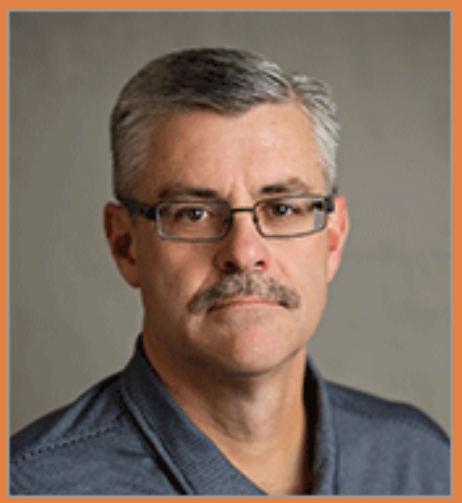
Fall 2016

Volume 2 | Issue 2

THE INNER COR

A quarterly eNewsletter dedicated to North Carolina Data and Information Management News and Business Trends.



A Note from Chris

At COR365 we firmly believe in our information management services. In fact, we utilize our own services internally to assist in running the business side of things.

Our internal use of iCOR, a powerful ECM (Electronic Content Management) system, best demonstrates our “use what you sell” mentality. Our first class development team built a powerful CRM that manages our entire sales process, our internal contract handling and our client communication tracking.

In addition to managing sales and client activity, iCOR is also capable of automating internal business processes such as:

- HR Online – Automating

Protecting Against Insider Threats

By Robert Martin and Mark Whitteker

According to the National Counterintelligence and Security Center (NCSC), “an insider threat arises when a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States” (NCSC, n.d.). According to fbi.gov, there exists a direct relationship between Economic Espionage and Insider Threat. This billion dollar threat is so menacing that the FBI categorizes it as an issue of National Security (FBI, 2011). These threats, however, are not just an issue of National Security affecting the government. Insider threats are a growing concern for public and private sectors alike, often resulting in financial damages, corporate liability, and loss of intellectual property. So how can public and private organizations protect against Insider threats?

Data that is transformed into information fuels our global economy. Outside of human life, it is the most important asset

- the application and hiring process of new employees
- Expense Reporting – Automating and capturing business expenses
- Contact Relationship Management – Automating contact management
- IT trouble tickets - Automating the workflow from creation to resolution
- And soon to follow:
  - Purchase Order Approval and Processing
  - Asset Tracking Module.

These business processes are vital to not only our business, but yours as well. Our daily use and reliance on iCOR by M-Files has validated our decision to partner with M-Files in early 2015.

We would love the opportunity to discuss how iCOR can simplify and solve the information chaos challenges you may be facing. Contact us at 336-499-6020 to schedule an appointment with one of our Account Executives today.

to any organization. In fact, many 21st century companies have entire business models where data is central to their existence (think Google, Dropbox, Facebook and the like). Although there are multi-faceted approaches in building an effective program to protect this valuable asset, two specific measures that can help thwart insider threats and provide a layer of protection are Data Loss Prevention systems and data backups.

Data Loss Prevention (DLP) systems aid an organization in managing the flow of data across the network, in storage, and while being transferred between devices. This helps in detecting when a malicious or oblivious individual tries to move data to an unauthorized location. This can be accomplished by using tools, like Symantec Data Loss Prevention. Symantec DLP can identify restricted data stored within the organization's infrastructure. Symantec DLP can detect data leaks using Described Content Matching (DCM), Exact Data Matching (EDM), Indexed Document Matching (IDM), and Vector Machine Learning (VML) (Symantec, n.d.).

According to Symantec.com, "Exact Data Matching (EDM) detects content by fingerprinting structured data sources, including databases, directory servers, or other structured data files. Indexed Document Matching (IDM) applies fingerprinting methods to detect confidential data stored in unstructured data, including Microsoft Office documents; PDFs; and binary files such as JPEGs, CAD designs, and multimedia files. IDM also detects 'derived' content, such as text that has been copied from a source document to another file. Vector Machine Learning (VML) protects intellectual property that has subtle characteristics that may be rare or difficult to describe, such as financial reports and source code. It detects this type of content by performing statistical analysis on unstructured data and comparing it to similar content or documents. Unlike other detection technologies, VML does not require you to locate, describe, or fingerprint the data you need to protect. Described Content Matching (DCM) detects content by looking for matches on specific keywords, regular expressions or patterns, and file

properties" (Symantec, n.d.). "File Type Detection recognizes more than 330 different file types including email, graphics and encapsulated formats, and can also recognize virtually any custom file type" (Symantec, n.d.).

Data backups ensure an organization is able to restore critical data in the event a system is corrupted, unintentionally or maliciously deleted, or is transformed into an unusable format. According to cor365.com, "Routinely backing up critical business information and storing them in a safe, secure environment makes it possible for businesses to continue to operate seamlessly, even when the unexpected happens" (COR365, n.d.). The unexpected can come in the form of a compromised system, a disgruntled employee, a natural disaster, a hardware failure, or even something as precarious as ransomware. In each of these instances, having a backup of the data in a secure physical location can help ensure that business operations can quickly recover, and that impact is negligible. Backing up seems like a simple task to complete, but sadly, many businesses do not have an established backup solution. While an effective insider threat program should include DLP and data backups, neither will be manageable or effective unless coupled with data classification.

