Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Inaugural Health Care Survey

Copyright SANS Institute
Author Retains Full Rights
There is no doubt that health care—and the technology that supports it—is changing. Digital health care offerings, such as patient access to records from any device, are affecting the way that patients and providers interact both with each other and with clinical and payment data. Electronic health record systems (EHRs), health information exchanges (HIEs), and health insurance exchanges (HIXs)—are all new to a health care community still largely dependent on paper-based workflows.

More stringent regulatory oversight is also impacting all aspects of health care, including medical instruments and applications. New, productivity initiatives such as bring your own device (BYOD) are also being added to this work and regulatory environment.

What challenges do individual providers and organizations face as the traditional controls around privacy and security drop away with the disappearing infrastructure? What is the role for “securing the human” in this changing landscape? And what are their perceptions about regulation versus security posture?

These questions provided the focus for this SANS Inaugural Survey on Health Care, which drew 373 respondents, predominantly from the United States. This survey reveals aspects of security in the health care arena from the perspective of IT security staff—managers, analysts, and executives. In it, respondents indicate that their concerns around cloud and mobile computing do not outweigh their need for adoption of these technologies. More than 50% of respondents report that they are using cloud computing in whole or in part. Personally owned devices are operating alongside company-issued devices in most organizations as well, although not at as high a percentage.

Respondents also indicated that their business drivers for security are focused primarily on regulatory compliance. This leads us to believe that decision makers need a more balanced understanding of the technical, clinical and compliance requirements to establish a solid security framework that enables their workforce to effectively manage risk while also complying with regulatory mandates.

These and other trends based on this survey are revealed in the following full report.
Between July 28 and Sept. 19, 2013, SANS surveyed professionals working or active in the health care community who are involved in promoting better security and privacy through policy, practices and technology. The vast majority—82%—considered themselves an employee of the health care organization for which they work as opposed to a business associate (10%) or other type of relationship (8%).

Mostly IT Focused

Although the survey was promoted to clinical, executive and IT members of the health care community, the respondents overwhelmingly represented IT management and staff, with a total security leadership representation of 40%—IT security management (33%) combined with CSO/privacy officer (7%). IT staff (25%) and IT management (13%) were the other primary groups, as shown in Figure 1.

Given respondent emphasis on compliance as a business driver for organizational security priorities, we were surprised by the relatively low percentage of respondents whose primary role involved auditing/compliance (7%) or serving as a quality assurance/risk manager/compliance officer (less than 1%).

Compliance personnel usually understand the regulatory “business rules” that affect the privacy and security posture of the organization, but may not be fully aware of what can be achieved with state-of-the-art technical controls nor fully conversant with IT security “best practices.” Limiting a compliance audit to a “spreadsheet analysis” of policies and procedures, putting faith in a single penetration test or depending on a “certified” system without regard to its networked configuration are all potential shortfalls associated with a lack of technical knowledge by compliance personnel. On the other hand, the IT security staff needs to understand the business needs of an organization as they relate to compliance as well as the tough security practices required to guard sensitive information against the ever-changing threat environment.
Also of interest was the extremely low percentage of clinical personnel involved in the security space. We would have liked to gain the viewpoint of more clinically oriented staff. Future surveys will need to take this into consideration.

Ultimately, outreach between clinical, compliance and IT staff is needed to achieve better awareness of security-related business drivers and a more effective organizational structure that can meet the threats of an increasingly dynamic electronic environment.

**Hospitals and IT Services Most Represented**

The participants who took the survey represent a broad range of organizations within the health care industry, as well as a wide range of organization sizes and IT security budgets. The largest group represented IT staff working in some form of clinical setting (hospital, physician groups, rural/critical access hospital, or individual provider). Figure 2 shows the distribution of health care organizations for which respondents work.

Hospitals (32%) and providers of IT services (25%), such as hosting, telecommunications and other support, accounted for more than 55% of the organizations represented. This was followed by those that classified their organization as “Other” (17%), representing an interesting mix of organizational types, including:

- Medical certification and credentialing services
- Health care staffing agencies
- Group purchasing
- Call centers support
- Legal services to the health care industry
- Manufacturing medical systems and devices
- Benefits management
Representation from health payers and plans (13%) was slightly higher than that of physician group practices (12%), followed by ancillary service providers (10%), such as radiology and laboratory and pharmacy organizations (10%).

