IBM Security

Thought Leadership White Paper

Healthcare

Securing the healthcare enterprise

Taking action to strengthen cybersecurity in the healthcare industry

Contents

Executive summary

With disastrous data breaches making headlines far too often, healthcare executives need to re-think the dangers of today's digital environment. What are the best ways to protect the business in the face of fast-evolving threats?

Keeping one step ahead of attackers will require a combination of measures, including robust system defenses, analytics to spot intruders fast and the ability to react quickly whenever an intrusion occurs. Over 75 percent of all security incidents target a handful of industries—the healthcare industry is now ranked in the top five with finance and insurance, manufacturing, telecommunications and retail, while at the same time the value of medical identities are becoming much more lucrative on the black market.[1] Chances are that your perimeter has already been breached, with cybercriminals just waiting for the right opportunity to attack. The perpetrators of such attacks are becoming more and more sophisticated, and the scale and destructiveness of their intrusions is growing dramatically. In the face of such a dangerous landscape, healthcare organizations are now taking additional steps to address the issue of security: implementing stronger defenses, rethinking process controls and working with law enforcement to investigate intrusion attempts. But are these efforts enough? What are the best ways to safeguard against digital security failures? How can management be confident that the choices it is making in this regard are as effective—and cost efficient—as they can be?

At IBM, we're convinced that the healthcare industry should address the challenge of digital security in a long-term, strategic way, using a multilayered approach:

- Anticipate security threats that are likely to manifest in the future, and put in place in-depth defenses to reduce the likelihood of a successful attack.
- Use advanced, automated detection mechanisms to identify patterns and catch incipient intrusions before they get to your network.
- Establish a culture of informed vigilance with regard to security, and be prepared to react swiftly and effectively to arrest attacks.

In this white paper, we describe the long-term nature of the digital security challenge, the array of defenses and practices that are likely to be most effective in protecting an enterprise from attack and how healthcare organizations should approach this area of concern within the context of the many other business priorities that vie for executive attention.

A fast-moving target: the evolving nature of digital security threats

The realm of digital security is, by nature, something of an open-ended arms race between system and data defenses on the one hand and creative, highly persistent attackers on the other. There will likely never be any point at which one side “wins” conclusively—each successful defense strategy or attack plan simply changes the game to a degree and raises the standards for the next round of attack-and-defend.

And let’s be clear: *security* is not the same as *compliance*. Simply striving for compliance with privacy regulations such as the Health Insurance Portability and Accountability Act of 1994 (HIPAA) doesn’t remotely assure that an enterprise is, in fact, well defended against attack.

It’s a safe assumption that, at any given moment, numerous intrusion attempts are underway against healthcare organizations as you read this paper. For criminals, healthcare can be quite a low-risk and high-profit target. Many of these intruders are located in countries and jurisdictions that have minimal law enforcement with regard to cybercrime, making attackers largely immune to arrest and punishment. And in the case of one of the most commonly sought targets for theft—medical identities—there is a growing global black market where such data is bought and sold on hundreds of websites, allowing successful perpetrators to profit instantly from their attacks. From medical records, to insurance and credit card information, pharmaceutical data, high-profile records and medical research data, the healthcare industry represents a bounty for criminals.

Digital complexity and pervasive connectivity opens many new avenues of attack

The healthcare industry’s inherent exposure to security risk is increasing steadily for many reasons. It has been slow to digitize relative to some other industries. As a result, medical facilities may not be as knowledgeable about security as they should be. At the same time, cybercrimes have become more sophisticated. This combination sets up healthcare organizations to be ideal targets. Since 2010, criminal attacks on healthcare organizations have more than doubled.[2] More sophisticated criminals are not the primary concern among these organizations; however; employee negligence topped the list as the biggest worry, followed by public cloud adoption and “bring your own device” (BYOD).

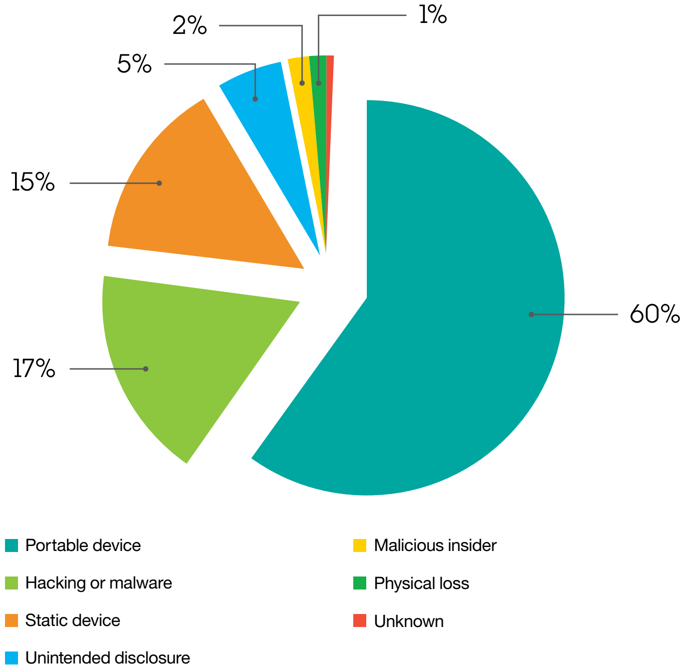
Most obvious is the vastly increased pervasiveness of network connectivity, as more and more sensitive information is held on networked and distributed systems that are accessible to a widening array of entry points. The broad adoption of mobile and social applications adds many other new points of vulnerability. Enterprise applications and data must, in some cases, be made accessible to employee-owned mobile devices. This problem is pervasive throughout healthcare organizations. Even credit card systems used to process copayments and other financial transactions within medical facilities often lack adequate encryption. One study also found that unauthenticated and unencrypted communication among medical devices not only left them vulnerable to hacking, but also provided direct access to digital medical records. The same study noted that vendors frequently don’t do enough to secure these devices before providing them to hospitals.[3]

In short, everything is becoming more connected, and the Internet is becoming ever more vital to the functioning of global society and the global economy. With this comes untold benefits and efficiencies, but also some insidious risks and dangers. The recent *Heartbleed* incident has drawn attention to our heavy reliance on—and the vulnerability of—some of the basic building blocks of the Internet. *Heartbleed* worked by compromising OpenSSL, which is used to secure sensitive pages and transactions by over half of the world's websites across all industries, including healthcare.

The nature of today's cyber attackers

The leading source of data leaks is simple negligence. Electronic medical records (EMRs) stored on portable storage devices such as hard drives and universal serial bus thumb drives has led to nearly 23 million data records lost or stolen(Figure 1). This data is rarely encrypted, which is a step that any institution should be taking before storing or transferring data onto a portable device.[4] The human-related factors of employee negligence or unintentional mistakes that expose information, such as the disclosure of information on websites or lost or misplaced files or devices is of greatest concern, as reported by the recent Healthcare Information and Management Systems Society Annual Security Survey, followed by the concern that workforce members would bypass security access controls or interfere with access controls.[5]

As shown in Figure 1, over 38 million medical records have been leaked, lost or stolen. While this may seem like an incredibly high number, it pales in comparison against industries such as financial or retail, whose counts run over 200 million. What does that say for the healthcare industry? Medical records have recently become a hot commodity, and stealing them a lucrative business with more large-scale breeches expected in the near future, with more extremely sensitive personally identifiable information (PII) data traded and sold.



Method of data loss	Records lost
Portable device	22,916,465
Hacking or malware	6,624,447
Static device	5,534,794
Unintended disclosure	2,002,091
Malicious insider	600,385
Physical loss	473,119
Unknown	164,900
Grand total	**38,316,201**

Figure 1. Leading source of data leaks in healthcare institutions[7]

And of growing concern is that many of these groups and individuals attacking externally are located in jurisdictions where they may be virtually immune to prosecution or punishment. The recent attack by Chinese hackers on a Tennessee-based health system stole 4.5 million records illustrates this threat.[6] Many intrusion attempts are executed by attackers who operate opportunistically to exploit "doors left unlocked." These are still remarkably common and can make life easy for criminals: They include basic security lapses caused by lack of discipline and poor adherence to process controls, as well as system misconfigurations that can remain unrecognized and uncorrected for an extended time.

A smaller but still substantial number of intrusion attempts are the result of sustained, concentrated efforts to gain knowledge of a company's systems and controls, so that the perpetrators can employ an informed approach—using malware or another method—to thwart these controls. Their objective may be to gain access, steal data or sometimes go even further, such as taking clandestine control of specific systems.

First things first: addressing the most common vulnerabilities

First take a look at the most common failure points that let intruders gain easy entry. Attackers prefer to hit wherever security is weakest and where it will take the least effort to steal something valuable.

According to the IBM Cyber Security Intelligence Index, these are the five most-common vulnerabilities that attackers exploit. A healthcare organization that takes steps to address these weak spots will close the door on a wide range of intrusions that would otherwise likely be successful:

- **End user didn't think before clicking to open an email or website:** This is still painfully common, and needs to be addressed primarily by effective process controls and an informed culture of vigilance.
- **Weak or default passwords in use:** Again, processes and internal controls are central here, and can be reinforced by advanced system security to consistently enforce password standards.
- **Insecure configurations:** Attackers are always probing to discover misconfigurations that have inadvertently created open-ended security holes. This issue must be addressed through a combination of greater vigilance in process controls and improved testing during the process of system configuration, as well as by the use of analytics to detect and report irregular activity that could indicate an intrusion that is taking advantage of a system misconfiguration.
- **Use of legacy or unpatched hardware or software:** Attackers are always probing to find lapses of this kind. This issue has to be addressed in a similar manner, through improved process controls and through analytics to detect irregular activity.
- **Lack of basic network security protection and segmentation:** Too often, existing controls and defined safe practices are simply ignored or disregarded, as security takes a back seat to other priorities. Healthcare organizations need to institutionalize critical practices around network protection and data-access security, and take proactive steps to monitor and ensure adherence.

Beyond the basics: crafting an in-depth healthcare security strategy

Given the ongoing evolution of the tactics used in intrusion attempts, it's important for healthcare organizations to keep in mind not just the methods that have been used in the recent past, but also the patterns that suggest the shape that defenses will need to take in the future.

IBM's recommended enterprise security strategy relies on three key elements. Each must be robustly implemented to establish effective defenses in depth:

- Deploy an *advanced system security* to provide defense at every network access point, with intelligent security fences to impede breaches and isolate threats, supplemented by defenses to help protect each type of sensitive data.
- *Use advanced analytics as a weapon* to continuously scan for and detect patterns that may indicate an intrusion, so these can be brought to management's attention and contained before they do serious harm.
- Establish *effective process controls and rapid response mechanisms* to enforce good habits regarding digital security, to establish a culture of informed vigilance and to enable quicker action when a breach does occur.

These three layers of protection can be consistently effective in frustrating intruders and mitigating attacks. When employed in a thorough and consistent manner, they can help address future security issues through early detection, removal and remedy.

Advanced system security: defending at every network access point

Barriers at access points are designed to keep intruders off the network. These are the first line of defense against external attack.

We choose to use the term *network access point defense* here, rather than *perimeter defense*, because "perimeter" may suggest a single boundary line that one might intuitively equate with the boundaries of the enterprise. But in today's interconnected environment, a provider or payer's secured network can extend far beyond this to include elements that are the responsibility of suppliers, contractors, business partners, employees and others.

For this reason, in order to more effectively secure the network, attention must be paid to each of these access points and each must be secured by an appropriate defense. Accounting for every network access point is becoming more challenging as the shape and interconnectedness of the digital world gets more complex. To cite an example of a relatively recent development that can have an impact here: connected applications may extend to mobile platforms, hybrid clouds and into arenas like Infrastructure as a Service (IaaS) and virtual data centers. When combined with the emerging "Internet of Things"—the widening range of network-connected devices—this represents more avenues for intrusion and attack. Since connected apps are frequently updated and repaired via automatic patches that might contain a virus or other malware, this represents another source of danger.

Attackers who find their way onto any given component on a network can conceivably find a way to get to seemingly unrelated components—even the "crown jewels" of the enterprise. Consider an example from the retail industry: the 2013 breach at Target, which highlights how important it is to secure every access point—even those outside the enterprise itself. In this incident, the attackers were apparently able to use the stolen credentials of one of Target's heating and air-conditioning contractors to work their way onto the retailer's store network, eventually succeeding in stealing a huge quantity of customer credit card data from their point-of-sale systems.[8] News accounts indicate that the initial intrusion happened several months before the mass theft of data was executed.

The bottom line here is that organizations need to take careful inventory of all their network access points and assess the risk posed by each. Then the appropriate defenses and controls must be implemented and enforced. At the same time, a process must be put in place to review this inventory of access points on a regular basis in order to identify changes and additions.

The widening array of network access points

The range of access points healthcare organizations must identify and secure continues to grow. At a minimum, these may include:

- Electronic medical records systems and billing and payment systems
- External-facing healthcare websites
- Links with health information exchanges and health insurance exchanges
- Links with each third-party vendor, supply-chain vendor, ecosystem partner and contractor
- Employee-facing access points—including BYOD mobile devices—and the social workplace
- Links to connected data centers via the cloud
- Links to insurance companies, financial institutions and payment processors
- Links to managed service providers
- Links to other healthcare, governmental and public health systems
- Links to all other contractors who are provided with network access
- Business-to-business (B2B), intranet and extranet portals
- Wireless routers, patient kiosks and networks
- The expanding "Internet of Things": medical devices, remote monitoring, IP-based printers, IP-linked surveillance cameras, and so on

Data security: protecting valuables inside the enterprise

If effectively implemented and maintained, network access point defenses can keep most intruders from penetrating a provider or payer's systems. But there will be intrusion attempts that make their way past these defenses. The second line of access defense, therefore, is specific protection for each form of sensitive data.

Healthcare organizations today have more data than ever that they must share throughout the healthcare supply chain to support the delivery of efficient and proper care to patients. However, the fluid networks operated by these organizations, along with the number of endpoints, greatly increase their security challenges. Even medical devices, such as heart monitors and lab equipment, collect and store sensitive personal information and can provide an avenue for hackers to access other databases in a healthcare organization's system. Despite these threats, the healthcare industry has been slow to use encryption for its internal operations, in large part because it is often considered a hindrance to productivity.

Healthcare organizations need a process to identify every kind of data that needs protection, and then every instance of such data that must be secured. These protections might take the form of access and port restrictions, strengthened encryption methods, tokenized data vaults, selective network segregation, identity management and other barriers. The goal must be to maintain the access that is required to conduct business smoothly, while frustrating unauthorized or suspicious access attempts.

Using analytics as a weapon: detecting and blocking intruders before they get to your network

Access-point and data-specific safeguards notwithstanding, every healthcare organization should expect that at least a few intruders will make it past both these barriers. For that reason, analytics must be in place to watch for patterns that could indicate an intruder in the system and to issue alerts so counter-actions can be taken quickly.

Analytics therefore represents the proactive counterpart to defensive access-point barriers. While many intrusion attempts will be defeated, the prudent approach is to assume that barrier walls can never be high enough. The questions then becomes, “How quickly can we identify and counter each successful entry?” and “Will we be able spot intruders immediately, before harm is done, or only much later, after a disastrous disruption or loss of data?”

Security analytics tools work by scanning to identify anomalous behavior within your network: patterns that might indicate that something suspicious is taking place. Monitoring infrastructure logs, security logs, database logs, network data packets, domain name system (DNS) transactions, configuration changes and even social chatter, these tools look for unusual activity, with specific attention paid to actions that touch upon sensitive data. Advanced analytics tools even go a step further and watch for patterns as they may manifest across signals from different sources and different kinds of activity.

When they identify an action or pattern that appears out of place, security analytics tools can alert managers, who can then take a closer look to determine whether further investigation is warranted. The best and most advanced of these tools are designed to “learn” from the evolution of network activity, so as to dynamically refine the criteria around what may constitute unusual behavior. They are also regularly updated to watch for new intrusion tactics.

An effective and well-deployed security analytics tool can identify genuinely suspicious patterns of activity while avoiding an excessive number of false alerts. It will also present to security managers the relevant information on the nature of activities in a concise and accessible way. Both of these characteristics are critical to timely and appropriate counteraction.

Effective process controls: establishing a culture of security, and reacting rapidly

Once network access defenses and analytic defenses are in place, the goal becomes to keep system security up to date and as advanced as possible while maintaining and strengthening process controls. Security must also include the human element: the need to foster a culture of informed vigilance is a “softer” and more elusive part of an effective security posture, but nonetheless a vital component.

Looking back at the most common vulnerabilities discussed earlier, it bears mention that the top two of these indicate a deficient culture of vigilance: end users not thinking before clicking on an email or attachment, and the use of weak or default passwords. Some of these vulnerabilities can be policed through automation, such as enforcement of strong passwords, but technology solutions can be only part of the answer. These topics must be addressed directly with employees, clinicians, suppliers and others who have access to secured assets, and whose behavior has an inevitable impact on security. Management at every level of the enterprise must make it a priority to address the issue of security regularly to make it a central feature of the organization’s life and culture.

And since an actual breach is always possible, healthcare organizations need to be ready to react decisively. The goal is to quickly contain the intrusion, assess the damage and address the situation in terms of rectifying the failure as well as in communicating responsibility outwardly to patients and the public in a proactive and thorough way. Doing so can limit the direct cost of the intrusion as well as the potential damage to trust and reputation.

Learning from the experience of others

It's a truism that one tends not to get rewarded for disasters that didn't happen—and the measures that have prevented disaster may erode over time, in the absence of a costly failure that would demonstrate their value and importance. Yet in a recent study, less than half of the healthcare organizations surveyed indicated that their security budget increased in the past year, with half reporting spending three percent or less of their overall IT budget on securing patient data. The same respondents ranked the maturity of their security environments on a scale from one to seven, where one was not at all a mature security environment and seven was highly mature. Respondents recorded an average score of 4.35.[9] This risk of complacency is one of the challenges inherent in maintaining effective security over the long term.

For this reason, when addressing security within their organizations, healthcare executives should certainly make reference to failures that occur at other healthcare institutions and to the intrusion attempts that are taking place everywhere, all the time, in all industries. These should serve as constant reminders of how close and immediate the threat remains.

This means that whatever security is in place can never be assumed to offer perfect protection. This is an arena in which the weaker players can expect to be victimized more readily than the strong. Whenever a security failure is reported at another enterprise, an immediate re-evaluation to assess one's own vulnerability is warranted. This is particularly true if a failure is the result of a new form of intrusion. Healthcare organizations will need to be ready to take new pre-emptive steps as information about new threats emerges in order to stay one step ahead of attackers.

Ten essential practices to address cybersecurity

Your approach to cybersecurity needs to be comprehensive enough to protect your healthcare data, applications and other assets from current threats, but also flexible enough to evolve with the changing threat landscape. It should be capable of addressing multiple attack vectors and of allowing your organization to detect, prioritize, address and prevent security breaches across virtually all of your hardware, software and services. Figure 2 shows the various components such an approach should include.

1. Build a risk-aware culture: This idea is elementary. Every single person can infect the enterprise, whether it's from clicking on a dubious attachment or failing to install a security patch on a smartphone. So the effort to create a security-rich enterprise must include everyone. Building a risk-aware culture involves setting the risks and goals, and spreading the word about them. But the important change is cultural. Think of the horror that many experience if they see a distracted parent on a cell phone while a child runs into the street. That same intolerance should exist, at an organizational level, when employees are careless about security. Management needs to push this change relentlessly from the top down, while also implementing tools to track progress.

2. Establish intelligent security operations and rapid threat response: Say that two similar security incidents take place—one in hospital, the other in a remote clinic or physician's office. They may be related, but without the security intelligence needed to link them, an important pattern—one that could indicate a potential incident—may go unnoticed. An organization-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system can enable an enterprise to monitor its operations and respond quickly.

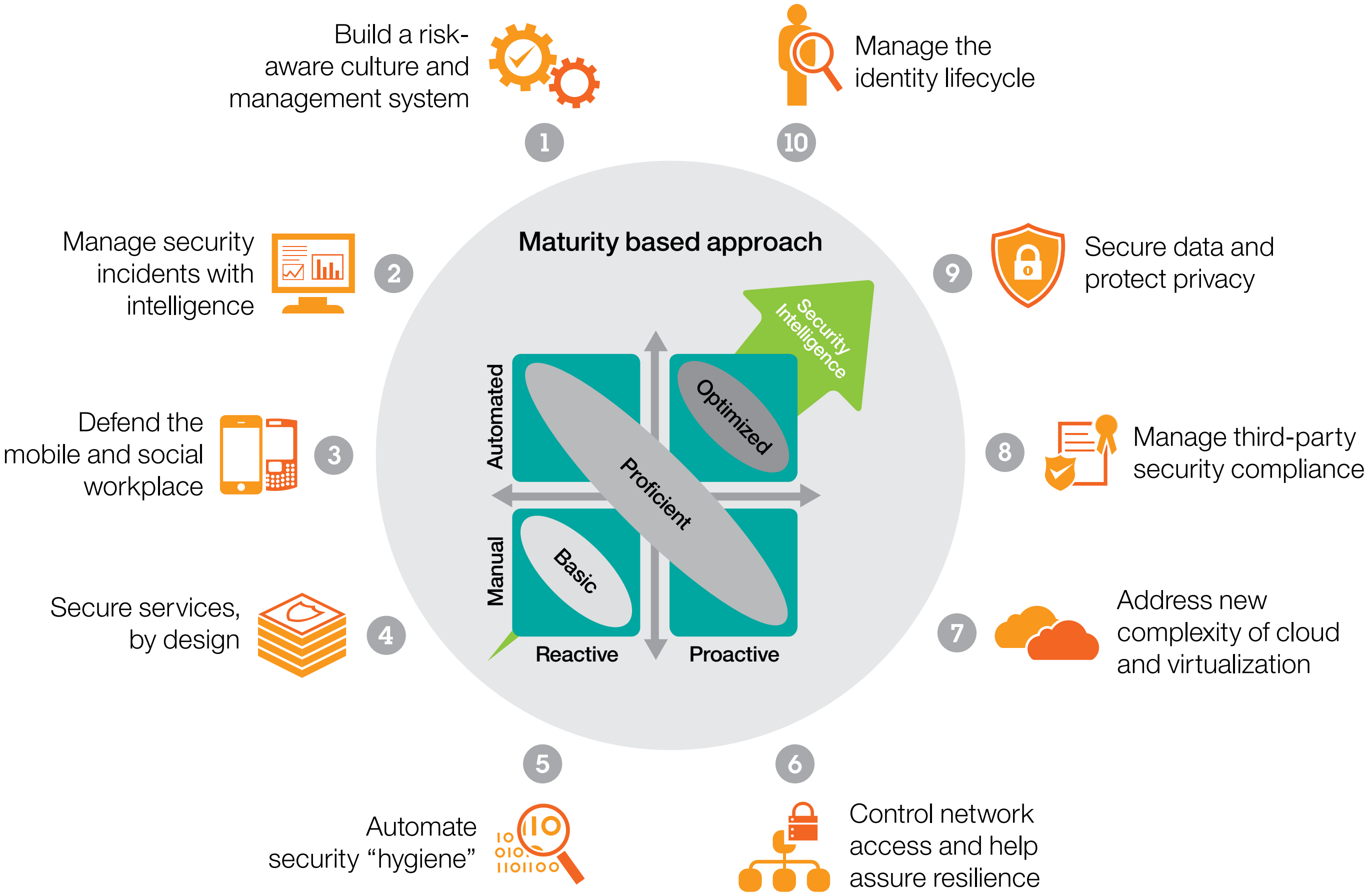

Build a risk-aware culture and management system
1
Manage the identity lifecycle
10
Maturity based approach
Manage security incidents with intelligence
2
Secure data and protect privacy
9
Security Intelligence
Automated
Optimized
Proficient
Defend the mobile and social workplace
3
Manage third-party security compliance
8
Manual
Basic
Reactive
Proactive
Secure services, by design
4
Address new complexity of cloud and virtualization
7
5
6
Automate security "hygiene"
Control network access and help assure resilience

Figure 2. Ten essential security practices for a smarter defense

3. Defend the workplace, including security-rich collaboration in social and mobile sites: Cybercriminals are constantly probing for weaknesses. Each work station, laptop or smartphone provides a potential opening for malicious attacks. The settings on each device must not be left up to individuals or autonomous groups. They must all be subject to centralized management and enforcement. And the streams of data within an organization and across the enterprise need to be classified, each one with its own risk profile and routed solely to its circle of users. Securing the work force means vanquishing chaos and replacing it with confidence.

4. Develop security rich products, by design: Imagine if the auto companies today, manufactured their cars without seat belts or airbags, and then added them later, following scares or accidents. It would be both senseless and outrageously expensive. In much the same way, one of the biggest vulnerabilities in information systems—and wastes of money—comes from implementing services first, and then adding security on as an afterthought. The only solution is to build in security from beginning, and to carry out regular automated tests to track compliance.

5. Manage IT hygienically: It happens all the time. People stick with old software programs because they know them, and they're comfortable. But managing updates on a hodgepodge of software can be next to impossible. Additionally, software companies sometimes stop making patches for old programs. Cyber criminals know this all too well. In a security-rich system, administrators can keep track of every program that's running, feel confident that it's current, and have a comprehensive system in place to install updates and patches as they're released.

6. Create a security-rich and resilient network: Consider urban crime. Policing would be far easier if every vehicle in a city carried a unique radio tag and traveled only along a handful of thoroughfares, each of them lined with sensors. The same is true of data. Organizations that channel registered data through monitored access points have a far easier time spotting and isolating malware.

7. Address security complexity of cloud and virtualization: Cloud computing promises enormous efficiencies, but it can come with some risk. If an organization is migrating certain IT services to a cloud computing environment, it will be in close quarters with lots of others—possibly including scam artists. In that sense, a cloud is like a hotel in which a certain percentage of the customers have fallen ill. To thrive and remain healthy in this environment, guests must have the tools and procedures to isolate themselves from the others and to monitor possible threats.

