skills. One is asking questions to clarify what the other person said," said Chris Voss, a former FBI negotiator and head of the Black Swan Group, a firm that specializes in business and security negotiations. Another is paraphrasing—saying back to the other person, in your own words, what you think he just said. This is helpful because then "the other person gets to hear how their communication was received and whether or not it has been heard correctly."

www.csoonline.com/article/595563/?source=greatideas1

< 3 >

Enable password-protected screen savers. They're simple and free—what's not to love?

www.csoonline.com/article/219055/?source=greatideas1

< 4 >

Can't decide on one business solution? ***Come up with "gold, silver and bronze" options.*** "Help the business understand the risks associated with each option, then let its members make the final selection," said Dan Lohrmann, CTO, State of Michigan. Just be sure not to offer any alternatives that you can't live with.

www.csoonline.com/article/641819/?source=greatideas1

< 5 >

Be the Chief Self-Esteem Officer. Remember Stuart Smalley, the old "Saturday Night Live" therapist who began each skit with his daily affirmation? Channel him in your thinking: You are good enough, smart enough and, doggone it, people like you. Have confidence in your own judgment, and push back when it's necessary. We've been giving CSOs this advice for years, and we still believe it and know that, once in a while, you need to hear it.

www.csoonline.com/article/218675/?source=greatideas1

< 6 >

Think of one new way to pass costs back to business units. Having trouble increasing your security budget? Make it smaller, by finding ways to pass your expenditures back to the individual business units that are benefiting from your group's efforts. This takes some legwork and salesmanship, but it can quite literally pay for itself.

www.csoonline.com/article/218675/?source=greatideas1

< 7 >

Institute a clean-desk policy. Offer guidance on what should be locked up and when. Make sure employees know that it's not acceptable to keep sensitive papers out overnight.

www.csoonline.com/article/219055/?source=greatideas1

< 8 >

Be happy when you tweet. That is to say, definitely don't post content on Twitter, Facebook or LinkedIn when you're upset. "Posting any content when angry is about as dangerous as sending flaming emails, if not more so," said Scott Hayes, president and CEO of Database-Brothers Inc. "Think twice about clicking 'submit' because the world may be looking at your angry, immature rant for years."

www.csoonline.com/article/496314/?source=greatideas1

www.csoonline.com/article/529764/?source=greatideas1

<9>

Brush up on the basics of accounting. It may seem obvious, but it's important to have a good grasp of basic accounting principles. This will help you do effective training and awareness programs, as well as identify problems. The tenets will be familiar to you: trust, but verify.

www.csoonline.com/article/591654/?source=greatideas1

<10>

Simplify your PowerPoint slides. Supporting materials should cover the highlights, not repeat your entire message and then some. Jerry Weissman, the corporate presentation consultant who wrote "Presenting to Win: The Art of Telling Your Story," also said he has seen too many presentations where the legends are indecipherable, the gridlines are impossible to follow, and the numbers aren't even right-justified. "Any one of these violations of the depictions of the numbers is a distraction from the presenter and the presenter's message."

www.csoonline.com/article/219903/?source=greatideas1

<11>

Thinking about outsourcing security? **Think long-term.** Building relationships and trust takes time. But you knew that.

www.csoonline.com/article/479097/?source=greatideas1

<12>

Consider whether you adequately separate the people from the security. Businesses are made up of people, who have families, play golf (or another game) and cheer for local sports teams, said Dan Lohrmann, CT of the state of Michigan. Remembering this will help you separate the tough issue you're addressing from the person with whom you disagree. "Remember that the relationship will usually last longer than the current challenge."

www.csoonline.com/article/641819/?source=greatideas1

<13>

Memorize the 37-word description of how (in theory) to achieve perfect information security. There are exactly two keys to information security or information assurance, according to Stephen Northcutt, president of The SANS Technology Institute: "First, configure the system and network correctly and keep it that way. Because this is impossible to do perfectly, the second key to information assurance is to know the traffic coming into and out of your network." Recite five times in the shower. See, now isn't that simpler than you thought?

www.csoonline.com/article/342820/?source=greatideas1

<14>

Clearly identify your starting point. It might seem obvious, but before you decide to undertake a project, do whatever you can to establish a baseline. It's like knowing how much you can bench-press on your first day at the gym.

www.csoonline.com/article/219903/?source=greatideas1

<15>

Organizing a team? **Mix experienced staff and younger staff.** They can benefit from one another's perspectives.

www.csoonline.com/article/218675/?source=greatideas1

<16>

Look for hard numbers. Business people love metrics. Numbers can help you communicate and quantify the investment your organization is making in security. Be ready to share whatever numbers will help prove the value of the security organization, even if it's something simple like the number of desktop computers your team has scrubbed of viruses.

www.csoonline.com/article/219904/?source=greatideas1

<17>

Automate your patching processes. Rote tasks can zap your organization's time and funding. Set up systems to handle the software and OS updates, and save your staff for tasks that require more expertise.

www.csoonline.com/article/218675/?source=greatideas1

<18>

At overnight events, provide a safe place for employees to leave their laptops. Bonus points if you send out a letter before the event reminding attendees to leave their laptops in the designated area rather than in their hotel rooms—assuming they need to bring their laptops at all. This letter should be signed by the senior-most person attending the event.

www.csoonline.com/article/220282/?source=greatideas1

<19>

Share your knowledge. To be recognized as a leader at your business, don't hoard knowledge, said Michigan CTO Dan Lohrmann. Instead, freely give it away.

www.csoonline.com/article/641819/?source=greatideas1

<20>

Remember that processes are cheaper than technologies. **Instead of hiring guards and putting in an expensive card access control program, try locking a door or putting up a wall.** Training employees to be more aware of security risks is cost-effective – especially if you work with human resources to put in penalties for the petty but pernicious offenses of letting unauthorized people through access-controlled doors or propping a door open with a trash can.

www.csoonline.com/article/218675/?source=greatideas1

<21>

Need a social media security policy? **Make the most of what you have.** The communication landscape is so dynamic that if you create a policy specific to today's technology, tomorrow it may be obsolete. (If you see a policy that contains more than one

reference to MySpace, you know what we mean.) Instead, said Jack Phillips, IANS co-founder and CEO, try to draw attention to existing policies in a way that's relevant to new trends. As social media platforms come and go, some will ultimately become commonplace and integral to an enterprise, at which point it may become necessary for policies to be more specific.

www.csoonline.com/article/529764/?source=greatideas1

www.csoonline.com/article/505593/?source=greatideas1

< 22 >

When protecting intellectual property, sweat the small stuff. It doesn't take one large IP breach to destroy your business; instead, a thousand small ones could hinder your company's ability to stay competitive, said William Boni, vice president and CISO of Motorola and a co-author of "Netspionage: The Global Threat to Information." "I call it the death of a thousand cuts. Because most organizations don't have a means of tracking the loss of proprietary information; they go on constantly hemorrhaging, constantly losing market share. Gradually it takes the vitality out of the organization because it's hard to invent and create things faster than people are leaking it or stealing it."

www.csoonline.com/article/218034/?source=greatideas1

< 23 >

Make security policies only as strict as your organization needs them to be. You can do this by really knowing and understanding the business. Overly restrictive policies can backfire. "When this is the case, users will come up with workarounds that could be worse than the problem you are trying to prevent in the first place," said Ken Smith, a security solutions architect at Forsythe Technology.

www.csoonline.com/article/470095/?source=greatideas1

< 24 >

When evaluating network solutions, look at value, not cost. The cheapest or most conventional approach might result in only modest management gains, said Brian Neely, CIO of American Systems, an Virginia-based IT management and consulting firm. Use everything at your disposal to measure the full value of whatever product or service you are considering.

www.csoonline.com/article/507764/?source=greatideas1

< 25 >

Transform desktop support into security marketing. Did somebody step into the door of one of your staffers because he or she needed a simple password reset or a virus update? Use it as a chance to raise security awareness. Hang up a poster educating employees about common phishing ploys, or send them off with written instructions about choosing a secure password. Every interaction can be a teachable moment.

