Strategies for Achieving Network Intelligence

Adam D'Amico
Zanshin Security, LLC
adam@zanshinsecurity.com

June 20, 2005

Abstract

In order for security efforts to be effective in the contemporary threat environment, network professionals who have some responsibility for operational security or incident response in an organization will need actionable knowledge regarding network activity. This paper describes a strategic model for implementation of appropriate technologies, policies and procedures in pursuit of that goal. The content is not meant to be an exhaustive methodology, but rather one possible paradigm based on lessons learned in several distinct categories of organizations over the past decade. The approach will be most relevant to those in positions of management, but will also present information useful to anyone wishing to better understand the issues that surround network monitoring and security.

1 Introduction

The baseline practices of incident response evolved during a time when technologies for network monitoring were nascent at best, and the result has been a predominance of reactive, rather than proactive, security postures. Unfortunately, network and information security are pursuits subject to the well-known "Red Queen" phenomenon of evolution; it will always be necessary to move faster just to stay in the same place. Network administrators wishing to advance in the security arms race and adopt a more proactive posture need considerable information resources at their disposal, not the least of which is some kind of knowledge about how exactly the data networks under their management are being used.

Drawing on the author's professional experiences, including six years as a member of the security team at a large research university and several years as a consultant and strategist in the private sector, this paper will identify the need for such knowledge and present a framework for the formulation of strategies by which it may be attained. The intent is to show that the mechanical processes of network monitoring, auditing, or intrusion detection are not end states in themselves. The proper, precise combination of tools and practices can gain network professionals a superior class of actionable knowledge. The phrase "network intelligence" will be adopted to capture this concept. For purposes of this discussion, it will imply no specificity; rather, it will denote only the types, breadth and depth of information that would be of ultimate value to the implementor. By treatment of network intelligence in the business context, the resulting strategy will gain better traction with management organization-wide, in both technical and non-technical arenas.

2 Confirm the Business Need

Before becoming immersed in the organizational and technological minutiae of designing network intelligence, steps should be taken to ascertain that any solution would in fact address a problem that affects the organization's core mission. Although it is almost always advisable for network professionals to have this knowledge, it may not always mean that a broad-based strategizing exercise needs to be undertaken if the wider business need is not present. At the same time, recognize that the absence of explicit business need *now* in no way suggests that it will not appear *later.* Any network administrator who, at present, is comfortable and content with a less-than-complete picture of what is passing over the wires must keep in mind that the rapid growth of Internet use, and the resulting rate of environmental change, guarantee that the question will be called with some regularity. In view of that fact, benefit could be realized early from thought experiments regarding the basic focus of future network intelligence, for example collaborative incident response or auditing.

2.1 Internal Drivers

Within an organization, users of information resources share a desire for confidentiality and integrity of various types of information. The organization itself, as an abstraction from individual users, will also have such a desire, and typically policies will be in place to balance the two. However, it can be difficult to assess policy compliance without a thorough understanding of how data networks are being used.

As Internet usage grows, it is important to be able to classify and prioritize the traffic on data networks. When a network administrator faces problems with the performance or reliability of the network, solid network intelligence of this type is needed to execute an informed response. Increased Internet usage has also typically paralleled greater organizational dependence on IT as a whole. Forces driving economization of IT operations might prompt management to investigate network intelligence initiatives with the goal of reducing total operational cost.

2.2 External Drivers

Because the Internet is a shared global resource, network administrators are expected to make best efforts toward good citizenship. Lapses can cause significant reputational damage and embarrassment to the organization. Having a reputation for poor citizenship can create obstacles to collaborating with other organizations, and make it difficult to maintain credibility with peers in the security field.

High-profile scandals in recent years have caused regulatory concerns to take center stage with regard to IT governance. Educational institutions face the Family Educational Rights and Privacy Act (FERPA), publicly-traded corporations are now subject to the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act (HIPAA) looms over any organization that touches healthcare. These three examples are the most widely-recognized and broadly-applicable, but no matter what the core business of a given organization, it is highly likely that compliance pressure will be present, whether directly or indirectly through partners or customers.

