# CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## Security: A Key Enabler of Business Innovation

**Key Message**: Making security strategic to business innovation involves seven strategies and calculating risk-reward based on risk appetite.

**Executive Summary**

Protecting the security of information and the infrastructures that process, store, and transmit it is a critical business enabler for many of today's most innovative new initiatives. "In a world where employees, customers, partners, and even competitors around the globe can be collaborators in the business innovation process, security strategies have the power to make or break major business goals (product quality, time to market, customer loyalty, company reputation, and shareholder value)."

In this podcast, Roland Cloutier, Vice President and Chief Security Officer for EMC, and Laura Robinson of Robinson Insight, discuss how security can serve as a critical enabler for business innovation. Today's conversation is based on the first two reports in RSA's Security for Business Innovation series. Roland is a member of the Council that advises RSA. [Report #1]

---

**PART 1: THE SECURITY FOR BUSINESS INNOVATION INITIATIVE AND COUNCIL**

**Defining Business Innovation**

For the Security for Business Innovation series, business innovation is defined as "enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or achieve operational transformation." [Report #1, Report #2]

Innovation has become a top-level strategy for many organizations. That said, protecting the information that supports business innovation is usually not addressed strategically.

RSA formed the Security for Business Innovation Council to address this gap.

**RSA's Security for Business Innovation Council**

The Council is made up of ten senior security executives from global 1000 enterprises, both U.S. and international, representing a range of market sectors. The list of Council members is available.

**Report #1: The Time Is Now: Making Information Security Strategic to Business Innovation**

The first report in a planned four-report series identifies seven strategies that connect security to business innovation. These are:

1. Have the right mindset. Security professionals know that their job is to enable the business, not inhibit it.
2. Know the business and speak the business
3. Recognize and seize opportunities to add value
4. Build relationships and win influence
5. Become a risk-versus-reward expert
6. Build repeatable processes
7. Make time for strategic thinking

---

## PART 2: SECURITY MUST SPEAK THE BUSINESS; INTRODUCING RISK-REWARD

### Connecting Security with the Business

Security leaders and staff must develop their ability to understand what their organization delivers to their end-users and customers; in other words, what is at the end of the Internet that you are responsible for protecting.

Security's capacity to drive a protection program is based on its ability to understand the business value chain and how services are delivered.

Speaking the business means being able to articulate risk in business terms as it relates to the delivery of products and services.

Security's success relies on the ability to translate security needs and initiative to business impact and business risk mitigation.

### The Unique Role of the Security Executive in Business Innovation

Security executives need to understand both long-term strategy and short-term goals, for example:

- designing new third-party access solutions so partners can access intellectual property and trade secrets safely and securely
- providing technical services faster, quicker, and cheaper
- ensuring that the organization has the infrastructure resources it requires to go global

Security executives:

- examine each new business initiative to communicate both business impact and security impact
- serve as capable, competent internal consultants to the business

### EMC's Theater Threat Management Program

One specific EMC example is their Theater Threat Management Program that addresses risks associated with moving into new countries.

The Program answers the question "What are my (geopolitical, economic, infrastructure, cyber) risks?" It presents country-by-country analyses with respect to assets that need to be deployed and services that can be offered, keeping risks in mind.

This Program allows EMC to conduct business anywhere, anytime – so business leaders actively seek Security's expertise before making plans and commitments.

This is one example where security and business innovation go hand-in-hand.

### Security and Risk Joined at the Hip

In helping craft solutions to mitigate risk, Security helps answer these questions:

- What are you putting at risk?
- What are the downstream impacts of a bad security decision, and what is it going to take to recover? Examples include:
    - brand equity
    - ability to market products and services in a specific region
    - liability costs resulting from negative impacts

**Report #2: Mastering the Risk-Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards**

The second report describes a step-by-step process for making risk-reward calculations for new business initiatives.

**The Risk-Reward Equation**

Risk assessment addresses:

- the type of information
- its level of sensitivity
- protection requirements
- how the information is being stored, processed, and transmitted
- threats and vulnerabilities
- systems and applications that use the information
- the likelihood and impact of compromising events

Most risk assessments only examine potential impacts of realized risks – the negative perspective.

The risk-reward equation determines the right level of controls to implement given an acceptable level of risk. This means that risk owners are willing to take responsibility for a defined level of risk in order to maximize rewards.

If Security is going to enable business innovation, it needs to focus on rewards.

---

**PART 3: DETERMINING RISK APPETITE; USING A SELF-SERVICE MODEL; FUTURE REPORTS**

**Risk Appetite; Risk Threshold**

Security professionals typically think about the downside: cost and loss avoidance.

Security's job is to serve as an internal consultant, stating "Here's the problem. Here's how we fix it. And here's how you can remediate it, or here is how you can avoid it."

A significant factor is determining an acceptable level of risk – risk appetite. Risk appetite stays fairly constant in all baseline risk and security assessments.

That said, security executives observe business leader behavior to determine if they are willing to accept more risk, and then capture this as a trend.

An effective way to confirm a change in risk appetite is to say "So I understand that you're okay with this type of risk, because for the last three months you've accepted things at this level. Is this going to continue?"

This ongoing dialogue becomes part of the decision making process.

**Security Action based on Risk Appetite**

If Security personnel know what the risk level is, they provide leaders with options at that level. Then they monitor progress and occasionally check in, conveying to leaders that they understand the business context.

**Using a Self-Service Model**

In more mature information security programs, Security provides business leaders with a security self-service model that is embedded within their project organizations.

Some example questions that are asked at the beginning of any new project definition include:

- What type of information are you touching?
- Is it internal or external?
- Is PCI (Payment Card Industry) or PII (Personally Identifiable Information) data involved?

Each self-service model produces a risk score. The score is an indicator of what risk services are needed by the project, for example:

- a full risk assessment
- an application assessment
- a security technology review
- meeting a regulatory requirement
- the need to budget "x" hours for any or all of these as part of the project budget

The self-service model sets expectations up front and ensures there are no surprises at the end.

**Self-Service Tools**

Security also provides self-scanning tools so projects can examine their products throughout the entire development life cycle.

**Establishing Decision Authority**

At EMC, the Executive Security Council is the oversight committee. Members include an executive chair and vice-chair (business VP/SVP), CFO (Chief Financial Officer), CIO (Chief Information Officer), CSO (Chief Security Officer), General Counsel, and a few others.

The Council determines what roles can accept what levels of risk. Company-wide issues are resolved at the Council level. The CSO does not accept risk; all risks are accepted by business executives.

The decision process allows for mediation and escalation if a decision cannot be reached.

**Future Reports**

Report #3 is titled "Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy."

This report addresses moving business innovation forward in a tough economy, including these questions for security leaders:

- How do you determine priorities?
- How do you get the resources you need?
- How do you build the rationale for key processes?
- How do you share costs with the business?
- Where should you use automation?

The fourth report, yet to be released, will examine what a future security model might look like given globalization and all of today's new business challenges. Topics that may be covered include cloud computing, virtualization, social networking, and the explosion in mobile devices.

**Resources**

RSA's Security for Business Innovation web site

Report #1: The Time Is Now: Making Information Security Strategic to Business Innovation

Report #2: Mastering the Risk-Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards

Report #3: Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy

Corporate Executive Board's Information Risk Executive Council

Department of Homeland Security's US-CERT