Report *based on* discussions *with the*

Security for Business Innovation Council

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

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

AstraZeneca
SIMON STRICKLAND, *Global Head of Security*

Automatic Data Processing
ROLAND CLOUTIER, *Vice President, Chief Security Officer*

The Coca-Cola Company
RENEE GUTTMANN, *Chief Information Security Officer*

eBay
LEANNE TOLIVER, *Office of the Chief Information Security Officer*

EMC Corporation
DAVE MARTIN, *Vice President and Chief Security Officer*

FedEx
DENISE D. WOOD, *Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer*

Fidelity Investments
TIM MCKNIGHT, *Executive Vice President, Enterprise Information Security and Risk*

HDFC Bank
VISHAL SALVI, *Chief Information Security Officer and Senior Vice President*

HSBC Holdings plc.
BOB RODGER, *Group Head of Infrastructure Security*

Intel
MALCOLM HARKINS, *Vice President, Chief Security and Privacy Officer*

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*

SAP AG
RALPH SALOMON, *Vice President IT Security and Risk Office*

TELUS
KENNETH HAERTLING, *Vice President and Chief Security Officer*

T-Mobile USA
WILLIAM BONI, *Corporate Information Security Officer (CISO) and Vice President, Enterprise Information Security*

Walmart Stores, Inc.
JERRY R. GEISLER III, *Office of the Chief Information Security Officer*

TRANSFORMING INFORMATION SECURITY

Future-Proofing Processes

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

- **Where to focus process improvement**
- **How to optimize key security processes**
- **Guidance on documenting business processes**
- **Upgraded techniques for risk assessment**
- **Achieving evidence-based controls assurance**
- **Tips for attaining a data analytics capability**

An industry initiative sponsored by RSA

Contents

Report Highlights

THE AD-HOC PROCESSES put in place for the days of perimeter-based security can't handle the scale and complexity of managing cybersecurity risks for a global enterprise today.

KEEPING PACE WITH CYBER threats and the latest business and technology trends requires an overhaul of information security processes.

KEY AREAS FOR IMPROVEMENT in many organizations are:

Risk Measurement: Describing risks in technical terms such as "number of intrusions or vulnerabilities" makes it difficult to advise business leaders on how to manage cybersecurity risks.

Business Engagement: The processes for tracking risks should be easy and efficient for the business to use, but are often still based on cumbersome manual methods.

Controls Assessments: Point-in-time, piecemeal assessments are no longer sufficient. The health of security controls should be measured as a continuity of capabilities.

Third-Party Risk Assessments: The current model of risk assessment is inefficient, repetitive, and does not provide ongoing visibility into the service provider's security controls.

Threat Detection: An intelligence-driven security approach is required, but most security teams are still unsure about what data to collect and how to perform meaningful analysis.

This report provides a valuable set of recommendations from 19 of the world's leading security officers to help organizations build security strategies for today's escalating threat landscape.

FIVE RECOMMENDATIONS zero-in on how to address critical issues, move information security programs forward, and prepare for the future:

1. SHIFT FOCUS FROM TECHNICAL ASSETS TO CRITICAL BUSINESS PROCESSES

Move away from a strictly technical viewpoint of protecting information assets, such as servers and applications. Take a bigger-picture perspective by looking at how information is used in conducting business. Think about how to protect the most critical business processes from end-to-end. Work with business units to document critical business processes.

2. INSTITUTE BUSINESS ESTIMATES OF CYBERSECURITY RISKS

Develop techniques for describing cybersecurity risks in business terms and integrate the use of business estimates into the risk-advisory process. Define detailed scenarios which describe the likelihood of security incidents and the magnitude of business impact. Where feasible or required, quantify the risk and increasingly move towards financial estimates.

3. ESTABLISH A BUSINESS-CENTRIC RISK ASSESSMENT PROCESS

Move to more automated tools for tracking information risks as they are identified, evaluated, accepted, or remediated, in order to speed decision-making and enable business units to be held accountable for managing risks. Look to service providers for mundane, repetitive assessments. Build flexibility into the risk-acceptance process to enable the business to take advantage of time-sensitive opportunities.

4. SET A COURSE FOR EVIDENCE-BASED CONTROLS ASSURANCE

Develop the capability to collect relevant data to test the efficacy of controls on an ongoing basis. Begin by documenting and reviewing controls, focusing on the most important controls that are protecting critical business processes. Determine what evidence will attest to each control and set up procedures to collect and report evidence systematically and make continual adjustments. Over time, automate collection of evidence and reporting in order to improve internal and third-party assessments.

5. DEVELOP INFORMED DATA COLLECTION METHODS

Start by looking at the types of questions data analytics can answer in order to identify relevant sources of data. Build a set of data analytics use cases. Modify logging where original data is insufficient, negotiating with system owners when necessary. Know how to apply external threat intelligence to enrich analysis. Comprehensively plan to improve overall collection architecture, produce more data-rich logs, and increase data-storage capacity.

1 Introduction: Preparing for Tomorrow

The ad-hoc processes put in place for the days of perimeter-based security can't handle the scale and complexity of managing cybersecurity risks for a global enterprise today. Forward-thinking security teams recognize that keeping pace with cyber threats and the latest business and technology trends requires an overhaul of their information security processes.

Based on the perspectives of some of the world's leading information security executives, this report examines the key areas in security programs that need attention now. It provides actionable recommendations for new processes and upgraded techniques, enabling security teams to face today's issues and prepare for tomorrow's.

Read the first report

What does an effective and forward-leaning information security program look like?

The Security for Business Innovation Council (SBIC) is producing a series of three reports on "Transforming Information Security" to answer that question. Fusing the knowledge and vision of top information security leaders, the reports deliver actionable recommendations. The first report was a playbook for designing a state-of-the-art extended team. This report explores the forefront of information security processes. The third will identify some of the essential technologies for evolving information security programs.

2 Key Areas for Improvement

If security programs were issued report cards evaluating their processes, in most organizations the following areas would be identified as "not meeting expectations – needs improvement."

1. Risk Measurement

Executives and boards of directors worldwide have come to realize that cybersecurity risks can significantly affect a company's bottom line. Recent events have demonstrated the magnitude of impact. Over the past 12 months, many banks have been hit by Distributed Denial of Service (DDoS) attacks targeting their online banking sites. A report by the IP Commission released earlier this year estimated the scale of international theft of American intellectual property to be in the hundreds of billions of dollars per year.[1]

Seeing the potential for greater financial losses, business units in many organizations are getting more interested in proactively managing their cybersecurity risks. From their perspective, cybersecurity risks are best described just as other risks are – in financial terms. Further, the U.S. Securities and Exchange Commission (SEC) expects U.S. public companies to disclose material information regarding cybersecurity risks and incidents.[2] In the EU, the Markets in Financial Instruments Directive (MiFID) requires financial-services companies to adopt adequate risk-management measures.[3]

The information security team must advise business leaders on how to manage cybersecurity risks, report on "materiality," or demonstrate "adequacy." This is difficult to do if risk is only described in technical terms such as the number of intrusions or vulnerabilities.

2. Business Engagement

As business units begin to take more responsibility for managing their own cybersecurity risks, the security team must work in partnership with them to ensure they are successful. The process for identifying, evaluating, triaging, and tracking risks should be easy and efficient, and should enable the business to respond to competitive market pressures. Yet risk-assessment processes are often still based on cumbersome manual methods.

3. Controls Assessments

In most organizations, assessments to verify that security controls are working as intended are typically performed on a sporadic basis by various internal and external auditors. Point-in-time, piecemeal assessments are no longer sufficient. Given escalating threats and increasing security investments, security teams are expected to ensure that controls are efficient and effective at all times. The health of security controls should be measured as a continuity of capabilities. Still, most security teams don't consistently evaluate controls or make continual adjustments to them.

4. Third-Party Risk Assessments

The conventional model for risk assessment is questionnaires and on-site audits, with results recorded in documents and updated annually. For both service providers and their customers, this is an inefficient process with repetitive work on all sides. Moreover, it does not provide organizations with ongoing tactical and operational visibility into the service provider's security controls to ensure that the provider is meeting requirements for protecting information.

5. Threat Detection

It is well-established in the industry that advanced threats require organizations to move quickly towards more intelligence-driven detection approaches. Relying solely on monitoring events from perimeter network infrastructure is no longer effective. Intelligence-driven security makes use of data analytics, enables alerts on behaviors indicative of exploitation, and provides threat context. It requires the collection and analysis of data from a wide range of sources. Yet most security teams are still unsure about what data to collect and how to perform meaningful analysis.

[1] The Report of the Commission on the Theft of American Intellectual Property, National Bureau of Asian Research, 2013.
[2] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[3] http://ec.europa.eu/internal_market/securities/isd/mifid/index_en.htm

③ Recommendations

These recommendations are not intended as a comprehensive "how-to" for re-engineering security processes; instead, they zero-in on how to fix some of the key processes that need attention in order to address critical issues, move information security programs forward, and prepare for the future.

1. Shift Focus from Technical Assets to Critical Business Processes

To address the shortcomings in today's security processes, the first thing to do is to step back and reconsider how to frame the problem. Traditionally, information security professionals have thought in terms of protecting information assets, such as servers and applications. This technical viewpoint, although necessary, is not sufficient – it does not provide enough context regarding how information is used in conducting business. And it will have limited success against targeted attacks, which are designed specifically to undermine business processes such as customer orders, financial transactions, product-development or manufacturing processes, or accounts receivable procedures. Instead, take a bigger-picture perspective and think about how to protect critical business processes from end-to-end.

Change Your Perspective

By shifting emphasis from technical assets to business processes, the security team will have a more informed perspective and know where to focus their efforts. They can determine which processes are the most critical and need the most protection. Knowing how information flows within each process, they can understand how an attacker might be able to thwart a process and what security controls would be most effective.

Recommendations

1. **Shift Focus from Technical Assets to Critical Business Processes**
2. **Institute Business Estimates of Cybersecurity Risks**
3. **Establish a Business-Centric Risk Assessment Process**
4. **Set a Course for Evidence-Based Controls Assurance**
5. **Develop Informed Data-Collection Methods**

UNDERSTANDING BUSINESS PROCESSES FACILITATES BUILDING IN SECURITY RATHER THAN BOLTING IT ON.

Consider a new-product-development process. If the security team has no knowledge of the process, they will not know what "normal" activity is, such as how and when individuals from the design team access the design application, how and when emails are used to communicate specifications to third-party contractors, and so on. By delving into the process, they will be better-equipped to instrument controls to discover and prevent non-normal conditions and protect the intellectual property.

With knowledge of business processes, the security team can see how security controls affect processes with an eye towards minimizing friction. For example, in examining the steps in a business process, it may be possible to remove the need to transfer confidential data, in turn eliminating the need for encryption. In some cases, it might be necessary to make minor modifications to a business process in order to make monitoring more effective. For example, it is hard to detect that an intruder is stealing information by downloading transaction data if normal usage calls for downloading all the transactions in a database every day.

Understanding business processes facilitates building in security rather than bolting it on. For instance, a procurement process could incorporate a protocol for the purchasing team to screen for a list of security and privacy issues. It also helps the security team to see that technical security controls are not necessarily the only solution for securing a process. If there's a problem with access certification, for instance, putting a manual reconciliation step into the process may be an effective solution.

