LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Cybersecurity is one of the largest threats that companies, governments and organizations have to overcome. Perhaps your organization has provided specialized training, maybe you learned best practices by seeking out information, or someone in another department is in charge of maintaining security so you believe your organization is relatively secure? Whichever way you answered, the following facts are startling:

- The rate of cybercrime increased by 600% during the COVID-19 pandemic.
- The total cost of all cybercrime damages in 2021 is expected to amount to about $6 trillion worldwide.
- The financial sector suffered the largest financial losses in 2020. Financial institutions took an average of 233 days (approximately eight months) to detect and address data breaches affecting their systems.
- A staggering 90% of healthcare staff in 2020 did not receive any updated training on cyber security best practices after the COVID-19 pandemic forced them to work from home.
- Although 95% of organizations provide phishing awareness training, 30% trained just a portion of their user base. 78% of organizations say their security awareness training activities resulted in measurably lower phishing susceptibility, but 31% of employees failed a phishing test.

More compiled statistics on cybercrime/cybersecurity: [26 Cyber Security Statistics, Facts & Trends in 2022 (cloudwards.net)]

In This Issue

Fraud Talk Podcast

Crossed Wires: Unraveling the Relationship Between Cybersecurity and Fraud - Roderick Chambers- Fraud Talk - Episode 122

The intersection of cyber security and fraud examination is ever-expanding in our new technological landscape. At the 33rd Annual ACFE Global Fraud Conference, ACFE Research Manager Mason Wilder, CFE, and Deputy Superintendent and Director of the Intelligence Unit at the New York Department of Financial Services (NYDFS), Roderick Chambers sat down to discuss the importance of technical controls and knowledge to protect your organization from fraud.

https://acfe.podbean.com/e/crossed-wires-unraveling-the-relationship-between-cybersecurity-and-fraud-roderick-chambers-fraud-talk-episode/

UPCOMING EVENTS

LOCAL:

ACFE South Florida Chapter #11 presents
Asset Tracing: Finding the Truth Behind the Numbers
Webinar
September 22, 2022
12:00 – 1:30 pm
Learn more: https://acfesouthflorida.org/event-4829232 and see poster below!

The Twin Cities and Georgia ACFE Chapters present a seminar to discuss the psychology of a fraudster, the importance of data in healthcare, and cognitive biases to set the stage for the "Bad Blood" story
Zoom Seminar
November 9, 2022
11:00 – 4:15 pm
When registering, LACFE Members should select the Other ACFE Chapter (or other participating organization) Member Ticket and enter the name of their Chapter or participating organization.
Learn more: https://twincitiescfe.org/meetinginfo.php?id=63&ts=1656693218 and see poster below!

Lansing Chapter of the ACFE is working on topics and to procure a speaker for the Fall Conference. Details will follow as soon as we have a date and topic.

NATIONAL:

ACFE
2022 ACFE Government Anti-Fraud Summit
Virtual
November 4, 2022 (early registration ends October 5th)
Learn more:
https://www.fraudconference.com/governmentsummit2022.aspx?_ga=2.249887365.2010161558.1661945286-1723614460.1601549018

ACFE
Detecting Fraud Through Vendor Audits
Virtual Seminar
October 26, 2022 (early registration ends September 26th)
Learn more: https://www.acfe.com/training-events-and-products/all-events/calendar-of-events/event-detail-page?s=Detecting-Fraud-Through-Vendor-Audits-1022Virt-VA

If you have an event that you would like posted in our newsletter or if you wish to share an article, please contact Jennifer Ostwald at jenny1661@hotmail.com

ASSET TRACING

FINDING THE TRUTH BEHIND THE NUMBERS

FOCUS - Estate and Trust Matters and Fiduciary Fraud

SEPTEMBER 22, 2022

12:00pm - 1:30pm

WEBINAR

FEATURED SPEAKER:

BRANDI STEINBERG

IAG Forensics & Valuation

Brandi Steinberg, CPA, CFE is a forensic manager at IAG Forensics & Valuation. She has over 10 years of experience as a tax preparer, auditor, controller, and forensic accountant. She specializes in family law, estate and trust litigation, business valuations, and complex financial analyses. She is also Vice President of the Georgia Chapter of the Association of Certified Fraud Examiners.

