Clearwater

Whitepaper

Enterprise Cyber Risk Management Software (ECRMS): Securing Healthcare's Digital Transformation

Table of Contents

Introduction

Explosion of healthcare data, systems and devices... and compromises!

The digital transformation of healthcare is rapidly driving the adoption of new technology and information systems to support key business and clinical initiatives. We are experiencing a veritable explosion in healthcare data, systems and devices. Healthcare data has grown by 878% since 2016[1], and the number of endpoints from which it can be accessed is growing exponentially. It is estimated that 25,000 petabytes of healthcare data will be online by 2020.[2] The Internet of Medical Things (IoMT) is expected to grow to more than 50 billion devices by 2021[3]. In addition to the external devices like wireless IV infusion pumps or heart monitors that may be attached to our patients, the IoMT includes wireless implantable devices such as deep brain neurostimulators, cochlear implants, gastric stimulators, cardiac defibrillators / pacemakers, foot drop implants and insulin pumps.

Healthcare data, systems and devices are more voluminous, more visible, more valuable and, at the same time, more vulnerable than ever. According to one survey, more than 1 in 3 healthcare organizations have suffered a cyberattack while 1 in 10 have paid a ransom.[4] In terms of vulnerability, in its April 2014 Private Industry notification, the FBI wrote "The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors; therefore, the possibility of increased cyber intrusions is likely."[5] We have certainly seen evidence of that over the last five years.

These continuing trends are resulting in even greater cyber risk exposures for healthcare organizations. In the first half of 2019, there were 285 reported breaches affecting 32 million individuals, more than double the total for all of 2018[6].

1 Dell EMC annual Global Data Protection Index, 2019.

2 https://archive.siam.org/meetings/sdm13/sun.pdf

3 https://www.i-micronews.com/products/connected-medical-devices-market-and-business-models-2017/?cn-reloaded=1

4 https://www.businesswire.com/news/home/20180523005185/en/Survey-Reveals-1-3-Healthcare-Organizations-Suffered%5D

5 April 2014 FBI PIN #: 140408-009 (U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain

6 https://www.fiercehealthcare.com/tech/32m-patient-records-breach-2019-double-all-2018-

In the wake of so many largescale data breaches, the Office for Civil Rights (OCR) has stepped up HIPAA enforcement, levying a record $28.7M in fines in 2018, representing an increase of almost 50% over 2017. Comprehensive, and high-quality risk analysis and risk management are among the highest areas of their focus as OCR official Nick Heesters recently commented:

> **"Some of the risk analysis we get back just doesn't really reflect what the rule requires. The rule requires that it be done in an accurate and thorough manner. To accurately and thoroughly assess the risks to an organization's ePHI. Frankly, that's not what we get."[7]**

Risk analysis failures and enforcement

As of this writing, an analysis of 66 OCR Enforcement Actions indicates there were 48 cases involving electronic protected health information (ePHI), where risk analysis and risk management were to have been performed by the organization who suffered the breach. In those 48 cases, OCR found 43 organizations or 90% had not completed an OCR-quality risk analysis. Forty of the 48 (83%) had adverse findings when it came to risk management. To date, OCR has collected $106.9 million in negotiated settlement amounts and civil money penalties.[8] To illustrate, following are some statements made by OCR Director Roger Severino regarding the mandate for comprehensive, enterprisewide risk analysis:

Failure to conduct an enterprise-wide risk analysis can be expensive: $3.5 million.

"The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprisewide risk analysis for a covered entity." – Roger Severino, Director, OCR[9]

Failure to update a risk analysis following changes can be painful: $3.0 million.

Two separate breaches following changes in the technology environment. "The Cottage settlement reminds us that information security is a dynamic process and

protenus-reports

7 https://clearwatercompliance.com/blog/key-takeaways-from-breakfast-breaches-d-c/

8 U.S. Dep't of Health and Human Servs., Resolution Agreements. Accessed September 1, 2019. Available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

9 HHS Press Office. Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules. February 1, 2018. HHS.gov. Accessed September 1, 2019. https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html

the risks to ePHI may arise before, during, and after implementation covered entity makes system changes." – Roger Severino, Director, OCR[10]

Warnings to Business Associates – You must conduct a comprehensive risk analysis too: $100,000.

"Entities entrusted with medical records must be on guard against hackers," said OCR Director Roger Severino. "The failure to identify potential risks and vulnerabilities to ePHI opens the door to breaches and violates HIPAA." – Roger Severino, Director, OCR[11]

State attorney generals are becoming much more active in investigating data breaches, and now banding together to initiate multi-state suits. They are working in coordination with OCR and bringing their own actions against healthcare organizations that have violated HIPAA regulations, including most recently in cases where there has been a failure to conduct a risk analysis, such as the aforementioned MIE case that resulted in an additional $900,000 being paid out in a multi-state lawsuit involving 16 State AGs. Of the 21 State AG enforcement actions that have occurred over the last few years, 16 of them (76%) involved ePHI.[12]

In addition to satisfying regulatory requirements, there is a growing need for healthcare organizations to understand where their highest exposures are in order to ensure they are protecting their assets appropriately by prioritizing and investing in the most optimal security controls to maximize their limited budgets. Despite 82% of hospitals reporting breaches, only 5% of hospital IT budgets go to cybersecurity. Financial services, which is considered much more mature in Cyber Risk Management (CRM), spends 7.1%.[13] Miniscule budgets and limited cybersecurity staff make it critical for hospitals to ensure they focus resources on mitigating their highest risks. A hospital, or other healthcare provider, can only be certain it is implementing the right controls if it knows where it has gaps.

10 HHS Press Office. OCR concludes All-Time Record Year for HIPAA Enforcement with $3 Million Cottage Health Settlement. February 7, 2019. HHS.gov. Accessed September 1, 2019. https://www.hhs.gov/about/news/2019/02/07/ocr-concludes-all-time-record-year-for-hipaa-enforcement-with-3-million-cottage-health-settlement.html

11 HHS Press Office. Indiana Medical Records Service Pays $100,000 to Settle HIPAA Breach. May 23, 2019. HHS.gov. Accessed September 1, 2019. https://www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html

12 Clearwater proprietary research

13 https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html

Third-party vendors (business associates under HIPAA) must also understand and respond to cybersecurity risks. In fact, this has become an essential part of doing business if one wants to sell its products or services to healthcare providers. As a result of the wave of vendor-related breaches, hospitals and other providers have become hypersensitive to privacy and security. They are holding their vendors accountable to much higher standards, in some cases higher than the ones they hold themselves to. As one healthcare technology firm executive said "demonstrating we can protect their data is table stakes – without it, we don't even get a shot at the business." Another referenced that his company's ability to demonstrate it has a CRM program in place that "follows the regs, gives them a competitive advantage."

Enterprise Cyber Risk Management Software (ECRMS): A better way to manage cyber risk

In response to growing threats, increased regulatory scrutiny and customer demand, leading healthcare organizations are recognizing that traditional approaches to assessing and managing cyber risk are not effective. A well-designed information security program begins with an enterprise risk analysis, which assesses vulnerabilities and risks that apply to each and every information system that maintains protected health information. It continues with an integrated risk management program, which tracks and manages risk remediation action items that ultimately reduce risk to acceptable levels.

Until recently, most healthcare organizations have struggled to execute an enterprisewide, information system-based risk analysis and risk management program as they have lacked the software tools and methodologies to do so. Without a system in place to identify and remediate high risks, these organizations face the very real potential of experiencing a preventable compromise of healthcare data, systems and devices, which can lead to fines, lawsuits, legal and other fees, disruption in operations, reputational damage and loss of customers.

> In the last couple of years, covered entities have paid $25,996,000 in fines because of breaches in their business associates and vendors, representing more than 20% of all enforcement actions.

Many healthcare organizations struggle to:

- Maintain an inventory of their healthcare data, systems and devices – many have not even identified their "crown-jewel" information assets
- Establish a common definition of risk and their cyber risk appetites
- Perform risk analysis on all information systems across the enterprise
- Assess likelihood and impact of asset-vulnerability-threat scenarios relevant to their systems
- Retain a single source-of-the-truth for risks
- Track and manage risk mitigation action items effectively
- Report on progress of risk analysis and risk response to governance functions
- Treat CRM as a continuous process

A well-designed information security program begins with an enterprise risk analysis, which assesses vulnerabilities and risks that apply to each and every information system that maintains protected health information.

Managing cyber risk in healthcare today is complex. Risk presents itself in an ever-changing threat landscape, filled with bad actors who don't play by the rules. A healthcare organization trying to manage this cyber risk without software designed for this purpose is no better off than one who is trying to manage payment processing, payroll, or electronic medical record keeping with spreadsheets.

As discussed in this white paper, a best-in-class ECRMS platform not only facilitates compliance with regulations, but also creates the basis for a comprehensive, integrated, and holistic approach to identifying, managing and reducing cyber risk across the evolving healthcare IT ecosystem. Deploying an ECRMS in a healthcare organization is no longer an option – it is a necessity in order to maintain secure operations in today's increasingly digitized health environment.

ECRMS helps ensure gaps are not missed while removing guesswork

If an organization truly wants to know where its exposures are, it must first acknowledge that each information system comprises healthcare data, systems and devices that have distinct properties, and that as a result, it must assess the

unique vulnerabilities and threats that are applicable to each of those components. The healthcare organization must evaluate and understand what components make up these systems, and which controls are in place for each of them. The process of assessing risk at the system-component level of an information system is known as an "asset-based" risk analysis, and it is seamlessly facilitated with ECRMS.

In the past, many organizations have taken a high-level approach because assessing risks at the system and component level is a highly granular process and can be difficult to execute. Performing it manually requires both tedious work as well as a strong knowledge base and expertise. An ECRMS tool, however, that is based on the NIST approach to CRM uses a built-in, proven methodology which automates much of the process and also provides the applicable risk scenarios as part of its built-in knowledge base.

Many organizations attempt to build their own surveys and Excel spreadsheets to complete risk analyses and undertake CRM. These home-grown solutions rarely scale, are not updated with ever-changing threats and vulnerabilities and provide no way in which to implement and mature an ongoing risk management program. These spreadsheets usually combine regulatory requirements such as the HIPAA Security Rule or PCI DSS with a column designated to use for some level of risk. This checklist-based approach conducted via these spreadsheets typically do not create value, have not been found acceptable evidence of compliance or security in OCR enforcement actions and, more importantly, have failed to help organizations become more compliant or more secure.

Unlike checklists and spreadsheets, an ECRMS:

1. enables the organization to comprehensively include all healthcare and other sensitive data, systems and devices,
2. uses algorithms to group system components logically according to their unique properties,
3. enables an analyst to associate these components with one or more information systems for which they are utilized,
4. employs built-in algorithms to determine potential vulnerability and threat scenarios that should be considered,
5. automatically suggests which controls (e.g. based on NIST 800-53[14]) are

14 Currently revision 4, revision 5 will be released soon.

recommended to mitigate threats exploiting vulnerabilities in these specific scenarios,

6. provides a means to assess risk based on both the likelihood of an event (based on the controls in place or not in place), and the harm that would be caused (based on the importance of the information system or its data), and
7. enables an organization to prioritize and report on risks across the enterprise in a consolidated or "drill down" manner through integrated reporting tools and dashboards

As a result, ECRMS drives a highly efficient process for performing a comprehensive asset-based risk analysis at the granular component-system level of the IT ecosystem and rating risks from most serious to least serious. It enables the analyst to perform the work faster by identifying all of the risk scenarios and controls that are relevant for those components. By analyzing risk at this level and leveraging the established algorithms of ECRMS, the healthcare organization will identity and close key gaps that it otherwise would have missed, greatly reducing risk of a compromise of healthcare data, systems and devices.

ECRMS enforces consistent risk analysis and common definitions

Risk analysis measures the effectiveness of controls in addressing asset-threat-vulnerability scenarios that are relevant for specific information systems. The process involves estimating likelihood of the compromise of confidentiality and/or integrity and/or availability of healthcare data, systems or devices and the potential impact to the organization if that compromise event were to occur. It is imperative that this risk score or rating is derived from consistent definitions of impact and likelihood. Measures of likelihood and impact can be defined within the ECRMS according to definitions provided in NIST SP 800-30 Guide for Conducting Risk Assessments[15] and then enforced consistently across the organization as various risk analysts are performing their assessments.

With a consistent definition of the criteria that results in the risk rating, the

15 National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, SP 800-30, Rev. 1 (Sept. 2012). Accessed September 1, 2019. available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

organization will have an "apples-to-apples" measure of risk, regardless of where or when the analysis was performed. Therefore, an ECRMS aids healthcare organizations in managing cyber risk consistently across the enterprise. When risk is measured the same way, and used to make security investment decisions, the organization can be more confident that its investments have been allocated to best reduce risk overall.

ECRMS results in an enterprisewide, scalable risk analysis

In announcing a $3 million settlement with Touchstone Medical Imaging, OCR Director Roger Severino stated that "neglecting to have a comprehensive, enterprisewide risk analysis, as illustrated by this case, is a recipe for failure."[16] Conducting an enterprisewide risk analysis across a large organization, which may have dozens or hundreds of information systems that span numerous hospitals, clinics, ambulatory centers, practice groups and other locations may be daunting – unless the organization is using an ECRMS.

A scalable ECRMS platform enables large healthcare organizations to define organizational hierarchies, which reflect their IT and organizational structures. This capability enables large organizations to gain efficiencies by assessing risk at a "parent" level (such as a data center) and then cascade relevant risks and controls to the child level (such as hospitals the data center serves). An ECMRS also facilitates the risk analysis at the child level for assessment of local applications or of physical controls associated with end point devices that are connected to corporate systems. In addition to improving management of risk, this segmentation helps an organization to limit the risk analysis data sets that are submitted to a regulatory authority during an investigation, thereby reducing regulatory risk to the healthcare organization.

Conducting an enterprise-wide risk analysis across a large organization, which may have dozens or hundreds of information systems that span numerous hospitals, clinics, ambulatory centers, practice groups and other locations may be daunting – unless the organization is using an ECRMS.

16 HHS Press Office. Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients' protected health information. May 6, 2019. Accessed August 28, 2019. https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html

ECRMS makes managing risk analysis as an on-going, continuous process a reality

The HIPAA Security Rule[17], as well as NIST and other standards, stipulate that a risk analysis and risk management process should be ongoing, and not performed at a single point in time. However, many healthcare organizations treat risk analysis as a once and done process. The OCR "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule[18]" is based on NIST SP 800-30 Guide for Conducting Risk Assessments and further emphasizes the requirement for continuous, ongoing CRM. When systems, technology, or processes change, an organization's risk posture becomes obsolete, leaving the possibility that current controls no longer adequately address significant risk. In order for a healthcare organization to update and document its security posture appropriately, it should be conducting risk analysis as a part of its ongoing operational security program.

Adding new systems to the IT environment

A best practice risk analysis and risk management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. For example, if an organization is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure that all healthcare data, systems and devices are reasonably and appropriately protected. An ECRMS provides a mechanism to efficiently perform a risk analysis before the new technology is brought online. This is consistent with NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations | A System Life Cycle Approach for Security and Privacy," which aligns the risk analysis and risk management process with the system development life cycle." The ECRMS will identify the risk scenarios and required controls to mitigate risks appropriately and enable "authorization to operate" and "authorization to use" decisions to be made when risk ratings fall within the organization's risk appetite. As a result, the organization can factor the cost and effort to implement these controls into its budget and project plan, while also meeting required regulations and OCR's expectations.

17 U.S. Dep't of Health and Human Servs., The Security Rule. Accessed September 1, 2019. Available at https://www.hhs.gov/hipaa/for-professionals/security/index.html

18 U.S. Dep't of Health and Human Servs., Final Guidance on Risk Analysis, available at https://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (accessed Apr. 25, 2018).

Changing use or scale of systems

An ECRMS enables an organization that materially changes the use of a system to seamlessly reassess risk in accordance with any additional impact that may be relevant to the change in scope. For example, consider a workstation that may have been previously risk-analyzed for use in one department, with access to only hundreds of patient records, that is now integrated into the EHR system, providing access to tens of thousands of patient records. This device should be risk-analyzed again to consider whether there is an increase in risk as a result of the additional harm that could be caused.

Adapting to New Threats and Vulnerabilities

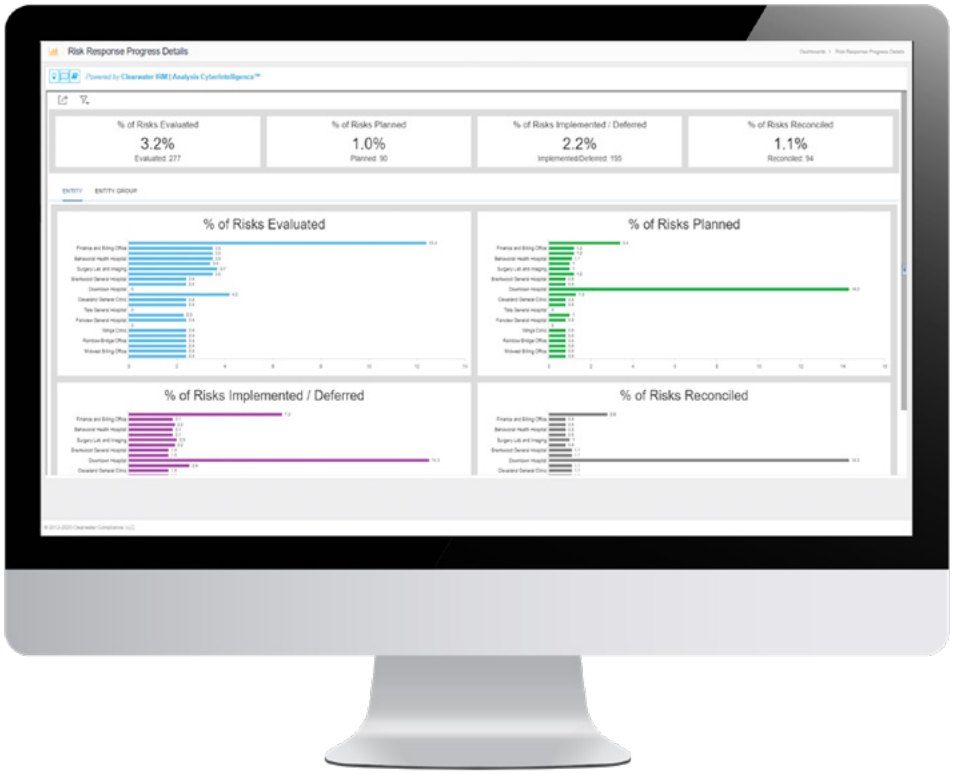
In addition to changes in technology, organizations must consider new threats and vulnerabilities as they are discovered. The risk landscape is changing on a daily basis[19] as new threats and vulnerabilities are determined to be reasonably anticipated to certain environments. A key benefit of ECRMS is that it provides periodic updates to its algorithm so the organization can assess (1) whether the current controls continue to be appropriate, (2) if the current controls provide the same level of risk reduction, (3) if any additional controls are appropriate and the extent to which they are in place, and (4) the resulting risk rating based on all of the above.

An ECRMS platform provides the capability of managing cyber risk as an on-going process, rather than at a point-in-time. As a result, the healthcare organization can be confident that its risk posture is up-to-date and accurate. Any new high risks are identified and therefore can be treated by the healthcare organization.

ECRMS matures operational reporting, analysis, and governance with better visibility

With all risk mitigation items logged and managed in a centralized ECRMS database, information security teams can use integrated reporting tools to track and manage risk remediation efforts according to different categories, such as risk level, location/entity, category, department owner, and so on. As a result, the CRM function can provide accurate and timely remediation progress and risk posture reports to senior management.

19 https://www.symantec.com/security-center/threat-report



ECRMS enables security organizations to keep the C-Suite and board apprised of the overall status of its cyber risk profile. With the ability to report on risks across the enterprise, as well as to drill down to specific control deficiencies, the risk management team's investment recommendations will be fully supported by compelling rationale.

ECRMS helps organizations effectively treat risks to reduce exposures faster

ECRMS enables organizations to make more informed risk treatment decisions (i.e., accept, avoid, mitigate or transfer), respond to risks faster and to mitigate them more efficiently. Once risk levels have been established, the healthcare organization can review each of the risks rated above its risk appetite and respond accordingly with action plans to implement mitigating controls. This may entail using the ECRMS's workflow and collaboration tools to create action plans and assign them to stakeholders along with implementation dates.

In addition to maintaining a database of all risk mitigation items, ECRMS facilitates a workflow process, whereby the assigned project owners can update progress

on risk remediation action items. An ECRMS will typically issue notifications to remind assigned individuals when work is due, as well as escalate items that are overdue. ECRMS promotes collaboration and efficiency in workflow among various stakeholders, while also bringing visibility and awareness to the status of remediation efforts. As a result, projects are completed faster, enabling quicker reduction in risk and lower costs to the healthcare organization. Importantly, the ECRMS platform and workflow enables greater cross-functional engagement in the CRM program, a key objective to transform CRM from being viewed as an "IT problem" to an enterprise risk management matter.

ECRMS enables healthcare organizations to increase ROI on security programs

An ECRMS reduces risk faster and more efficiently, while drastically improving protection of a healthcare organization's business operations, reputation, and its patients. An ECRMS facilitates a consistent, information system-based risk analysis, and as a result provides information that is critical in driving effective risk management decision making. For example, an ECRMS can tell an organization not only where it has the the most highly-rated cyber risks, but also what the most common control deficiencies contributing to those risks are.

An ECRMS can report which hospitals, divisions, information systems, or even component types present the most cyber risk to the organization. Using this information, which would not otherwise be available, an organization can optimize its resources to implement controls that offer the most benefit, i.e. the most risk reduction. Measured on a "dollars invested per risk reduced" scale, an ECRMS enables the information security team to confidently demonstrate measurable improvement and positive ROI.

Using this information, which would not otherwise be available, an organization can optimize its resources to implement controls that offer the most benefit.

ECRMS solves the resource problem and delivers out-of-the-box expertise

Across all industries, it is estimated that there will be 1.8 million unfilled cybersecurity positions by 2022 according to a number of industry reports.[20]

20 https://venturebeat.com/2017/06/07/global-cybersecurity-workforce-to-be-short-by-1-8-million-personnel-by-2022-up-20-on-2015/

Today, that number exceeds 300,000.[21] Of course this shortage affects healthcare organizations.

A healthcare-specific ECRMS solves the resource issue that commonly exists among most healthcare organizations that do not have teams available to implement a sophisticated, best-in-class risk management process. Unlike traditional Governance Risk and Compliance (GRC) programs, ECRMS implements specific CRM workflow processes based on established, NIST-based risk management standards and regulatory compliance requirements without the need for customization or configuration. These benefits are delivered out-of-the-box with all information securely stored and accessible via the cloud.

In addition to its functional capabilities, ECRMS provides a knowledge base that drives proprietary algorithms that identify asset-threat-vulnerability scenarios that are applicable to the healthcare organization's specific information systems. The database and the algorithms are maintained by the vendor, whose team of expert analysts keep these scenarios up-to-date on an on-going basis, thereby eliminating the need for the healthcare organization to have this expertise in house.

A cloud-based ECRMS enables a healthcare organization to begin assessing and responding to cyber risk immediately, thereby enabling it to improve its CRM program right away. The healthcare organization will continue to benefit from the on-going updates delivered as a service (with no software upgrades required), and as a result will continue to stay ahead of emerging threats.

21 https://www.cyberseek.org/heatmap.html

Between 2019 and 2022, unfilled cybersecurity postions are expected to increase by 500%.

ECRMS provides clear business value

As a platform that allows healthcare organizations to effectively manage the evolving risk landscape, ECRMS drives direct and indirect cost savings and value creation that is measurable and material. From senior management to IT staff managing remediation tasks on a daily basis, ECRMS streamlines and focuses resources and investments, enabling a proactive and preventative cyber security posture with an attractive return on investment.

Direct savings opportunities include reduced labor and the elimination of separate, often siloed tools. Add to that the indirect savings such as reduced cost of cyber standards compliance, better management of third-party cyber risk, among others, and ECRMS presents an even stronger business case.

In addition, as organizations contemplate adding or increasing their cyber liability insurance, there is the opportunity to lower the cost of cyber liability insurance premiums. Most insurance companies use checklists, interviews and audit-type discovery to gather data for setting coverage and premium levels. A fully deployed and actively used ECRMS platform offers organizations a compelling platform to demonstrate their improving cyber risk posture and their ability to streamline and focus the remediation process to minimize cyber risk.

Moody's, Fitch and S&P – the three leading credit agencies – have all announced they will consider an organization's cyber risk posture when determining their credit rating. Recently, as an example, Moody's downgraded the ratings outlook for Equifax, which was the target of a massive data breach in 2017 that impacted nearly 150 million people, from "stable" to "negative."[1] Keeping the cost of capital as low as possible is a benefit of a strong CRM program, enabled by purpose-built software, and could be regarded as a source of funding.

1 https://www.cpomagazine.com/cyber-security/equifax-downgrade-shows-the-lasting-financial-impact-of-a-massive-data-breach/

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact