Harnessing the Power of NIST
Your Practical Guide to Effective Information Risk Management

By
Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO Clearwater Compliance LLC
# Table of Contents

Executive Summary 3  
Introduction 5  
Three (3) Components of the NIST IRM Approach 7  
1. NIST Cybersecurity Framework 7  
2. NIST IRM Process 8  
3. Maturity Model 8  
Four (4) Major Phases of the NIST IRM Process 10  
1. Frame Risk — Create Your Strategy 11  
2. Assess Risk — Understand Your Exposures 12  
3. Respond to Risk — Implement Appropriate Treatment 14  
4. Monitor Risk — Assess Your Controls Effectiveness 15  
Five (5) Next Actions to Adopt the NIST IRM Approach 16  
1. Review and evaluate the overall NIST IRM approach 16  
2. Adopt the NIST Cybersecurity Framework and NIST IRM process 16  
3. Embrace a continuous process improvement / maturity model approach 17  
4. Educate your team on the NIST IRM Process 16  
5. Consider the Clearwater IRM|Pro™ software suite to help operationalize your IRM program 17  
Six (6) Top Benefits of Using the NIST IRM Approach 18  
1. Market Differentiation Benefit 18  
2. Continuous Process Improvement / Mature IRM Benefit 18  
3. Legal and Regulatory Compliance Benefit 18  
5. Proactive vs. Reactive Security Management Benefit 19  
6. Program Defensibility Benefit 19  
Conclusion 20  
About Clearwater Compliance LLC 21  
Endnotes 22
Executive Summary

The subject of information risk management is on the radar screens of more and more executive teams and Boards. Advice on managing cyber risk is emerging from numerous organizations, including the National Association of Corporate Directors\(^1\) and the New York Stock Exchange\(^2\). The subject of information risk management is on the Congressional agenda as well with Senate Bill 754 and a goal to: “To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.”\(^3\)

In response to the “call to arms” from within and outside their organizations, senior leaders are exposing a current state of siloed, tactical, technical spot-welding and firefighting when it comes to managing these risks.\(^4\) Industries, especially those comprising the national critical infrastructure must move to a more strategic, business-oriented and architectural Information Risk Management (IRM) approach and posture. Organizations in the private and public sector must do a better job protecting our national digital assets and safeguarding the sensitive personal information with which they have been entrusted.

The single most important decision that senior leaders and board members must make about IRM … is how they are going conduct IRM in their organizations.

We recommend that organizations adopt the holistic National Institute of Standards and Technology (NIST) approach to conduct IRM. Organizations today may be overspending or underspending in their information security capital and operating expenses. A well designed and executed IRM program will assist executive teams and Boards in making higher quality decisions about these IRM investments.

Order, process and discipline are needed to establish, implement and mature a formal IRM program. Controls-based “checklists” and made-up frameworks do not and will not protect our national digital assets and the exploding amount of sensitive information organizations are creating, receiving, maintaining and transmitting. Too many organizations that rely on and have designated their preferred security checklist of controls too often use standards simply as checklists (e.g. ISO, PCI, HITRUST, SOC 2, CSF, etc.).

Third party certifications based on these checklists simply do not result in a well-designed and executed IRM program. As an example, given all the major breaches in the healthcare payer community (e.g., Anthem, CareFirst, Premera, Excellus), largely the organizations behind the HITRUST checklists, it seems likely that further consideration will be given to a more process-based, architectural approach.\(^5\) In fact, inherently incorrect in these checklists of controls is their failure to consider other key elements of any
robust IRM program: an organization’s unique information assets, threat sources, threat actions, and vulnerabilities. Nor do these checklists take into account the strength of any controls or safeguards that have been implemented or the likelihood and impact of adverse events. They simply “checklist away” such unique considerations in a one-size-fits-all manner.

Many argue over which checklists organizations should adopt. It’s confusing, and a huge waste of time. Organizations cannot check-list their way to good IRM and information security! That’s not what real IRM is about.

Organizations serious about IRM will proactively drive three priority initiatives to completion:

1. Strategically – they will make IRM a C-suite and Board agenda item in order to facilitate meaningful dialog and decisions about cyber and other information risks within their organizations;
2. Tactically – they will establish, implement and mature an IRM program to ensure ongoing improvement in the management of these growing risks; and
3. Operationally – they will become expert at conducting bona fide, comprehensive risk assessments which serve as a foundational step in any well-executed IRM program.

This Clearwater Compliance white paper focuses primarily on the tactical agenda item above – to establish, implement and mature an IRM approach -- by recommending formal adoption of the NIST information Cybersecurity Framework and, specifically, the NIST IRM process detailed in NIST’s Managing Information Security Risk: Organization, Mission, and Information System View (Special Publication 800-39). The Cybersecurity Framework is simply that: a framework. It requires a risk management process to enable organizations to inform and prioritize sound cybersecurity decisions. The NIST IRM process will be discussed in detail. Further, this white paper recommends that organizations complement the adoption of the NIST IRM process by embracing a continuous process improvement approach embodied in a process capability maturity model.

Finally, the white paper presents the case for action along with practical, actionable steps to take to adopt the NIST IRM approach, including continuous process improvement. Numerous resources are cited and provided for those leaders and staff members interested in better management of and higher quality decisions about information risks.

Think: Framework + Process + Maturity Model = Effective and Efficient IRM
Introduction

One of the highest priorities facing organizational leadership today in all industries of all sizes is safeguarding the exploding amount of sensitive data with which the organization has been entrusted. A breach of this sensitive data not only compromises the confidentiality, integrity, and/or availability of information created, received, maintained or transmitted by the organization’s internal systems, but it also damages or destroys long-term relationships with their customers.

Today we don’t have to look further than the national headlines to understand the weaknesses that exist in IRM in all sectors of all industries. From Target, to Home Depot, to Anthem, to Sony, to OPM, there have been dozens of news stories about serious cyber breaches that have adversely affected millions of consumers. What’s more, experts predict that cyber attacks are only going to increase and become even more harmful.8

The central problem is that while organizations are implementing some countermeasures to protect information from these threats, they are not necessarily doing the right things to actually make informed treatment decisions about all their risks. In particular, they have not yet adopted an effective information security framework and process that contains critical components — including information assets, sources of threats, threat actions, vulnerabilities and effective controls; then, implementing the process of assessing the likelihood and impact of adverse events in order to make better risk response decisions. Further, they have not adopted the maturity model mindset that is critical to effective cybersecurity — one that fosters and supports continuous process improvement.

Checklists do not result in effective IRM; only a framework and a process combined with continuous process improvement will do so.

No industry is safe from the threat of external or internal attacks. Cyber criminals (inside or outside of the organization) indiscriminately attack entities in every sector — from banking to retail to healthcare to social media. This means that every organization of any type or size needs to adopt an approach that is strong enough to protect their information assets.

Until recently, it was believed that cybercriminals were not as interested in healthcare data as they were in financial data. But healthcare breaches are on the rise, especially as more cybercriminals understand the value of patients’ personal data — and how to “monetize” it on the dark web.10 This recognition is among the reasons why over 155 million patient health records have been reported to have been compromised in data breaches since 2009.11 And the frequency and severity of these breaches are likely to increase.

According to Tom Kellerman, Chief Cybersecurity Office at Trend Micro:
“The healthcare industry is being hunted and hacked by the elite financial criminal syndicates that had been targeting large financial institutions until they realized healthcare databases are more valuable.”12

Further, Jim Trainor, Deputy Assistant Director of the FBI Cyber Division, stated: “Now healthcare is considered a top target. The speed of these attacks and the volume with which they are occurring is increasing significantly. It just requires a much more robust response across the U.S. government and private sector … Major intrusions into healthcare providers’ computer systems now are happening at the pace of two or three a day.”13
While the risks are greater now than ever, adopting and maintaining a strong IRM program and posture is becoming more challenging. In fact, managing information risk and keeping information secure is a complex, multi-faceted program that requires the involvement of the entire organization — from Board members adopting and setting guiding principles; to senior executives providing the strategic vision and top-level goals and objectives; to mid-level leaders planning, executing and managing projects; to individuals on the front lines operating and using the information systems supporting the organization’s mission and business functions.

Clearly, organizations must raise the effectiveness of their IRM programs to levels that facilitate better management of these risks. The most powerful, efficient, and effective way to address this business imperative is to adopt an industry standards-based, proven, trustworthy approach that gives organizations the structure and process steps they need to build a fortifying IRM program that protects all sensitive data from compromise — and by adopting a mindset focused on continuous process improvement.

One of the most powerful IRM frameworks and processes already exists — the NIST Cybersecurity Framework and the NIST IRM process. The NIST Cybersecurity Framework is detailed in the Framework for Improving Critical Infrastructure Cybersecurity. The NIST IRM process is detailed in NIST’s Managing Information Security Risk: Organization, Mission, and Information System View (Special Publication 800-39). The NIST IRM approach (Framework + Process + Maturity Model) gives organizations a proven security infrastructure, along with an abundance of critical guidance on managing information risks. The process is outlined in the NIST Special Publication 800-39 and detailed in a compendium of related Special Publications describing Risk Assessments, Risk Management and controls. By combining the power of the NIST approach with a continuous process improvement mindset, any organization can establish, implement and mature their IRM programs to protect their information from today’s growing number of unrelenting threats.

This white paper introduces the NIST IRM approach comprising the NIST Cybersecurity Framework and, in a more detailed way, specifically covers the essential components of the the NIST IRM process. The white paper further makes a strong business case for why today’s organizations should adopt this overall NIST IRM approach along with a maturity model mindset.
Three (3) Components of the NIST IRM Approach

In this paper, we define the NIST IRM approach as comprising:
1. the NIST Cybersecurity Framework;
2. the NIST IRM process; and,
3. a Maturity Model.

