InfoAssure, Inc.

The Trusted Source for Information-Centric Security

Persistent, Vigilant Data Protection
Anywhere-Anytime

Data Has Become The New End Point

Computers Do Not Steal Data-People Do

Proactive Information Centric-Security (InfoCenSec®) Insider Risk Mitigation Strategy

2020

James G. Lightburn, CEO
InfoAssure, Inc.
j.lightburn@infoassure.net

ALL RIGHTS RESERVED © 2020
INFOASSURE.COM, INC. D/B/A INFOASSURE, INC.

InfoAssure, Inc.
www.infoassure.net

Data Has Become The New End Point. Computers do not steal data-people do. People will always find a way in from outside or inside. It is well known that the insider threat risk is growing, and regardless of an internal or external attack, the endgame for the cyber attacker is the data and not the device. The device is just a tool.

Today, to protect the data most of the attention and financial resources is on protecting the endpoint devices and networks and yet we still see more data breaches than ever before. Maybe the term "endpoint" has been too narrowly defined? If you are an information security professional, likely the term endpoint refers to a desktop, laptop, smart phone or other end-user devices. But if you are an attacker, in fact, the endpoint is the data itself and the endgame is to steal, or modify or disclose the data. The attacker will often exploit the user's device with malicious malware as a tool to get to the data but they are not stealing the device. Confusion aside, both device security and data security are critical, but often data security has taken the back seat while device security has most of the attention and products.

There are two common factors at play in data breaches and they are **people and high value data (HVD)**. Progress is being made by emerging DLP/EDR/UAM/EUBA vendors with improved AI/ML Agent based tools with agent based monitoring, activity alerting, device controls and behavior analytics which has given information security professionals the ability to monitor people, devices and data and produce a fusion of the data into a Common Operating Picture (COP) and Common Intelligence Picture (CIP) in near real time. A growing trend in the industry with DLP is that some DLP tools now have the ability to do data discovery, labeling and classification. That is good news. The bad news is that many CIOs/CISOs are not taking advantage of this capability. Even worse news is that strong end to end persistent encryption is not yet being used widely. Data is shared, and data is mobile and data loss will happen. It is not about IF it is going to happen it is about WHEN and you may not even know that it has already happened especially is it was done with help of a trusted insider.

With the increasing news on growing threat from the trusted insider and massive data breaches with the looming GDPR compliance fines, enterprises will be motivated to shift focus to a Proactive Information Centric-Security (InfoCenSec®) Risk Mitigation strategy. They must assume their users' devices will be compromised and as a result make the data (the attackers' endpoint) as difficult as possible to steal, compromise, expose, and/or modify the HVD while increasing the likelihood that they will be stopped or caught and punished.

The next generation of Cyber Insider Risk Management will be Proactive InfoCenSec® Risk Mitigation to reduce the consequences of stolen HVD. The key enabling factors will be the formation of an enterprise InfoCenSec® policy which calls for the adoption of strong end to end persistent encryption integrated with enterprise DLP, Entity/User Behavior Analytics, Data Discovery, Data Labeling and Data Classification tools. With strong end to end persistent encryption, the HVD remains protected when at rest, in transit and use.

The HVD must be monitored, labeled, classified and persistently protected from creation, through consumption to destruction covering the full data life cycle. With the integration of ALL of these into an evergreen ecosystem of protection the result is a more effective Risk Mitigation Management solution and the enterprise CISO/CSO/CRO will know what HVD they have, what level of sensitivity it has, who has access to it, and who is using it on what device when and where.

Proactive (InfoCenSec®) Cyber Insider Risk Mitigation

- **InfoCenSec® is people and data centric. Its goal is risk mitigation management of enterprise high value data (HVD)**
- **InfoCenSec® Ecosystem is evergreen with the integrated tools and policy working together**
  - ✓ Establish new Info-Centric security doctrine, policies and procedures
  - ✓ Make it difficult for untrusted or authorized insider user to find, use and steal HVD
  - ✓ Monitor, audit, and analyze both people and the HVD in context while also persistently protecting the HVD
  - ✓ Mitigate risk, make it more expensive to steal HVD and increase the chances of getting caught
  - ✓ Persistently protect HVD with crypto labeling making it useless when breached to reduce the impact/consequence
- **Core concept is continuous monitoring of people, devices and HVD with persistent protection of HVD with strong end to end Object Level Encryption (OLE)**
  - ✓ Proactive InfoCenSec® Risk Mitigation (monitor, audit and control people + persistent protection of HVD)
  - ✓ Monitor people in virtual and physical world and fuse data use and monitoring analysis with semantic/event behavior modeling
  - ✓ Self-protecting and monitored data objects = always on protection of HVD and reduces and mitigates impact of insider threat

  - ✓ OLE crypto labeling enforcement is application, device and network agnostic which provides an enterprise risk mitigation solution
- **Self-protecting data affords application, device and network independent protection of HVD**
  - ✓ The traditional logical device controls in use today are resource dependent and expensive to manage
  - ✓ Self-protecting data objects with RBAC and monitoring are not expensive…they are easy to manage and implemented as an extension of current tools
  - ✓ Enables more efficient/cost effective enterprise proactive data governance and privacy compliance
  - ✓ Enables proactive and dynamic enterprise insider threat risk mitigation solution

To learn more contact:

James G. Lightburn, CEO
InfoAssure, Inc.
(410) 991-9611 cell
j.lightburn@infoassure.net
www.infoassure.net