

Synopsis of the Report
based on discussions with the

Security for Business Innovation Council

An industry
initiative
sponsored by
RSA



ABN AMRO

DR. MARTIJN DEKKER,
Senior Vice President, Chief
Information Security Officer

ADP INC.

ROLAND CLOUTIER, Vice
President, Chief Security Officer

AIRTEL

FELIX MOHAN, Senior Vice
President and Chief Information
Security Officer

THE COCA-COLA COMPANY

RENEE GUTTMANN, Chief
Information Security Officer

CSO CONFIDENTIAL

PROFESSOR PAUL DOREY,
Founder and Director; Former
Chief Information Security
Officer, BP

EBAY

DAVE CULLINANE, Chief
Information Security Officer and
Vice President, Global Fraud,
Risk & Security

EMC

DAVE MARTIN, Chief Security
Officer

GENZYME

DAVID KENT, Vice President,
Global Risk and Business
Resources

HDFC BANK

VISHAL SALVI, Chief
Information Security Officer and
Senior Vice President

HSBC HOLDINGS plc

ROBERT RODGER, Group Head of
Infrastructure Security

JOHNSON & JOHNSON

MARENE N. ALLISON,
Worldwide Vice President of
Information Security

JPMORGAN CHASE

ANISH BHIMANI, Chief
Information Risk Officer

NOKIA

PETRI KUIVALA, Chief
Information Security Officer

NORTHROP GRUMMAN

TIM MCKNIGHT, Vice
President and Chief Information
Security Officer

SAP AG

RALPH SALOMON, Vice
President, IT Security & Risk
Office, Global IT

T-MOBILE USA

WILLIAM BONI, Corporate
Information Security Officer
(CISO), VP Enterprise Information
Security

WITH GUEST CONTRIBUTOR:

WILLIAM PELGRIN, President
& CEO, Center for Internet
Security; Chair, Multi-State
Information Sharing and
Analysis Center (MS-ISAC); and
Immediate Past Chair, National
Council of ISACs (NCI)

GETTING AHEAD OF ADVANCED THREATS

Achieving Intelligence-Driven Information Security

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES



This synopsis is a brief summary of a comprehensive report on this topic. To view the full report or other reports on this topic please go to www.rsa.com/securityforinnovation.



The Need for Cyber-Risk Intelligence



In today's threat landscape, organizations worldwide face a growing number of sophisticated cyber adversaries. "Advanced threats" are increasingly targeting corporations and governments in order to conduct industrial espionage, undermine business and financial operations, and/or sabotage infrastructure. The hard truth is most organizations don't know enough about the threats or their own security posture to adequately defend themselves against the rising tide of cyber attacks.

Today's dedicated adversaries have the means to evade commonly used defenses such as signature-based detection. In the era of advanced threats, greater situational awareness is essential to effectively detect and mitigate cyber attacks. Organizations need to obtain the latest data on threats, relate that to real-time insights into their dynamic IT and business environments, determine what's relevant, make risk decisions, and take defensive action. Yet most IT security programs are not set up for this.

The ninth report of the Security for Business Innovation Council (SBIC) calls for a fresh and comprehensive approach to information security. It provides a playbook for building an organizational competency in cyber-risk intelligence, including fully leveraging data from internal and external sources to detect, predict, prevent, and defend against cyber attacks.

The value proposition is clear. By harnessing the power of information, the organization can create and implement more precise defensive strategies against evolving threats. Security will not only improve but also become more cost-effective because it will be targeted at countering the most significant threats and protecting the most strategic assets.

"The threat can be broken down into three components: intent, opportunity, and capability. Organizations need to know, 'What is the intent of adversaries? What are the opportunities available to them? And what capabilities do they have to exploit the opportunities?'"

FELIX MOHAN, Senior Vice President and Chief Information Security Officer, Airtel



Actionable Intelligence

For this report, "cyber-risk intelligence" is defined as "knowledge about cyber adversaries and their methods combined with knowledge about an organization's security posture against those adversaries and their methods." The goal is to produce "actionable intelligence," which is knowledge that enables an organization to make risk decisions and take action. To gain that knowledge, organizations must take input data and process it.

Data is available from a range of sources, including open source data that is publicly available to classified sources. It comes in many formats, such as word-of-mouth, emails, news feeds, automated data streams, output of numerous internal and external sensing platforms, and custom research. Some types, such as a list of IP addresses on a watch list, are generally applicable to all organizations. Other types are unique to an organization, for example notification that it is being targeted by a particular group.

Collecting more and more data is not the end goal, though. Having volumes of unanalyzed or unused data is of no value. An organization must produce actionable intelligence through analysis and by fusing the data with other relevant facts. To be valuable, the data must result in intelligence that can be applied defensively, for immediate action in combatting a current or imminent cyber-attack and/or for informing defensive strategies. The report presents categories of cyber-risk data including examples of sources, formats, and potential defensive applications.



A New Approach

DEFINITION: Intelligence-driven information security

Developing real-time knowledge on threats and the organization's posture against those threats in order to prevent, detect, and/or predict attacks, make risk decisions, optimize defensive strategies, and enable action.

There is mounting evidence that organizations are increasingly targeted by sophisticated adversaries. For example, the Enterprise Strategy Group surveyed companies in the U.S. and Europe regarding advanced persistent threats (APTs) and found that 59% of security professionals surveyed at U.S. companies¹ and 63% of those at European companies² believe it is “highly likely” or “likely” that their organizations have been APT targets.

In today's threat landscape, organizations face targeted, complex, multi-modal attacks which can be carried out over periods of time. The time has come when successful defense requires evolving past conventional approaches in information security.

A new approach, called “intelligence-driven information security” includes:

- ➔ The consistent collection of reliable cyber-risk data from a range of government, industry, commercial, and internal sources to gain a more complete understanding of risks and exposures.
- ➔ Ongoing research on prospective cyber adversaries to develop knowledge of attack motivations, favored techniques, and known activities.
- ➔ The growth of new skills within the information team focused on the production of intelligence.
- ➔ Full visibility into actual conditions within IT environments, including insight that can identify normal versus abnormal system and end-user behavior.

“It can be hard to digest having to develop a multi-year plan to learn who your adversaries are and how they're going to steal from you. Quarter-by-quarter, you may not see any losses. It could be years until you see the losses – when all of a sudden, out of the blue, a company in another part of the world becomes the leader in your space, having subsidized itself with your R&D investments.”

- ➔ A process for efficient analysis, fusion, and management of cyber-risk data from multiple sources to develop actionable intelligence.
- ➔ Practices to share useful threat information such as attack indicators with other organizations.
- ➔ Informed risk decisions and defensive strategies based on comprehensive knowledge of the threats and the organization's own security posture.

Improving Information Sharing

Sharing cyber-risk intelligence and defensive strategies has become imperative in today's threat landscape. One of the most propitious aspects is the exchange of cyber-attack indicators. If large communities of organizations could readily and continuously exchange data on current attack methods, it would seriously impede attackers' operations.

Most information-security professionals have established informal networks of trusted contacts at other companies. Informal networks can be invaluable; they are often the most frequent way organizations share information. However, informal networks do not enable information sharing on a large scale.

For achieving large-scale exchange of information, there are a growing number of industry or government-led information-sharing initiatives as well as public/private partnerships. As information-sharing groups have gained experience, a set of criteria for success has emerged

including a formalized structure, adequate funding, protocols for data exchange, legal framework, standardized procedures, and genuine participation. Trust and timeliness are essential components for information sharing.



TIM MCKNIGHT, Vice President and Chief Information Security Officer, Northrop Grumman

¹U.S. Advanced Persistent Threat Analysis: Awareness, Response, and Readiness among Enterprise Organizations, Enterprise Strategy Group, October 2011

²Western Europe Advanced Persistent Threat (APT) Survey, Enterprise Strategy Group, October 2011



Recommendations

The report lays out a six-step roadmap to achieving intelligence-driven information security:

- 1 Start with the Basics**
Inventory strategic assets, strengthen incident-response processes, and perform comprehensive risk assessments.
- 2 Make the Case**
Communicate the benefits of an intelligence-driven security program to executive management and key stakeholders. Identifying “quick wins” to prove value out of the gate is essential for gaining broad organizational support, including funding.
- 3 Find the Right People**
Look for professionals who can blend technical security acumen with analytical thinking and relationship-building skills.
- 4 Build Sources**
Determine what data from external or internal sources would help prevent, detect, or predict attacks; evaluate sources on an ongoing basis.
- 5 Create a Well-Defined Process**
Codify a standardized methodology to produce actionable intelligence, ensure an appropriate and timely response, and develop counter-measures.
- 6 Implement Automation**
Find opportunities to automate the analysis and management of large volumes of data from multiple sources.

“You get a fire hose of information from potentially thousands of sources and need somewhere to put it – ideally a platform that enables fast searches in an un-normalised form, rapid analysis, and automated anomaly detection.”



ROBERT RODGER, Group
Head of Infrastructure Security,
HSBC Holdings plc

Conclusion

In this era of advanced threats, conventional approaches to information security are no longer sufficient. An intelligence-driven approach can deliver comprehensive situational awareness, enabling organizations to more effectively detect and mitigate cyber attacks.

Developing a cyber-risk intelligence capability will take investments in people, process, and technology. It will challenge the information-security team to grow beyond the current skill set and to commit to a change in mind-set. And it will require not only the steadfast efforts of the security team but also broad organizational support.

Although many organizations have developed capabilities in competitive and market intelligence to understand their competitors and customers, most have not developed a cyber-risk intelligence program. Given that most business processes and transactions are now conducted in cyber space, activities such as fraud, espionage, and sabotage have also moved online. Cyber-risk intelligence has become a required competency to understand the online risks.

Advanced threats represent an escalating risk to business innovation. This report lays out a roadmap to achieving intelligence-driven information security in order to get ahead of the threats and protect critical information assets.





About the Security for Business Innovation Council Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies.

Yet there is still a missing link. Though business innovation is powered by information, protecting information is typically not considered strategic – even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or the organization could be put at great risk.

At RSA, we believe that if security teams are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with top security leaders from around the world to drive an industry conversation and chart the way forward.

