Hello ISSA Kansas City Members and Happy September!


The ISSA and ESG (Enterprise Strategy Group) have joined forces again to launch the 2nd Annual Global Research Survey, which provides the collective voice of cyber security professionals. This groundbreaking research survey gained enormous media attention in 2016 because of the value placed on qualified responses from individuals who are experienced cyber security professionals – our ISSA members. Complete the survey now!!

ISSA International conference is October 9-11, 2017 at the Sheraton Hotel & Marina in San Diego, California. We look forward to welcoming you and over 800 of your colleagues and peers at the conference. If you have not registered yet. Please register early to save!

Please let us know how we are doing? Complete the ISSA KC bi-yearly Survey by September 29th!

Sincerely,
Naeem Babri
President, ISSA Kansas City
Using the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool

On August 24, 2017, the ISSA-KC Chapter members and other security professionals held a meeting at Hereford House restaurant to network and attend the monthly chapter meeting, on the topic “Using the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool: A Guide for Financial Institutions”. David Nelson, CISSP, from Integrity discussed the implications of the growth of cybersecurity threats to financial institutions. David discussed the newly released tool, the Cybersecurity Assessment Tool that can help institutions understand and rate their risk levels. This session covered the basics of the tool, who should use it and how it can help institutions address cyber risk. David also discussed what the tool will not do, and what institutions need to do to fill in the gaps.

Please join me in congratulating Dan LaMastres winner of the ISSA Visa $50.00 gift card.

A critical Apache Struts security flaw makes it 'easy' to hack Fortune 100 firms

Servers and data stored by dozens of Fortune 100 companies are at risk, including airlines, banks and financial institutions, and social media sites.


A critical security vulnerability in open-source server software enables hackers to easily take control of an affected server -- putting sensitive corporate data at risk. The vulnerability allows an attacker to remotely run code on servers that run
applications using the REST plugin, built with Apache Struts, according to security researchers who discovered the vulnerability.

All versions of Struts since 2008 are affected, said the researchers.

Apache Struts is used across the Fortune 100 to provide web applications in Java, and it powers front- and back-end applications. Man Yue Mo, a security researcher at LGTM, who led the effort that led to the bug's discovery, said that Struts is used in many publicly accessible web applications, such as airline booking and internet banking systems. Mo said that all a hacker needs "is a web browser."

"I can't stress enough how incredibly easy this is to exploit," said Bas van Schaik, product manager at Semmle, a company whose analytical software was used to discover the vulnerability. "If you know what request to send, you can start any process on the web server running a vulnerable application," he said.

The vulnerability is caused by how Struts de-serializes untrusted data, Mo said. An attacker can exploit the flaw to run any command on an affected Struts server, even behind a company firewall. "If the server contains customer or user data it's not hard at all to collect that data and transfer it to somewhere else," van Schaik said. The attacker can also use the server as an entry point to other areas of the network, effectively bypassing the corporate firewall and gaining access to other shielded-off areas of the company, he said.

"An attacker can use the vulnerability to find the credentials, connect to the database server, and extract all data," he said. Worse, he added, an attacker could delete data. "A creative attacker will have a field day," he said. "And even worse: The organization under attack may not even notice until it is well too late."

An exploit has been developed by the security researchers but has not been released to give companies time to patch their systems. He said that he's not aware of anyone exploiting the vulnerability but warned that he expects this to change "within a few hours" of the bug's details being made public.

"Companies may indeed scramble to fix their infrastructure," van Schaik said. A source code fix was released some weeks prior, and Apache released a full patch on Tuesday to fix the vulnerability. But many companies will be vulnerable to attack until their systems are patched.

Several government websites, including the IRS and California's Department of Motor Vehicles, along with other major multinational companies, such as Virgin Atlantic and Vodafone, use the software and are potentially affected by the vulnerability -- but van Schaik said that the list was "the tip of the iceberg." As many as 65 percent of the Fortune 500 are potentially affected by the vulnerability, said Fintan Ryan, an industry analyst at Redmonk, in an email.

Ryan said the figure was based on the known usage of Struts across the Fortune 100, such as developer metrics and hiring data. He said that Struts is used typically to sustain or augment existing applications, rather than newer web applications.

There's no specific way for security researchers or attackers to externally test if a server is vulnerable without exploiting the vulnerability. "It turns out that there is no other way than to announce the vulnerability publicly and stress how important it is that people upgrade their Struts components," van Schaik said. "There is simply no other way to reach the companies who are affected," he said.

---

**Cyber breach at Equifax could affect 143M U.S. consumers**

Kevin McCoy. USA TODAY Published Sept. 7, 2017 |

An estimated 143 million U.S. consumers could be affected by a cybersecurity attack carried out by suspected criminal hackers, national credit-reporting company Equifax said Thursday.
The unauthorized access to information for nearly 44% of the U.S. population occurred from mid-May through July 2017 and primarily involved names, Social Security numbers, birth dates, and addresses and, in some cases, driver's license numbers, the company said in a detailed announcement of the attack.

Additionally, the hackers gained access to credit card numbers for roughly 209,000 consumers, plus certain dispute documents with personal identifying information for approximately 182,000 consumers. Equifax also identified unauthorized access to limited personal information for certain United Kingdom, and Canadian residents. However, there was no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases, the company said.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do," Equifax Chairman and CEO Richard Smith said in a statement issued with the announcement. "I apologize to consumers and our business customers for the concern and frustration this causes."

The company also posted questions and answers about the incident for investors.

The news sent shares of Equifax (EFX) down nearly 9% to $130.05 in after-hours Thursday trading.

Financial regulatory filings show that three of the company's top executives sold shares of Equifax stock after July 29, the date the firm said the cyber breach was detected. On Aug. 1, Chief Financial Officer John Gamble sold shares with a market value of nearly $946,400, while Joseph Loughran, president of Equifax's U.S. Information Solutions, exercised options to sell nearly $584,100. Rodolfo Ploder, president of business unit Workforce Solutions, sold shares valued at nearly $250,500 on Aug. 2, the filings show. The three executives continued to hold tens of thousands of Equifax shares after the transactions.

News of the cyber-attack comes less than three months after the global Petya ransomware attack spread through computers across North America and Europe, affecting 65 countries. Similarly, the massive attack of the 'WannaCry' ransomware virus infected computers around the world in May.

Computer systems for the IRS, Target, and other government agencies and private companies have also been struck by cyberattacks in recent years. And Yahoo last year disclosed that information from an estimated 500 million of the internet giant's accounts was stolen in 2014.

Atlanta-based Equifax is one of the nation's largest credit-reporting companies, along with Experian and TransUnion. Equifax says it organizes and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and the company's databases hold employee data submitted by more than 7,100 employers. After discovering the electronic intrusion, Equifax said it hired an independent cybersecurity firm that has since been conducting a forensic investigation aimed at determining the scope of the electronic intrusion and the specific data accessed. Equifax also reported the attack to law enforcement agencies and is continuing to work with them, the company said.

Additionally, the company established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine whether their personal information may have been accessed and sign up for credit file monitoring and identity theft protection. The program, offered without charge to U.S. consumers for one year, includes monitoring of Equifax, Experian and TransUnion credit reports, copies of Equifax credit reports, identity theft insurance, internet scanning for Social Security numbers and the ability to lock and unlock Equifax credit reports. Separately, Equifax said the company would send direct mail notices to consumers whose credit card numbers or dispute documents were affected by the cyber breach. The company also is contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general about the incident.
Hackers stole names, social security numbers, addresses, birth dates, driver’s license numbers and approximately 209,000 credit card numbers using what Equifax is calling a “U.S. website application vulnerability to gain access to certain files.” The files affected are from May through to early July 2017 and while Equifax reports that there was no unauthorized access to core consumer and commercial credit reporting databases, Equifax also identified unauthorized access to “limited personal information for certain Canadian and U.K. residents.”

