MEDITOLOGY
SERVICES

2019
THE YEAR OF METAMORPHOSIS FOR HEALTHCARE DATA SECURITY

WHITE PAPER | JUNE 2019

TABLE OF CONTENTS

INTRODUCTION

In the world of nature, metamorphosis is the development process that many insects experience on their way to full maturity. These complex creatures typically originate in the form of an egg, with low level sophistication. They then migrate into a nymph, a middle stage of development, and later are considered adult, with fully developed systems that help the insect adapt, survive and fulfill their purpose in the ecosystem.

The current state of the healthcare data security industry can also be looked at varying stages of metamorphosis. The metamorphosis model can be used to characterize any healthcare risk management program's current stage of development and assist in setting goals for future growth and maturity.

This paper will look at the current state of healthcare IT security practices and trends and evaluate them according to three stages of metamorphosis common to insects: The Egg Stage (Beginning); the Nymph Stage (showing varying levels of maturity) and the Adult Stage (fully mature and adaptable). The analysis will also consider the latest threats to healthcare organizations from data thieves as well as the security vulnerabilities and regulatory exposures facing the industry in 2019 and beyond.

METAMORPHOSIS & ADAPTATION

The management and storage of sensitive data in healthcare can be compared to the environment in which insects are born. Insects reside and lay eggs in a variety of shelters and locations. Wherever the insect can exist, it is likely to leave offspring to proliferate its life form. This happens in the transmission of healthcare information as the adoption of ever-emerging technologies and dependence on third-party services results in data proliferation and replication of sensitive patient data.

Healthcare entities have evolved from storing patient information in paper forms (or a single primary electronic health record system) to sharing and storing patient information in hundreds of applications both internally and externally with third-party Business Associates. Data is also maintained in medical devices, telemedicine applications, and mobile applications as patient care moves away from traditional inpatient and outpatient settings into the patient home. This data sprawl, (proliferation and replication), makes it extremely difficult for healthcare security professionals to secure data everywhere it resides. However, if an organization can adapt, systems can be designed to adjust and deal with data sprawl as the risk management program matures.

THE STAGES OF METAMORPHOSIS IN HEALTHCARE DATA SECURITY

Let's consider the stages of insect metamorphosis to think about the maturity and adaptation that organizations must implement to adapt to the labyrinth of sensitive data that has evolved in the healthcare ecosystem. There are three stages in insect metamorphosis, the Egg, the Nymph and the Adult Stage. Let's take a look at each stage in terms of healthcare security program adaptation.

THE EGG STAGE

In the Egg Stage, the insect is at inception and contained in a sac that protects it and is located near a food source. For a healthcare data security program, the Egg Stage could be characterized as the inception point of assigning formal responsibility and oversight for the cybersecurity and compliance functions. Healthcare security programs in this stage may typically be driven by paper-based security polices and may have only basic security controls defined.

Healthcare security programs in this early stage tend to be focused predominantly on compliance drivers for the security program including HIPAA, Meaningful Use, and MACRA obligations. The responsibilities for security program implementation are frequently decentralized and distributed across Information Technology and other departments.

Organizations at this stage may be fairly consistent in providing HIPAA-based training to the workforce and maintaining formal security policies and contractual obligations with third-parties. However, they may also be lacking in implementing robust security controls that align with industry standards like NIST and HITRUST to adequately protect sensitive patient information and systems.

Healthcare entities in this early stage often under-invest in information security protections for critical risk management areas like third-party risk management, audit logging and monitoring, incident response, and enterprise-level risk analysis processes.

Indeed, many healthcare organizations are still in the inception stages of their security program development. The U.S. Department of Health and Human Services (HHS) reported recently that 3 out of 4 hospitals lack a designated information security representative.[1]

Healthcare entities have also experienced record-breaking breaches and fines levied by The Office for Civil Rights (OCR) for failures to adapt fundamental security controls and HIPAA compliance mandates. Two organizations receiving HHS fines of $3 Million in recent years were Cottage Health and Fresenius Medical Care North America (Fresenius). These provide an example of organizations in the Egg Stage.

In both cases, the HHS cited the lack of thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI and lack of security measures as the justification for the HIPAA violation fine.[2]

OCR Director Roger Severino commented on the Fresenius breach involving five affiliate locations, "The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity. Covered entities must take a thorough look at their internal policies and procedures to ensure they are protecting their patients' health information in accordance with the law."[3]

In presentations at HIMSS in 2019 and HIPAA Summit[4], OCR representatives highlighted compliance trends that further indicate that many healthcare entities remain in early stages of maturity. The OCR noted that breaches and hacking incidents are on the rise including email-based attacks; however, many Covered Entities still lack effective enterprise risk analysis and remediation tracking processes to identify and correct security weaknesses in their environments. The OCR representatives also noted a trend for ineffective inventory, tracking, and assessment of third-party Business Associates.

Healthcare entities in this early stage often under-invest in information security protections for critical risk management areas like third-party risk management, audit logging and monitoring, incident response, and enterprise-level risk analysis processes.

THE NYMPH STAGE

As insects mature into the Nymph Stage, they develop a more sophisticated body and exoskeleton, but still do not reflect a fully developed adult (with more defense features such as hardened skeletons and wings).

For healthcare data security programs, the Nymph Stage represents those organizations that have moved beyond purely compliance-focused programs and have begun to establish risk-based security models aligned with industry security standards like the NIST Cybersecurity Framework (NIST CsF) and the HITRUST Common Security Framework (HITRUST CSF).

Security programs in this middle stage of maturity often have dedicated, qualified security teams and well-defined security plans and procedures. However, organizations in this stage often struggle with a lack of comprehensive controls and processes to protect data across the entire ecosystem both internally and externally.

Organizations in this stage may provide reasonable security protections for core infrastructure and primary electronic health records systems and applications, but they may also struggle with keeping track of data as it proliferates among internal business functions and hundreds of third-party business partners and their supporting information systems and processes.

As a Nymph Stage healthcare organization moves closer towards full maturity, the scope and scale of risk is better understood through the execution and tracking of enterprise-level risk assessments for any areas where sensitive information may reside. These middle-stage programs may have wide range corrective action and remediation plans and a multi-year outlook to prioritize and sequence security improvements.

Nymph Stage organizations also begin to conduct more targeted approaches to security and compliance education for specific departments with access to sensitive information including Information Technology, Finance, biomedical, and clinical functions. There is usually some form of formal security and compliance governance processes defined and security program progress is actively reviewed. Investments and resources for security protections are also planned out in this stage.

But even with the increased security controls, there often remain critical- and high-risk security and compliance exposures that could lead to high profile breaches of sensitive information and systems. Organizations in this stage are also continually playing "catch up" with known security control gaps and struggle to stay ahead of emerging threats and security control mechanisms.

These middle-stage programs often have risk-based security models based on industry standards in place like NIST and HITRUST as well as a wide range corrective action and remediation plans to sequence security improvements. Still, they may be playing "catch-up" with known security gaps and struggle to keep ahead of emerging security threats.

THE ADULT STAGE

For adult insects, their bodies have reached maturity, providing the maximum level of protection. They are not impervious to all forms of attack and malady, but their rate of survival is substantially increased by virtue of the maturity of the physical and behavioral protections they have developed as adults.

For example, caterpillars in this stage have cocooned and emerged as beautiful and adaptable butterflies, which can fly away from most prey. In the case of the Monarch butterfly, the Adult Stage consists of a long and complex migration across North America to fulfill its role and purpose in life. Like the Monarch butterfly taking flight, a fully mature healthcare information security program is a beautiful thing to see fly.

In an Adult Stage organization, a healthcare security program is proactively managing risk, laying out its own flight pattern that assures the greatest success. These organizations frequently measure and proactively manage risk through targeted and enterprise risk analyses, ethical hacking and technical penetration testing, and integration of security into core business functions on a day-to-day basis. Risks are identified, prioritized, tracked, and progress is reported to leadership and other key stakeholders to validate effective remediation. Governance processes for Adult Stage security programs include the reporting of well-defined metrics and key risk indicators and active engagement from senior leadership for the healthcare entity.

Adult Stage security programs also adapt to learn from the attacks and response approaches from other peer organizations. This often includes maintaining a network of intelligence gathering and protection models including threat data sharing, monitoring, and alerting that allow for quick and effective responses to attacks from predators. Mature healthcare data security programs also tend to have incident response plans established and regularly communicated and tested to bolster the organizations resiliency against inevitable attacks. These response practices also include targeted threat simulations including email and phishing-based attacks and response exercises including on-the-spot education and training to heighten end-user awareness of security threats.

These more mature programs tend to have a robust set of security protection tools including an integrated portfolio of technical capabilities and well-defined processes, roles, and responsibilities for effectively using security tools to manage risk.

Another common characteristic of an Adult Stage security program is the acquisition and maintenance of information security certifications. These certifications reduce the resource efforts needed to meet compliance requirements and to communicate security standards to business partners, investors and other stakeholders. Common healthcare security program certifications include HITRUST CSF certification, NIST CsF certifications (available via the HITRUST Alliance), and SOC 2 Type 2 attestations.

A key indicator of security program maturity is the ability of the organization to move beyond basic security controls adoption and compliance and into a model that supports effective risk-based decisions around security investments. Mature security programs are a vehicle for enabling the business, protecting patients and the company brand, and supporting effective enterprise risk management.

MATURATION OF SECURITY PROGRAMS

EGG STAGE

LEVEL 1

Few-to-no controls
(i.e. relying on policies)

- Security policies defined
- Ad hoc security controls, inconsistently applied across the organization
- Decentralized security responsibilities across IT/other functions
- Limited scope or application-focused risk assessments
- Point security solutions (e.g. anti-malware, email encryption)
- Sporadic assessments of third-party Business Associates
- Annual HIPAA education and training for the workforce

NYMPH STAGE

LEVEL 2

Informal, unenforceable or not comprehensive controls and processes

LEVEL 3

Process and /or technology controls implemented and operating correctly

- Dedicated and qualified security leadership and team
- Alignment with a security standard like HITRUST or NIST
- Routine organization-wide risk assessments and remediation tracking
- Documented security plans and procedures
- Some security metrics tracked and reported
- Policies routinely reviewed and updated
- Assessments conducted for new products, services and Business Associates
- Targeted security and compliance education for specific departments
- Governance-based security program metrics reported to leadership

ADULT STAGE

LEVEL 4

Periodic, regular testing and evaluation of the controls

LEVEL 5

Integration of controls and business processes (i.e. defined, tracked metrics reported to executive management regularly)

- Security team depth including leadership, management, and specialized resources
- Metrics, KPIs, and KRIs routinely generated and automated
- Proactive audit logging, monitoring, and response
- Routine incident response testing
- Integrated portfolio of security tools
- Formal risk management program that normalizes and prioritizes risks from all sources
- Formalized third-party risk management program
- Routine ethical hacking and penetration tests
- Robust training and education, phishing simulations
- Governance-based risk management decisions
- Certified in one or more security frameworks (HITRUST, SOC 2, NIST CsF)

PREDATORS: DATA THEIVES

Insects face many varied threats from other insects, birds, reptiles and mammals like the anteater and even humans. Survivalist trainer, Bear Grylls, is famous for his knowledge of edible insects that can provide protein and nutrients for human survival. Even plants, such as the Venus fly-trap, can be deadly.

Likewise, healthcare data is on the menu for a varied group of thieves seeking to monetize on the rich "nutrients" found in personal and sensitive data. There are several groups of threat actors operating within healthcare organizations to steal, compromise and control sensitive patient data. A threat actor is an entity that is partially or wholly responsible for an incident that impacts, or has the potential to impact, an organization's security with respect to the information they hold.

Below is a list of some common threat actors associated with compromising the confidentiality, integrity, or availability of healthcare resources:

Financially-motivated malicious outsiders (e.g. organized crime)

Nation States (malicious outsiders)

Hacktivists (malicious outsiders)

Terminated workforce

Insiders: non-malicious & malicious

Environmental factors

TYPES OF THEFT

Common uses for stolen data include identity theft of financial information as well as medical identify theft of personal treatment information. These types of information can be used for financial theft, medical insurance claims fraud, and the fraudulent acquisition and sale of prescription drugs on the black market.

Theft is more likely to occur on devices and systems which distribute information across a variety of locations such as medical and IoT devices, remote access platforms, mobile devices, patient portals and third-party devices, services and providers.

Tactics Used to Steal Data

Insects face creative predators that can trick or lure them into traps, such as the plants that offers a delicious nectar, but then close and trap the insect. Often called threat vectors, specific tactics are used to enable an individual to gain access to information systems with an intent to disrupt operations or obtain protected information. These methods could directly result in the loss of the confidentiality, availability, or integrity of the data belonging to healthcare entities.

Common threat vectors within the healthcare environment:
Ransomware
Hacking
IT Systems Failure
Environmental
Unintended or Accidental Disclosure
Malware
Phishing
Social Engineering
Unauthorized Access
Distributed Denial of Service (DDOS)

HEALTHCARE VULNERABILITIES

Just as a spider spins a web to catch many unsuspecting insects, data predators spin their own clever traps to capture data from patients in healthcare settings. Ransomware and malware continue to infest the industry; with malicious actors continually inventing and re-inventing novel ways to bypass security controls.

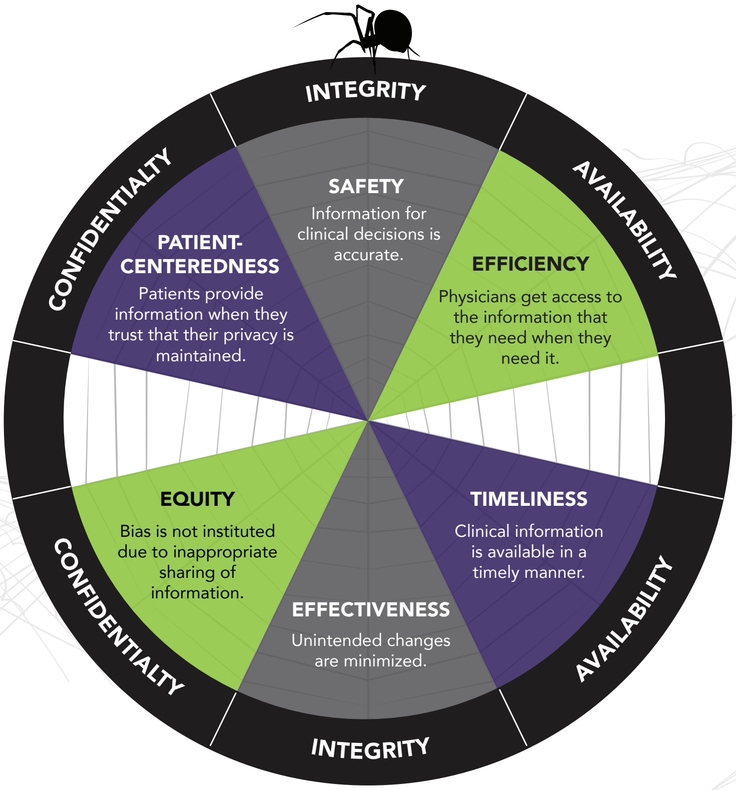
Threat actors have created elaborate and convincing phishing email schemes to trick users into providing credentials and other unauthorized information. In a 2019 HIMSS study, 59% reported that email phishing was the initial point of data compromise for all organizations surveyed, and 69% of incidents at hospitals.[5]

In healthcare settings, the impact of successful breaches extends well beyond concerns about compliance and data loss as these events have the potential to adversely impact patient safety. Quality patient care is increasingly dependent on quick access to healthcare information. This information access opens new data security vulnerabilities.

There are indicators that the health care industry lags significantly behind other regulated industries in securing and protecting sensitive information. Healthcare is 30% more likely than the financial industry to have sensitive assets stolen, 17% more likely to experience a security incident related to employee errors, and 20% more likely to experience an incident related to the misuse of privileged access.[6] This state of affairs creates an increased likelihood that medical device security may continue to lack effective security.

Attacks are often indiscriminate and use malware that affects unpatched systems. Loss, corruption, and interception of data can endanger the lives of patients. Failure to protect the confidentiality, integrity, and availability of healthcare data systems and the sensitive information they maintain has the potential for broad-reaching business and clinical impacts.

Maintaining Confidentiality, Integrity, & Availability of Healthcare Data Systems


INTEGRITY
AVAILABILITY
CONFIDENTIALTY
SAFETY
Information for clinical decisions is accurate.
EFFICIENCY
Physicians get access to the information that they need when they need it.
PATIENT-CENTEREDNESS
Patients provide information when they trust that their privacy is maintained.
EQUITY
Bias is not instituted due to inappropriate sharing of information.
TIMELINESS
Clinical information is available in a timely manner.
EFFECTIVENESS
Unintended changes are minimized.
CONFIDENTIALTY
AVAILABILITY
INTEGRITY

Mobile malware and AI-powered cyberattacks are becoming more common as patient data is increasingly stored in off-site locations and systems. Predators will continue to leverage the trend of remote data storage to their advantage in hijacking and using sensitive patient data for financial gain. A planned approach to risk identification and reduction across distributed devices is necessary to move a security risk management program to a higher maturity level.

Impact of Data Sprawl

Data sprawl means data can live virtually anywhere in the healthcare electronic ecosystem including patient care settings, financial applications, and many and varied business support systems. Adaptation to data sprawl is imperative to better manage sensitive data as it traverses our healthcare delivery system.

As the use of IoT technologies, medical devices and cloud storage grows, valuable data assets are increasingly being stored in new and more vulnerable arenas. Even more concerning is that healthcare organizations commonly lack capabilities to track the movement of a patient's data across a complex network of Business Associates.

The distributed design of healthcare delivery networks means that each location has varying levels of security protections. Data predators (criminals) are aware that valuable healthcare data is often insecure because of this highly fragmented data storage and transmission ecosystem. These malicious actors will often take the "path of least resistance" and attack peripheral data and systems rather than aiming for networks and applications that have more fortified protections.

Emerging Threats

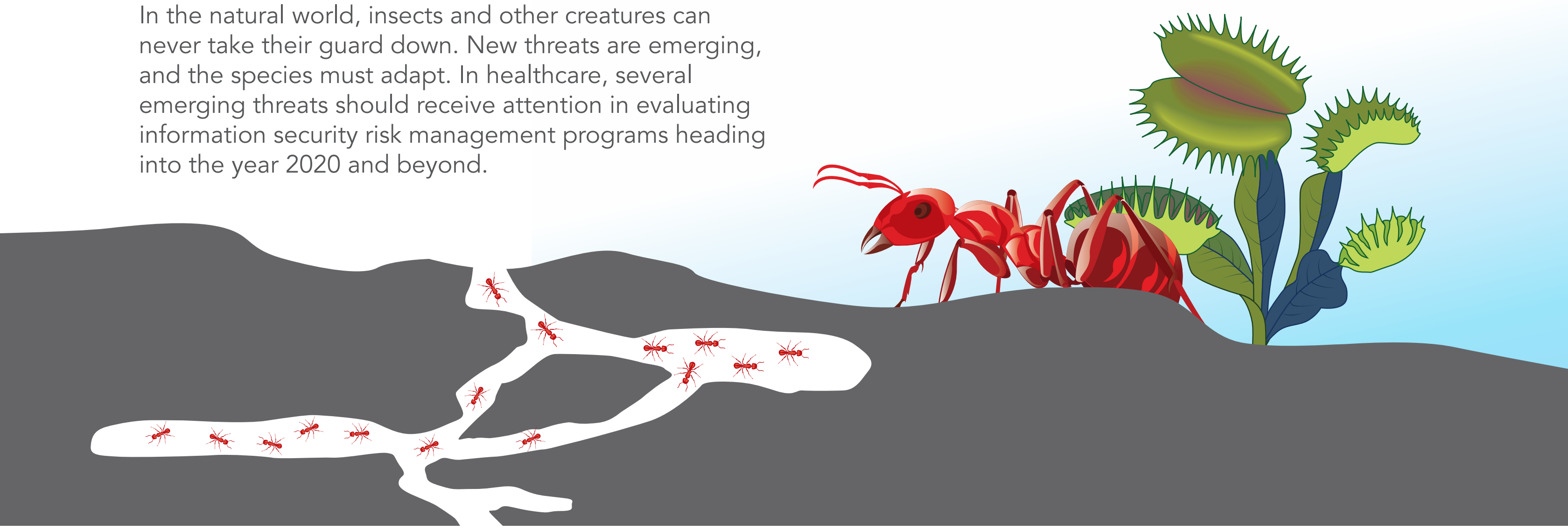
In the natural world, insects and other creatures can never take their guard down. New threats are emerging, and the species must adapt. In healthcare, several emerging threats should receive attention in evaluating information security risk management programs heading into the year 2020 and beyond.

Widespread use of medical devices and IoT devices have escalated the spread of data proliferation and thus create new vulnerabilities in data security. Medical and IoT devices typically in use in healthcare settings fall into several categories including monitoring (blood pressure, temperature, glucose levels), diagnostic (ultrasound, MRI), treatment (infusion pumps, LASIK, etc.), therapeutic, analytical and life sustaining devices.

Devices that are directly connected to patients can be reconfigured by malicious attackers to deliver lethal dosages of medications, prevent life-saving alerts, or rendered completely useless through ransomware and other similar attacks. In addition to physical harm, many networked medical devices can be a gateway to a healthcare organization's domain, opening the door to a trove of protected health information.

The 2017 WannaCry ransomware attack was a high-profile example of malware impacting medical devices on a large scale. Although most impacted health systems were in the United Kingdom, the attack served as a warning sign to health systems across the globe that security protections for medical devices remain woefully insufficient.[7]

Home health care and telemedicine delivery networks are also changing the landscape of healthcare data security. This is transforming healthcare delivery and shifting devices and information into the patient home setting. It was already challenging to secure devices within the confines of healthcare provider and business settings, now increased attention must be placed on new security methods that will work with remote healthcare devices and mobile applications.



Cloud data storage can provide a false sense of security. Simply because data has shifted to the cloud does not mean that data security is at its highest level or at the standard of healthcare compliance. Securing cloud-based platforms requires shared responsibility between healthcare entities and the vendors and platforms that host sensitive patient information. For example, access controls and configurations must be actively managed. Remote access must be controlled through multi-factor authentication, and systems require continual monitoring to detect and prevent the escalation of cyberattacks on cloud infrastructure. Attainment of security certifications is fast becoming table stakes for healthcare applications and Business Associates to provide more assurance that data stored within cloud-based systems are meeting the required standards for PHI security.

All three of these emerging threats involve using third-party service solutions. Thus, the role of third-party risk management has become an essential component of data security programs and forward-looking strategies. Mature organizations understand the importance of third-party data security and allocate resources to identify, remediate and report on third-party data vulnerabilities for new and legacy products and services.

MATURATION: MOVING TOWARDS MATURITY

A central goal of any security risk management program is to reach maturity, so your program can truly "spread its wings and fly". To migrate to more mature stages, there are three focus areas to address in your security risk management program: regulatory compliance activity, managing information risk and preparing for cyberattacks. Let's look at each of these areas more closely.

Regulatory Compliance Activity

The OCR enforcement of the HIPAA Security Rule and Privacy Rule remain at the top of the food chain for healthcare regulatory compliance activity. However, the OCR has evolved to become more efficient in their audit process. Going into 2019 much of their audit and investigations focus on the most egregious cases.

Performing regular (i.e. at least annual) security risk analysis on your organization's information security policies, procedures and systems is a foundational expectation in HIPAA regulatory mandates. Security risk management programs must include risk registers that are updated more frequently than just annually to capture new vulnerabilities and related remediation activities as they arise.

Risk registers provide a method of documenting each identifiable risk event or vulnerability point in the organization, including those with Business Associates. A regularly updated risk register provides the OCR evidence of a continual risk management program. Update the risk register anytime a new security risk identified (e.g. new technology added or new business systems). Use the risk register as a way to continually prioritize and track remediation of identified risks throughout the year.

Driven by data sprawl, healthcare regulatory approaches must also expand to evaluate International influences such as the Privacy requirements of Europe's Global Data Protection Regulation (GDPR) mandate. These latest regulations provide frameworks that "follow the data" and require privacy and security protections wherever that data may reside. Healthcare organizations must have a clear understanding of their entire health delivery system and how data is stored and moved throughout the system.

RISK REGISTER COMPONENTS

The Risk Register provides a list of potential data security risks and evaluates each by:

- ✓ Likelihood of occurrence
- ✓ Potential impact
- ✓ Maturity level of security control
- ✓ Overall risk score
- ✓ Priority
- ✓ Remediation Status

Managing Information Risk

A key element in evolving risk management is changing security processes and procedures to follow the data and apply security protections to sensitive organizational data wherever it may roam. In the early Egg Stage of program development this may be as simplistic as maintaining an inventory of applications that store and maintain PHI and applying appropriate security controls. In the Nymph or Adult Stage, focus shifts to developing formal data governance programs that track data throughout its complete lifecycle within and outside the organization. Not all information is created equal; mature security programs have meaningful data classification schemes and protection mechanisms that calibrate the level of security protections to the relative sensitivity of the data.

Planning and Testing

A strategic approach to planning and testing the security program is another hallmark of an advanced stage of development. By implementing a multi-year plan, information security stakeholders can clearly see the priority level for each security initiative and determine how resources should be allocated to meet specific goals.

Routinely evaluating the security program against security frameworks is also feature of "Adult" (mature) security management programs. These programs leverage security frameworks such as HITRUST and NIST to benchmark and measure the security program's breadth and the organization's level of preparedness for cyberattacks and incidents.

Manage Infrastructure and Internal Issues

Developing a suitable exoskeleton is critical as an insect reaches maturity. As it reaches maturity, insects develop a structure which provides additional defenses (e.g. butterflies grow wings, beetles develop a hard shell).

In healthcare information security, a formal information security risk management program is what gives an organization its core strength and defense design against predator attacks. The security program infrastructure must also be somewhat flexible in order to adapt and survive through mergers, acquisitions and new business affiliations.

And it's not just predator attacks from outside healthcare organizations that security teams must protect against; data thieves often lurk within healthcare entities (e.g. workforce members system access). Perhaps there is a hornet in your productive bee hive that needs to be exterminated. Internal actors represent 56% of data security breaches according to Verizon's 2018 Data Breach Investigations Report.[89]

Since most organizations leverage cloud-based services and third-party solutions, the security infrastructure of outsourced services has become a critical area to assess and monitor. In November 2018, the Ponemon Institute reported that among U.S. firms surveyed, 61% experienced a breach caused by third parties, which is up from the previous year at 56%. Even as third-party data breach activity continues to grow, only 46% of firms surveyed said managing relationship risk is a priority.[10]

> In healthcare information security, a formal information security risk management program is what gives an organization its core strength and defense design against predator attacks.

61%
experienced a breach caused by third parties

only
46%
said managing relationship risk is a priority

Leverage Security Technology

Data sprawl centers on data replication and proliferation. Remember those pesky insect eggs laid everywhere? Technology can help secure data as it proliferates in more and more unexpected locations and environments by automating security risk identification and remediation. Security automation solutions can help organizations stay ahead of security threats such as ransomware, phishing, mobile malware and AI-powered attacks.

Emerging technologies such as blockchain and artificial intelligence are piquing the interest of security risk managers grappling with how to deal with even more data sprawl. In the future, blockchain technology (with built-in encryption features) may become part of the backbone of healthcare information exchanges (HIEs), insurance/payment solutions and asset management services. Experts are watching the progression of blockchain against cloud databases, to see which system will emerge as a preferred information distribution system.[11]

Preparing for Cyberattacks

Mutation and resiliency are two important survival methods insects use to better prepare for environmental threats and predators. Healthcare organizations must also "mutate" their security and privacy programs to be better prepared for unpredictable, emerging threats. They must be ready to "morph" their security and privacy approaches to be a more resilient "species".

Security leaders must regularly ask themselves: "How well prepared are we for a cyberattack? Could our organizations be healed and bounce back from a cyber-attack? How long and difficult would it be?"

There are a few strategies that can help to create a more resilient and alert security function.

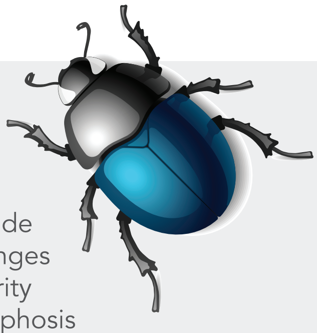
Identify and Evaluate Potential Threats

Keeping your "ant antennas" or radar up is key to identifying new data predators, threats or environmental vulnerabilities. Just as many insects share information in a "colony", security leaders can share threat intelligence in cyber-threat intelligence sharing groups. If you do not know where to start, check with your regional healthcare security and information security networking groups.

Incident Response Planning

Resiliency is the underlying goal of an incident response plan (IRP). Updating an incident response plan may get overlooked in the myriad of security risk assessment and remediation tasks, but it is key to bouncing back after a cyberattack.

Involve the "whole colony" in testing the plan. This means that Incident Response Planning also includes incident response education and testing. Security teams are getting better at training, communication and involving the business and clinicians in Incident Response Planning. This is critical to organizational adaptation and survival as new data threats and predators are coming on the scene all the time.



CONCLUSION

Like insects, healthcare organizations are complex creatures grappling for survival against a wide array of predators seeking to impair, consume or destroy them. Insects approach these challenges by using metamorphosis and adaptation to strengthen their defenses and escape harm. Security and compliance professionals within healthcare may benefit from understanding the metamorphosis stages of a data security program. Security programs can be viewed by their stage of maturity, which helps give a clearer picture of how to adapt and structure their security systems going forward.

ABOUT MEDITOLOGY SERVICES

Meditology Services is a top-ranked provider of information risk management, cybersecurity, privacy, and regulatory compliance consulting services exclusively for healthcare organizations. Our organization was named the top-ranked provider in the healthcare industry for Cybersecurity Advisory Services in the 2019 Best in KLAS: Software & Services Report. We service hundreds of healthcare clients coast-to-coast and maintain offices in Atlanta, Philadelphia, Nashville, Denver, and San Diego.

info@meditologyservices.com | MEDITOLOGYSERVICES.COM

MEDITOLOGY
SERVICES

Meditology Services, LLC
5256 Peachtree Road, Suite 190
Atlanta, GA 30341

REFERENCES

[1] Davis, J. (2017, May 19). Healthcare is Facing a Security Staffing Crisis. *HealthcareITNews*. Retrieved from: https://www.healthcareitnews.com/news/healthcare-facing-security-staffing-crisis-hhs-says

[2] Office of Civil Rights, H.H.S. (2019, Feb. 7). Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million. [Press Release]. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/cottage/index.html

[3] Office of Civil Rights, H.H.S. (2018, Feb. 1). Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules. [Press Release]. Retrieved from: 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

[4] Mosley-Day, S., Office of Civil Rights, H.H. S. (2019, March 4). HIPAA Enforcement Ongoing Patterns of Non-Compliance. HIPAA Summit 2019 Conference presentation. Washington, D.C.

[2] Office of Civil Rights, H.H.S. (2019, Feb. 7). Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million. [Press Release]. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/cottage/index.html

[3] Office of Civil Rights, H.H.S. (2018, Feb. 1). Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules. [Press Release]. Retrieved from: 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

[4] Mosley-Day, S., Office of Civil Rights, H.H. S. (2019, March 4). HIPAA Enforcement Ongoing Patterns of Non-Compliance. HIPAA Summit 2019 Conference presentation. Washington, D.C.

[5] HIMSS. (2019). *2019 HIMSS Cybersecurity Survey Report*. Retrieved from : https://www.himss.org/sites/himssorg/files/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

[6] Verizon. (2016). *Verizon 2016 Data Breach Investigations Report.* Retrieved from: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[7] Syal, R. (2018, Feb. 5), Every NHS trust tested for cybersecurity has failed, officials admit. *The Guardian.* Retrieved from: https://www.theguardian.com/technology/2018/feb/05/every-nhs-trust-tested-for-cyber-security-has-failed-officials-admit

[8] Donovan, F. (2018, April 11). Healthcare Industry Worst in Stopping Insider Data Breaches. *HealthcareITSecurity.com.* Retrieved from: https://www.theguardian.com/technology/2018/feb/05/every-nhs-trust-tested-for-cyber-security-has-failed-officials-admit

[9] Verizon Enterprise Solutions. (2018, April). *Verizon's 2018 Data Breach Investigations Report (DBIR).*11th Edition. Retrieved from: https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report.pdf

[10] Ponemon Institute, LLC. (2018, November). *Data Risk in the Third-Party Ecosystem*. Retrieved from: https://www.ponemon.org/library/data-risk-in-the-third-party-ecosystem

[11] Garrity, M. (2019, April 19). Blockchain to Emerge in 5 to 10 Years. *Becker's Health IT & CIO Report.* Retrieved from: https://www.beckershospitalreview.com/healthcare-information-technology/blockchain-to-emerge-in-healthcare-in-5-to-10-years.html