**Mostly Large and U.S. Based**

The survey was available to international respondents, although respondents’ emphasis on the HIPAA Omnibus Rule as a business driver infers that the majority of the respondents are from the United States. The majority of respondents (29%) were affiliated with large organizations having more than 15,000 workforce members, while another 15% had 5,001 to 15,000 workers, showing that mostly large organizations took this survey, as shown in Figure 3.

![Figure 3. Workforce Size of Respondent Organizations](image)

Larger health care organizations have greater resources and can leverage economies of scale because they are most likely already heavily dependent on systems that must protect electronic protected health information (ePHI)—electronic billing is the norm.

On the other hand, smaller practices and individual providers, especially in remote or rural environments, are faced with a potentially daunting challenge of stretching already thin resources even further. As one respondent stated in his comments, “HIPPA, PCI, FISMA and all of the other security acronyms are too much for small practices. Easy-to-implement solutions are desperately needed.”

These solutions also need to be cost effective, as another respondent noted when he mentioned the unwillingness of smaller practices to spend money on security. If it comes down to a choice between getting reimbursed for services being provided to a patient or complying with security overhead (and not getting paid), the smaller practice will accept the risk of not being compliant.
**Investment in Security**

We also asked respondents to provide the percentage of their total IT budget devoted to security. The largest group of respondents (35%) was unsure of the percentage of the total IT budget devoted to security. The next largest group (25%) spends 1% to 3% of their IT budgets on security, fairly standard for most IT operations; 29% of respondents spend over 4% on security; and 5% of respondents indicated that security is more than 10% of the IT budget.

When comparing organizational size to budget committed to security, you can see that assets and resources are lacking completely in the smallest of organizations, with an interesting bump up between the 6–10 member organizations where more than 10% of budget was the most chosen answer; and again in the 51–100 member-size organization, where 4% to 6% was their most common answer, as shown in Figure 4.

When asked to estimate any changes in this percentage over the next 12 months, those respondents that reported percentages of under 6% of the total budget indicated a slight reduction from the current levels in the expected percentage of the budget devoted to IT security for the next 12 months. Those investing over 6% showed no change. The percentage of those unsure about the percentage of IT budget devoted to information security was slightly higher—39% as opposed to 35% for the current budget spent on security.
When asked to rank the major business drivers for their organization’s information security priorities, drivers that deal with compliance and monetary aspects of compliance as a business driver rose to the top of the list.

**Regulations Drive Security**

Respondents cited the following top six business drivers, all of them related to compliance (with 1 being the most important and 6 being least important):

1. Compliance with the HIPAA Omnibus Rule
2. Meaningful use standards of the Centers for Medicare and Medicaid Services (CMS) incentives
3. Concern over CMS audits, being compliant with CMS audit criteria
4. Compliance with standards and other regulatory requirements such as PCI, FISMA
5. Implementation of breach notification rules and procedures
6. Concern over possible recovery audits for fraud, waste and/or abuse

Top on survey takers’ minds must be the recent start of formal compliance for the HIPAA Omnibus regulation, which commenced Sept. 23, 2013. The next key driver is Meaningful Use (MU), the set of standards defined by the CMS Incentive Programs governing the use of EHRs and allowing eligible providers and hospitals to earn incentive payments from CMS by meeting specific criteria.

MU criteria calls for providers or hospitals to attest to the protection of “electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities” by conducting or reviewing a security risk analysis per the HIPAA Security regulation, correcting any identified deficiencies as part of the [provider’s or hospital’s] risk management process.¹ HIPAA security compliance is a major consideration for those providers or hospitals that have received funding under the EHR Incentive Program—their attestation may very likely be verified by audit.

Actual IT security practices as drivers emerge lower on the list of business drivers and included, again in descending order, the following:

- Managing the workforce, including security training and awareness
- Mobile device security challenges (with or without BYOD policies)
- Establishing resiliency of IT operations
- Taking advantage of cloud computing
- FDA regulations over equipment (e.g., biomedical, medical devices, etc.)
- Impacts of big data and analytics (e.g., all-payer claims database [APCD], etc.)
- Other considerations

An organization’s investment in security can also be measured by its commitment to security practices as part of its system development life cycle (SDLC) for major projects.

Starting Early

To be effective, the practice of information security cannot be separated from the business and should be part of the system development lifecycle from the start. We asked our respondents when their information security resources are normally involved in the system development lifecycle for major IT-related projects.

It was gratifying to see activity going on at all levels of the project life cycle, with 21% of respondents reporting that security resources are engaged at inception (the first occurrence of the project idea); 10% at ideation (project is worked within the group without stakeholder participation); 17% at formalization (the project is initially funded and stakeholders are formally engaged); and 5% at refinement (stakeholder feedback is incorporated as part of detailed requirements). Figure 5 illustrates these results.

However, another 26% report that security resources are engaged only “as needed,” and approximately 14% wait until later SDLC phases to involve their security resources.

Note that the later an organization’s IT risk management group gets involved in security of their new acquisitions, projects and acquisitions, the more costly it becomes to implement secure processes and remediate vulnerabilities. Most, if not all, major security frameworks should start with risk assessment to understand the threats and vulnerabilities facing an organization’s use of information systems and networks. This is a basic tenet of the Critical Security Controls that many health care, financial and federal agencies are using to augment their compliance-based approach to security and audits.2

---

2 www.sans.org/critical-security-controls
Perception of Risk

Respondents indicated that their organizations have a strong grasp on the risk to their applications and data. The risks posed by negligent insiders (65%) was their biggest concern. This result is in line with the Third Annual Benchmark Study on Patient Privacy & Data Security by Ponemon Institute, published December 2012, which found that “insider negligence continues to be at the root of the data breach.” The primary cause of breaches in the Ponemon study was a lost or stolen computing device (46%), attributed in many cases to employee carelessness followed by employee mistakes or unintentional actions (42%).

Insider negligence was followed closely by a related concern of respondents over the lack of investment in user awareness (53%), a concern also echoed in the Ponemon report, which states, “Employee training is the most common activity but does not seem to be effective in reducing insider negligence.”

Interestingly, these internal issues take precedence over the threat of malicious outsiders, in which 51% indicated this was a top concern. Not far behind is risks imposed with adoption of new forms of media and device use (39%), such as mobile or BYOD, which circles right back to concerns over user awareness. The results are shown in Figure 6.
Infrastructure-related failures (32%) and networked biomedical equipment and medical devices (26%) rank lower among respondent concerns. We find this surprising in light of issues around medical devices—and now applications—being hard to upgrade and add security due to FDA rules protecting these devices and applications because they are considered patient-care equipment.\(^5,6\)

The emphasis on threats afforded by biomedical equipment and medical devices may also escalate in light of increased scrutiny on problems surrounding devices such as radiology workstations, echocardiogram machines and human-embedded monitoring devices. These equipment and devices, touted as “appliances” that are “plug and play” for patient care, are actually sophisticated computing devices, often running outdated versions of operating systems and applications not resilient against purposeful attacks.\(^7\)

**Business Critical Assets**

When asked about their most critical assets, respondents reported their top three were the following:

1. Electronic medical record (EMR)/electronic health record (EHR)
2. Personal health record (PHR)
3. Major clinical applications, such as lab, radiology and pharmacy ancillary services

The emphasis on the EMR/EHR as a critical system asset is not surprising because this capability represents a major investment for providers and organizations, impacting on clinical workflow. The risks associated with an EMR/EHR are also a relatively new concern for many individual providers and smaller organizations because, in light of cost incentives, patient health records are being pushed out to solutions in the cloud. Controls around the data must be auditable in the cloud; however, we are not sure whether the controls or the cloud are the biggest concern.

What is surprising is that respondents ranked PHRs as their second most critical information system, a possible early indicator of emerging health care industry trends. When it comes to PHRs, there are two distinctions: tethered and untethered.

A “tethered” PHR, such as a patient portal provided by an EHR vendor (e.g., Cerner or Epic), is tied directly to the EHR system owned by the organization with information in the portal managed by the organization. This type of PHR is subject to the same regulations that govern the EHR for that organization.

---

5. [www.fda.gov/MedicalDevices/default.htm](http://www.fda.gov/MedicalDevices/default.htm)
6. [www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm](http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm)
An “untethered” PHR, such as Microsoft HealthVault, is free standing, under patient control and not necessarily highly regulated by legal means. With the increased emphasis being placed on patient-controlled data, a key objective of MU criteria in the United States,8 concerns over risks increase as patients, not trained clinically and uneducated as to the privacy and security risks involving electronic data, contribute to their health care record’s vulnerabilities. Patient use also ties back into the cloud, wherein these providers are connecting to access data, which we discuss in more detail in the next sections.

Meanwhile, the rest of the response rankings for most critical system assets are, in descending order:

- Practice management/billing
- Health information exchange (HIE)
- Supporting infrastructure (e.g., underlying middleware, network as a whole)
- Security monitoring and defense tools
- Mobile devices
- Health insurance exchange (HIX)
- Telemedicine/telehealth data

The ranking of what information systems respondents considered most at risk from a security or compliance perspective did not exactly track with the criticality of their assets, which we discuss in the following section.

8 www.healthit.gov/providers-professionals/how-attain-meaningful-use
When it comes to criticality of their organization’s assets, respondents chose EMRs/EHRs as their top ranking (65%), in line with their criticality of assets. Then they veer away to list mobile devices (51%) as their next most risky asset, probably because of their high probability of exploitation or compromise. See Figure 7 for the full ranking of their concerns.

Of the information system assets you ranked in the previous question, which are the top three that you consider to be most at risk from a security or compliance perspective?

This, again, tracks back to new forms of cloud (information exchanges) and mobile device usage as contemporary risks that program managers should be wrapping into their risk management and compliance policies and procedures.
Clouds and Sunshine

Health care has been moving toward adoption of cloud computing for many years. Almost 48% of respondents indicate that their organization uses some form of cloud computing to process protected patient and financial information. Of these, almost all indicate dependence on cloud-based services, either totally or partially, for applications that might contain sensitive information (see Figure 8).

Comments input under the “Other” category include practice management and billing services, application development (which raises potential concerns around the use of representative test data drawn from “live data”) and niche applications such as registries and case management. One respondent raised a key point that an organization may have “side apps,” which are not intended to hold protected health information but nonetheless do. Because these applications may not normally be monitored as part of overall administration activities around sensitive data, these side apps can offer a potential source of exposure that may not normally be accounted for.

One of the current topics involving cloud computing is the architectural decision around using the public versus private versus hybrid cloud (both public and private). Security considerations must include the separation of functionality and data between allocation of services and data storage between on-premises and off-premises cloud assets. Reliance on cloud-based computing will most likely challenge the current state of the supporting infrastructure and modify reliance on traditional, network perimeter-based controls.
Cloud Concerns

We next asked respondents to identify their organization’s greatest concerns about the security of using cloud solutions. Respondents are most concerned about data leakage/disclosure (75%) and organizational loss of control over protected data (66%). This latter concern is especially critical because it is a major impediment to the exchange of health information between unaffiliated entities, who are most often concerned over patient loss to potential competitors. The results are shown in Figure 9.

Overall, respondent concerns indicate that the traditional mindset around information assets and data has to change in a cloudy world:

• One respondent mentioned that the organization’s cloud vendor was not willing to sign a contractually related business associate agreement (BAA), a common problem being encountered with major vendors such as telecommunications carriers or hosting services. (Note: In the United States, the HIPAA Omnibus Rule clarifies when organizations, such as covered entities and business associates, would be liable for breaches of “downstream” business associates. The Rule makes covered entities and business associates liable under § 160.402(c) for the acts of their business associate agents, in accordance with the federal common law of agency, regardless of whether the covered entity has a compliant BAA in place. In short, even if a vendor refuses to sign a BAA, the vendor may still be found responsible for security as if a BAA were signed.)

• Another respondent mentioned the loss of control over security monitoring, inferring that their business associate was not monitoring the right type of security events, a situation that potentially could be corrected by contract, BAAs and required audits of performance and conformance.

Figure 9. Perceived Risks of Cloud Computing

• One Australian respondent raised the issue of liquidity of data as a potential problem. The respondent noted that we cannot put EHR into the cloud unless we can guarantee the EHR and its data reside in Australia, a common problem regardless of the country.

What laws govern access and audit of remote-hosted data—those of the jurisdiction of the data owner or those where the data is actually hosted? How is data to be managed in a multitenant environment? In smaller data centers, the organization may mandate that its data be resident on dedicated hardware but, in a world that is moving toward virtualization, this may become economically unfeasible if an organization wants to capitalize on the opportunities afforded by cloud computing.

Mobile Adoption Also Rising

Mobile health care (mHealth) is rapidly evolving, and the future is emerging quickly. Research and Markets predicts, “mHealth applications will become an integrated part of doctors’ treatment plans” by 2017. The use of mHealth is not confined to countries with well-developed economics as indicated by a November 2012 report by Ipsos on a study commissioned by the Groupe Speciale Mobile Association (GSMA) conducted among 2,000 health care practitioners, patients and consumers in U.S., Brazil, India and China. The report concludes that “it is widely believed that mHealth solutions can help to address many challenges resulting from chronic disease: high healthcare costs, inequality of care, behavioral challenges, cost inefficiencies and low quality care.”

From a mobile device perspective, respondents indicate that both BYOD and organization-issued devices are available for accessing informational resources, as shown in Figure 10.

What information systems/assets are mobile devices allowed to access in your organization?

Please select all that apply, indicating whether your policy allows access by company-issued devices, BYODs, or both.

Figure 10. Mobile Device Access to Organizational Assets

---

10 www.researchandmarkets.com/research/nhc8j7/mobile_health
11 www.ipsos.com
12 www.gsma.com/mhealth
Either BYOD or organization-issued devices are considered compatible for non-sensitive data and application access to include email, calendar and Internet access. Organization-issued devices become the norm for access to the more sensitive information for that entity—health, financial and HR data—although there remains a residual policy that these applications can be accessed from both personal and organization-issued devices.

The greatest security concerns for respondent’s organizations over the use of mobile devices are shown in Figure 11.

Of the respondents, 83% cite loss or theft of mobile devices as a chief concern, a concern that is still substantiated by the statistics reported by OCR. As of Sept. 17, 2013, theft remains the leading reason for reported breaches within the United States, followed by unauthorized access/disclosure and loss. Lack of employee awareness, a perfect justification for increased investment in workforce awareness training around mobile security policies is the next concern, mentioned by 73% of respondents before moving into those security practices that can be more effectively monitored by technical means such as insecure/unprotected endpoints (slightly fewer than 73%), corrupt or malicious mobile applications (67%), insecure Wi-Fi use (48%) and insecure web browsing (46%).

14 www.melamedia.com/HIPAA.Stats.home.html
Managing New Risks

The survey asked how organizations are managing the new risks of cloud and mobile, and how they feel overall about their full security and compliance programs.

**Overall Security Controls**

Respondents consider network/perimeter defenses for security as the “most effective” (50%) or “effective” (40%) security controls for their organization, as shown in Figure 12.

![Most Effective Current Security Controls](chart)

While no other control approaches the weight placed on network/perimeter defenses, respondents also rely heavily on “effective” controls, including administrative policies and procedures (50%), identity and access management (48%), contractual measures (48%), vulnerability management (48%), endpoint protection other than encryption, application security, and database security.

“Least effective” controls included those around big data initiatives and data governance (37%), a definite concern for governmental entities that store and exchange personal (citizen) data, including health information, electronic medical device protection (32%), which again talks to the complexity of security issues dealing with biomedical equipment and medical devices, and policies and procedures (32%). This points to a fairly wide variation in how these administrative controls are developed, managed and enforced.

Given the variation in how respondents reported on the effectiveness of their security controls, it is clear that no one is relying primarily on one or two control families. This indicates that a layered, defense-in-depth approach to security is being followed. However, reliance on network/perimeter defenses being the most effective control will need to be realigned as sensitive data and the boundary for data protection move off premises into the cloud.