www.csoonline.com/article/219904/?source=greatideas1

< 26 >

Be mindful of every communication to recruiters. A key differentiator of a ho-hum CSO candidate and a top-notch one is great communication skills. A four- or five-word response in an incomplete sentence may take you out of the running.

www.csoonline.com/article/220903/?source=greatideas1

< 27 >

See if the marketing department is interested in the new video surveillance system. Not only will you be more likely to get the funding you need, you also will do a good turn for the business. "Marketers can do things like people counting," said Charles Foley, CEO of TimeSight Systems, a video surveillance vendor in Mount Laurel, N.J. "They can analyze how many people were clustered around that end-cap display, and how long were they there?" That kind of data can help marketers optimize the business, potentially a very great benefit.

www.csoonline.com/article/479097/?source=greatideas1

< 28 >

Set up a fraud hotline. Give employees a way to anonymously report violations of company policies. Not only will the fraud department learn about problems that might otherwise have gone detected, such a hotline is also a surprisingly simple way to deter fraud.

www.csoonline.com/article/220704/?source=greatideas1

< 29 >

At the same time, don't over-rely on tipsters. Historically, most fraud was reported via a tip, said Brad McFarland, director of corporate security with The South Financial Group, a South Carolina-based financial services holding company. Today, however, it's important that companies implement data analysis as well. Strong data, analyzed in tandem with knowledge of potential criminal schemes, can help organizations mitigate their risk of fraud.

www.csoonline.com/article/591654/?source=greatideas1

< 30 >

K.I.S.S.: **"Keep it simple, stupid" (or "keep it simple in security").** The more complicated your network gets, the harder it is to track where sensitive information is going, and the ever more difficult it is to secure.

www.csoonline.com/article/?source=greatideas1

< 31 >

Keep work for work and play for play. When using social media, know your objectives. "I can't tell you how many times I have been invited to Facebook by a work colleague only to find things on their wall or profile that are definitely not politically correct or are downright offensive," said Benjamin Fellows, a senior IT security and risk consultant at Ernst & Young. "I keep all my work friends in LinkedIn and my personal friends in Facebook. Even then, I am very

careful what I say on either site. I guess you could also put this under the heading of know your audience."

www.csoonline.com/article/496314/?source=greatideas1

<32>

Practice thinking like a spy. What information do you want to keep from your competitors? If you worked for a competitor, what devious tricks might you use to find out this information? Don't be afraid to get creative as you brainstorm, and then look for the most basic vulnerabilities that might lead your competitor to this information.

www.csoonline.com/article/218034/?source=greatideas1

<33>

Fine-tune your protection of trade secrets. Employees usually know that trade secrets are valuable, and stealing them is illegal under the 1996 Economic Espionage Act. What's more complicated is helping employees understand how seemingly innocuous details can be strung together into a bigger picture that could be advantageous to your competitors.

www.csoonline.com/article/218034/?source=greatideas1

<34>

Learn to say "yes... but." Security practitioners get a reputation of being no-guys. Instead, try to offer a solution for whatever plan the business has come up with. If they don't like the plan once security has been factored in, perhaps they'll come up with another plan.

www.csoonline.com/article/219569/?source=greatideas1

<35>

Remember what web browsers are designed for. Browsers are meant to make information exchange simple, not safe. Until security becomes the most important priority for web browsing software (unlikely), problems will persist. SANS President Stephen Northcutt said this is especially true with the new web 2.0 interfaces that use extensions to AJAX, a programming language supported by web browsers. These extensions deliver enhanced functionality, but at the cost of increased risk.

www.csoonline.com/article/342820/?source=greatideas1

<36>

When brainstorming risks, don't worry about precision. You're looking for any event or scenario that could create a risk in whatever area your group is focusing on. Rank risks loosely by likelihood and impact, and then turn the focus to solutions.