> *Documenting business processes has to be a collaborative effort, to decide what the risks are to the system. We'll never understand the business value of the information to the same degree as the business owner, and they'll never understand the threats to the same degree as the security team.*

DAVE MARTIN
Vice President and Chief Security Officer, EMC Corporation

9 QUESTIONS TO ASK IN DOCUMENTING BUSINESS PROCESSES

Documenting processes for data-protection purposes generally involves going through the processes step-by-step, detailing how information is used. Examples of relevant questions are:

- **Is any confidential, sensitive, or regulated data being generated, exchanged, or stored as part of this process? If yes, what existing security controls are part of this process? Is the use of this information being monitored? How?**
- **How you would know if something went wrong in the business process? Are there detective controls at those key points? Is the right information being logged? Is monitoring consistent with potential indications of compromise or fraud?**
- **Are there privacy issues in terms of where data is stored and moved? For example, is data going from Europe to the U.S. without appropriate legal paperwork in place?**

Get Business Processes Documented

Understanding business processes requires documentation. The security team will need to work with personnel in the business units in order to get critical processes documented (see sidebar). Each process description should be a living document requiring an owner in the relevant business unit who will be responsible for keeping it current. Companies with a continuous quality improvement (CQI) or business process improvement (BPI) team might have documentation that can be used as a starting point, but often companies have little to no existing documentation. It may be possible to leverage personnel from the organization's business resiliency, business continuity, or internal audit group to help do business process documentation.

2. Institute Business Estimates of Cybersecurity Risks

Effective information risk management today requires the security team to act as risk advisors to the business units and executives. For risk-advisory services to succeed, the security team should develop methods for describing cybersecurity risks in business terms and integrate the use of business estimates into the risk-advisory process.

An effective approach for describing cybersecurity risks in business terms is defining detailed scenarios, articulating the likelihood of security incidents and the magnitude of business impact such as reputation loss, regulatory non-compliance, or lawsuits. Where feasible or required (e.g., for SEC 10K filings of material risk), the security team should be able to have business-impact discussions in order to quantify risk. Over time, the team should hone their risk-quantification techniques and become proficient at approximating projected monetary losses. Often this involves working with business units to determine the financial impact of potential events such as business processes going off-line, product designs getting stolen, regulated data being exposed, and so on.

Quantifying cybersecurity risks in financial terms is a nascent field. There are often concerns among security professionals that risk quantification could lead to analysis paralysis and long discussions defending the numbers. Keep in mind that as with other business estimates, such as sales forecasts, it is not possible to make precise calculations. An order-of-magnitude estimate is often sufficient, e.g., is it a $1 million, $10 million, or $100 million risk? To business executives, a reasonable but inexact financial estimate will be more informative than a technical description of risk.

One of the pitfalls of financial estimates is to over-engineer estimates of likelihood or frequency of events. Instead it is important to focus primarily on determining the financial impact. The fact that something is only a "once-in-a-century event" doesn't matter if it happens to your organization.

Leverage Risk-Quantification Tools

Security teams can get a sense of the magnitude and likelihood of possible monetary losses from reports about major information security incidents in similar companies. Most organizations have data from previous incidents of their own. Some also use tools such as the FAIR (Factor Analysis of Information Risk) standard nomenclature and framework for performing risk analysis. Many in the financial-services industry use the Operational Risk eXchange Association's (ORX) data, which provides anonymous data of actual operational risk events and the associated scale of loss.

Business estimates of cybersecurity risks will enable organizations to better weigh risk versus reward, determine appropriate levels of risk-mitigating investments, and prioritize cybersecurity risks against other types of risks in the enterprise. Using business estimates will also facilitate discussions of the "materiality" of cybersecurity risks or the "adequacy" of risk-management programs as required by regulations such as the SEC guidance or MiFID.

MARTIJN DEKKER
Senior Vice President, Chief Information Security Officer, ABN Amro

"The security profession is under pressure now to come up with ways to quantify security risks. Because as organizations spend more on security, they're asking 'Why are we spending so much on this? How big are the risks?' It's becoming more and more important that we can justify that spend."

3. Establish a Business-Centric Risk Assessment Process

In many organizations today, information security risk assessments are still done using spreadsheets. Typically, at the start of a project, the project owner fills out a form following a spreadsheet template and emails it to the security team. The security team uses the information provided in the form and in follow-up discussions to assess the risk and recommend a risk-mitigation strategy.

With this method, there is little provision for personnel in the business units to regularly maintain and review an up-to-date picture of the risks that belong to them. It is also difficult for the security team to get a composite view of all of the risks throughout the enterprise.

Automate the Process

Moving to more automated tools can make procedures much less cumbersome. Automation can speed decision-making and make it workable for business units to be held accountable for

managing information risks. Many organizations are automating the risk-assessment process using governance, risk, and compliance (GRC) tools. Business units and the security team can track risks as they are identified, evaluated, accepted, or remediated through the GRC system. A more automated and measurable process better integrates into an overall enterprise risk management perspective and better aligns the security organization to the company.

The following example illustrates a risk-assessment process based on a relatively new approach which incorporates an outsourced service provider and integrates the service with the enterprise's GRC system. By using a service provider for mundane and repetitive assessments, the process eases the load for the business units and security team.

In this approach, business units starting new projects are required to purchase a risk assessment from the security team's designated service provider and budget for follow-up assessments. The service provider performs the assessments and inputs the findings directly into the GRC system. Once an assessment is complete, the security team and business unit have immediate access to the results, which also roll up into an overall picture of information risks.

For more routine projects, the risk officer within the business units coordinates the remediation, making sure they have actionable plans to address the identified risks according to the security team's standards and within a specified period. The risk officer then reports back on their progress to the security team. For projects that go over a specified threshold of risk, the security team is called in for further analysis and to work with the business to develop more custom risk-remediation and acceptance plans. An added benefit of using risk assessment as a service is that it can be easily accounted for based on a cost-of-goods-sold model, using the business unit's budget instead of the security team's resources.

Build Flexibility into Risk Acceptance

Organizations must often balance the need for risk management with the need to get new products and services to market quickly. To enable the business to take advantage of time-sensitive opportunities, the security team should allow the business units to accept a higher level of risk than they normally would for a short period of time. In this case, the organization's risk management committee (such as the CISO, General Counsel, Chief Procurement Officer, and others) would provide the initiative with a formal risk exemption for, say, a six-to-18-month period, at which point the risks are revisited. This type of success-based risk remediation model increases the security controls proportionally to the success of the product or service. For example, it might make business sense to accept higher risks for a small initial number of customers, with the understanding that once the product or service has a significant number of customers, it will have the revenue stream to justify security enhancements. The residual risks (other than accepted risks) would be quantified and managed.

> *"A key aspect of risk management is having a process in place to ensure that for every initiative in your organization, a risk assessment is done at a very early stage in the lifecycle."*

VISHAL SALVI

Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

***OLD-SCHOOL* VS STATE-0F THE-ART APPROACH TO RISK-MANAGEMENT PROCESSES**

Old School	State-of-the-Art
Ad-hoc methods	Formalized, consistent processes built into business processes
Technical descriptions of risk	Risk quantified in monetary amount losses with percent likelihood
Treat all risks equally	Prioritization system that sets threshold for priority risks
Security considered responsible for risk management	Shared responsibility for risk management: The business units own the risk/reward decisions and there is a process in place to hold them accountable for managing their risks
Risk-acceptance process is uniform	Flexible risk-acceptance model whereby for certain select business opportunities higher risks are accepted on short-term basis to enable fast time to market
Risk reviewed in silos	Holistic view of risk enabled through automation

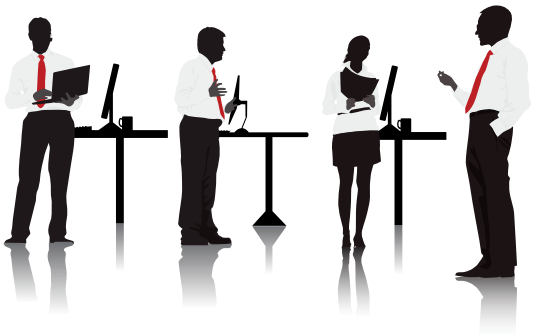
4. Set a Course for Evidence-Based Controls Assurance

Organizations today must ensure that security controls are constantly meeting standards, protecting against real-time threats, providing value for the investment, and enabling business agility. The most effective way to achieve this is evidence-based controls assurance, which involves ongoing collection of relevant data to test the efficacy of controls.

Although it takes time to set up and requires a high level of maturity with respect to security and IT processes, evidence-based controls assurance is becoming a required competency for security teams. It will provide for more transparency, facilitate early identification of defective controls

Evidence-based controls assurance is becoming a required competency for security teams.

or control failures, and enable remediation of issues and optimization of the protection strategy through continuous adjustments. Having a stream of evidence will also make it considerably easier for organizations to demonstrate compliance. Audits will be more efficient and less disruptive.



A TYPICAL AUDIT PROCESS

In a typical audit process, auditors pull staff away from their usual work to ask for evidence of compliance.

AN AUDIT PROCESS WITH CONTINUOUS CONTROLS MONITORING

With continuous controls monitoring, a system ingests logs which attest to the efficacy of controls. Ideally, auditors can query the system or view reports without disrupting normal work.

the 80/20 rule

Quality not Quantity

COMPANIES IN HEAVILY REGULATED industries may need to ultimately document, review, and gather evidence on all of their security controls. For other companies, however, it often makes sense to prioritize on a small subset of security controls: the most important controls protecting only the most critical business processes.

FOR MANY ORGANIZATIONS, THE 80/20 rule applies: twenty percent of controls provide the vast majority of security. Try to identify these early and focus on documenting, reviewing, and gathering evidence on them. Don't aim for quantity when it comes to evidence-based controls assurance – what matters is not the number of controls, but that you gain visibility into the controls your organization relies on the most.

Document Controls

The first step in implementing evidence-based controls assurance is to document the organization's security controls as a set of statements that can be verified or measured. Focus on the most important controls that are protecting critical business processes (see sidebar).

A simple example of a control statement is a description of password use including length, complexity, and update requirements. For a data-protection control, the description might include how data is tagged, encrypted, and watermarked and what tools are required. The documentation process can often involve refactoring long documents into a set of discrete statements.

Perform a Controls Review

Use the opportunity of documenting the controls to also do a comprehensive review of all of the controls. Ask questions to ascertain, for example: Is each control still needed? In the right place? Redundant? Outdated? Inefficiently operated? Creating unnecessary load on business processes? Causing convoluted user experience? Effective given current threats? As well, what does the control cost? Underperforming controls should be managed at a lower cost or scheduled for decommission and/or replacement.

Gather Evidence

The next step is to determine what evidence will attest to each control (see chart below for examples) then set up procedures to systematically collect and report this evidence. The security team needs to ask, "What is our short- and long-term capability to be able to demonstrate this evidence?" Over time, more of the collection and reporting can be automated, enabling organizations to find out about issues much sooner than with regular manual checks. Linking and combining results gathered via vulnerability and threat management activities is crucial to identifying defects in controls at an early stage.

EXAMPLES OF
EVIDENCE FOR DIFFERENT TYPES OF CONTROLS

Type of Control	Source of Evidence
Password	Application logs showing passwords have been updated
Datacenter entry system	Badging system logs regarding entries allowed or denied
Mobile device acceptable-use policy	Records of lost or stolen devices which show if the devices are reported within specified time periods

Security teams should work towards increased automated monitoring of controls wherever possible, with results sent to a central repository (such as a GRC system). Manual evidence should also be stored centrally (within the GRC system). With centralized storage of assessment results, audits will require less effort and could be performed independently from the process and/or control owner.

As a longer-term goal for many organizations, continuous controls monitoring will enable them to generate a visual report on what controls are working and a real-time alert if a control is not. Continuous controls monitoring typically entails the use of technologies for log aggregation, GRC, and/or data analytics and warehousing. Many organizations are developing overarching strategies for security data management, to manage the collection and use of data for multiple purposes such as controls assurance, risk management, and threat detection.

Improve Third-Party Assessments

Evidence-based controls assurance goes a long way towards improving third-party assessments. Traditional methods – based on questionnaires, site visits, and yearly re-evaluation – are unwieldy and fail to yield timely, actionable information. If clients and service providers have capabilities in evidence-based controls assurance, it facilitates shared assessments; clients can set standardized requirements for control attestations and service providers can deliver standardized evidence. Standardized assessments of service providers could then be used by multiple clients.

The evidence-based approach also enables increasingly automated third-party assessments. For example, two leading organizations in the financial-services industry, a bank and a business service provider, are partnering to work out a set of measurable requirements for security controls. The service provider will provide the bank with ongoing evidence that particular controls are effective via access to a GRC system. The GRC system will sit at the edge of the service provider's network and ultimately be used by multiple clients to gain visibility into some of its key controls.

"Evidence-based controls assurance is a holistic look at the efficacy of the controls in your own environment. And if I'm going to accept a shared assessment, an attestation from a third party, I'd like to know, 'What is the evidence that the controls they have committed to are actually working on an ongoing basis?'"

ROLAND CLOUTIER
Vice President, Chief Security Officer,
Automatic Data Processing, Inc.

5. Develop Informed Data-Collection Methods

Data analytics has become an essential capability for cyber threat detection. Once you have a data store and analytics engine in place and a data analyst on-board, attaining a data-analytics capability requires setting up processes for determining what data to collect and where to find that data.

Build a Set of Use Cases

A fundamental step is to look at the types of questions data analytics can answer. An example of a question is, "How do we know whether system administrator activity on this particular system is legitimate or that of an intruder?" The answer might be, "If we could see unusual patterns of activity such as multiple sets of credentials being used in quick succession on one machine or an admin connecting into a system that is not associated with any of their work orders." By thinking through the key questions and answers related to protecting critical business processes, the security team can begin to identify relevant sources of data.

The security team should build a set of data-analytics use cases. For each use case, you will typically go through an iterative process with multiple cycles of data collection, algorithm development, testing, and refinement. For example, the team may be interested in answering the question, "How can we flag possible groundspeed violations" (cases in which a user seems to be active in two far-apart physical locations within a short amount of time)? The team could start with data such as: geographic location of badge swipes in buildings, IP addresses, mobile-device connections, and static VPN connections; the timestamps in these logs; and corporate travel itineraries to indicate where the user ought to be.

The data analyst would then develop an algorithm that generates a risk score based on the calculated speed at which the user is apparently moving. After running the analytics and looking at the results, the team would figure out which cases might actually be normal behavior but generate high risk scores. The next step would be to refine the algorithms, perhaps with additional data, to reduce the false positives.

A very common issue is that the data needed to answer critical questions is not readily accessible. The security team may need to go back to the original devices to reconfigure how logging is done. For example, proxy logs may need to include the IP address from the originating source, but this data might not yet be reported in the logs. The data-collection effort can call for skilled negotiations with system owners, since they may be reluctant to increase logging since it could negatively affect system performance.

In parallel to stepping through specific use cases, the security team should also identify the data that would be valuable for baselining normal activity on critical systems. For example, a few months of network history and user-access patterns from sources such as firewall logs and authentication systems could be useful to start baselining.

THINK BEYOND SECURITY LOGS.

Apply Data from Various Sources

It is also important to include the right sources of data. Think beyond security logs. Security teams need to see what's occurring in the business environment, not just in the security technology around the business environment. The integration of business information such as process, transaction, and application logs will help provide a more comprehensive look at the business being protected.

Data from internal sensors should be combined with data from external sources such as commercial, government, or industry threat feeds. If organizations only look at internal data they won't see the full potential impact of threats to their environment; they are only monitoring what has happened, not what could potentially be prevented. Consider focusing a resource on effective integration of data from various internal sources and external intelligence.

As many organizations have found, it is easy to subscribe to threat feeds, but more difficult to make that data actionable. Know how to specifically apply the data and develop a scheme to integrate external data with internal data to enrich the analysis. Data from commercial threat feeds on emerging attacks can be applied by testing specific, known areas of vulnerability within your environment to see if the threats are exploiting these methods to extract data. In this case, external data may help to pinpoint unusual activity on channels not typically used for outgoing communications.

Comprehensively Plan Data Collection

Building a competency in data analytics often requires a multi-year plan to improve the overall collection architecture and to modify applications to produce more data-rich logs. Try to find out early on what data (such as packet capture, NetFlow data) and data-aggregation capabilities (for example log management, central aggregation, or correlation of logs) are missing that would be valuable for a data-analytics capability and plan for increased data-storage capacity.

"The biggest challenge of data analytics is getting meaningful outcomes. You must take time to develop a cohesive strategy. Focus on the information that runs your business and develop the questions you want to ask. Otherwise you'll be swimming in data."

TIM McKNIGHT

Executive Vice President, Enterprise Information Security & Risk, Fidelity Investments

Conclusion

To meet today's practical challenges while charting a path forward, top security teams are working through major changes to their ingrained processes. "Business as usual" will not keep pace with today's threat environment or technology-driven business initiatives.

Much of the work to be done involves developing a deep understanding of business processes and working much more closely with the business units. Cybersecurity risks are finally a mainstream theme in business, and in many organizations there is more of a willingness to fund programs in this space. Even though personnel in the business units are worried about cybersecurity risks, they don't know how to manage them. At this point in time, it is incumbent on security professionals to educate people regarding cybersecurity risks. While there has been talk of evolving information security into risk management for years, it's time to take it seriously by up-leveling security processes and making them integral to the business.

As security processes are re-engineered, optimization will be a key success factor – and an ongoing endeavor. Information security processes need to be subject to continual re-evaluation to ensure the effective use of resources and the effective mitigation of risk to the business.

As security teams consider how to renew processes they must also, of course, plan to keep up with shifts in technology. New technologies – particularly those for analyzing big data – are driving some of the key process changes discussed in this report. The next and final report in this series on Transforming Information Security will explore some of the most important emerging and evolving security technologies – and provide further practical insight into managing the forces reshaping information security.

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 and IT systems, protecting information and IT systems 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 put the organization 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 some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA HAS CONVENED A GROUP OF HIGHLY successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores these topics. Go to www.rsa.com/securityforinnovation to view the reports or access the research. Together we can accelerate this critical industry transformation.

Report Contributors

Security for Business Innovation Council

MARENE N. ALLISON
Worldwide Vice President of Information Security,
Johnson & Johnson

ANISH BHIMANI CISSP
Chief Information Risk Officer,
JPMorgan Chase

WILLIAM BONI CISM, CPP, CISA
Corporate Information Security Officer (CISO), VP, Enterprise Information Security,
T-Mobile USA

ROLAND CLOUTIER
Vice President,
Chief Security Officer,
Automatic Data Processing, Inc.

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

JERRY R. GEISLER III GCFA, GCFE, GCIH, Office of the Chief Information Security Officer,
Walmart Stores, Inc.

RENEE GUTTMANN
Chief Information Security Officer,
The Coca-Cola Company

MALCOLM HARKINS
Vice President, Chief Security and Privacy Officer,
Intel

KENNETH HAERTLING
Vice President and Chief Security Officer,
TELUS

PETRI KUIVALA
Chief Information Security Officer,
Nokia

DAVE MARTIN CISSP
Vice President and Chief Security Officer,
EMC Corporation

TIM McKNIGHT CISSP
Executive Vice President, Enterprise Information Security and Risk, **Fidelity Investments**

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

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

RALPH SALOMON CRISC
Vice President IT Security and Risk Office,
SAP AG

VISHAL SALVI CISM
Chief Information Security Officer and Senior Vice President,
HDFC Bank Limited

SIMON STRICKLAND
Global Head of Security,
AstraZeneca

LEANNE TOLIVER
Office of the Chief Information Security Officer,
eBay

DENISE D. WOOD
Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer,
FedEx Corporation

To see *the SBIC members' full bios, please visit EMC.com*

EMC²

RSA®