Concerns of citizenship, reputation and compliance all contribute to the case for attaining a complete view of network activity.

2.3 Source of Initiative

One important aspect to consider when developing a network intelligence strategy is where in the organization the initiative originated. In most cases, network administrators themselves will be the initiators, and this is the desired scenario. However in rare instances, the suggestion will filter up from below, or may be handed down from above.

In the case where management at a higher level announces a requirement for network monitoring, care should be taken to ascertain that such a system will in fact address the perceived problem. Marketing hype, media sensationalism, inscrutable jargon, and bandwagon forces can sometimes prompt non-technical managers to dabble in areas where their lack of expertise becomes a liability. It may be that what upper management really wants is a way to capture usage data for metering and billing, or a policy-based traffic shaper. Network professionals will need to learn how to "manage up" in these situations in order to maintain the integrity of IT strategy.

If the call for network intelligence originates from below, network administrators will have to examine why systems already in place are not meeting the informational needs of lower-level IT staff. The real motivation might be "cool factor" or a desire for newer, better toys to play with. On the other hand, staffers who perform the daily hands-on tasks related to security or network operations will often have the best visibility to changes on the horizon, and hence their suggestions should be given appropriate weight.

2.4 Threats

Ideally, any system for collecting network intelligence will be designed and implemented in response to some threat or collection of threats, and not merely for its own sake. If the operational purpose of such a system is not explicitly stated and known, it is more likely to be subverted for other, perhaps inappropriate, uses. Beyond the initial identification of threats, it is also useful to categorize and examine them at a lower level.

There can exist a wide disparity between threat perception and reality. A threat perceived by other groups within the organization may translate to a distinctly different threat that is real, or may simply not exist at all in the real scenario. Alternatively, de-prioritizing a perceived threat, which may gain legitimacy over time, in favor of issues that are immediately critical can lead to unpleasant surprises when the environment merges perception with reality. Careful triage of asserted threat models can reduce the complexity of system requirements and build better overall preparedness.

In other instances, some threats may be of a mandated nature. This circumstance essentially conflates the real and perceived classes. Whether due to regulatory compliance pressure, immutable internal policy, stubborn leadership, or other organizational dysfunctionality, a mandated threat is best approached as a necessary evil to be included in system design.

As a final note on threats, it should go without saying that network professionals must always design with an eye toward the future. The nature of threats will always be changing at a faster rate than the set of solutions, and network administrators are typically called upon to implement technology that is several months old, at best, in response to problems whose ages range anywhere from minutes to weeks. In recognition of this, an examination should be made as to whether it is the correct strategy to favor flexibility, extensibility, and upgradeability in solutions that are evaluated, possibly at the expense of other attributes.

2.5 Liability

While working to confirm a business need for network intelligence, it is also prudent to consider the possible existence of contrary motivations. The example that most immediately manifests is the extent to which acquiring network intelligence may create liability. Particularly for organizations that could be considered common carrier service providers, gathering certain types of information can lead to awareness of illegal activity. Beyond the question of whether or not the organization wishes to dig that deeply, the further question of whether detected illegal activity should (or must) be proactively reported is of great import. Depending on the legislative and regulatory environment, failure to make such reports could lead to undesirable consequences. Careful combing of internal policies or perhaps consultation with legal counsel will be necessary.

2.6 Urgency

The existence of any time dependency for a network intelligence initiative will greatly affect other decision points further along in the strategizing process. Network professionals who find themselves with an urgent need for a solution in an abbreviated time frame will need to short-circuit some elements of an otherwise wholesome system design. In such cases, comprehensive research and evaluation, full flawless integration, and fine customization would be examples of potentially unaffordable luxuries. Any network administrator under time pressure will have to be resigned to the possibility of implementing systems that lack in terms of cost, coverage, adaptability, and maintainability.

At the same time, it is important to keep in mind that the fear factor present around some issues of security can make true urgency difficult to measure. The urge to act with swift decisiveness should always be given a cursory "sanity check" in order to make sure that such action would not exacerbate the situation.

3 Evaluate Solution Options

Having identified the business case for adopting a mature network intelligence strategy, the next step is to begin the design and appraisal of technology/process option bundles.

3.1 Target Environment

The nature of the environment into which a network intelligence system will be deployed is the earliest determinant of major design parameters. Evaluating the network according to the following characteristics is useful in narrowing the field of potential solutions.

3.1.1 Network Size

As one might expect, gaining network intelligence for a collection of a few hundred nodes is a very different problem from that faced by sites with many thousands. Some software and hardware solutions simply will not scale to the degree needed by larger networks. Some others might scale, but only at costs that quickly become prohibitive.

3.1.2 Device Distribution

Networks that are widely dispersed, either in terms of geography or topology, will require a different breed of solution than localized networks. Systems that do not support the appropriate types of interconnects, or that cannot operate with multiple points of presence, may be able to be eliminated early based on these factors. Another point to consider is how various systems deal with the occurrence of multiple copies of the same traffic. In the case of a highly segmented network, local traffic may be seen as mirror images by distributed sensors.

3.1.3 Openness

The relative open *vs.* protected nature of a network comes heavily into play when pursuing a network intelligence strategy. Unprotected or uncontrolled networks will have greater tendency to produce "noise" in network intelligence systems, while sites with stringent perimeter or second-tier security will exhibit traffic patterns that are much easier to rationalize. Solutions must be evaluated on the capability to tune the reporting volume to an appropriate level, with an acceptable configuration and maintenance commitment.

3.1.4 Platform Constituency

Heterogeneity *vs.* homogeneity among the platforms represented on a given network is another important dimension along which to measure the expected effectiveness of a network intelligence solution. The detection or reporting capabilities of some solutions may be more oriented toward a particular operating system, or may not be able to cope gracefully with rare, special-case platforms. Event correlations can become problematic when behavior that is undesirable on one platform is exhibited safely by another.

3.1.5 Integration Requirements

Integration requirements, whether at the network, platform, or application level, can present a formidable challenge when implementing a network intelligence system. Especially where proprietary solutions come into play, network professionals may find that the effort involved is well outside the comfort zone. Access controls, administration, reporting mechanisms and data formats are all prime examples of integration items that can monopolize a deployment, causing time and effort to spiral out of control.

3.1.6 Demographics

Understanding and classifying the user base of the network will help to inform the choice of tools used in gathering network intelligence. If network use occurs with relatively regimented timing, and consists generally of a small range of tasks (as would typically be the case in a bank), this would allow fairly straightforward classification of network traffic patterns. If, on the other hand, network usage is less time-constrained and the user base is very heterogeneous (as is the case for most higher education sites), network administrators must be prepared to perform much more rigorous analysis and segmentation of network activity.

3.2 Technology and Approach

A snapshot of the current state of the art for systems related to network intelligence gathering reveals a remarkable diversity in both high-level approaches and low-level mechanisms. Applicable tools on the market may bear monikers such as Intrusion Detection Systems, Flow Monitors, Network Traffic Probes, Security Information Managers, Audit Generators, or other clever rearrangements of synonymous terms. Keeping current with the momentary alphabet soup of acronyms requires no small span of attention.

3.2.1 General Classifications

At a high level, the realm of devices and applications that can fit into a network intelligence strategy can be classified as follows:

General-purpose sniffers and monitors. Tools in this category are handy in the small scale of operations, but lose their effectiveness when the target network achieves a certain critical mass of size and complexity. Examples include Iptraf, Ntop, and the venerable Tcpdump.

Accounting and/or auditing tools. These are network capture systems oriented toward output in the middle range of detail. Some can be used as a basis for metering bandwidth consumption. IPAudit and Argus are typical examples.

Scanning and discovery tools. In larger networks and environments that are geographically distributed, there is higher likelihood of unknown devices appearing on the network. Administrators will find it beneficial to make use of tools like netdisco and SolarWinds Network Discovery. These allow for the identification of network devices via various methods, and can provide information about topology and platform constituency.

Network Intrusion Detection Systems (NIDS). NIDS, also known simply as IDS, were the first class of applications targeted directly at obtaining network security awareness on a large scale. Though they enjoyed intense popularity for a time, they eventually succumbed to the criticism that they are really *Attack* Detection Systems, due to the fact that most of them are unable to distinguish between successful and unsuccessful intrusion attempts. The result is an extraordinary degree of attention required to avoid an overwhelming number of false positives. This is especially true in environments without perimeter security, although an alternate tactic for those cases is to reverse the detection polarity (effectively creating a Network *Extrusion* Detection System). The value of a NIDS is further limited by the fact that once an alert is generated, it must be acted upon outside of the system. The most notorious NIDS is probably the open-source tool Snort, but many other free and commercial examples can be found. Nearly all are software-only tools designed to run on commodity hardware that may or may not be re-branded by the vendor.

Intrusion Prevention Systems (IPS). Over the past few years, attitudes toward IDS caused many players to respond by evolving their products one step further. The new species includes mechanisms for mitigating detected intrusions in real time. This capability causes some functional overlap with the new breed of application-layer firewalls, and indeed some are able to function quite well in that role. Due to the increased complexity of function and need for wire-speed operation, some vendors have chosen to implement IPS as a hardware appliance with proprietary Application-Specific Integrated Circuit (ASIC) components. In general, the ASIC-based solutions are better able to cope with very high traffic loads, and are easily extensible into multi-function platforms. In service of greater network intelligence, administrators often use IPS devices to turn down the volume of the most egregious incoming abuses. Certain types of activity, while malicious in intent, are

a simple fact of Internet life, and as such can be safely ignored under low-alert conditions. Early examples of IPS solutions were the TopLayer Networks Attack Mitigator and the TippingPoint UnityOne, both of which are being marketed.

Forensics consoles. Capture forensics tools have existed for quite a while as standalone desktop applications. Recently, however, the market has begun producing more robust tiered-architecture systems that allow fine-grained analysis on very large traffic volumes. The most mature solutions provide dashboard views at multiple levels of detail, along with a console for mining deeper into data streams. Ethereal is perhaps the most popular standalone capture analysis tool. Examples of larger scale solutions include Sandstorm NetIntercept and NIKSUN NetDetector.

Security Information Management Systems (SIMS). SIMS are an attempt to capitalize on the heavy fragmentation of the security product space. Their primary function is to aggregate metadata from disparate systems for a dashboard-like picture. Sites that have invested deeply in emerging technology over the years find that there are too many reporting streams, in too many different formats, to make ready use of on an individual basis. Products like ArcSight and Guarded-Net neuSECURE can enable recapture of value from older systems by consolidating a multiplicity of information sources about network events. The major downside of these products, much like with NIDS, is that the level of customization and tuning required out of the box is considerable.

Amalgamations. A number of appliances on the market are multi-function systems that perform in more than one of the above capacities. Some include all features in the base configuration, while some others offer enhanced functionality as snap-on components, for an enhanced price. Examples are the X-series products from Crossbeam Systems, Sleuth9 by DeepNines, and to a lesser extent, ISS' Proventia product line. At this stage, it is difficult to assess if these attempts toward generalist solutions are viable, or whether feature bloat is resulting in overall diminished value.

Special Environments. One clever set of methods for catching malicious activity involves deploying specially-engineered environments such as honeypots, honeynets, and darknets. A honeypot is a system that is deliberately made vulnerable in order to observe the activities of the attacker who exploits it. A honeynet is a more complete environment that may provide more targets or a more realistic set of interactions between sacrificial and normal systems. Unlike honeynets, darknets have no systems to be targeted. A darknet is just what the name implies - a subset of public, routable network addresses with no host population. The principle behind their use is simple. Since there are neither sources nor destinations on the darknet, any traffic that originates from or is directed toward it is probably not legitimate.

3.2.2 Collection Method

The mechanism by which these various tools obtain data bears on their suitability. Most will take as input SNMP, raw packets, traffic flows, syslog/eventlog data, or some type of third-party metadata. Significant architectural considerations accompany any of these choices. To take advantage of SNMP or log data, routers, switches, and perhaps even server platforms will have to be chosen or configured for that capability. Capturing raw packets is very resource intensive, and has topological requirements. Collecting flows, whether via Cisco NetFlow, sFlow or some other implementation, is less resource intensive, but also contains much less data, and is not suitable for deep inspection. Other system-specific metadata types may create undesirable vendor lock-in.

3.2.3 Detection Method

Once data are collected, the precise method by which network activity is determined to be good or bad is another significant differentiator. In the early history of the Internet, a pair of eyes was the only means of detection that was both widely available and effective. As the Internet grew, the eyeball method became less viable, and a means of automating some aspects had to be found.

The first large-scale solutions were languages for filtering and pattern matching. Systems making use of these methods are generally referred to as signature-based detectors. They can be effective in picking out well-known attack types, but offer less value for extremely short time periods between vulnerability announcement and exploit release. The bane of all signature-based systems is the dreaded zero-day exploit scenario, or a situation in which a clever attacker can alter existing exploits in just the right way to avoid detection.

More recently, in an effort to address the shortcomings of signature-based detection engines, development focus has shifted toward anomaly-based systems. A number of approaches are represented in this category. Some systems match traffic against a database of historical activity patterns, and apply algorithms to judge whether perturbations in the pattern are worthy of alarm. Others reject all activity that is found not to conform to protocol specifications or well-formed application data exchanges. The latter are less common and less useful. The former tend to break down in very large environments, due to the size and complexity of the historical database. More nodes mean more data gathered, and when the space into which that data may fit is finite, aggressive pruning becomes necessary. At some inflection point, the shrinking size of activity history renders matching against it fruitless.

3.2.4 Activity/Passivity

A major distinguishing feature of many security devices continues to be active *vs.* passive operation. Sniffers and NIDS are classic passive devices; they can perform their functions without ever affecting the traffic that they see. By contrast, some devices are capable of mitigating attacks in real time via some response mechanism. For example, IPS appliances may sit inline at the border and simply refuse to forward malicious traffic. Another method uses ARP cache poisoning to defang traffic from any misbehaving host.

Strictly speaking, active response by network appliances does not further the goal of achieving network intelligence. However, devices that boast this feature often have other redeeming qualities, some discussed previously. If the additional cost and maintenance are not a significant obstacle, some network administrators may opt to take advantage of what high-powered inline devices have to offer above and beyond their passive cousins.

3.2.5 Positioning and Topology

Different types of systems have different requirements for where they need to be plugged in. While some systems are only effective at the perimeter, others yield best results when placed at the network core, and still others can be useful in both places. Some may be designed for placement at neither the perimeter nor the core, but rather at two or more midpoint links. By way of illustration, it is not difficult to imagine a scenario where an anomaly detection system placed at the perimeter would have limited effectiveness, due to the fact that its data set would be skewed to profile all hosts simply as being Internet-active and never intranet-active.

The more physical devices required for a given system, the harder it will be to accommodate the implied topology. If a particular solution has a tiered architecture comprising multiple machines performing different functions, this can add further complexity. Administrators of sites that do not have the luxury of a centralized network operations core or extra lines for out-of-band infrastructure management may face insurmountable challenges in deploying the systems that might otherwise serve their needs perfectly.

Related to the active/passive question addressed previously, some systems need to sit inline, whereas others can operate fully out-of-band. For systems designed to operate inline, it may be possible to trick them, so to speak, into thinking that they are functioning as intended, even though in reality they have been placed out-of-band. This would require careful configuration and advice from the vendor to ensure against unpredictable and potentially dangerous results.

3.2.6 Propriety

For software solutions, the nature of the development or licensing model can play an important role in decision making. Any network professional with appreciable experience has faced the build/buy/license choice. The relative costs and benefits in the case of network intelligence initiatives are no different than for any other IT project. In general, the types of tools discussed previously have roughly equal representation in both the proprietary/commercial and free/open-source realms. The most notable exception is to be found in anomaly-based detectors and/or preventors. No free or open-source tool currently matches the maturity and effectiveness of commercial offerings. But while many of these applications are necessarily quite large and complex, that has not prevented many network administrators from pursuing development of home-grown solutions in service of a higher level of customization for their unique environment.