---

Cloud Controls

Cloud computing will push aside some of the traditional dependencies, like reliance on supporting infrastructure and perimeter controls that are tied to a definitive system or network boundary.

Respondents rank the security controls they believe can best address cloud security as shown starting with the most effective at the top:

- APIs for reporting, auditing and providing alerts on security events
- A scalable encryption mechanism for data in the cloud
- Vulnerability management/patching status
- Data segregation and use monitoring
- Secure, multifactor access to cloud applications
- High integrity infrastructure, free of malware
- Master data management, including effective patient matching and provider identification
- Unified policies applied across cloud solutions

As noted by one respondent in the comments section, the greatest concerns are lack of visibility into cloud-based security events and lack of encryption (or assurance that encryption is present) for data at rest.

Mobile Controls

Respondents also prioritized the controls they felt would be the most effective in addressing their concerns around mobile, including, in order of perceived effectiveness:

- Strict mobile device management (MDM) controls around all mobile/BYOD endpoints allowed access
- Awareness education/training
- Data encryption
- Network access control (NAC) or other access controls that will scan the BYO device before granting access without MDM
- Sandboxing/not permitting actual data storage on devices (even in memory)
- Mobile media encryption
- Cloud-based scanning/inspection services are carried out on BYO devices before granting access
Satisfaction with Security Programs

Most respondents feel that their organization could improve its ability to counter security threats, whether internal or external to the organization. Almost 50% of respondents consider that their organization needs some improvement to effectively counter threats, with an additional 15% feeling that their approach needs complete rework, as shown in Figure 13.

On the other hand, some respondents feel their organization is basically in good shape, with 12% reporting their ability as “adequate,” 16% as “above average,” and 4% as “excellent.” It was refreshing that only 2% stated they didn’t know the ability of their organization. The few that responded as “Other” provided the following comments that demonstrated a sense of realism about their organization’s ability:

- “Good, but only as good as the next emerging threat.”
- “[It] “depends on the environment; some are adequate, others are in need of complete re-work.”

Figure 13. Ability to Counter Security Threats
Looking Forward

Universally, and substantiated by concerns around cloud and mobile computing, we have seen an emphasis on security awareness training for an organization’s workforce. Overall, this is tagged by respondents as the top priority—even though it may not be the first priority. They’re also just as concerned with resiliency and improved response, as shown in Figure 14.

Improved creation and enforcement of administrative controls, chiefly policies and procedures, are also key. The need for increased surveillance due to health care industry trends (such as increased value of medical identities and recovery efforts related to fraud, waste and abuse) should be kept in mind to balance operational and compliance needs. There is a need to incorporate policy awareness into cloud-based infrastructures, as well as monitoring practices that can carry over into that environment and act as a deterrent to insider abuse.
In the end, the practice of effective cybersecurity in health care comes down to an assessment of the business risk. Unfortunately, as we have seen from the results of this survey, the business decision may be, “What is the chance I will be audited, versus what will the practice of security cost me?,” as opposed to the simpler “What should I do to defend my systems and my data against emerging threats?”

Especially for smaller practices, many will be unwilling to spend money on security or dedicate needed resources in an office where staff is already stretched too thin undertaking reimbursable activities around patient care.

The health care industry is truly incentivized to adopt cloud and mobile computing for numerous reasons—not the least of which are cost, improved workflow, better interoperability and innovation. These trends are game changers for the way an organization must approach security (and privacy) in new ways that no longer rely on traditional, infrastructure-driven controls such as network/perimeter security. That said, the actual supporting infrastructure—the last mile connection to the EHR in the cloud—will become an even more critical asset than it is today as it must ensure availability to the mission-critical data of health care.

Health care providers and organizations need to become more aware of the nature of their sensitive data, how to ensure its integrity and its confidentiality while entrusting its safekeeping to a remote third party. Data governance will become even more important, and policies around data, enacted and enforced by technology, will become more and more the norm.
Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls “policy, process, platforms, pipes and people.” She has focused most recently on HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system development lifecycle as well as its relation to many of the issues faced by a modern society dependent on automation—privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold) and GCIH (Gold), and the GHSC.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>