InfoAssure, Inc.

The Trusted Source for Information-Centric Security

Persistent, Vigilant Data Protection
Anywhere-Anytime

Information-Centric Security

InfoCenSec®

Enterprise *InfoCenSec®* Ecosystem

2017

James G. Lightburn, CEO
j.lightburn@infoassure.net
410.991-9611

© 2014, 2015, 2016, 2017 All Rights Reserved InfoAssure.com, Inc.
www.infoassure.net

Enterprise InfoCenSec® Ecosystem:

The Information-Centric Security (InfoCenSec®) approach to data security shifts the priority to the high value data or info object itself. Also to monitor, audit and control people and extend from only the current approach of logical protection of devices or networks to safeguard data. The core concept of InfoCenSec® is that the data object can be **persistently protected** or **always on protection** and should remain so at rest and in motion, at all times, wherever it goes or wherever it is stored. This process transforms data into self-protecting objects which in turn can be trusted objects. The InfoCenSec® approach enables role based access control which is a more efficient and cost effective enterprise solution to data privacy compliance because it allows for protection at the data object level independent of the application, device and network. The device, network perimeter status quo security approach in place today has proven to be resource dependent and expensive to manage with limited protection results and serious consequences resulting from major data breaches.

With the InfoCenSec® approach the data protection policy is burned onto the data object regardless of what application produced it or where it is stored or goes. The information centric security model also means that each data element contains access policies that explain the rights of users and the actions that can be taken on that data object and these policies are embedded with the data itself, thus transforming the data into a self-protecting data object. The Enterprise InfoCenSec® Ecosystem is evergreen and it is an integrated combination of related and interdependent capabilities. **Figure 1** depicts the integrated evergreen components that make up the InfoCenSec® Ecosystem.

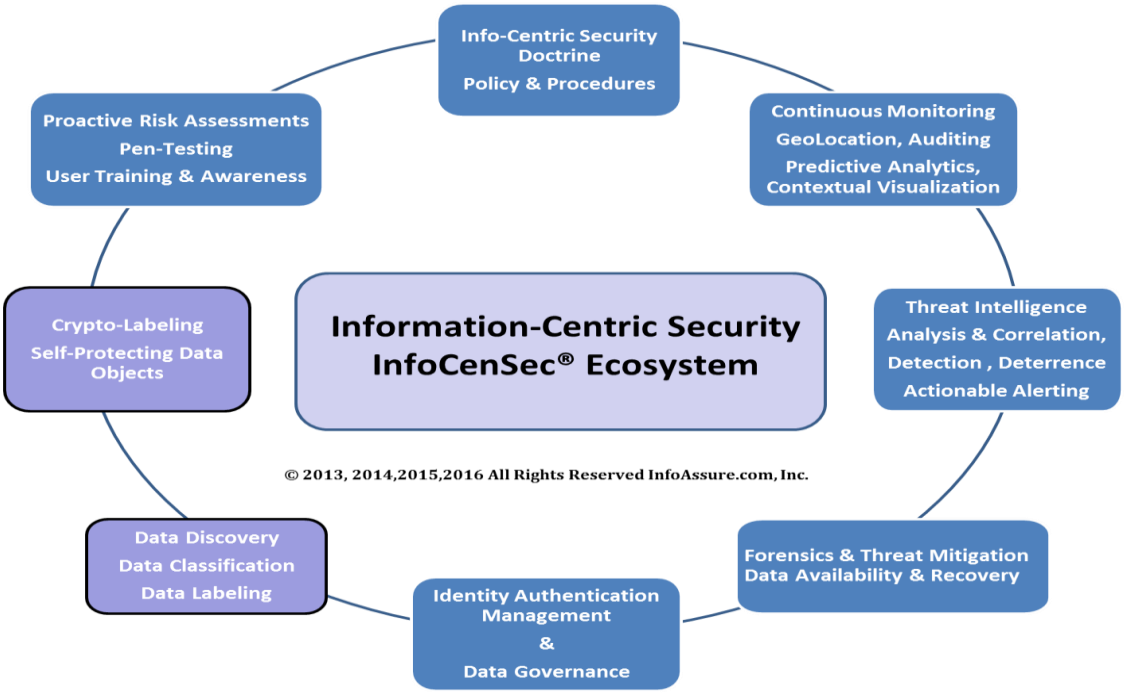

Figure 1: InfoCenSec® Ecosystem Components

InfoCenSec® Ecosystem components:

- **InfoCenSec® Doctrine, Policy & Procedures**

InfoCenSec® Doctrine is simply embracing the fact that a data breach will happen and implementing tactics, techniques and procedures to reduce the impact and consequences when it does happen. This policy development and oversight needs to be a top priority for the board of directors, the senior leadership and ultimately every employee of the Company.

The Info-Centric policy and procedures are the official enterprise statements of authority and guidance on InfoCenSec®. They are the defined procedures to follow to enforce policy and to keep the enterprise in compliance with privacy enforcement. It is recommended that both the policy and procedures documents are signed off on by all of the C-level management team. Further, all employees full and part time, consultants, business associates and contractors should be required to read and sign a statement that they have read both policy and procedure documents and agree that they will abide by them. This agreement will also have legal wording that gives the Company full power to terminate the employment or contract if the terms and conditions are violated.

- **Data Discovery & Data Classification**

The first step in implementing an InfoCenSec® plan is to know what data you have, where it lives, who uses it, what level of sensitivity it has and then classify and label it for producing a crypto wrapping label. The data discovery and classification process should be concurrent with the enterprise info-centric risk planning. The data discovery and classification tools available today can crawl throughout an enterprise and identify all data both structured and unstructured. The logical access control tools for structured data are much more mature than with unstructured data. Also most of the mobile data will initially be unstructured and thus the initial focus for data object crypto protection should be on mobile data and unstructured data.

- **Crypto-Labeling & Self-Protecting Data Objects**

The crypto labeling process transforms data into self-protecting data objects. The crypto labeling process is based on "information-centric" security architecture where authorized users/members have access to specific information content based upon a "need-to-know" or role based methodology. One crypto labeling technique uses a combination of symmetric and asymmetric cryptography for layered protection which is very powerful. The self-protecting data system protects information at the object level while supporting information sharing across the enterprise creating virtual Communities of Interest (vCOI).

The crypto labeling process empowers the <u>data owner to control</u> <u>who</u> can see <u>what data</u>, on <u>which device</u>, <u>when and where</u> especially when in the cloud or on mobile devices.

Armoring your data with crypto labeling means that the system administrators (trusted insiders like Edward Snowden-NSA case) no longer have unauthorized access to your data on the servers that they manage. The same can be true for protecting your data in the cloud.

The crypto labeling process and self-protected data object reduces the consequences and impact of the trusted insider data theft and breach. The crypto labels are applied to the member's roles/duty, devices and data object based on risk management and privacy compliance enforcement policies. The crypto labeling process is capable of providing assured data protection, data separation (information domains), and data access controls for information at the object level. Crypto labels can also be applied or embedded into network and sensor systems resources. This object level access control and protection is possible by controlling the assignment and distribution of crypto "Labels" (protected cryptographic keys) to authorized and authenticated users/devices enrolled into the crypto labeling key management system.

The crypto labeling process provides a unified management solution for digital object access control. This process enables access control of digital assets based on Role-Based Access Control (RBAC) of the user, Content-Based Access Control (CBAC) on information content of the objects and Device Based Access Control (DBAC). RBAC, CBAC and DBAC functionality can be easily implemented using Crypto Label assignment management. The crypto labeling servers implement an "information-centric" security architecture where authorized members have access to specific information content based upon a "need-to-know" methodology.

Labeled encryption keys are distributed to Client workstations based on the individual user's authentication; authorized access privileges and "need-to-know" for document and data object encryption and decryption. With object level encryption the keys are created at the time a user clicks on the data object and attempts to open it. <u>There are no keys to store or manage</u>.

The crypto labeling provides both data-at-rest and data-in-transit protection end to end. It incorporates a cryptographic data object labeling process and cryptographic key management technology to enforce access control and privacy at the object level. The crypto labeling process transforms data objects into self-protected objects before storing it in the cloud. The crypto labels need to be hashed or burned to the data object to insure the crypto labels stay with the object persistently. This hashing keeps the access control policy embedded with the encrypted data object and provides integrity of the encrypted object anywhere-anytime. This process results in a trusted data object.

The crypto labeling allows "the data owner" to establish virtual Communities of Interest (vCOI) or a Circle-of-Trust™. Only approved members access your data in the Cloud or on a mobile device anywhere-anytime. A vCOI can be as simple as you, family, or friends or as complex as a hub-of-commerce or a research collaboration with global research entities. **<u>The bottom line is that by applying crypto labels to any data object, it transforms that data object into a "self-protecting trusted data object" with persistent protection anywhere-anytime.</u>**

- **Continuous Monitoring, Auditing, GeoLocation, Predictive Analytics, Contextual Visualization Analysis**

The enterprise IT environment is complex and distributed and often major portions have been outsourced to a systems contractor to manage. Email, HR, Finance and PC desktop management are good examples. More of these applications are migrating to the cloud. Regardless if they are on premises or off in the cloud or at a contractor's data center the data still belongs to the Company and due care must be given to protect it. Continuous monitoring and auditing is complex and yet it is a very valuable component of the InfoCenSec® Ecosystem.

Continuous Monitoring and auditing should be integrated with the enterprise identity and access management system to provide audit data on the authenticated and authorized users on the enterprise network. Agents/sensors provide valuable data on which of your users accessed what data, from which device along with data about where and when. If possible what was done with the data that was accessed is an added bonus. For example if a trusted employee has been exfilling sensitive data to social media sites and external web sites the type of data and the locations, dates, times, links to user IDs and much more become valuable in identifying and establishing patterns of insider abuse. All of this data when combined with enterprise monitoring data becomes useful in the security big data analytics process to assist in detection and deterrence.

All sensitive/high value data must be identified and classified before crypto label wrapped. The auditing of authenticated and authorized users accessing and opening the crypto labeled data and on what device becomes a good baseline of trusted and untrusted behavior. When a trusted user is observed, via monitoring and auditing of data access, attempting to open data that they are not authorized to open then this behavior should send a warning to security operations center (SOC) for closer review. They will determine if this activity was malicious or just a case of the user doing their job but not having the updated access privileges assigned yet. This issue can be easily resolved by updating the crypto labels assigned to the user that matches the labels that were bound to the data and in turn giving them access.

Either way, this kind of auditing power is available today and it can be integrated with other state–of- the art monitoring and predictive analytics tools to give time sensitive detection and deterrence capabilities resulting in higher assurance of your data. This entire continuous monitoring sensor data collection process across both monitoring and auditing tools can then be combined either in real time or offline for analysis with sensor data collected from the enterprise network. This data can be both external and internal activity and when all combined it can provide valuable input for predictive behavior analysis, correlation, detection and deterrence systems. The integration of the multi-sensor feeds into a topological intelligence engine to provide contextual situational visualization of the current attack vectors and open access points in the enterprise gives the new capability of direct contextual and actionable mitigation of the most serious and damaging attacks.

The goal of this kind of integrated approach to info-centric sensor data from internal and external sources, is to identify and predict good and bad behavior patterns and prevent or reduce the threat before serious damage occurs while acting ASAP to reduce, isolate or stop the bad behavior. This is proactive risk mitigation.

- **Actionable Alerting & Threat Intelligence, Analysis, Correlation, Detection & Deterrence**

"Own the Endpoint device" which is a fist line defense for detection and deterrence against the APT or malicious mobile code attacks. Your cybersecurity teams must be able to identify and contain new malware code attacks. Also the use of trusted container technology to run vulnerable applications is a wise strategy for overall damage mitigation. The endpoint protection strategy must include a three way focus of Identify, control and contain with the ability to link to AI based analytics to assess in real time and act-contain. Beware, not all of these products live up to their claims. Trust but verify.

Big data analytics also provides very powerful insight into insider threat behavior as well as identifying malicious mobile code behavior on the network and connected endpoint devices. It is becoming main stream in the security event information management (SEIM) space. Some products have shown to have smarter engines for analysis than others. It is recommended that operational testing and analysis of these products be done before purchase and deployment. You want to avoid being distracted by the products with only an attractive user interface and management dash boards. Many of these nice user friendly interfaces have weaker analysis engines and higher false positives indications and will not customize the intelligence to your specific needs. However it is possible to integrate a weaker analysis engine with a nice user interface on top of a more powerful analytics, ontology and link analysis tools to achieve a lower rate of false returns and higher quality analysis. You may want to investigate how to maximize proven capabilities from multiple products to achieve an integrated capability.

There are a growing number of vendors who provide threat intelligence, analysis, correlation and detection portion of this process as a service from the cloud or as an on premise solution with SME staffing. Then depending on the nature of the IT security operations solution architecture consider outsourcing the deterrence as a SaaS. Regardless of good intelligence reporting or the kind of technology for monitoring and auditing, it all comes down to the quality of the trained experts that are viewing the data reports and the level of preauthorized response that they have on hand. They need to be well trained, vetted and certified. They need to know what they are looking at and what they need to do and have the authority to act fast. A quality active cyber intelligence vendor will at minimum focus on:

- Threat Actors: Tracking nation-state activities, organized cyber criminals and hacktivists
- Vulnerabilities and Exploitation: Uncovering zero-days on a daily and weekly basis, monitoring CVEs and tracking exploitations in the wild

- Mechanisms and Indicators: Analyzing malware family derivatives, tracking APT and DDoS technology, techniques and tactics, its evolution, monitoring command and control infrastructures, etc.
- Actionable Advice: Providing clients with ongoing, daily stream reporting to filter the noise and to drive decision advantage over the adversaries that confront them

Consider the healthcare analogy of a patient getting a reliable mammogram or MRI diagnosis which depends on the quality of the MRI picture/data and the quality and expertise of the Radiologist. The same holds true with InfoCenSec® monitoring, analysis, correlation, detection and deterrence. It depends on both the quality of the collection and sensor technology combined with the trained experts who know what they are looking at and what to do with the information.

A recent example of not having quality trained security analysts on duty is the case of the Target breach where over 100,000,000 customer records were breached over several weeks and months. Target had invested in state of the art network monitoring and forensic tools but did not have the properly trained security SOC staff on duty to respond.

To make matters worse when Target was informed of the breach the management ignored the warning and did not take any action for several weeks resulting in even worse damage. Maybe if they had acted sooner following policy and procedures for InfoCenSec® they could have executed effective remediation and recovery plans and capabilities.

- **Mitigation, Availability & Recovery**

Once a threat has been identified and vetted it must be mitigated and that can be in many forms and techniques, tactics and procedures (TTP) vary as well as the technical capabilities.

Mitigation can be as simple as the CISO, HR and GC interviewing an employee who has displayed suspicious behavior to determine further actions required. Or it can also be as complex as automated and integrated processes for the monitoring and auditing system alerting the crypto object access control label management system of a suspicious behavior by a trusted user and either temporarily suspend access privileges or revoke them.

When HR knows ahead of time that an employee is leaving or is being terminated they make the changes in the HR system and the enterprise AD which is linked to the Identity Access Management (IAM) and the crypto label access control management system to update the systems so that that user no longer has access to data inside the enterprise or to mobile data on their BYOD mobile device or in the cloud.

Data availability and recovery are critical components of the InfoCenSec® Ecosystem. To support on-demand info-sharing anywhere-anytime the CISO must employ a tested and reliable backup and recovery solution. This may be in combination with a cloud strategy to provide the authorized anywhere-anytime access along with the hot back up of mission critical systems and processes. Ideally this solution will alleviate any one single point of failure of IT infrastructure.

This availability and recovery solution is also best coordinated with the internal auditor and general council to keep them up to date on the status and capability.

This way when it comes time for the formal compliance and governance audits and assessments they are ready and in sync with the CISO. The availability and recovery solution should be documented, updated and tested on a regular basis. The test should follow real world scenarios and include professional trainers to work with operational IT staff when necessary.

In the case of outsourced services, they must provide proof to the CISO that they are doing the same. The CISO should have oversight control and authority of the contractor in event of a disaster or interruption of services. The CISO should observe when possible the IT contractor's recovery tests.

- **Identity & Privilege Access Authentication Management (IAM)**

The IAM technology has been around for a few years and is almost the foundation of any enterprise security solution. The IAM is evolving into new products and services focused on monitoring and controlling the access for the "privilege users" like the bad actor Edward Snowden who worked at a NSA contractor and had access to the highest levels of access to classified data and used his access identities to steal classified data. The IAM becomes info-centric when data on the authenticated and authorized users across the enterprise gets integrated together with the self-protecting Info-centric crypto label management system. By leveraging data from both solutions together with biometric technology in both the IAM and the Self-protecting data access solution, the result is InfoCenSec® control at the data object level. The combination of user/role, identity, data object level based access control provides a previously unequaled granular access control capability and greatly reduces the potential impact of an insider data breach.

The enterprise can achieve a higher trust level when only authenticated and authorized users are on the network and systems with logical access controls integrated with object level crypto labeling techniques controlling access to the data with object level access control. This role based object level approach can be considered for use as on premise system or with a managed cloud based service with data stored in the cloud.

- **InfoCenSec® Risk Assessments & Penetration (Pen)-Testing**

The InfoCenSec® risk model paradigm shift is to reduce the consequences and impact of a data breach while increasing the difficulty of data exfiltration. The InfoCenSec® risk formula is **Risk =∑ [(Threat + Vulnerability + Difficulty) x Consequence]**. This common sense approach to risk management uses a **Sliding Scale of Trust (SSoT™)**. This pragmatic approach to risk management has an evergreen awareness of what is most at risk and when.

What data has the greatest impact to the enterprise at a given point in time? This accounts for practical everyday changes in the threat and operating environment.

This also assumes that the insider threat already exists and some form of malicious code attack has already infected some device or devices on your network. Plan to recover as if you are already under attack.

Penetration or pen-testing is an important component of the InfoCenSec® Ecosystem. It provides an objective picture at a point in time of how secure various aspects of the enterprise security status is. It quickly identifies vulnerabilities and how they can be exploited by both inside and external attacks. Pen-testing needs to be done both externally and internally using both tools and insider techniques together to include social engineering. The use of qualified and vetted contractors is suggested over a full time internal team. Either way it is advised to require the pen test contractor provide both proof of background investigations on the testers and have liability insurance in force. Also it is advised that the contractors should be rotated on a quarterly or semi-annual basis. This rotation of pen testing contractors provides for an objective fresh approach and view as well as reduces the potential of trusted insider abuse.

The pen-testing process needs to be managed by the CISO and coordinated with legal and results need to be reported to internal audit and legal.

- **InfoCenSec® Security Training & Awareness Program**

Health Insurance Portability and Accountability Act ("HIPAA") as defined in the Code of Federal Regulations, 45 C.F.R. 164, section 164.308, requires that every organization in the healthcare industry implement a security awareness and training program for all members of its workforce including management. Other industry segments are already following this policy.

Your employees can all be sensors if told that they are, and are trained on how. Training and awareness programs work well when used in conjunction with policy. They can impact the work culture to enhance the acceptance of security and evolve to a vigilant minded work force.

The first line of defense to the insider threat and internal fraud is an aware, vigilant and willing work force. It is recommended that professional trainers be used with SMEs and the CISO on implementation of an awareness program which should also include training on how to recognize unauthorized behavior and what to do when it happens.

Once you've decided to implement an InfoCenSec® awareness training program, there are many decisions to be made. There is no "one size fits all" solution; the right choices are dependent on many factors, including:

- The number of computer users inside your organization and outside as suppliers to your organization,
- The computer skill level and existing security knowledge levels of your users
- Identify and place into special group the "privileged users" so you can also profile them in training for possible behavior traits indicative of a possible lack of trust
- The type and sensitivity of the data that your workers handle

- Your existing use policies (Are workers allowed to use work computers for personal web surfing, emailing, etc. during breaks/lunch?
- Are your workers allowed to connect their own devices to the company network? (BYOD smart phones or iPads etc.)
- Is there a specific policy and legal forms for BYOD?
- Are workers allowed to install applications, run web technologies such as Java, ActiveX, Flash, etc.?
- Legal, HR or industry mandates that apply
- Skill level and workloads of your CISO personnel and outsourced contractors
- Budgeting and funding approvals are required

There's a difference between implementing an InfoCenSec® awareness program "just so we can say we did it" and implementing an ***effective*** InfoCenSec® awareness program that's proactive and tailored to meet your unique needs. A single training curriculum can't effectively address the needs of every company; neither can the exact same material best provide the training needed by different workers within a single organization. That's why **NIST** bases its training standards on a ***role-based*** **model**.

While there will be basic security awareness information that is applicable to all employees and contractors who interact with the computer systems in your organization, you should go beyond that and provide training that is relative and specific to each worker's or group's existing knowledge and skills and to the tasks that they perform and the data they handle.

One of the first decisions that you will need to make before you actually deploy an InfoCenSec® awareness program is who will develop and deliver the training. Specifically, will it be developed and delivered by your personnel and if so, will it be done by the CISO, the IT department, the general council and the HR department, together as a team or someone else?

Or will you contract with a company that specializes in specialized training? There are advantages and disadvantages both ways. By doing it yourself, you may (or may not) save money. When looking at it from a cost standpoint, it's important to consider not just the time that will be spent actually delivering the course(s) but also the time spent to develop the curriculum, to put together training aids and to prepare for the course. What is internal time worth versus cost of hiring an outside firm? Instructors often expend as many or more hours outside the classroom as in. What is the hourly value of the time at the pay grade of the employees who will be doing this extra work?

Going with a training company may allow you to benefit from economies of scale; the curriculum may likely already be developed and in place and the development costs are spread among many clients. This also means we will probably be able to put the training program in place much more quickly. However, it may also mean that the training is more of a "canned" package that's not specifically tailored to your policies and people who work there.

In some cases, your workers might be more receptive to training from someone who is "one of them," because there's a sense that they understand the unique challenges of working there.

In other cases, they may have more respect and be more likely to give credence to training from an outsider who is seen as more of an "expert" in the topic of information security and insider threat mitigation. We will have to evaluate the attitudes of our people across some of the key departments identified for the first wave of awareness training and evaluate the findings and then make a recommendation to senior management on best course of action.

Regardless of do-it-yourself or contracting with a pro your goal should be to take your employees beyond the level of mere *awareness* of InfoCenSec® issues, and actually *educate* them in the why and how to assess the risk/security implications of various situations and the why and how to apply InfoCenSec® best practices as they perform their job duties on a daily basis. Your people are the first line of defense against the trusted insider threat.

People are great sensors if you tell them in a policy that they are and they should do it. Then train them how and reward them for doing so. **Make it positive fun to be vigilant and rewarding.**

Conclusion:

The Information-Centric Security (InfoCenSec®) approach to data security and privacy compliance is proactive and shifts the priority onto the high value data object (HVD) or info object itself along with the monitoring, auditing and control of people. This approach shifts resources, policies and priority away from the traditional singular logical protection of devices or networks to safeguard data. This concept requires a paradigm shift in thinking from board directors, senior level management and operational management. The risk management style thinking must shift away from reactive to proactive. This new proactive approach for risk mitigation merits serious consideration in the board room as well as in evolving cloud data management and cloud info-sharing security dialog.

"The only limitation on the use of the InfoCenSec® model is your imagination."