3.2.7 Obsolescence

As the realm of threats changes and grows, many different methods or approaches for mitigation will be born, grow old, and sometimes die out. Understanding how each basic approach or technology is applicable, and further, forecasting which will have staying power, is a daunting prospect for busy network professionals. Nevertheless, time should be invested toward keeping informed not only about contemporary trends and product offerings, but also about current security research. Doing so will enable better judgment as to whether the present state of the art reflects technologies and methods that will still be relevant in following years.

3.3 Vendors

Dealing with vendors of technology products can be a very demanding, confusing activity. Ideally, any vendor would simply sell an organization exactly the solution needed at exactly the price the organization is willing and able to pay. Unfortunately, market forces in this area are not as efficient as economists would have us believe.

While most technology managers would like to be able to stay current with technology trends and offerings, and maintain an appreciable level of hands-on skill, sacrifices must be made for the duties of management. This is where the art of marketing comes into play. Vendors know that they will be selling into organizations primarily at a level where knowledge is less than complete, and so make extensive use of jargon, hype, and fear tactics to differentiate product messages. The

targeted nature of some of these messages allows vendors to get away with making some truly outrageous claims on occasion. If every advertisement in the popular trade magazines were true, the implication would be that only a single offering from a single given vendor would be necessary to service all IT security needs. Thankfully, sanity (or industry analysts) will usually prevail, and it is well understood that the market is not yet mature enough to produce any so-called "god boxes" or viable one-size-fits-all solutions.

The best way to pre-empt a vendor's marketing machine is to mine for personal contacts. The old adage, "It's not what you know, it's *who* you know" is very true when it comes to vendor relations. If introductions can be made using previous relationships as leverage, not only is there is higher likelihood of being spared the aforementioned hype and jargon, but also of receiving straightforward information about capabilities, limitations, and competition. In the best possible scenario, these relationships also result in deeper pricing discounts.

Whenever any technology solution is being evaluated, certain caveats apply. If a particular vendor is too new, appears not to be gaining traction, or has a decent probability of no longer existing in a year's time, that vendor is probably not a good option. Where network intelligence solutions are concerned, there are several other aspects upon which vendors should be evaluated. As previously mentioned, the threat environment for data networks has an extraordinarily rapid rate of change. Accordingly, a judgment should be made as to whether the specific technological approach taken by the vendor's product will have continued relevance in the evolving landscape. Further, it is important to discover whether sufficient engineering support exists within the vendor organization to keep pace with emergent trends. Vendors should also be pressed for information about the product roadmap, to make sure that the solution in question will still exist, in its current form, after nine to eighteen months have passed. If the vendor seems not to have full commitment to advancing the product line, or if it is a likely target for outside acquisition, it may be prudent to defer purchase.

Of course, if a decision is made to use only free or open-source software and commodity hardware, many of these concerns evaporate. However, in this case, the greatest "vendor" shortcoming will be lack of support and documentation, which is a characteristic that many organizations strive to avoid.

3.4 Policies and Procedures

Having considered the technological aspects of the network intelligence strategy, attention must now be turned to specifying explicit parameters for how the organization will realize benefit from the system.

3.4.1 Data Collection and Retention

The decision of precisely what data to collect straddles the fence between technology and policy. If, for example, an organization has selected a technological approach utilizing raw packet capture, that decision must be checked against relevant policies regarding privacy. In the same example, it may also not be a consideration if operational procedures are exacting enough to prevent capture of payload data along with packet headers. If, at the policymaking stage, a network administrator finds the technological solution blocked by policy in every permutation, it will be necessary to reformulate the set of options with a policy-led approach.

Beyond the specification of what data will be gathered, it is also necessary to set a clear policy for how long it will be stored. Network data retention can be attractive for historical reference purposes, but has undesirable features as well. Having more data on hand not only brings higher costs for storage, but also higher potential for compromise of confidentiality. Additionally, retained data can become a strain on resources if an agency of law enforcement or government should ever demand access to it.

3.4.2 Baseline Data

A key procedural element following data collection is the establishment of a baseline. In all but the most tightly controlled and heavily monitored networks, examination at a certain level of detail will always reveal something "interesting." Over time, codified knowledge of such interesting activity should be worked into the baseline data. If there is no current, accurate baseline, precious time can be wasted in an emergency when interesting yet innocuous activity leads investigative efforts in the wrong direction.

3.4.3 Access Control

Creating controls for data access is just as important as deciding what data to gather. Network administrators should be prepared to implement robust measures for control over which people and processes have access to what data, from where, at what times, and at what levels of detail. Given the security implications of such a data store, the importance of auditing in this matter cannot be understated. The existence of an audit trail can also help assuage any concerns of trust that may arise elsewhere in the organization.

3.4.4 Usage Model

Clear documentation describing how the systems supporting network intelligence should be used is valuable both for policy and as a procedural specification. If no procedure is defined, then it cannot be enforced as a safeguard against misuse, whether intentional or unintentional. If in the course of work any staff member finds the usage model to be a hindrance, it can be a clue that the implemented procedures are not producing information adequate to meet the overall goal. When properly crafted, detailed usage models will serve as a validation of the broad applicability of the chosen intelligence strategy.

4 Identify Critical Success Factors

There are a number of factors related to network intelligence strategy that, if not observed or appropriately managed, can easily derail even the most carefully-planned efforts of network administrators.

4.1 Organizational Support

It is essential to take stock of the resources, both tangible and intangible, that are available within the organization for the support of a network intelligence initiative. First and foremost, human resource requirements cannot be overlooked. Though marketing literature for applicable tools gives

the impression that systems are self-contained and effortless to run, the actual process of extracting value from network intelligence systems on a daily basis can be costly in human resources. Network administrators should be prepared to dedicate double-digit utilization percentages of multiple staff members to the tuning and basic operation of the systems.

As is true with any project, budgetary awareness and preparation remain important. Beyond basic expenses for the purchase of hardware and/or software products, though, there may be ancillary costs for such items as service contracts, upgrade or signature subscriptions, customization and consulting services, and integration needs. In an effort to implement the right solution, some managers may find that the projected costs quickly surpass available budget. In such cases, a possible tactic would be to explore mechanisms by which costs could be classified and apportioned in creative ways to other groups within the organization. Caution should be observed in that scenario however, as that course of action could later result in greater vulnerability to ownership contention, as discussed in the next section.

The political aspects of organizational support are more difficult to gauge, and consequently, intangible resources with political implications are harder to acquire. To implement an IT system with such potentially high resource requirements and implications for privacy, it is necessary to secure buy-in from upper management early in the process. If upper management was the original source of the initiative, then full sponsorship is implied, but otherwise it can be a very ephemeral asset when unfavorable politics manifest.

Of somewhat lesser concern are attitudinal obstacles that may be encountered. History or tradition may produce predilection or aversion toward particular platforms, vendors, or design philosophies. Individuals within the organization who wield great influence, whether by formal or informal authority, often succeed in getting their "religious" convictions adopted by the majority. Where technological or methodological zealotry is in opposition, the importance of political prowess cannot be overstated.

4.2 Control and Ownership

Security mindshare has only recently begun to infiltrate the highest levels of most organizations. Unfortunately this means that it will be some time yet before the practice and ownership of security is fully institutionalized in the mainstream of management. Until then, security projects with wider operational applicability (and similarly, but less often, IT projects with implications for security) will be subject to issues of control within the organization. Network intelligence systems fit squarely into this category.

There is wide variance in the origin of Computer Security and Incident Response Teams (CSIRTs) in the global context. Whereas in some organizations, a CSIRT will spring up whole and be given autonomy, in others, it may be an offshoot of, and remain subordinate to, the general network operations group. Some organizations confine information security capability and practice fully within the IT directorate, while others conflate all aspects of security (physical, data, and otherwise) into a separate silo with greater reach across the org chart. In another possible model, organizations appoint a Chief Information Security Officer, or similarly-designated top level manager, whose purview is outside of the IT function but does not include physical aspects. In any of these situations, the nature of a network intelligence system can cause a desire for its control on behalf of multiple groups.

Still other organizations have further exposure to ownership ambiguity due to the relative autonomy of various departments. One example would be an institution of higher education that

has not only a central IT function, but also numerous smaller IT groups local to individual schools or laboratories. A second example would be a large industrial corporation that handles IT operations differently for administrative staff *vs.* personnel on the manufacturing floor. In another possible case where a firm's IT department is called upon to deliver a network intelligence solution for use by the internal auditing or compliance department, questions of funding source, functional design, and end-to-end operation can all complicate the ownership model.

The overall lesson to keep in mind is that where lines of authority are murky, control of data and metadata can cause strife. No matter where in the organization a network intelligence initiative lands, those in charge of it must be prepared to deal with attempts by other groups to co-opt, or even usurp completely, its ownership and ultimate control.

4.3 Privacy

The relationship between security and privacy is complex, and has special bearing on the problem of network intelligence. For a typical consumer on a data network, security best practice and privacy best practice are essentially identical. For organizations, however, some of the most effective ways to ensure security involve invading the privacy of individual users. Which party's interests prevail in any specific circumstance is determined by a combination of the regulatory environment and internal politics.

If it is not immediately clear which privacy-related regulations apply in the organization, a good place to look for codified knowledge on the subject is the internal policy documentation. Regulatory requirements will often set a non-negotiable baseline. Beyond that set of constraints, it is the responsibility of the organization to specify clear policies for data capture, retention, and ownership. The monitoring and analysis of network traffic must of course align with these policies, but further, it is prudent to actively manage users' privacy expectations. This holds true for a wide spectrum of use cases, from coffee shop WiFi patrons on one end to researchers in high-security labs on the other.

In some cases, the question of "who watches the watchers" may be raised by concerned parties. If the concerned party is another group within the IT function of the organization, it may be a portent of control issues, as discussed previously. If one or more individual users is stating the concern, that suggests a need for wider dialogue to restore a level of comfort. In either case, implementing a system of checks and balances among several groups may be a necessary compromise.

4.4 Adaptation

The final element critical to the success of any network intelligence strategy is the ability to adapt. As noted previously, both the problems encountered and the technology solutions to those problems are mutating rapidly, and there is every reason to believe that this course will continue. Despite best efforts at mitigating obsolescence, normalizing threat conditions, and politicking internally, it will be necessary to reformulate a network intelligence strategy from time to time. The interval between each retooling can be extended by remaining vigilant toward the aspects of the strategy that historically presented the greatest challenges to the implementor.

5 Conclusion

A common anecdotal thread noted by the author among colleagues has been that security professionals often come to the business "by accident." It is an adolescent field, and its practitioners face a daunting set of challenges. In spite of the circumstances, it is unacceptable to allow security to continue to exist as an accident in contemporary organizations. The need for strategic rigor in all aspects of security practice is urgent and paramount.

This philosophy is patently applicable to the process by which security professionals and network administrators arm themselves with information assets. Without critical examination and planning, these individuals and their teams will squander opportunities to transform voluminous data into valuable intelligence. The ultimate best-case scenario depends upon the invention and execution of a complete strategy that surpasses ordinary tactical initiatives. Pursuit of network intelligence as a problem to be solved at the organizational level, by first making the business case, and next generating strategic options, will contribute to initial success. Early detection of crucial dealmakers and dealbreakers will ensure that benefits can continue to be realized. The administrator who achieves network intelligence may one day discover his organization comfortably positioned in the race against security threat evolution.

6 Acknowledgements

The author is very grateful to Sherri Davidoff, Bob Mahoney, Pratt DeWorm, James Kretchmar, Jonathan Reed and Oliver Thomas for their advice and support during the writing of this document.

References

[1] Bejtlich, Richard. *The Tao of Network Security Monitoring: Beyond Intrusion Detection.* Addison-Wesley, 2004.

[2] Cottrell, Les. *Network Monitoring Tools.* Stanford Linear Accelerator Center. `<http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>` Retrieved April 28, 2005, from source.

[3] Egan, Mark with Tim Mather. *The Executive Guide to Information Security: Threats, Challenges, and Solutions.* Addison-Wesley, 2004.

[4] Ridley, Matt. *The Red Queen: Sex and the Evolution of Human Nature.* Penguin, 1993.

[5] Honeynet Project. `<http://www.honeynet.org/>` Retrieved May 18, 2005, from source.