Certain government organizations subject to the Federal Information Security Modernization Act\(^7\) (FISMA) are required to follow the NIST IRM approach. For commercial organizations, especially those that comprise the 16 critical infrastructure sectors of our economy\(^8\), including the Healthcare and Public Health Sector as an example, following the NIST IRM approach is highly advisable. Otherwise, the NIST IRM approach is a voluntary standard that can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. Further, the approach can be used by organizations that already have extensive IRM programs, as well as by those just beginning to put IRM in place. The same general approach works for any organization, although the way in which organizations make use of the approach will differ depending on their current state, organizational priorities, size, information assets, etc.

1. **NIST Cybersecurity Framework**
   The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. The NIST Cybersecurity Framework is not designed to be a checklist.

   The NIST Cybersecurity Framework comprises three major components – the Core, Implementation Tiers and Profiles. As with other frameworks, it provides structure but does not provide a process. The Framework:
   - Leverages five (5) international standards
   - Organizes reconciliation and de-confliction of legislation, regulation, policy, and industry best practice (Core)
• Guides organization and management of an information security program (Core)
• Measures current state and expresses desired state (Profile)
• Enables investment decisions to address gaps in current state (Profile)
• Communicates cybersecurity requirements with stakeholders, including partners and suppliers (Profile)
• Enables informed trade-off analysis of expenditure versus risk (Tiers)

To help health care organizations covered by the Health Insurance Portability and Accountability Act (HIPAA) to bolster their security posture, the Office for Civil Rights (OCR), in February 2016, released a crosswalk entitled “HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework” developed with NIST and the Office of the National Coordinator for Health IT (ONC), that identifies “mappings” between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) and the HIPAA Security Rule.

The Cybersecurity Framework requires a formal IRM process with detailed steps to enable organizations to inform and prioritize cybersecurity decisions; the Cybersecurity Framework is not a process itself. It is adaptive to provide a flexible, information risk-based implementation that can be used with a broad array of risk management processes, including, for example, NIST SP 800-39.

The Cybersecurity Framework provides guidance on the approach to IRM; the NIST SP 800-39 process provides detailed steps to actually implement the Cybersecurity Framework.

2. NIST IRM Process
The NIST Cybersecurity Framework and the NIST IRM Process were created by the Computer Security Division within the Information Technology Laboratory within NIST, which is part of the U.S. Department of Commerce. The work and special publications that comprise the approach came about through a collaboration between industry and government. The methodology was written by the world’s top experts in the field of information security. NIST’s mission is to develop and promote measurement, standards and technology to enhance, strengthen and improve IRM, thereby helping organizations better understand, manage and reduce their risks. NIST is also responsible for establishing computer- and information technology-related standards and guidelines for Federal agencies to use. Many private sector organizations have made widespread use of these standards and guidelines voluntarily for several decades, especially those related to information security. In fact, both the NIST Cybersecurity Framework and the NIST IRM process are continuously validated through ongoing collaboration between NIST and industry.

The NIST IRM process, which includes standards, guidelines and practices, is intended to provide owners and operators of critical information assets with a trusted methodology to better protect information entrusted to their organizations and to conduct ongoing, effective IRM. The NIST IRM process was designed to foster communication between both internal and external organizational stakeholders in IRM. The process assists them in several critical steps including:
• **Frame** - Determining the organization’s risk strategy
• **Assess** - Identifying, prioritizing, and estimating risks
• **Respond** - Finding best ways to treat the known risks
• **Monitor** - Establishing processes to continually monitor security and the IRM process

3. Maturity Model
Effective IRM is a dynamic process, requiring an ongoing commitment to continuous improvement. When the NIST IRM approach is used in concert with a maturity model, organizations can establish, implement and mature their IRM programs more efficiently and with greater confidence. Maturity models typically follow the Deming “Plan, Do, Check, Act” model to achieve “Continuous Process Improvement.” Further, coupling a maturity model with the NIST IRM approach provides a clear mechanism for demonstrating a program is being established, implemented and is maturing. This approach also helps reduce the challenge of
demonstrating the ongoing management of compliance and information security risks to all stakeholders, including customers and regulators.

While the NIST Cybersecurity Framework describes Framework Implementation Tiers ("Tiers"), the Tiers are not intended to be maturity levels. These Tiers are intended to provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The key tenet of the Tiers is to allow organizations to take stock of their current activities from an organization wide point of view and determine if the current integration of cybersecurity risk management practices is sufficient given their mission, regulatory requirements, and risk appetite.

We strongly recommend that organizations adopt a maturity model approach to apply to the Tiers concept introduced in the Framework in order to formalize its ongoing continuous process improvement efforts and, more importantly, increase the effectiveness and efficiency of its IRM program over time.

The NIST IRM approach lends itself to and requires building a capability that transcends time, information assets, media types, sources of threats, threat actions, vulnerabilities, controls, changes in industry likelihood data and changes in organizational impact (loss or harm) data.

Checklists are point-in-time, spot-assessments that are typically limited to controls only and, therefore, do not facilitate continuous process improvement and change management. The NIST IRM approach facilitates continuous process improvement, change management and the use of a maturity model.

Today the NIST IRM approach is being utilized across the U.S. in a host of sectors, and by organizations ranging from multinationals to small organizations. These organizations are using the approach in a variety of ways including:

- To raise awareness and communicate with stakeholders within their organizations, including executive leadership.
- To improve communication across the organization, allowing IRM expectations to be shared with business partners, suppliers and sectors.
- To map the process to current IRM approaches to learn and illustrate how they match up with the process’s standards, guidelines and best practices.
- To reconcile and de-conflict internal policy with legislation, regulation and industry best practice.
- To strategically assess current practices and plan future processes.

The NIST IRM approach is an industry-standard, proven approach that can be effective for your organization.
Four (4) Major Phases of the NIST IRM Process

The NIST IRM approach can scale up and down and provides a comprehensive structure that includes policies, standards and systems. Within this approach, IRM is carried out as a holistic, organization-wide activity that addresses information risk across the organization — from the strategic level to the tactical level — thereby, ensures that risk-based decision-making is integrated into every aspect of the organization by design. The NIST IRM process recognizes and accommodates the requirement that IRM must be driven by the organization’s mission.

Integrated, enterprise-wide IRM includes consideration of several organizational planning components, for example:

- Key strategies
- Key tactics
- Key initiatives and processes
- Key sensitive information
- Key information risks

The prioritized, flexible and repeatable NIST IRM process lays out the fundamental concepts associated with managing information risk across an organization into eight categories:

1. Components of risk management
2. Multi-tiered risk management approach
3. Risk management at the organization level (Tier 1)
4. Risk management at the mission and business process level (Tier 2)
5. Risk management at the information system level (Tier 3)
6. Risk related to trust and trustworthiness
7. Effects of organizational culture on risk
8. Relationships among key risk management concepts

According to U.S. Department of Commerce, the process should not be implemented as a non-customized or one-size-fits-all checklist within all organizations. Organizations have unique risks — different information assets, different threats, different vulnerabilities, different controls and different risk tolerances — and how and the extent to which they implement the steps within the process to achieve positive outcomes will vary. To be most effective, the NIST IRM process should be tailored by different sectors and individual organizations to best suit their risks, situations and needs. Extracting, building and only using checklists of controls leaves out key ingredients of IRM and key process steps...and is just plain wrong.
The NIST IRM process includes four major phases: frame risk, assess risk, respond to risk and monitor risk. This section briefly describes each of these four phases. As the NIST IRM process model shown illustrates, these process phases are highly interdependent and inform one another, as an organization establishes, implements and matures its IRM program.

1. Frame Risk – Create Your Strategy
This phase is where the NIST IRM process journey begins. In this NIST IRM phase, the process addresses how organizations frame risk or establish a context for risk-based decision making — in other words, how they describe the environment in which risk-based decisions are made and how they will go about managing risks. In the framing phase, organizations articulate and document risk assumptions about their IRM programs, including what information assets are included, what assets are not included, what constraints exist in executing its IRM program, their risk tolerance and the risk architecture they need to support their IRM program. The NIST Cybersecurity Framework provides a perfect backdrop for this frame risk phase—it is a framework after all.

The purpose of the risk-framing phase is to produce an IRM strategy that addresses how organizations intend to assess risk, respond to risk and monitor risk — making explicit and transparent the risk perceptions, assumptions and guidelines that organizations routinely use in making both organizational investment and operational decisions. The risk frame phase establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

Phase one begins with strategic-level decisions on how risks to the organization’s operational and information assets, individuals and other organizations are to be managed by senior leaders. To establish a realistic and credible risk frame requires that the organization identify and document the following:

- **Risk assumptions.** These are hypotheses about the information assets, threats, vulnerabilities, and the impacts and likelihood of occurrences that affect how risks will be assessed, responded to and monitored over time.
- **Risk constraints.** These are limitations on the organization’s risk assessment, response and monitoring alternatives under consideration due to, for example, limited resources, legacy technology or higher business priorities.
- **Risk tolerance.** This is the level of risk that the organization is willing to accept in pursuit of strategic goals and objectives.
- **Priorities and trade-offs.** These are the articulation of the relative importance of missions and business functions, trade-offs among different types of risk that the organization faces, timeframes in which the organization must address risk and any factors of uncertainty that the organization will consider in responding to risk.
Key Deliverable of Risk Framing Step:
IRM Framework and Strategy Document
For example, this document would include sections such as the following:

- Introduction
- IRM Process
- Risk Appetite and Risk Tolerance
- Risk Framing Guidance
- Risk Assessment Guidance
- Risk Response Guidance
- Risk Monitoring Guidance
- IRM Automation Tools
- Records
- Reporting
- Timing of IRM Activities
- Roles and Responsibilities
- Early Warning Indicators
- Risk Budget

2. Assess Risk – Understand Your Exposures
The second phase of the NIST IRM process addresses how organizations assess specific risks within the context of the organizational risk frame. This phase requires identifying, prioritizing, and estimating all risks — that is, enumerating all the ways in which a compromise of the confidentiality, availability or integrity of sensitive information may occur and an assessment of the loss or harm to the organization and its stakeholders that may result from such a compromise. In the risk assessment phase, the organization must identify and analyze the following:

- **Information Assets.** A business application, system or solution that creates, receives, maintains or transmits sensitive information.
- **Threats.** Any circumstance or event with the potential to adversely affect information assets. Threat sources are typically categorized as adversarial, accidental, structural and environmental.
- **Vulnerabilities.** These are internal and external weaknesses within the organization. They are not confined to information systems, but can include, for example, vulnerabilities in governance structures, mission and business processes, enterprise architecture, information security architecture, facilities, equipment, system development lifecycle processes, customers, workforce members, supply chain activities and external service providers.
- **Likelihood.** A factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities, taking into consideration the current safeguards and controls in place.
- **Impact.** These are consequences or impacts to the organization that may occur given the potential for threats exploiting vulnerabilities, including loss or harm within the organization and that experienced by other stakeholders.
• **Risk.** The measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

The NIST Risk Assessment process is illustrated in the figure below and detailed in NIST SP800-30 Guide for Conducting Risk Assessments23.

To support the “assess risk” phase of the NIST IRM process, the organization should consider and document these factors, many of which are outputs of the “frame risk” phase:

- Tools, techniques and methodologies used to assess risk
- Assumptions related to risk assessments
- Constraints that may affect risk assessments
- Roles and responsibilities
- How risk assessment information is collected, processed and communicated
- How risk assessments are conducted within the organizations
- How often risk assessments are conducted
- How threat information is obtained, including sources and methods
- How vulnerability information is obtained

Comprehensive, bona fide risk assessment – a critical, foundational phase of the NIST IRM approach – involves creation of a detailed inventory of information assets and underlying media on which sensitive information resides; identification of sources of threats and threat actions; analysis of the vulnerabilities to such assets and media, along with assessment of the likelihood
of threats exploiting those vulnerabilities and, if they did, the weighting impact to the organization’s sensitive information and stakeholders, were such an exploitation to occur.

If, indeed, the organization is seeking to avoid the compromise of the confidentiality and/or integrity and/or availability of this sensitive information, its leaders need to carefully consider all and each of these variables. It’s not simply about controls and checklists of controls. Comprehensive risk assessment is a multi-phase process with multi-step sub-processes within each phase, focused on the consideration of multiple variables. It is not simply an examination of controls on a checklist.

### 3. Respond to Risk — Implement Appropriate Treatment

The third phase of the NIST IRM process addresses how the organization will respond to the risks that have been identified in phase two. The purpose of the risk response phase is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by:

- Developing alternative courses of action for responding to risk
- Evaluating the alternative courses of action (e.g., cost, feasibility, effectiveness, etc.)
- Determining appropriate courses of action consistent with organizational risk tolerance

---

**Key Deliverable of Risk Assessment Step: Risk Register or Risk Rating Report**

For example:

### Risk Rating Report

<table>
<thead>
<tr>
<th>MEDIA AND STORAGE DEVICES</th>
<th>ASSET NAME(S)</th>
<th>THREAT AGENT</th>
<th>THREAT ACTION</th>
<th>VULNERABILITY</th>
<th>RISK LIKELIHOOD</th>
<th>RISK IMPACT</th>
<th>RISK RATING</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone</td>
<td>Electronic Medical Record System</td>
<td>Burglar, Thief</td>
<td>Access to sensitive data once in possession of the device</td>
<td>Vulnerabilities related to encryption of sensitive data</td>
<td>5</td>
<td>5</td>
<td>25</td>
<td>02-16-2016, 5:21 PM, Jon Stone — We should consider encryption of our phones. In combination with the lack of authentication the risk is very high.</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Electronic Medical Record System</td>
<td>Burglar/Thief</td>
<td>Theft of equipment</td>
<td>Vulnerabilities in media handling</td>
<td>5</td>
<td>5</td>
<td>25</td>
<td>02-05-2016, 5:34 PM, Jon Stone — There has been a pattern of team members not securely storing Smartphone’s when not in use. A number of phones are thought to have been stolen. We need to increase training and oversight of secure storage.</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Electronic Medical Record System</td>
<td>Burglar, Thief</td>
<td>Access to sensitive data on laptop once in possession of the laptop</td>
<td>Vulnerabilities in user authentication</td>
<td>5</td>
<td>4</td>
<td>20</td>
<td>02-16-2016, 5:19 PM, Jon Stone — Our Smartphone’s do not require any user authentication. This gap requires immediate attention. 03-16-2016, 5:31 PM, Jon Stone — Given the frequency of use by our physicians in accessing the EHR we should seriously consider two factor authentication.</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Electronic Medical Record System</td>
<td>Burglar/Thief</td>
<td>Physical security vulnerabilities</td>
<td></td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>02-16-2016, 5:24 PM, Jon Stone — We currently do not have Policies and Procedures in place for physical Security Controls of Smartphone. Phones are often not secured. Steps must be taken immediately to address this.</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Electronic Medical Record System</td>
<td>Careless IT personnel</td>
<td>Improper destruction, disposal or reuse of storage media</td>
<td>Destruction/disposal vulnerabilities</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>02-16-2016, 5:26 PM, Jon Stone — Our Device Destruction and Disposal Policies and Procedures do not refer to smartphones. Our procedures should be amended to correct this gap. Bring this up at the next compliance committee meeting.</td>
</tr>
</tbody>
</table>
Implementing risk responses based on selected courses of action

To support the risk response phase, the organization must describe and document the following:

- Types of risk responses that can be implemented — including accepting, avoiding, mitigating, sharing or transferring risk
- Tools, techniques and methodologies used to develop courses of action for responding to risk
- How courses of action are evaluated
- How risk responses are communicated across the organization and, as appropriate, to external entities, including customers, external service providers and supply chain partners

### 4. Monitor Risk — Assess Your Controls Effectiveness

The fourth phase of NIST IRM process addresses how the organization will monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of the organization. The purpose of the risk-monitoring phase is to:

- Verify that planned risk response measures are implemented and information security requirements derived from business functions, Federal legislation, directives, regulations, policies, standards and guidelines are satisfied.
Five (5) Next Actions to Adopt the NIST IRM Approach

Every organization should choose its own manner and timetable in the adoption of the flexible NIST IRM approach to continuous process improvement. Following are a set of steps to get started:

1. Review and evaluate the overall NIST IRM approach

Read about the NIST Cybersecurity Framework and review these NIST Special Publications:

a. NIST SP800-39-final_Managing Information Security Risk
c. NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments
d. NIST SP800-53 Revision 4 Final, Security and Privacy Controls for Federal Information Systems and Organizations

2. Adopt the NIST Cybersecurity Framework and NIST IRM process

Be very wary of control checklists that profess to be IRM solutions or even risk assessments. The only effective and efficient way to establish, implement and mature an IRM program is to start with a bona fide, industry-standard, widely-accepted IRM approach. Unfortunately, many organizations profess to manage risk with control checklists because real IRM takes too much work and “hard thinking.” Those organizations that have implemented bona fide IRM know what that means. The easier way is to use a checklist of controls, with no real consideration of information assets, threats and vulnerabilities. Some of our nation’s largest Blues plans and other large
insurance organizations in healthcare have found this out the hard way, having endorsed a checklist approach.

The NIST recommended phased approach for implementing the NIST CSF includes the following steps:

- **Step 1**: Prioritize and Scope
- **Step 2**: Orient
- **Step 3**: Create a Current Profile
- **Step 4**: Conduct a Risk Assessment
- **Step 5**: Create a Target Profile
- **Step 6**: Determine, Analyze, and Prioritize Gaps
- **Step 7**: Implement Action Plan

3. **Embrace a continuous process improvement / maturity model approach**

The Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM™) maturity model that describes six levels of IRM process maturity (i.e., maturity levels 0 – 5) based on maturity in five key Capability areas:

- **Governance, Awareness of Benefits and Value**. Including processes and controls that ensure that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-upon enterprise IRM objectives.
- **People, Skills, Knowledge & Culture**. Including board and senior level engagement, creating a risk-aware workforce and establishing appropriate levels of IRM staffing and expertise across the organization.
- **Process, Documentation, Discipline & Repeatability**. Including predictable, measurable, controlled and standards-based IRM processes, protocols and procedures.
- **Use of Standards, Technology Tools/Scalability**. Including automation of key IRM workflows, key IRM activities and controls monitoring.
- **Engagement, Delivery & Operations**. Including embedding IRM issues in decision making and employing a consistent framework for continuously improving risk management programs and processes.

The IRMCAM™ maturity model includes an assessment capability that determines an organization’s current maturity level and identifies any meaningful gaps that may exist between the desired state of maturity and the current state. Such a maturity level assessment facilitates important discussions within a specific organization about whether or not addressing these gaps will result in better overall IRM outcomes. If an organization decides to achieve a higher level of IRM maturity, the IRMCAM™ maturity model facilitates setting forth a plan of action and milestones.

4. **Educate your team on the NIST IRM Process**

There are three areas of IRM about which the Clearwater team is particularly inspired and which serve as the basis of the work we do to assist organizations and their leaders become educated about IRM and proactively drive three IRM priority initiatives to completion:

a. Strategically – assist in making IRM a C-suite and Board agenda item in order to facilitate meaningful dialog and decisions about cyber and other information risks within their organizations;
b. Tactically – assist in establishing, implementing and maturing an IRM approach to ensure ongoing improvement in the management of these growing risks; and,
c. Operationally – assist individuals and organizations in becoming expert at conducting bona fide, comprehensive risk assessments which serve as a foundational step in any thoughtful IRM program.

Clearwater’s educational offerings focus on the priorities above. Consider taking advantage of these offerings including:

- Complimentary HIPAA and IRM webinars;
- Our NIST-based IRM Education track; and,
- The Clearwater HIPAA Compliance and Cybersecurity BootCamp™.

Tailored educational programs are also available from Clearwater.
5. Consider the Clearwater IRM|Pro™ software suite to help operationalize your IRM program

Used by 100s of organizations across the U.S. and having received the exclusive endorsement of the American Hospital Association, this industry-leading IRM|Pro™ software suite includes the IRM|Analysis™ application which automates key phases and workflows of the NIST IRM approach. The IRM|Capability™ application facilitates creation of the NIST CSF “Current Profile” and “Target Profile”. National Security Agency / Centers of Academic Excellence (NSA/CAEs) are currently using the software to train the nation’s next generation of information assurance and cyber defense leaders. This same software also earned Clearwater the designation of sole source provider of risk analysis and risk response software from the U.S. Air Force.

Six (6) Top Benefits of Using the NIST IRM Approach

There are six essential benefits organizations can realize with the implementation of NIST IRM approach — including market differentiation, continuous process improvement to achieve a mature IRM program, legal and regulatory compliance, better cloud security management, proactive cybersecurity management and program defensibility. This section provides an overview of these benefits.

1. Market Differentiation Benefit

According to Forrester Research: “In the battle to win, serve and retain customers, data security and privacy have become competitive differentiators and, thus, a top business technology agenda item.” This speaks to the fact that today’s consumers, business partners and other stakeholders are well aware of the risks to their information. One of the ways to raise confidence levels and trust in an organization’s IRM program is by sharing the fact that they are executing effective and mature IRM programs. Adopting the NIST IRM approach (Framework + Process + Maturity Model) affords this level of sophistication, security and trust. As a result, using the approach will not only deepen marketplace trust for organizations, but also give organizations a competitive advantage in the marketplace. Organizations that use the NIST IRM approach may have an advantage over their competitors in the eyes of consumers and business partners who are increasingly sensitive about keeping their information safe.

It is more compelling for an organization seeking a competitive advantage to present a proven, industry-standard approach like the NIST IRM approach to demonstrate its commitment to safeguarding sensitive information than to show they have completed an unproven, made-up, out-of-date checklist.

2. Continuous Process Improvement / Mature IRM Benefit

The NIST IRM approach provides organizations with a process-based approach designed to help compliance, privacy, security and IRM professionals establish, implement and mature their IRM programs. Coupled with the IRMCA™ maturity model, organizations may benchmark their progress internally and against other organizations. According to the Six Sigma methodology, “Process maturity is an indication of how close that process is to being complete and capable of continual improvement through qualitative measures and feedback. Thus, for a process to be mature, it has to be complete in its usefulness, automated, reliable in its information and continuously improving.”

Maturity in IRM means adopting an overall approach that gives organizations, their customers and their partners the assurance that their IRM processes are more sophisticated and effective than are the less mature checklists and unproven models. The NIST IRM approach, with its framework and process, provides a mechanism to better integrate IRM into organizations’ overall enterprise risk management strategy and lends itself to using a maturity model for continuous process improvement, unlike the checklist approach.

3. Legal and Regulatory Compliance Benefit

Organizations today are in legal and regulatory overload. There is an ever-expanding list of Federal,
state and local laws and regulations along with growing contractual requirements related to information privacy, security and breach notification. The good news is that most compliance requirements can be met by implementing the NIST IRM approach, because this standard gives organizations an ideal methodology that can be used to address these regulations. The risk-based decision-making inherent in the NIST IRM approach serves as the basis of, and is referenced in, many privacy, security and breach notification legal requirements, regulations and industry standards across numerous industries throughout the U.S., including HIPAA, FERPA, GLBA, SOX, PCI DSS and more.

Compliance is more readily and consistently achieved through alignment with an approach like the NIST IRM approach. Using the NIST IRM approach, changes to organizational processes can be made once in a consistent fashion and applied across multiple requirements, which saves both time and money.

Even though cloud computing has been used by many organizations for some time, it is now vital that organizations apply the same sound, consistent approach to safeguarding information assets hosted in a cloud environment that organizations consider for any other sensitive data. At the end of the day, good IRM is not about where your data resides; it is about the flexible, adaptable approach used to keep the data safe — whether sensitive information resides on hard drives in a Tier 4 data center, a server in a computer closet, on mobile devices or on an array in the cloud. Effective IRM requires the same considerations in all cases, including inventorying their information assets, identifying the sources of threats, understanding threat actions, determining vulnerabilities and implementing appropriate controls to eliminate or mitigate the possibility of threats exploiting vulnerabilities.

5. Proactive vs. Reactive Security Management Benefit
The only constant in today’s IRM world is change. External threat vectors are always evolving. New vulnerabilities are being discovered every month. Information assets are retired and new information assets are deployed. Not only do organizations have to evolve their IRM program to manage these changes, but they also need to proactively flex to mitigate the risks in this dynamic, changing environment. Checklists are static and are usually reactive at best. By conducting IRM with the NIST approach, organizations are much better positioned to proactively identify and respond to their most critical risks — thereby, protecting themselves from much of today’s changing risk landscape. What’s more, the NIST IRM approach results in reduced resource effort and time to respond to security inquiries, shortens the organization’s sales cycle, reduces the number of audit or review cycles, minimizes customer complaints and lowers the probability of a breach — all of which leads to the increased efficiency resulting from an IRM-by-design stance.

6. Program Defensibility Benefit
Evidence and analysis are needed to determine and prove the effectiveness of any IRM program. With a checklist approach, claims or hypotheses about effectiveness generally are based on point-in-time score card that is often dead-on-arrival. In fact, most control checklists are out-of-date at the onset of the exercise; critical other variables in risk determination are changing too quickly for static checklists to keep up.

The NIST IRM approach delivers widely-accepted proof of a reliable, defensible, trustworthy, standards-based IRM approach of analyzing assets, threats, vulnerabilities, controls, likelihood, impact and overall risk ratings— all key ingredients representing a defensible IRM posture in our current cyber risk environment.
Conclusion

“First, do no harm.”

This is not just a guiding principle for medical care today. It also has to be the rallying cry for protecting sensitive information of all types from the compromise of the confidentiality, integrity or availability resulting from all adversarial, accidental, structural and environmental threat sources exploiting vulnerabilities. Organizations must take the right actions to safeguard the sensitive information they create, receive, maintain or transmit. There is too much at stake if organizations do not adopt a holistic approach.

The risks in handling healthcare information are significant and growing. Today the information needed to deliver care resides in more places than ever before, including electronic health records, mobile devices carried by physicians and other caregivers, intelligent medical devices like smart pumps, monitors and implants, not to mention provider partners, business associates and other members of the patient care ecosystem. Safe, quality care depends on timely access to this information. Therefore any threats to information security represent threats to patient safety.

The NIST IRM approach (Framework + Process + Maturity Model) properly implemented and executed, delivers the most substantial and effective approach available today to help organizations establish a powerful, trustworthy IRM program. Organizations adopting the NIST IRM approach will be better equipped to accomplish the critical tasks of effective IRM.

With the OCR and the ONC further affirming their commitment to the NIST Cybersecurity Framework by completing their mapping between the NIST CSF and the HIPAA Security Rule, Clearwater Compliance strongly recommends the NIST IRM approach as the most powerful approach available today. Combined with the IRMCAM™ maturity model and Clearwater’s award-winning software, organizations become immediately empowered to establish, implement and mature their IRM programs to achieve more optimal IRM decision making, fewer failed audits, better regulatory compliance and reduced cybersecurity risk.
About Clearwater Compliance LLC

Clearwater Compliance assists health care organizations to establish, operationalize and mature their compliance and cybersecurity programs. Led by veteran, C-suite health care executives, Clearwater provides award-winning software, tools, professional services and a variety of related educational events and resources.

Clearwater works with health care organizations and business associates that are committed to safeguarding the privacy and security of sensitive information. The company’s varied and loyal customer base is a testament to the scalability of their solutions. Each year Clearwater’s solutions are trusted by hundreds of organizations including covered entities ranging in size from major integrated health systems and health plans to community hospitals, institutional pharmacies, specialty clinics and medical practices. Business associate customers include technology service providers, benefits management companies, law firms, business process outsourcing companies, third-party administrators, software hosting organizations, population management and data analytic companies and many more, from Fortune 100 companies to health care startups.

Clearwater recruits and hires only the most highly skilled, credentialed and experienced privacy, security and information risk management professionals. These experts can tackle a wide range of professional services engagements, each defined specifically around the needs of the customer. Clearwater’s core mission is to create value for our customers by equipping them with the tools and education they need to build strong compliance and cybersecurity programs, while helping them become as self-sufficient as they wish to be.

Since 2009, the company has served hundreds of organizations nationwide and internationally and has been highlighted as one of the top cybersecurity companies in The CyberSecurity 500 and the CIOReview 20 Most Promising Cyber Security Solutions list. They also are featured in CIOReview’s Top 500 Enterprise Security Solutions in 2016, and have authored respected white papers on the topics of the NIST Cybersecurity Framework and HIPAA compliance best practices. Health care information privacy, security, compliance and risk management solutions from Clearwater Compliance LLC have earned the exclusive endorsement of the American Hospital Association.

Find out more at clearwatercompliance.com. Connect via Twitter: @ClearwaterHIPAA or LinkedIn: https://www.linkedin.com/company/clearwater-compliance-llc.

Copyright © 2015 Clearwater Compliance LLC. All Rights Reserved.
Any replication or dissemination shall only be authorized by the express written permission of Clearwater Compliance LLC.
Endnotes

1 NACD Cyber-Risk Oversight Handbook
2 NYSE - Definitive Cybersecurity Guide for Directors and Officers of public companies.pdf
3 Cybersecurity Information Sharing Act of 2015
4 The Perils of Silos in Risk Management, CFO Magazine
5 HITRUST or High Risk? The Health Information Trust Alliance’s Common Security Framework
6 http://www.nist.gov/cyberframework/
7 NIST SP800-39-final_Managing Information Security Risk
8 http://www.scmagazine.com/dapper-tells-senate-committee-that-cyberattacks-are-worsening/article/442563/
14 Framework for Improving Critical Infrastructure Cybersecurity
15 NIST SP800-39-final_Managing Information Security Risk
16 NIST SP800-39-final_Managing Information Security Risk
17 http://www.dhs.gov/fisma
18 http://www.dhs.gov/critical-infrastructure-sectors
20 ISO/IEC 15504 Process Assessment Standard
23 https://clearwatercompliance.com/thought-leadership/white-papers/hipaa-compliance-software