CYNERGISTEK

DATA: DISCOVERY, LOSS AND BREACH RISK ASSESSMENT™

Understanding Risk from the Inside Out

What's Current?

Where does sensitive data live in your network? What are your employees doing with that data? How vulnerable is your organization to data loss or data breach as a result? Is your patients' sensitive data at risk? Is your company-confidential data at risk?

Shortcut

- Regulatory Reference:
  45 CFR §§164.308(a)(1)(ii)(A) and 164.316(b)(1)
- Understand where ePHI lives in your network's structured and unstructured data
- Observe what users are doing with your patient and other sensitive data
- Qualify and quantify your data loss and data breach risk

Assessment Approach

The Healthcare Data Loss Assessment measures the amount of sensitive patient data (or other sensitive data that you want to study) lost over a fixed period of time. The process identifies sensitive patient data being lost and the applications or individuals putting your patients' sensitive data at risk.

CynergisTek will conduct a true data loss/data breach risk assessment that targets key systems that contain ePHI (e.g. application databases, servers, file shares, workstations, etc.) employing content fingerprinting capability, an active data discovery process, and passive monitoring. This service provides both quantitative and qualitative insight into your enterprise data loss/data breach risk.

We seek to answer the following questions:

- Is patient information being communicated via webmail?
- Is patient information being posted on social networking sites or blogs?
- Is patient financial information being sent to partners securely?
- Is patient clinical data being transmitted to partners over insecure channels?

Assets for Evaluation

The depth and value of study for the evaluation is enabled by the selection of target assets - applications, file shares, servers, workstations - that provide the greatest visibility into potential data loss occurrences.

- ☑ A **key application(s)** that can serve as the "source of truth" from which key patient data can be extracted to complete the content fingerprint baseline is critical.
- ☑ Up to **5 file shares** upon which data discovery and passive monitoring will be performed.
- ☑ Up to **10 servers** upon which data discovery and passive monitoring will be performed.
- ☑ Up to **50 workstations** upon which data discovery and passive monitoring will be performed.

Complete Content Fingerprinting

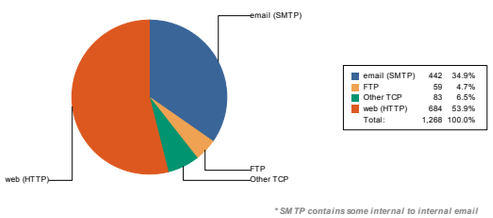
Sensitive patient data is securely registered with the Code Green CI Appliance.

Conduct Data Discovery

We locate and identify sensitive data at rest on endpoints and servers across the network that have been targeted for the study, providing visibility and audit reporting of potentially unsecured information.

Perform Passive Monitoring

The CI Appliance passively monitors outbound Internet traffic for sensitive patient data. If sensitive data is identified in network traffic the appliance captures details such as Source IP, Destination IP, Protocol and Category of information lost.



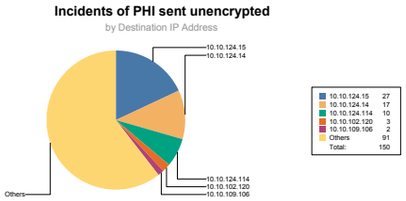
** SMTP contains some internal to internal email*

DATA LOSS

Analysis and Reporting

At the end of the assessment you will receive a comprehensive Healthcare Data Loss Assessment Report. The report details:

- Patient demographic information lost
- Patient clinical information lost
- Patient Credit Card, Billing and insurance information lost
- Unencrypted HL7 and X12 transmissions detected
- Channel where the loss occurred (SMTP, WebMail, HTTP, FTP, TCP/IP
- Recommended steps for remediation



We want to be able to be as granular in our evaluation of risk as possible.
Some other things that we can incorporate into the analysis, after the data collection is complete, are:

- Observations and trends in certain employee cohorts (e.g. departments, access control groups)
- Observations and trends within third-party relationships

Conduct Findings Workshop

The Healthcare Data Loss Assessment will help guide the creation of an effective data loss prevention strategy.

About Cynergistek

CynergisTek is leading provider of information security management, regulatory compliance, IT audit, security technology selection and implementation, and IT infrastructure architecture and design services and solutions for the healthcare, financial services and real estate industries. We bring relevant and practical insights and guidance to our clients, we are disciplined in our methods, responsible stewards of our clients' resources, and generous in our service. These are our commitments. Learn more at www.cynergistek.com.

About Code Green

Organizations today are increasingly challenged in protecting customer data and safeguarding intellectual property from internal malicious use and accidental mishandling. Unauthorized disclosure of confidential information can result in loss of revenue, financial penalties and irreparable damage to an organization's image, brand and customer loyalty. Code Green Networks takes a radically different approach to data loss protection and content filtering. While other vendors would have you believe that DLP is a costly and complex solution. Code Green Networks believes that DLP should be easy to install, implement and require a minimum amount of resources to operate.

CODE GREEN NETWORKS

Contact Us

CynergisTek's dedicated team of client services professionals would be delighted to speak with you further about our services or expertise. Contact us at info@cynergistek.com or call 512.402.8550.

CYNERGISTEK

DATA LOSS