LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

LACFE Spring Fraud Conference & Networking

The LACFE Spring Conference is May 21, 2024, to be held at Hungerford Nichols in Grand Rapids. Registration is now open!

Networking opportunity following the training:

Please join us for an informal networking event at Thornapple Brewing Company following the training until 7pm. An RSVP is appreciated, but not required, to help ensure we have enough space. Please RSVP by emailing Rebecca at brinkleyr@michigan.gov and include any dietary restrictions. Weather permitting, we will be on the patio.

Thornapple Brewing Company
6262 28th St SE
Grand Rapids, MI 49546

Networking is open to members and non-members, even if you didn’t attend the training. Feel free to bring a friend!

In This Issue

Fraud Talk Podcast

Fraud Examiners: The Bearers of Bad News - Amii Barnard-Bahn - Fraud Talk - Episode 142

In this month’s episode of Fraud Talk, Rihonna Scoggins, ACFE Content Manager, sits down with Amii Barnard-Bahn, an acclaimed coach for legal and compliance executives, to dissect the nuances of navigating difficult conversations as anti-fraud professionals. Barnard-Bahn outlines a six-step strategy to not only prepare the messenger but also to prime the audience, ensuring a blend of empathy and clarity. From psychological readiness to the rehearsal of delivery and understanding the influence of gender dynamics, this episode is packed with insights.

https://acfe.podbean.com/e/fraud-examiners-the-bearers-of-bad-news-amii-barnard-bahn-fraud-talk-episode-142/

UPCOMING EVENTS

LOCAL:

ACFE South Florida Chapter #11 presents
3rd Annual Golf & Fraud Training
If your LACFE registration is up to date, be sure to register as a "Local ACFE member" for a discount. The Lansing ACFE Chapter will receive a portion of registration fees for our members who attend virtually.
Webinar/In-Person
May 7, 2024
Learn more: ACFE South Florida Chapter #11 - 3rd Annual South Florida Chapter Golf Classic

ACFE SW Ohio Chapter – Refund Fraud: Have We Created a Monster?
In-Person and Virtual
Friday, May 10, 2024
12:00 PM - 2:00 PM
Learn more: https://swohacfe.org/events

The Lansing Chapter of the IIA - Breakfast and Networking with a Fraud Investigation Presentation by Dan Crowell, Senior Director of Corporate and Financial Investigations for Blue Cross Blue Shield of Michigan
In-Person
May 14, 2024 (registration ends May 7th)
8:30 am - 10:30 AM
MSUFCU - Farm Lane
4825 Mt Hope Rd, East Lansing, MI 48823
Learn more: https://na.eventscloud.com/ereg/index.php?eventid=797901&

LACFE Spring Fraud Conference - *Red-Collar, White-Collar Crime*
Presented by Frank S. Perri, JD, CPA, CFE
In-Person
May 21, 2024
8:30 – 4:30 PM
Hungerford Nichols CPAs + Advisors,
2910 Lucerne Dr. SE
Grand Rapids, Michigan 49546
Learn more: https://www.lansingacfe.com/?page_id=90

Save the Date: SAAABA 2024 Annual Business Seminar
If your LACFE registration is up to date, register at SAAABA's member rates through our reciprocal member relationship with SAAABA. Contact LACFE President Mark Lee at president@lansingacfe.com and let him know you will be attending.
Virtual
June 6, 2024
8:00 am - 4:40 PM
Details to come soon: Events3 | SAAABA

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at newsletter@lansingacfe.com

The Lansing Chapter of the Association of Certified Fraud Examiners

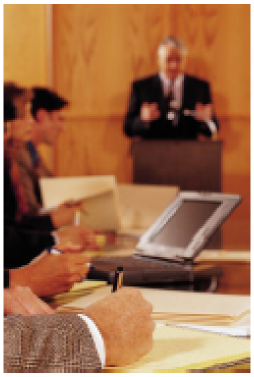
Spring Fraud Conference

Tuesday, May 21, 2024

Red Collar Crime

Presented by Frank S. Perri, JD, CPA, CFE

Hosted by Hungerford Nichols CPAs + Advisors,
2910 Lucerne Dr. SE Grand Rapids, Michigan 49546



CONFERENCE DETAILS	
Sign In:	8:00 am – 8:30 am
Conference:	8:30 am – 4:30 pm
Conference Fee:	Chapter members $160, Non-members $195
Lunch Included:	12:00 pm – 12:45 pm
Registration:	Through Friday, May 17, 2024
CPE Credit:	8 Hours
Dress:	Business Casual

Considerations for Operational Technology Cybersecurity

April 30, 2024
https://thehackernews.com/2024/04/considerations-for-operational.html

Operational Technology (OT) refers to the hardware and software used to change, monitor, or control the enterprise's physical devices, processes, and events. Unlike traditional Information Technology (IT) systems, OT systems directly impact the physical world. This unique characteristic of OT brings additional cybersecurity considerations not typically present in conventional IT security architectures.

The convergence of IT and OT

Historically, IT and Operational Technology (OT) have operated in separate silos, each with its own set of protocols, standards, and cybersecurity measures. However, these two domains are increasingly converging with the advent of the Industrial Internet of Things (IIoT). While beneficial in terms of increased efficiency and data-driven decision-making, this convergence also exposes OT systems to the same cyber threats that IT systems face.

Unique Cybersecurity Considerations for OT

Real-time requirements

Operational Technology systems often operate in real-time and cannot afford delays. A delay in an OT system could lead to significant operational issues or even safety hazards. Therefore, OT cybersecurity measures that introduce latency, such as multi-factor authentication, just-in-time access request workflows, and session activity monitoring, may not be suitable for OT environments.

Note that the impact of these features on system performance can vary based on the specific PAM solution and how it's configured. Therefore, it's crucial to thoroughly test any PAM solution in a real-time environment to ensure it meets performance requirements while still providing necessary security controls.

Legacy systems and connectivity

Many Operational Technology systems are still old in the tooth. They're proprietary and customized to meet the needs of longevity and resilience under harsh conditions. Cybersecurity was not a high-priority consideration for legacy OT systems, so they lack resilience against contemporary OT cybersecurity threats, resulting in high risk.

They may lack basic security capabilities such as encryption, authentication, and Multi-Factor Authentication (MFA.) Modernizing these systems presents significant challenges in terms of cost, operational disruptions, and compatibility issues. People with knowledge and skills may not be available, making understanding the design and the code impossible.

With the increasing integration of these systems into IT networks and, occasionally, the internet, their susceptibility to cyber threats is amplified. While beneficial for operational efficiency, this connectivity inadvertently expands their attack surface, thereby escalating their vulnerability.

Some examples of unique security challenges include:

- Outdated Hardware and Software: Obsolete hardware and software introduce significant security challenges due mainly to incompatibility with modern off-the-shelf security solutions and best practices. This exposes legacy OT systems to unauthorized surveillance, data breaches, ransomware attacks, and potential manipulation.
- Lack of Encryption: Encryption is crucial for safeguarding sensitive data and communications. Nonetheless, older OT systems might not have the capability to support encryption, which exposes them to attacks that could jeopardize the confidentiality and integrity of data.
- Insecure Communication Protocols: Legacy OT systems may use insecure communication protocols that attackers can exploit. For example, Modbus, a widely used communication protocol in legacy OT systems, does not include authentication or encryption, making it vulnerable to attacks.
- Limited Ability to Implement Cybersecurity Controls: Traditional OT systems frequently have a restricted capacity to apply cybersecurity measures. For example, they might have been provided before the importance of cybersecurity was recognized and managed by OEMs, complicating their security.
- Third-Party Remote Connections: Older OT systems might support remote connections from third parties to manage OT devices linked to an internal network. Intruders can target a network established by a vendor and exploit it to contaminate other devices.
- Lack of Security Awareness: Operators and technicians who manage legacy OT systems may lack security awareness and training, making them vulnerable to social engineering attacks.
- Embedded or Easy-to-Guess Credentials: Certain OT devices, such as those in the IoT category, might possess inherent or predictable passwords, along with other potential design shortcomings.

Safety and reliability

In Operational Technology environments, the primary focus is maintaining the safety and reliability of the physical processes they control. This is a significant departure from traditional IT environments, where the focus is often on the confidentiality and integrity of data.

- Safety: OT systems control physical processes that can have real-world consequences if they malfunction. For example, in a power plant, a failure in the control system could lead to a shutdown or even a catastrophic event. Therefore, ensuring the safety of these systems is paramount.
- Reliability: OT systems must be available and function correctly to ensure the smooth operation of physical processes. Any downtime can lead to significant operational disruptions and financial losses.

In contrast, in OT environments, confidentiality (preventing unauthorized access to information) and integrity (ensuring that data remains accurate and unaltered) often take a backseat. While these elements are significant, they usually don't hold as much weight as safety and reliability.

This order of priority can affect the implementation of cybersecurity measures. A cybersecurity action that safeguards data (boosting confidentiality and integrity) but jeopardizes the dependability of an OT system might not be deemed suitable. For instance, a security patch could rectify a known vulnerability (improving integrity), but you might consider it unsuitable if it results in system instability (undermining reliability).

While many cybersecurity best practices and frameworks focus on traditional IT environments, OT can also benefit. For example, OWASP Top 10 addresses web application cybersecurity concerns such as injection, broken authentication, sensitive data exposure, and security misconfigurations, which are common vulnerabilities that can also be found in OT environments. OWASP also has a separate list for the Internet of Things (IoT), which is often a significant component of OT environments.

Cybersecurity strategies in OT environments must be carefully designed to balance the need for safety and reliability with the need for data confidentiality and integrity

Thus, cybersecurity strategies in OT environments need to be carefully designed to balance the need for safety and reliability with the need for data confidentiality and integrity. This often requires a different approach than traditional IT security, focusing more on minimizing disruptions to physical processes. It's a delicate balancing act that requires deep knowledge of operational processes and potential cyber threats.

Securing OT environments requires a different approach compared to traditional information technology security. It requires understanding OT systems' unique characteristics and requirements, as well as designing cybersecurity measures that can protect them without compromising their operation.

As IT and OT continue to converge, the importance of OT cybersecurity will only increase. The use of encryption is crucial for safeguarding sensitive data and communications. Nonetheless, older OT systems might not have the capability to support encryption, which exposes them to attacks that could jeopardize the confidentiality and integrity of data.

What does cybersecurity like this cost? Not as much as you think. Get a quote for the easiest-to-use enterprise-grade PAM solution available both in the cloud and on-premise.

Fresh Phish
CLICK HERE!
IT
TIM RICKARD
... AND **THIS** CYBER SECURITY TOOL ELIMINATES THE **HUMAN** FACTOR!

Navigating Dangerous Waters

April 23, 2024
By Clarisse Persia, CFE
https://www.acfeinsights.com/acfe-insights/navigating-dangerous-waters

Since the 15th century, the maritime industry has flourished thanks to the trade of exotic spices and later the slave trade. In the 17th century the establishment of the Dutch East India Company (VOC), the world's first multinational corporation, privatized maritime trade, bringing the logic of profit to the seven seas. According to the UN Conference on Trade and Development, in 2023 maritime trade accounted for over 80% of international trade, carried out by vessels flagged and owned by different countries and manned by international crews. The multiple jurisdictions involved and the distance to land contribute to making maritime trade prone to the exploitation of labor, environmental and human rights laws, as we will see shortly.

Not All Flags Are Equal

Since ancient times, “false flags” were used by traders and pirates to hide a vessel’s intended use or destination. The name, “flag of convenience” can be traced back to the 16th century when English traders illegally used the Spanish flag to circumvent trade restrictions. Today, flying a flag of convenience means that the owner has registered the vessel in a country other than their own. Typically, the flag state offers advantages such as fewer regulations, lower employment requirements, and thus cheaper labor, lower or no registration fees and taxes.

This practice began in the 1920s when U.S. ships registered in Panama to smuggle alcohol during Prohibition. According to Lloyd’s List ranking of largest flag states, in 2023 Liberia became the largest flag state, followed by Panama. These open registries guarantee anonymity to the owners, making it difficult for them to be held accountable. In Europe, the Maltese flag has become the most common flag allowing registration irrespective of nationality, low registration and tonnage tax.

‘’Part of the Crew, Part of the Ship’’

One of the main benefits of having a flag of convenience is that it allows vessels to circumvent stricter labor laws. A July 2023 guidance by the International Transport Workers’ Federation (ITF), a trade union federation, reported extreme cases concerning seafarer abandonment, abuse and human trafficking in the shipping industry. MSC Cruises was convicted by a Brazilian Labour Court in 2015 for exploiting 11 crew members. In 2012, P&O Cruises hit the headlines over its crew who was paid a basic salary of 75 pence per hour, while in 2023 Carnival UK was reported to have threatened to fire 919 of its staff if they refused to take pay cuts.

Environmental Crimes

Two case studies included in a report by ITF Global reveal how flags of convenience are exploited to commit criminal activity. In 2011, Spanish shipowner Antonio Vidal Pego was found guilty in the U.S. for illegally importing toothfish and obstructing justice. His affiliated company Vidal Armadores SA owned or operated five fishing vessels, two of whom were registered to North Korea, after being renamed and reflagged multiple times. UN Food and Agriculture Organization (FAO) tons of fish yearly amounting to USD 10–23 billion as of 2016.

With mounting concerns for environmental pollution, a 2020 study by the International Maritime Organization revealed that shipping accounted for 2.89% of global manmade emissions in 2018. A high-profile pollution case involved the Maltese-flagged tanker Erika, which sank off the coast of France pouring 30,000 tons of fuel in 1999. In 2008 a French tribunal ruled against multiple defendants including its owner, Italian financier Giuseppe Savarese, who hid behind a layer of Liberian and Maltese companies. French courts' efforts to hold the Malta Maritime Authority accountable failed because it is subject only to Maltese laws.

Shadow Fleets and Ghost Ships

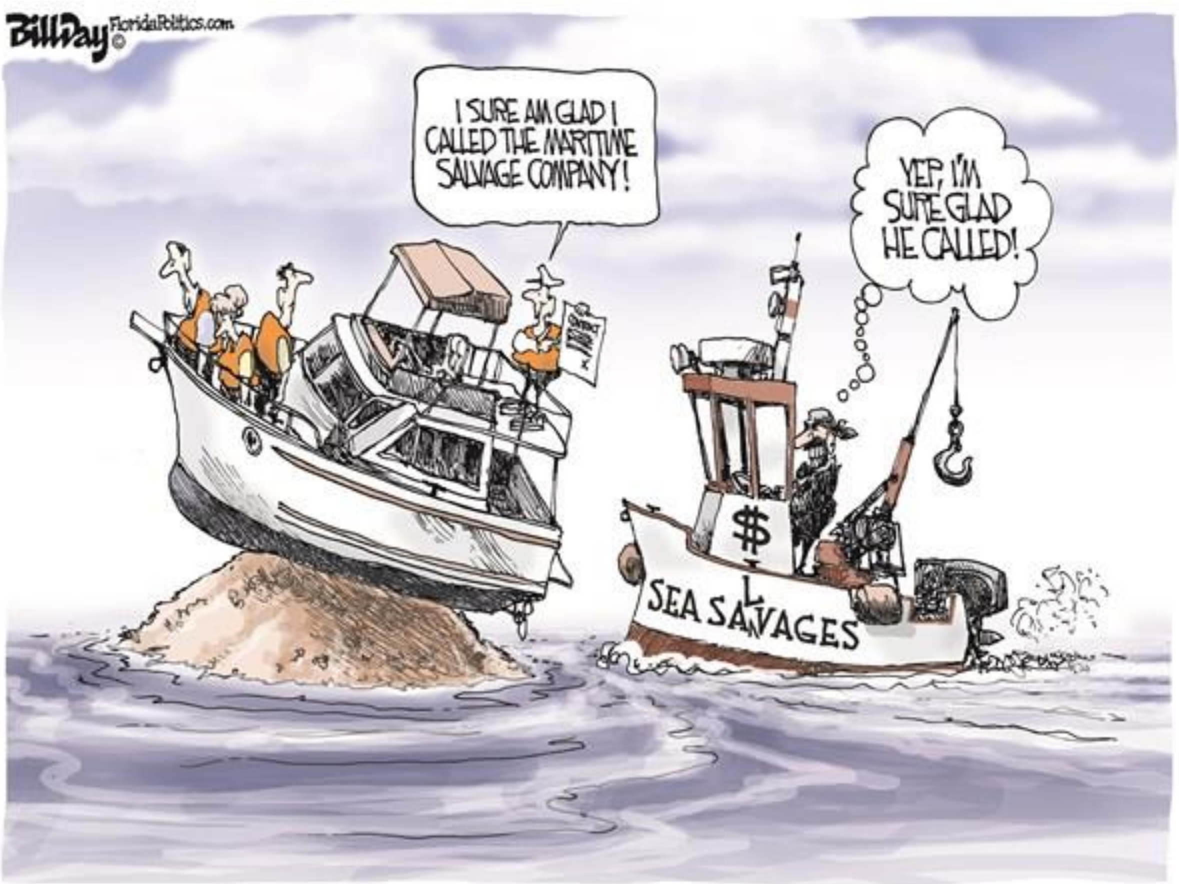
After the 2022 invasion of Ukraine, Russia has relied on a network of companies, based in Dubai and the EU (the Spanish enclave of Ceuta and Greece) to transport Russian crude oil. These vessels often turn off their navigation systems to hide the fact they are docked at Russian ports or take on fuel from other tankers at sea to obscure their origins. The EU prohibits the docking of vessels suspected of buying oil exceeding the USD 60 barrel cap imposed by the G7 countries in 2022. The problem is that much of the product is headed for China and India.

Apart from oil, illegal fishing is another major issue. In 2017 the UN Security Council sanctioned North Korea following a ballistic missile test it conducted in November 2017 and penalized North Korea by not allowing it to sell fishing rights in its waters in exchange for foreign currency. Chinese vessels fishing illegally in North Korean waters under false names, stolen identification numbers and ship-to-ship transfers at sea. Most of these vessels sail under flags of convenience.

Maritime Insurance Fraud

The 1900 Dutch play *Op hoop van zegen* is about a Dutch ship owner sending an unsound fishing boat out into a stormy sea, with the deliberate result that it sinks with the owner pocketing the insurance money. Although this is just a play, one of the most clamorous real-life cases involved *Achille Lauro,* the Italian ship known as the "Queen of the Seas", that sank near Somalia in 1994 after three fires broke out, of which two were suspicious. For this, there was talk of insurance fraud and a mysterious instigator. Until this day there is no proof of this.

Another famous case was reported by *Bloomberg* in 2022 and involved the oil tanker *Brillante Virtuoso*, which was hijacked and set on fire in July 2011 by pirates as it drifted through the Gulf of Aden. Shortly after David Mockett, a maritime surveyor, inspected the vessel, he was killed in a car bombing. The incident left a consortium of British and American insurers having to pay ~USD 100 million to Marios Iliopoulos, the Greek owner of the vessel. In 2016 he was arrested by British police on suspicion of fraud. To this day he has not been charged.


BillDay FloridaPolitics.com ©
I SURE AM GLAD I CALLED THE MARITIME SALVAGE COMPANY!
YEP, I'M SURE GLAD HE CALLED!
$
SEA SA L VAGES

Quote of the Month

“Everyone you’ll ever meet knows something you don’t.”

– Bill Nye, an American mechanical engineer, science communicator, and television presenter.