Hello ISSA Kansas City Members and Happy March!

Hope you enjoyed the February presentation on “Beyond Password Management: Seven Steps to an Effective Privilege Program” by Troy – CyberArk. The presentation and supporting documents have been forwarded to the attendees.

Did you know that ISSA organizes and provides international conferences, local chapter meetings and seminars that offer educational programs, training and valuable networking opportunities; Provides access to information through the ISSA Website, as well as online E-Newsletters and in the monthly ISSA Journal. You can earn CPE credits by attending chapter meetings, ISSA Web Conferences, subscribing to the ISSA Journal or serving as a chapter or international council leader. ISSA offers opportunities for members to volunteer by joining committees or KC volunteer, which provides leadership opportunities in the security industry; and enhances professional stature. Being a volunteer advances the profession by sharing your expertise as an event speaker or contributor to ISSA.

Sincerely,

Naeem Babri

President, ISSA Kansas City

---

**Upcoming ISSA-KC Monthly Chapter Meeting Schedule**

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 22, 2018</td>
<td>Zero Trust with Zero Resources</td>
<td>Critical Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRIO’s, Kansas City, MO</td>
</tr>
<tr>
<td>April 26, 2018</td>
<td>Topic: Hot Topics in Data Privacy</td>
<td>Lathrop &amp; Gage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hereford House, Leawood, KS.</td>
</tr>
<tr>
<td>May 24, 2018</td>
<td>Topic: More to Come</td>
<td>Securonix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lidia’s Italy</td>
</tr>
</tbody>
</table>
On February 22, 2018, the ISSA-KC Chapter members and other security professionals held a meeting at Lidia’s Italy restaurant to network and attend the monthly chapter meeting, on the topic: Beyond Password Management: Seven Steps to an Effective Privilege Program.

Troy Brueckner is a Certified Information Systems Security Professional (CISSP) with an extensive record of assisting organizations improve network and data confidentiality, integrity, and availability.

Troy presented and discussed management of passwords, keys, and secrets how it’s being addressed within every organization in one way or another (or many), but does your privilege account management program really keep attackers from fulfilling their mission ... or does it just make administration less cumbersome? We will explore the common elements in nearly every high-profile breach and how compromised credentials were necessary to the overall "success" of the attack. More importantly, we discussed the steps every organization can take to reach an acceptable level of "cyber-hygiene" within their privilege program.

CONGRATULATIONS to Greg Harper winner of ISSA’s $50.00 gift card give-away!
Spoliation of Digital Evidence

Author: Dr. Cheryl O. Cooper, CISSP with Kansas City ISSA

Abstract

Spoliation is the intentional or negligent withholding, hiding or destruction of relevant evidence in a legal proceeding. Corporations need to be aware of spoliation issues from the time they become aware of a potential claim. Waiting until a suit is filed is often too late. Spoliation occurs when a company has lost or destroyed evidence that it knew or should have known to preserve for a lawsuit. Awareness of potential litigation imposes a duty on business or corporation’s to preserve evidence that may relate to that lawsuit. The evidence could consist of electronic records like e-mail, personnel files, databases, or hospital records. If a company or person is under criminal investigation, criminal liabilities may be incurred because the Federal Rules of Evidence was not adhered. If the company, law enforcement or individual does not preserve the evidence it may result in case law supporting a separate claim for spoliation or destruction of evidence. This article documents the cases of, (1) Jackson v. Michael Reese Hospital and Medical Center, 294 Ill.App.3d 1, 18, 689 N.E.2d 205 (1st Dist. 1998), (2) Procter & Gamble Co. v. Haugen 179 F.R.D. 622, D.Utah, 1998, (3) Linnen v. Robins 1999 WL 462015, 10 Mass.L.Rptr. 189 (Mass Super. Court, 1999), (4) Telecom Intern. America, Ltd. v. AT & T Corp. 189 F.R.D. 76, S.D.N.Y., 1999, and (5) Lexis-Nexis v. Beer 41 F.Supp.2d 950 (D.Minn., 1999), and (6) Texas Supreme Court cases, Trevino v. Ortega and Malone v. Foster. These court cases illustrate how spoliation of evidence can have an impact on the judge’s decision. Spoliation is a criminal act in the United States under Federal and most State law.

Spoliation of Digital Evidence

Spoliation of digital evidence is one of the fastest growing areas of the law. Cases on the subject are delivered by courts in jurisdictions all over the world daily. Knowing the law in this important area can save a digital evidence expert’s client literally millions of dollars in sanctions. According to Marcella and Menendez (2008) “Spoliation refers to the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in a pending or reasonably foreseeable litigation; in some courts, the failure to suspend a document destruction policy when litigation is anticipated may constitute spoliation” (p. 50). In layperson language, it is the act of destroying or suppressing evidence.

The purpose for article was to research some of the recent digital evidence spoliation cases and write a summary, briefly explaining and discussing one of the cases you read that you think is important. This article also explains why the author thinks these cases are important.

Jackson v. Michael Reese Hospital and Medical Center, 294 Ill.App.3d 1, 18, 689 N.E.2d 205 (1st Dist. 1998)

Michael Jackson was born with serious medical problems. His parents filed a medical malpractice action against several defendants in 1985. They voluntarily dismissed the claims and filed an amended complaint in 1991, alleging negligent spoliation of evidence against Michael Reese Hospital and Medical Center when hospital officials revealed that a warehouse flood destroyed x-rays vital to the case (Appellate Court of Illinois, First District, First Division, 1997). The Illinois Supreme Court held that an action for negligent spoliation of evidence can be established under existing negligence theories. The hospital was being sued for malpractice however; the District court dismissed the suit because the evidence had been destroyed (Appellate Court of Illinois, First District, First Division, 1997).

According to Case Law, “In its June 3, 1996, order, the trial court denied plaintiffs' motion to reconsider the dismissal of the first amended complaint, which asserted a claim under the X-Ray Retention Act. The court granted defendant's section 2-619 motion to dismiss for failure to attach a certificate of merit under section 2-622, and granted defendant's section 2-615 motion to dismiss for failure to state a cause of action for negligent spoliation of evidence” (Appellate Court of Illinois, First District, First Division, 1997).
P & G sued competitor and competitor's distributors for spreading rumors of P & G's Satanism, specifically alleging defamation, unfair competition, violations of Lanham act, Utah Truth in Advertising Act, etc. Judge Kimball dealt with various motions here, including sanctioning P&G for failing to preserve relevant emails, and allowed P&G to do a keyword search of Defendant's database on issues concerning agency or control in general, but limited search so that it would not yield general commercial or competitive information.

Fen-Phen litigation. Defendant Wyeth failed to preserve emails and then fails to turn over all emails and database info requested in discovery and subject to court order. This memo orders production of relevant emails by Wyeth and imposes costs of production on Wyeth. Also sanctions Wyeth and allows spoliation inference to jury for Wyeth's destruction of emails. Refers to "inexcusable conduct" by Wyeth several times. The court was sympathetic to the plaintiffs. “It granted the second and fourth sanctions. It denied the first because it would allow evidence that was too far-reaching, and it denied the fourth based on the fact that it was Wyeth or its counsel that was being uncooperative. Nonetheless, the strictly-worded language clearly indicated that the judge shared the plaintiffs' concerns about Wyeth's lack of cooperation” (Cyber Law Harvard, 1999). According to Marcella and Menendez (2008) the defendant was ordered to pay cost and feed to the plaintiff for failing to promptly provide the documents to the plaintiff (p. 321).

In a discrimination claim, order-sanctioning AT&T for failing to preserve records of long-distance calls in its database after specific discovery request had been made. The court ruled that specific request put AT&T on notice of relevance of records and thereafter, AT&T had a duty to preserve.

Lexis-Nexis sued an employee for misappropriation to trade secrets. A temporary restraining order required the employee to turn over copies of databases he made when he resigned. Beer, the employee, made a copy of the database and deleted several files; many that were related to the non-compete agreements. The employer moved for sanctions, claiming the employee had destroyed critical parts of the databases to avoid discovery. The court found that sanction of drawing inferences against employee for missing info was not appropriate; however, the courts stated the actions committed by him warranted some monetary sanctions for Lexis-Nexis, and in some of the charges such as Trade Secrets no monetary award was provided because the files had been deleted from the database. The forensic expert in the case was only able to access that files had been deleted, but the files were unrecoverable (State of Minnesota Court of Appeals, 2006).

Texas Supreme Court cases, Trevino v. Ortega and Malone v. Foster.
The Texas Supreme Court recently ruled in Trevino v. Ortega and its companion case, Malone v. Foster, that Texas does not recognize the independent tort of spoliation. In the Ortega decision the majority reasoned that destroying evidence is an evidentiary issue similar to perjury or is best dealt with within the context of an underlying lawsuit. In Ortega, the plaintiff filed a suit against his doctor's physician for intentional spoliation of evidence (medical records of daughter's birth). The trial court granted the defendant's special exception based on failure to state a claim. On the review, the Corpus Christi Court of Appeals reversed and remanded the trial court decision stating that there was an independent tort of spoliation (Supreme Court of Texas, 1998). The Supreme Court, however, reversed the appellate court's decision and rendered judgment. Though the Supreme Court ruled against the plaintiff on his spoliation cause of action, he still had a separate cause of action for medical malpractice pending at the time of the Appellate decision.(Supreme Court of Texas, 1998).

Author’s thought on the Importance of the Cases
Spoliation of evidence is something that is proven by way of a motion or declaration to the court. One party in the lawsuit requests a sanction be imposed on the party that cannot provide pertinent evidence. These articles are important because a failure to provide electronically stored information could result in the courts not providing sanctions. If a prosecutor or a defendant's attorneys fail to present to a court the digital evidence this could result in a case dismissal, or limited monetary award. Additionally, spoliation has two consequences: (1) the act is criminal by statute and may result in fines for the parties who engaged in the spoliation, and (2) case law has established that proceedings that might have been altered by the spoliation may be interpreted under a spoliation inference (Marcella & Menendez, 2008).
'Kill Switch' to Mitigate Memcached DDoS Attacks — Flush 'Em All


Security researchers have discovered a "kill switch" that could help companies protect their websites under massive DDoS attack launched using vulnerable Memcached servers. Massive Memcached reflection DDoS attacks with an unprecedented amplification factor of 50,000 recently resulted in some of the largest DDoS attacks in history.

To make matter even worse, someone released proof-of-concept (PoC) exploit code for Memcached amplification attack yesterday, making it easier for even script kiddies to launch massive cyber-attacks.

Despite multiple warnings, more than 12,000 vulnerable Memcached servers with UDP support enabled are still accessible on the Internet, which could fuel more cyber-attacks soon.

However, the good news is that researchers from Corero Network Security found a technique using which DDoS victims can send back a simple command, i.e., "shutdown\r\n", or "flush_all\r\n", in a loop to the attacking Memcached servers in order to prevent amplification. Where, the flush_all command simply flush the content (all keys and their values) stored in the cache, without restarting the Memcached server.
The company said its kill-switch has efficiently been tested on live attacking Memcached servers and found to be 100% effective, and has already been disclosed to national security agencies. Based on this finding, security researcher Amir Khashayar Mohammadi—who focuses on malware analysis, cryptanalysis, web exploitation, and other cyber-attack vectors—has created and released a simple DDoS mitigation tool, dubbed Memfixed, that sends flush or shutdown commands to the vulnerable Memcached servers. Written in Python, Memfixed automatically obtains a list of vulnerable Memcached servers using Shodan API to trigger shutdown/flush commands.

### Stealing Sensitive Data From Memcached Servers

What's more? Corero Researchers also claimed that the Memcached vulnerability (CVE-2018-1000115) is more extensive than initially reported, and can be exploited beyond leveraging it for a DDoS attack. Without revealing any technical detail, the company said the Memcached vulnerability could also be exploited by remote attackers to steal or modify data from the vulnerable Memcached servers by issuing a simple debug command.

Dynamic database-driven websites use a Memcached application to improve their performance by caching data and objects in the RAM. Since Memcached has been designed to be used without logins or passwords, attackers can remotely steal sensitive user data it has cached from its local network or host without requiring any authentication. The data may include confidential database records, emails, website customer information, API data, Hadoop information and more.

"By using a simple debug command, hackers can reveal the 'keys' to your data and retrieve the owner’s data from the other side of the world," the company said. "Additionally, it is also possible to maliciously modify the data and re-insert it into the cache without the knowledge of the Memcached owner."

Server administrators are strongly advised to install the latest Memcached 1.5.6 version which disables UDP protocol by default to prevent amplification/reflection DDoS attacks.

---

### How the Governance Process Can Shape Good Ethical Policy

**Author: Dr. Cheryl Cooper, CISSP, with Kansas City ISSA**

The governance process can be used to help shape good ethical policy and behavior through oversight. According to Reynolds (2012) governance is necessary to prevent major scandals; and tougher laws have been implemented in an attempt to avoid scandals, such as the Sarbanes Oxley Act of 2002. For example, in the case of Countrywide Mortgage/Financial companies the board of directors knew of the unethical conduct. The reason for the housing collapse that caused a recession between 2007 and 2012 was due to the financial institutions issuing sub-prime loans, and loans with adjustable mortgage rates. Countrywide in other words issued loans to homeowners that were not qualified (Reynolds, 2012). Additionally, when Countrywide over appraised homes, when the housing market begin to adjust home owners were not able to refinance their homes because they owned more on the home than the home was
worth. One of the causes of this was a lack of housing policies and government regulation. There were also structural weaknesses in the financial arena due to a lack of regulation and supervision. These issues could have been avoided with corporate governance in which the financial institutions conducted reckless behavior without anyone or any entity to stop them. In reference to investment banks back around 2007 these financial institutions were self-regulated; implementation of a governance program would have prevented the unethical issuance of false credit ratings and borrowing of monies which resulted in the collapse of the housing market and mortgage fraud.

The Sarbanes Oxley Act of 2002 was signed into a federal law July 30, 2002 by former President George Bush. The law was named after Senator Paul Sarbanes and Representative Michael Oxley who drafted the act. The law applies to all public companies in the United States (SOXs Online, 2012). The purpose or intent of the act was to create reforms to enforce corporate responsibility. The act creates reforms for financial accounting and was created to prevent or reduce accounting fraud. As a part of the act the Public Company Accounting Oversight Board (PCAOB) was created to manage the actions of the auditing activities to protect investors (U.S. Security and Exchange Commission). Congress thought the act was necessary due to a number of corporate financial scandals such as Enron, WorldCom, and Tyco. Congress also found there was a need to increase board of director oversight and to improve financial accounting activities. WorldCom, Tyco, and Enron had one thing in common, skewed, fraudulent, and misrepresented financial accounting records (SOXs Online, 2012). The document outlines corporate board responsibilities and penalties for failing to adhere to the law. Prior to SOX’s auditing firms were self-regulated; there was no oversight.

Two key points covered under the law are; (1) In section 302 it requires that the accuracy of the reported financial statement be certified by senior management, section 302 addresses “Corporate Responsibility for Financial Reports” and (2) in section 404 there is a requirement to establish internal controls and reporting methods on the competence of those controls, these controls must be implemented by management and auditors. Section 404 pertains to “Management Assessment of Internal Controls” (Sarbanes Oxley Act 2002). If I had to provide a correlation in good ethical design it would be the law was designed to improve financial and corporate governance and accountability to protect consumers and investors.

Governance is not just about rules and regulations. It is about corporate culture and the way a company conducts its business in an ethical, responsible way. “Tone at the top” is an often-used term because it captures the essence of where a commitment to responsible business behavior begins: with the CEO. From the top, the executive team follows the chief executive’s lead in fostering a strong ethical environment in their various dealings with employees, customers, suppliers, investors, creditors, insurers, regulators, competitors, auditors and other stakeholders. Countrywide had a world-class code of conduct. Words mean little by themselves.

Countrywide’s former CEO, Angelo Mozilo, along with David Sambol, its president, and Eric Sieracki, the CFO were charged in the Countrywide mortgage scandals for failing to reveal to investors the truth about Countrywide’s practices of backing subprime risky mortgages. The governance process through corporate governance could have been used to ensure the company’s financials were transparent to their investors. A solid governance process can aid in ensuring the CEO’s, CFOs and employees make ethical decisions to prevent unfavorable publicity. Moreover, the board of directors is responsible for careful management and management of the company’s activities for the benefit of all stakeholders and the organization (Reynolds, 2012).

In the case example of Countrywide, had the board of directors’ implemented teams and assigned responsibilities to committees to oversee the day-to-day management and operations, the collapse and bailout of Countrywide could have been avoided.

References


ISSA Kansas City Chapter Mentor Program in 2018!

The program is designed to formalize relationships between more senior professional individuals in the chapter (Mentors) and the various levels of security professionals seeking entry or moving through the different phases of this profession (Mentees). Since 2018 is the pilot year for this program for our chapter we need your participation to make it successful! The ISSA KC Board of Directors are working aggressively to launch the program. WATCH THE NEWSLETTER FOR UPDATES.

Call for Mentors & Mentees
Complete and submit a Mentor/Mentee application:

Mentor Application
Mentee Application

Why should I be a mentor?
Contribute to the professional development of the future workforce;
Help build stronger community fabric;
Impart the principles of an experienced security professional;
Gain a broader view of your own community; and
Give something back to the profession!

Mentor Criteria:
Must actively participate and support chapter events
Must be a current or recently retired security practitioner
Must be willing to commit to the Mentoring Program for a specified period of time

How will I be able to sign up?
We will be accepting applications for Mentors throughout the year. If you are interested reach out to Cheryl Cooper for more detail, vp@kc.issa.org. Complete and submit a Mentor application at www.kc.issa.org
March 2018
Volume 16 - Issue 3, Members: please click on the following Journal issue links for access:
Computer: Bluetoad - PDF; Mobile: ePub - Mobi

Feature articles include:

- Security in Mergers and Acquisitions | Miriam T. Levenstein – ISSA member, Capitol of Texas Chapter
- The Basics of Privileged Access Management | Michael Rogers – ISSA member, Minnesota Chapter
- Baking an IT Risk Program from Scratch | Steve Horstman – ISSA member, Fort Worth Chapter
- Orchestrating the Responses Between Information Security and Privacy During a Data Breach | David R. Jackson – ISSA member, National Capital (Washington, DC) Chapter
- Dilemmas of a Security Architect: How to Protect Critical Systems without Disrupting Continuity of Their Services | Mariusz Stawowski – ISSA Senior member, Poland Chapter

Not a member? Read this month’s feature article - Security in Mergers and Acquisitions - at no charge or Join Now and gain full access to the ISSA Journal.

Certification Corner

ISC2 CISSP Certification 2018 Changes
For those of you with the CISSP certification, or those who are pursuing a CISSP certification, there will be changes in 2018. Effective April 15, 2018, the CISSP exam will be based on a new exam outline, and the domains and their weights will change. The delivery method will change to Computer Adaptive Testing (CAT) that provides fewer questions in less time. There will be 100 to 150 questions, versus the 250 questions that were offered on the linear fixed exam that many of us have taken. The exam will no longer be up to 6 hours to complete, but up to 3 hours, on the average of 2 hours to complete.

For more information on the changes, check out ISC2’s web site, https://www.isc2.org/Certifications/CISSP

Contact: Nicole, Director of Education/Certification, at certification@kc.issa.org
Contact: Mark Waugh, ISSA Education Committee Member For CISSP,
Chapter Membership Corner

Contact: Wai Cheng, ISSA Director of Membership, Membership KC membership@kc.issa.org

Webinars/Conferences


- Interface 2018 is open for registration. The KC tour date is July 12. Other cities and dates available for those outside of KC. Free to attend. http://interfacetour.com/tour/kcm18/

On March 22, 2018 the ISSA-KC Chapter members, and other security professionals will hold a meeting at BRIO’s Restaurant in Kansas City, MO, to network and attend the monthly chapter meeting, with presentation topic.

**Speaker:** Ricky Allen, is the Vice President for Critical Start LLC and President of the South Texas ISSA chapter. He holds certifications such as SABSA Security Architecture, CISSP, CISA, and Six Sigma. Ricky previously held roles at Accenture as an executive in their strategic information security consulting practice and at HP Enterprise Security Products as the practice lead for developing Security Operations programs for ArcSight SIEM products. Ricky was focused on retail and manufacturing industries while at PricewaterhouseCoopers where he performed penetration testing and risk assessments for companies across the US. Ricky has presented at conferences such as BSides, Black Hat, API Cybersecurity, HOU.SEC.CON, SANS, Secure World, and Data Connectors. Ricky is based in Houston, TX and has a degree in Management Information Systems from Texas A&M University.

**Topic:** Zero Trust With Zero Resources

**Topic Summary:** Most security operations team are facing alert tyranny with an endless number of notifications, false positives, and distractions causing important events to fall through the cracks. Critical Start will address how a Zero Trust architecture approach can help end alert tyranny by optimizing security operations through the principle of "never trust, always verify". With Zero Trust there is no default trust for any entity, regardless of what it is and its location on or relative to the corporate network. By definition, every access attempt by a user, device, and application must be verified. But with resource constraints for both budget and qualified personnel, zero trust can potentially create a mountain of work that a strapped security team can’t handle. We’ll discuss the benefits of a zero trust strategy and how it can help you identify and contain threats that traditional known good approaches miss. We’ll also explore options to apply this approach in efficient manner that you can realistically support with a limited resources.

**Location:** BRIO Tuscan Grille, Country Club Plaza, 502 Nichols Rd, Kansas City, MO 64112

Agenda:
- 11:30 AM - 12:00 PM Greeting and registration
- 12:00 PM - 1:00 PM - Meeting & Presentation
- 1:00 PM - 1:30 PM - Questions, Answers & Networking

Menu:
- Salad Choice of Chicken, Salmon or Pasta
- Soft drinks, Iced Tea, Coffee
*Vegetarian option available, please note at registration at Brio

**Price:**
- $25.00 for ISSA Members,
- $35.00 for Guests/Non-Members
  Maximum Reservation: 35

Credit(s): 1 CPE credit

We look forward to seeing you at the event. If you have any questions about the event or how to register, please email our RSVP email, or contact the venue for directions.

Register
The Information Systems Security Association (ISSA) is an international organization providing educational forums, publications and peer interaction opportunities that enhance the knowledge, skills and professionalism. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

President
Naeem Babri
president@kc.issa.org

Vice President
Cheryl Cooper
mailto:vp@kc.issa.org

Secretary of Board
Rochelle Boyd
secretary@kc.issa.org

Newsletter Chief Editor
Cheryl Cooper
newsletter@kc.issa.org

Treasurer
Gary Kretzer
treasurer@kc.issa.org

Director of Membership
Wai Cheng
membership@kc.issa.org

Director of Education
Nicole Windholz
certification@kc.issa.org

Director of Programs
Carmen Banks
programs@kc.issa.org

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Marketing
Kristin Mehler
marketing@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney