New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations

A SANS Survey

Written by Barbara Filkins

December 2014

Sponsored by
Qualys

Executive Summary

Health care is often considered a lucrative business for those involved in waste, fraud and abuse.[1] Today's ever-accelerating technology changes make data related to health care, medical and financial issues even more attractive (and profitable) to cybercriminals who sell medical identities and siphon money from stolen financial records. Risks are exponentially increased because of organizations' reliance on electronic systems for mission-critical functions. According to 61% of respondents to the SANS 2014 State of Cybersecurity in Health Care Organizations survey, medical/health record systems are considered the most at-risk information asset among the 224 health care-related organizations represented in the survey.

Security Gains

Slight budgetary increase:
13% of small companies now receive 4–6% of the overall IT budget for security

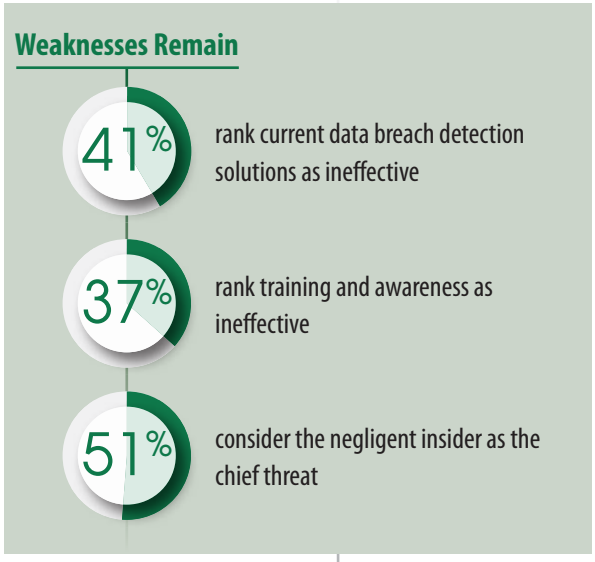
Controls closer to the data:
70% of respondents rated application and database security controls as effective/very effective

Security in development:
3% more respondents in 2014 than in 2013 incorporated security into the funded phases of the product development life cycle

This survey also reveals new risks created by the increasing reliance on mobility for delivery of health care information. The survey indicates that the growing presence of online personal information and new methods of accessing and transferring medical data are increasingly putting sensitive protected data at risk. According to the survey, 42% of respondents are concerned about the risks associated with personal health records and 36% with patient portals, while another 21% are most concerned about consumer-facing mobile apps.

Ultimately, the trend of pushing sensitive data outside an organization's protected environment via cloud computing, mobile identity and access, and the "Internet of [Care] Things" demands that security be pushed closer to the actual data. This is one of many challenges health care IT organizations are starting to take seriously and improve upon, according to the results of the second SANS Survey on Health Care Cybersecurity.

[1] www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf



Progress starts with increased awareness, as triggered by several events early in 2014. In February, SANS published a report[2] based on cloud-based threat intelligence data collected over a 12-month period that demonstrated the compromise of thousands of IP addresses owned by health care organizations in the United States. In April, the FBI issued a Privacy Impact Note (PIN) alerting the health care industry about cyberthreats, citing the SANS report.[3]

The good news, based on responses to the current survey, is that the health care industry recognizes its data is out of the box, so to speak. Industry protection, prevention and response processes must address the openness of systems, while also addressing older legacy systems and the Internet of Care Things, such as medical devices that are also subject to regulatory compliance. Although compliance is still the top driver of information security priorities for most respondents, they are now turning their attention to threat response and other measures. Security budgets are increasing slightly, further highlighting respondents' increased awareness of the vulnerabilities and threats affecting their organizations.

[2] www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

[3] www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf

Understanding the Environment—Size and Complexity

84% considered themselves an employee

11% considered themselves a business associate

6% had another type of relationship with the health care organizations for which they worked[4]

During September and October 2014, 224 professionals involved in promoting better security and privacy through policy, practices and technology took this SANS survey. Although the survey was promoted to clinical, executive, IT and other members of the health care community, the respondents were overwhelmingly technical (72%), with 23% representing IT security leadership (chief security officer, chief information security officer, or security director or manager), 33% IT security staff (IT security engineers and administrators), and 16% IT staff and management. These respondents represented a population especially qualified to address the drivers and effectiveness of information security in their organization.

Hospitals remained the most widely represented entities in this survey, with 32% of respondents working for this category in both 2013 and 2014. This year, the survey included an option for describing the organization as a health care system/health care delivery network, and 28% chose this option, as shown in Figure 1.

Which of the following describes the health care organization where you work?
Select all that apply.

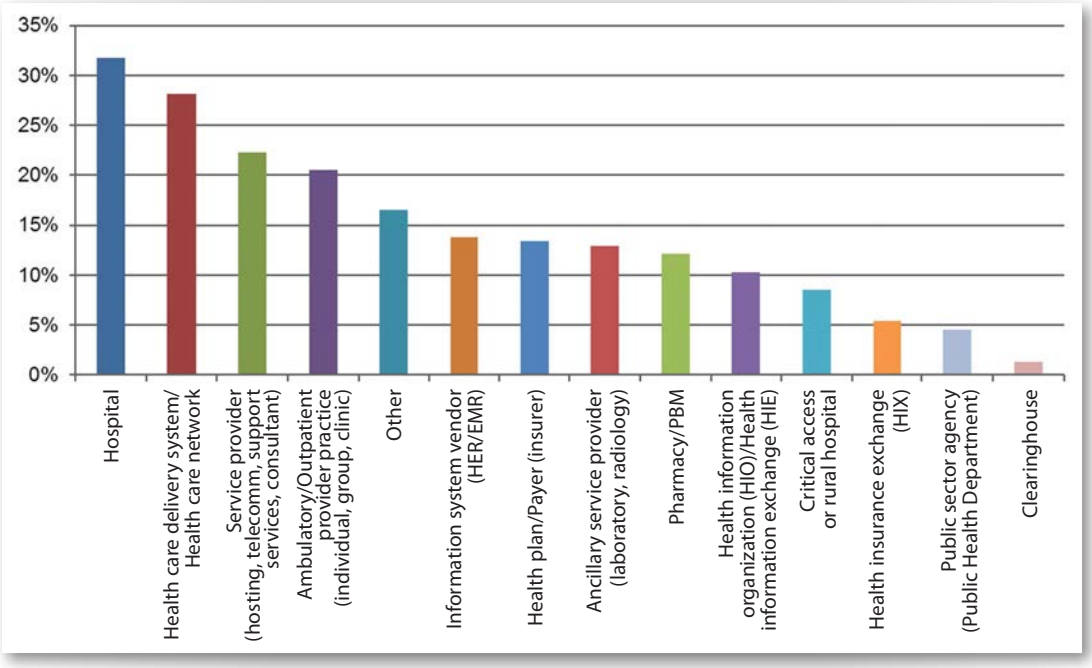


Figure 1. Types of Organizations

[4] Results total to more than 100% due to rounding.

A closer examination of the data reveals that the 49% of the hospitals and 30% of ambulatory/outpatient provider practices in this report belong to a delivery network, accounting for the high ranking of this new category. Membership in a health care network has implications for the complexity of data for which it is responsible and access to resources to manage and secure this information.

Enterprise and very large organizations were most strongly represented in this survey, with 43% of respondents from enterprise (more than 25,000 employees) and very large (5,001–25,000 employees) organizations. Another 23% of respondents represented organizations of 1,001–5,000 employees, and the rest represented organizations of up to 1,000 employees.

Hospitals and delivery networks, as expected, account for the highest numbers of workforce members, when service providers and information system vendors are excluded from the analysis, as shown in Figure 2.