www.csoonline.com/article/610063/?source=greatideas1

<37>

Use education to prevent and detect fraud. Fraud is likeliest to involve employees in accounts payable or purchasing functions, as well as any employee who submits expense reports, said Mike Osborne, senior security manager at Kimberly-Clark. It's crucial to train employees in general—and these individuals specifically—on company policies, procedures and code of conduct.

www.csoonline.com/article/220704/?source=greatideas1

<38>

Build teams to assess risk in targeted areas. If you're evaluating risks to internal investigations, for instance, your working group might include a representative from every department that plays a role in internal investigations, such as human resources, corporate security, information security, facilities, finance and legal. If you're evaluating risks to brand protection, though, it will be more important to include marketing, and perhaps less important to include facilities.

www.csoonline.com/article/610063/?source=greatideas1

<39>

Don't cry wolf. Declare an emergency only rarely—like, you know, when there's an emergency.

www.csoonline.com/article/641819/?source=greatideas1

<40>

Double-check that your organization is keeping its original logs. If records are requested from your organization, the requesting entity will most likely be using a completely different technology tool set. For that reason, it's important that copies of your original logs are kept in their native, unaltered state, wrote David Torre, an experienced security professional and CTO of Atomic Fission. If this isn't possible, then at the very least, logs should be easily exportable to a standardized format without loss of important information.

www.csoonline.com/article/626296/?source=greatideas1

<41>

Resist the urge to look down everything in sight. Creating a security-minded organization is a process not unlike raising teenagers, said Corey Thomas, vice president of marketing and product management for Rapid7, a Boston-based consulting firm. You want to establish a dialog so that employees will know how to make the right choice when the time comes. "Aim for progress, not perfection," he said.

www.csoonline.com/article/479097/?source=greatideas1

<42>

Going global? **Remember that people in different counties and cultures have vastly different ideas about ethical business practices.** Fuld & Company, an intelligence consulting company in Cambridge, Mass., once did a scruples survey asking 122 competitive intelligence professionals whether it was normal, aggressive, unethical or illegal to take off your badge before approaching a competitor at a trade show. In North America, 34 percent of respondents considered this behavior aggressive, and 50 percent

found it unethical. In Europe, however, 56 percent of respondents said this was normal behavior.

www.csoonline.com/article/218034/corporate-spying-snooping-by-hook-or-by-crook

<43>

When evaluating firewalls, put them to the test. This is one great thing about choosing a firewall. "Pick two or three of your favorites and bake them off in real-world situations," said John Kindervag, senior analyst at Forrester Research. "You can test them on a live production environment because they are passive tools." See how well they do at finding unused rules, optimizing configurations and so on, and then compare the reports.

www.csoonline.com/article/593151/firewall-audit-dos-and-don-ts

<44>

Always offer trade-offs. Security departments have long been the opposite of yes-men. "No, we can't do that." "No, we shouldn't try that." "No, that's not a good idea." Try to work "yes" into your vocabulary more often, but just be clear what the tradeoffs are. Another way to view this is offering alternatives instead of ultimatums.

www.csoonline.com/article/219569/in-depth-democratic-party-convention-security

<45>

Articulate your career results. Recruiters and other gatekeepers in the hiring process want to know what kinds of results you have achieved, so be prepared to explain them in a succinct way. "The best way [for job candidates] to differentiate themselves is to be able to describe a situation, the action they took and the results that were accomplished in a way that displays an overall understanding of risk," said Joyce Brocaglia, founder and CEO of Alta Associates in Flemington, N.J. "I don't care about how many nodes and this and that. Did they display an understanding of the problems or risks before they implemented a solution? Did they tailor the solution to meet the risk appetite of the business?"

www.csoonline.com/article/220903/make-yourself-a-dream-security-job-candidate

<46>

Know the three processes of information security. Not only can SANS's Stephen Northcutt describe in a most succinct manner the keys to information security, he can also break it down into three basic processes – useful for explaining the basics to even the most business-minded project manager. Step one is protection, where we configure our systems and networks as correctly as possible. Step two is detection, where we identify the configuration has changed or that some network traffic indicates a problem. Finally, step three is reaction – when, after identifying quickly, we respond to any problem and return to a safe state as rapidly as possible. Any security process fits into one of these three categories. Really it does.

www.csoonline.com/article/342820/network-security-the-basics

<47>

It's OK to be a fast follower. Let other companies work out the kinks in new security technologies, then benefit from their successes and failures. It may sound dull compared to testing out the latest and greatest, but it's a whole lot easier to justify to the board.

www.csoonline.com/article/218675/security-budgets-money-well-spent

<48>

Use social media policies to your advantage. When compliance regulations came into play, savvy security teams were able to create new policies to comply, while also letting employees know why they were important. The same holds true for social media. "This issue is an opportunity for info sec leaders to refocus attention on information security and risk management," said Jack Phillips, IANS co-founder and CEO. You might even be able to use social media to raise security awareness. People are paying attention to social media, so use that to your advantage.

www.csoonline.com/article/505593/4-tips-for-writing-a-great-social-media-security-policy

<49>

Look for ways to do some incident response remotely. Not only does avoiding travel save money, it can reduce your company's carbon footprint as well.

www.csoonline.com/article/410513/?source=greatideas1

<50>

Give employees the tools to secure their desks. Make sure employees have locking desk drawers, filing cabinets and office doors. Face whiteboards away from the windows, not towards them. Install blinds. Provide paper shredders. Make laptop docking stations lockable. Employees have the keys to security, literally.

www.csoonline.com/article/219055/?source=greatideas1

<51>

At a sensitive meeting, keep the signage simple. No need to hang up a sign that says "Strategic Planning for Acme Corp." Instead, why not just hang up a sign that says "Private Meeting"?

www.csoonline.com/article/220282/?source=greatideas1

<52>

Think partnerships, not dictatorships. Even the U.S. Secret Service, when planning for national security events, tries to enlist people as participants in their security efforts. "We can't show up and say, Here's what we're going to do," said Secret Service Agent Scott Sheafe, who helped lead security efforts for the 2004 Democratic National Conventions. "....It has to be a partnership."

www.csoonline.com/article/219569/?source=greatideas1

<53>

Make sure employees know that they'll be accountable for their actions. When employees realize the company will take a hard stance on fraudsters, they'll think twice about committing a felonious act, said Mike Osborne, senior security manager at Kimberly-Clark. "I have seen companies publish a quarterly newsletter containing articles about dishonest acts perpetrated against the company, travel security advice and safety measures. The important item within these stories regarding fraud was the disposition of the case so the readers would know the company's stance on these

issues."

www.csoonline.com/article/220704/?source=greatideas1

<54>

Thinking about access control? Look for the sweet spot. George Johnson, chief security officer at the National Center for Crisis and Continuity Coordination, said IT shops often assign everyone administrative access to reduce the workload tighter controls involve. This, he said, is a recipe for a massive compromise. But the opposite practice of allowing only executives administrative access while locking everyone else out is fraught with danger as well, because you end up putting too much control into one person's hands. Aim for the sweet spot right in between.

www.csoonline.com/article/470095/?source=greatideas1

<55>

Understand that sloppiness will hurt your company more than thieves. "Sure, there are people out there who want to take your information," said Leonard Fuld, owner of Fuld & Company, an intelligence consulting company in Cambridge, Mass. "But more often than not, your own company is doing damage to itself by not being tight about how it controls information." That laxity is what allows his company to gather competitive intelligence—both for companies that want to keep tabs on rivals and those that want to identify their own leaks.

www.csoonline.com/article/218034/?source=greatideas1

<56>

If you know an event is in the works, try to get involved in planning before the location is chosen. Some sites offer more security challenges than others. If you can offer advice early in the planning process, you might save event planners a lot of expenses – and your department a lot of headaches.

www.csoonline.com/article/219569/?source=greatideas1

<57>

When giving a presentation, don't fade into the background. When you're watching the evening news, do you watch the newscaster, or the screen behind him or her? You look at the newscaster, of course, and the screen behind him just gives a few highlights. Be sure you're using any visual aids as a backup and not the main attraction.