1.5 CPE Credits

FREE

ACFE South Florida chapter members

$25

for non-members

VIRTUAL EVENT

ACFE

Association of Certified Fraud Examiners

South Florida Chapter #11

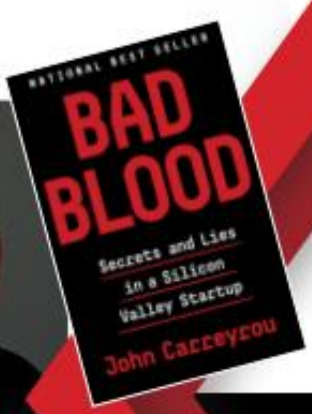
Reserve your spot today!

http://southfloridaacfe.org/event-4829232

ACFE
Association of Certified Fraud Examiners

TWIN CITIES AND GEORGIA CHAPTERS

Present:



NOVEMBER 9TH

DATE: November 9, 2022
FROM 11:00AM - 4:15PM CST
(5.25 CPE credits)

KEYNOTE SPEAKER:

- **John Carreyrou**
  – *Elizabeth Holmes Case*

- **John Gill** – *Psychology Mindset of a fraudster*
- **Rebecca Mendoza** – *It's All About the Data*
- **Mary Breslin** – *Cognitive biases*

SPONSORS:

GOLD SPONSOR:

Verracy

SILVER SPONSORS:

IDInsight

PRICES:

EARLY BIRD TIER ONE:	**July 1st-July 31st**	*Members* = **$75** | *Non-Members* = $100
EARLY BIRD TIER TWO:	**August 1st-August 31st**	*Members* = **$100** | *Non-Members* = $125
REGULAR PRICING:	**September 1st -November 4th**	*Members* = **$125** | *Non-Members* = $150

Register Now! at Twin Cities Chapter of the ACFE - Home Page
https://twincitiescfe.org

For more information on this speaker please visit **https://prhspeakers.com**

New Cybersecurity Regulations Are Coming. Here's How to Prepare.

August 29, 2022
by Stuart Madnick
https://hbr.org/2022/08/new-cybersecurity-regulations-are-coming-heres-how-to-prepare

Cybersecurity has reached a tipping point. After decades of private-sector organizations more or less being left to deal with cyber incidents on their own, the scale and impact of cyberattacks means that the fallout from these incidents can ripple across societies and borders.

Now, governments feel a need to "do something," and many are considering new laws and regulations. Yet lawmakers often struggle to regulate technology — they respond to political urgency, and most don't have a firm grasp on the technology they're aiming to control. The consequences, impacts, and uncertainties on companies are often not realized until afterward.

In the United States, a whole suite of new regulations and enforcement are in the offing: the Federal Trade Commission, Food and Drug Administration, Department of Transportation, Department of Energy, and Cybersecurity and Infrastructure Security Agency are all working on new rules. In addition, in 2021 alone, 36 states enacted new cybersecurity legislation. Globally, there are many initiatives such as China and Russia's data localization requirements, India's CERT-In incident reporting requirements, and the EU's GDPR and its incident reporting.

Companies don't need to just sit by and wait for the rules to be written and then implemented, however. Rather, they need to be working now to understand the kinds of regulations that are presently being considered, ascertain the uncertainties and potential impacts, and prepare to act.

What We Don't Know About Cyberattacks

To date, most countries' cybersecurity-related regulations have been focused on privacy rather than cybersecurity, thus most cybersecurity attacks are not required to be reported. If private information is stolen, such as names and credit card numbers, that must be reported to the appropriate authority. But, for instance, when Colonial Pipeline suffered a ransomware attack that caused it to shut down the pipeline that provided fuel to nearly 50% of the U.S. east coast, it wasn't required to report it because no personal information was stolen. (Of course, it is hard to keep things secret when thousands of gasoline stations can't get fuel.)

As a result, it's almost impossible to know how many cyberattacks there really are, and what form they take. Some have suggested that only 25% of cybersecurity incidents are reported, others say only about 18%, others say that 10% or less are reported.

The truth is that we don't know what we don't know. This is a terrible situation. As the management guru Peter Drucker famously said: "If you can't measure it, you can't manage it."

What Needs To Be Reported, by Whom, and When?

Governments have decided that this approach is untenable. In the United States, for instance, the White House, Congress, the Securities and Exchange Commission (SEC), and many other agencies and local governments are considering, pursuing, or starting to enforce new rules that would require companies to report cyber incidents — especially critical infrastructure industries, such as energy, health care, communications and financial services. Under these new rules, Colonial Pipeline would be required to report a ransomware attack.

To an extent, these requirements have been inspired by the reporting recommended for “near misses” or “close calls” for aircraft: When aircraft come close to crashing, they’re required to file a report, so that failures that cause such events can be identified and avoided in the future.

On its face, a similar requirement for cybersecurity seems very reasonable. The problem is, what should count as a cybersecurity “incident” is much less clear than the “near miss” of two aircraft being closer than allowed. A cyber “incident” is something that could have led to a cyber breach, but does not need to have become an actual cyber breach: By one official definition, it only requires an action that “imminently jeopardizes” a system or presents an “imminent threat” of violating a law.

This leaves companies navigating a lot of gray area, however. For example, if someone tries to log in to your system but is denied because the password is wrong. Is that an “imminent threat”? What about a phishing email? Or someone searching for a known, common vulnerability, such as the log4j vulnerability, in your system? What if an attacker actually got into your system, but was discovered and expelled before any harm had been done?

This ambiguity requires companies and regulators to strike a balance. All companies are safer when there’s more information about what attackers are trying to do, but that requires companies to report meaningful incidents in a timely manner. For example, based on data gathered from current incident reports, we learned that just 288 out of the nearly 200,000 known vulnerabilities in the National Vulnerability Database (NVD) are actively being exploited in ransomware attacks. Knowing this allows companies to prioritize addressing these vulnerabilities.

On the other hand, using an overly broad definition might mean that a typical large company might be required to report thousands of incidents per day, even if most were spam emails that were ignored or repelled. This would be an enormous burden both on the company to produce these reports as well as the agency that would need to process and make sense out of such a deluge of reports.

International companies will also need to navigate the different reporting standards in the European Union, Australia, and elsewhere, including how quickly a report must be filed — whether that’s six hours in India, 72 hours in the EU under GDPR, or four business days in the Unites States, and often many variations in each country since there is a flood of regulations coming out of diverse agencies.

What Companies Can Do Now

Make sure your procedures are up to the task.
Companies subject to SEC regulations, which includes most large companies in the United States, need to quickly define “materiality” and review their current policies and procedures for determining whether “materiality” applies, in light of these new regulations. They’ll likely need to revise them to streamline their operation — especially if such decisions must be done frequently and quickly.

Keep ransomware policies up to date.
Regulations are also being formulated in areas such as reporting ransomware attacks and even making it a crime to pay a ransom. Company policies regarding paying ransomware need to be reviewed, along with likely changes to cyberinsurance policies.

Prepare for required “Software Bill of Materials” in order to better vet your digital supply chain.
Many companies did not know that they had the log4j vulnerability in their systems because that software was often bundled with other software that was bundled with other software. There are regulations being proposed to require companies to maintain a detailed and up-to-date Software Bill of Materials (SBOM) so that they can quickly and accurately know all the different pieces of software embedded in their complex computer systems.

Although an SBOM is useful for other purposes too, it may require significant changes to the ways that software is developed and acquired in your company. The impact of these changes needs to be reviewed by management.

What More Should You Do?

Someone, or likely a group in your company, should be reviewing these new or proposed regulations and evaluate what impacts they will have on your organization. These are rarely just technical details left to your information technology or cybersecurity team — they have companywide implications and likely changes to many policies and procedures throughout your organization. To the extent that most of these new regulations are still malleable, your organization may want to actively influence what directions these regulations take and how they are implemented and enforced.

Video of the Month

Facts about Zelle Scams 2022 [Protection] - YouTube

We’ve got some facts about Zelle Scams, Zelle fraud in 2022. We’re here with Lynn Larson to share this newest twist on current Zelle scams. Plus, she’ll do a quick review of some of the other ways Zelle scams are perpetrated.

Three Ways Open Platforms Can Boost Cybersecurity Defenses

August 30, 2022
by Sandeep Lahane
https://www.forbes.com/sites/forbestechcouncil/2022/08/30/three-ways-open-platforms-can-boost-cybersecurity-defenses/?sh=e61c56815a6a

Open source is eating the world, with one exception: cybersecurity. While there are many cybersecurity platforms aimed at securing open source applications, there has been a void where open cybersecurity platforms should be.

Most modern applications are the result of free, open, collaborative efforts. It makes sense, then, that cybersecurity could also be rooted in the collective expertise of the community—and, with today's non-stop barrage of new attacks, the community's collective energy and wisdom.

Indeed, the real power of an open source cybersecurity platform is that it is available to all—not just large enterprises or companies with a deep cybersecurity bench—and that it benefits from the contributions of all. An open cybersecurity platform also plays an important role in educating users—security experts or not—on the importance of securing applications from development through production and beyond.

The ascent of open source has not been without its bumps. We've seen a 146% increase in ransomware attacks on Linux, and manufacturing has replaced financial services as hackers' top target as they shift their attention to IoT, according to X-Force Threat Intelligence Index.

The software supply chain developers are using is leaving the systems they are building vulnerable. A synopsis that found 78% of applications use open source reckons 81% of that code contains at least one vulnerability. And attackers are weaponizing vulnerabilities, with the software supply chain serving as an avenue for attack for two-thirds of companies, according to a 2022 report from Anchore.

Counterpunch Required

Securing the software supply chain will take a cyber defense of comparable scale and breadth. The foundations of such a defense must be community-based—and that makes open source a good option.

Some argue against an open-source approach, saying code developed in the open lets the bad actors see as much as the good guys. However, some of the most vulnerable and exploited software that runs on desktops, network appliances and servers are closed source and developed by some of the largest enterprises in the world behind closed doors.

Further, a core tenet of open source—that more eyeballs on code equal greater security—would seem to have been disproved by the rising threats. Eric Raymond, author of the seminal Cathedral and the Bazaar, stated that “given enough eyeballs, all bugs are shallow.” Translated: The security of open source is reinforced by more people looking for bugs and vulnerabilities.

But this does not work universally. It succeeds in projects with a large and dedicated community for such diligent and dedicated code review. But not every open-source component is lucky enough to attract such large or attentive followings.

Open source, however, is more than code contributions and eyeballs. It’s a model of collective development that can help cybersecurity pivot to the challenge. When looking to open source to boost cybersecurity defenses, check for three key things.

1. Knowledge Transfer

Open source has been built on the open exchange of ideas and knowledge. It eliminates needless duplication of effort and, therefore, helps drive the development, innovation and delivery of robust products and projects.

The task of collecting and analyzing data about vulnerabilities, code dependencies and attack vectors is daunting. MITRE, which publishes regular lists of vulnerabilities, now tracks more than 18,000 vulnerabilities. And it’s not just newly discovered vulnerabilities that are a problem. Vulnerabilities can lay hidden for an average of four years—plenty of time for attackers to develop their attacks before fixes arrive.

Knowledge transfer on vulnerabilities and attacks in cybersecurity would be a public service.

2. Greater Sharing Of Data To Empower More People To Act Faster

Exposed vulnerabilities often do less damage than the ones that catch everyone off guard, and information sharing in developer communities is one way to share data that can empower people to act faster.

Open standards are a hallmark of successful open source. Standards are distilled collectively rather than established de facto by one vendor or through the work of a distant committee. Standards developed openly map to practical requirements and are compelling to adopt. One promising area for open standards is the relatively new concept of a software bill of materials (SBOM)—a catalog of open-source and third-party components in a code base.

A basic tenet for an SBOM, according to analyst Gartner, is metadata that could be used to identify key attributes of those components—such as the code’s author, the supplier and any dependencies. Metadata developed as an open standard would provide the lingua franca for SBOM to be effective. This would mean software components and libraries can be tracked as they cross the supply chain and be mapped to helpful tools such as vulnerability databases.

3. A Shared Platform

Open source can bring the power of a shared platform that would help refocus the cybersecurity sector's work. Open platform is long-overdue in cybersecurity.

One reason that customers are struggling under the weight of tool sprawl is that two-thirds of security teams are working with as many as 25 unique security tools. Vendors are reinventing core components and security platforms with an overlap in features.

This is not an effective way to secure a technology infrastructure built on hundreds of components with thousands of dependencies. A more efficient approach is to converge on a common platform through plug-ins and integration using open and shared APIs.

The software supply chain our world relies on is under attack. With open source, we can bring together parties from across the community to harness their wisdom and forge a collective response.

Quote of the Month

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."

— Stephane Nappo, Global Head Information Security for Société Générale International Banking and Financial Services