HEALTH CARE DELIVERY SYSTEM:
"The organization of people, institutions and resources that deliver health care services to meet the health needs of target populations."[5]

HEALTH CARE NETWORK:
"A group of physicians, hospitals and other health care providers that agree to provide medical services at pre-negotiated prices and rates."[6]

Workforce Size by Organization Type

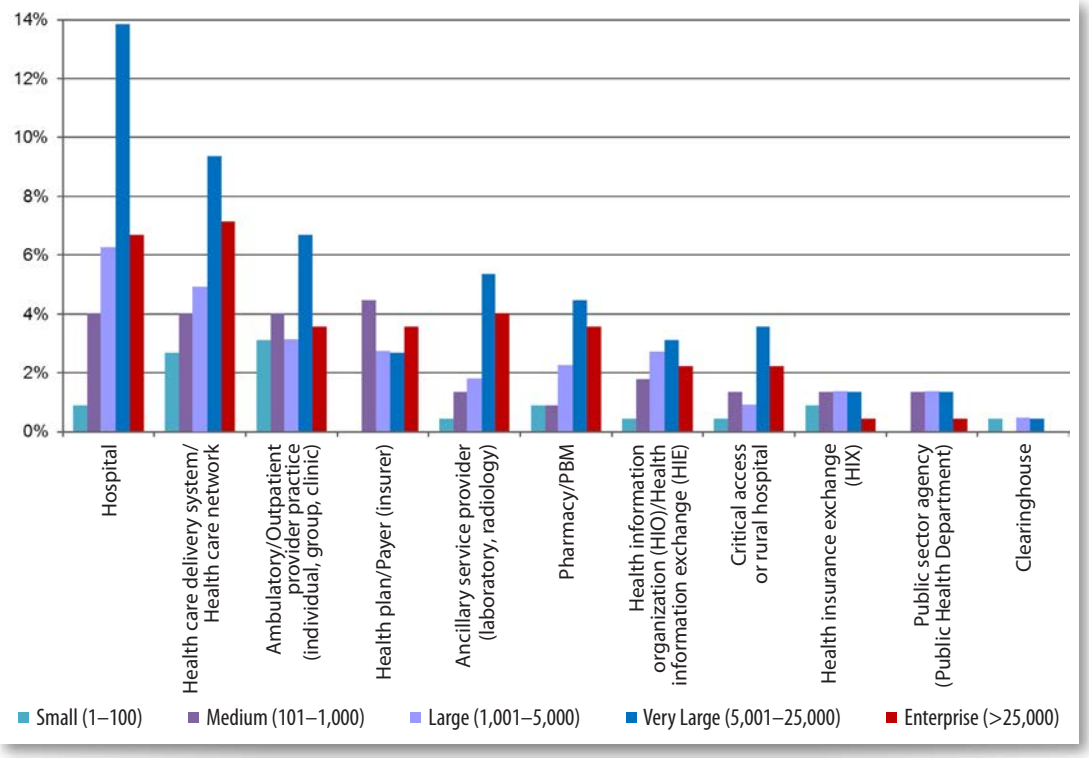


Figure 2. Workforce Size by Organization Type

Of the service providers, ambulatory and outpatient services covered the gamut of size ranges, with the 5,001–25,000 range prominent among this group, again indicating these practices are most likely affiliated with a health care network or hospital.

[5] http://en.wikipedia.org/wiki/Health_system

[6] www.goldenrule.com/videos/what-is-a-health-care-network

Priorities Echo Real Risks

Mobile and cloud technologies, as well as health care exchanges, are all changing the way health care organizations manage risk internally, extend security to their partners and ensure security in concert with their application providers. Demand for consumer-facing applications, especially mobile applications (and emphasis on patient engagement, which drives portal access), spawns a whole new set of concerns and risks because such applications rely on consumers to manage their own sensitive data.

Demand for consumer-facing applications, especially mobile applications, spawns a whole new set of concerns and risks because such applications rely on consumers to manage their own sensitive data.

The good news is that, across these systems and technologies, respondents cited a consistent set of security and compliance drivers for their practices and controls. Drivers for securing sensitive data across a variety of systems and platforms, based on a weighted average of the top three choices by respondents, are, in order:

1. Complying with standards and other regulatory requirements (HIPAA, PCI, FISMA, FDA)
2. Ability to respond to new or emerging threats or advanced persistent threats (APTs)
3. Ability to recover quickly from a breach incident
4. Assuring resiliency of IT operations
5. Managing the workforce, including security training and awareness
6. Improving efficiency and lowering cost of IT operations
7. Supporting consumer-facing applications (patient portal, mHealth, wearables)
8. Managing vendors and business associates
9. Adopting or developing mobile health initiatives (mHealth)
10. Supporting new cloud applications (electronic health records [EHRs], health information exchanges [HIEs])
11. Supporting telemedicine/telehealth

As in the 2013 survey, meeting compliance standards and regulatory requirements was identified as most important by respondents. The next three most frequently selected items in this year's survey (response capabilities, recovery and resiliency) differ from those selected most often last year and reflect the need for an organization to respond effectively and quickly to an incident.

A separate study reported in iHealthbeat recently rated health care and pharmaceuticals as the lowest performing industry in incident response, with the average time to contain a security breach a worrisome 5.3 days.[7] See the next page for some basic steps to improve your response plan.

[7] www.ihealthbeat.org/insight/2014/health-care-providers-look-to-improve-security-incident-response

Develop a plan to ensure quality response and timely recovery.[8]

- Assess your ability to detect, respond to and contain threats.
- Make sure the organizational incident response (IR) strategy is consistent with organizational security policy.
- Grant sufficient authority to the IR team to take specified actions.
- Define roles and responsibilities of the IR team and parties participating in the response process.
- Establish a list of prioritized information assets and services, as well as acceptable downtime.
- Develop and communicate procedures for reporting, escalation and other needed activities.
- Test your IR processes.
- Educate the team on emerging threats and train team members to handle both expected and unexpected incidents.

Information at Risk

Electronic medical/health record systems are considered most risky, according to 61% of this year's survey respondents. This concern also topped the list in 2013. What is interesting is that the supporting infrastructure (encompassing underlying middleware and the network as a whole) was ranked as second by 45% of respondents, a clear indication that compromise of the infrastructure is considered key in today's cyberthreat landscape. Personal health record systems and patient portals were ranked third and fourth by respondents, underscoring the importance and risks of consumer-facing applications. See Figure 3 for a full risk ranking of respondents' health care-related systems.

What information system assets do you consider most at risk?
Select all that apply.

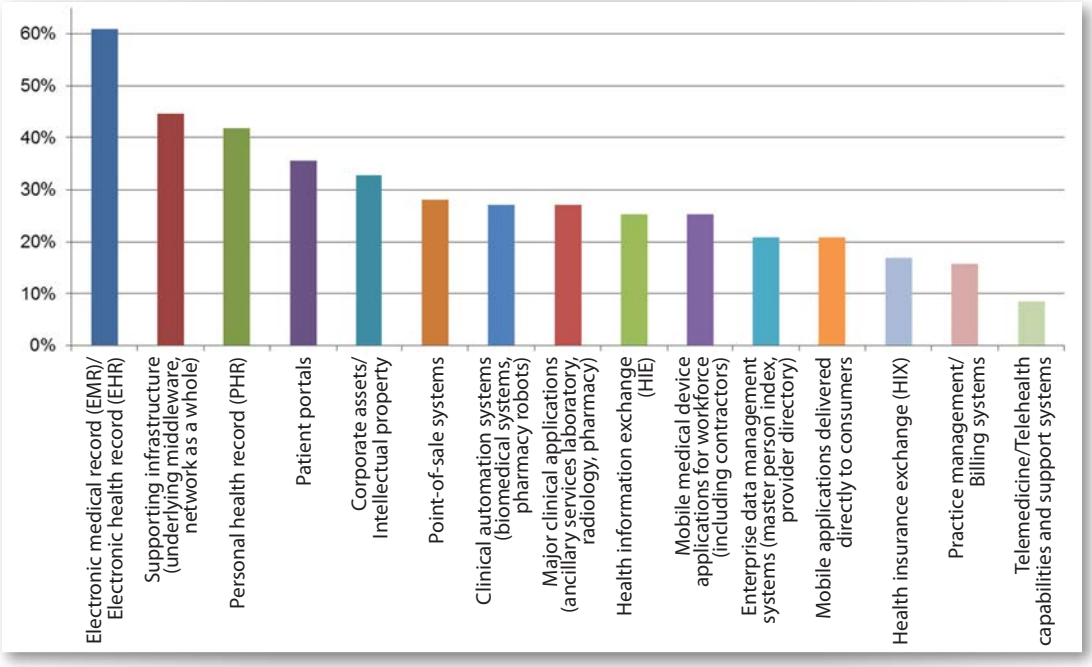


Figure 3. Risk Ranking for Information Assets in Health Care Systems

[8] For more suggestions, see Incident Response: How to Fight Back (A SANS Survey), www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342

Despite changes to the response structure used to identity information assets considered most at risk by respondents,[9] the majority of categories from 2013 retained their ranking for 2014, as shown in Table 1.

Table 1. Comparison of Information Assets Most at Risk—2013 vs. 2014[10]

	Percentage	
Information Assets at Risk	**2013**	**2014**
Electronic health record/Electronic medical record (EHR/EMR)	65%	61%
Supporting infrastructure	40%	45%
Personal health record	36%	42%
Patient portals	NR	36%
Corp. assets/intellectual property	NR	33%
Security monitoring	26%	NR
Point-of-sale systems	NR	25%
Clinical automation systems	NR	27%
Major clinical apps	38%	27%
Health information exchange (HIE)	20%	25%
Mobile medical devices	51%	25%
Enterprise data management	NA	21%
Mobile apps to consumers	NA	21%
Health insurance exchange (HIX)	4%	17%
Practice management/Billing	16%	16%
Telemedicine support	10%	9%

Mobile devices were identified in two response categories for 2014, and the total response percentages roughly equaled the 2013 total. Health insurance exchange (HIX) was identified as being in the top three risks by only 4% in 2013 and by 17% in 2014, possibly as a result of the attention drawn to the insurance exchanges by the security breach on a healthcare.gov server.

Continued emphasis on the electronic health record/electronic medical record (EHR/EMR) as a critical system asset is not surprising because this capability represents a major investment for most providers and organizations. Respondents also acknowledge the criticality of the supporting infrastructure in securing EHR/EMR and its data, a dependency that is changing with EHR/EMR solutions being pushed to the cloud for better flexibility, performance and price.

[9] In 2013, respondents were asked to identify the top three information assets most at risk from 11 categories, whereas in 2014 they were asked to check all assets that applied.

[10] In this table, NR stands for no response, meaning that no survey participants chose that option. NA stands for not asked, meaning the option was not included in the survey.

In our 2014 survey, patient engagement and wellness are major business drivers for this industry, fueled by numerous social, political and monetary incentives to attract and support the health care consumer. The continued high ranking of personal health record assets in 2014, combined with two new categories this year (mobile apps to consumers; patient portals), reveals that organizations are putting increased emphasis on protecting related assets.

Cloud/Mobile Risks

Health care organizations rely on cloud services for applications processing sensitive information, including protected health care patient records as well as PCI-protected financial information. Respondents plan to expand these services in the next 12 months. Open-ended responses by several respondents reflect the bias against cloud services, most often prompted by concerns over loss of control or oversight over sensitive data, but more than 60% are either using or planning to use the cloud for multiple applications containing sensitive data, as shown in Figure 4.

TAKEAWAY:

New methods that access, transmit and share sensitive information present expanded attack vectors for cybercrime. These include patient records transmitted on various media, HIPAA-compliant texting between patient and physician, telemedicine services via smartphone, remote monitoring tools, and patient-implanted "intelligent" devices.

Which of your cloud-based applications contain (or may contain) sensitive information, in whole or in part? ***Select all that apply.***

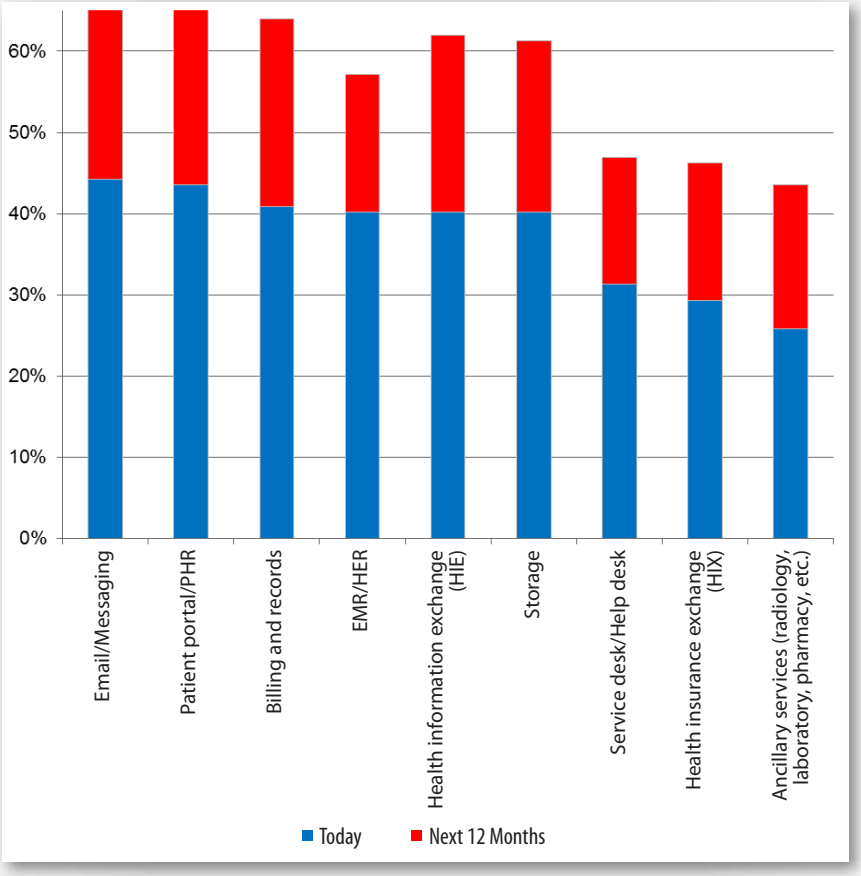


Figure 4. Cloud-based Assets That Access Sensitive Information

Mobile devices are also a source of additional risk, according to respondents. Not surprisingly, 92% of respondent organizations allow access to calendar and email via mobile devices. However, 52% also allow respondents to access health record information from their mobile devices, and nearly as many access data from cloud-based applications, through which they may be processing highly sensitive data, as discussed previously (see Figure 5).

What kind of data can be accessed by employee or consumer devices in your organization? *Select all that apply.*

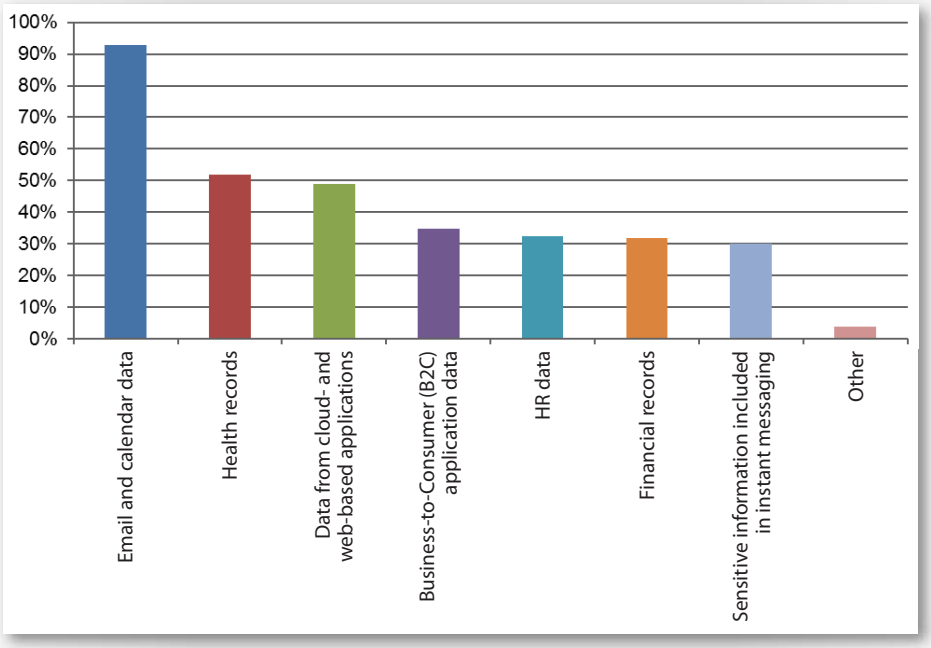


Figure 5. Data That Can Be Accessed by Mobile Devices

Although only 30% of respondents indicate that sensitive data is being included in instant messaging, texts and SMS messages passed between health care providers and patients are among the most vulnerable exposure points for personal identifiable information compromise. For example, insecure mobile apps or bad surfing habits can put such sensitive data at risk by introducing malware to the device that searches for health information.[11] As one respondent stated, "Employee mobile device management [MDM] is probably the best security policy we have as a business unit. However, sensitive info can and often is shared via email, which can be accessed anywhere with [the] Microsoft Exchange portal."

[11] www.mhealthnews.com/news/mobile-security-still-far-maturity

Tips to Protect and Secure Mobile Devices That Access Sensitive Information[12]

1. Be aware that most texting/SMS applications are not secure. Avoid providing delivery confirmation, and use an abbreviated format. Text only established patients from whom you have written consent, and limit the electronic personal health information you send via text.
2. Use a masked password/code/ PIN or other method to authenticate yourself to your device. Activate screen locking after a set period of time to prevent unauthorized access.
3. Enable encryption on the device.
4. Treat all mobile devices as uncontrolled endpoints. Install and activate remote wiping/disabling, and verify that it works.
5. Use file-sharing applications with caution, especially those that are cloud-based.
6. Install and enable a personal firewall, even on a smartphone!
7. Install/enable security software to protect against malicious applications, viruses, spyware and malware-based attacks. Update this software regularly!
8. Research a mobile app thoroughly and verify what services it will access before downloading it. Check the privacy notice on the download site.
9. Maintain physical control over the mobile device. Don't rely on services that will locate your device remotely.
10. Protect against the device unexpectedly sending or receiving health information over public Wi-Fi networks. Turn off automatic sensing of Wi-Fi or Bluetooth until you need a connection. Establish SSL VPN connectivity for users accessing corporate resources, and perform deep packet inspection at the gateway.
11. Delete all stored health information before discarding or reusing the mobile device.

This data is accessed from one common point that may or may not be managed under company policy. Devices can be hardened and applications managed, but the user still remains a vulnerability in how sensitive information is accessed and shared. Organizations need to invest in ongoing education and awareness to "secure the human" mobile workforce. Modern MDM and other device management programs are beginning to help reinforce these efforts with such capabilities as alerting a user when a possible policy violation is detected.

The security of applications needs to be thoroughly tested in the environment in which they will be used, taking into consideration how modification or configuration of the environment itself can help secure the application. Securing the smartphone can also help protect data accessed through the cloud. This will involve a combination of policies and controls working together, including:

- Device management
- Secure application design, development and testing
- Data protections
- Access controls
- Network monitoring and analytics

[12] List drawn both from best practices and www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

Navigating New Risks

Application and data-centric risks are of top concern to respondents, regardless of where those apps and data sets are housed and processed. When looking at their entire ecosystems (including their internal networks, cloud and mobile apps), 18% of respondents listed application, systems or network failure as their first concern (blue bar, Figure 6), and 16% were most concerned with application compromise.

What do you consider to be the top three risks/threats to your organization's information security?

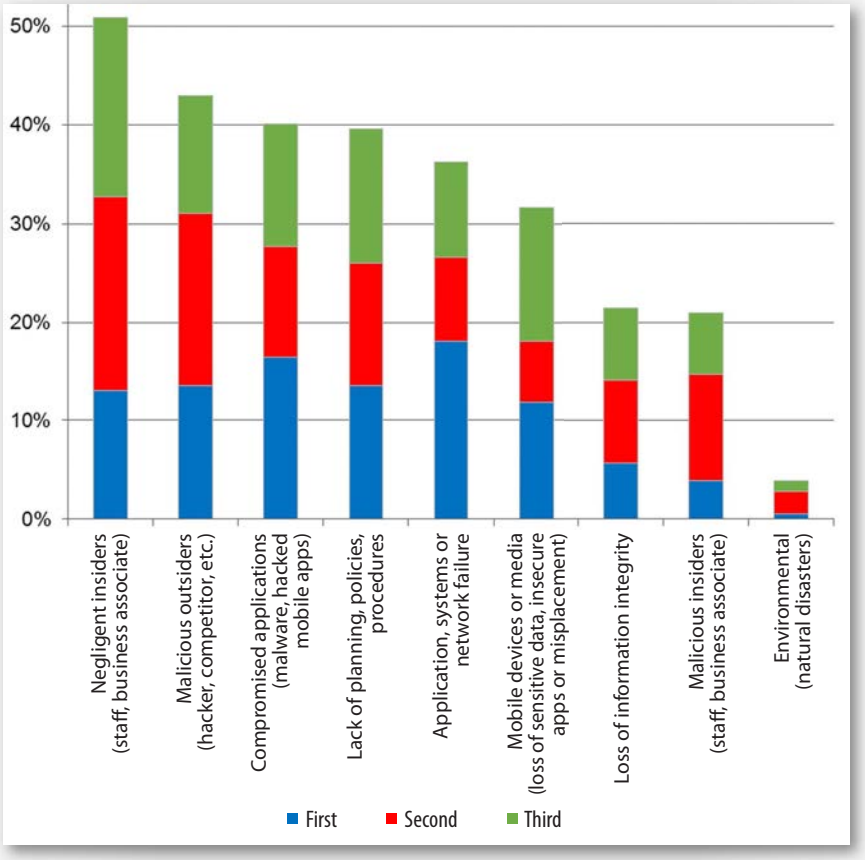


Figure 6. Top Concerns (Risks/Threats) to Organization Information Security

As in 2013, negligent insiders were ranked as the top risk in this year's survey by 51% of respondents. This is another indicator of the need for continued workforce awareness training. Key here is that negligent insiders have no malicious intent—their focus can be on providing care or getting work done, but having the work laptop stolen from the back seat of a car, dropping an unencrypted USB in the parking lot, downloading a malicious mobile app, inadvertently clicking on a malicious web link or being duped by a phishing email are common examples of negligence that result in a data breach. In fact, the unintentional exposure of private or sensitive information was 83% higher for health care organizations than for other industries overall, according to a co-sponsored report by PwC (PricewaterhouseCoopers), the CERT® Division of the Software Engineering Institute at Carnegie-Mellon University, *CSO* magazine, and the United States Secret Service.[13]

TAKEAWAY:

The integrated use of mobile devices with cloud-based computing—mobile cloud computing[15]—demands that health care policies and technical controls work together across platforms to secure sensitive data.

Overall, malicious outsiders moved up from sixth place in 2013 to the second biggest concern in 2014. This concern, held by 43% of respondents in 2014, is closely coupled with compromised applications (whether as a result of malware, hacked mobile access or other infrastructure vulnerabilities), which is the third overall concern in 2014, cited by 40%.

This survey also included a new option—lack of planning, processes and procedures—as a risk to sensitive data. A significant percentage (40% overall) of respondents see this as a true risk to their organization's sensitive data. Organizations should prioritize their resources on planning, policies and procedures that center around access to applications and data protection, particularly because these are their most critical and risky assets. A good resource related to administrative controls is the SANS Securing the Human site's health care training information.[14]

What is interesting is that, overall, only 4% of respondents are concerned about environmental factors. This lower level of concern could be the result of several factors: There have been no recent disasters on the scale of Hurricane Katrina that have taken out data centers; nor is this considered a security risk but rather an availability issue. Or, it could be that this concern over single point of failure during a disaster has been mitigated by the industry trend of moving toward the use of more distributed architectures.

[13] www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

[14] www.securingthehuman.org

[15] http://thoughtsoncloud.com/2013/06/mobile-cloud-computing

Universal Controls

Given the concerns around data and applications in ever-expanding environments, it's heartening to see that security is now more focused on protecting both critical health care applications and the sensitive information being accessed. For example, the use of encryption is growing to protect data at its source. Table 2 presents the ranking of controls based on their overall effectiveness and indicates the percentage of respondents who felt each control was not effective. The *Total Sum of Effectiveness* column represents the sum of the *Very Effective* and *Effective* columns.

Table 2. Ratings of Control Effectiveness

Security Controls	Very Effective	Effective	Total Sum of Effectiveness	Not Effective
Network/Perimeter defenses	25%	51%	76%	25%
Application security	10%	62%	72%	10%
Database security	16%	55%	71%	16%
Endpoint protection (centrally managed)	19%	51%	69%	19%
Administrative (policies and procedures)	10%	58%	68%	10%
Data protection/Encryption	20%	47%	67%	20%
Contractual relationships with business associates	14%	50%	64%	14%
Vulnerability management	7%	53%	61%	7%
Security risk management framework	11%	48%	59%	11%
Identity and access management (IAM) controls	12%	44%	56%	12%
Training and awareness	10%	43%	53%	10%
Mobile security and access controls	8%	41%	49%	8%
Data breach detection solutions	4%	43%	48%	4%
Big data initiatives and data governance	3%	43%	47%	3%
Malware analysis systems/Honeypots	10%	37%	46%	10%

Similar to the SANS 2013 health care security survey, in this survey, network and perimeter defenses (including firewall and IDS/IPS) ranked the highest, with 76% of respondents rating these controls as effective or very effective. Application and database security, indicated as effective or very effective by 72% and 71%, respectively, were much more highly rated in 2014 than in 2013. Application security, rated by 61% in 2013 as effective or very effective, moved from a tenth place rating to second place in terms of effectiveness. Database security, rated by 68% in 2013 as effective or very effective, moved from eleventh to third place. These are both areas where critical improvements must continue, especially as health care further embraces big data[16] and the growth of health care analytics.

[16] www.computerweekly.com/podcast/Big-data-storage-Defining-big-data-and-the-type-of-storage-it-needs

TAKEAWAY:
Implement awareness and training programs that make users aware of risks. Ignorance can lead to negligence, which can lead to exploitation.

In big data environments, patient information is used for multiple purposes in a wide variety of applications. The ability to protect personal health information as it is pulled from the data repository to be utilized in the applications is critically important. Yet, identity and access controls slipped from the third most effective ranking in 2013 to the tenth most effective in 2014. In 2014, 56% ranked this control as effective or very effective, compared to 76% of respondents in 2013. Given the mobility of their applications and consumer data, this may indicate a slippage in controls working across these new applications and provides a strong call for federated identity networks.

Other tools, such as data breach detection solutions (BDS), are relatively new technologies that improve upon existing security defenses to detect advanced persistent threats (APTs). Similar to perimeter defenses, such as next-generation IPS or firewall, BDS can use signatures and heuristics for identifying malware. BDS can also "analyze the patterns of network traffic, identify malicious domains, and model the behavior/impact of files that are being downloaded and executed on an attack surface."[17] As a relative newcomer to the list of security controls in use, the 48% effectiveness rating of these technologies signals that BDS are adding value for enterprises that adopt and implement BDS protocols.

TAKEAWAY:
Don't depend solely on a network perimeter defense strategy to help in timely breach detection—especially if you have a "mobile first" or "cloud first" approach.

Access controls and data protections are critical to support secure data access through cloud/mobile migration, so it's good to see emphasis given there. However, because insider risk remains a major concern, it's a shame to see training and awareness scoring so high on the "not effective" list.

These positive and negative rankings for effectiveness speak to an overabundance of faith being placed in perimeter defenses, which are not detecting the actual breaches of data in a timely manner. Organizations need security controls that are more attuned to the expected behavior of the application or data for more timely detection of an incident/potential breach.

[17] www.techrepublic.com/blog/it-security/breach-detection-systems-take-aim-at-targeted-persistent-attacks

Cloud Controls

As with mobile computing, cloud computing provides another scenario where security controls need to be put as close to the data and their applications as possible. When it comes to cloud technologies, 73% are most concerned about data leakage, 69% are concerned about loss of control over their protected data, and 52% about legal issues/ disclosure, an option introduced in this year's survey, as shown in Figure 7.

What are your organization's greatest security concerns about using cloud solutions? ***Select all that apply.***

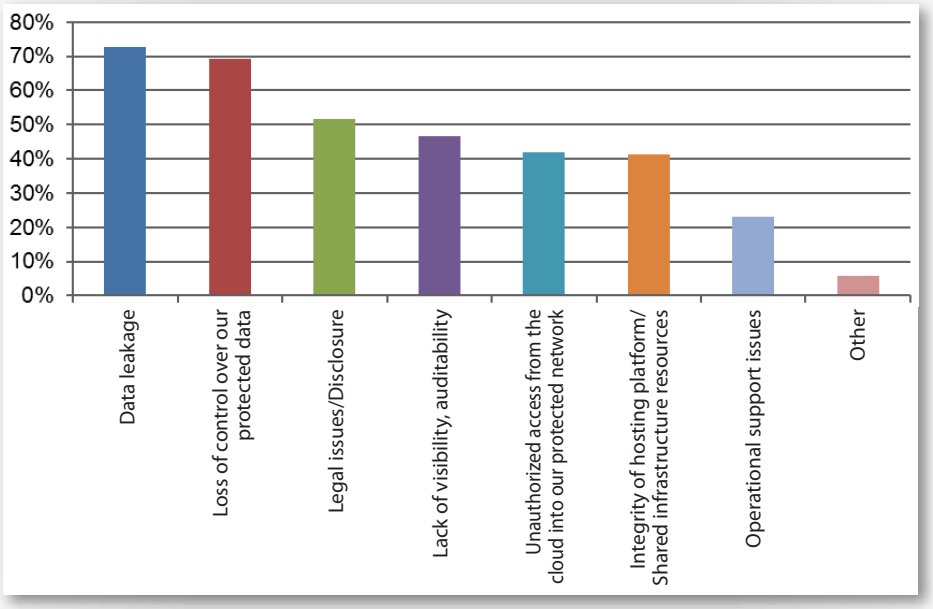


Figure 7. Top Concerns About Cloud Computing

The top two concerns about cloud computing reported in 2014 are consistent with those expressed in 2013. Concerns over data leakage and loss of control over data are similar year over year, whereas concerns related to more operational issues (represented by the bottom four concerns) seem to be significantly reduced in 2014. This indicates increased adoption of cloud applications and the maturation of these applications and their security offerings. See Table 3.

Table 3. Leading Concerns Over Cloud Computing

Concern	% 2013	% 2014	% Change
Data leakage	74.5%	72.8%	-1.7%
Loss of control over data	66.0%	69.2%	+3.2%
Legal issues	NR	51.5%	—
Lack of visibility/availability	59.6%	46.7%	-12.9%
Unauthorized access	46.8%	42.0%	-4.8%
Integrity of host platform	55.3%	41.4%	-13.9%
Operational support	31.2%	23.1%	-8.1%

Currently, respondents indicate that the most effective controls are those that provide control over access to cloud applications (60%) and data segregation and usage monitoring (also 60%), as shown in Figure 8.

What security controls do you feel can best address cloud security concerns?
Select all that apply.

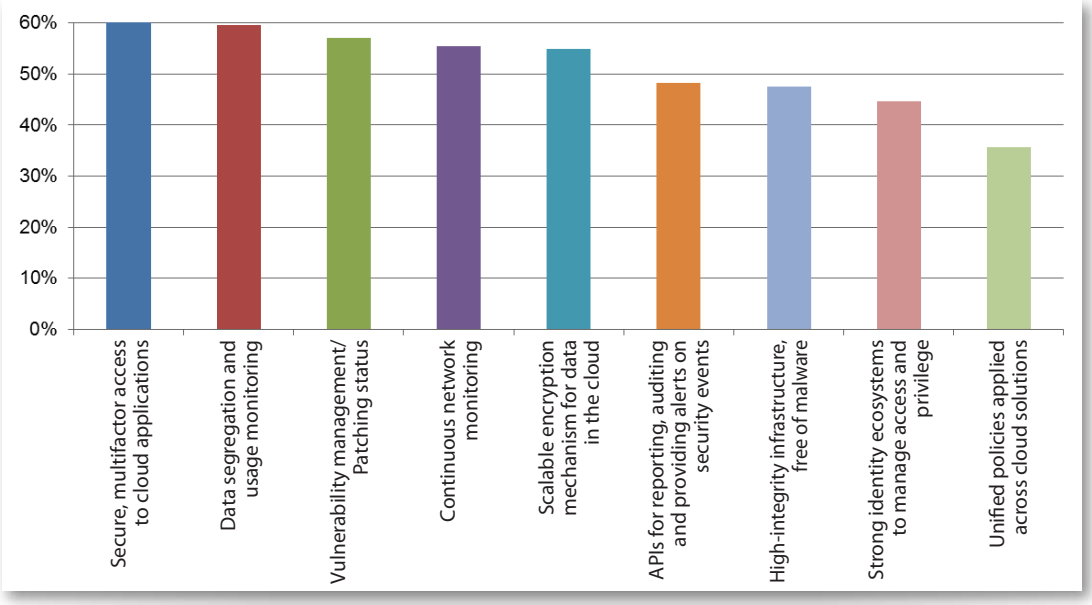


Figure 8. Security Controls That Can Best Address Cloud Security Concerns

This emphasis indicates that the cloud-computing industry has matured. Respondents are now looking toward secure access and data-centric controls and are less concerned with operational considerations such as monitoring of cloud applications for vulnerabilities and threats.

Cloud computing may be an area where secure, multifactor authentication, which combines two or more independent credentials—such as what the user knows (password), what the user has (security token) and what the user is (biometric verification)—also takes off. This year, 60% of respondents said they are using multifactor authentication as their top control to address the risk to data and applications in the cloud. This represents a shift from 2013, where APIs for data reporting, auditing and providing alerts were cited by respondents as the top security control for addressing cloud security concerns.

TAKEAWAY:

Begin to adopt a data-centric security approach that focuses on protecting sensitive data, rather than just protecting the network or application in which the data lives.

Cloud computing is also driving a more data-centric method of security, which focuses on protecting data rather than just protecting the network or application in which the data lives. Starting a data-centric security plan involves learning and understanding where sensitive data resides, as well as how that information will be used, accessed, managed, retained or retired across its life cycle. The next step is to assess the risks and determine the policies and resources needed and available to monitor and control risk in cloud-based computing models. For example, storing data in the cloud demands encryption for the data at rest. Is that provided through the internal application or the cloud services provider? Sharing that same data among individuals with different roles and levels of access might demand further modification of data to protect it, such as redaction, masking or a combination of both.

Mobile Controls

Concerns over mobile security involving employee usage and protection of mobile endpoints have remained relatively consistent from 2013. The top three concerns are the same, although their order has shifted slightly, perhaps as a result of improved tracking and the ability to deactivate lost or stolen devices, as shown in Table 4.

Table 4. Mobile Security Concerns

Concern	% 2013	% 2014	% Change
Lack of awareness about security policies	73.2%	73.9%	+0.7
Insecure/unprotected endpoints	72.5%	73.3%	+0.8%
Lost or stolen devices	82.6%	70.3%	-12.3%
Corrupt, hacked or malicious apps	66.7%	58.2%	-8.5%
Insecure wireless use	47.8%	49.7%	+1.9%
Insecure web browsing	46.4%	38.2%	-8.2%

In line with these concerns, 79% of respondents identified awareness education and training as the leading control to address mobile/BYOD security concerns. Data encryption on the device was identified by 75% and mobile device management by 62%. However, technologies such as sandboxing (53%) and full disk encryption (50%) that can protect the actual information on the mobile device were not considered as effective. These technologies likely indicate the difficulties in managing information on devices that are not owned by employers and that still need to be worked out.

Evidence of Improvement

Another good indicator of progress is that respondents appear to have gotten down to the real work of identifying and managing risk across platforms and environments and are now witnessing improvements in their ability to counter threats. In this year's survey, twice as many respondents as last year (24% compared to 12%) feel their ability to counter security threats is adequate, 11% (as opposed to 15% in 2013) feel their programs need complete rework. On the other hand, only 6% believe their programs are excellent, as shown in Figure 9.

How would you rate your organization's ability to counter security threats in your environment, whether the threats are internal or external to your organization? ***Select the best answer.***

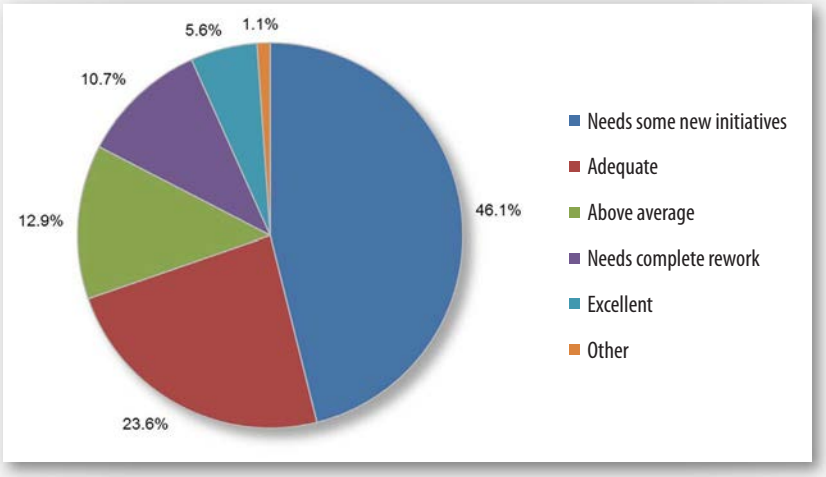


Figure 9. Effectiveness of Organization to Counter Security Threats

These results indicate that more attention is now being paid to information security, particularly detection and mitigation in light of industry concerns over cyberthreats targeted at health care electronic records, as well as new vulnerabilities with mobile and cloud computing.

Integration Roadmaps

Comparing 2013 results with this year's results reveals a decrease in the number of organizations involving security in project inception or ideation. However, there is a corresponding rise in those incorporating security in the formal elements of a project from the time it is initially funded (formalization) through quality assurance and implementation. The takeaway here is that fewer are waiting until implementation to consider the security of their projects; and fewer respondents are inserting security at the last minute, or on an "as needed" basis.

TAKEAWAY:

Build security into all stages of the development life cycle. Security "bolted on" afterward almost always leads to quality problems with a system or application from various standpoints, including information integrity, performance and usability!

Table 6 compares times at which security is involved in the project life cycle.

Table 5. Involvement of Security in Project Life Cycle

Development or Integration Project Life-Cycle Stage	% 2013	% 2014	% Change
Inception: First occurrence of the project idea	20.5%	15.6%	-4.9%
Ideation: Project idea is worked within the group (no stakeholder engagement)	10.3%	8.9%	-1.4%
Formalization: Stakeholders are formally engaged when project is initially funded	17.1%	19.6%	2.5%
Refinement: Stakeholder feedback incorporated as part of detailed requirements	4.8%	5.6%	0.8%
Development: Coding or product acquisition	6.2%	9.5%	3.3%
Quality Assurance: Internal testing prior to implementation in production	3.4%	4.5%	1.1%
Implementation: Full production implementation/go-live in the market	4.8%	6.1%	1.3%
As needed	26.0%	19.0%	-7.0%

The results indicate important changes have been made in the integration of security resources into the life cycle of information projects. Security needs to be formally introduced into all stages of the development or integration life cycle and applied consistently throughout. System designers, architects and developers often concentrate on developing a "good" automated solution to meet the business need, but if security is ignored until the end, the defense of the system can be easily compromised.

Comparing trends from 2013 with 2014 reveals growing investments in security and increased or stabilized budgets. Although budgets of 1–3% are the expected slice of the security budget for most verticals, 13% of 2014 respondents are receiving 4–6% of the overall IT budget for security.

Overall, however, there is a slight decline in the 4–6% group between 2013 and 2014, but that is expected to be made up if more than 10% increase their security spending to 4–6% over the next couple years as planned. See Figure 10.

Percentage of IT Budget Devoted to Security

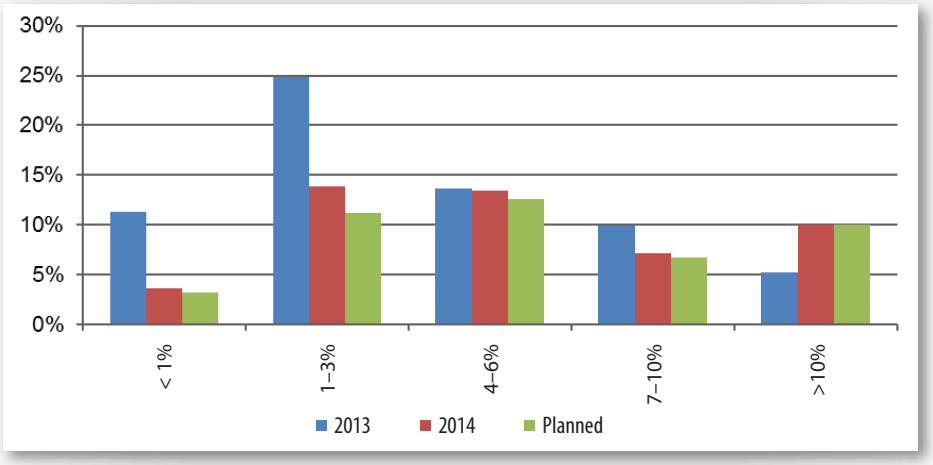


Figure 10. Budget Devoted to Security

Not shown in this figure is that a full 47% of respondents report being unsure of the percentage of the total IT budget devoted to security. This level of ignorance is troublesome, especially because this number was only 35% in 2013. However, this lack of knowledge about budgets is consistent with the changes in survey demographics between the two years. Very often security staff members, including mid-level managers, are not aware of the financial constraints on their activities.

Size Impacts Budget

Correlating budgets against the size of the workforce reveals that the medium-sized groups (organizations with 101–1,000 employees) and enterprise organizations (those with more than 25,000 employees) are most frequently allocating more than 3% of their budgets to security, as shown in Figure 11.

Percent IT Budget by Workforce Size

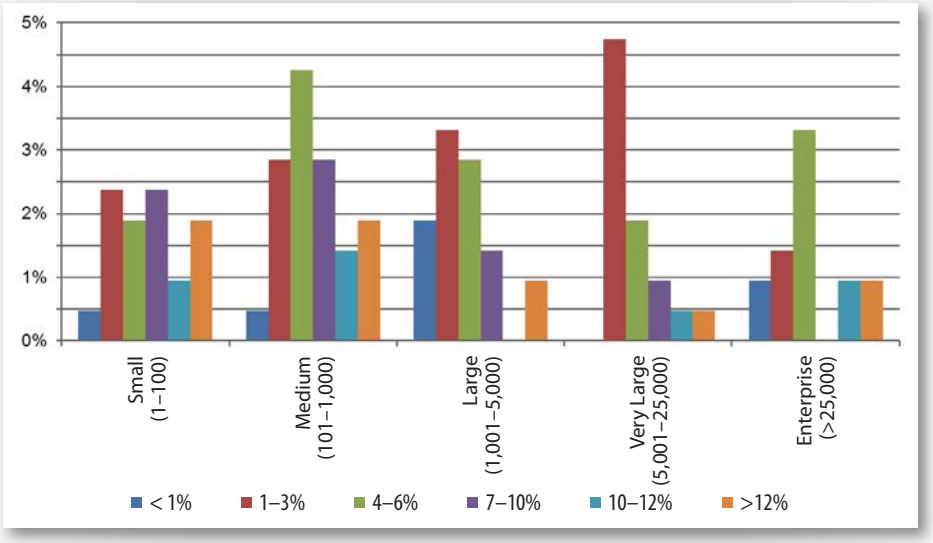


Figure 11. Security Budget Relative to Size of Organization

Compared to the 2013 budget versus size analysis, the data also shows a trend toward increased security budgets for smaller organizations with workforces of fewer than 100 as well as mid-size organizations with 100 to 1,000 workforce members. This is a change from 2013, where assets and resources were definitely lacking in the smaller organizations. Medium-sized organizations in 2014 have increased their budgets from the 1–3% range into the 4–6% range. However, the 1–3% range still appears to be the norm for organizations with workforces from 5,000 to 25,000 employees.[18]

Physician practices, typically having fewer than 100 full-time physicians, may have improved the percentage of their IT budget devoted to security based on acknowledgment of security risk and vulnerabilities (and the corresponding effect of an incident or breach on the cost of care and/or reputation).

[18] www.sans.org/reading-room/whitepapers/analyst/inaugural-health-care-survey-34855

Industry consolidation may also have an effect here. According to *Modern Healthcare*'s annual survey of hospital systems, 2013 witnessed the nation's biggest for-profit and not-for-profit health care systems creating giant health care networks that rival Fortune 500 companies.[19] The creation of larger organizations that can leverage greater resources may be a key factor in improved security spending (and cost containment for an incident or breach).

For organizations that are not realizing an effective budget for security, IT security management should present a business proposal outlining the risks and corresponding costs/benefits of a proactive approach to security to the appropriate decision makers. An individual provider practice may want to approach the regional extension center or medical association for further justification of security expenses.

TAKEAWAY:

To enhance the security budget, provide appropriate decision makers with a business proposal outlining the risks and corresponding costs/benefits of a proactive approach to security.

Looking Forward: Advice and Resources

Based on this survey's results, the health care industry is slowly improving, with better awareness of risk and improved commitment of resources and support.

Here is some actionable advice that can keep the momentum of positive change going:

- **Assess your information ecosystem.** Take into account data classification and the locations and conditions under which it is accessed and used. Who's accessing what systems for what purposes from what locations? When and how are these systems being accessed? These are critical assessment questions to ask when determining risk and compliance posture.
  - Conduct a vulnerability assessment to understand the dependencies and gaps in your information security infrastructure.
  - Once this assessment is completed, a whitelist of approved applications and users can be created. Unknown users and applications can be scrutinized and possibly blocked based on rules.
  - Assessment should also lead to and integrate with vulnerability management systems and workflow programs to monitor the approved systems and applications for vulnerabilities, such as default user passwords and outdated or unpatched programs, and ensure they are patched.
  - Automate assessment for continuous monitoring of systems, applications and networks, per the Critical Security Controls.[20]

[19] www.modernhealthcare.com/article/20140621/MAGAZINE/306219980/consolidation-creating-giant-hospital-systems?utm_source=frontpage&utm_medium=newsitem309&utm_campaign=carousel-traffic

[20] www.counciloncybersecurity.org/critical-controls

- **Establish data-centric security controls.** Understand that an attacker will use all abilities at his or her disposal—targeted threats, malware, password breaking, spearphishing and other such tactics to access data. Focusing on the information, not just the infrastructure, allows an adaptable approach to risk management that expands naturally to mobile endpoints and the cloud. Endpoints include virtual users, smartphones, tablets and external consultants. Data breach monitoring, data loss prevention (DLP), and encryption are some of the controls that can be put close to the data.
- **Manage identities.** Data controls should be tied closely with identity and access management. Bring your own device practices allow identities to be both enterprise and individual. Collectively across these identities, information is pushed and pulled to devices internally and externally, increasing the risk of exposure and potential data theft. Consider the cloud, and you have just added another level of complexity. This provides an excellent opportunity for identity ecosystems, such as federated identities combined with reputational services, to have a chance of taking off. Access controls should be multifactored, and access monitoring should detect anomalies in policy and respond accordingly.
- **Invest in incident response.** Document a formal response process, maintain an incident response team and establish relationships with outside experts, if necessary, before an incident occurs.
  - Interact with the National Health Information Sharing and Analysis Center (NH-ISAC) to gain advance and timely knowledge about emerging threats to improve your incident response time.[21]
  - Know how regulations such as HIPAA influence the time frame for reaching certain incident response milestones.
  - Increase visibility with better analytics and intelligence to enable determination of whether a threat applies to a specific environment and where to take action.
  - Measure your response readiness and invest in building a holistic security program that includes response findings (undisclosed vulnerabilities, etc.) for continued improvement.
- **Formalize security around an actionable and agile risk framework.** Use frameworks such as the Critical Security Controls[22] and the NIST Framework for Improving Critical Infrastructure Cybersecurity[23] as more than a checklist to achieve compliance. Use them to prioritize actionable items that can start automating risk management and improving overall risk posture.

[21] www.nhisac.org

[22] www.counciloncybersecurity.org/critical-controls

[23] www.nist.gov/cyberframework/index.cfm

Conclusion: More Work Ahead

This past year (2014) brought heightened recognition that health care information and health care identity are worth money—and that the bad guys can and will launch cyber attacks against vulnerable health care networks. According to an article in *United States Cybersecurity Magazine*, the health care industry has seen more targets being discussed in 2014 than any other year (see Figure 12).[24]

Cybercrime Targets by Industry (January 1 – May 15, 2014)

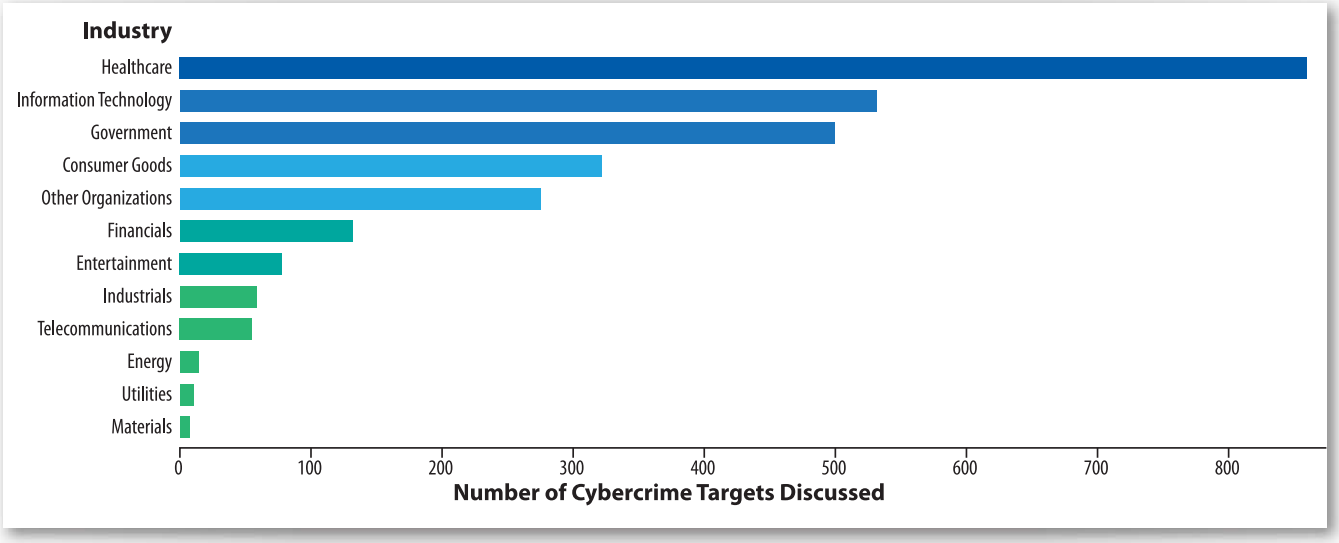


Figure 12. Attack Targets by Industry [25]

Trends such as mobile and cloud computing are game changers for the way individuals and organizations must approach the security of their systems, the privacy of protected sensitive data, and compliance. Health care organizations must complement traditional, infrastructure-driven controls such as network perimeter security with protections for the newer and evolving threat vectors where their data and applications are outside of the protected network. Providers, payment plans, insurers and other related industries now allow patients unprecedented access to helpful, sophisticated health information and digital tools. Patients have online access to their doctors, and immense social support is also provided online.

The fact is that the attack surfaces are many, and the movement to detect, protect and defend in the health care industry, as shown by the small improvements in this survey, is still not enough to keep up the pace. Investment in understanding the new threat landscape and designing solutions to protect against these attacks, including leveraging newer tools for protecting data and responding to new forms of attacks, become critical to staying ahead of attackers.

[24] "Healthcare is a Growing Target for Cybercrime, and It's Only Going to Get Worse," *United States Cybersecurity Magazine*, Summer 2014, 1(4), p. 56. www.uscybersecurity.net/Pages/online_magazine.html

[25] "Healthcare is a Growing Target for Cybercrime, and It's Only Going to Get Worse," *United States Cybersecurity Magazine*, Summer 2014, 1(4), p. 56. www.uscybersecurity.net/Pages/online_magazine.html

About the Author

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 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 (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system development life cycle, 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 ISC^2 CISSP, SANS GSEC (Gold) and GCIH (Gold), and the GHSC certifications.

Sponsor

SANS would like to thank this survey's sponsor:

QUALYS®
CONTINUOUS SECURITY