www.csoonline.com/article/219903/?source=greatideas1

<58>

Random tip, because you just never know: When negotiating with a kidnapper, never confirm the hostage is alive by asking about her childhood stuffed animals. Questions along those lines are a signature of law enforcement in the kidnapping world, said Chris Voss of the Black Swan Group. "When a family starts asking a question of that type, there's a pretty good chance that they're being coached by the cops, which makes kidnappers very nervous."

www.csoonline.com/article/595563/?source=greatideas1

<59>

This afternoon, reach out to someone outside your company. Talk with peer institutions and law enforcement. Perpetrators are operating in multiple geographies and with multiple institutions. "If we want to prosecute fraudsters effectively, it's important to have dialogue with others to try and get the full picture," said Brad McFarland of The South Financial Group.

www.csoonline.com/article/591654/?source=greatideas1

<60>

Think of one new way to have fraud and security departments rub elbows. Brad McFarland, director of corporate security with The South Financial Group, said increasingly the line between the departments is blurred, especially in financial services.

www.csoonline.com/article/591654/?source=greatideas1

<61>

Ask an open-ended question at your next meeting. Whether you're negotiating with a potential business partner or kidnapper, try to draw out the real issues by asking questions that can't be answered in just a word or two. "An open-ended question forces the other side to take an honest look at you and answer your question," said Chris Voss of the Black Swan Group.

www.csoonline.com/article/595563/?source=greatideas1

<62>

Speak the language of whatever tribe you're addressing. Every culture has its own lexicon and jargon. To be an effective communicator, said the late Robert Garigue, CISO of the Bank of Montreal, "you have to use examples from the tribal culture that you want to influence"—including the tribes that co-exist within any large organization. Strive to use metaphors that will help your audience understand how and why they can help improve the security of your organization.

www.csoonline.com/article/219904/?source=greatideas1

<63>

In any crucial area, find a way to increase separation of duties. Separation of duties is a common policy when people are handling money. With separation of duties, fraud requires collusion of two or more parties, which greatly reduces the likelihood of crime. Information should be handled in the same way, since it can be bought and sold easily. If your system administrators claim that their duties cannot be broken up, it is important to understand that well run organizations do just that, according to the SANS Institute.

www.csoonline.com/article/342820/?source=greatideas1

<64>

Look for the most bang for your buck. When looking for solutions, rank possible controls based on cost, difficulty, and effectiveness. In particular, note controls that can reduce likelihood and impact across multiple types of event. With good luck, you might be able to pay for a new control by reducing the redundancy of existing controls.

www.csoonline.com/article/610063/?source=greatideas1

<65>

If you're hosting a long offsite meeting, consider booking an extra room to be used as a lounge. That way, you can keep sensitive conversations about the meeting from taking place in public areas of the conference facility. And yes, employees will use the room (and be grateful for it) if you keep it stocked with snacks and drinks.

www.csoonline.com/article/220282/?source=greatideas1

<66>

Keep up appearances. "There is an element of appearances to security, and I don't mean this in an unfavorable way," said Gavin de Becker, author of the book "The Gift of Fear." "Precautions that are expected to deter often draw some of their effectiveness from appearing to be this or that. Effective security professionals know that demeanor and appearances are a language that can communicate confidence far more keenly than mere words."

www.csoonline.com/article/219895/?source=greatideas1

<67>

Find a trusted colleague to help you maintain your ethics. Michigan CTO Dan Lohrmann said, "Find one or more accountability partners who share your professional values. Remember that accountability is for winners, not losers. The best musicians, artists and athletes are accountable to coaches. Everyone who strives to improve needs accountability."

www.csoonline.com/article/641819/?source=greatideas1

<68>

Step back and evaluate your career at least once a year. Schedule some time to get away, and try to disconnect for at least part of the break, Michigan's Dan Lohrmann said. "Talk about how things are going at work with those you trust but who have a different perspective." If you're feeling burned out, remember that a career is more like a marathon than a sprint.

www.csoonline.com/article/641819/?source=greatideas1

#

