

TIMOTHY E. FOLEY, CISSP

IT Security Executive with an Outstanding COC Reduction & OD Record

excellence in secure business-driven technology development

Leesburg, VA

703/443-2421

the_foleys@verizon.net

http://timfoley.info

EXECUTIVE PROFILE

"By balancing and integrating the potential reward of cutting-edge technologies against their inherent risks, I have provided cost-effective, competitive-advantage-conferring sustainable business solutions."

COST-OF-COMPUTING REDUCTION AND IT ORGANIZATION DEVELOPMENT HIGHLIGHTS

- Delivered over \$20 million dollars in annual net savings by devising and enacting legacy-system extension solutions.
- Risk mitigation accomplishments include savings of over \$50 million for one major program; accomplished by devising a solution using existing resources.
- Translates business goals into IT platforms--led client needs analysis and streamlining initiatives which returned tens of millions of annual savings.
- Manages multi-department application portfolios inclusive of negotiating service level agreements for user communities.
- Designed, implemented and continually improved a global end-user computing framework featuring standardized desktop applications coupled with off-the-shelf software to minimize expenses.
- Functioned as corporate security ambassador for over a decade; developed formal technology presentations for global education of internal engineers and managers on security technologies; facilitated bi-directional communications with the global design teams.

CAREER HISTORY

CITIGROUP, Silver Spring, MD

March 1996 - Oct. 2008

Vice President and Manager, Encryption & Authentication Architecture

(1999-2008)

Leadership: Nodal director integrating technology, vendor management, business process improvement (automation and business virtualization), R&D (emerging technology assessment), and IT governance. Senior decision-maker & negotiator with respect to assessing and purchasing encryption and authentication technologies; negotiated stipulations & Service Level Agreements and generated the reporting matrices for Administration & Operations. Senior security & operational strategic planner--developed business requirements, project plans, and resource allocation schedules. Apani® EpiForce® (Enterprise Security Solution for Corporate Networks) deployment lead. Functioned as senior analyst--Benchmarked and generated improvement options. Articulated bid requirements for all hardware and software upgrades, reviewed submitted bids and selected vendors. Authorizing officer for all system deployments inclusive of developing articulated business cases with fully-worked-out cost/benefit analyses. Oversaw provision of end-user services, including help desk and technical support services.

Controls: Administered a \$60-80 million annual global security / technology budget. Directed, through a team of 10-12 VPs & AVPs, up to 5 multi-discipline (business analysts, web masters, programmers, hardware engineers) international teams of up to 250 staff responsible for global implementation of secure computing solutions. Constantly reviewed systems performance to minimize operating costs.

Technical Subject Matter Expert: Chief architect of enterprise-wide end-to-end encryption and cross-functional team lead for ISO 17799/BS 7799-2 certification. Implemented cross-platform server isolation and layering solutions using EpiForce's logical securing zoning and policy-based encryption of Data in Motion technologies. Architect and Program Manager for global Public Key Infrastructure [PKI] (high- and low-assurance) deployments.

Contributory Highlights

- **COC Reduction**--Devised a \$5M solution to a \$50M problem--by implementing EpiForce, saved coding-level changes to over 10,000 legacy systems. By process re-engineering aspects of a PKI initiative

delivered a one-time savings of \$10M and annual savings of \$500K in labor by emphasizing low-assurance targets. For a Data Linkage Prevention/Enterprise Rights Managements initiative, consolidated four existing technologies into a common platform to reduce costs by \$7M. For security upgrading, devised an automated solution that shaved off millions in support costs. For a Secure File Transfer Project, developed an enterprise-wide SFT solution which replaced over 5 separate systems and which delivered a \$4-7 million annual savings. For a tape encryption project, identified an opportunity to dramatically increase ratio of drives to encrypters and brought in the project in half the time and cost, a savings of over \$30 million.

- **Metrics**--Brought in over 90% of projects before due time and under budget. Supervised 8 major re-engineering initiatives (consolidations, software/hardware upgrades, centralization, etc).
- **Vendor Management**--led contract renegotiation with a major systems security solutions provider to reduce virus & malware protection costs by millions; negotiated millions of dollars worth of extras from key suppliers throughout tenure.

Product Assurance Manager (1996-1999)

Controls: Administered a \$3-5 million annual global LAN deployment project budget. Project Managed cross-functional teams composed of up to 100 staff, 30% of whom were engineers.

Leadership: Maintained and evolved an 80,000+ node global network. Senior Technical Liaison to main outsourcing partner and top-tier executive committee technology advisor.

Bottom-Line Summary: Generated \$20 million net save by developing a superior migration methodology and an annual \$1.5 million net save in operating costs.

TRAWICK AND ASSOCIATES, Bethesda, MD 1994 - 1996

Senior Network Engineer (Department of Energy engagement)

UNIVERSAL FROZEN FOODS, Twin Falls, ID 1991 - 1994

Network Manager

EIMCO PROCESS EQUIPMENT COMPANY 1990 - 1991

Systems Analyst

NETWERX 1988 - 1990

Principal

USA COMPUTER TRAINING CENTER 1988 - 1989

Instructor

SEARS BUSINESS SYSTEMS CENTER 1986 - 1988

Systems Engineer

INTEGRATED TECHNOLOGY SYSTEMS 1984 - 1986

Technician

PROFESSIONAL DEVELOPMENT

Education: Computer Information Systems studies (1981-1984), Washburn University.

Accreditation: CISSP CERTIFICATION (2004), (ISC)2. Certified Network Engineer (1995), Orange Systems. Sniffer TCP Analyst (1996), Sniffer University.

Additional Training: Human Interaction Laboratory (1997), NTL Institute. Strictly Business (2004), Dale Carnegie Training Center.

Development & Implementation of Data Protection for Transportation of Customer Personal Information (PCI/PII)

Situation

The company shipped over 10,000 tapes per day from over 1,000 sites containing customer and business data. On more than one occasion some of the tapes were found to be missing, indicating a possible compromise of Personal Information. It was determined that significant and immediate action was required after appearing in the Wall Street Journal for the loss of 3.9 million customer records.

Action Plan

- Conducted global feasibility study to mitigate identified risk, including technical and procedural controls after initial loss. Modification of existing processes and utilization of preferred carriers appeared to be the most cost effective approach at the time.
- Utilized the results of the completed feasibility studies to put together a high-level plan and budget in 72 hours for presentation to the board, after a second loss occurred while using the preferred carrier option. The initial budget approved was \$60 million, including funding for the procurement of tape encryption hardware at 25% off list price and contractor resources for the rapid deployment. Global deployment to remediate all sites was projected at 12 months.
- Negotiated contract with encryption vendor for 50% off list. Also negotiated for on-site support during the installation phase, thus removing the need for contractor resources.
- Realigned and matrix-managed resources globally to form 250 member strike team.
- Directed engineering team to explore options to maximize usability with an eye towards reducing cost. Team identified methodology that established a 5:1 ratio between tape drives and encryptors, as opposed to the projected design of 1:1 for high-density sites.
- Designed operational processes that segregated the duties between three different areas within the IT organization, allowing the workload to be more evenly distributed and eliminating the need to hire additional resources.
- Developed scorecard to track remediations by site. This was centerpiece of weekly status presentation to Senior Management which clearly showed accountability.

Results

The scorecard and weekly status reports were a huge success with most site managers requesting to be moved up in the schedule. Our largest issue became one of the vendor being able to ship equipment quickly enough to fulfill these requests. Overall the project was completed in under 9 months at a total cost of \$27 million, a net savings of 55% off projections.

Strategic Development of Enterprise Secure Transmission Solution with Optimal Return on Invested Capital

Situation

Thousands of legacy scripts and applications spread across tens of thousands of hosts needed to be modified to address clear-text transmission of passwords. The company determined the transmission of identity credentials in clear text presented an unacceptable level of risk. This policy had developed as an internal security policy based upon industry best practices without consideration to the operational impact.

Action Plan

- Assessed impact of re-writing existing applications to utilize a secure transmission method. Company-wide estimate was 5-7 years of development at a cost of \$60 million dollars.
- Conducted feasibility studies for alternative technologies coupled with potential automated remediation methods. Identified cross-platform IPSec solution.
- Negotiated enterprise agreement for IPSec solution at \$3 million.
- Designed global implementation plan and operational model for new solution.
- Developed educational materials to raise awareness surrounding clear-text password issue including IPSec mitigation.
- Deployed solution globally and remediated all affected systems in 18 months at a cost of \$2 million.

Results

The global roll-out of the heterogeneous IPSec solution reduced the total cost of remediation by 92% and in half the time. The solution has since been extended to address other areas deemed at risk, including the transmission of Personally Identifiable Information (PII/PCI) and continues to generate savings.

Innovative Consolidation of Technologies with Reduced Costs

Situation

In 1990 company was implementing a full MRP/2 solution, including interfaces to key upstream & downstream suppliers. This created a need for high-speed data networking between the manufacturing plants and corporate headquarters. The direct solution was to deploy additional leased lines to each of the plant facilities at a cost of \$40,000 per month.

Action Plan

- Analyzed existing connectivity between the plants and corporate HQ. Discovered that trunk lines already existed for voice traffic. Traffic study indicated the lines were utilized at 10% level over 85% of the time.
- Devised innovative approach to share the same leased line between the new data needs and the existing voice traffic. Determined the commercial availability of advanced technology allowing the dynamic sharing of bandwidth.
- Created & presented executive briefing detailing cost avoidance opportunity. Built consensus through presentation to CIO council and each plant manager.
- Negotiated leased line rate and cutover with local telco. Optimized voice connectivity at the same time eliminating 70% of voice trunk lines.
- Produced & managed implementation plan for 5 plants in 3 states. Conversion was transparent to all parties.
- Design infrastructure to achieve six sigma uptime.

Results

By identifying and embracing the vanguard of voice/data integration technologies, the company realized a \$40,000/month cost avoidance. Additionally, the optimization of the voice environment resulted in several thousand/month more net cost savings. The program was well received as it addressed the immediate data bandwidth needs while producing a net reduction in operating costs.

- Generated \$20 million one-time & \$1.5 million recurring cost avoidance by devising a unique solution which leveraged existing server technology in a non-traditional fashion.
- Saved over 100,000 man-hours per year previously spent in remediating non-compliant low-risk issues by transforming the IT governance model from industry best practice to risk based approach.
- Generated an annual cost reduction of \$6.5 million by consolidating 5 overlapping data security technologies into a single leading edge technology.
- Developed standardized engineering methodology that reduced time to market by 40%. By creating standardized templates for engineering projects, engineering team was able to reduce the time required to introduce new technology into the company from 18 months to 11 months.
- Achieved ISO27001 certification for Security Administration teams. This was the first certification of a multi-national financial institution.
- Consolidated 5 independent file transfer systems to a single transfer platform generating annual operational cost savings of \$6 million. Additionally, sales increased 2% above projection due to cross-sale opportunities.
- Designed 3-tier infrastructure to support MRP/2 implementation: Granular plant production data remained at each plant on Intel-based platforms; aggregated data rolled up to division AS/400's; historical data was warehoused in System 390.
- Devised methodology to allow secure data exchange with upstream and downstream partners whose systems did not support EDI (Electronic Data Interchange).
- Achieved Year 2000 regulatory compliance for PKI after receiving management responsibility for it with only 4 days till deadline. Assessed issues and created remediation plan in first 8 hours of PKI ownership. Completed remediation effort with 12 hours to spare.
- Created corporate secure email solution including operation & administration process manuals, awareness memos, and training program. Conducted train-the-trainer seminars in London, Singapore, and São Paulo.
- As part of corporate merger, devised methodology for extraction, normalization, and insertion of user data from disparate corporate systems, allowing the smooth transition to a single universal desktop identity store.
- Created methodology to reduce operational costs through the standardization of technology configurations. Solution allowed for central engineering and testing of technologies with distributed deployment and support.
- Before Internet mass availability, created remote portal allowing secure remote access to all sales data allowing sales force immediate access to customer data, inventory levels, and order creation from any locale with a phone line (1989).

To Whom It May Concern:

I managed Citigroup's Security Architecture and Assessment group as a Senior Vice President until I retired from Citigroup earlier this year. Citigroup is one of the world's largest financial corporations spanning 110 countries with hundreds of thousands of employees. Citigroup has a complex electronic network with each country having different networking capabilities and regulations in both security and privacy.

I have known Tim Foley since 1996. Tim started out as a network engineer until the Security Engineering department was consolidated under Dan Tigar. Tim and I both reported up to Dan with Tim heading up the most difficult area, the encryption group. Citigroup was one of the first financial corporations to adopt a public key infrastructure (PKI) and it was because of Tim's efforts that this became a reality for Citi. Not only was Tim able to grasp the complexities of this technology but he was able to work with the vendor in coming up with solutions to technical difficulties. He was also involved with negotiating financial contracts with the vendor as well as presenting the technical capabilities to senior management and Citi's various businesses. Tim has a talent for making a complex technology understandable to those who are not technically inclined and has excellent presentation and writing skills.

For legacy applications that don't lend itself to a PKI solution, Citi had the need for an encryption solution that would work end-to-end across different platforms transparently, with good performance and local administrative control, and without re-writing these legacy applications. Tim worked with a promising vendor in creating a corporate solution that has also been deployed throughout Citi today.

Tim's exceptional quality is his ability to grasp complex technical details and implement solutions while working with senior management and with vendors to get things done. Tim has the ability to fit the current technical model into longer-term strategic solutions from both a financial and technical point of view. Over the years I have seen Tim's diplomatic skills grow as he had more exposure to senior management and with Citi's various businesses throughout the globe. Tim has the intelligence and the drive to work in difficult environments. He is extremely articulate as is evidenced by his many excellent presentations and technical papers he has written throughout the years. He has shown great leadership and skill in overcoming technical difficulties and strives for excellence in all that he does.

Please feel free to contact me if you would like to discuss this further.

Regards,


Janet Cugini

When you sit in a boardroom with Tim Foley, it becomes clear that he is a key contributor and valued advisor within the IT Security environment. What may not be as readily apparent is a more personal side that compliments and adds depth to his management style. Often using humor and real-life examples to illustrate a point, Tim brings an air of levity to an often dry and complex technical discussion. Recently, when explaining the current mortgage crisis to a neighbor, he likened it to buying strawberries at Costco and created an entire scenario surrounding the process. Afterwards, the neighbor remarked that although he had been trying to understand the mortgage crisis situation for months, he had never truly understood it clearly until this discussion. Being an avid reader, Tim brings a wealth of general knowledge into his discussions, making him an engaging conversationalist.

An enthusiastic leader both in and out of the office, Tim is known for his ability to create and articulate a vision and then move others to embrace it. When his minister recently approached him with a technical question regarding the church's sound system, Tim readily volunteered to lead the sound team effort. Within two weeks, he had researched, purchased, and learned the new hardware and software that now provides the church with a professional sound system. He has been effectively running the sound system for his church and his son's school ever since. He embraces a work/life ethic based on positive-thinking, service to others, hard work, honesty and respect, and is able to motivate and mentor others through his personal example and direct one-on-one interactions, having often assisted others as a personal life-coach.

Being the true "geek-at-heart" that he is, Tim met his wife, Lynn, online via AOL *beta*, back in 1993 - when only geeks were on the newly immersing Internet! After a year of long-distance dating, he moved from Idaho to Virginia where they now live with their 5-year old son. The family enjoys outdoor adventures such as camping, hiking and biking. On Saturdays during the spring and summer, you may find Tim being the "pit crew" for his wife's auto-cross racing car, Roxy - a Mazda RX-8 that won 6 trophies its first year of car shows. On Sundays, you will find Tim donating his time and talents in pursuit of his other hobby, "sound technician", at his local church. When asked how to best describe Tim, his wife answered "When I posted my online ad all those years ago, I titled it "Looking for Mr. 90%", assuming that no one would ever live up to 100% of my expectations. And, believe me, I'm not saying that Tim does! However, I will definitely say that he gives 110% to everything he undertakes, whether it's at work or at home."



"Some men see things as they are and ask - why. I dream things that never were and ask - why not?"
George Bernard Shaw

Information Security in the Enterprise

A New Paradigm

Most Enterprises have become well versed at reacting to security events, effectively mitigating the probability of recurrence. What is needed today is business-driven pro-active Information Security.

Overview

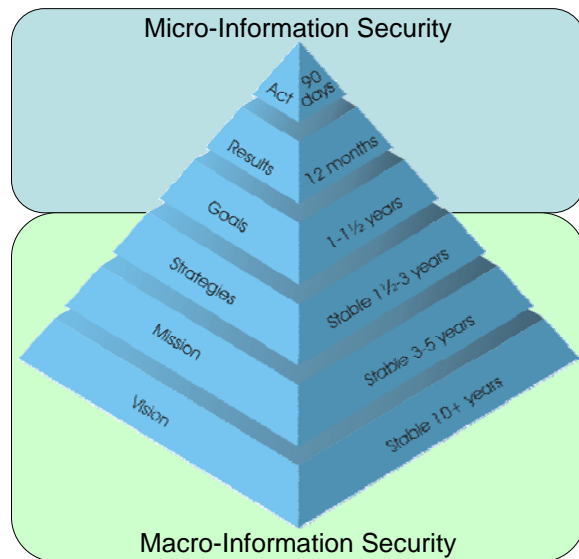
Information Security inside the corporation has evolved in last decade from a siloed, reactive endeavor to an accepted enterprise business practice. With this evolution it becomes obvious that information security and its constructs and underlying technologies must be fully integrated into the business. However, the continuing overuse of fear, uncertainty, and doubt (FUD), compliance edicts, audit findings, vulnerabilities, and credible threats have undermined the positive value proposition of information security to the lines of business. In turn, senior managers primarily responsible for information security find their positions in jeopardy when they are perceived as the impediment to growth and change, rather than a respected and contributing business management peer. This leads many business individuals outside of Information Technology to ask “What is *Information Security*” or possibly more accurately “What value does *Information Security* provide me”, thus complicating business integration and convergence.

