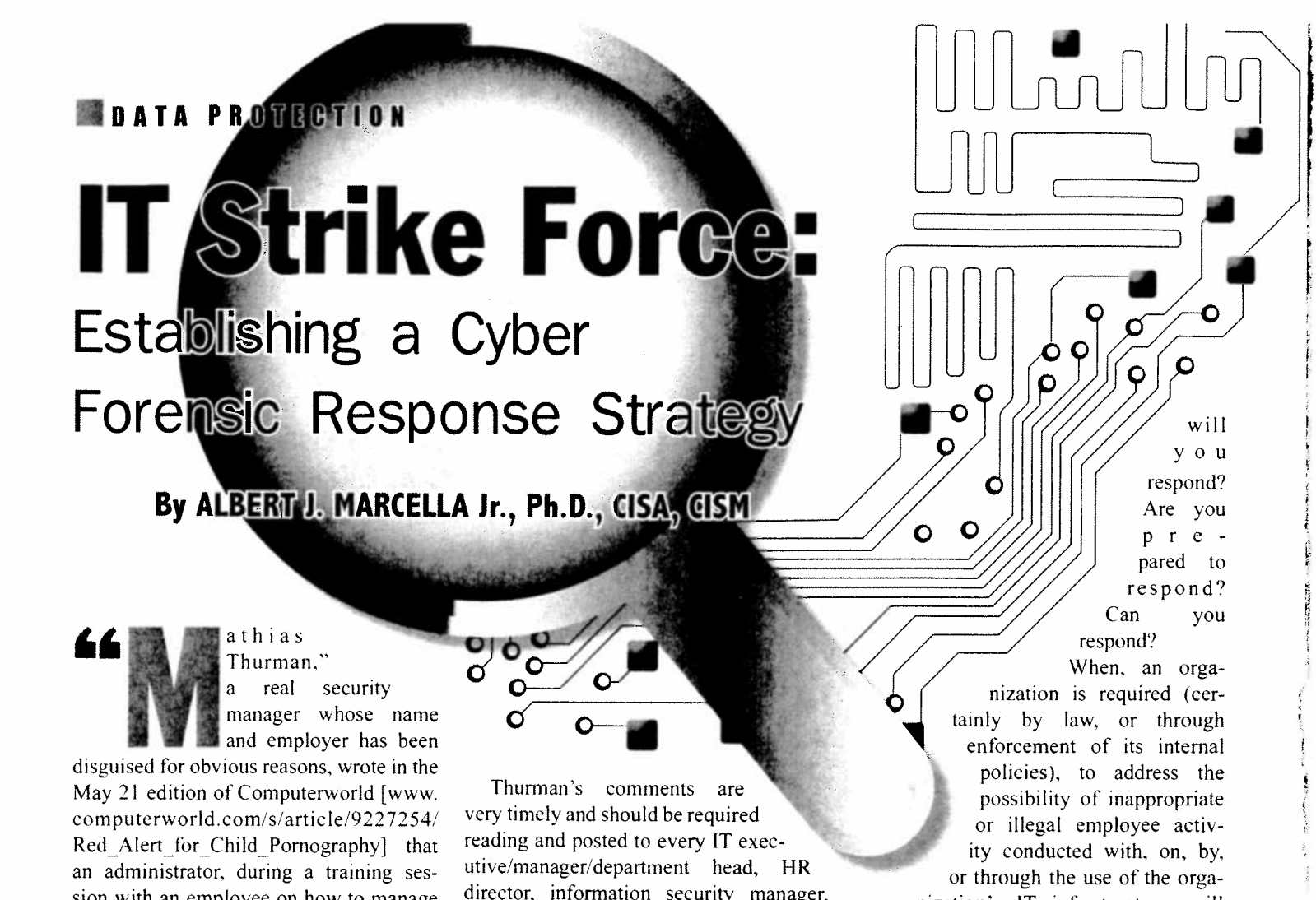
IT Strike Force:

Establishing a Cyber Forensic Response Strategy

By ALBERT J. MARCELLA Jr., Ph.D., CISA, CISM



"Mathias Thurman," a real security manager whose name and employer has been disguised for obvious reasons, wrote in the May 21 edition of Computerworld [www.computerworld.com/s/article/9227254/Red_Alert_for_Child_Pornography] that an administrator, during a training session with an employee on how to manage the organization's antivirus infrastructure while reviewing the reports of machines with infected files, spotted what appeared to be a very suspicious file with a ".mov" extension.

This particular employee had an MOV file on his G drive with a name that indicated the video potentially involved child pornography. The file was found to be on a device of an employee located in Europe.

Thurman posed the question whether an MOV file with a highly suggestive name is enough to kick off an investigation into what is on an employee's PC. He went on to discuss the various legalities and issues that would surround such an investigation.

This all-too-real scenario is out there, lurking, waiting to strike any organization that is dependent upon technology or that allows its employees access to this technology. In essence, any company which desires to remain competitive in today's global marketplace. Every organization, regardless of its size, is prone to be a victim of illegal, unauthorized use of its IT infrastructure.

Thurman's comments are very timely and should be required reading and posted to every IT executive/manager/department head, HR director, information security manager, auditor, and legal counsel with an organization. That goes as well for those professionals responsible for business continuity planning. The illegal use of an organization's IT infrastructure, if unchecked, could result in a significant disruption of organizational services, legal and financial exposure, as well as loss of company goodwill and customer base.

If not addressed properly, legal ramifications brought by wrongfully accused, emotionally scarred, or professionally injured employees will compound the situation, exposing the organization to additional legal and financial liabilities and possibly unflattering public exposure and legislative scrutiny.

Currently, this is not primarily a technical issue but, strategically right now, it is a procedural issue.

As Thurman aptly states, there are plenty of repulsive people out there tramping about in many unsavory and illegal areas. In today's technology-rich workplace, it is not a matter of "if" but "when." When your organization faces these same issues, how will you respond? Are you prepared to respond? Can you respond?

When, an organization is required (certainly by law, or through enforcement of its internal policies), to address the possibility of inappropriate or illegal employee activity conducted with, on, by, or through the use of the organization's IT infrastructure, will your organization be prepared to legally conduct an appropriate investigation, in order to acquire the evidence necessary to evaluate guilt or innocence? Respond to a request for such data from external legal or law enforcement authorities?

Given the ever increasing individual and organizational dependency on technology and devices that store, process and transmit billions upon billions of bits of data per day, organizations must begin to immediately investigate, organize, staff , train, and formulate an internal, cyber forensic response strategy along with a comparable, well-trained, cyber forensic investigation team.

Child pornography is certainly repulsive, and any indication that organizational infrastructure is being utilized to support this activity would require swift and decisive action on the part of any organization to identify and stop it immediately.

Child pornography, however, is not the only violation that would activate the organization's cyber forensic response team. Theft of intellectual property, violation of

company policy, cyber espionage, fraud, non-compliance issues, threat of cyber extortion, etc., would be reason enough to have a pro-active cyber forensic response capability. In fact, any event that by its very nature elevates data to the status of digital evidence, will require specifically trained and skilled cyber forensic response professionals to follow documentable and strict investigatory procedures and processes, to identify, recover, extract and analyze these potentially evidentiary data.

For most organizations, these professionals won't just be sitting around waiting for the call to action. They will be trained to perform a variety of anti-fraud, compliance, and security responsibilities as well. Teams will consist of properly-trained cyber forensic investigators, ready to respond globally to an organizational need to secure, identify, extract, and analyze potential digital evidence, all in a manner legally acceptable in a court of law.

The court of law and the rules which must be followed for attaining legally acceptable digital evidence, differs here in the U.S. verses in global destinations where the organization may be located, have employees or agents conducting company business, or have their data "parked" via a third-party cloud provider.

Even if the investigation is performed only to enforce compliance with internal company policy, conducting the investigation as if the results are to be used in court, makes those data collected admissible as evidence should things turn nasty and heading into court becomes an unforeseen necessity.

On an international scale, the ability to access these data and to perform a cyber forensic investigation may be hampered by conflicting privacy laws, data security legislation, and to a greater extent, the lack of country-specific data security and privacy legislation addressing the scope and limitation of conducting a cyber forensic investigation by a U.S. company on foreign soil.

Right now, before the alarm to action sounds, companies should be addressing a host of preparatory questions to assess their readiness to respond to the need to conduct a cyber forensic investigation.

Questions such as ...

Exactly what is unacceptable material? Is this defined by the organization? By legal doctrine? By both? Is this simply left up to the individual discretion of the employee?

Are those items, data, etc., deemed unacceptable by definition, clearly communicated to all company personnel? External vendors with access to company-owned technology? Guests? Visitors? Anyone with access privileges to company-owned technology?

Do all employees know what to do and whom to call, should they accidentally access or encounter unacceptable material?

Do we have ...

1. a proactive cyber forensic investigation (CFI) policy in place?
2. properly-trained cyber forensic investigators on staff that can respond in a proper and legally defensible manner, to the need for a CFI? If not, have we pre-assessed and pre-qualified a third-party cyber forensic investigation organization that can respond and perform the required cyber forensic investigation processes, in an authorized, legally defensible, and timely manner?
3. a current, up-to-date inventory registry of all company provided technology assigned to an individual employee? Can we "tie" an individual piece of company owned and distributed technology back to an individual employee, via an employee signature attesting to the receipt of these technologies?

Have we ...

1. defined and communicated to all employees what constitutes unacceptable use of company IT infrastructure and data, both from an organizational policy perspective as well as legally defined?
2. discussed an appropriate protocol with third-party service vendors, should these vendors encounter unacceptable materials (read images) on company-owned hardware during servicing operations?
3. instructed all employees not to probe or to take any further actions, which may potentially alter or destroy data, upon discovering questionable (unacceptable) material on any company-owned technology?

Based upon an evolving business impact analysis (BIA) and risk assessment process, do we ...

1. conduct proactive cyber forensic investigations at all levels of the organization?
2. as part of an employee exit interview process, secure and forensically acquire (following strict chain of custody processes and procedures) any hard drive technology accessible by the employee, thus preserving these original data, should these data be required to be forensically analyzed at a future date?

   Note ... this acquisition process would not be performed on every employee leaving the organization, only those employees whose job responsibilities have been identified as having access to sensitive, critical, essential data, based upon the BIA and risk assessment.

Does every employee know that the organization has a cyber forensic response team? That this team should be called first prior to any action on the part of an employee to assess or analyze any suspicious and/or company defined unacceptable data? How do we intend (or can we) enforce this policy?

Does the organization's acceptable use policy extend to all external vendors connecting to the organization's IT infrastructure? Have these external vendors/contractors agreed to submit any connected device for forensic examination, upon request by the organization's legal counsel?

For each foreign operation, where company data is processed and held (backed up on site or "parked" by a cloud service provider), do you have specific knowledge of the country's cyber-crime laws (if they exist) and how these laws will affect your abilities to perform a cyber forensic investigation of a suspected employee, who may be a foreign national? How about a U.S. citizen working in a foreign country?

These preparatory questions can go on for many pages. The point is that *now* is the time to assess the organization's preparedness and ability to successfully perform a legally defensible, valid, accurate and thorough cyber forensic investigation.

It is not solely a technical question or response. Preparedness will require the intimate involvement of and between IT, business continuity planning, HR, legal, and executive management.

The time to act is now. Act or accept!

❖

Albert J. Marcella Jr., Ph.D., CISA, CISM is president of Business Automation Consultants, LLC. He is an internationally recognized public speaker, researcher, and seminar leader with 35 years of experience in IT audit, security and assessing internal controls. He is an author of numerous articles and 26 books on various IT, audit, and security-related subjects. Marcella's most recent book, "Cyber Forensics: From Data to Digital Evidence," was released in May 2012. For more information, contact him at amarcella@mindspring.com or visit www.businessautomationconsultants.com.