



Unified Risk Management: Part 1

**Towards A Business-Driven Information Survivability
Architecture**

Christofer Hoff, CISSP CISA CISM

Chief Security Strategist

Crossbeam Systems, Inc.

February 2006

ABSTRACT

Managing risk is fast becoming a lost art. As the pace of technology's evolution and adoption overtakes our ability to assess and manage its impact on the business, the overrun has created massive governance and operational gaps resulting in exposure and misalignment. This has caused organizations to lose focus on the things that matter most: the survivability and ultimate growth of the business.

Overwhelmed with the escalation of increasingly complex threats, the alarming ubiquity of vulnerable systems and the constant onslaught of rapidly evolving exploits, security practitioners are forced to choose the unending grind of tactical practices - focused on deploying and managing security infrastructure - over the strategic art of managing and institutionalizing risk-driven architecture as a business process.

In order to understand the nature of this problem and its resolution we have separated this discussion into two separate papers:

- In Part One (this paper), we analyze the gap between pure technology-focused information security infrastructure and business-driven, risk-focused information survivability architectures.
- In Part Two (a second paper), we show how this gap is bridged using sound risk management practices in conjunction with best of breed consolidated Unified Threat Management (UTM) solutions as the technology foundation of a consolidated risk management model. We will also show how governance organizations, business stakeholders, network and security teams can harmonize their efforts to produce a true business protection and enablement strategy that delivers security as an on-demand service layer at the speed of business. This is a process we call Unified Risk Management or URM.

THE WAY THINGS ARE

Today's constantly expanding chain of technically-complex security point solutions do not necessarily reduce or effectively manage risk; they mitigate threats and vulnerabilities in the form of products produced by vendors to solve specific technical problems but without context for the assets which they are tasked to protect and at a cost that may outweigh the protected assets' value.

But how does one go about defining and measuring risk?

Spire Security's Pete Lindstrom best defines being able to measure and manage risk by first describing what it is not:

- Risk is not static; it is dynamic and fluctuates constantly with potentially high degrees of variation.
- Risk is not about the possibility that something bad could happen; it is about the probability that it might happen.
- Risk is not some pie-in-the-sky academic exercise; you have all of the necessary information available to you today.
- Risk is not a vague, ambiguous concept; it is a continuum along which you can plot many levels of tolerance and aversion.

It is clear that based upon research available today, most organizations experience difficulty aligning threats, vulnerabilities and controls to derive the security posture of the organization (defined as acceptable or not by the business itself.) In fact, much of what is referred to as risk management today is actually just complex math in disguise indicating an even more complex extrapolation of meaningless data that drives technology purchases and deployments based upon fear, uncertainty and doubt. Nothing sells security like a breach or new worm.

As such, security practitioners are typically forced into polarizing decision cycles based almost exclusively on threat and vulnerability management and not a holistic risk management approach to deploying security as a service. They are distracted by the market battles to claim the right to the throne of Network Security Supremacy to the point where the equipment and methodology used to fight the war has become more attractive than the battle itself.

In most cases, these security products are positioned as being either integrated into the network infrastructure such as routers or switches or bolted onto it in the form of single vendor security suite appliances. These products typically do not collaborate, interoperate, communicate or coordinate their defensive activities with solutions not of a like kind.

Realistically, there is room for everyone at the table. Network vendors see an opportunity to continue to leverage their hold on market share by adding value in the form of security while pure-play security vendors continue to innovate and bring new products and solutions to market that address acute needs that the other parties cannot. Both are needed but for different reasons.

Neither of the extremes represents an ultimate answer. Meeting in the middle is the best answer with an open, extensible, and scaleable network security reference architecture that integrates as a network switch with all of the diversity and functionality delivered by on demand best of breed security functions.

As the battle rages, multiple layers of overlapping proprietary technologies are being pressed into service against risks which are often not quantified, threats that are not recognized and attempt to defend against vulnerabilities which within context may have little recognized business impact.

In many cases, these solutions are marketed as new technology when in fact they exist as re-badged products with additional functions cobbled together onto outdated or commoditized hardware and software platforms, polished up and marketed as UTM or adaptive security solutions.

It is important to make clear the definition of UTM within the context of the mainstream security solution space offered by most vendors today. UTM solutions are those which provide an aggregate of security functionality comprised of at least network firewall, network intrusion detection and prevention, and gateway anti-virus. UTM solutions are often extended to offer additional functionality such as VPN, URL filtering, and anti-spam capabilities with a recognized benefit of squeezing as much functionality from a single product offering in order to maximize the investment and minimize the number of arterial insertion points throughout the network.

Most of the UTM solutions on the market today provide a single management interface which governs the overall operation of many obfuscated moving parts which deliver the functionality advertised above.

In many cases, however, there are numerous operational and functional compromises made when deploying typical single application/multiple function appliances or embedded security extensions applied to routers and switches. These compromises range from poor performance to an inability to scale based on emerging functionality or performance requirements. The result is what some hope is "good enough" and implies a tradeoff favoring cost over security.

Unfortunately, this model of “good enough” security is proving itself not good enough as these solutions can lead to cost and management complexities that become a larger problem than the perceived threat and vulnerabilities the solutions were designed to mitigate in the first place.

SO WHAT TO DO? FOCUS ON RISK!

Prudent risk management strategy dictates that the best method of securing an organization’s most critical assets is the rational application of policy, technology and processes where ultimately the risk justifies the cost.

It is within this context that the definition of information survivability demands an introduction as it bears directly on the risk management processes described in this paper. In their paper titled “Information Survivability: Required Shifts in Perspective,” Allen and Sledge introduce the concept of information survivability as a discipline which is defined as “...the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.”

They further juxtapose information survivability against information security by illustrating that information security “...takes a technology centric point of view, with each technology solving a specific set of issues and concerns that are generally separate and distinct from one another. Survivability takes a broader, more enterprise-wide point of view looking at solutions that are more pervasive than point-solution oriented.”

Information survivability thus combines elements of business impact, continuity, contingency and disaster recovery planning with the more narrowly-focused and technical information security practices, thereby elevating the combined foundational elements to an enterprise-wide risk management concern.

From this perspective, risk management is not just about the latest threat. It is not just about the latest vulnerability or its exploit. It is about how, within the context of the continued operation of the business and even while under duress, the organization’s mission-critical functions will be sustained and the most important data will be appropriately protected.

THE LANGUAGE OF RISK

One obvious illustration of this risk gap is how disconnected today’s enterprise security and networking staffs remain even when their business interests should be so very much closely aligned. Worse yet is the resultant misalignment of both teams with the enterprises’ mission and appetite for risk.

As an example, while risk analysis is conducted on one side of the house with little understanding of the network and all its moving parts, the device sprinkling of network and security appliances are strung together on the other side of the house with little understanding of how these solutions will affect risk or if they align to the objectives or matters to the business at all.

To prove this point, ask your network team if they know what OCTAVE or CoBIT frameworks are and how current operational security practices map to either of them. Then, ask the security team if they know how MPLS VRF, BGP route reflectors or the spanning tree protocol function at the network level and how these technologies might affect the enterprise’s risk posture.

Then, ask representative business stakeholders if they can articulate how the answers given by either of the parties clearly maps to their revenue goals for the year and how their regulatory compliance requirements may be affected. Where are the metrics to support any assertion?

Thus, while both parties seek to serve the business with a common goal of balancing security with connectivity neither speaks a common language that can be used to articulate the motivation, governance or value of each other's actions to the business.

At the level of network security integration, can either team describe the mapping of asset-based risk categories across the enterprise to the network infrastructure? Can they tell you tomorrow what the new gaps are at each risk category level and provide a quantifiable risk measurement across the enterprise of the most critical assets in a matter of minutes?

This illustration defines the problem at hand; how do we make sure that we deliver exactly what the business requires to protect the most critical assets in a manner fitting the risk profile of the organization and no more.

Interestingly, from an economic point of view, the failure to create a tightly integrated risk management ecosystem results almost by definition in a completely inefficient and ineffective solution. Without risk management basics such as asset and data classification and zoned network segmentation by asset class, the network has the very real potential to actually be over-defended at risk boundaries and thus drive costs and complexity much higher than they need to be.

Consequently, most, if not all, security controls and prescribed protective technologies are applied somewhat indiscriminately across the enterprise as a whole. Either too much security is applied or many of the features of the solution are disabled since they are not needed. Where is the return on investment there? Do you need URL filtering in a DMZ? Do you need SOA/XML schema enforcement applied across user desktops? No. So why deploy complex blanketed security technology where it is neither needed nor justified?

For example, since all assets and the data they contain are not created equal, it is safe to assume that the impact to the business caused by something "bad" happening to any two assets of different criticality would also not be equal. If this is an accepted corollary, does it make sense to deploy solutions that provide indiscriminant protective umbrellas over assets that may not need any protection at all?

In many cases, this issue also plays out in a different direction as security architectures are constrained based on the deployment of the physical wiring closets and switch and router infrastructures. Here, the ability or willingness to add one after the other of point solution devices in-line between key network arteries, incrementally add specialized security blades into core network components or even forklift switching and routing infrastructure to provide for "integrated security" is hideously problematic.

In these cases, overly-complex solutions consist of devices sprinkled in every wiring closet because there will probably be a representative computing resource of every risk category in that area of the network.

Here we are being asked to change the network to fit the security model rather than the other way around. If the network was built to accommodate the applications and data that traverse it, should we not be just as nimble, agile and accommodating in our ability to defend it?

Referring back to the definition of risk management, the prudent answer is to understand exactly where you are at risk, why, the business impact, and exactly what is needed from a control perspective to appropriately manage the risk. In some cases the choice may be to assert no control at all based upon the lack of business impact to the organization.

One might ask if the situation is not better than it was five years ago. The answer to this question is unclear – the effects of the more visible and noisy threats such as script kiddies have been greatly mitigated. On the other hand,

the emergence of below-the-radar, surgically-focused, financially motivated cyber-criminals has exposed business assets and data more than ever. The net effect is that we are not, in fact, safer than we were because we focus only on threats and vulnerabilities and not risk.

SECURITY IS IN THE NETWORK...OR IS IT IN THE APPLIANCE OVER THERE?

Let us look for a moment at how technology visions spiral out of control when decoupled from risk in a technology centric. The most blatant example is the promise of security embedded in the network or all-in-one single vendor appliances.

On the one hand, we are promised a technically-enlightened, self-defending network that is resilient to attack, repels intruders, self-heals when infected and delivers security as a service as applications and data move about fluidly pursuant to policies enforced across every platform and network denizen.

We also are told to expect intelligent networks that offer solution heterogeneity irrespective of operating system or access modality, technology agnosticism, and completely integrated identity management as a way to evolve from being data rich but information poor, providing autonomic response when bad things happen.

Purveyors of routing and switching products plan to branch out from the port density penetration foothold they currently enjoy to deliver end-to-end security functionality embedded into the very fabric of the machinery meant to move bits with the security, reliability and speed it deserves and which the business demands.

At the other end of the spectrum, vendors who offer single-sourced, proprietary security suites utilizing integrated functions by way of appliances integrated into the network suggest that they will provide the architecture of the future.

They both suggest they will provide host-based agents that provide immune system-like responses to attempted "infection" and will take their orders from a central networked "nervous system" that coordinates the activities of the various security "organs" across the zones of trust defined by policy.

They propose the evolution of the network into a sentient platform for the delivery of business in all its forms, aware of and able to interact with and control the applications and data which travel over it.

Data, voice, video and mobility with all of the challenges posed by the ubiquity of access methodologies – and of course security – are to be provided by the network platform as the launch pad for every conceivable level of service. The network will take the place of complex business logic such as Extraction/Transform/Load (ETL) layers and it will deliver applications directly and commit and retrieve data dynamically and ultimately replace tiers of highly-specialized functions and infrastructure that exist today.

All the while, as revolutionary technology and architectures such as web services emerge, new standards compete for relevancy and the constant demand for increased speeds and feeds continue to evolve, the network will have to magically scale both in performance and functionality to absorb this change while the transparency of applications, data and access modality blurs.

These vendors claim that security will simply be subsumed by the "network" as a function of the delivery of the service since the applications and data will be provided by a network platform completely aware of that which traverses its paths. It will be able to apply clearly articulated business processes and eliminate complex security problems by mitigating threats and vulnerabilities before they exploit an attack surface.

These solutions are to be “open,” and allow for collaboration across the enterprise, protecting heterogeneous elements up and down the stack in a cooperative defense against impact to the delivery of applications and data.

These solutions promise to be more nimble and will be engineered to provide adaptive security capabilities in software with hardware assist in order to keep pace with exponential increases in requirements. These solutions will allow for quick and easy update as threats and vulnerabilities evolve. They will provide more deployment flexibility and allow for greater coverage and value for the security dollar as policy-driven security is applied across the enterprise.

WHAT'S WRONG WITH THESE ANSWERS? MR. FOX, MEET MS. CHICKEN

Today's favorite analogy for security is offered in direct comparison to the human immune system. The immune system of modern man is indeed a remarkable operation. It is there, inside each human being, where individual organs function independently, innocuously and in an autonomic fashion. When employed in a coordinated fashion as a consolidated and cooperative system, these organs are able to fight infection by adapting and often become more resistant to attack and infection over time.

Networks and networked systems, it is promised, will provide this same capability to self-defend and recover from infection. Networks of the future are being described as being able to self-diagnose and self-prescribe antigens to cure their ills, all the while delivering applications and data transparently and securely to those who desire it.

It is clear, however, that unfortunately there are infections that humans do not recover from. The immune system is sometimes overwhelmed by attack from invaders that adapt faster than it can. Pathogens spread before detection and activate in an overwhelming fashion before anything can be done to turn the tide of infection. Mutations occur that were unexpected, unforeseen and previously unknown. The body is used against itself as the defense systems attack both attacker and healthy tissue and the patient is ultimately overcome. These illnesses are terminal with no cure.

Potent drugs, experimental treatments and radical medical intervention may certainly extend or prolong life for a short time, but the victims still die. Their immune systems fail.

If this analogy is to be realistically adopted as the basis for information survivability and risk management best practices, then anything worse than a bad case of the sniffles could potentially cause networks – and businesses -- to wither and die if a more reasonable and measured approach is not taken regarding what is expendable should the worst occur. Lose a limb or lose a life? What is more important? The autonomic system can't make that decision.

These glimpses into the future are still a narrowly-focused technology endeavor without the intelligence necessary to make business decisions outside of the context of bits and bytes. Moreover, the deeper and deeper information security is pushed down into the stack, the less and less survivable our assets and businesses will become because the security system cannot operate independently of the organ it is protecting.

Applying indiscriminate and sometimes unnecessary layers of security is the wrong thing to do. It adds complexity, drives costs, and makes manageability and transparency second class citizens.

In both cases, these promises will simply add layer upon layer of complexity and drive away business transparency and the due care required to maintain it further and further from those who have the expertise to manage it. The reality is that either path will require a subscription to a single vendor's version of the truth. Despite claims to the

contrary, innovation, collaboration and integration will be subject to that vendor's interpretation of the solution space. Core competencies will be stretched unreasonably and ultimately something will give.

Furthermore, these vendors suggest that they will provide ubiquitous security across heterogeneous infrastructure by deploying what can only be described as homogenous security solutions. How can that be? What possible motivation would one vendor have to protect the infrastructure of his fiercest competitor?

In this case, monoculture parallels also apply to security and infrastructure the same way in which they do to networked devices and operating systems. Either of the examples referenced can potentially introduce operational risk associated with targeted attacks against a single-vendor sourced infrastructure that provides both the delivery and security for the data and applications that traverse it. We have already seen recent malicious attacks surgically designed and targeted to do just this.

What we need is perfectly described by Evan Kaplan of Aventail who champions the notion of a "dumb" network connectivity layer with high speed, low latency, high resiliency, predictable throughput and reliability and an "intelligence" layer which can deliver valued added service via open, agile and extensible solutions.

In terms of UTM, based upon a sound risk management model, this would provide exactly the required best of breed security value with maximum coverage exactly where needed, when needed and at a cost that can be measured, allocated and applied to most appropriately manage risk.

We pose the question of whether proprietary vendor-driven threat and vulnerability focused technology solutions truly offer answers to business problems and if this approach really makes us more secure. More importantly, we call into question the ability for these offerings to holistically manage risk. We argue they do not and inherently cannot.

THE SOLUTION: UNIFIED RISK MANAGEMENT UTILIZING UNIFIED THREAT MANAGEMENT

A holistic paradigm for managing risk is possible. This model is not necessarily new, but the manner in which it is executed is. Best-of-breed, consolidated UTM provides this execution capability. It applies solutions from vendors whose core competencies provide the best solution to the problem at hand. It can be linked directly to asset and information criticality.

It offers the battle-hardened lessons and wisdom of those who have practiced before us and adds to their work all of the benefits that innovation, remarkable technology and the pragmatic application of common sense brings to the table. The foundation is already here. It does not require years of prognostication, massive infrastructure forklifts or clairvoyant bets made on leveraging futures. It is available today.

This methodology, which we call Unified Risk Management (URM), is enabled by applying a well-defined framework of risk management practices to an open, agile, innovative and collaborative best-of-breed UTM solution set combined in open delivery platforms which optimize the effectiveness of deployments in complex network environments.

These tools are combined with common sense and the extraordinary creativity and practical brilliance of leading-edge risk management practitioners who have put these tools to work across organizational boundaries in original and highly effective ways.

This is the true meaning of thought leadership in the high technology world: customers and vendors working hand-in-hand to create breakthrough capabilities without expensive equipment forklifts and without the associated brow-beating from self-professed prophetic visionaries who pontificate from upon high about how we have all been doing

this wrong and how a completely new upgraded infrastructure designed to sell more boxes and Ethernet ports is required in order to succeed.

URM is all about common sense. It is about protecting the right things for the right reasons with the right tools at the right price. It is not a marketecture. It is not a fancy sales pitch. It is the logical evolution and extension of Unified Threat Management within context.

It is about providing choice from best-of-breed offerings and proven guidance in order to navigate the multitude of well-intentioned frameworks and come away with a roadmap that allows for true risk management irrespective of the logo on the front of the machinery providing the heavy lifting. It is, quite literally, about “thinking outside of the box.”

URM combines risk management – asset management, risk assessment, business impact analysis, exposure risk analytics, vulnerability management, automated remediation – and the virtualization of UTM security solutions as a business process into a tight feedback loop that allows for the precise management of risk. It iteratively feeds into and out of reference models like Spire Security’s Pete Lindstrom’s “Four Disciplines of Security Management” that include elements such as:

- Trust Management
- Identity Management
- Vulnerability Management
- Threat Management

This system creates a continuously iterative and highly responsive intelligent ecosystem linked directly to the business value of the protected assets and data.

This information provides rational and defensible metrics that show value, the reduction of risk on investment, and by communicating effectively in business terms, is intelligible and visible to all levels of the management hierarchy from the compliance auditor to the security and network technicians to the chief executive officer.

This re-invigorated investment in the practical art of risk management holds revolutionary promise for solving many of today’s business problems which are sadly mislabeled as information security issues.

Risk management is not rocket science, but it does take innovation, commitment, creativity, time, the reasonable and measured application of appropriate business-driven policy, excellent technology and the rational application of common sense.

This tightly integrated ecosystem consists of solutions that embody best practices in risk management. It consists of tightly-coupled and consolidated layers of UTM-based information survivability architectures that can apply the results of the analytics and management toolsets to business-driven risk boundaries in minutes. It collapses the complexity of existing architectures dramatically and applies a holistic policy driven risk posture that meets the security appetite of the business and it does so while preserving existing investments in routing and switching infrastructure that serves the business well.

CONCLUSION: ON TO THE RECIPE

In this first part of our two-part series, we have tried to define the basis for looking at network security architectures and risk management in an integrated way. Key to this understanding is a move away from processes in which disparate appliances are thrown at threats and vulnerabilities without a rationalized linkage to the global risk profile of the infrastructure.

In the second paper of the series we will demonstrate exactly how the lightweight processes that form the foundation of Unified Risk Management can be implemented and applied to a UTM architecture to create a highly responsive, real-time enterprise fully aware of the risks to its business and able to respond on a continual basis in accordance with the ever-changing risk profile of its critical data, applications and assets.

www.crossbeamsystems.com

Worldwide

Crossbeam Systems Inc.
200 Baker Ave.
Concord, MA 01742
Tel: (978) 318-7500,
Fax: (978) 287-4210

Europe, Middle East, Africa

Crossbeam Systems, Inc
E. Space, Bat C
Parc Int ; de Sophia Antipolis
45 allée des Ormes
06250 Mougins - France
Tel: +33 4 92 28 89
Fax: +33 4 92 28 72 60

Asia Pacific

Crossbeam Systems, Inc.
80 Raffles Place
Levels 36 UOB Plaza 1
Singapore 048624
Tel: +65 6248 4684
Fax: +65 6248 4988