Global Information Assurance Certification Paper

The evolution of the information security mindset: A hypothesis of Stages of individual and enterprise security MATURATION

Glenn Fourie

May 8, 2002

Abstract

This paper explores the evolution of individual and enterprise thinking around information security. A theoretical model of how corporations typically develop and mature in their security strategy is postulated with corroboration from some leading security consultants. The premise of this work is if you can gauge your security stage, you can not only manage it better, but could think through and possibly transcend intermediary stages to fast track you to the ultimate stage of being practically secure. The potential benefits of this work arise from minimizing activity that does not take you on the shortest path to the ultimate stage.

Introduction

Like many things in life, one's understanding of a concept is a catharsis; an evolutionary process as the knowledge gained systematically shines light into the darkness of ignorance. Is there a parallel that applies to security? Could the way companies think about and react to security challenges follow some type of pattern?

Individuals experience paradigm shifts that galvanize them into evangelism of some new security strategy, or renewed support for a management idea. The catalyst that triggers these responses can be anything from a newspaper-caliber exploit which rocks the organization, to something as simple as someone stumbling over a really dumb thing a developer did to open a security hole. This paper is an attempt to establish if there is a pattern to this maturation process. This is an effort to quantify some possible milestones along the road of security maturation. Having identified some of these milestones, enterprise management would possibly consider strategies to effect the end-point sooner than would otherwise be reached.

Methodology

To establish what companies go through as their security-awareness matures, analysis of documented security behavior is warranted. There is unfortunately a dearth of published material on this topic, most security related thinking studies seems to have focused on the mindset of the hacker, instead of that of the hacked (Rogers, 2000; Gordon, 2000; Quitner, 2002,: Shaw *et al,* 1998). A few models exist and are discussed later, but more commonly documented are cases of enterprise response to threats and even cataclysmic examples like the September 11, 2001 terrorist attack (Armour Group, 2001). It was the information gleaned from personal communication with respected security professionals (Fossen; Prosier; Shunn) that confirmed there was merit in what was alluded to in published material. It was the experience of these professionals that is of particular interest, because they are seasoned consultants. As such, they get exposure to many companies, and almost always engage the leadership on strategies to secure their organization. This provides valuable insight to the questions of patterns and the thesis of thought evolution.

Stages in Security Thought Evolution

What follows is a postulation of the different macro security stages employees, and by implication, corporations may experience. Though executive management, technical, business and product management staff may individually be at different stages at any one time, the stage that applies to the enterprise is the one which best describes the bulk of the employees.

The stages are summarized below:
Stage 1 – **Ignorant** – where the bliss of ignorance causes no discomfort
Stage 2 – **Awake** – where some catalytic event breaks a core paradigm
Stage 3 – **Vulnerability Flood** – knowledge exposes the scale of the problem
Stage 4 – **IDS** – Fighting back
Stage 5 – **Forensics** – Building in the non-repudiation components for prosecution
Stage 6 – **Practically Secure**

In more detail, these stages could be characterized by some or all of the following activities:

Stage 1 – Ignorant – where the bliss of ignorance causes no discomfort.

This is the condition where the bliss of ignorance causes no discomfort! People may even be engaging in brief security discussions when building some applications, but these are typically focused in isolated areas, use out-dated technology or worse, implement "security" into applications out of step with the real world, thus giving a false sense of security.

The over-riding common characteristic of this phase is *ignorance*. This ignorance extends to the hostility of the internet or the nature of hacking, tools and ease with which vulnerabilities can be introduced into a system through procedural or systemic issues in application development or poor installation practices.

Characteristics of this Stage

- There is a pervasive ignorance of the hostility of the internet and the current state of hacking, including hacker tools, techniques and exploits.
- There is a belief that systems are generally secure, being patched and never have been hacked without measuring any of these to get the real picture.
- Management has an unrealistic trust of their team's diligence and knowledge regarding security
- Security planning and design in applications tends to be out of touch with reality and often misdirected.
- Security audits may in fact be undertaken during this stage on key systems, but often the auditors used are also not in touch with the real world and primitive security fixes are recommended
- Sensitive documents are not secured – like database models on passageway walls as decorations
- The enterprise does not appreciate the value of its assets at risk.
- The focus of business is to keep the operation going and IT budgets and activities are driven to that end.

Stage 2 – Awake – where some catalytic event breaks a core paradigm

This is the condition where some event brings security into focus. This can be an exploit, sometimes publicly made known or even just a key person gaining some insight of current hacker practices, often from a training course. In most cases this acts as a catalyst which reverberates through senior management – initially with only a few believers and the rest somewhat skeptical that the situation is as bad as the evangelists are saying. This phase triggers a call to action, most significant of which is a

plan to measure/audit the condition. Sometimes the catalyst is a hack that has a devastating consequence, like the Homepad Domain Service. Their status page detailing their trials after a successful exploit caused them to conclude they needed to re-architect their systems (Homepad, 2000).

Auditing the systems on a large scale is a common response during this stage. Typically companies audit only myopically or not at all, until a catalytic event occurs. (Bernstein, 2000).

Components of typical post-catalyst actions are detailed below:

Characteristics of this Stage

- A security breach or a key person gains knowledge which acts as a catalyst to get a critical mass of management to appreciate that there is a security problem
- If this was an exploit, most people still believe this was an isolated event and that the remaining systems have never been hacked – though typically they cannot prove otherwise because it is not measured.
- The security evangelists get enough momentum to conduct an inventory of applications operated by the enterprise, with a view to prioritizing an audit of those considered most at risk.
- If the auditing team used has the necessary skills, this results in a mass of vulnerabilities being recorded, which heralds the next stage.

Stage 3 – Vulnerability Flood – knowledge exposes the scale of the problem

As the auditing process proceeds, the reality of the situation starts to dawn to more and more employees. This typically results in more audits of other systems in the enterprises. The gap between the increasing number of believers and the skeptics become more visible.

Characteristics of this Stage

- The process of auditing the systems results in far more recorded vulnerabilities than anyone expected.
- This triggers audits of other systems in the enterprise, which in term results in more recorded vulnerabilities.
- The management of patch and deployment gets more attention and accountability loops could be setup to address the state of servers in the enterprise. Policies are starting to emerge.
- Application development, infrastructure teams and especially business people, find the concepts and mechanics of the vulnerabilities hard to

understand and foreign.

- Some naysayers often call the evangelists bluff by requiring them (or the auditors) to prove that a particular vulnerability is potentially as devastating as alleged – usually resulting in a spectacular demonstration which immediately settles the argument!
- Mechanisms are set in place to manage the vulnerabilities and track their remediation to completion
- Key individuals are sent for quality security training which rewards the enterprise with more accurate planning for the real world and a better focused strategy.
- At this stage the entire enterprise focus changes to security and business activities take second place – particularly as demonstrated in budgets and human activity.
- The executive starts to call for accountability and this often leads to heated discussions of how the situation was allowed to get so bad in the first place.

Stage 4 – IDS – Fighting back

Soon it becomes apparent that with all these vulnerabilities, no-one can unequivocally prove the exact extent of any exploits other than the obvious - like web-site defacement. The next course of action follows when it is felt that the network is adequately under the control of the System Admins and that all reasonable steps have been taken to secure the network, though the need to know when an attack was taking place is still a nagging issue (Fratto, 2000). The realization triggers interest and investment in an IDS and initially, or in the latter parts of the phase, people start discussions around deploying honeypots.

Characteristics of this Stage

- Intrusion Detection Systems are now deployed to address both the state of hosts and network segments.
- The results are usually staggering and further prove how out of touch the enterprise has been
- Security departments (newly created and existing) get staffed to entrench security into the organization's processes, thinking and applications deployment.
- Applications start to get developed with security from the ground up instead of applying it as a Band-Aid™ remedy to harden a system
- Bastion servers are created as a new generation of systems is deployed.
- Enterprise legal staff is engaged.
- The first criminal proceedings are considered which points out that

inadequate evidence has been gathered – heralding the transition to the next phase

Stage 5 – Forensics – Building in the non-repudiation components for prosecution

The realization that more infrastructure and better processes are need to effectively prosecute criminals attacking the enterprise's systems characterize this phase. Steps taken to address are then implemented.

Characteristics of this stage

- Enterprise legal staff are seriously engaged
- The requirements for evidence for prosecution are defined and the enterprise is found to require further steps and infrastructure to effect these.
- Infrastructure like time-stamping systems, refined log management, better profiled IDS systems and particular attention for prosecution modifies security activities in the enterprise.
- Exploits are also getting fewer as the hardened systems are now holding up to the attacks much better.
- Honeypots continue to attract script kiddies and packet monkeys
- Security is becoming entrenched and pervades thinking of even the most junior staff.
- The first successful prosecution transitions the enterprise to the next stage.

Stage 6 – Practically Secure

This stage describes the enterprise that is as secure as is practical; marrying business, IT and operational interest together to result in a reasonable compromise. Security-mindedness is pervasive, from the most junior staff to the executive. Every one appreciates the reality of this situation that one can never claim to be perfectly secure, but only secure enough.

Characteristics of this stage

- Systems are significantly hardened
- Audits yield very little evidence of vulnerabilities
- Criminal prosecutions continue
- Sensitive information is available to those to who need to have access to it and there are few cases where people have access to more than they should

- Security mindedness is pervasive throughout the enterprise
- Focus returns to business priorities
- Checks and balances are built into the development and deployment of all systems
- Testing of systems (drills) for business continuance, massive denial of service attacks and physical calamity occur at regular intervals

Discussion

In the preceding section describing the stages of security maturation, a model of security thought-development is presented. What needs to be addressed is:

- How does this model compare to any others?
- What detracts from the realism of the model?
- What can be learnt from the model?
- How applicable is the model to fast-tracking an enterprise to the latter stages?
- Is there a central theme to the model?

How does this model compare to any other?

Clearly something as obtuse as predicting enterprise security response - or even individual response given the diversity of IT professionals / management – is as best to be considered with suspicion. However, do we go to the other extreme and declare there is neither point nor value in trying to postulate 'typical' patterns, or more accurately, commonly observed responses. When someone dies, we are after all likely to grieve according to the celebrated five stages the psychologists tell us we should anticipate (Kubler-Ross, 1969). Why should we respond to the shock of a major exploit in our systems any differently - albeit not with such deep emotion?

Another model of enterprise security evolution is described in an ArcSight IDS product brochure (ArcSight Corporation, 2002, p.8). The stages proposed are:

1. Awareness
2. Focus
3. Consolidate, Optimize & Manage
4. Extend & Enhance
5. Configure & Control

In contrast, the ArcSight model sees enterprise awareness as stage one: "The first stage of security maturity is characterized by awareness-an enterprise knows that security issues exist". This seems implausible, because clearly there are companies out there that are not aware and have not begun their journey of security maturation. In fact, it would appear that the ArcSight model is more oriented to stages of evolution in the context of deploying an IDS system – which should not be surprising given that the material is presented as a product backgrounder.
Another model of Enterprise Security Maturation is presented by Jeff Recor of Nortel Networks (Recor, 2001). This model presents five stages of maturity:

1. Minimal
2. Aware
3. Functional
4. Integrated
5. Enlightened

This model is considered by the author as more probable than that of ArcSight because it at least provides for a pre-aware state. A notable component of this model is how security focus wanes in stage 3 (Functional) as described as follows: "However, once the initial studies have been done, the protection strategies developed, and the security measures installed, the intensity for information security diminishes".

How an enterprise evolves after this period is clearly pivotal in determining how integrated and effective their security culture will be. As Recor points out, after the top-down security mandates characterize stage 3, it is a bottom-up phenomenon which indicates the advent of Stage 4. This rings true as security focus shifts from management and the security team into the mindset of every employee – a quantum increase in the number of eyes looking out for security issues.

eSecurityOnline is an Ernst & Young LLP enterprise that has proposed a Vulnerability Management Maturity Model (VM3), a security maturity framework (eSecurityOnline, 2001).

This model proposes three stages, namely:

1. Knowledge
2. Deployment
3. Accountability

They postulate that stage 1 describes companies having gathered security knowledge in systems and not having a sustainable, repeatable process to manage it and any incidents. Again this ignores companies in some prior stage of security ignorance. The Deployment Stage describes where these processes are in place and the final Accountability Stage where measurement with consequences is entrenched. Again, this model appears more geared to a consultancy methodology than to a universally applicable model for enterprises information security maturation.

What detracts from the realism of the model?

As already mentioned, it is a near impossibility to develop a universally applicable model of security evolution. This stems from the diversity of people, and by implication enterprise thinking, culture and your staff's subjective response to the subject of security. As is often borne out, security staff will allude to the widely different response of employees to a particular security issue. This appears to some extent, related to how one's own prejudice influences your openness to new ideas. People for example that have been subject to a period of stringent military disciple, say, having been in a country where they were conscripted, are more likely to understand the thoroughness with which security needs to be applied in order to be effective. Does this mean that humans - and consequently corporations - are so diverse as to not try to model something like this in the first place? Probably not - if you are one of those who can at least buy into the concept that there are general trends and attitudes that apply to much of what we do and how we behave.

One of the most significant detracting factors includes national culture; some cultures simply respond to - and embrace discipline - differently than others. This as much applies to how long the skeptics take to be convinced as much as it affects the how fast the vision of a secure enterprise is assimilated by employees who in turn determines their changes in behavior.

Another key factor, considered by the author as significant, is that of the enterprise attitude to training. Clearly, if enough people in an enterprise are exposed to quality security training, the prevalence of Stage 1 would - by definition - be short-lived, as ignorance could not survive for very long.

To some extent the financial standing of the enterprise plays a part. This may be – for example - directly related to training. Consider if management simply decreed that exotic training (often considered a luxury) is on-hold

until some financial situation improves. However as mentioned above, out-of-house training is often what is needed to provide the catalyst to initiate a transition to Stage 2.

What can be learnt from the model?

The model describes a path followed by a number of companies on their security journey – in part or in total. It has value in that those who review it and hold their own prejudice against it, may find parallels to their own situation. Hopefully this then sparks thoughts of how they can influence their situation. As a manager, one may consider re-thinking ones current security strategy - now with an end-point a little clearer than before. As a security worker, this may precipitate a commitment to seek out and assimilate the best training available. To a business person, the impact may be one of re-thinking how business processes may need to be re-engineered to minimize security exposure.

How applicable is the model to fast-tracking an enterprise to the latter stages?

The model has not yet been tested for its ability to change an enterprise from its current track to one where future stages are anticipated and multiple projects kicked off to expedite Stage 6. By implication, a healthy dose of skepticism should be employed. Again, enterprise culture and agility are factors in determining how well an enterprise will respond to a stimulus of this type. It is the authors hope that this indeed does occur – even if the entire model is not adopted in its entirety for an enterprise's situation.

Is there a central theme to the model?

To find a central theme to the model, one needs look at the role that knowledge plays in each of these stages. If the management of an enterprise knew the path that companies took in their evolution of security and resultant behavior, they would not make the same mistakes. Of the influencing factors described above, the author's opinion is that training is the most likely antidote to the malady of insecurity. When enough of an enterprise learns from the knowledgeable, security can be entrenched. Even discipline can be effected through policy when there is accountability.

Conclusions

A theoretical model of the evolution of enterprise thinking and response to information security is presented, which is borne out by some noteworthy consultants in the field. The key factor in determining if it can be used to change the way an enterprise will respond to the security challenge, is postulated to be a commitment to security obtained through specialized knowledge. The nature and quality of security training is considered to be a key element in security thought maturation. Conclusive remarks can only be made once a statistically significant sample garnered through further research proves or disproves the viability of the model presented. None of the authors of other models reviewed in preparing this paper presented any evidence that their model was based on statistically tested research.

References

ArcSight Corporation Product Backgrounder. "Security Management for the Enterprise". *ArcSight Corporation.* 2002. P8.
URL: http://www.arcsight.com/graphics/news/ArcBckGrd.pdf (2001)

Bernstien, David S. "We've Been Hacked" *Inc. Magazine*
URL: http://www.inc.com/search/20252.html (1999)

eSecurityOnline. "Online Methodology Framework". *eSecurityOnline*.
URL: http://www.esecurityonline.com/products/vm3.asp (2001)

Fossen, Jason. Founder and President of Fossen Networking & Security; Faculty Member of SANS. Personal Interview. 2002.

Fratto, Mike. "Knowledge is Power". *Network Computing*.
URL:
http://www.networkcomputing.com/columnists/1114colmike.html (2000)

Gordon, Sarah. "Technologically Enabled Crime: Shifting Paradigms for the Year 2000." 2000. Originally published in Computers and Security magazine. *Published by Elsevier Press' Computers and Security 1995*
URL:
http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html (2000)

Homepad Status Page. URL: http://www.homepad.com/html/status.html (2000)

Kübler-Ross, Elisabeth. On Death and Dying, *Tavistock Publications*, London, UK.1969

Prosier, Chris. Vice-President of Customer Service, Foundstone Corp. Personal Interview. 2002

Quittner, Jeremy. "Hacker Psych 101".*TLC Online*
URL:
http://tlc.discovery.com/convergence/hackers/articles/psych.html (2002)

Recor, Jeff. "Security Services to Enable your Business". *Nortel*

Networks Global Security Practice.
URL:http://www.nortelnetworks.com/enterprise/events/2001a/gps_sec/quiz.html (2001)

Rogers, Marc. "Psychological Theories of Crime and "Hacking" ". Graduate Study. University of Manitoba.
URL: http://www.escape.ca/~mkr/crime.doc (2000)

Shaw, Eric, Keven G. Ruby and Jerrold M. Post. "The Insider Threat to Information Systems." *Reprint from Security Awareness Bulletin.*
URL: http://www.escape.ca/~mkr/sab.pdf (1998)

Shunn, Arjuna. Security Consultant, formerly of Foundstone Corporation. Personal Interview. 2002.