Gartner Research

Publication Date: 26 March 2009 ID Number: G00165816

Top-Five Issues and Research Agenda, 2009-2010: The Chief Information Security Officer

Jay Heiser, Tom Scholtz

Business and organizational issues, including a clear and explicit alignment with business needs, will be critical for chief information security officers (CISOs) in 2009. Use Gartner's evolving research agenda to prioritize and address five primary issues during what promises to be an extremely challenging year.

Key Findings

- CISOs will face a more widespread and more dangerous threat environment in 2009, with a significant increase in "insider" threats, as a result of deteriorating economic conditions.
- The CISO will need to address growing security risks with strained — and in some cases declining — budget and staffing resources.
- Emerging technology trends, including the use of relatively insecure consumer-grade IT and externally provisioned software as a service (SaaS) and cloud offerings, present serious new security challenges, and the technologies and processes addressing them are immature or nonexistent.
- Targeted, audience-specific security awareness communications will be a critical element of the successful CISO's work.

Recommendations

- Create a security-enabled enterprise culture, one in which line-of-business managers are the "owners" of information assets, with ultimate accountability for the security of those assets, and end users have the awareness and skills necessary to recognize and successfully address security threats.
- Build relationships with key enterprise decision makers, providing them with the context and risk assessment information they need to make informed decisions about accepting and controlling information asset risk.
- Ensure that any budget-driven reductions in security levels, and resulting increases in risk, are understood and accepted by the affected stakeholders.
- Design and implement processes to ensure that use of personally owned IT, and externally provisioned applications and services meet enterprise security standards.

ANALYSIS

The CISO is responsible for managing and coordinating information security risk assessment, communication and policy management processes across the entire enterprise, with the overarching goal of protecting the enterprise's information assets and IT systems in the most cost-effective manner possible. Security is increasingly recognized as being a service or set of services offered by IT to meet specific business needs. The CISO must ensure that business managers have a basic understanding of the security risks associated with their use of IT, and enable them to make appropriate choices about security mitigation expenditures.

Enterprise security, as well as the CISO's role in it, continues to evolve. Enterprise security organizations are often distributed and federated, with security functions and responsibilities dispersed throughout corporate management, IT organizations and business units. A few enterprises are still experimenting with moving the strategic security function out of the IT organization, but some have moved in the opposite direction, returning the CISO into the CIO's organization.

It is increasingly recognized that where the CISO reports is less important than what the CISO is actually responsible for doing. The key issues the CISO faces, especially in larger and globally distributed enterprises, continue to be less about choosing and managing technology, and more about ensuring that business security goals are well understood and met effectively through IT services and the coordinated activities of all employees, contractors, and service providers (see "No More Dr. No: Developing a Strategy for Business-Aligned Information Security").

Gartner has identified five primary issues that will be the focus of our research for CISOs in 2009:

Issue 1: How can security be maintained when IT budgets are shrinking and employees are concerned about their jobs?

The worldwide economic situation will be extremely difficult throughout 2009, affecting security programs in three primary ways. The first is that many enterprises will spend significantly less on IT than in the past, and CISOs should expect extremely low or nonexistent increases over 2008 spending on security. They should define their priorities clearly, to prepare for unanticipated budget reductions.

In times of economic difficulty, it is more important than ever that security efforts align with the needs and expectations of the business. In some cases, enterprises may explicitly decide to accept higher levels of IT risk because of resource constraints or competitive pressures. These cutbacks may be justified or even unavoidable, but will inevitably lead to higher security-incident rates. CISOs will need to simultaneously accept the reality of highly constrained resources and avoid taking the blame for security failures that result from them. Detailed records need to be kept of the decision-making processes underlying reductions in protection levels, and ideally, business managers should accept the resulting additional risk in writing.

CISOs will also face a broader and more-highly motivated threat environment — and particularly "insider" threats — in 2009. Employees who are concerned about their employer's long-term viability, or their own short-term job prospects, will inevitably be less loyal to the enterprise. This makes employees (full-time, part-time and temporary) and independent contractors far more likely to steal data — credit card numbers, customer or prospect lists, design documents, or anything else that might be useful in a future position or salable in the criminal market.

CISOs should also be prepared for deliberate sabotage. Several incidents have recently been reported of employees who, expecting to be downsized, created software "time bombs" to

damage IT systems or assets after their departure. Gartner expects such sabotage to increase. Crime, in general, inevitably increases as economies slow, and enterprises will also be at increased likelihood of attack from outsiders, such as competitors, former employees and cybercriminals.

Finally, enterprises will be subject to governmental and regulatory demands for higher levels of governance and transparency, largely because of the series of financial scandals that have marked this crisis. Enterprises and government agencies alike will face even greater demands for the protection of sensitive personal data. For these reasons, Gartner does not expect security and compliance budgets to shrink as much as overall IT budgets. Nonetheless, 2009 will unquestionably be a very challenging year for security professionals (see "Is Security a Luxury in a Declining Economy?").

Issue 2: How can security policies, controls and processes be aligned with business needs?

Despite the self-evident need to align security practices with business needs, enterprises find it extremely difficult to develop and implement sets of security policies, controls and processes that reflect and serve their current business needs. Effective alignment requires the cooperation of line-of-business managers who have long assumed that information security is the IT organization's problem — no matter how the business uses the information that must be secured. Security/business alignment requires that accountability for the security and integrity of information systems and assets rests with their "owners."

This represents a fundamental change in process and culture, one that will not take place unless the CISO convinces the CIO, and a coalition of executive-level sponsors, that it makes business sense. CISOs will also need to work with both the CIO and the line-of-business managers to communicate an understanding of security as being composed of a set of service offerings. This enables asset owners to contract with the IT organization for well-understood levels of security and risk management services and to do so cost-effectively. The IT service management principles outlined in ITIL v3 provide guidance on how security management can be integrated into an overall IT service management life cycle (see "Preparing for the Impact of ITIL v.3 on GRC Strategies").

Security policy management should be viewed as an ongoing process that is continuously developed, refined and improved in response to the identified needs of the business. To achieve this very difficult goal, the CISO must establish strong working relationships with senior corporate executives and line-of-business managers to determine the real-world security requirements of the business and articulate them in effective, actionable policy. For most enterprises, the best approach will be to develop a comparatively flexible and tiered policy framework, rather than a "one size fits all" policy document or policy library, so that different policies, and levels of policies, can be applied to different constituencies and target audiences (see "Toolkit Best Practices: Creating a Security Policy Process [Security Policy Guidelines, Part 1]," "Toolkit Best Practices: Creating a Security Policy Framework [Security Policy Guidelines, Part 2]" and "Toolkit Best Practices: Creating Security Policy Documents [Security Policy Guidelines, Part 3]"). A key element of the necessary formalization and maturation is the integration of security with other service management and business processes (see "Toolkit: Formalizing Security Processes," and "Toolkit: Security Process Definition Template for Security Architecture"). One example is the "onboarding" of new users, which requires integration between business processes and the security organization's user-provisioning process.

Issue 3: What processes need to be in place to assess and control the risks associated with the growing use of

nontraditional IT, such as consumer-grade hardware and software as a service (SaaS)?

Business units and individual users are increasingly buying and controlling computing resources without the involvement of IT (see "Optimal Security Approaches for the Secure Use of Consumer IT"). The risks associated with business use of consumer-type hardware, including notebook computers and mass storage devices, are comparatively well understood, but many enterprises continue to struggle with data leakage caused by USB devices, and occasionally with malware introduced by them. The technology for controlling personal hardware is less effective and less convenient than it needs to be, and many enterprises rely on very weak policies — and the hope their incumbent security vendors will soon provide stronger functionality. CISOs need to work to bring about appropriate, consensus-based decisions about the acceptable use of consumer-grade hardware and other digital devices that are connected to the enterprise, but not owned or controlled by the IT department. Their annual plans should recognize that better control technologies — which will allow greater user flexibility at lower risk — will become available during the next few years.

The risk issues associated with the use of alternative IT delivery models, such as SaaS and cloud computing, are much less clearly understood. Budget considerations will drive greater use of externally provisioned services in 2009. IT organizations' rigor in scrutinizing service providers varies widely. Although business managers typically lack the skills to evaluate the sourcing or security risks of a SaaS offering, they sometimes contract for them without consulting IT or the CISO. However, Gartner research shows that 86% of enterprises do have a process for evaluating the security risks of an external party, and 54% make site visits to assess risk in person (see "Gartner Survey Highlights Company Burden of Vetting Third-Party Security Controls"). As long as enterprises feel the need to perform on-site evaluations, it will limit the growth potential for SaaS and cloud computing.

Issue 4: How can individual and organizational behavior be influenced to reduce security incidents?

The CISO must work to create a security-enabled culture, with an enterprisewide sense of the importance of information security and the IT user's role in maintaining it. This requires that individuals at all levels and in all areas understand the security consequences of their IT practices and have the knowledge and skills necessary to do something about them. The success of the CISO's efforts to effect these fundamental changes in enterprise culture and individual behavior will depend heavily on security awareness communications being presented in a positive, compelling and audience-appropriate manner. The various stakeholders must understand not only that information security has value for them and for the enterprise as a whole, but also that they can take steps to improve security. Security awareness is not the end goal of the necessary cultural change effort. In fact, it is only the beginning. Individuals must be aware of information security risks and be willing and able to take specific actions to reduce risk.

Enterprise security awareness programs have historically tended to take a broad-brush approach, presenting a single security message to the entire organization. CISOs in 2009 and beyond must target their security messages at specific constituencies. The message, and the way it is communicated, will be very different for IT developers and operations staff from that presented to end users. Line-of-business managers represent the most critical target, because they set the agenda for the end user, telling them which policies to follow and which to de-emphasize. More significantly, in the long term, business managers are IT's customers, and they should request specific security service levels as a normal part of their functional requirements. An enterprise culture in which business managers routinely and proactively seek out secure applications is much less likely to suffer security failures.

Issue 5: Where does the CISO report, and what is the CISO's role responsible for?

The full-time responsibility for IT risk management is an inherently "political" activity, and the question of where the CISO reports is, therefore, a sensitive one. There is no perfect reporting structure for IT risk management, and all the reporting models carry both advantages and disadvantages. Whether the CISO is in IT or not, the role is becoming increasingly more strategic, with relatively less day-to-day responsibility for operational tasks, and a commensurately larger responsibility for enterprisewide coordination of security management activities, and promulgation of the IT risk management agenda.

Effective governance requires that all the affected stakeholders within the enterprise — the IT organization, the security team, line-of-business managers and many others — work together to make informed decisions about security investments, policies and controls. The larger the enterprise, the greater the benefit in establishing one or more decision-making bodies made up of individuals who work for the constituencies involved. Increasingly, the CISO is responsible for organizing and ensuring the success of bodies, such as governance committees, coordinating or steering committees, and information-sharing forums.

The Gartner CISO Research Agenda for 2009

Throughout 2009, Gartner's CISO-oriented research agenda will address the five issues discussed above. We will continue to expand our research materials on security architecture practice, business alignment and culture change. Our library of policy template material will be expanded, and we will continue to enhance the Gartner risk assessment tool, and the Gartner Risk Assessment Methodology (GRAM).

RECOMMENDED READING

"Gartner for IT Leaders Overview: The Chief Information Security Officer 2009-2010"

"No More Dr. No: Developing a Strategy for Business-Aligned Information Security"

"What Does an Information Security Strategic Plan Contain? 25 September 2008"

"Optimal Security Approaches for the Secure Use of Consumer IT"

"Is Security a Luxury in a Declining Economy?"

"Risk and Security Officer Role Responsibilities Broaden"

"Gartner Survey Highlights Company Burden of Vetting Third-Party Security Controls"

"Toolkit Best Practices: The Information Security Organization, 2010"

"Toolkit Best Practices: Creating a Security Policy Process (Security Policy Guidelines, Part 1)"

"Toolkit Best Practices: Creating a Security Policy Framework (Security Policy Guidelines, Part 2)"

"Toolkit Best Practices: Creating Security Policy Documents (Security Policy Guidelines, Part 3)"

"Toolkit: Formalizing Security Processes"

"Preparing for the Impact of ITIL v.3 on GRC Strategies"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner