SC MAGAZINE

AWARDS 2011

Honored in the U.S.

Entry kit

scmagazineus.com/awards

Table of contents

Entry rules & information

Judging information

Reader Trust Awards

Excellence Awards

Professional Awards

Entry rules & information

Who can enter?

The 2011 SC Magazine Awards U.S. are open to all information security vendors, service providers and professionals.

Vendors and service providers who offer a product and/or service for the commercial, government, educational, non-profit or other industries can enter the Reader Trust and Excellence categories. All of these categories relate to products, services and/or information security companies. Entrants should be executing work in North America.

Information security professionals from end-user companies can enter into the Professional categories, which honor teams and CSOs/CISOs. These professionals and teams should be working in North America. It is acceptable and, indeed, encouraged for vendors to nominate their thought-leading customers.

Other Professional categories relate to both professional certification providers and those professional advancement companies that offer training on various information security issues to end-user companies. These, too, should be based in North America.

Entry requirements and qualification questions

Each category requires you answer a set of questions in order to qualify your nomination. Please see each category for the full list of qualifying questions. Answer these completely. Also, we advise that if you are entering multiple categories, it behooves you to offer unique answers for each. That is, avoid copying and pasting the same answers for each category you enter as this may yield a negative response from our judging panel.

New this year, the Reader Trust categories require that entrants' products and/or services meet some minimum requirements to qualify. You must COMPLETELY answer questions about these requirements. If you do not meet all of the requirements noted, please DO NOT enter to compete in that category. Any submissions made that do not meet the qualifications will be disqualified without refund.

Online nomination submission

Each nomination must include:

1. Answers prepared for the qualification questions for each nomination.
2. Nomination fee (online payment required): Visa, MasterCard, American Express. Once you have prepared your nominations, please visit our website: **scmagazineus.com/awards** to submit your nomination.

Key info

Nomination entry fees:

- Reader Trust Awards and Excellence Awards categories is **$275 per entry**.
- Professional Awards categories is **$200 per entry**.

Deadline for nominations:

The deadline for nominations is Sept. 3, 2010. Nominations submitted after Sept. 3, will be considered late and will incur a late fee.

Late nominations:

Late entries will be received until Sept. 10. However, all nominations received after Sept. 3 will incur a penalty of $115 per entry.

Judging information

How will the nominations be judged?

Reader Trust Awards

Winners are chosen by a panel of readers who represent the circulation of *SC Magazine*. The Reader Trust Voting Panel is comprised of *SC Magazine* readers who have volunteered their time and experience to carefully consider each of the contenders in each category to cast votes. This panel represents a cross-section of *SC Magazine* readership, which is comprised of large, medium and small enterprises from all major vertical markets, including financial services, health care, government, retail, education and other sectors. In addition to reviewing the materials provided by entrants, they have been advised to vote in each category for what they view as the solution that is the most effective in helping them and their companies address the problems for which the product was designed. Voters also can take into consideration the functionality, manageability, ease-of-use and scalability of the product or service, as well as the customer service and support provided for it. The Reader Trust Voting Panel also has been directed to peruse any applicable product reviews that *SC Magazine* has published in the last year. There will be one winner chosen per category.

Excellence Awards

Winners are decided by an expert panel of judges. These judges are hand-picked by *SC Magazine*'s editorial team for their breadth of knowledge and experience in the information security industry. Luminaries come from all walks of life – from end-user companies to the analyst and consulting communities to academia. Many are practicing and former chief security officers from the private and public sectors, who also may have been honored themselves at SC Magazine Awards Galas in previous years. Not only are judges advised to review the materials provided by entrants, they also are asked to review any applicable research or analyst reports, as well as product reviews appearing in *SC Magazine*. There will be one winner chosen per category.

Professional Awards

With the exception of the Editor's Choice Award recipient, winners in the Professional Awards category will be decided by an expert panel of judges. Like the Excellence Awards, not only are judges advised to review the materials provided by entrants, they also are asked to review any applicable research or analyst reports, product reviews by *SC Magazine*, and/or any additional documentation/input provided by *SC Magazine* and/or other Haymarket Media publications. In some cases, the panel may be offered further insight or add additional notes from *SC Magazine*'s editorial team members who may decide to interview or already have interviewed contenders. There will be one winner chosen per category.

Editor's Choice Award

Based on feedback from *SC Magazine*'s editorial team, its Editorial Advisory Board, readers and other sources, a small list of contenders is created internally. Those considered for this award can be industry bodies, professionals, companies or products.

The award winner finally is decided by the editor-in-chief of *SC Magazine* and announced at the SC Magazine Awards Gala. This award enables the editorial team to pay homage to those individuals or entities that are making a positive impact on the industry as a whole.

Finalist notification

Finalists will be announced in the January 2011 issue of *SC Magazine* and/or on **scmagazineus.com**. The winners will be announced at the 2011 SC Magazine Awards U.S. Gala held on Feb. 15, 2011 in San Francisco.

Questions

Please contact Natasha Mulla, events manager, at 646-638-6108 or via email at natasha.mulla@haymarketmedia.com.

Sponsorship opportunities

For information on sponsorship opportunities, please contact Mike Alessie at 646-638-6002 or via email at mike.alessie@haymarketmedia.com.

Terms & conditions

The mission of the 2011 SC Magazine Awards U.S. is to honor the achievements of companies and information security professionals striving to safeguard businesses, their customers and critical data in North America. Information security products and services nominated for the Reader Trust Awards, therefore, should be available for sale to U.S. and Canadian companies, as well as provide both customer service and support to users in these countries. Competitors are voted on by end-users, readers and objective judges. After averages for each category are tallied, finalists and winners are decided. Results are completely independent. Financial considerations play no part in the results. That is, no one can "buy" a win!

Categories & requirements

Reader Trust Awards

Qualification questions (150 word maximum on all summaries)

1. How does this product or service answer the specific market need or application for which it was designed and is being nominated?
2. How does this product or service significantly differ from its competitors?
3. What are the business and technical advantages to enterprises or SMEs investing in this product or service?
4. How has this product or service helped customers to meet/surpass corporate budgetary expectations?
5. How does this product or service show a sound business benefit and/or return on investment? That is, how is it enabling customers and their businesses?
6. What is the market share for the sales of this product?

Best Anti-Malware Gateway

Products in this category generally are appliances. Their purpose is to act as gateways, usually at the perimeter of the enterprise, protecting against various types of malware attempting to enter the enterprise from outside.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Protects against at least viruses and worms.
- Is centrally managed (i.e., an enterprise product).
- May, optionally, protect against one or more of the following: Spam/Spyware/Adware/Phishing emails/Other malware.
- Optionally, works with multiple anti-malware products.
- Optionally, works with client-side anti-malware products (desktop).

Best Anti-Malware Management (client-based, typically software only)

These products are used to provide a central management point for mitigation of the threat of malware. They manage the anti-malware software/appliances from a central point, facilitating data file updates, reporting, alerting and more. They are not in themselves anti-malware products. Malware management, for the purposes of this category, is defined as a product that reduces the threat of malware for small, medium or large enterprises on an organization basis by managing instances of an anti-malware product or products residing on endpoints, servers or gateways.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Has centralized gateway malware management.
- Has centralized critical device malware management.
- Has centralized endpoint device malware management.
- Has centralized logging.
- Has centralized reporting.

Best Email Security

Email security addresses the ability to exchange email messages securely. This includes ensuring the privacy of sensitive messages, limiting the repercussions of email forgery, and managing other aspects of email security within the organization. These email security products should be evaluated on their effectiveness, manageability, non-intrusiveness, ease of use and other factors that impact the implementation of this type of product in the enterprise environment.

Please note: *These products are not email content management solutions that may filter email messages based on content, source or other criteria. That category and its requirements are noted next.*

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Provides email encryption.
- Allows digital signatures.
- Provides automatic shredding of messages and attachments based on a pre-defined policy.

Reader Trust Awards continue on next page

Categories & requirements

Best Email Content Management

These products may filter email messages based on content, source or other criteria. Direction of flow may be either to the organization, from the organization or both. These products are enterprise-centric and should have, but are not required to have, some form of centralized management. They may include spam filters, junk mail filters, malware filters, unauthorized content (sometimes called "extrusion protection" or "data leakage protection"), phishing and other types of undesirable content. However, these are not simply anti-spam filters.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Filters email in both directions (to and from the enterprise).
- Filters based on email content.
- Filters based on source address or sender.
- Notifies, blocks, sidelines or some combination of such action taken.
- Works in an enterprise environment.

Best Data Leakage Prevention (DLP)

Includes products that help organizations safeguard their intellectual property and customers' critical data persistently – inside and outside the company. Network-based and endpoint data leakage prevention products (also sometimes called extrusion prevention products) will be considered. Products should prevent data from unauthorized exit from the network or protect data on the endpoint, whether the endpoint is connected to a network or not (e.g., laptops that are removed from the network for travel). Products must be policy-driven and should include scanning of all data, regardless of protocol or application leaving the network, and/or keep track of peripherals, such as removable storage and attached to the endpoint – reporting that inventory to a central location or adminstrator. All entrants should have the capability of being managed by a centralized administrator. Those products considered part of this category include: network DLP products, which are typically gateways; those products protecting only endpoints; and hybrid products, those that operate at both the gateway to the network and at the endpoint. Products should be transparent to the user. Specifically for endpoint DLP, traffic should be monitored and encryption should be available. Products that offer encryption exclusively are inappropriate for submission, although encryption may be part of a larger package of DLP capabilities.

To be eligible for this category you must be able to confirm your product/service meets either the network-based or the endpoint-based qualifications below.

Network-based:

- Scans information leaving the network for keywords, phrases, file types and more.
- Scans must be one or more of the following:
  Email and attachments/FTP/IM/IRC (or similar, such as ICQ).
- Works in an enterprise environment and is centrally managed.
- Offers various action options, such as quarantine, stripping attachments, notifying sender, notifying administrator.
- Has a centrally managed policy engine.

Endpoint-based:

- Inventories and monitors all peripherals, including removable storage attached to the endpoint.
- Is network-centric (logging, management and reporting to a central administrator).
- Offers endpoint and peripheral encryption.
- Provides offline usage tracking.
- Has a centrally managed policy engine.

Reader Trust Awards continue on next page

Categories & requirements

Best Endpoint/UTM Security

Solutions should take an "in-depth" defense approach. Entrants should have an integrated, multifunction endpoint/UTM offering – not a single-function product. These products typically aggregate a wide variety of threat data into a single unified tool. Many organizations define those threat categories as anti-virus, content management, IDS/IPS and spam filtering. The minimum functionality, according to IDC, is IDS/IPS, anti-virus and firewall/VPN. Entrants should meet this IDC minimum functionality. As well, all products must function at the endpoint as opposed to the gateway, although hybrid gateway/endpoint devices will be allowed as long as there is an integral endpoint piece to the product.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Centrally managed.
- Policy driven.
- Operates at the endpoint.
- Operates at the gateway (optional addition to the endpoint).
- Meets the minimum IDC requirements (firewall, IDS, anti-virus).

Best Mobile/Portable Device Security

More and more employees are using smaller and smaller devices with loads of applications to access corporation data. Some examples include iPhones, BlackBerries, Palm and other PDAs and more. Products in this category deal with not only a collapsing perimeter, but also consumer-owned and -controlled devices being used to get at corporate resources. At a minimum, these devices likely will require strong endpoint security, point-to-point encryption and more. This is a broad category. If your product is used to secure this type of small device/handheld/etc. it may fit. Security can be for data at rest in the device itself, secure access to data in the enterprise, and encryption for data in motion between the enterprise and the device. *Includes anything from hard disk encryption solutions and tools that track lost mobile devices to USB/thumb drive security solutions.*

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Centrally administered and intended for an enterprise environment.
- Has some form of encryption as appropriate to the application.
- Endpoint device is a small device, such as a PDA, smartphone, thumb drive, and more.

Best Enterprise Firewall

Products in this category are organizational firewalls, not personal firewalls. Firewalls must provide a mechanism to filter incoming and outgoing traffic based on port, protocol, source IP address and destination IP address. All products must have the ability to terminate network traffic based on the above filtering criteria. Additional details below.

Product is a proxy-based firewall. Proxy-based firewalls are firewalls that terminate the Time-to-Live (TTL) field in the IP header as the packet is processed. They must protect all layers of the OSI model, including the application layer. Also, they must maintain two separate data streams (client to proxy firewall and proxy firewall to destination).

Product is a stateful inspection-based firewall. Stateful inspection firewalls are firewalls that maintain a state of connections database or table. Stateful inspection firewalls track the state of connection and make filtering decisions based on information in the state table or database. With stateful inspection firewalls, a single stream of data is maintained.

Product is a packet filter firewall. Packet filter firewalls use source IP, destination IP, source port and destination port to determine if a packet is permitted. A packet filter firewall does not terminate the TTL field in the IP header. A packet filter firewall does not use a state table or database for filtering of traffic.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Uses deep packet inspection (filtering into the data portion of the packet).
- Provides logging AND reporting.
- Provides distributed enforcement (e.g., firewall software is distributed to each client and managed through the central configuration management).
- Provides alerting capability AND has auto-update feature.
- Can block real-time traffic through management interface.
- Has web-based access to reporting and/or logging.
- Performs web caching.
- Has a mechanism for configuring authentication of user for permitted traffic types.
- Provides anti-virus.
- Provides content filtering.
- Has a mechanism for high availability.

Reader Trust Awards continue on next page

Categories & requirements

Best Web Application Firewall

Application firewalls inspect the body of packets and restricts access to legitimate application traffic while blocking access to other parts of the operating system.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Uses deep packet inspection (filtering into the data portion of the packet).
- Provides logging AND reporting.
- Provides distributed enforcement. (e.g., firewall software is distributed to each client and managed through the central configuration management).
- Provides alerting capability AND has auto-update feature.
- Can block real-time traffic through management interface.
- Has web-based access to reporting and/or logging.
- Performs web caching.
- Has a mechanism for configuring authentication of user for permitted traffic types.
- Provides anti-virus.
- Provides content filtering.
- Has a mechanism for high availability.
- Has auto-update feature.
- Has web-based access to reporting and/or logging.
- Protects traffic from reaching the underlying operating system.
- Filters application traffic to only legitimate requests.

Best Web Content Management Product

Products in this category provide web content filtering for laptops, desktops and, optionally, servers.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- May block or filter objectionable websites and content.
- Uses a blacklist or whitelist and must have a means to keep the list(s) updated from vendor-provided data.
- Must be centrally manageable (i.e., an enterprise product).
- Must support all popular web browsers.

Best Intrusion Detection/Prevention Product

Products in this category monitor networks for malicious behavior and block or prevent those activities.

To be eligible for this category, you must be able to prove your product/service meets the below qualifications:

- Provides intrusion detection services.
- Provides intrusion prevention services.
- Is an enterprise product (i.e., not a purely desktop product).
- IDS/IPS is the product's primary function.

Please note *The product is not an email gateway that additionally provides IDS services. Secondary services are permitted; but product may not be classed as a UTM, anti-malware/anti-spam gateway, or other tool not considered to have classic IDS/IPS functionality.*

Best Identity Management Application

Products in this category address the identity management lifecycle in an enterprise environment.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Password management.
- User provisioning (creation of the user entity, authorization and permissions).
- Enterprise-access management (e.g., single sign-on).
- Is enterprise-centric with central management.

Reader Trust Awards continue on next page

Categories & requirements

Best Integrated Security/UTM Product

These products generally are appliances that are implemented at the gateway to the enterprise. Typically, they will comprise several services, such as firewall, IDS/IPS and more.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- IDS and/or IPS.
- Firewalls.
- May include anti-malware gateway, anti-spam gateway, anti-phishing gateway and more.

Best Multifactor Product

Products provide enhanced security to end-users or devices by offering credentials for access to an authenticator or authentication server. Software and hardware that specializes in the biometric authentication of users is also included here.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Uses a tangible device, "something you have," for authentication.
- Uses knowledge, "something you know," for authentication.
- Offers centralized logging AND centralized reporting.
- Provides self-password or equivalent reset AND centralized management.
- For biometrics, the solution provides identification and authentication using any of the following methods: Finger/thumb print/Retinal scan/Voice recognition/Hand/palm geometry/Facial recognition
- Is applicable to an enterprise environment.
- May be centrally managed.
- Provides centralized activity logging.

Best Security Information/Event Management (SIEM) Appliance

Security information and event management tools (SIEMs) are used to collect, aggregate and correlate log data for unified analysis and reporting. Typically, these tools can take logs from a large number of sources, normalize them and build a database that allows detailed reporting and analysis. While forensic analysis of network events may be a feature of a SIEM, it is not the only feature, nor is it the primary focus of the tool.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Log consolidation (IDS/IPS, Syslog, Windows event logs, Netflow, and other types).
- Threat correlation.
- Incident management/forensic analysis.
- Extensive reporting, including preconfigured reports that support regulatory requirements.

Best Computer Forensics Tool

Products in this category fall into two sub-categories: network and media. The network tools *must* be exclusively intended for forensic analysis of network events/data. If the product is a SIEM with forensic capabilities, it should be placed in the SIEM category. Media tools cover just about all other non-network forensic tools, including those tools that collect data from media over the network and live forensics tools. This also includes specialized forensic tools that are not intended to analyze network data.

To be eligible for this category you must be able to confirm your product/service meets either the Network or the Media qualifications below.

Network:

- Network log aggregation, correlation and forensic analysis.
  (Must be intended strictly for forensic analysis. SIEMs, including those that also provide forensic analysis, go into the SIEM category.)

Media:

- Media acquisition and analysis.
- Must address one or more of the following:
  The MS Windows and Linux file systems/Tools for managing evidence, case notes, and more/Small media-device tools that address other types of devices such as cell phones, PDAs, memory sticks, digital cameras and more.

Reader Trust Awards continue on next page

Categories & requirements

Best Managed Security Service

These security offerings provide a turnkey approach to an organization's primary technical security needs.

To be eligible for this category, you must be able to prove your product/service meets the below qualifications:

- These offerings can be either a co-located device at the client organization facility or can be a completely outsourced solution where the application to be protected would reside at the vendor's data center.
- Areas of interest are: managed firewalls, IDS/IPS, fraud (such as phishing or spam) and any other security-related managed service.

Best Policy Management Application

These products are used to enforce configuration policies to devices in an enterprise. This can include but is not limited to network configuration, encryption configuration, software configuration and hardware configuration. These products are able to audit devices against a policy created by an administrator, as well as have the ability to make policy changes to devices in the enterprise. Important functionality will include compliance management.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Enterprise-centric (i.e., centrally managed).
- Provides support for compliance reporting.
- Endpoint configuration management, enforcement, auditing and reporting.
- Includes risk management module(s).

Best Vulnerability Management Tool

These products perform network/device vulnerability assessment and/or penetration testing. They may use active or passive testing and are either hardware- or software-based.

To be eligible for this category, you must be able to confirm your product/service meets the below qualifications:

- Perform either vulnerability assessment, penetration testing or both.
- Provide reporting that supports compliance management.
- Reports vulnerabilities using some standard format/reference, such as CVE or CVSS.
- Production system that uses a GUI to speed and simplify testing (as opposed to a collection of command line scripts).

Best IPsec/SSL VPN

For this category, we are focusing on IPsec and SSL VPN products. IPsec products usually provide encrypted point-to-point (as opposed to end-to-end) remote access using IPsec. SSL VPN products provide encrypted remote access to client machines using the SSL/TLS protocol. Client machines may use either a web browser or a standalone SSL VPN client. The SSL VPN must provide access to a client network – not only a web application interface. Product must support multiple simultaneous SSL VPN connections. Many of these products are integrated VPN/portal products.

To be eligible for this category you must be able to confirm your product/service meets either the IPSec or the SSL VPN qualifications below.

IPsec criteria:

- Uses IPsec to secure remote network traffic.
- Select which best describes your product: Is a standalone appliance/Is integrated into a router or other gateway product.

SSL VPN criteria:

- Uses SSL or TLS to secure remote network traffic.
- Select which best describes your product from the following two choices: Requires no client software (e.g., browser-based VPN)/Requires client software/Is integrated with portal software.

Categories & requirements

Excellence Awards

Qualification questions (150 word maximum on all summaries)

Company

1. How strong is the company's customer base and continued customer growth?
2. Please provide two to three customer references with contact details.
3. Does the company have a strong product/service portfolio? Explain.
4. Does the company offer strong customer service and support for the products/services it supplies? How?
5. Is the company engaged in compelling research and development efforts that will lead to continued innovation? How?
6. How well is the company meeting its overall mission and vision? In what ways?
7. How is the company using its products and services to help enable/strengthen its customers' business?
8. Are customers seeing a benefit in using its products/services to differentiate from the competition? That is, are they finding market value in touting the use of the company's product/service?

Best Security Company

Nominees should be the tried-and-true, longer-standing companies that have been offering products and services to customers for at least three years. Nominations can come from all sectors. Areas that will be accounted for in the judging process include: product line strength, customer base, customer service/support, research and development, company growth and solvency, innovation and more.

Rookie Security Company of the Year

Nominated companies should be new to the IT security field, offering an initial, strong, flagship product that is within two years of its initial release. Nominees can come from any IT security product/service sector and will be continuing their efforts in further product development, customer growth and overall fiscal and employee growth.

Please note *in your submission the launch date of your initial flagship offering. If this initial offering or any of your other products have been on the market for longer than two years, please do not submit a nomination to this category.*

Product/service

1. How strong is the customer base and continued customer growth for this product or service?
2. Please provide two to three customer references with contact details.
3. Does the company offer strong customer service and support for this product/service? How?
4. Are efforts underway to continue developing and strengthening this product or service? What do these efforts entail?
5. Overall, how well is this product or service meeting the needs of its customers?
6. What is the market share for the sales of this product?
7. How is the company using its products and services to help enable/strengthen their customers' business?
8. Are customers seeing a benefit in using their products/services to differentiate themselves from the competition? That is, are they finding market value in touting the use of the company's product/service?

Best SME Security Solution

This includes product nominations from all product sectors specifically designed to meet the requirements of small- to mid-sized businesses. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Best Enterprise Security Solution

This includes product nominations from all product sectors specifically designed to meet the requirements of large enterprises. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Best Regulatory Compliance Solution

Nominated solutions should help organizations comply with specific regulatory requirements demanded of companies in the health care, financial services and government markets. Solutions should help customers meet mandates noted in such legislation as *HIPAA*, *SOX*, *GLBA*, FISMA or in guidelines noted by the likes of the FFIEC or the PCI Security Standards Council. Nominees must be prepared to offer references of customers who are engaged in or have already completed real, fully fledged deployments, and should be ready to address specific questions posed to them during the judging process.

Categories & requirements

Professional Awards

CSO of the Year

Qualification questions (150 word maximum on all summaries)

1. How has the CSO developed and managed a strong IT security team?
2. Please provide two to three professional references with contact details.
3. By what means has the CSO gained the support of corporate leaders and colleagues?
4. How has the CSO helped to propel the CISO/CSO position to a footing of influence within their organization and the corporate world as a whole?
5. How has the CSO helped to strengthen the influence of its department in meeting business initiatives and goals?
6. How has the CSO strengthened end-user and customer awareness of IT security threats and safeguards?
7. In what ways does the CSO continue to better the expertise of internal IT security?
8. What steps is the CSO taking to better position risk management/information security planning as business enabling? That is, how is she/he educating the rest of the company to understand that security is just as integral to the business' success and profitability as any other traditional division's function?

CSO of the Year

Contenders should include those who work for end-user companies only. No vendor CSOs will be considered. Nominees are the cream of the crop, having spearheaded a viable IT security program, gained the support of their company's executive leaders, as well as their colleagues, and helped – through their indefatigable efforts – to propel the CISO/CSO position to a footing of influence within their organization and the corporate world as a whole. Specific projects and undertakings, as well as over-arching security programs to propel these various goals, should be noted. Nominees should be prepared to answer further questions during the judging process, offer at least two references, and be open to holding confidential interviews with members of the *SC Magazine* editorial team if warranted.

Rookie Security Professional

Qualification questions (150 word maximum on all summaries)

* **Please note** *that entrants to this category should have under two years experience in the information security profession. They should work for end-user companies only. No vendor security pros will be considered.*

1. Professional's career history
2. Professional certifications
3. Information about the contender's current position and responsibilities
4. Why he/she should be considered for this recognition
5. Additional details: i.e., examples of exemplary work overseeing and/or handling information security technology deployments, information security policy/risk management planning development and/or implementation; initiatives tying information security plans to business goals; collaboration with other business units and higher-ups, etc.
6. Two to three references from other colleagues, bosses

Rookie Security Professional

Entrants should include those practitioners who have been in the information security profession for under two years. Nominations should come from employers, educators and mentors. Submissions should include the professional's career history, professional certifications, information about the contender's current position and responsibilities, and why he/she should be considered for this recognition. Additional details should include examples of exemplary work overseeing and/or handling information security technology deployments, information security policy/risk management planning development and/or implementation; initiatives tying information security plans to business goals; collaboration with other business units and higher-ups, and more. Two to three references from other colleagues, bosses, and more should also be included.

Professional Awards continue on next page

Categories & requirements

Best Security Team

Qualification questions (150 word maximum on all summaries)

1. How has the security team developed and managed itself within the corporate environment?
2. Please provide two to three professional references with contact details.
3. By what means has the security team gained the support of corporate leaders and colleagues?
4. How has the security team helped to propel the CISO/CSO position to a footing of influence within the organization and the corporate world as a whole?
5. How has the security team strengthened the influence of its department in meeting business initiatives and goals?
6. How has the security team strengthened end-user and customer awareness of IT security threats and safeguards?
7. In what ways does the security team continue to better the expertise of internal IT security?
8. What steps is the security team taking to better position risk management/information security planning as business enabling? That is, how are they educating the rest of the company to understand that security is just as integral to the business' success and profitability as any other traditional division's function?

Best Security Team

Contenders should only include end-user teams that have executed and are managing exceptional and strong security programs, which they have built from virtually non-existent ones. They should have successfully established and implemented an integral and/or innovative/cutting-edge component of their security program and should have spearheaded various areas of support for its success, such as strong end-user awareness training, good configuration management, etc.

Best Information Security Program

Qualification questions (150 word maximum on all summaries)

1. Has the IT security program received the recognition needed at the highest management levels? Explain how this recognition is shown and why this is important to the longevity of the program. Include any mention of funding or resources received because of this recognition.
2. Has the staff upgraded the program's IT security best practices as shifts in IT security technology occur? Note how this has been done and why. Explain how these constant upgrades are relayed to staff, business units, business partners and lead executives.
3. Does the IT security program include ongoing internalized training and awareness programs? Explain what these programs consist of, how they are conveyed to staff and how they are tested and reinforced.
4. Has the IT security program improved various aspects of IT security architecture development and implementation processes (data, network, applications, physical, and more)? Explain how these have been executed, what improvements have been made and how have they been measured.
5. Has the IT security program either led to or resulted in the maintenance of certified (e.g., CISSP, CISM) internal staff, as well as certified personnel in any supporting IT security outsourced vendors? Please explain what certifications have been maintained, why this is important, and methods used to enlist this additional training to ensure relationships with various vendors also meet the corporate standards and expectations of security.
6. Has the IT security program improved compliance with the various regulatory mandates that exist (PCI, SOX, HIPAA, and more)? In what ways?
7. Is the efficacy of the security program considered and measured, i.e., is the most effective technology being used, is manpower being properly allocated, and have parallel tracks been created so other groups (including end-users), within the business can do their part to help security?

Best Information Security Program

For this category, we're looking for programs that have successfully tied information security and risk management initiatives to enable the business. That is, these programs should demonstrate how IT security programs are just as integral to the company as any of the more traditional business divisions. They, of course, should be documented, well-managed and constantly updated (at least annually, but typically more often) programs supported by the over-arching IT security strategy and supportive of the business. These are truly functioning management-endorsed programs for IT security strategic plans that include well-documented IT security policies and standards for everything from operating systems and networks to applications and data security. They should not be reactive programs that include only essential IT security policies and standards, lacking real and published IT security strategic plans. These programs should have great support and buy-in from lead executives and appropriate business units and, as a result, have received the resources and funding needed to be consistently sustained – either through direct budget or through indirect business units' budgets as other divisions play a hand in their continued success and operations.

Professional Awards continue on next page

Categories & requirements

Best Professional Training Program

1. How is the professional training organization helping to educate and strengthen the knowledge of the IT security professional?
2. Please provide two to three professional references with contact details.
3. How does the training program differentiate itself from other offerings?
4. How well is the professional training program meeting the needs of the IT security professional? Explain.
5. How are offerings enhancing end-user awareness and training or enabling end-user companies' IT security professionals to strengthen their secure coding or other IT security practices?

Best Professional Training Program

Programs are defined as those geared toward strengthening expertise of information security professionals via training on secure coding, end-user awareness, and more, by an outside industry expert. Entrants can include companies offering such training and which does not conclude with the winning of a particular professional certification..

Best Professional Certification Program

1. How is the certification organization helping to educate and strengthen the knowledge of the IT security professional?
2. Please provide two to three professional references with contact details.
3. How does the certification program differentiate itself from other offerings?
4. How well is the certification program meeting the needs of the IT security professional? Explain.

Best Professional Certification Program

Programs are defined as professional industry groups offering certifications to IT security professionals wishing to receive educational experience and credentials. Entrants can include organizations in the industry granting certifications for the training and knowledge they provide.

Editor's Choice Award*

Based on information culled from *SC Magazine* events, through research conducted by the *SC Magazine* editorial team for various features and news articles, and conversations with/feedback from readers, analysts, vendors and our *SC Magazine* Editorial Advisory Board, this award is given to a group, person, company or product at the discretion of the U.S. editor-in-chief.

* This category does not accept nominations.

Key info

Contact information:

Natasha Mulla, events manager, at 646-638-6108 or via email at natasha.mulla@haymarketmedia.com.

Mike Alessie, national account manager - event sales, at 646-638-6002 or via email at mike.alessie@haymarketmedia.com.