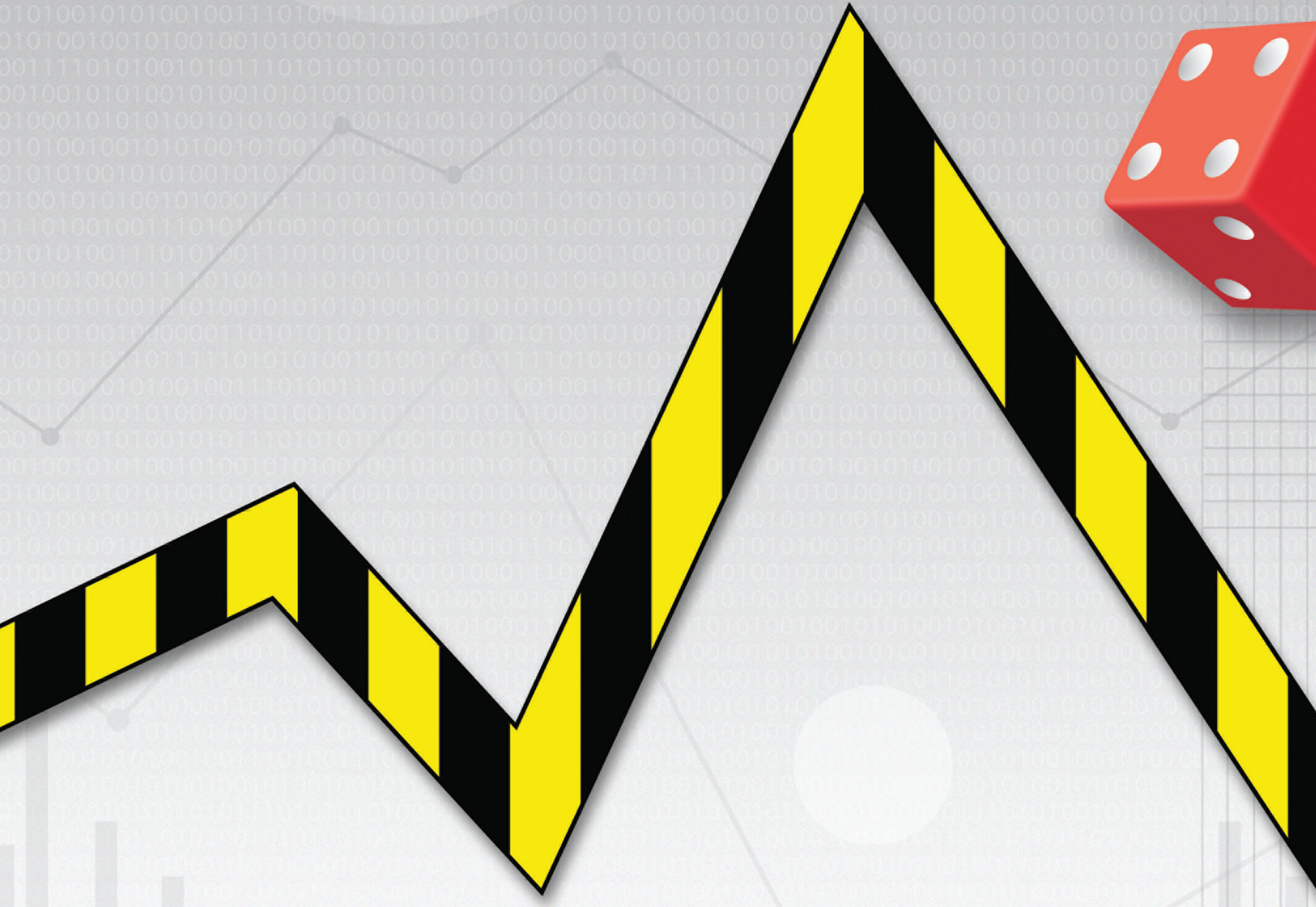
COVER STORY | BY BRIAN J. ALLEN, CPP



A PROFESSIONAL PATH

Enterprise security risk management will raise the profile of security from a task-bound trade to one of the key business drivers in the C-suite.

UNTIL RECENTLY, security has been considered a trade, with practitioners fighting for proper standing in the institutions they protect. But the industry is now at a crossroads.

Before us lie two paths. One is a continuation of the status quo. We may continue to glide down this road, but it is not a self-determined path. It has been chosen for us because we have not clearly defined security's role. Given this failure to self-define, security has traditionally been defined by others by the task it performs, such as information security, investigations, physical security, or executive protection. This type of definition diminishes the value of the security function; our role is more than just our allocated tasks.

The second road is one of self-determination and opportunity. It offers a chance for the industry to advance from a trade to a fully respected profession. On this road, we can take control of the dialogue, shape the conversation surrounding our field, and make our own way forward. As an industry—with ASIS taking the lead—we can keep advancing until security is considered a profession.

How can we advance on this second road? First we need a clear definition of the role of security in the private sector. We also need a core base of knowledge that supports our understanding of that role, which can be taught—not only to college students, but to transitioning personnel coming into our industry and to our hiring managers. There also needs to be an established expectation that practitioners will share this knowledge of security's role and the core competencies associated with it.

ASIS International has already started defining this role through the concept of enterprise security risk management (ESRM). With its embrace of ESRM, ASIS has positioned our industry to travel down the road of opportunity and self-determination, with ESRM as the guiding principle to help chart our course.

ILLUSTRATIONS BY STEVE McCRACKEN

Not everyone in the industry is ready for this journey, however. For some who may have heard of the concept but still find it vague, questions remain. Primarily: What exactly is ESRM and why is it needed?

What is ESRM?

At its core, ESRM is the practice of managing a security program through the use of risk principles. It's a philosophy of management that can be applied to any area of security and any task that is performed by security, such as physical, cyber, information, and investigations.

The practice of ESRM is guided by long-standing internationally established risk management principles. These principles consist of fundamental concepts: What's the asset? What's the risk? How should you mitigate that risk? How should you respond if a risk becomes realized? What is your process for recovering from an event if a breach happens? Collectively, these principles form a thoughtful paradigm that guides the risk management thought process.

When pursued, these questions elicit valuable information, and they can be asked of every security-related task. For instance, investigations, forensics, and crisis management are all different security functions, but when they are discussed within the ESRM framework they are simply different types of incident response.

Similarly, every function of physical and information security, such as password and access management, encryption, and CCTV, is simply considered a mitigation effort within the ESRM paradigm. These may seem to be merely semantic differences, but they are important nuances. When we define these functions within the ESRM paradigm, we also start to define the role we play in the overall enterprise.

ESRM elevates the level at which the role of security management is defined. Instead of defining this role at task level, it defines the role at the higher, overarching level of risk management.

By raising the level of security's role, ESRM brings it closer to the C-suite, where executives are considering much more than individual tasks. And by defining the role through risk principles, it better positions the security function within the business world at large. Business executives in all fields understand risk; they make risk decisions every day. Using ESRM principles to guide our practice solidifies our place within the language of business while also defining the role we play within the business.

Business executives in all fields understand risk; they make risk decisions every day.

For example, consider a company with a warehouse and a server. In the warehouse, security is protecting widgets and in the server, security is protecting data. Under the common risk principles, we ask: What are the risks to the widgets and data? How would we protect against those risks? Who owns the widgets, and who owns the data?

We may decide to put access control and alarms on the warehouse or a password and encryption on the data. In both instances, we're protecting against intrusion. The goal is the same—protection. For each task, the skill set is different, just like skill sets differ in any other aspect of security: investigations, disaster response, information technology. But the risk paradigm is the same for each.

Why We Need It

We need ESRM to move beyond the tasks that security managers and their teams are assigned. For instance, if you manage physical security, your team is the physical security team. If you do investigations, you are an investigator. If you manage information security, your team is the information security team.

But these tasks merely define the scope of responsibility. Our roles are broader than our assigned tasks. Our responsibilities should be viewed not as standalone tasks, but as related components within our roles as security risk managers.

Having a clear, consistent, self-defined role provides significant benefits. First, it preempts others from defining our role for us in a way that fails to adequately capture and communicate our value.

Second, it helps better position ourselves in the C-suite. C-level executives often struggle with what security managers do, and where to align us. This is often reflected in the frustrations expressed in some of our own conversations about needing a proverbial seat at the table. In one sense, this exclusion may seem justified: if we can't define our role beyond describing our tasks, why would upper management charge us with higher-level leadership and strategy?

Third, it provides guidance to our industry. Greater use of ESRM will provide an always-maturing common base of knowledge, with consistent terms of use and clear expectations for success.

This benefits not only practitioners in our industry, but also all other executives who may need to interact with the security practice or work with the security manager. This can be especially valuable during times of change, such as when a security manager switches companies or industries, or when new executives come into the security manager's firm.

ASIS has started to lead the effort of defining security's role through ESRM.

In those situations, security managers often feel that they are continually educating others on what they do. But this endless starting over process wouldn't be necessary if there were a common understanding of what security's role is, beyond the scope of its responsibilities.

Why Now?

This industry at large has talked about ESRM for at least the last 10 years. But as relevant as the topic was a few years ago, the present moment is the right moment for ESRM because security risks now have the potential to become more disruptive to business than in the past.

There are several reasons for this. The use of technology in the current

economy has allowed businesses to centralize operations and practices. While this consolidation may have increased efficiency, it has also made those centralized operations more susceptible to disruption. When operations were more geographically dispersed, vulnerabilities were more spread out. Now, the concentrated risks may have a more serious negative impact to the business.

We are also moving beyond traditional information security and the protection of digitalized data. Now, cybersecurity risks pose threats of greater business disruption. For example, the threats within the cyber landscape to the Internet of Things (IoT) have the potential to cause more harm to businesses compared with the negative effects they suffered in the past due to loss of information.

Many executives understand the significance of these risks, and they are looking for answers beyond the typical siloed approach to security, in which physical security and information security are separately pursued. They realize that the rising cyber risks, in tandem with the increasing centralization of business operations, have caused a gap in security that needs to be closed.

Boards are also becoming more engaged, which means that senior management must also become engaged, and someone will have to step in and fill that gap. That could be a chief risk officer, a board-level committee, an internal audit unit...or security. Hopefully, it will be the latter, but to step up and meet this challenge, security professionals must be able to consistently define their role beyond simply defining their tasks.

Making the Transition

What we need is a roadmap toward professionalization.

Five Insights on ESRM

By Rachelle Loyear and Brian Allen, CPP

THERE ARE FIVE overall concepts that provide guidance about the nature of enterprise security risk management (ESRM). These concepts describe what ESRM is, what it can do for security managers, how security can gain C-suite approval for it, and how to implement a vibrant ESRM program for the enterprise.

ESRM Is a Philosophy

ESRM is not a standard, nor is it a rigid set of rules to follow. ESRM is a philosophy of managing security. It is based on standard risk management practices, the same ones that guide most of the other business decisions made by the enterprise. It requires partnership with the business leaders in the organization.

This philosophy gives the security leader the ability to manage security risks. This ability is not based on the latest incident or scare in the news, nor is it based simply on the manager's own ideas of what is most important to protect. Instead, it is based on a shared understanding of what the business deems critical for risk mitigation, and what level of risk the business is willing to accept in different areas. This ability also requires that the business fully understand why the security risk mitigation tactics have been put in place, and what the impact of not having those mitigations might be.

The emphasis here is on business. ESRM philosophy recognizes that security risk does not belong to security. It is a business risk, like any other financial, operational, or regulatory risk, and final decisions on managing that risk must belong to the business leaders. That shift in understanding sets a security program up for a greater level of success because security leaders are delivering only what the business needs, and, more important, what the C-suite understands that it needs.

ESRM Is a Process

ESRM is not merely an academic philosophy. A general approach for setting up and running a security program can be derived from it. Under that approach, ESRM in action is a cyclical program, and the cycle of risk management is ongoing:

1. Identify and prioritize the assets of an organization that need to be protected.
2. Identify and prioritize the security threats that the enterprise and its assets face—both existing and emerging—and the risks associated with those threats.
3. Take the necessary, appropriate, and realistic steps to protect and mitigate the most serious security threats and risks.
4. Conduct incident monitoring, incident response, and post–incident review, and apply the lessons learned to advance the program.

ESRM Aligns with the Business

Aligning the security program with business requirements is the most critical component of the ESRM philosophy. This means that the security program must receive governance and guidance from the business. We recommend the formation of a security council to ensure this alignment.

There are several ways to implement a council. It could be a loose, informal group that provides input as needed, or it could be a board-level initiative that has formal roles, meetings, charters, and documented responsibilities for ensuring security compliance. The council can be a venue for discussing security topics and risk management strategies, and it can host resolution attempts for conflicts in the process.

ASIS is leading the effort of defining security's role through ESRM. At ASIS 2017 in Dallas, you will hear more conversation around ESRM as well as more maturity and consistency in that conversation. As the leading security management professional organization, ASIS is best positioned to guide us through the roadmap from a trade to a profession.

The ASIS Board of Directors has made ESRM an essential component of its core mission. It has started incorporating ESRM principles into its strategic roadmap, which means that ASIS is starting to operationalize this philosophy—a critical step in building out this roadmap. Other steps will be needed; it is essential that volunteers, both seasoned and new to the field, embrace this shift towards professionalization for it to gain traction.

This transition will not occur with the flip of a switch. It will take dedication to challenge our own notions of how we perceive what we do, the language we use to communicate to our business partners, and our approach toward executing our functions. It will take time and comprehensive reflection, and the ability to recognize when we don't get it right. We may not be totally wrong either, but thoroughness in developing consistency is critical.

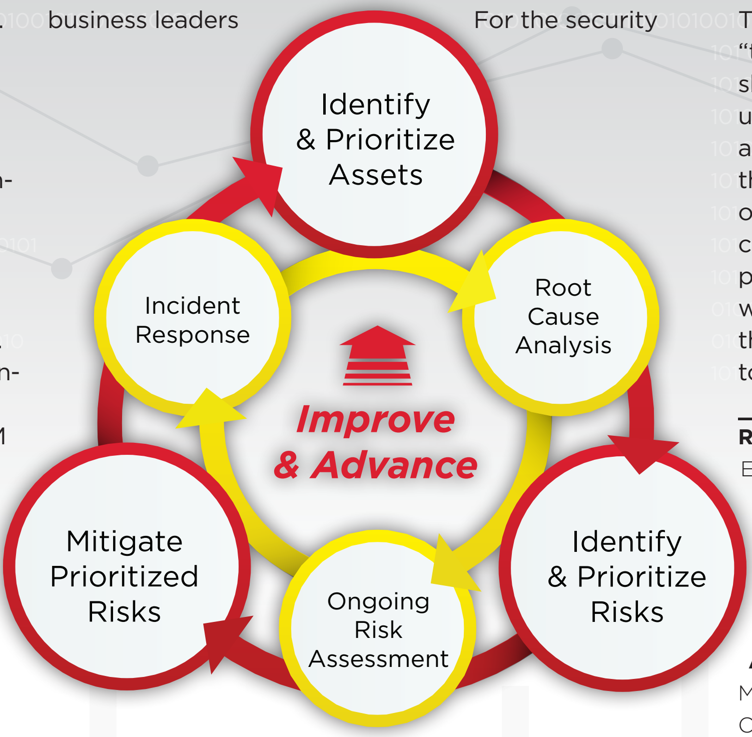
There are some core foundational elements that need to be in place for this ESRM transition to be successful. First, there needs to be a consistent base of knowledge for our industry to work from: a common lexicon and understanding of security's role that is understood by practitioners and the business representatives we work with.

We also need both a top-down and bottom-up approach. New security practitioners entering the industry from business or academia, or transitioning from law enforcement or the military, need a comprehensive understanding

ESRM Covers All Security

There is no aspect of security that cannot be managed in alignment with the ESRM philosophy. Many security professionals already practice much of the ESRM philosophy without thinking of it that way. For example, performing a physical security risk assessment on a facility is equivalent to the ESRM steps of identifying and prioritizing assets and risk. And setting up a crisis management plan can be considered an aspect of ESRM risk mitigation, as well as incident response.

The critical difference between programs that do these activities as part of a traditional security program versus an ESRM program is the consistency of approach in ESRM. In ESRM, these activities are not performed on an ad hoc basis but consistently across all areas of security risk. They are not applied to one area of the organization and not to another. And, vitally, they are not performed in a vacuum by security and for security, but in full partnership with the business leaders driving the decision making process for all risk mitigation.


Identify & Prioritize Assets
Root Cause Analysis
Identify & Prioritize Risks
Ongoing Risk Assessment
Mitigate Prioritized Risks
Incident Response
Improve & Advance

ESRM Is Possible

Implementing ESRM cannot be done overnight. It's an iterative process that allows your security program to evolve over time into a pure risk management approach. For the security manager, the first step to fully understanding the ESRM philosophy is to communicate it to the executives and business leaders in the enterprise.

When implemented thoughtfully and practiced consistently, ESRM can completely change the view of the security function in any organization. The old view of security as "the department of no" will shift when business leaders understand that security is a partner in ensuring that the assets and functions of the enterprise most critical to the business are protected in accordance with exactly how much risk the business is willing to tolerate.

RACHELLE LOYEAR IS ESRM PROGRAM MANAGER FOR G4S AND CHAIR OF THE ASIS CRISIS MANAGEMENT AND BUSINESS CONTINUITY COUNCIL. **BRIAN J. ALLEN, ESQ., CPP,** IS A MEMBER OF THE ASIS ESRM COMMISSION. ALLEN AND LOYEAR ARE COAUTHORS OF *THE MANAGER'S GUIDE TO ENTERPRISE SECURITY RISK MANAGEMENT* AND THE FORTHCOMING BOOK *ENTERPRISE SECURITY RISK MANAGEMENT: CONCEPTS AND APPLICATIONS.*

of risk management principles and how a risk paradigm drives the security management thought process. There should be an expectation that these foundational skill sets are in place when someone enters the security field. Working from a common base of knowledge, these ESRM concepts should be incorporated into the security management curriculum, consistently established in every security certification, and inherent in job descriptions and hiring expectations at every level.

We also need to build expectations regarding what security's role is, and how it goes beyond its assigned tasks, from the top-down—among executives, boards, hiring managers, and business partners. A clear and common understanding of security's role will make it easier to define success and the skill sets that are needed to be successful. Organizations like ASIS will assist in providing the wherewithal to support these leaders.

If we truly are security risk managers, then there must be an expectation of foundational and comprehensive risk skill sets when hiring decisions are made. There could be educational opportunities through ASIS, through global partnerships with universities, and through publications coordinated with organizations that reach the C-suite, such as the Conference Board of the National Association of Corporate Directors.

Clearly academia needs to play a role as well. College students interested in entering this dynamic industry will come in more prepared to assist security leaders and businesses with a solid knowledge base of security risk management fundamentals. And once a rigorous ESRM body of knowledge is established, ASIS has the clout, expertise, and standing to provide a certification for academic institutions that meet concepts in their curriculum, which would will provide for a more consistent understanding of security's role.

ASIS has established ESRM as a global strategic priority and has formed an ESRM Commission to drive and implement this strategy. One of the commission's first steps is developing a toolkit comprising a primer and a maturity model.

Benefits to ASIS Members

There is a question I ask of every candidate I interview: “Tell me about a time when you've been frustrated in this industry.”

Every answer comes down to one of two issues. One, we do not know and cannot clearly define our role. Two, our business partners cannot clearly define our role. Both of these frustrations are manageable, and both are our fault as an industry for not establishing clarity. This leads to strained relationships with our business partners in how we are perceived and how likely our expert guidance is to be accepted.

Having a clearly defined security role through ESRM helps build a foundation for a more satisfying career in the security industry. It would provide us with proper standing in our enterprises, and better positioning for us to have a seat at the table for the right reasons, ones that executives understand and can support.

For the practitioner, a consistent security program through ESRM provides a framework to bring together security mitigation tasks under one proper umbrella: physical, investigations, cyber, information, business continuity, brand protection, and more.

The human resources industry has professionalized over the last decade or so. We see this through their standing within business, their seat at the table, and their upgrades in title and pay. Now, with the rise in threats and potential business disrupters, our industry has an opportunity. Business leaders and boards are looking for answers. We have the necessary skill sets and a dedicated and supportive professional association in ASIS to take the lead.

We are at a crossroads. It is time to choose the path of self-determination, take control of this conversation, and make the transition from trade to profession.

BRIAN J. ALLEN, ESQ., CPP, IS THE FORMER CHIEF SECURITY OFFICER FOR TIME WARNER CABLE, A FORMER MEMBER OF THE ASIS BOARD OF DIRECTORS, AND A CURRENT MEMBER OF THE ASIS ESRM COMMISSION.