This is a major catastrophe for those affected. Unlike other breaches, it looks like this one exposes everything cyber thieves need to commit identity theft and more in your name. “For those affected, they will need to be diligent in monitoring their financial life forever,” says Kelley Keehn, personal finance expert and author of *Protecting You and Your Money – A Guide to Avoiding Identity Theft and Fraud*

So what do you do if you are one of the unlucky Canadians who are affected and how can anyone properly protect themselves from identity theft going forward?

**Put your credit file on ice**

“It’s important that people realize that more than likely their Social Security or Social Insurance number is in the hands of a criminal. In 2016 alone, there have been almost 4 billion records compromised globally,” says Robert Siciliano, CEO of IDTheftSecurity.com.

“When on a scale of one to ten, I’d say this breach is about a nine and the reason I don’t say a ten is because as far as we know the only data not involved in this hack is mobile phone numbers and biometric information,” he says.

In cases like this, both he and Keehn recommend those affected put a Fraud Alert (known as a credit freeze in the U.S.) on your credit file. This means that lenders will have to verify your identity before they can issue credit in your name. They may personally call you or require additional identification if you are trying to obtain credit in person. An initial fraud alert lasts 90 days, but if you are a victim of fraud or identity theft a fraud alert can be placed on your file for seven years with proof that incident took place. A Fraud Alert entitles you to one free copy of your credit report and once you notify one credit reporting company such as Equifax, they are legally obligated to notify the other one (TransUnion) on your behalf.

“If you don’t know if you’ve been affected, you can still put a pro-active credit alert on your file with each credit monitoring service for a small fee,” says Keehn. “Check your credit report often, keep track of your mail,— if some of it goes missing, that might be a red flag your mail is being diverted by a criminal — change all of your passwords and PINs, notify all financial institutions that you deal with and check your bank and credit card statements meticulously.” Of course, doing all this takes time, but you don’t necessarily have to do it all yourself.

**Peace of mind for a small fee**

For those who want to be extra pro-active Keehn and Siciliano both recommend investing in Identity Theft Protection.
“I know for some that might ring hollow due the fact that Equifax is one of the largest suppliers of identity theft protection services compromised, but that does not mean you shouldn’t engage in identity theft protection because you should,” says Siciliano.

Equifax isn’t the only company to offer this additional layer of protection. Companies like idAlerts will offer identity theft protection, detection and recovery services for about $20 per month, per person. This includes 24/7 monitoring of your credit file, notifications of any changes to your file, full recovery services if your identity is ever compromised and unfettered access to your credit report and credit score (Canadians are entitled to one free credit report per year).

“Security is all about layers of protection like when your mom tells you to wear multiple layers in the winter time,” says Siciliano. “The more layers you have, the more secure you’re going to be and the level of notification provided by Identity Theft Protection can give you real time insight as to how your credit is being used.” Read more, https://ca.finance.yahoo.com/news/protect-equifax-hack-165102890.html

---

The FTC’s Uber Consent Order: A Warning to Fast-Growing Companies

https://www.natlawreview.com/article/ftc-s-uber-consent-order-warning-to-fast-growing-companies

Author: Brian H. Lam and Cynthia Larose

August 23, 2017

Recently, Uber agreed to a proposed Federal Trade Commission (FTC) consent order (“Consent Order”) to settle charges in an FTC complaint (“Complaint”) regarding behavior stemming back to at least 2014. Acting Chairman Maureen K. Ohlhausen has stressed the implications this has for other companies:

“Uber failed consumers in two key ways: First by misrepresenting the extent to which it monitored its employees’ access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data,” and further explained that “This case shows that, even if you’re a fast growing company, you can’t leave consumers behind: you must honor your privacy and security promises.” Implications of the Complaint: The Complaint provides invaluable insight into the activities that the FTC considers unfair or deceptive acts that violate Section 5(a) of the FTC Act. At a high level, the FTC has alleged that:

- Uber Collected a Lot of Personal Data: Uber collects data from both transportation providers (“Drivers”) and consumers of these services (“Riders”). From Drivers, Uber collects personal information including consumer names, email addresses, phone numbers, postal addresses, profile pictures, Social Security numbers, driver’s license information, bank account information (including domestic routing and bank account numbers), vehicle registration information, and insurance information. From Riders, Uber collects personal information including names, email addresses, postal addresses, profile pictures, and detailed trip records including precise geolocation information. Furthermore, Uber also collects geolocation data describing the route of the trip from a Driver’s mobile device and associates it with a specific rider. While the collection itself was not a violation, Uber’s collection and use (or misuse) of this data formed the basis for much of the allegations that followed.
• Uber May Have Misused Personal Data: Articles published in November of 2014 alleged that Uber used what Uber termed a “God View” to display the personal information of Riders, including potentially that of journalists who had criticized Uber.

• Uber Broke Its Own Privacy Promises: The FTC alleges that Uber failed to follow through on promises it made to consumers, including those made through a November 2014 statement on its website promising that there was a “strict policy prohibiting all employees at every level from accessing a rider or driver’s data” except for a “limited set of legitimate business purposes” and that “access to rider and driver accounts is being closely monitored and audited by data security specialists on an ongoing basis.” The FTC has alleged that Uber did not cause data security specialists to closely monitor and audit internal access to consumers’ personal information, thus failing to follow its own promises.

• Uber Failed to Provide Reasonable Security for Rider and Driver Personal Information: Uber used an Amazon resource, called an Amazon S3 Datastore, to store personal information for Riders and Drivers. Via statements on its website, its privacy policy, and through customer service representatives, Uber promised that it would provide reasonable security for Rider and Driver personal information. The FTC alleges that Uber failed to provide reasonable security by allowing engineers to use a single access key instead of access keys by individual, failing to restrict access based on job function, not having a written information security program, and storing personal information without encryption, among other issues.

Uber Consent Order Obligations: The Consent Order, which will remain in effect for a 20-year period once approved, defines Personal Information broadly to mean individually identifiable information collected or received, directly or indirectly, by Uber from or about an individual consumer, and includes persistent identifiers associated with a particular consumer or device as well as precise geolocation data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information. Uber will be obligated to undertake a detailed compliance program as outlined below:

• Prohibition against Misrepresentation: Uber is prohibited from misrepresenting the extent to which it monitors or audits internal access to consumer Personal Information, as well as its protection of the privacy, confidentiality, security, or integrity of any Personal Information.

• Mandated Privacy Program: Uber must establish and maintain a privacy program for new and existing services for consumers, including protecting Personal Information, identifying foreseeable risks, and implementing appropriate controls.

• Privacy Assessments by Third Party: Uber must undertake third party assessments with each individual selected to conduct such an assessment to be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, at his or her sole discretion, with the assessment to cover the first 180 days, as well as each 2 years after for 20 years.

• Recordkeeping: Uber is required to maintain records pertinent to the order, including disseminated representations such as privacy policies, materials necessary for privacy assessments, and relevant consumer complaints.

Consent Order - Lessons Learned: Companies that interact with consumers, and collect, use, store, or transfer information, should pay close attention to the Complaint and resulting Consent Order. While every business model may present different challenges, the Complaint and Consent Order demonstrate that there are certain activities the FTC will not tolerate. Below are areas of common interest that most every company will wish to consider:

• The FTC Views Personal Information Expansively: Within the Consent Order, the FTC defined Personal Information to mean individually identifiable information collected or received, directly or indirectly, by Uber
from or about an individual, including persistent identifiers associated with a particular consumer or device as well as precise geolocation data of an individual or mobile device, including GPS-based, Wi-Fi-based, or cell-based location information. This confirms that companies should consider how they are using and protecting collected mobile device identifiers and location-based information.

- The FTC Expect Companies to understand and Follow Company Policies and Statements: FTC allegations that Uber failed to follow statements on its own website and privacy policy, as well as statements made by its own company representatives, formed a key aspect of the Complaint. Companies understandably want to be able to reassure consumers regarding Company privacy and data security measures. However, companies have to make sure to actually meet any promises made. The FTC will not tolerate companies that fail to meet their own policies and statements: As we continue to advise, say what you mean and mean what you say.