Data classification is a daunting task at best. Data must be classified based on type and appropriate recipients, labeled consistently, and handled properly with the objective of preserving confidentiality, integrity, and availability. This can be a tremendous hurdle to overcome if a company is not equipped with the right tools, policies, and procedures. Solutions, like iCOR by M-Files®, can provide a secure platform for classifying and accessing data with "built-in content and process management capabilities" (COR365, n.d.). This type of solution can help address the need to classify and label mission critical data. Then, once the labels (or tags) have been applied to the various types of data, DLP solutions can use those labels to prevent users from accidentally (or intentionally) distributing proprietary information to unauthorized recipients or locations,

both inside and outside the network.

To harden endpoints and servers used in this architecture, a password management solution should be implemented to "ensure the controls are in place to centrally secure, manage and monitor privileged accounts" (CyberArk, n.d.). Industry compliance and standards dictate that controls must be in place to administer, secure, and maintain administrator accounts to protect critical data. Solutions like, CyberArk effect change with industry leading "solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done" (CyberArk, n.d.).

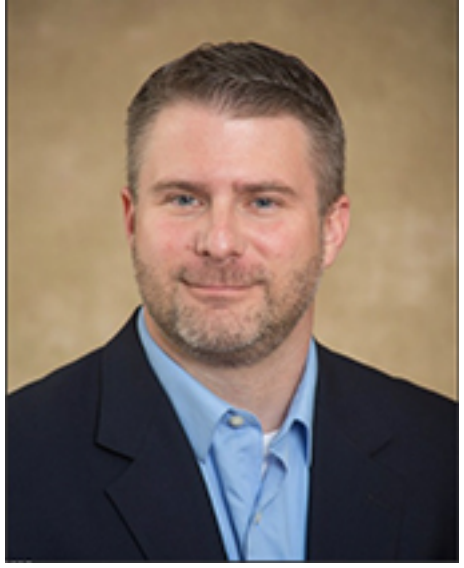
Cost, unfortunately, can be the final determining factoring in the decision to implement security solutions. Blinded by cost, businesses can be under the misconception that Return on Investment (ROI) will not be able to be measured with an investment into data protection and data classification. In my experience, businesses are already paying out more in operational cost to combat data loss issues then it would take to purchase and maintain a comprehensive solution. Consider the amount of time spent by help desk, Tier 2, and security teams chasing down issues related to data loss and data breaches. Businesses are either blindly paying to shore up ineffective security solutions or do not have an effective security solution in place. Each of these options can eventually lead to data breaches and data loss. Businesses must redirect focuses to comprehensive solutions to protect data and help prevent insider threats in order to continue to exist in this ecommerce driven economy.

NCSC. (n.d.). National Counterintelligence and Security Center (NCSC): Contact Us. Retrieved July 25, 2016, from https://www.ncsc.gov/contact/index.html FBI. (2011, November 30). Economic Espionage and the Insider Threat. Retrieved July 25, 2016, from https://www.fbi.gov/audio-repository/news-podcasts-thisweek-economic-espionage-and-the-insider-

threat.mp3/view COR365. (n.d.). Data Protection Services, Loss Prevention & Backup | COR365. Retrieved August 8, 2016, from http://www.cor365.com/services/data-protection Symantec. (n.d.). Symantec Data Loss Prevention. Retrieved August 22, 2016, from https://www.symantec.com/en/uk/products/information-protection/data-loss-prevention Symantec. (n.d.). Data Sheet. Le Corbusier. The Villa Savoye. doi:10.1515/9783035603958.132a CyberArk. (n.d.). Privileged Password Management and Control Solutions - CyberArk. Retrieved August 31, 2016, from http://www.cyberark.com/solutions/by-project/privileged-password-management-control/

Raleigh ISSA Board Member

Robert Martin is a Certified Information Systems Security Professional with over twelve years of experience in information security. He works as a Security Engineer at Cisco System Inc. in RTP, NC. Robert specializes in such areas as risk management, regulatory compliance, security solutions architecture, security audits, vulnerability assessments, and penetration testing. He serves as the Sponsorships Director of the Raleigh Chapter of the Information Systems Security Association. He has held several other IT Security Advisory Board positions over the years with a focus to bring about awareness of information security threats in an ever changing global IT Security economy.



Mark Whitteker, MSIA, CISSP, ISP, is the manager of the Government Security & IT Services team at Cisco Systems, Inc. Leading a geographically dispersed team of veteran security and IT professionals, Mark has over 20 years of experience in security architecture, secure solutions development, systems and network auditing, forensic discovery, vulnerability assessments, and security management. He has an extensive background in the application of US government regulations and requirements, including both physical and logical security, with notable success and accomplishments in directing a broad range of corporate security initiatives through the design, planning and implementation of classified and unclassified solutions supporting key business objectives. He has served as the chapter's Vice President for the past three years.

About COR365 Information Solutions

COR365® Information Solutions provides clients with industry-leading solutions that streamline operations, lower costs, and simplify compliance. The company offers hardcopy records management, secure tape vaulting, offsite records storage, document imaging and shredding services—with redundancy and durability built into every critical component. For more information, visit www.COR365.com or contact Chris Kelley, 336-331-4901 or email ckelley@COR365.com

Facebook LinkedIn

3302 Old Lexington Road, Winston-Salem, NC 27107