8. Manage third-party security compliance: Say a contractor needs access to the system. How do you make sure she has the right passwords? Leave them on a notepad? Send them in a text message? Such improvising has risk. An organization's culture of security must extend beyond company walls, and it should establish best practices among its contractors and suppliers. This is a similar process to the drive for quality control a generation ago. And the logic is the same: Security, like excellence, should be infused in the entire ecosystem.

9. Assure data security and privacy: Somewhere in the trove lies the company's critical data. Perhaps those include protected health information, scientific and technical data, maybe some documents regarding possible mergers and acquisitions, or clients' non-public financial information. Each enterprise should carry out an inventory, with the critical data getting special treatment. Each priority item should be guarded, tracked and encrypted as if the organization's survival hinged on it. In some cases it may.

10. Manage the digital identity lifecycle: Say a contractor gets hired full time. Six months pass and he or she gets a promotion. A year later, a competitor swoops in and hires him or her. How does the system treat that person over time? It must first give him or her limited access to data, then open more doors before finally cutting his or her access off completely. This is managing the identity lifecycle. It's vital. Organizations that mismanage it could be vulnerable to intrusions. This risk can be addressed by implementing meticulous systems to identify the people, manage their permissions and revoke them as soon as they depart.

Critical security steps for healthcare organizations to take:

Fortify your identity and access management:

- Develop standardized and repeatable entitlement processes and develop an entitlement verification process.
- Automate with alerts for all access to electronic protected health information (e-PHI) and other sensitive data.
- Implement newer technologies like provisioning workflow, strong authentication and single sign-on (SSO) or reduced sign-on (RSO).
- Consolidate directory services with single authoritative service as the goal.

Test your application security:

- Start testing applications and interfaces before they go online.
- Pen test websites and all external facing systems, test internal key systems for breach risks and strengthen them.
- Work with vendors to ensure they are implementing security-rich coding and software design practices.
- If applications are not HIPAA and Health Information Technology for Economic and Clinical Health Act-enabled, look for other options.
- Log, log, log … and automate or source reviewing process and alerts.

Monitor your physical security:

- Review video surveillance approaches and technologies.
- Integrate physical security systems and approach (badging, human resources and access control).
- Integrate and enhance relationship with facilities management and physical security.
- Pen test physical security of facilities.

Strengthen your governance, risk and compliance management:

- Conduct or review a security risk analysis per 45 Code of Federal Regulations 164.308(a)(1) of the certified electronic health record (EHR) technology, implement security updates and correct identified security deficiencies as part of its risk management process.
- Identify the e-PHI within the organization. This includes e-PHI that you create, receive, maintain or transmit.
- Identify the external sources of e-PHI (such as, do vendors or consultants create, receive, maintain or transmit e-PHI?).
- Review HIPAA security gap assessments and address key issues—develop an implementation approach and plan and a common operating framework or a measurement framework.
- Enforce your IT and operational policies vigorously up to and including termination of employment.

Establish comprehensive data security:

- Establish a framework or strategy for data security.
- Update security policies and procedures and perform training for staff.
- Implement whole-disk encryption across enterprise for mobile and at-risk devices.
- Conduct data loss prevention (DLP) analysis and implement data loss prevention tools.
- Evaluate options for Multi Factor Authentication (MFA) for elevated privileges and ePHI.
- Log data access and control data security.

Monitor for threats:

- Review patch, compliance and configuration management and ensure a standardized approach and tools.
- Enhance testing, response and protection capabilities for network and environment and at-risk areas.
- Develop breach notification plan and emergency response approach.
- Implement business continuity and data recovery plans including analyst involvement and table-top testing.
- Ensure firewall, intrusion detection system, intrusion protection system, antivirus and associated security infrastructure technologies are up to date.

Conclusion

With a greater push to implement electronic health records and increasingly complex and rapidly changing healthcare environments, cybercrimes are all but guaranteed to increase in number unless healthcare organizations significantly improve their cybersecurity systems. These concerns are driving today's boardroom discussions, and healthcare executives are being asked some tough questions about:

- Their organization's data security, compliance and privacy priorities
- The potential risks associated with these priorities
- How these priorities might affect the organization's bottom line
- The security risks associated with the adoption of mobile or cloud initiatives

Addressing these issues requires taking a broader view of the healthcare environment and a more comprehensive approach to privacy and security. Healthcare organizations must apply such an approach to all their systems, including those that track patient data; those that contain information about healthcare providers, insurers, pharmaceutical manufacturers and distributors; those that contain credit card information; and those that control medical devices.

Technology changes alone will not adequately mitigate security issues. An organization-wide shift in thinking is necessary, and such a shift requires a commitment to security from the top. Organizations need to implement better training, audits, and security policies and procedures that are communicated throughout the facility—as well as to outside vendors.

Healthcare executives will need to allocate more resources and staff to security, but skills shortages and rapidly changing techniques make the task difficult. Engaging knowledgeable and experienced outside professionals along with advanced research capabilities can fill skills gaps, help the organization understand threats and increase visibility.

Healthcare organizations seeking to take a fresh look at their security posture should:

- *Establish a recurrent process that comprehensively reevaluates all security measures in place*, including network access point defenses, analytics to detect incipient intrusions and the maintenance of a vigilant internal culture through strong process controls and habits. To be robust, such reevaluations must be performed by someone other than those who have been responsible for defining and implementing current security defenses. This helps to ensure objectivity, and provides a fresh view on existing defenses to help spot vulnerabilities that the organization itself has not identified. External security specialists should be used to help assure that the assessment will be thorough and independent.
- *Use the findings of security assessments to prioritize the next steps*, and define an action plan to bring all elements up to strength.
- *Keep an eye on the evolving nature of security threats:* Success in preventing intrusions means that the organization needs to watch how the failures of others occur and immediately take steps to preempt similar incursions.
- *Establish security as an ongoing theme and priority*, shared by executives at all levels and reflected in the culture as well as the engrained habits of employees, partners, suppliers and other relevant parties.

Certainly, there is no "magic formula." Digital security will remain a primary concern into the future, and must therefore be treated as a continuing and significant risk by organizations of all kinds.

The essentials:

IBM Security brings together our powerful, industry-leading security software, analytics capabilities and deep expertise for hybrid deployment using on-premise, cloud-as-a service delivery and managed services.

Security software:

- Security intelligence and analytics
- Advanced fraud and threat protection
- Identity and access management
- Application and data security
- Mobile and cloud security
- Network and end point protection

Key software:

- IBM® QRadar®: Security Intelligence Platform
- IBM Guardium®: Data Security
- IBM Trusteer®: Fraud Protection
- Fiberlink: Mobile Security and Management
- IBM BigFix®: Endpoint Security and Management

Key Services:

- IBM Security Strategy, Risk and Compliance
- IBM Security Intelligence and Optimization
- IBM Cyber Security Assessment and Response
- IBM Identity and Access Management
- IBM Application and Data Security
- IBM Infrastructure and Endpoint Security

Why IBM?

IBM offers one of the most advanced and robust portfolios of security-related services and solutions for the healthcare industry. Our security consultants help you plan, implement and manage virtually all aspects of your security strategy. Our senior security professionals have honed their skills through years of engagements with the financial services industry. We can optimize your level of control by providing consulting services to help establish your security strategy. We can also provide implementation and integration services using market-leading technologies to help protect your applications, prevent data loss and employ sophisticated encryption.

IBM monitors—in real time—some of the most complex corporate networks in the world and develop some of the most sophisticated testing tools in the industry. Our team of highly skilled security professionals is constantly identifying and analyzing new threats, often before they are even known by the world at large. In fact, we maintain one of the largest single databases of known cyber security threats in the world. With our unique place in the industry and deep security expertise, IBM can be an ideal partner in the effort of safeguarding your enterprises' critical assets.

For more information

To learn more about IBM Security, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

Notes

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

[1] IBM Security Services 2014 Cyber Security Intelligence Index, June 2014

[2] Ponemon Institute, “Fourth annual benchmark study on patient privacy and data security,” March 2014

[3] WIRED, “It’s insanely easy to hack hospital equipment,” April 25, 2014, http://www.wired.com/2014/04/hospital-equipment-vulnerable

[4] IBM MSS Healthcare Industry Overview: Healthcare Report, October 7, 2014

[5] 6th Annual HIMSS Security Survey, sponsored by Experian® Data Breach Resolution, February 19, 2014

[6] Ibid, IBM MSS Healthcare Industry Overview

[7] http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/

[8] Krebs, B. “Target Hackers Broke in Via HVAC Company.” Krebs on Security. February 14, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[9] Ibid. 6th Annual HIMSS survey.