The Security Leader's Bill of Rights

By Ray Bernard, PSP CHS III

For more than a decade security practitioners, risk managers and their professional associations have worked to elevate the importance of corporate security. *As a result, security risk is now a senior management and board level concern.*

In addition to the efforts of security and risk management professionals, escalating levels of homeland security risk and cybersecurity risk have also worked to bring security into the spotlights of ownership and senior management.

This means that security practitioners no longer have to "sell" management on the importance of security.

This is a big change—a good change and a long-awaited one—from the corporate security picture of 15 and 20 years ago.

With this big of a change, why hasn't *advancing the cause of security* gotten significantly easier? Due to information technology trends, there are basically two different answers to this question, depending upon your security practitioner role.

Corporate and Physical Security Leaders

For corporate and physical security leaders, many owners and managers think that stronger security simply means either "more of the same" or "doing a better job with what we have". They are not fully aware of the security implications of today's higher levels of business change and the resulting impact on the organization's risk picture. The rate of change and the multiplicity of impacts require more flexible and more adaptive approaches to security, including the selection of an appropriate security framework that is a good fit for the business.

IT Security Leaders

For IT security leaders, the increasingly rapid pace of information technology advancement, and the magnitude of the resulting business technology changes, have significant impacts on security planning and execution. Technology changes tend to create a technology-focused perspective. Technology changes poke holes in security at all levels: in individual security controls, in layers of protection, and in the application of security frameworks. Additionally, great change messes with high-level security thinking. When IT is still struggling to align information systems, services and the underlying infrastructure with the business—it is a significant challenge to align IT security align with the business.

Rights and Responsibilities

Security practitioners still have the same or greater responsibilities, and management is keenly aware of them. *But what about a security practitioner's rights?* This is not a new concept, but it is one that rarely gets any thought. And a key thought is this: **Failing to exercise your security leadership rights means that you may not be fully enabled to fulfill your security responsibilities.**

The flip side of that coin is, by **exercising your rights you can assure that you will be fully enabled, and properly supported, to do your job**.

The fact that ownership, senior management and the board are paying attention to security risks means that their thinking is consistent with the big picture for security, which is:

- **Business assets are the property of the business owners**, who have **delegated** the care and protection of those assets **to the executive management team**.
- **Risks to business assets**—and risk decisions, including decisions about security investments—**are the responsibility of executive management**.
- Because **executive management must make the important risk decisions**, security leaders **must** provide **security risk information and make risk treatment recommendations (people, process and technology)** to executive management so that they can make informed risk decisions to support and invest in appropriate risk treatment.
- The organization's **ownership**, **executive management**, and **security executives and managers** are all stakeholders in business security, *each with their own rights and responsibilities*.

These rights and responsibilities are presented below in three Security Bill of Rights statements for:

- Security Leaders
- Ownership
- Senior Management

The rights and responsibilities flow down from Ownership, to Senior Management and to then to the organization's Security Leaders by virtue of delegation.

A Security Leader's Bill of Rights and Responsibilities

Security Leaders have the right and responsibility to:

1. Develop security objectives, strategies and policies for the organization, for Senior Management approval or amendment

2. Identify security risks to the organization's critical assets and business functions, and their potential business impacts
3. Identify and develop security risk mitigation options and recommendations, including their costs and business impacts, for Senior Management approval or amendment
4. Monitor for and identify changes to the security risk picture, and to timely act on them
5. Keep Senior Management timely informed about changes to the security risk picture.
6. Keep Senior Management timely informed about the current state and rationale of corporate asset protection and legal and regulatory compliance
7. Have adequate organizational resources allocated for the achievement and implementation of the security objectives, strategies and policies approved by Senior Management
8. Receive visible support from the Senior Executives regarding the approved security objectives, strategies and policies, and their related security initiatives
9. Implement corporate security as an ongoing process, by means of a security framework or a security management system that incorporates continuous process improvement
10. Plan and execute security programs and projects to achieve the security objectives and implement the security policies set or approved by the Senior Executives
11. Maintain his or her continuing education in enterprise security risk management, organizational resilience and security operational excellence

(Note: Senior Management means the senior executives of the organization such as the Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Risk Officer and anyone in charge of a principal business unit or function.)

Ownership's Security Bill of Rights and Responsibilities

Ownership has the right to:

1. Delegate the care and protection of business assets to an executive management team.

Ownership has the right and responsibility:

2. Be kept accurately informed by Senior Management about the current state and rationale of corporate asset protection and legal and regulatory compliance.
3. Be timely informed by Senior Management about major security incidents, their actual and potential business impacts, and the organizational response actions planned and under way.
4. Approve or amend the organization's security objectives, priorities and strategies if desired.
5. Approve or amend security high-level policies and planning if desired.
6. Approve or amend large-scale security programs and projects if desired.

Senior Management's Security Bill of Rights and Responsibilities

Senior Management has the right and responsibility to:

1. Be informed about security risks to the organization's critical assets, their potential business impacts, and to be timely informed about changes to the security risk picture.
2. Be informed about the organization's security risk mitigation options including their costs and business impacts.
3. Set or approve the organization's security objectives, priorities and strategies.
4. Approve or amend security high-level policies and planning.
5. Approve or amend large-scale security programs and projects.
6. Provide visible support for the approved security objectives, strategies and policies, and their related security initiatives.
7. Be accurately informed about the current state and rationale of corporate asset protection and legal and regulatory compliance.
8. Keep ownership accurately informed about the current state and rationale of corporate asset protection, and legal and regulatory compliance.
9. Be accurately informed about current and projected security costs.
10. Be timely informed about security incidents, their actual and potential business impacts, and the organizational response actions planned and under way.
11. Establish a Chief Security Officer or other senior security executive position to lead and manage the organization's security functions. (In a small organization this responsibility may be assigned to an executive or manager with other non-security responsibilities.)
12. See that security is implemented as an ongoing process, by means of a security framework or a security management system that incorporates continuous process improvement.

Download this document from:
http://www.go-rbcs.com/articles/download-security-bill-of-rights