The challenge becomes how to best ensure this integration. More than trial and error and experience are required. All information security professionals – engineering, operations, administration, compliance, and ISO (Information Security Officers) personnel – need to become knowledgeable in a new vernacular, *information protection stewardship*. They should be comfortable in verbalizing the tenants to not only their management, but also to the equivalent layer within the lines of business. They should have familiarity and be able to readily access knowledge of economics and business theory to aid them in socializing security initiatives.

As an example of the application of this let’s look at two terms from economics - *Microeconomics* and *Macroeconomics*. Microeconomics deals with economic behaviors at the individuals’ level, what is being bought and sold, and what is driving the decisions to allocate limited resources. Macroeconomics, on the other hand, involves the “sum total of economic activity, dealing with the issues of growth, inflation and unemployment, and with national economic policies relating to these issues.”

The concepts of Micro and Macro can be readily applied to an information security model. Micro-information security is defined as the technology, controls, countermeasures, and tactical solutions employed day-to-day to defend against cyber threats. It’s the nuts and bolts that support the corporation’s information security practice. It can be reduced to a step-by-step guide for securing the enterprise given the current set of requirements. By nature, it is fully reactive.

Macro-information security is defined as *business* structures and plans that influence and protect our enterprise. It is the “*big picture*” which can be leveraged to keep management in the loop. It’s the blueprint, framework, strategic plan, road map, governance, and policies designed to influence and protect the enterprise. It’s the *bottom line*.

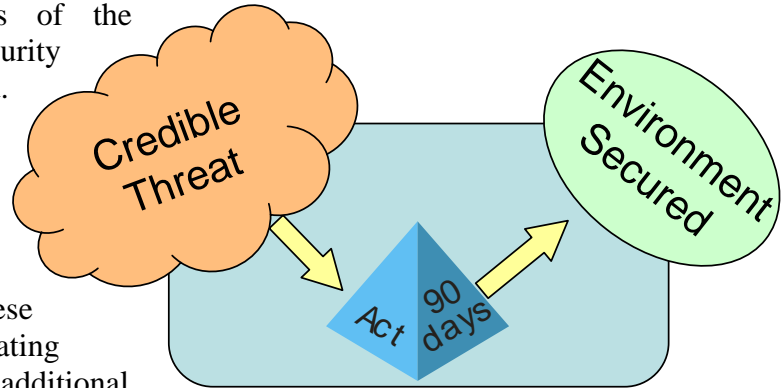


At this point it might be worthwhile to examine the corporations current and past information security practices to establish the historical foundation upon which we will build the next paradigm.

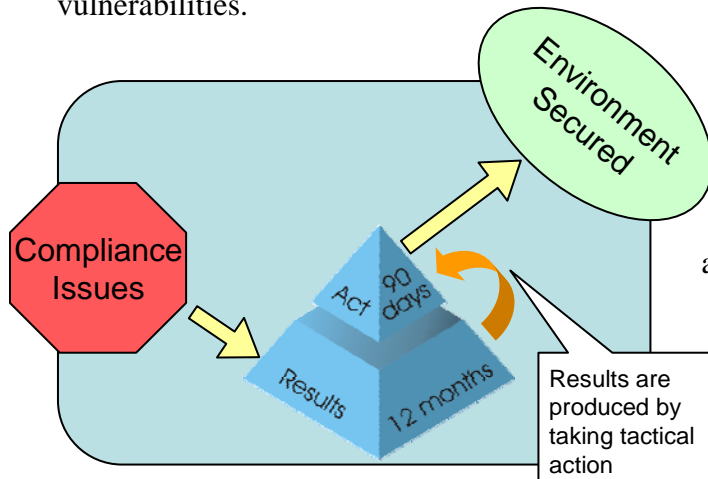
Background

Over the last 10 years, the security engineering team has been highly successful in addressing the security concerns of the enterprise. During this time, security engineering has steadily progressed. Initially, it utilized a highly-responsive threat-driven model.

Under this model, the engineering teams typically responded with solutions in 90 days. Many times these solutions were one-off fixes necessitating additional updates and/or presenting additional vulnerabilities.



At the same time, security engineering was working diligently to address compliance issues. While equally complex, there was greater latitude in the timeframe to address these issues.

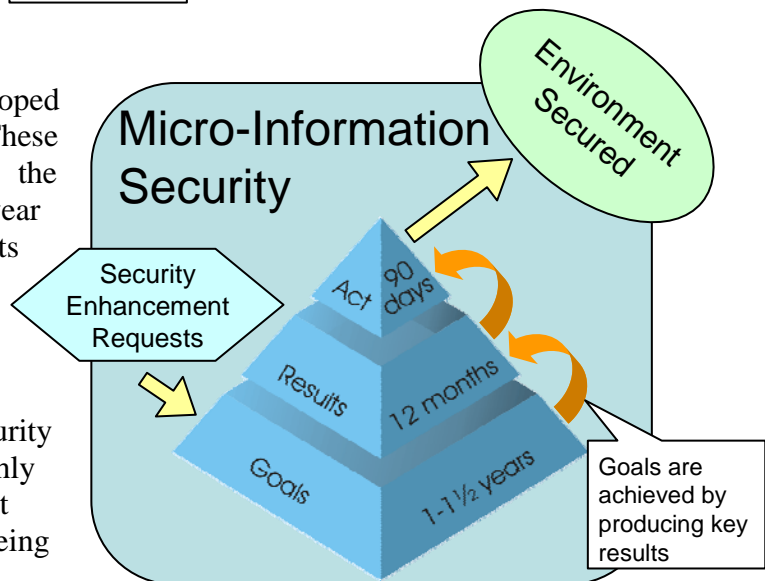


Corrective Action Plans (CAPs) were developed to address identified issues. These typically had a duration of 12 months and

were fully engineered solutions.

Finally, security engineering developed product roadmaps annually. These roadmaps served as establishing the target goals for the group in 1-1½ year timeslices. Typically, these requests were enhancements driven by the lines of business and/or the operations team.

Taken together, this has allowed security engineering and operations to be highly effective and successful. However, it has limited security engineering to being re-active to outside forces.



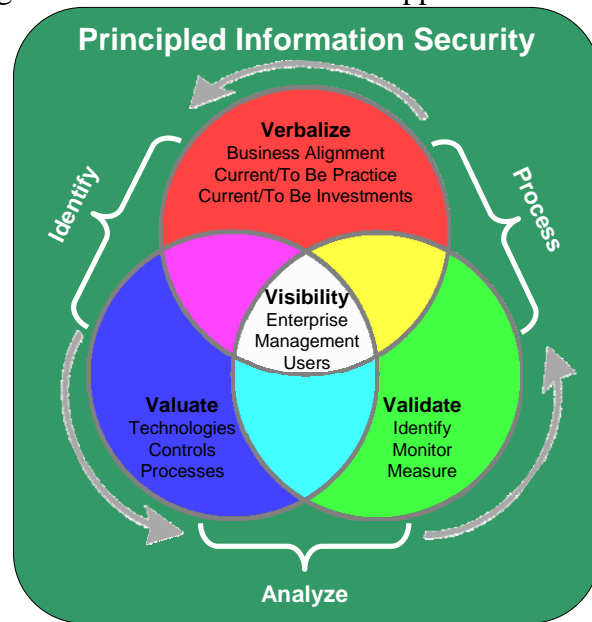
A paradigm shift is required for security to move from a re-active state and towards a proactive state. This shift can best be described as *Principled Information Security*.

Principled Information Security

Many of the corporation's information security professionals hold CISSP certifications. Ask them to define *information security* and they will faithfully recite the CISSP Information Security Tenants surrounding the Confidentiality, Integrity, and Availability of information. And that's OK, especially when having discussions among peers or when educating co-workers. However, they are probably not necessary for management presentations. Instead, information security can be conveyed as a *principled* approach, which may resonate better with management and non-security professionals.

The primary goal of principled information security is to raise information security's visibility to management such that it is considered for inclusion in all future business programs. This should not be limited to technology alone, but extended to business marketing and sales opportunities as a significant differentiator. This approach ensures success through the following principles:

- 1) Information security management, practices, and investments are verbalized in a manner that aligns with the business;
- 2) Controls, processes, and technologies are managed throughout their lifecycle to ensure the value proposition of the investment is sustained and possibly even enhanced;
- 3) Key investments are identified, monitored and measured on an ongoing basis for validation of their effectiveness.



Principled Information Security involves *Information Protection Stewards*, their programs, staff, and resources at the *onset* of every new business venture or project. It ensures up-front business alignment rather than after-the-fact input.

Information Protection Stewards

The concept and execution of information stewardship is nothing new within the corporation. We have recognized that our information assets are more than a valued corporate resource; it has significant value to entities outside our enterprise. Information stewardship, at its fundamental level is limited in scope to ensuring accountability. To this end, we have created Information Security Officers (ISO) and bestowed the title of Business ISO (BISO), Group ISO (GISO), and Technical ISO (TISO) on individuals for over a decade.

While the accountability of information use cannot be dismissed, the responsibility of protecting these assets – whether virtual, logical, or physical – is of the utmost importance. ISOs have become the de facto protection stewards in the company.

However, protection stewardship needs to extend beyond individuals with IT backgrounds and into the general enterprise in order to fully secure the constructs that enable our core business systems. Protection stewards include executive management,

legal, human resources, procurement, and any person or department handling information assets deemed vital to our ongoing operations and growth.

While education and training of our personnel has made strong inroads towards an understanding of each individuals' responsibility regarding protection stewardship, the bulk of effort has continued to fall on the information security professionals in the corporation to recommend and oversee the implementation of the controls and processes that protect us from cyber threats.

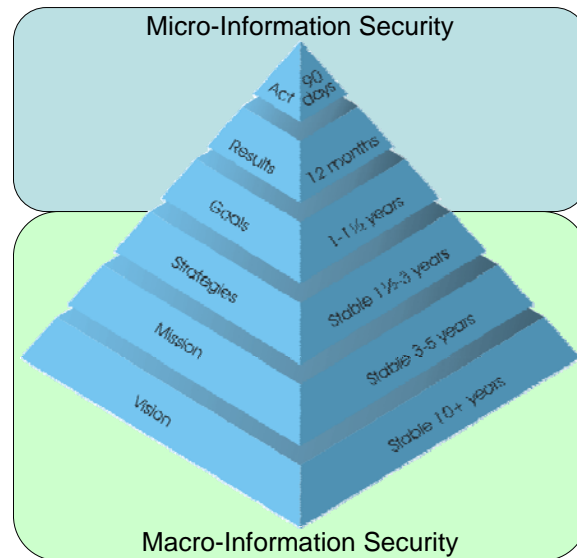
To be truly effective, protection stewardship needs to blend the tenets of information security, brand marketing, and business alignment. This presents a challenge, as most information security professionals in the company have a background in IT with a focus towards micro-information security. What is required is the paradigm shift towards the *principled information security* model. This may best be accomplished through the application of *macro-information security*.

Macro-Information Security

Economists figured long ago that in order to fully understand the economy, they would have to employ a two-pronged approach. The first approach would look at the economy by gathering data from individuals and companies on a small scale. The second would tackle the analysis of the economy as a whole. Thus was born micro and macro economics.

We can create an information security model that is better understood by borrowing from economics. By dividing information security in the same manner as economics, we get micro-information security and macro-information security.

Micro-information security is the reactive application of our technologies, controls and processes deployed on a day-to-day basis for defense against cyber threats. The corporate information security professionals have excelled at this and continue to provide world-class service. Where our security professionals could have more rigor is around business planning, i.e. *Macro-Information Security*.



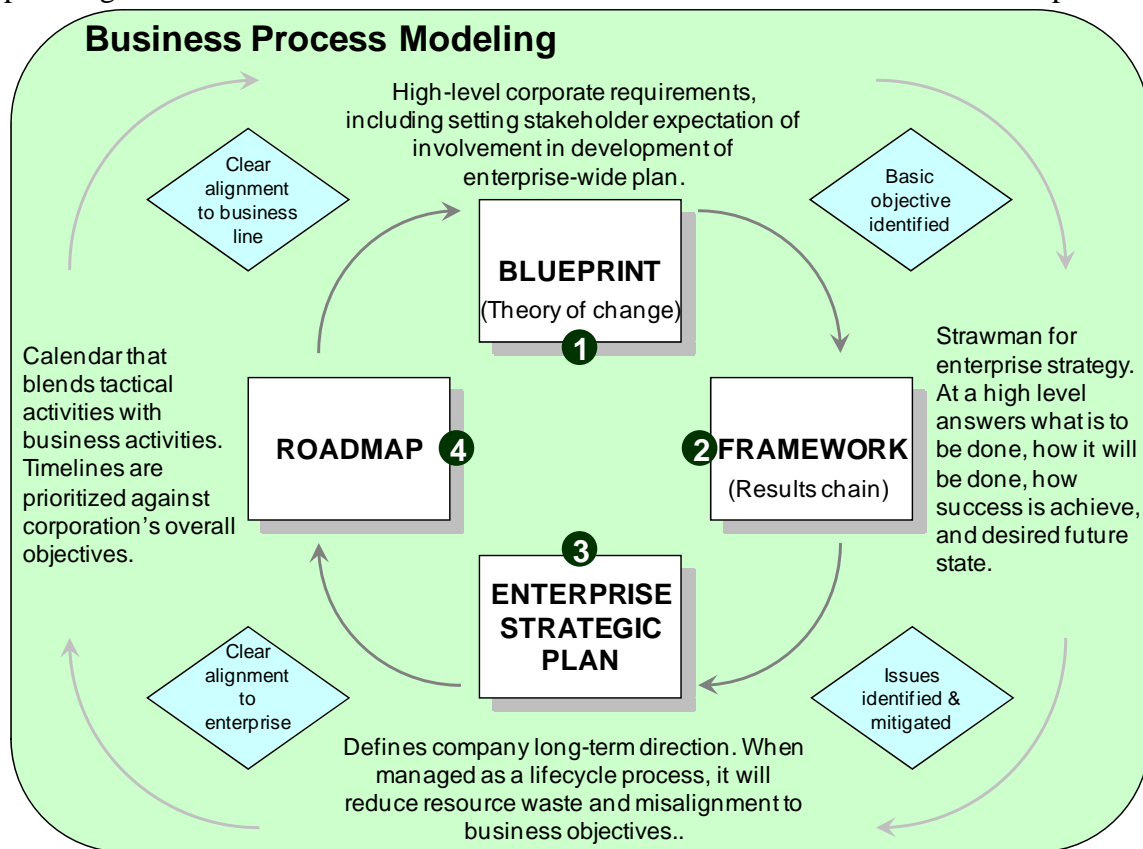
Macro-information security is the “big picture” that is designed to keep our executive management fully in the loop. It’s the stable strategic aspects of a multi-year plan designed to protect the enterprise while ensuring business alignment. It also extends externally to support our partners, customers and key vendors as well as ensuring compliance.

Macro-information security enables our security leadership to align the company’s security programs with the lines of business. It bridges *CISSP InfoSec-speak* with traditional business intelligence. When used correctly, macro-information security can be the tool that brings long-term success. And, success is being included in the planning stages for each new business venture, marketing campaign, or development project.

In order to plan strategically, our security architects, senior managers, engineering leads and operations managers must have an understanding of the business programs and objects that extends beyond IT. This understanding lends itself to the creation of concise and clear strategies and roadmaps that integrate security into the business sectors and show the value-add that information security can bring to the table, ultimately answering the question: “What is information security?”

Our business peers want to know the answer to this as well as why information security should truly matter to them. The typical business approach to answering this is through a strategic plan. However it can be tedious to focus on the technical details present in micro-information security roadmaps to those not well versed in IT and information security.

One method to address this and gain reasonable acceptance of a strategic security plan is to allow the business units to shape and mold the plan prior to it being formalized through an incremental, iterative process. Essentially, this means borrowing and applying traditional business process modeling techniques throughout the strategic security planning process.



1) Blueprint:

The goal is to gather enterprise-wide requirements, provide a visualization of those requirements, and continue the process of interweaving information security into the fabric of the corporate culture.

One approach is to utilize a *Theory of Change* logic model. Why? *Theory of Change* models stimulate critical thinking among stakeholders to identify early and intermediate accomplishments that will support sustained long-term change. These models help identify ways information security can provide positive impact to a business group, a sector, and/or the whole enterprise. Like any good planning and evaluation method for

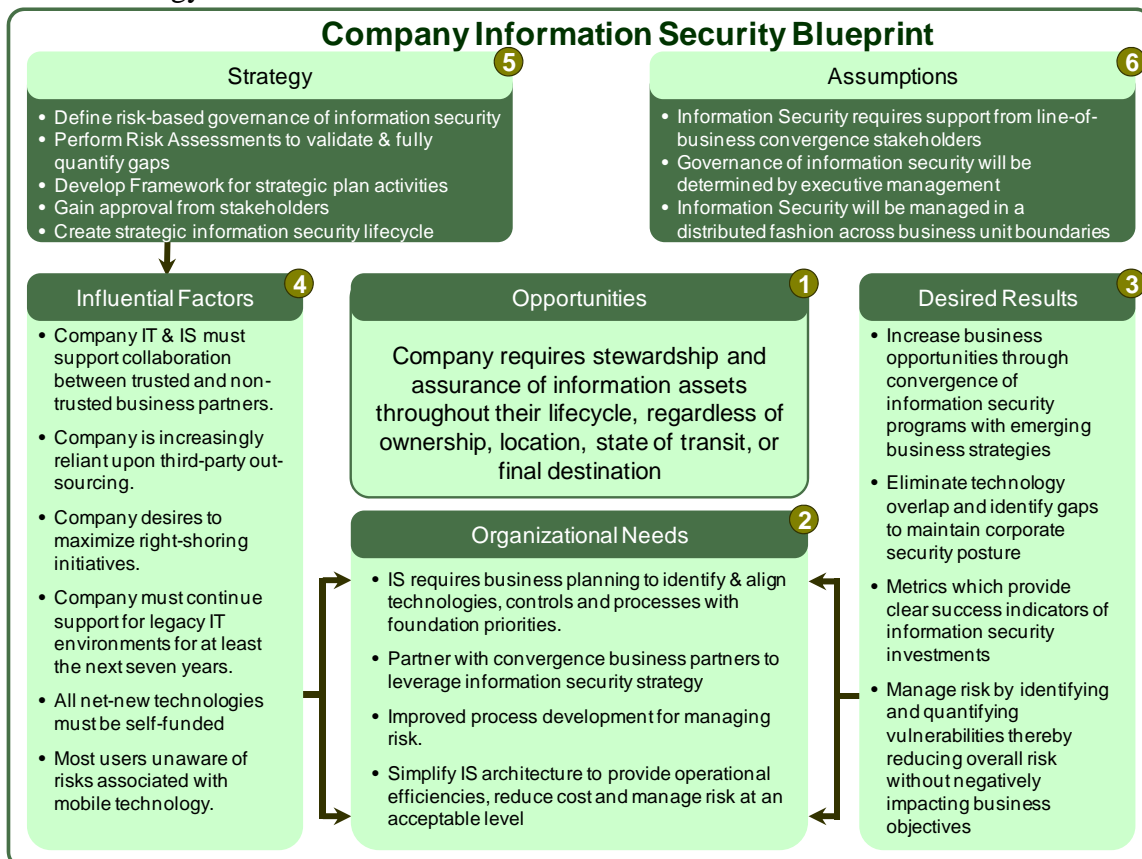
change, it requires participants to be clear on long-term goals, identify measurable indicators of success, and formulate actions to achieve goals.

It differs from any other method of describing initiatives in a few key ways:

- it shows a causal pathway from here to there by specifying what is needed for goals to be achieved.
- it requires us to articulate underlying assumptions which can be tested and measured.
- it changes the way of thinking about initiatives from what we are doing to *what we want to achieve* and starts there.

A *Theory of Change* model provides a high-level plan to get us from here to there. To do this, it should answer the following:

- 1) What do the lines of business, the sectors and enterprise require and what opportunities exist that can be addressed through information security?
- 2) What does the corporation need today?
- 3) What results should be reflected?
- 4) What factors will influence the success?
- 5) What strategic activities will be required to achieve desired results?
- 6) What conditions exist that are outside our zone of control that may affect the strategy?



Once the blueprint is completed, we will have re-defined information security in business terms at a very high level, engaged key business stakeholders, mapped out security priorities, and developed a long-term vision of information security within the company.

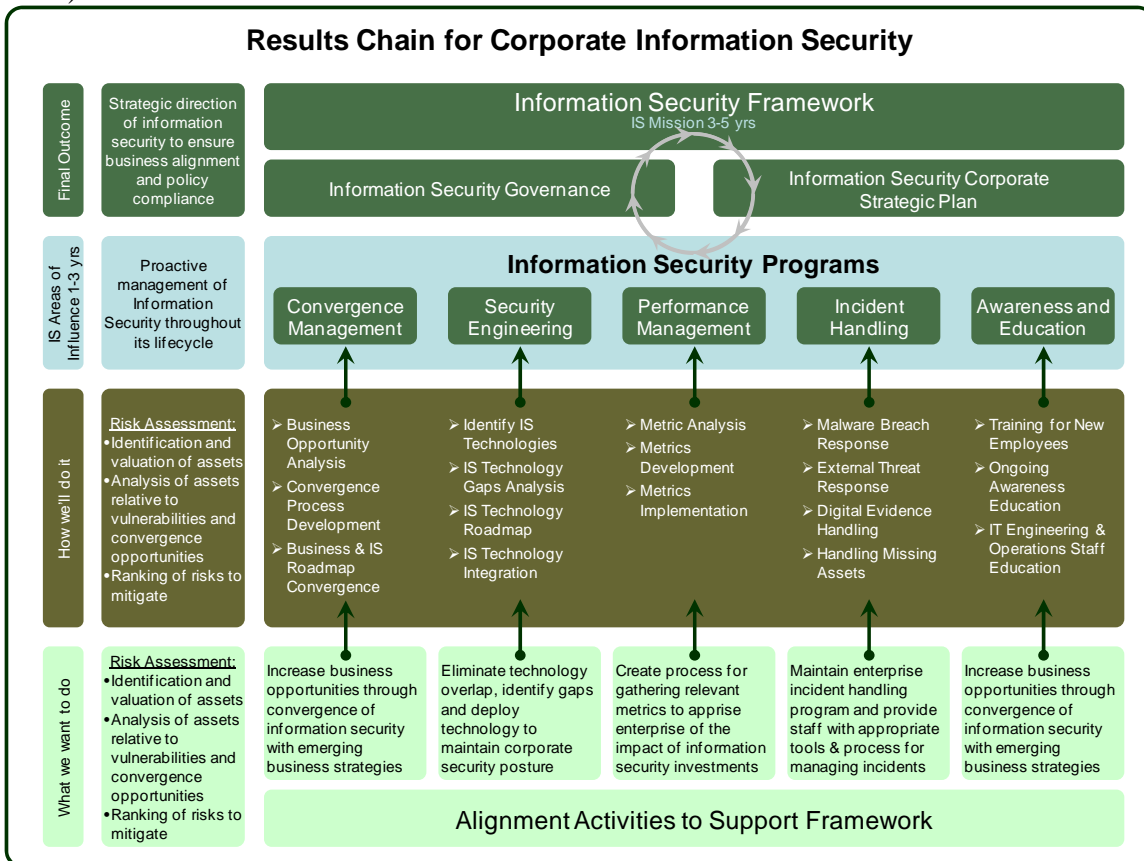
2) Framework:

The framework is based on the information gathered in the *Blueprint*. Use of a *Results Chain* logic model in building the framework allows us to clearly identify and present the high-level actions that will be taken to achieve the desired overall outcome. This five step process involves:

- I. Identify the driving forces/hindering forces impacting the vision conveyed in the *Blueprint*.
- II. Identify potential solutions and changes needed, generating a means-end model
- III. Analyze alternative strategies and prioritize results
- IV. Analyze conditions necessary for success – document risks and assumptions
- V. Develop indicators & identifying means of verification

Wider involvement at progressively lower levels within the organization is necessary to successfully build the framework as it is a comprehensive document. The *Results Chain* logic model provides a functional framework that answers these key high-level questions:

- 1) What do we want to do? What activities are required? This is a direct expansion of the results from the *Blueprint*.
- 2) How shall we do it?
- 3) What will be the rate of influence by years? This is a list of the major categories or programs that address what will be influenced.
- 4) What is the final outcome?



Completion of the framework yields a complete picture of the information security programs, the high-level activities necessary to build and sustain each program and identification of actionable goals. At this point it might be prudent to engage a third-party, such as Internal Audit, to perform a risk assessment, identify gaps, and validate the framework.

3) Strategic Plan:

The *Strategic Security Plan* defines the corporate information security’s intermediate direction, encompassing 1½ – 3 year event horizon. When managed as part of a business planning lifecycle, it can reduce resource waste and misalignment to business objectives. The information gathered in producing the *Framework* will be used in the strategic plan as major milestones.

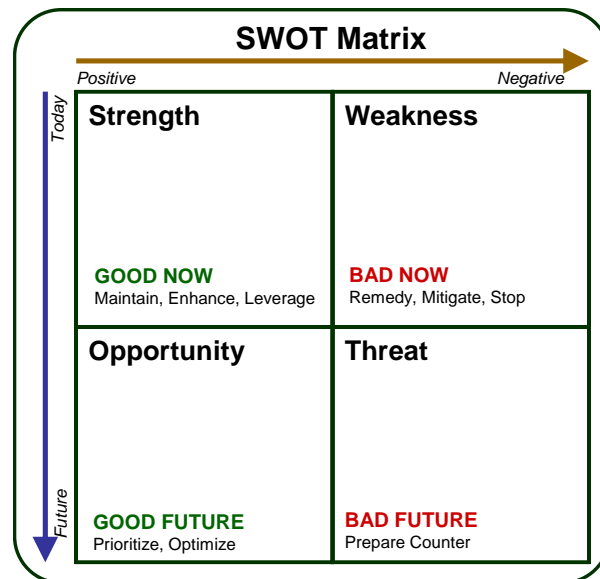
The body of the strategic plan contains the assemblies to be addressed. These are the targeted assemblies and the respective programs they roll up to, which were identified in the *Framework*. The assemblies are identified from the list of activities laid out in the framework document. Flowing from these targets are the components and projects necessary to achieve the targets.

Additionally, the plan will contain elements such as cost, people resources, and challenges. All targets identified in the strategic plan must clearly map to and support the corporate vision for information security, as defined in the *Blueprint*. For each identified program, the strategic plan will answer:



- 1) Where are we today? This should include a description of the current environment and is pivotal to justifying the identified activities.
- 2) Where do we desire to be? This should include the identified targets, their associated costs and resources.
- 3) What barriers exist and what are the critical success factors?
- 4) What are the drivers?
- 5) How will the plan be monitored?

To gather the information necessary to address these questions an *environment scan* should be completed and the results charted on an SWOT (Strengths, Weaknesses, Opportunities, Threats) matrix. This gives a good visible reference to work from that when coupled with the *Blueprint & Framework* will allow for successful completion of the *Strategic Security Plan*.



Quite often the planners already know much of what needs to go into a strategic plan, especially if they have been involved in the *Blueprint & Framework* processes. However, development of the strategic plan greatly helps to clarify those plans and ensure key stakeholders are all on the same page. Far more important than the strategic plan document, is the strategic planning process itself.

4) Roadmap:

The strategic roadmap is the functional calendar that blends IS tactical activities with business activities over a multi-month calendar. Its timelines and delivery schedules have been prioritized by the findings of the SWOT matrix and aligned with identified business convergence opportunities. It is the path taken to satisfy the targets in the strategic plan. This is the cross-over point from stable macro-information security to actionable micro-information security and serves as one of the drivers for annual goal setting and project planning activities. At best, when viewed in conjunction with the *Blueprint*, *Framework*, and *Security Strategic Plan*, the strategic roadmap will be easily interpreted by leaders from the business lines and those who support technology.

Together, they will communicate without requiring further verbal narratives the value proposition of *Information Security*. At a minimum, the road map contains the targets, high-level activities, destinations, timelines, milestones and interdependencies.

Once completed, the Macro-Information Security model will answer the question “What value does *Information Security* provide me”.