- Companies Will Not Be Excused From Responsibility for Appropriate Privacy and Security Protections by Using Third Party Vendors: Uber used an Amazon offering, specifically the Amazon S3 Data store, to store Personal Information from Riders and Drivers. Through the Complaint, the FTC alleged that Uber failed to provide reasonable security to prevent unauthorized access to Driver and Rider Personal Information stored in the Amazon S3 Data store. At times, certain companies seem to think that using a third party provider may relieve them of their responsibility to provide appropriate security. Per the Complaint, the FTC considers companies responsible for their own privacy and security protections, regardless of the use of third parties.

**Persistent Identifier Definition** - A “persistent identifier” is a piece of information “that can be used to recognize a user over time and across different web sites or online services,” such as “a cookie, an internet protocol (IP) address, a processor or device serial number, or unique device identifier”. Persistent identifiers do not identify a human being but a device or object.
Data Connector’s IT Security Conference is coming on September 21st.

DoubleTree by Hilton Kansas City - Overland Park
10100 College Blvd.
Overland Park, KS 66210

REGISTER HERE  VIEW AGENDA

Join us October 9-11, 2017 at the Sheraton Hotel & Marina in San Diego, California for solution oriented, proactive and innovative sessions focused on the Digital Danger Zone.

Each day, cyber threats become increasingly intricate and difficult to detect. Over the past year, we saw that with the rise of device connectivity came boundless opportunities for malicious hackers to attack device vulnerabilities. No cyber security professional can become an expert on these digital dangers without continued efforts to educate themselves on the industry's latest trends and technologies.
We look forward to welcoming you and over 800 of your colleagues and peers in San Diego as we discuss topics ranging from incident response to application security to business skills for the information security professional. Join us at the 2017 ISSA International Conference and we’ll help you navigate the *Digital Danger Zone*.

**Detailed Schedule**

**Click here for session descriptions**

[Register Now]
September 28, 2017 ISSA Chapter Meeting

Topic: New Era in End Point Security

Topic Summary: Taking a look at the current state of endpoint security and how we need to change our way of thinking in order to get ahead of the attackers

Speaker: Rich Perkins

Bio Highlights:
• Executive Level IT Security Professional with 25+ years of experience in Information Technology, 12+ years focused on Information Security and Risk Management.
• Co-Creator of the Wireless Aerial Surveillance Platform, an autonomous aircraft with onboard Wi-Fi, Bluetooth and Global System for Mobile Communications (GSM) penetration testing capabilities as featured on CNN’s “The Situation Room” and the November 2011 issue of Popular Science. Currently on exhibit at the International Spy Museum in Washington DC.
• Served as the Data Loss Prevention SME, setting governance and policy.
• Served as Air Force voting member on the Cross Domain Technical Advisory Board.
• Served as the Air Force voting member on the Technical Risk Rating panel certifying the technical risk of mission critical cross-domain technologies
• Served as instructor and mentor leading the EADS NA DS3 companywide CISSP mentoring program from 2006-2010.
• Created the patented Advanced Risk Management of Enterprise Security (ARMOES®) to enable automatic tracking/reporting of vulnerabilities within DODI 8500.2 compliant systems.
• Lead technical security engineer performing Accreditation Security Tests on the DoD Global Information Grid (GiG).

Location: Lidia’s Italy Restaurant, 101 W. 22nd street, Kansas City, MO. 64108

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:
Pasta Tasting Trio - A sampling of three daily-made fresh and filled pastas.  
Biscotti Platters - An assortment of house-made cookies & sweets to pass and share family style.  
Soft drinks, Iced Tea, Coffee

*Vegetarian option available, please note at registration at Brio
* Menu subject to change. **

Price:
$20.00 for ISSA Members,  
$30.00 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

Director of Social Media
Melissa Salazar
socialmedia@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
Wei Cheng
membership@kc.issa.org

Director of Education
Larry Dilley
certification@kc.issa.org

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

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Events
Dan Boethe
events@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney