Executing an effective security program.

With all the major data breaches in the news, many wonder why it seems so hard to have an effective, affordable and adequate security program. Security management should be no different than any other enterprise discipline, endeavor that needs a comprehensive plan, based on the organization’s success factors. A security plan includes a prioritized task list, backed up with adequate resources, to ensure the product or service is built effectively, and that both the product and the organization are safe. This is especially true with cyber where, like all efforts, security leadership needs to get the requirements right first, or they end up resourcing and building the wrong cyber environment, and security incidents and data breaches follow. Following that, they need mature operational processes (and especially configuration management, the critical security control) and a comprehensive security policy to effectively implement and operate the security architecture. Given all the competing resources in any organization, the security leadership, generally led by a Chief Information Security Officer (CISO) or equivalent, must show the C-suite / directors and officers / business line managers the value proposition of their enterprise cyber program, how it is a business enabler. For any enterprise initiative to work well and be effective, including cyber, there needs to be a senior leadership champion that makes security a priority within the organization, supports security policy enforcement and resources it effectively. The CISO needs to convince the senior leadership with a security program that shows an integrated cyber story that is seen as a business enabler and addresses both the “what” and “how” of an effective cyber environment within an enterprise risk management (ERM) framework.

So given all the complexities to prioritize, balance, and resource in a security program, how does one execute the essential CISO functions effectively and authoritatively - so that the C-suite is beyond convinced, and champions too! As in most endeavors, it comes down to doing the fundamentals well, knowing and monitoring your environment (security baseline), operating according to an overall enterprise master plan (risk in this case), and communicating the program’s value to all stakeholders, in a “360” manner. For cyber security that can be summarized as – the typical “plan – do – check - act” approach, with a “management by walking around” leadership style – all wrapped around ERM!

We recommend management first read our 2-page ‘CISO fundamentals’ paper, so they are aware of the 10 or so key activities we recommend to implement for an effective, affordable, and authoritative ‘due diligence’ level of cyber security. In fact, a solid first activity by any security manager would be to pass this paper to all the business managers for an early heads up on what it takes to provide a well-rounded, complete, integrated security program, within an ERM framework. Then let leadership know you will come back with an updated security program after your indoctrination (re: the rest of this article’s purpose).


In this 2-page paper we provide the key “what” to do tenets of cyber, the essential requirements, which then need to complement the “how” (process) operational aspects of your security program. From the CISO fundamentals paper’s major cyber tenets, we provide the more critical “what” to do aspects below. Following these cyber requirements, we provide a summary of the key “how” processes, timelines (the first 90 days), and general security plan development and execution recommendations.

Many of the cyber activities in the CISO fundamentals paper themselves entail a detailed process and their own storyline; thus one question might be “how to prioritize the most impactful tasks when initially starting?” That is, which of the 10+ activities do we recommend focusing on first? One could sense there would be half a dozen or so really key activities that can be further distilled from the 10 cyber tenets into no kidding fundamental “must dos” to act on first and do well – the key “whats” – and there are, we suggest these:

– Know your IT / security baseline – the security architecture - and get an independent review and assessment if at all possible. Yet at least review the cyber suite and overall HW / SW status - are the current inventories managed (e.g., do you even know what is on the network, let alone its operational state?).

– Verify a secure back-up process is in place and working, and if a BCP exists with detailed recovery processes. If back-up / recovery processes exist, are they tested? Can the company continue operations after an attack?
– Ensure SCM / SIEM / monitoring at some meaningful level is used, and an assigned security manager frequently reviews those logs, trends. The system monitoring activity includes some level of DLP (& DRM) are used to track data movement.

– Since virtually ALL security incidents are traced back to poor cyber hygiene, review and assess the security processes in use - how is the cyber equipment maintained? Are patches, upgrades, etc. current and tracked? Is access control managed – with minimized root privileges and enforced least privilege in the enterprise? If nothing else, just do the five activities that the National ‘cyber hygiene’ effort recommends – these are ‘management’ type items you need to do anyway, that net a relatively easy 85% reduction in security incidents. https://www.cisecurity.org/about/CyberCampaign2014.cfm

- Make data protection and privacy a top corporate priority. As it only takes one data breach lawsuit (coming from anywhere) to potentially put you out of business or at the very least cost $10Ms in damage, along with brand and reputation lost. Make “Privacy PAYs” a mantra to show both the positive enhancement (brand) and negative reduction (reduced data breaches) aspects of privacy.

– Review all recent security inspections and compliance reports – are there any known actions? Are there residual risks / issues that were supposed to be remediated, but stalled?

- Your organization, business, product / service etc are ALL about managing risk, thus your ERM’s risk management plan (RMP) (and risk reduction activities therein), combined with a security policy that guides and enforces the directions in the RMP, is your principle artifact to map your security program into and keep current, with metrics to back it all up.

- Finally, we all know how important security education is, so make it effective. You don’t need a massive internal training effort, just leverage existing free resources and make being “cyber safe” personal, with natural extensions to the work environment, as the effects will last longer.

AND THEN after doing those, consider added these protections within your security architecture and methods to minimize the threat vector (which ideally imposes minimal user hindrance, but you must still put security first): a - white listing of web IP addresses, b - allow only applications with certs to execute, c - enforce downloads to central folder to be scanned (in both email and the web browser), d - lock down clients / end user devices (do not allow executables to be installed by users on edge devices), and e - tighten up the browser controls (active code, etc. and enforce the guest mode), among others.

Wow, those were a lot of recommendations on just the “key what” to do activities – based principally on prevention measures and assessments of the security elements. These best practices have extremely high-value and are affordable to any security program and risk reduction effort. So what about the “how” and processes to complement the what? In short, there are many great articles, posts, and resources on this aspect of a security program; thus to provide the most effective ‘how’ view in this “quasi-short” article, I listed a couple of my favorite sources below (top down), where I offer a little added clarification on each. As ‘how’ to implement cyber in your organization will need to fit within and be personalized by your organization’s size, culture, business sector, risk posture and resources, among others. Your best bet is to skim these articles, see what resonates, then build your own tailored, key best practices, security processes and methods from them. Take a best of breed approach, emulating the ‘New CISO’s first 101 days’ timeline - all led by you, the CISO.

-- “So you want to be a CISO – 5 initial steps” (by Gary Hayslip, San Diego City CISO). I strongly suggest you read this “how” at the LinkedIn post first. Gary provides the key, overall security management steps to take (within a ‘plan – do – check – act’ process), while using a hands on “management by walking around” leadership approach – all within an ERM framework. Which of course is how we should all lead any aspect of our business. The five steps are: 1. Meet & Greet - “Walk About”    2. Inventory    3. Assessments    4. Plan    5. Communicate. So start your ‘how’ process discovery here – then skim the other four sources for their suggestions. Especially to build your specific timeline – the key what to do when - i.e. the first 90 or 100 days. Develop your own tailored security assessment and program execution plan from the ‘best of breed’ therein.
-- The First 101 Days as a New CISO – A Chief Information Security Officer’s Playbook. Justin offers a very comprehensive timeline with ten, 10-day periods, up to 100 days. *I like this article a LOT – it harmonizes very well with what I would put out*, so why replicate a good thing (as CISO’s need to know how to leverage existing efforts and always look to “scale” efforts). The author offers a very complete and germane list of security things to do and suggestions on how to do them (and his tasks map well with Gary’s recommendations). All within a specific 100 day timeline, including doing many parallel activities - hey, you know CISO’s must do this better than anyone else! He does the how / process quite well, not much is missing, except for: (1) an emphasis on data security and privacy; (2) the criticality of effective hygiene and enforced access control; and (3) my favorite – a top-ten issues / risks tracker. Replicate his timeline, add in your own key focus areas and these missing items, and you will have a great start on your security plan and playbook.


-- A risk view of security - This is a short slide show; thus worth reading up front, as it’s only 15 or so pages with lots of pictures and a few infographics, so an easy skim for effect. While there is no timeline provided, the Accuvant VP of risk management points out five key items that an effective security program should have. I really love how she starts off with ADAPT - due to the issues we all face (a - infrastructure revolution, b - always on and connected society, c - data explosion, d - tougher regulations (re: the President’s recent edict at a FTC summit – ‘make privacy matter’), f - huge data breaches, and g - the shortage of skilled workers). Then she offers a great security program goal – establish the CISO and security team as trusted resources and also adds a nice security plan mind map on slide 6! Renee then offers some sage lessons learned: (a - get to know the business and people, b - understand perceptions, c - define key assumptions and risks, d - benching marking is critical – yet an art form, e - application security “pulls a long train,” and f - having the tough conservations). Then she offers five great points on how to support the role of executives (C-suite, et al) and the board (advisers, key stakeholders) – where as you know this is a must do for any manager. A lot of great advice and perspectives in such a short brief. Use it to frame your plans and detailed, tailored timeline.

[http://static1.squarespace.com/static/5419be5de4b062d1159bbce31/t/546b88d4e4b0cb1a83eb7ed5/141633524940/Information+Security++The+First+90+Days+and+Beyond.pdf](http://static1.squarespace.com/static/5419be5de4b062d1159bbce31/t/546b88d4e4b0cb1a83eb7ed5/141633524940/Information+Security++The+First+90+Days+and+Beyond.pdf)

-- CISO: Your First 90 Days - Pretty good overview, not as detailed a timeline as Justine, others, but Bill offers a great ‘big picture’ view, especially as it applies to getting executive leadership buy-in! His main points were derived from a webinar he gave and are: (1) Defining Chief Information Security Officer, (2) Expanded Scope, (3) Broader Relationships, (4) Executive Sponsorship, and (5) Recommendations. Where in #5 he offers his first 90 days immediate priorities as: (a - re-balancing prevention, detection, &response; b - DevOps: maturity in your development and operations processes; c - Excessive privilege / lack of CM; d - situational awareness: and e - know your IT architecture (proper segregation? Sufficient test environments?).

[https://www.co3sys.com/blog-post/ciso-your-first-90-days](https://www.co3sys.com/blog-post/ciso-your-first-90-days)

-- 90 Day Plan for New IT Security Managers. Allen also does a great job of providing the mechanics and priorities needed as a security manager of any sort – especially if there is no security department or it’s mostly the IT department (trying to do what they can in a complex cyber ecosphere). His premise - apply a tried and true multi-phase approach - assess the current state, determine the desired target state, perform a gap analysis, and then implement improvements based on priority. That is, use the gap analysis as the deliverables of the IT security program, prioritized and rationalized from a business benefit view, to gain the C-suite and business line managers understanding, facilitate a more effective approach to get the resources needed for cyber. For the more technically inclined, the gap analysis and justification approach herein are quite good, and recommended reading to add details and fidelity to your overall timeline (as he offers more of the “what” versus “how” / specific timeline) - yet is still quite a useful resource!


Mike.Davis.SD@gmail.com get more papers / briefs at [http://www.sciap.org/blog1/?page_id=1184](http://www.sciap.org/blog1/?page_id=1184)